



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNJU

DOKTORSKE STUDIJE
STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE

DOKTORSKA DISERTACIJA

**JEDNO REŠENJE KRIPTOGRAFSKOG
PROTOKOLA ZA REVIZIJU
INFORMACIONIH SISTEMA UZ ZAŠTITU
IDENTITETA KORISNIKA**

Mentor:

Prof. dr Mladen Veinović

Kandidat:

Viktor Polić, master

Beograd, 2014. godina



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE I MEĐUNARODNU SARADNJU

DOKTORSKE STUDIJE
STUDIJSKI PROGRAM: NAPREDNI SISTEMI ZAŠTITE

DOKTORSKA DISERTACIJA

**JEDNO REŠENJE KRIPTOGRAFSKOG
PROTOKOLA ZA REVIZIJU
INFORMACIONIH SISTEMA UZ ZAŠTITU
IDENTITETA KORISNIKA**

Mentor:

Prof. dr Mladen Veinović

Kandidat:

Viktor Polić, master
Br. indeksa: 460083 / 2010

Beograd, 2014. godina

Singidunum University Belgrade

PhD candidate Viktor Polić

Mentor Prof. PhD Mladen Veinović

CRYPTOGRAPHIC PROTOCOL FOR INFORMATION SYSTEMS AUDIT WITH USERS' IDENTITY PROTECTION

Dedicated to my wife and children,
and to their children, and all future generations and their well-being.

Key words: Cryptography, cryptanalysis, sigma protocols, zero-knowledge proofs, OR-proofs, non-interactive proofs, discrete logarithms, Witness-Hiding proofs, deniable protocols, identity protection, privacy protection, IT auditing, information security standards, e-government, e-voting, data protection legislation, privacy

Abstract: A practical construction of efficient cryptographic protocol that enables externalization of authentication from transaction processing in business information systems is proposed in this research. The construction takes advantage of efficiency and simplicity of sigma-protocols based on discrete logarithm problem. Carefully analyzed security taking into account the state of the art advances in cryptanalysis permits applicability of proposed cryptographic primitives and related security parameters in certain applications such as Internet-based voting. The focus is made on the review of data protection legislation and its practical effectiveness in identity protection to highlight the importance of technological identity protection solutions. Information systems audit is an important step in estimating the level of data protection and maturity of information systems and consequently in increasing users' confidence. However, audit of systems such as voting systems expose auditors to personally identifiable information about voters that could jeopardize some fundamental rules and regulations on voting and consequently diminish the applicability of information systems in this important aspect of e-Government. Proposed protocol offers technical solution to this problem and could be applied in other similar domains.

Contents

CRYPTOGRAPHIC PROTOCOL FOR INFORMATION SYSTEMS AUDIT WITH USERS' IDENTITY PROTECTION	2
1 Introduction.....	6
1.1 Research topic.....	6
1.2 Research objectives	8
2 Zero-knowledge proofs.....	9
2.1 Definition.....	9
2.2 Construction	12
2.3 Application	16
2.4 Importance of zero-knowledge proofs	17
3 Non-interactive Σ -protocols.....	19
3.1 Definition.....	19
3.2 Construction	20
4 OR-proof form of Σ -Protocol.....	24
4.1 Definition.....	24
4.2 Construction	25
5 Cryptographic protocol for information systems audit with users' identity protection	29
5.1 Construction	29
5.2 Cryptographic protocols prototyping and related simulations.....	30
5.3 Security analysis of the proposed protocol.....	43
6 Privacy protection in e-Government applications.....	50
6.1 Introduction to e-Government	50
6.2 European Union Data Protection Directive	54
6.3 Swiss Federal Act on Data Protection.....	57
6.4 Russian Federal Law on Personal Data	59
6.5 Serbian Law on Personal Data Protection	61
6.6 e-Government framework for assessing privacy readiness	63
6.7 Auditing e-Government applications.....	65
6.8 Applicability of the proposed cryptographic protocol in e-Government applications.....	73
7 Conclusion	79
7.1 Contribution.....	79
7.2 Further work	80
Annex I - SAGE Mathematics source code for the cryptographic protocol for information systems audit with users' identity protection	82
Bibliography	87

1 Introduction

1.1 Research topic

In the core of modern information systems lay business transaction data stored in relational, object-oriented and other types of databases. Business logic is typically implemented in software applications that perform processing and analysis of data stored in those databases. Recent trend is to link data from many heterogeneous systems into data warehouses and to perform complex analysis or data mining in order to facilitate business decision-making. Data mining process results in information about complex business relations called business intelligence and forms the basis for effective decision-making. However, data-warehouses contain much more data than needed for many business decisions. Details on information system users and participants in business transactions are not needed for every business decision. As a matter of fact, in large data warehouses those details may originate from different organizations, business environments, and geo-political jurisdictions. The exposure of this data surplus, unnecessary for decision-making, could present a risk of users' identity breach and jeopardize the security of the whole information system.

Many published cases of data confidentiality breaches illustrate that access to more data than needed expose organizations and their staff to risks at operational as well as strategic level. One example that recently attracted a lot of attention in the media is the case of a former UBS bank employee who was awarded 104 million US dollars for acting as a whistleblower and providing US authorities information on US citizens that evaded tax payments by keeping their funds in the Swiss bank.¹ This was not a unique case as many similar reports were published hitting many Swiss and other banks.² Although bank employees in many of above cases had privileged access to clients' data, this illustrates negligence in implementation of adequate preventive information security controls. Such negligence puts in question integrity of other bank employees and the whole working practice with international customers. Case like this poses the question if unnecessary large number of bank employees has access to clients' personal information due to the lack of identity protection within information systems.

Another aspect of data confidentiality protection that requires attention is related to the usage of cloud computing services. With the rise of cloud computing usage there are scenarios involving business partners with distributed responsibility in data storage and data processing. Cloud computing is based on massive virtualization of different information system components ranging from data processing, through data storage and transport, to data dissemination. In such systems geographic and organizational boundaries blur further complicating the implementation of fundamental procedural information security controls such as segregation of data access rights and rights to perform information systems audit. Business challenge to organizations is how to benefit from the economy of scale offered by cloud computing based systems and not to jeopardize fundamental principles of information security and customers confidence.³

¹ http://en.wikipedia.org/wiki/Brad_Birkenfeld

²

http://www.swissinfo.ch/eng/business/Swiss_bank_Julius_Baer_confirms_data_theft.html?cid=33387790

³ <https://cloudsecurityalliance.org>

Numerous recent research and studies focus on finding technology solutions to protect privacy of information systems users through implementations of advanced cryptographic functions and protocols. Proposed solutions mainly focus on certain information security aspects, for example users identification and authentication, protection of data integrity in storage, protection of data confidentiality in transport and so on. Holistic approach to data protection throughout the entire data life cycle and within boundaries of business transactions and not within a single technology phase is rarely efficiently integrated in practice. Nevertheless, such a holistic approach is required to minimize the access to individual data while enabling the processing of a complete business transaction and finding required information. It is also necessary to perform adequate information systems audit in order to ensure regulatory compliance, external and internal control of business practices, and maintain confidence of customers and business partners in information systems and staff that operate it and administer it. Following the breach of confidentiality social security numbers and credit card numbers of several millions taxpayers of South Carolina from the Department of Revenue it was revealed that data was not encrypted. When questioned about the case by journalists during the interview, the governor explained that data encryption is too complicated.⁴ This is not however an answer that majority of citizens would accept when using e-Government applications and providing their personally identifiable information and other confidential information.

Certain systems for identification of information system users enable protection of privacy through application of cryptographic controls based on zero-knowledge proofs. Recent cryptographic researches propose more efficient and secure construction for implementation of zero-knowledge proofs. Externalization of users identification from data storage and data processing increases complexity of information security requirements. Complex cryptographic protocols and management of large number of public and private cryptographic keys are challenge to secure implementation and open doors to many possible system vulnerabilities that increase information security risk levels. Acceptable information security solutions to above problems must be efficient, robust to known cryptanalysis attacks, with minimum possible complexity in order to reduce possibilities for side-channel attacks, and with as simple as possible cryptographic key management. Detailed analysis of security requirements from the aspect of data life cycle within the scope of specific business transaction, externalization of users identification and authentication, and minimizing data access rights based on “need to know” principle, are fundamental requirements to design adequate information security system. Throughout the design phase cryptographic primitives are carefully selected to satisfy security requirements with particular size of keys and efficient and secure cryptographic algorithms. Testing robustness and security of proposed solution is of a particular importance. The most effective testing is a peer review of the protocol within cryptanalysts community and penetration tests on the practical implementation by certified ethical hackers. The latter has a primary objective to discover technical vulnerabilities of the protocol and its components. The solution that passes these tests is ready for deployment in production systems. As new cryptanalyst techniques are discovered it is important to continuously verify security levels of the product and implement improvements.

⁴ http://threatpost.com/en_us/blogs/encryption-its-complicated-110112

1.2 Research objectives

A cryptographic protocol based on two forms of sigma-protocols unified in a construction with shared global security parameters is analyzed in this thesis both from information-theoretic and practical implementation aspect. In a proposed solution, the sub-system for identity verification is based on OR-proof form of sigma-protocol that provides identity protection. Non-interactive form of sigma-protocol constitutes the base for business transaction classification and meta-data storage sub-system. Construction of both sigma-protocol forms in these sub-systems is based on Schnorr's cryptographic schema that enables externalization and sharing of global security parameters and encryption keys in efficient way. The proposed protocol ensures identity protection during information systems audit.

Previous research in construction of cryptographic schemes for privacy protection based on zero-knowledge proofs is reviewed in the second chapter. In the third chapter previous work on sigma-protocol constructions and their applications in transaction systems are reviewed with the focus on their non-interactive form. In the fourth chapter the focus is on different solutions for protection of privacy and identity based on the OR-form of sigma-protocols. The model of the proposed cryptographic protocol is described in the fifth chapter. It is followed by the overview of modeling tools and techniques used for cryptographic protocols prototyping and simulations. Proposed protocol construction, practically implemented in the prototyping tool, is also presented in this chapter. Simulations with different security parameters are performed to support the analysis of protocol's efficiency and security. Security of cryptographic primitives is analyzed with particular attention on the latest published results of cryptanalyst research and latest industry standards for cryptographic controls.

Protecting privacy is the key for successful implementation of information systems in certain domains like e-Government. In 2011, Kessler et al [48] published the proposal for the framework for analyzing privacy protection level in the area of e-Government. The study highlights that the privacy protection within information systems is the vital element for the integration of information systems from different categories of e-Government as well as for the development of information systems for active participation of citizens such as e-Voting. Particular emphasis is placed on the technical aspects of privacy protection that enable protection of identity and controls of linking identities with particular transactions. Analyzing maturity levels of e-Government systems in Germany and Kenya the study concludes that further development is required to improve maturity levels from transaction level to integration and active participation levels.

The thesis further provides detailed review of the state of the art scientific literature that covers issues of linking identity protection technologies with the security of complex transaction information systems. Particular emphasis is made on the current regulatory requirements and industry standards in privacy protection for e-Government information systems. Finally methods for audit of e-Government information systems are overviewed with analysis of applicability of the proposed cryptographic protocol in improving maturity levels of such information systems.

2 Zero-knowledge proofs

Zero-knowledge proofs represent an interaction between the prover and the verifier in which the prover convinces the verifier that it knows the secret key to solve a complex computational problem without revealing any information about that key. Zero-knowledge proofs were demonstrated and formally defined in the eighties. Since then they have been in the focus of cryptography experts for their attribute to enforce honest communication of potentially malicious parties. Consequently, zero-knowledge proofs have become an important building block in many cryptographic schemes that require verification of the correct participation and where it is important to preserve privacy of participating parties. Zero-knowledge proofs must satisfy completeness, which means that a prover who possesses the secret key must be able to convince a verifier of its possession. They also must satisfy soundness in which a dishonest prover must not be able to convince a verifier. As it will be presented in later chapters, zero-knowledge proofs could be implemented as mitigation against certain types of cryptanalysis attacks such as chosen plaintext attacks, or chosen ciphertext attacks. Non-interactive form of zero-knowledge proofs is particularly interesting for their reduced communication overhead resulting in simplification of encryption schemes, and improvement of their performance. This is particularly important for practical implementation in mobile applications or systems that use smart cards.

Detailed overview of zero-knowledge proofs is given in Polic [57] with focus on their non-interactive form. A formal definition of non-interactive zero-knowledge proofs is given in the first part of the chapter. Different aspects are covered starting with the definition of knowledge to the definition of proof systems. Several examples of most recent proof constructions are reviewed analyzing their trust models, efficiency and security. Finally several examples of concrete applications are reviewed that are implemented using non-interactive zero-knowledge proofs.

2.1 Definition

Claude Elwood Shannon established the foundation for the information theory with his work on the mathematics of communication [56]. He represented a measure of information as the average number of bits required to store or process one symbol in a message. He distinguished the information stored in the message from its meaning. For Shannon, semantics of the message was irrelevant to the engineering problem which was to select a certain message from a set of messages and yet to receive expected amount of information. This measure of the information content Shannon called the entropy. His work in measuring information quantity and representing it with analytic expressions is used as the foundation to define zero-knowledge attributes of mathematical proofs.

Shannon's information content is used to quantify the amount of information associated with the outcome of a random variable.

An ensemble X is a triple (x, A_x, P_x) , where the outcome x is the value of a random variable, which takes on one of a set of possible values, $A_x = \{a_1, a_2, \dots, a_i, \dots, a_l\}$, having probabilities $P_x = \{p_1, p_2, \dots, p_l\}$, with

$$P(x = a_i) = p_i, p_i \geq 0 \quad (1)$$

and

$$\sum_{a_i \in A_x} P(x = a_i) = 1 \quad (2)$$

In case when a random variable is binary (i.e. the variable could have only values 0 or 1), Shannon's information content of an outcome $x = a_i$ is defined to be:

$$h(x = a_i) = \log_2 \frac{1}{P(x)} \quad (3)$$

For binary variables, entropy is also measured in bits.

As we will see from their formal definition, zero-knowledge proofs have to be simulated so that they do not carry any additional information not already transmitted through the simulation. Relation between the amount of information carried by random event and its probability is important for study and construction of zero-knowledge proofs. Further research of Shannon's information content demonstrated its additional important attributes. Information content is greater if the outcome of a random experiment is less probable as shown in MacKey [1]. This study showed further that information content is higher when the probability distribution over outcomes is uniform. Shannon's entropy is very precise in the boundary states of knowledge. These boundary states are defined as the state of total ignorance and the state of total knowledge. Samid [2] demonstrated how to quantify the knowledge gap between the state of uncertainty and a corresponding certainty by measuring Shannon's entropy. Knowledge about the outcome of an event selected from the finite set of possible random event outcomes is best described with Shannon's entropy.

Computational complexity theory is the area of theoretical computer science that focuses on the analysis of the resources needed to solve computational problems such as the problem of factoring, or the problem of computing discrete logarithms. A computational problem can be viewed as a set of instances, inputs to the problem, and corresponding solutions. A collection of problem instances is called a formal language. Computational problems are classified relative to computational models and required resources. In the research on the measure of knowledge from the aspect of the computational complexity theory Goldwasser, Micali and Rackoff [3] conceived zero-knowledge proofs. Languages were classified relative to the amount of knowledge that has to be released to prove the membership in them. An interactive proof system can be constructed that communicates zero-additional knowledge as it was demonstrated using the quadratic non-residuosity problem. The quadratic non-residuosity problem is defined within the NP complexity class which solution would imply the probabilistic polynomial time.

In 1936 Alan Mathison Turing invented a hypothetical device that manipulates symbols on a strip of tape according to a table of rules. A probabilistic interactive Turing machine has a read-only tape, a work tape, a random tape, a read-only communication tape and a write-only communication tape. The random tape contains an infinite sequence of random bits. Two interactive Turing machines form an interactive pair of Turing machines (P, V) if they share the same input tape and if V 's write-only communication tape is P 's read-only communication tape and vice versa.

Let $L \subseteq \{0,1\}^*$ be a language and (P, V) an interactive pair of Turing machines. (P, V) is an interactive proof-system for L if P (the prover) has infinite power, V (the verifier) is polynomial time and they satisfy the following properties:

1. For any $x \in L$ given as input to (P, V) , V halts and accepts with probability at least $1 - \frac{1}{n^k}$ for each k and sufficiently large n .
2. For any interactive Turing machine P' and for any $x \notin L$ given as input to (P', V) , V accepts with probability at most $\frac{1}{n^k}$ for each k and sufficiently large n .

Here n represents the length of the input and probabilities are taken only over V 's own random tape. According to the condition 1 above, prover's algorithm enables easily proving to the verifier a true theorem. This could be easily verified since the verifier is polynomial-time. Condition 2 stipulates that there is a very low probability to prove a false theorem. The verifier does not need to trust the prover with which it is interacting. It is enough that it trusts the randomness of its random tape.

Interactive Polynomial time (IP) is defined as a class of languages that possess interactive proof systems. It is suggested that knowledge complexity could be applied in proving the correctness of cryptographic protocols.

Goldreich [4] proposed a formal definition of zero-knowledge proof. Firstly, the simulation paradigm is defined such that whatever a party can do efficiently by itself cannot be considered a gain from the interaction with the outside. This paradigm is derived from already mentioned relation between the probability of the outcome and the information content that it carries. With this notion it is sufficient to generate a probability distribution that is computationally indistinguishable from the output of the verifier after it interacts with the prover. This leads to the formal definition of computational zero-knowledge assuming the above definition of an interactive proof system:

*Let (P, V) be an interactive proof system for some language L . (P, V) is **computational zero-knowledge** (or just **zero-knowledge**) if for every probabilistic polynomial-time interactive Turing machine V^* there exists a probabilistic polynomial-time algorithm M^* such that the following two ensembles are computationally indistinguishable:*

- $\{\langle P, V^* \rangle(x)\}_{x \in L}$ (i.e., the output of the interactive Turing machine V^* after it interacts with the interactive Turing machine P on common input x)
- $\{M^*(x)\}_{x \in L}$ (i.e., the output of Turing machine M^* on input x) Machine M^* is called a simulator for the interaction of V^* with P .

Zero-knowledge property of the above proof system implies that, if the statement is true (x is in language L), a cheating verifier does not learn anything more than the assertion of the statement. This is formalized with the existence of the simulator M^* that is able to simulate the interaction of the verifier with the prover without having access to the prover.

In addition, zero-knowledge proof must satisfy completeness and soundness properties. *Completeness* represents the ability of the prover to convince the verifier that the statement is true (for the statement belonging to a predetermined set of true statements). *Soundness* represents the ability of the verifier not to accept the false statement. In the above definition of zero-knowledge proofs, there is a probability that a cheating prover convinces verifier that a false statement is true. This probability is called the *soundness error*. The soundness error can be reduced exponentially with the

number of successive repetitions of the proof system. The error reduction is demonstrated also when the proof system is repeated concurrently although it is not proven that this is the general rule.

Because of the existence of the soundness error, zero-knowledge proofs are considered probabilistic proofs.

Bellare and Goldreich [5] developed further the definition of knowledge proofs introducing the concept of knowledge extractor, or an oracle machine. When given a proof, the knowledge extractor produces an output within the expected polynomial time inversely proportional to the probability that a given proof convinces the verifier. It is presented that satisfying the more restricted definition of knowledge proofs does not imply satisfying the above more general definition of the proof of knowledge that implies all probabilistic proofs. More restricted knowledge proofs are those that satisfy all deterministic strategies. Particularly in the case of zero-knowledge proofs, the ability to simulate any deterministic verifier strategy implies the ability to simulate any probabilistic verifier strategy. However, the procedure to consider the knowledge extraction of all residual deterministic strategies may not necessarily run in time that is inversely proportional to the probability that the prover convinces the verifier. Furthermore, when proofs of knowledge are the end objectives, for example, in the identification schemes, prover strategies are probabilistic. In other scenarios when proofs of knowledge are used as tools and the knowledge extractor is implemented in the form of a simulator, it may be sufficient to consider deterministic prover strategies.

Using the above formal definition of computational zero-knowledge, it is proven by Goldreich, Micali and Wigderson [6] that all languages in NP have zero-knowledge proofs. However, the above definition is restricted to interactive proof systems.

Blum, Feldman and Micali [8] demonstrated removing the interaction in zero-knowledge proof system by sharing a common random string. A common random string of a certain size is pre-selected by the prover and the verifier together. The prover communicates this string combined with a proof of a smaller or equal size to the verifier. This one-way communication is what constitutes an essential strength of non-interactive zero-knowledge proofs over their interactive counterparts reducing the possibility of a cheating verifier to use the interaction in order to extract more knowledge from the prover. It is important to highlight that in order to satisfy a zero-knowledge property of the proof system, the simulator of the communication of a proof has to include also a cryptographically strong pseudo-random generator. It is used to create a combination of random string and a simulated proof that is computationally indistinguishable from the real combination of a randomly selected string and a proof.

2.2 Construction

2.2.1 Trust Model

Trust relationship among provers and verifiers could take different forms for different cryptographic schemes. In public key based encryption schemes trust model practically consists of decisions to accept or not the public key of the other party. In various implementations this trust model assumes the existence of the central repository for managing public keys. In the RSA scheme for example, the public key directory serves as this third party. Each user of the RSA scheme generates its own key

pair. The trust could take a more complex form is users certify public keys of other users by signing them with their private keys. This may establish several levels of trust to enable trust domains for larger groups of users. The challenge is to maintain the history of revoked keys as every user may revoke its keys at any time. The revocation is not automatic so the directory must maintain the process of periodic verification of public keys validity. In addition every user may define different levels of trust to public keys of other users. Finally, information that has to be accessible to multiple users should be encrypted with public keys of all of them. As a result such schemes are inconvenient for large-scale authentication, identification, and signature purposes. They are typically used among smaller groups of users in which case users may exchange their public keys in person or by some other mean of communication without even using the public key directory. Companies may decide to implement internal public key directories to facilitate key management and ensure business continuity. In order to mitigate the risk of losing access to information in case of lost or compromised private keys companies may consider establishing key escrow by introducing master keys that may also be used to decrypt information. This opens up the whole new set of technical and procedural requirements for transparency and auditability to ensure that escrow keys are not misused.

Fiat and Shamir [7] demonstrated how to remove the interaction for verification of proofs through combining interactive zero-knowledge proofs and identity-based schemes with trusted third parties. In the proposed construction the trusted third party generates keys that are used to certify identity information of users. The public key has to be certified by the third party managing the public key directory. This involves signing of public keys with certificate authority's (CA) private key. The hierarchy of signatures requires distribution of CA's root and/or intermediate keys to all users and their integration with client applications. In addition, CAs have to manage Certificate Revocation Lists (CRL) so that the validity of keys could be verified. These are just a few aspects of implementing a Public Key Infrastructure (PKI) required to establish the trust model described. This scheme is much more convenient for large-scale identification and considerably more secure since the verification can be processed locally and without access to the list of each user's public key. The trust model is different from the RSA type scheme as the third party serves as the central authority for issuing keys and therefore has to be trusted by all users. In addition, a security breach of central authority's private key would compromise trust in all issued identity proofs. For example in 2011 Comodo's Web site secure certificate (SSL) issuing process was breached and perpetrators managed to obtain forged certificates for well known Web sites signed by Certificate Authority (CA)⁵. Similar breach has occurred later the same year when Diginotar Certificate Authority was compromised to issue fraudulent certificate for Google and other well known Web sites. Those certificates were used for man-in-the-middle attacks. Diginotar went bankrupt and their root certificates were removed from all major Internet browsers.⁶

As mentioned in the previous chapter, Blum, Feldman and Micali [8] introduced non-interactive zero-knowledge proofs. In their construction the interaction between the prover and the verifier is replaced with pre-selected common random strings. A

⁵ <http://www.infoworld.com/t/authentication/weaknesses-in-ssl-certification-exposed-comodo-security-breach-593>

⁶ <http://en.wikipedia.org/wiki/DigiNotar>

central repository for common random strings was proposed for the practical implementation of such encryption scheme. This trust model is similar to the RSA model described earlier which is implemented with the public key directory. Because each user generates its public/private key pair the third party that manages the public key directory has a very little chance to efficiently tamper with public keys. Likewise, the repository of common random strings is robust against tampering. Moreover, in case that the prover and the verifier have established a mutual trust when exchanging their public keys and when selecting together a common random string, the level of their trust in the third party that manages common strings repository does not have to be very high. However, for applications in scenarios with multiple provers and verifiers it was proposed to have a trusted third party that generates common random strings rather than just maintaining a repository of strings pre-selected by each user. This scenario is closer to the model of the above-mentioned Fiat and Shamir scheme with the Certificate Authority. Although the level of trust that provers and verifiers have to place in the third party that generates random strings is similar to the level of trust placed in the CA, security requirements for protection of certificates and for protection of common random strings are different. It is important to ensure the appropriate management of random strings. As we will see later in the discussion on the security of technical implementation, this may require the verification of the source of randomness and other technical security measures. A breach of strings management procedures would not necessarily violate the security of all encrypted communications, as it would be the case of a certificate authority's private key breach. We have referenced concrete cases of such a breach. Blum, Feldman and Micali model is known in cryptography as the common reference string model.

Common string model further evolved to the multi-string model where a single trusted third party is replaced with multiple parties each generating and publishing random strings. Parties that want to participate in such an encryption scheme have to agree from which third parties they want to use common random strings. Security advantage of this model over the previously described model with the single third party is within the fact that not all parties that generate strings have to be honest. This model is proposed by Groth and Ostrovsky [9]. In the proposed construction having the majority of honest string generating parties is sufficient to ensure the security of the encryption scheme. Moreover, even if certain third parties become dishonest at later time, their random strings could still be used to construct non-interactive zero-knowledge proofs.

2.2.2 Efficiency

An important aspect to consider when implementing zero-knowledge proofs is efficiency in terms of performance. Time to perform all required calculations and communication throughput overhead depends mainly on the size of data variables. The size is measured in bits. Comparison of efficiency of different cryptographic constructions begins with evaluation of the size of data variables such as common reference string size and proof size. As stated earlier a detailed comparative overview of different non-interactive zero-knowledge proof constructions was presented in Polic [57] and the summary is provided in the table below.

Non-interactive zero-knowledge proof construction	Proof size
Based on the subgroup decision problem	$\mathcal{O}(C \kappa)$
Based on the quadratic residuosity assumption	$\mathcal{O}(C \kappa^2 + \kappa^3)$
Based on the decisional linear assumption	$\mathcal{O}(C \kappa)$
A fully homomorphic public-key cryptosystem based on lattices	$ \omega + \text{poly}(k)$

Table 1: Proof size comparison with various NIZKP constructions

Groth, Ostrovsky and Sahai [10] proposed non-interactive zero-knowledge proof construction using the subgroup decision problem. The size of the common reference string is $\mathcal{O}(\kappa)$, where κ is the security parameter independent of the NP statements. We have stated earlier that the NP statements are inputs to the computational problem used as the basis for the cryptographic construction. The proof size listed in the above table consists of is the size of the Boolean circuit $|C|$ and the security parameter κ . It is much more efficient than the construction that uses the quadratic residuosity assumption. However, both constructions are based on the single common reference string. The efficiency of the multi-string model implies the proof size of $\mathcal{O}(n + |C|\kappa)$, where n is the number of random strings, $|C|$ is the size of the Boolean circuit, and the security parameter κ as the group element. In cases where n is much smaller than $|C|$, the efficiency is comparable to the above mentioned $\mathcal{O}(|C|\kappa)$ size.

Groth, Ostrovsky and Sahai [11] also demonstrated that efficient non-interactive zero-knowledge proofs could be constructed in the common random string model as well as in the common reference string model. This construction is based on the decisional linear assumption that represents a bilinear group variant of the decisional Diffie-Hellman assumption. As it can be compared in the above table, the proof size is the same like in the construction based on the subgroup decision problem. The replacement of common reference strings is achieved by implementing non-interactive “Zaps”, that are witness indistinguishable proofs. In this implementation a prover generates the common random string and provides both the chosen string and its transformation.

A fully homomorphic encryption scheme represents the construction in which when given only two ciphertexts it is possible to produce a resulting ciphertext that contains sums or products of the corresponding input plaintexts. The efficient construction is proposed in Groth [12]. It combines a fully homomorphic public-key cryptosystem based on lattices with a symmetric key cryptosystem resulting in the same size of the proof and the witness that is polynomial in security parameter κ as outlined in the above table. The proposed construction of the non-interactive zero-knowledge proof is based on the common reference string model. The size of the common reference string is $\text{poly}(\kappa)$. The proof size contains the witness ω for the statement which truth has to be proven. Witness ω is encrypted with a symmetric key cryptosystem, for example, a pseudorandom one-time pad.

To conclude, selecting a different computational complexity problem as the base for cryptographic construction could have significant implications to the application performance. This applies also to the selection of a different trust model that may result in a significant difference in the size of global security variables and resulting communication overhead. However, specific business models require different security levels and could not compromise security for performance benefits. Therefore in our research we focus on achieving secure and efficient constructions emphasizing security requirements for concrete applications. Moreover, security management is a dynamic process. This implies that the constant evolution of cryptanalysis and increasing availability of affordable computing resources require strengthening security levels of cryptographic constructions overtime. More complex base computational problems have to be considered for future implementations as well as larger sizes of global security parameters. Security analysis process is presented in chapter 5.

2.3 Application

As already stated zero-knowledge proofs have been a subject of growing importance in recent cryptographic research related to applications that require verification of the correct participation without revealing any additional information. A selection of recently published applications of zero-knowledge proofs for information systems auditing was presented in Polic [57]. We will highlight their most important aspects in this chapter to illustrate applicability in the construction of the protocol presented in later chapters.

Weber and Mühlhäuser [13] proposed a solution to protect privacy of emergency vehicles drivers involved in road traffic accidents during investigations. Although emergency vehicles may need to circumvent traffic regulations it does not necessarily mean that every accident involving those vehicles is a result of unlawful behavior. The proposed protocol allows auditors to examine logs for the vehicle's participation in traffic without revealing any information on drivers. Investigators may revoke privacy protection of personnel in case they find an evidence of unlawful behavior. Furthermore, implementation of non-interactive zero-knowledge proofs enables the transparency of the auditing process. Logged information could be made available to public inspection without revealing personally identifiable information on either auditors or emergency vehicle drivers.

Sang and Shen [14] proposed a protocol for monitoring computer networks with preserving privacy. Analysis of computer networks logs may reveal information on users their access to different systems and services. The proposed construction uses non-interactive zero-knowledge proofs and ensures security against malicious participants in the analysis as well as against malicious third parties that may have access to logs.

New electronic road toll pricing in Europe and the United States uses electronic devices installed in vehicles to track information about roads taken and use it later to calculate toll fees. Confidentiality of data on geographic location of vehicles must be ensured. Balasch, Rial, Troncoso, Preneel, Verbauwhede, and Geuens [15] proposed a system based on non-interactive zero-knowledge proofs to ensure correct calculation of fees without revealing information on vehicles location. In addition, the proposed system prevents tampering with data and ensures auditability of transactions.

One more example is selected to illustrate the importance of non-interactive zero-knowledge proofs. Goodrich and Kerschbaum [16] proposed a solution to ensure privacy in reputation feedback systems for on-line auctions. Some on-line auction systems evaluate buyers and sellers based on reputation. The proposed construction ensures not only protection of privacy, but also protection from extortion and other malicious behavior of feedback providers. It implements non-interactive zero-knowledge proofs based on the common random string model. In the proposed approach two parties can jointly compute the result used for the reputation feedback without learning the input of the other party.

2.4 Importance of zero-knowledge proofs

A quantity of data captured, processed, stored and transmitted that may have potential implication on privacy is progressively growing. Complex business relations are established among ICT service providers involved in handling these data. Regulatory and legal compliancy requirements imposed by authorities are growing. These requirements focus on transparency and auditability amongst other aspects. In such an increasingly complex environment it is of a vital importance to embed protection systems deep in the technology closer to data itself. Access to data has to provide mechanisms that could provide effective prevention against unauthorized data mining that may result in building knowledge about participants in transactions and data owners with potentially detrimental effects.

Protection mechanisms are more and more complex yet they have to be more efficient due to massive amounts of data that requires protection. These security controls consist of complex encryption protocols that require secure, robust and efficient basic building blocks. As we have seen previously in this chapter selection of particular computational problem as the basis for constructing cryptographic controls may have a satisfactory security levels but at the same time may be very inefficient and therefore practically not suitable. Advancement of fundamental research in cryptology permitted construction of secure cryptographic protocols that satisfy strict security and performance requirements for practical implementation in various systems from those with low available processing power, to those systems that store and communication huge amounts of data and have enormous processing power.

Advancement in construction of efficient non-interactive zero-knowledge proofs was an important achievement in the fundamental research in cryptology that enables construction of protocols that ensure verification of correct participation in transactions and protection of other related data. Implementation of privacy preserving information audit systems that satisfy above mentioned security requirements became possible with such research advancement.

Information security is process of continuous advancement in techniques that can result in making it more vulnerable such as more efficient cryptanalysis, as well as more robust such as more optimized cryptographic primitives. Therefore research in practical implementations and constructions of complex cryptographic protocols has to evolve in parallel with fundamental research in cryptography and related areas of science. Implementation of security controls is a trade of with accepting risks and carries its own resource overhead. Decision on the acceptable risk level must be made before the selection of protection controls in order to evaluate the most appropriate security level and relevant protection control complexity and related cost. This decision

is the result of risk analysis and is formalized in the risk mitigation plan. As we focus on the further development of zero-knowledge proofs and cryptographic protocol with equivalent security attributes like those mentioned in this chapter we will apply risk analysis methodologies that are used across ICT industry to address information security issues.

3 Non-interactive Σ -protocols

Challenge is to construct a cryptographic protocol with an efficient zero-knowledge proof. Possible answer to this problem is to use sigma-protocols. Similar to zero-knowledge proofs, sigma-protocols have also characteristics to be honest verifier and honest prover. Sigma-protocols are executed in three steps: commitment, challenge and response. Because the Greek letter sigma (Σ) visually reminds of these three steps it used in the name of the protocol. Asymmetric or public key cryptography is used as the basis for constructing sigma-protocols as demonstrated in Damgard [17]. This protocol construction is based on Schnorr's signature scheme because of its efficiency. This signature scheme is based on discrete logarithms as described in Schnorr [18]. The most CPU intensive computations could be performed separately from message-dependent computations therefore offloading processing resources during the protocol execution. Schnorr's scheme is also used in the Digital Signature Algorithm (DSA).

To reduce the number of interactions between two parties participating in the protocol the challenge sent by the verifier is replaced with the random oracle. Practically, in the protocol construction random oracle is replaced using the secure hash function. The secure hash function is available to both parties. The prover applies secure hash function on the original message. Both the original message and the result of the hash function execution are sent to the verifier. The verifier applies the same secure hash function on the received message and compares the result with the received result from prover's calculation. If both results are equal then the received message is equal to the original message. As stated in Damgard [17], non-interactive protocols in random oracle model are robust in the concurrent setting that makes them useful for networked applications, and for the Internet in particular. Secure Hash Algorithm (SHA) is selected as a cryptographic primitive for secure hash function in this protocol construction.

3.1 Definition

Sigma-protocol is formally defined in Damgard [19]:

Let R be a binary relation, i.e., R is a subset of $\{0,1\}^* \times \{0,1\}^*$, where the only restriction is that if $(x, w) \in R$, then the length of w is at most $p(|x|)$, for some polynomial $p()$. For some $(x, w) \in R$, x is an instance of some computational problem, and w is the solution to that instance. w is called a witness for x .

Protocols take the following form, where x is common input to both P , V and w such that $(x, w) \in R$ is private input to P :

1. P sends a message a .
2. V sends a random t -bit string e .
3. P sends a reply z , and V decides to accept or reject based on the data she has seen, i.e. x, a, e, z .

Let assume that both P, V are probabilistic polynomial time machines, so P 's only advantage over V is that she knows w .

A protocol P is said to be a Σ -protocol for relation R if:

– P is of the above 3-move form, and there is completeness: if P, V follow the protocol on input x and private input w to P where $(x, w) \in R$, the verifier always accepts.

– From any x and any pair of accepting conversations on input x , $(a, e, z), (a', e', z')$ where $e \neq e'$, one can efficiently compute w such that $(x, w) \in R$. This is sometimes called the special soundness property.

– There exists a polynomial-time simulator M , which on input x and a random e outputs an accepting conversation of the form (a, e, z) , with the same probability distribution as conversations between the honest P, V on input x . This is sometimes called special honest-verifier zero-knowledge.

To define a non-interactive version of sigma-protocol it is necessary to add the notion of random oracle. It is an entity that initially chooses (in private) a random function $R: \{0, 1\}^l \rightarrow \{0, 1\}^t$ for some l, t . Then any player can send any bit string a of length l to the oracle which will then return $R(a)$. Since R was completely random, $R(a)$ is a uniformly chosen string of length t , and is independent of a . Moreover, seeing the value of $R(a)$ gives no advantage whatsoever in predicting the value $R(b)$ for $b \neq a$. However, R is fixed, so every time someone sends a to the oracle, the answer will be the same value $R(a)$. This is known as the random oracle model as defined in Fiat and Shamir [7].

3.2 Construction

The following protocol construction is described in Damgard [19]. Let p be a prime, q a prime divisor in $p-1$, and g an element of order q in Z_p^* . Suppose a prover P has chosen w in Z_q at random and has published

$$h = g^w \bmod p \quad (4)$$

A verifier V who gets p, q, g, h can check that p, q are prime, and that g, h have order q . Since there is only one subgroup of order q in Z_p^* , this automatically means that $h \in \langle g \rangle$, i.e. there exists w such that $h = g^w$. But this does not necessarily mean that P knows such w . That could be verified using sigma-protocol proposed in Schnorr [18]. Sigma-protocol is constructed in the following way:

1. P chooses r at random in Z_q and sends

$$a = g^r \bmod p \quad (5)$$

to V .

2. P obtains the challenge e applying the hash function $H()$ on a . P sends

$$z = r + ew \bmod q \quad (6)$$

to V , who applies the hash function $H()$ on the received message a' to obtain e' . Using received z' V then checks that

$$g^{z'} = a' h^{e'} \bmod p \quad (7)$$

, V checks also that p, q are prime and that g, h have order q , and accepts if this is the case. This protocol construction is illustrated in Figure 1.

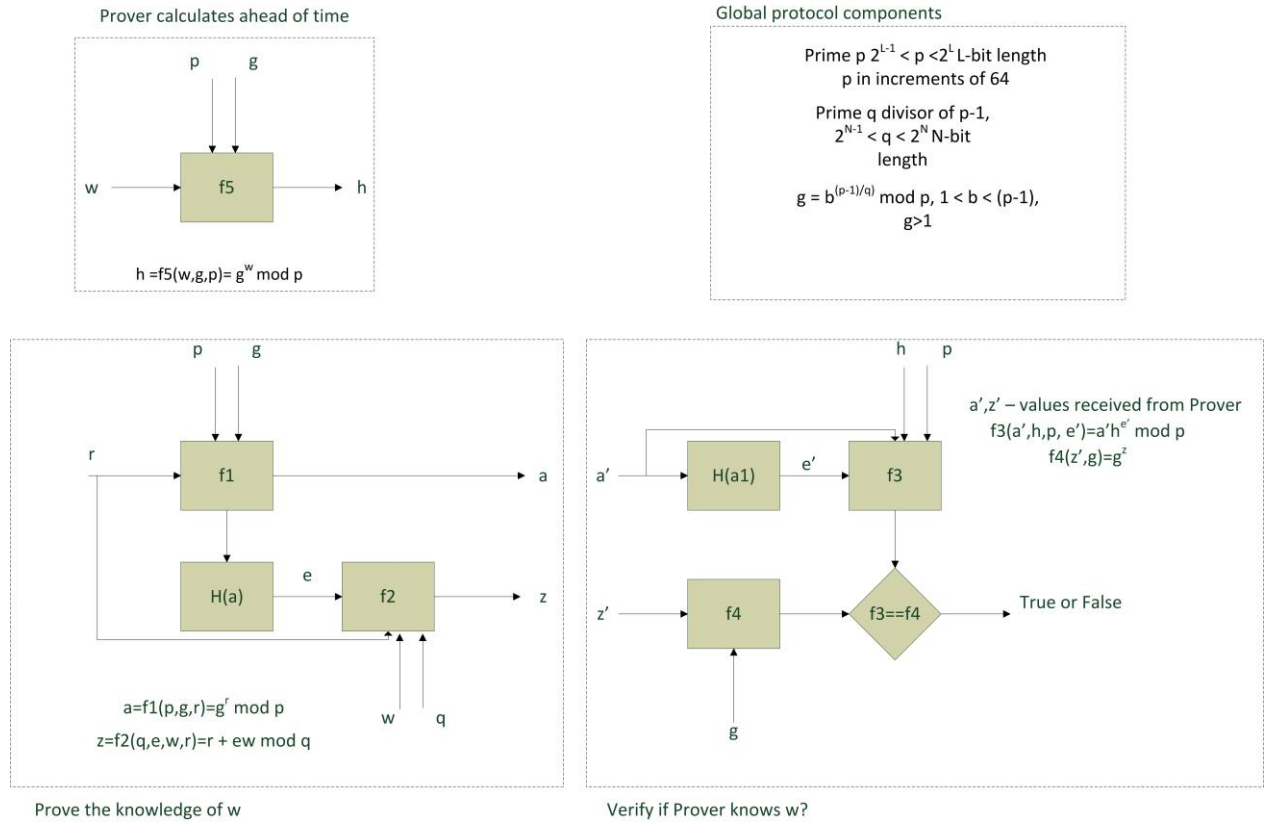


Figure 1. Sigma-protocol construction

As mentioned earlier, improved efficiency of Schnorr's signature schema results from the fact that resource intensive calculations are externalized from the protocol execution. Those calculations are used to check whether global parameters p and q are prime numbers. That verification could be performed only once for as long as values of global parameters are fixed.

Discrete logarithm problem is the complex computational problem which consists of finding solution x to the equation below given elements g and h of a finite cyclic group G :

$$g^x = h \quad (5)$$

It is used as a basis to construct Schnorr's signature cryptographic scheme.

It is believed that the discrete logarithm cannot be computed in polynomial time on classical (non-quantum) computers. The latest world record in solving the discrete logarithm problem was announced in May 2013 by Antoine Joux and his team who succeeded in computing discrete logarithms in the field with 2^{6168} elements using less than 550 CPU-hours.⁷ Consequently the period of time that security of global parameters has to be guaranteed must be shorter than the time required to break it. In 1994 the factoring algorithm for quantum computers was published in Shor [34] who demonstrated solution of discrete logarithm problem in polynomial time. Since that publication the focus of cryptanalysis community turned to the advancement in

⁷ <https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1305&L=NMBRTHRY&F=&S=&P=3034>

quantum computing. Recently several publications described practical implementation of Shor's algorithm on quantum computers. For example, in Lucero et al [35] prime factors of number 15 were found on 3-qubit solid-state quantum computer. Factoring number 143 was demonstrated on a liquid crystal quantum computer using adiabatic factoring algorithm as published in Xu et al [36]. Although these practical factoring results are still significantly shorter than bit-size of prime numbers proposed for our constructions it is prudent to take them into serious considerations as development of quantum computers may advance significantly as a result of advancement in fundamental research in quantum physics. A Canadian company D-Wave offers commercially the 128-qbits computer⁸. So, how safe it is to develop cryptographic protocols based on discrete logarithms while in several years from now quantum computers may be able to solve them in a very short time? The solution is in using alternative complex computational problems for which optimized solution algorithms do not exist for quantum computers. One group of such problems is known as optimization problems on lattices. Lattices were already mentioned in chapter 1 in the implementation of fully homomorphic encryption. Cryptographic primitives based on these problems could be used in place of primitives based on discrete logarithms in the construction of the cryptographic protocols. However, until quantum computers with large enough qbits size become available and become affordable for wider application it is safe to use efficient cryptographic primitives at least for public and commercial applications. Moreover, there are many practical applications where the security lifecycle of global parameters is not very long. Some examples are e-voting, Internet usage monitoring, some e-commerce transactions, and other. The history of cryptanalysis has shown that advanced algorithms and code breaking computers were kept in secret for decades when their use was of a strategic importance at national level. For example details on Collosus computer used to break the Lorenz cipher during the Second World War were published only in seventies. To conclude, with massive amounts of data globally exchanged at every moment, even if quantum computers already exist and are kept secret, they would be very few and available only to break a tiny portion of global data transactions. Nevertheless, cryptographic primitives robust against quantum computing cryptanalysis should be used whenever data are to be kept secret for more than a decade.

Practical implementation of the above protocol construction and related simulations are presented in Polic [23]. For cryptographic prototyping Sage mathematic software was used. This simulation platform supports Python programming language and the source code for the proposed construction of sigma-protocol is published in the annex to the article. Results obtained in protocol simulations lead into conclusion that selecting smaller p global prime and selecting larger q prime is optimal for applications that require shorter information protection period such as Internet-based voting systems. For such systems selecting 2048 bits p and 512 bits q would provide sufficient protection during one ballot. Selecting this size of global parameters messages exchanged by communicating parties would not exceed 1 Kbyte so the implementation could be based over the communication channel with low bandwidth. Larger size of global parameters should be selected for applications that require data protection during longer periods. From simulation results it is also concluded that whether the q prime size is 512 or 256 bits time required for calculations is not significantly different. Therefore it is better to use 512 bit for this global security parameter if communication

⁸ <http://www.dwavesys.com>

is not of a concern. Although it would take longer to calculate global protocol parameters it would not decrease the performance of the protocol execution during business transactions. Details about Sage mathematic software are presented in Stein et al [24].

4 OR-proof form of Σ -Protocol

Sigma-protocols in their simplest form cannot ensure identity protection of information system users. Protocol communication could be recorded and used as evidence that exchange of messages between parties really happened. One answer to this problem is offered with introduction of OR-proof form of sigma-protocols. In this form the prover executes sigma-protocol twice. One protocol execution is with real parameters and the other with simulated. Although the verifier doesn't know which parameters are real it can accomplish its verification function. Furthermore, recording such communication could not be used as evidence since anyone could have performed the simulation. Thus cryptographic protocol with witness-hiding and deniability properties could be constructed using OR-proof form of sigma-protocol.

4.1 Definition

Formal definition of OR-proof based on sigma-protocol is given in Damgard [19]:

Let R be a binary relation, i.e., R is a subset of $\{0, 1\}^* \times \{0, 1\}^*$, where the only restriction is that if $(x, w) \in R$, then the length of w is at most $p(|x|)$, for some polynomial $p(\cdot)$. For some $(x, w) \in R$, we may think of x as an instance of some computational problem, and w as the solution to that instance. We call w a witness for x .

Let's assume that prover P and verifier V are probabilistic polynomial time machines and P 's only advantage over V is knowledge of w . Assume also that two instances of above problem x_0, x_1 are common input to both P and V , and that w is private input to P . $(x_b, w) \in R$, where $b = 0$ or 1 .

1. P computes the first message a_b in sigma-protocol P , using (x_b, w) as input.

P chooses e_{1-b} at random and runs the simulator M on input (x_{1-b}, e_{1-b}) , let $(a_{1-b}, e_{1-b}, z_{1-b})$ be the output.

P sends (a_0, a_1) to V .

2. V chooses a random t -bit string s and sends it to P , such that s in Z_2^t where t is fixed at $2^t < q$.

3. P sets $e_b = s \oplus e_{1-b}$ and computes the reply z_b to challenge e_b using (x_b, a_b, e_b, w) as input. P sends (e_0, z_0, e_1, z_1) to V .

4. V checks that $s = e_0 \oplus e_1$ and that $(a_0, e_0, z_0), (a_1, e_1, z_1)$ are accepting conversations in sigma-protocol P on inputs (x_0, x_1) .

Let $R_{OR} = \{((x_0, x_1), w) \mid (x_0, w) \in R \text{ or } (x_1, w) \in R\}$.

The protocol P_{OR} above is a Σ -protocol for relation R_{OR} . Moreover, for any verifier V^* , the probability distribution of conversations between P and V^* , where w is such that $(x_b, w) \in R$, is independent of b .

There are several different values of w that a prover may know that would enable completion of the protocol successfully. However, one cannot tell from the conversation which of the values prover knows. This is known as *witness indistinguishable* (WI) property.

Furthermore, if R is a hard relation, then the protocol P_{OR} for R_{OR} is *witness hiding* (WH) as shown in Damgard [19]. Although it is weaker property than zero-knowledge, WH satisfies requirements for ensuring identity protection. Since the complexity of OR construction is only about twice that of P , it is still a very economic way to produce extra security.

4.2 Construction

OR-proof protocol is built on the basic sigma-protocol construction as defined in Schnorr [23]. Global parameters for the protocol are set in the following way. Let p be a prime, q a prime divisor in $p-1$, and g an element of order q in Z_p^* . Suppose a prover P has chosen w in Z_q at random and has published:

$$h = g^w \bmod p \quad (6)$$

A verifier V who gets (p, q, g, h) can check that (p, q) are prime, and that (g, h) have order q . Primality of (p, q) could be checked only once and not for every protocol execution. Since there is only one subgroup of order q in Z_p^* , this automatically means that $h \in \langle g \rangle$, i.e. there exists w such that $h = g^w$. As stated in the previous chapter, finding solutions w to this equation is known as discrete logarithm problem. The discrete logarithm cannot be computed in polynomial time on classical (non-quantum) computers so it is considered to be hard computational problem. Therefore protocol constructed with this hard problem is witness hiding (WH) as shown in Damgard [19].

Similarly to the conclusion made in the previous chapter the minimum size of the global prime p should be 2048 bits and the size of q at least 512 bits. This should satisfy security requirements for the most of applications with shorter than 10 years data retention period. For systems like Internet-based voting this would be optimal. Simulation results show that the longest calculation time is preparation of global security parameters while protocol execution is very efficient.

Let above global parameters p, q, g be given in advance to prover P and verifier V . Let also P chooses randomly a private key w in Z_q . P calculates a public key:

$$h = g^w \bmod p \quad (7)$$

and makes it available to V in advance. OR-proof sigma-protocol executes in the following way (Figure 2 schematically presents the protocol):

1. P chooses r at random in Z_q and calculates:

$$a_0 = g^r \bmod p \quad (8)$$

P chooses e_1 at random in Z_q , chooses z_1 at random in Z_p and runs simulator M to calculate:

$$a_1 = g^{z_1} * h^{-e_1} \bmod p \quad (9)$$

P sends (a_0, a_1) to V .

2. V chooses a random t -bit string s in Z_{2^t} and sends it to P . Here, t is fixed such that $2^t < q$. s has to be exponentially large in order to maintain negligible error.

V sends s to P .

3. P calculates

$$e_0 = s \oplus e_1 \quad (10)$$

and

$$z_0 = r + e_0 w \bmod q \quad (11)$$

P sends (e_0, z_0, e_1, z_1) to V .

4. V checks that

$$s = e_0 \oplus e_1 \quad (12)$$

and that

$$g^z = ah^e \bmod p \quad (13)$$

for both conversations (a_0, e_0, z_0) and (a_1, e_1, z_1) . If both statements are valid and p, q are prime and g, h have order q , V accepts that P knows the private key w . However, V does not know to which of two above conversations it corresponds.

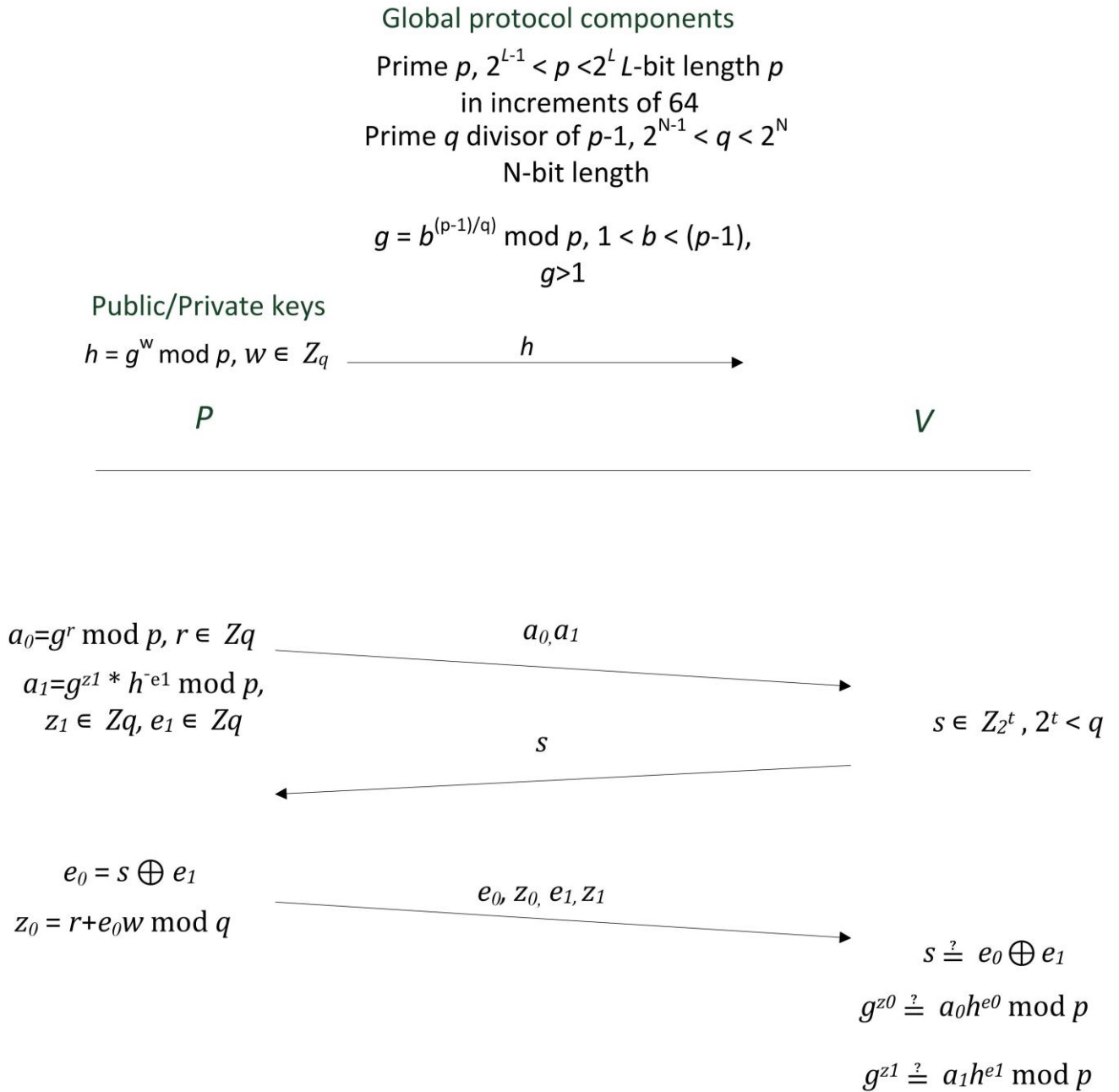


Figure 2 – OR-proof sigma-protocol diagram

Deniability is proven in Damgard [19]. Let's assume that V captures the trace of all communications with P . If V shows this trace to a third person C , C can not be convinced that the communication took place with P since V could have simulated it on its own. This important property is one of the main reasons for using this protocol to achieve identity protection in information systems.

Practical implementation with modelling and simulation is presented in Polic [31]. The source code in Python programming language from the referenced source is used to create one subsystem in later chapters. Simulation results illustrate the efficiency of the protocol. In the first communication step, the prover sends a message (a_0, a_1) of approximately 1.5 Kbytes to the verifier. In the second step, the verifier sends a message (s) of only 72 bytes to the prover. The final message (e_0, z_0, e_1, z_1) from the prover to the verifier is approximately 288 bytes. Size of messages depends on the

selected size of global parameters. Therefore, it is very important to make the right decision on parameter sizes that correspond to the security requirements of the application. Selection of larger parameters could impact protocol performance from the communication aspect. However, the advantage of using Schnorr's scheme is obvious since global parameters could be calculated ahead of time. This is very important conclusion that was also made in the previous chapter. As it will be demonstrated later, global parameters could be pre-calculated even in the more complex constructions where OR-form and noninteractive form of sigma-protocols are combined into one unified solution that carry advantages of both forms to satisfy security requirements of two different processes, authentication and authorization.

5 Cryptographic protocol for information systems audit with users' identity protection

5.1 Construction

The proposed protocol consists of two sub-systems, one for users' authentication and the other one for authorization to perform transactions. Two sub-systems share the same common global cryptographic parameters. This method of unification of two-subsystems will ensure performance advantage of Schnorr's cryptographic scheme as described in chapter 3. More specifically, resource intensive calculations of global cryptographic parameters will take place in advance of business transactions. The proposed protocol construction is illustrated in Figure 3.

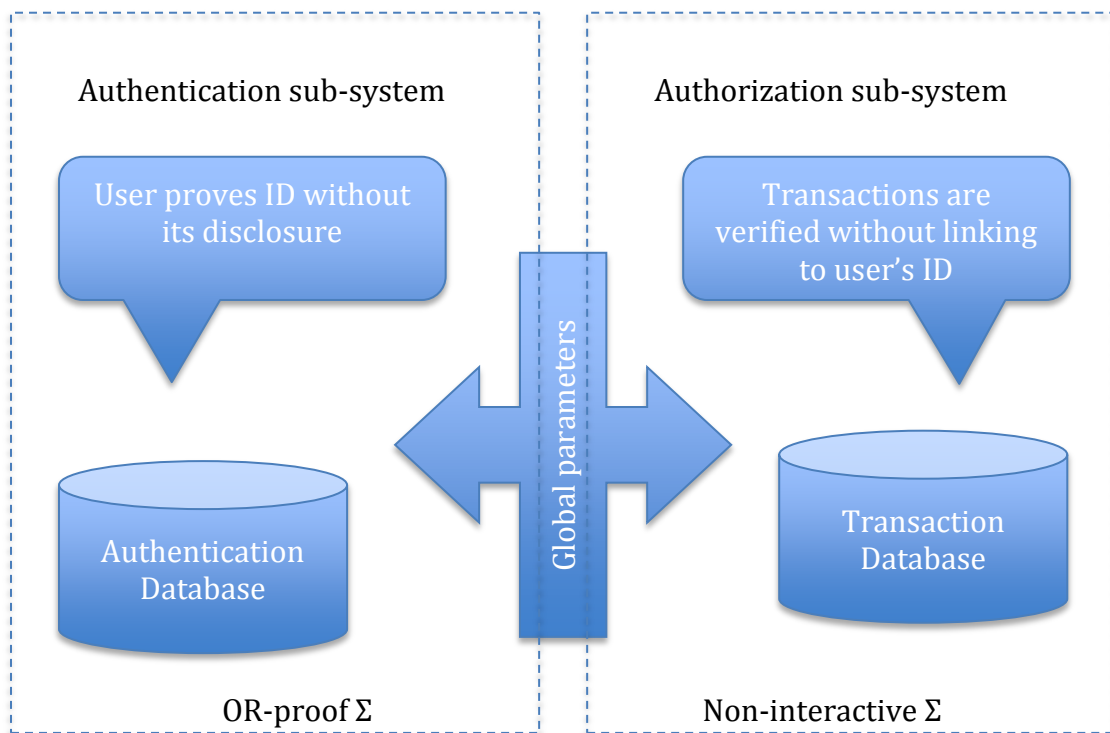


Figure 3 – OR-proof sigma-protocol diagram

Construction of the authentication sub-system is based on the OR-proof form of sigma protocol described in chapter 4. This form proves user's identity without its disclosure. To recall, OR-proof form of sigma protocol have following attributes that make this possible: witness-hiding, deniability, honest prover and honest verifier. Proving the possession of the private key identifies a user. The real private key is obfuscated from the verifier in a double protocol execution. One execution is performed with the real private key and the other with a simulated private key. The verifier confirms that both keys correspond to the challenge but doesn't know which one is the real. The same would apply to an eavesdropper who may not convince another party that the transaction took place since she could have simulated it on its own. Method for the distribution of public keys would have to be selected depending on the security requirements of the business application. In case of electronic voting (e-voting), for

example, public keys could be distributed without additional information about their individual owners. The fact that they originate from the group of authenticated individuals would satisfy information requirements for voting related transactions.

Construction of the authorization sub-system is based on the non-interactive form of sigma protocol described in chapter 3. Correct participation in the e-voting related transaction is verified by proving that an authenticated user performed it. Most importantly, the verifier doesn't know which user performed transaction since the verification is not directly linked to the user's private key used for authentication. It depends only on the result of the verification from the authentication sub-system. Since the authentication sub-system obfuscates the utilization of the private key it could not be ascertained whether it was a real or a simulated user. As described in chapter 3 the proposed construction of the authorization sub-system is based on the random oracle model to remove unnecessary interaction between the prover and the verifier. Non-interactive form of sigma protocols also enforces honest participation of both prover and verifier. This important attribute increases the overall security of the proposed schema by reducing the risk that any of participants cheat.

The proposed construction based on two separate sub-systems enables externalization of user's identity from business transaction. This externalization represents the main information security advantage of the proposed protocol construction. Business transactions could be represented as records in databases where any data related to the identity of users is excluded from the record itself. In such a construction access to the database of transactions will not compromise privacy of users. At the same time every record could be validated since it cannot be created, modified, or deleted by a user that does not have verified identity. This statement is valid for business application users where the security of transactions is built within the business application itself. Individuals with privileged access rights to the transaction database, database administrators for example, could manipulate transaction records directly in the database and not through the business application. Their authentication does not have to be implemented within the authentication subsystem although it can be. The same applies to the authentication database. Two databases don't have to be administered by the same group of people. This would depend on the business requirements and operational implementation. In case of e-voting, it would be preferential to have different administrators of two databases. Securing a database itself is already covered in many information industry standards, for example within ISO/IEC 27002:2005, so it will be left out of the scope of our research.

The main operational advantage of the proposed protocol is in its very efficient performance. Validations within both sub-systems could be calculated very quickly and would require exchange of very short messages as described in previous chapters. Therefore, this schema is applicable to very large databases and data warehouses. Measurements of operational parameters are performed during the protocol simulations and are described in the following chapter.

5.2 Cryptographic protocols prototyping and related simulations

As mentioned in chapter 3, Sage mathematics is used for simulation of the proposed protocol. Sage mathematics is described in Stein et al [24]. It is an open-source project with the mission to offer a non-commercial replacement for proprietary applications for mathematical modeling and research. Its main advantages are flexibility

and ease of use. It already includes nearly hundred open-source packages with a unified interface. Its open architecture represents another advantage with the possibility to integrate new modules and packages for additional functionality. It is well documented and maintained with the current version 5.10 released in June 2013. Similarly to other open-source projects, Sage mathematics is open to voluntary contribution.

It is simple to obtain Sage mathematics and to start immediately using it on many computing platforms. The most straightforward way to start using it rapidly is to install virtual Sage mathematics appliance. The package is available as virtual appliance for Oracle VirtualBox⁹. VirtualBox is open-source software based on GNU General Public Licence (GPL). It exists for both x86 and AMD64/Intel64 architectures.

The purpose of prototyping a cryptographic protocol is to perform a proof of concept and demonstrate its feasibility. A protocol prototype is constructed using cryptographic primitives available within mathematic software modules. Examples of such primitives are pseudorandom number generators, one-way hash functions and other. Mathematic model of the protocol is implemented in Python based programming language that could be directly entered in the Sage mathematics notebook. The notebook is web-based users interface to Sage mathematics and could be accessed using any Internet browser. The code could be executed either on the virtual machine running on the local computer or on a Sage server over the network. For the purpose of this research Python code is entered in the Sage mathematics notebook within the Firefox browser on the same physical computer on which the Sage virtual appliance is running.

According to the Sage mathematics documentation its performance, when used as a virtual appliance, does not differ significantly from the performance of a physical Linux-based installation. Therefore, it could also be used as a platform for measuring performance of the proposed cryptographic protocol execution. Furthermore, benchmarks are published that compare Sage mathematics with other mathematic modeling software¹⁰. They illustrate favorable results particularly in areas relevant to cryptographic protocol modeling such as pseudoprimality testing, large integer multiplication, integer factoring and other.

The Sage mathematics source code of the proposed cryptographic protocol is available in the Annex 1. The current stable version 5.10 of Sage mathematics was used for simulations. Oracle VirtualBox version 4.2.14 was used as a platform for Sage mathematics virtual appliance. The host operating system used was Apple Mac OS X 10.8.4 running on Intel Core i5 2.4 GHz CPU with 4GB of RAM. The default memory allocation for virtual appliance in the VirtualBox settings is 512GB. This is not enough for calculation of large prime numbers and results in “out of memory” errors during simulations. Therefore 2GB of RAM memory was allocated to the virtual appliance.

As described in previous chapters, global parameters for the protocol are calculated in the first phase of the simulation. According to previously discussed minimum-security levels for parameters, sizes of calculated prime numbers are:

$$q = 72 \text{ bytes}$$

⁹ <https://www.virtualbox.org/>

¹⁰ <http://www.sagemath.org/tour-benchmarks.html>

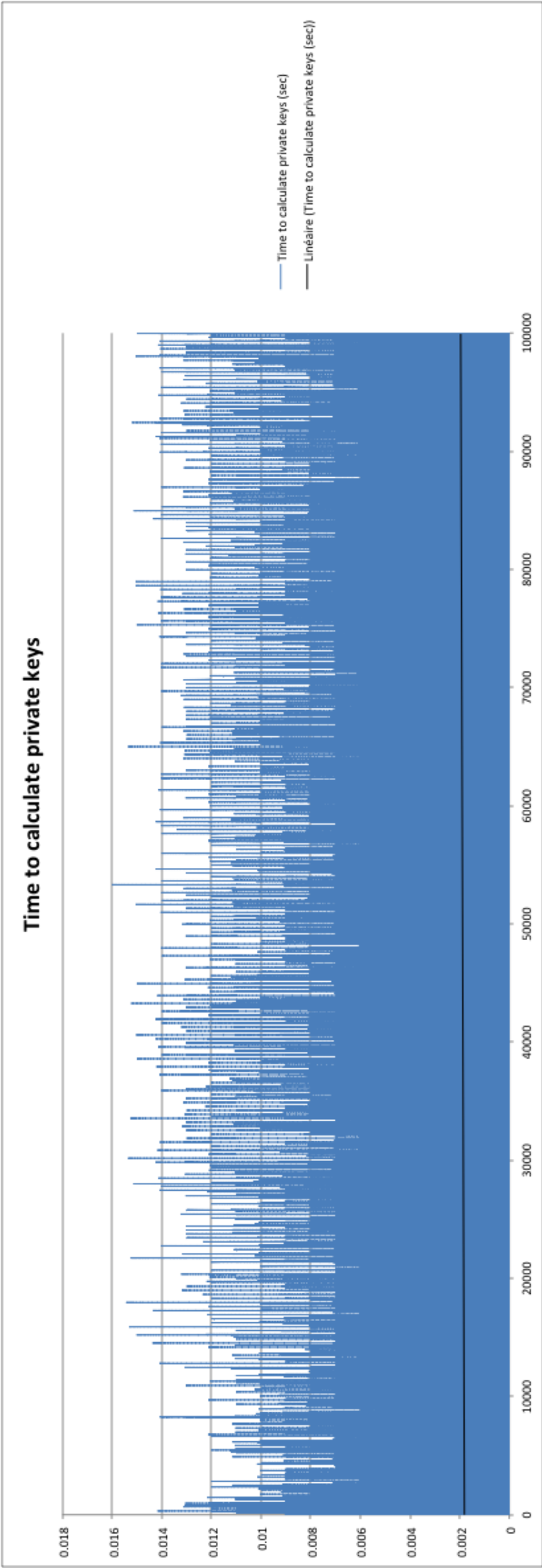
$p = 328$ bytes

Corresponding global parameter g is 668 bytes long.

CPU time spent on the virtual appliance to calculate global parameters was 124.597058 seconds.

To illustrate the performance advantage of Schnorr's cryptographic schema two simulations for the selection of private keys were performed on different scales. The first simulation consisted of the selection of 100,000 private key pairs. One key pair consists of the private key (w) and the corresponding public key (h). The longest time to select keys during the first simulation was 0.015998 seconds. The average time (calculated as the arithmetic mean) was 0.001881063 seconds. The standard deviation from the average time in the whole set of 100,000 measurements was 0.002514543 seconds. Total CPU time spent on the whole set was 240.341462 seconds. Simulation results are presented in the Figure 4.

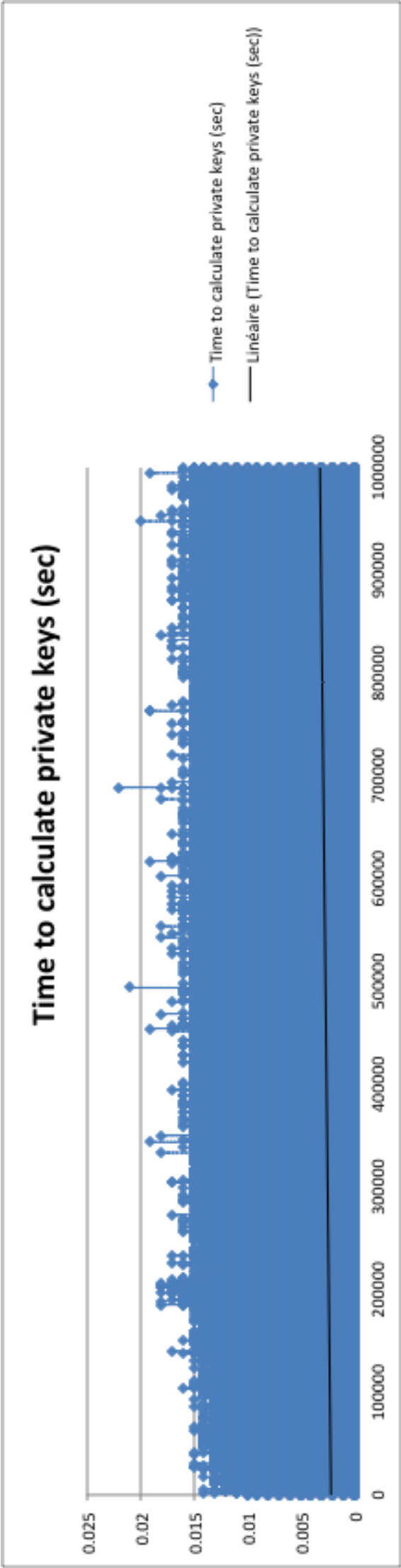
Figure 4



The second simulation consisted of selecting 1 million private key pairs. Total CPU time spent for this simulation was 3382.551774 seconds. For the whole population of 1 million CPU time measurements there was one outlier detected of 0.129981 seconds that was excluded from the analysis. The longest time measured was 0.021997 seconds. The average time (calculated as the arithmetic mean) was 0.002650144 seconds. The standard deviation from the average time in the whole set of 1,000,000 measurements was 0.003451083 seconds. Simulation results are presented in Figure 5.

Results from both simulations confirm expected high performance during the key selection phase of the protocol. Trend lines in both simulations are highlighted in Figures 4 and 5, and remain around 0.002 seconds.

Figure 5



Performance of the authentication subsystem was measured in the second phase of simulations. This phase consisted of 100,000 iterations of the complete OR-proof form of the sigma-protocol. In each iteration this protocol execution included selection of private key pairs, execution of the simulator, calculation of the challenge and the response, and verification. To recall, all this actions are illustrated in Figure 2. CPU time measurement excludes the selection of private key pairs. CPU time was separately measured for OR-sigma calculations and for verifications. Total CPU time to perform 100,000 iterations was 1578.660007 seconds. The longest time to perform OR-sigma calculations was 0.051993 seconds, while the longest time for verification was 0.045993 seconds. The average time (calculated as the arithmetic mean) for OR-sigma calculations was 0.007084014 seconds. The standard deviation from the average time in the whole set of 100,000 measurements was 0.007085706 seconds. Similarly the average time for verification was 0.006639869 seconds, while the standard deviation was 0.006890101 seconds. Simulation results are illustrated in Figures 6 and 7.

Figure 6

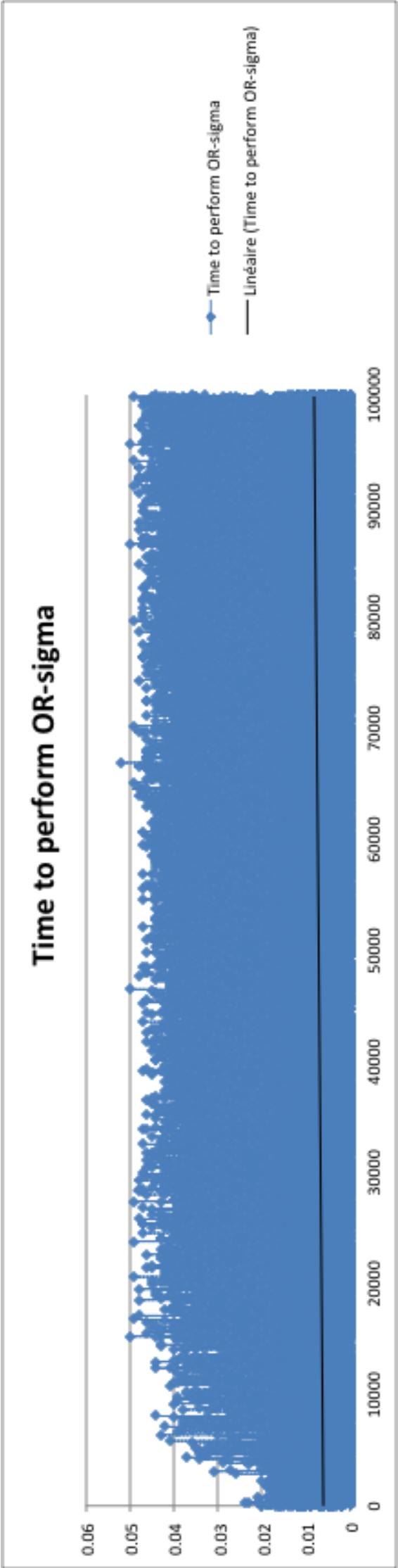
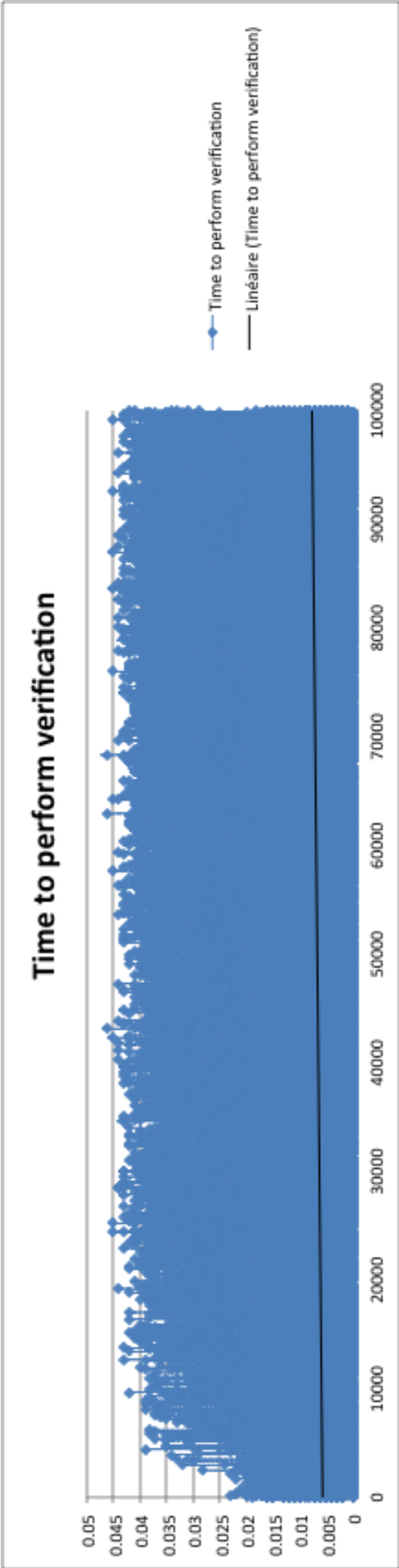


Figure 7



Performance of the authorization subsystem was measured in the final phase of simulation. As in the previous simulation phase 100,000 iterations of the noninteractive form of the sigma-protocol were performed. To recall, all this actions are illustrated in Figure 1. Total CPU time required was 13115.756103 seconds. Times required for protocol calculations and for verifications were measured separately. Time measurement of the first protocol iteration was 5.616146 seconds. This high value should be considered an outlier and excluded from analysis since it is due to the time required to import the hash code library. The longest time to perform non-interactive sigma-protocol calculations was 0.903863 seconds, while the longest time for verification was 0.034994 seconds. The average time (calculated as the arithmetic mean) for protocol calculations was 0.125878991 seconds. The standard deviation from the average time in the whole set of 100,000 measurements was 0.062016054 seconds. The average time for verification was 0.003094802 seconds, while the standard deviation was 0.003180809 seconds. Simulation results are presented in Figures 8 and 9.

Figure 8

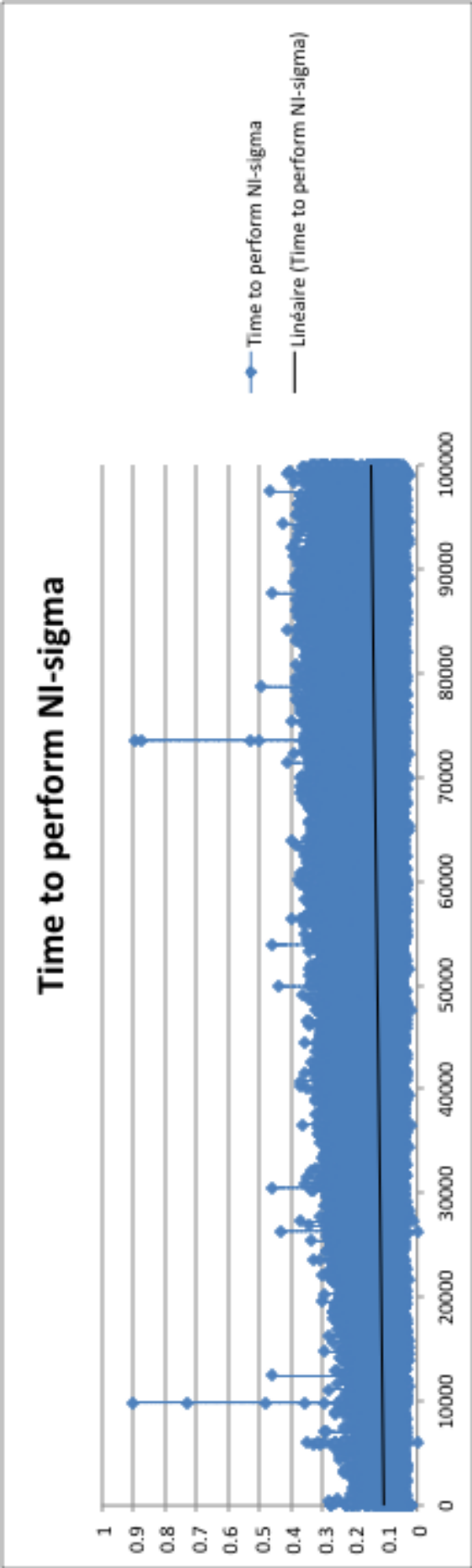
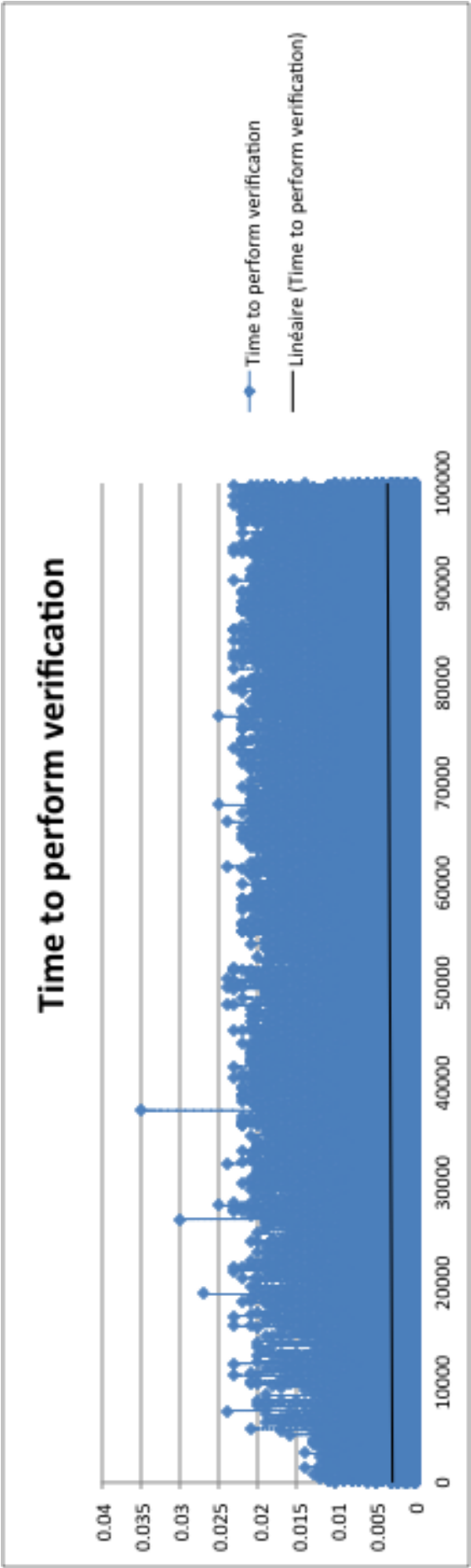


Figure 9



From above results it could be concluded that both subsystems are very fast even on large data sets. CPU time required for verification is comparable for both systems. While protocol calculations are much less CPU intensive for the OR-form than for the non-interactive form, it is important to highlight that OR-form requires more interaction between prover and verifier. That involves communication overhead that was not taken into consideration in this simulation. The communication is specific to the business-context of the protocol application. As stated earlier, for the purpose of this research all calculations were performed on the single physical computer. Therefore the communication overhead is minimal. Some implementations of the protocol may include communication over different kinds of data networks. Implementation specific simulations should be envisaged to take into account communication overhead.

5.3 Security analysis of the proposed protocol

Security evaluation of a cryptographic protocol consists of individual analysis of each component. Results should serve as input to the overall risk analysis process of the protocol with the objective to estimate the level of security of each component and to identify those components with the highest risk. A chain always breaks at the weakest link. That principle should guide the risk analysis of the protocol's security.

Risk is typically defined as the product of likelihood of occurrence of an event and the impact caused if that event actually occurs. The likelihood of occurrence of an event is determined by the degree of difficulty of exploiting vulnerability, by the skill of the attacker, and by the availability of software and hardware tools required for the exploit. Compromising security of the protocol could lead to unauthorized execution of business transactions, to repudiation or denial of transaction originator's identity, to disclosure of users' identities, and to denial of service. The proposed protocol consists of two subsystems as illustrated in Figure 3. Security of each subsystem relies on the security of cryptographic primitives used in its construction. In case of e-voting attacks on the authentication subsystem could result in compromise of the confidentiality and/or of the integrity of voters' private keys, on the integrity of public keys, and on the availability of authentication service. Attacks on the authorization subsystem could result in compromise of the integrity and/or availability of the voting verification process. Attack on the communication channel between two subsystems could result in unavailability of the e-voting service. Security of individual components of both the authentication and the authorization subsystem is analyzed in this chapter, and summarized in the overall risk analysis.

In chapter 3.2 it was already highlighted that the advancement of quantum computing could significantly reduce the time required to compromise private keys. Therefore its advancement should be closely followed by security professionals and adequate computationally difficult problem implemented in the protocol construction instead of a discrete logarithm problem in order to mitigate security risks. It is also important to define for how long the confidentiality and the integrity of private key pairs have to be protected. Since the proposed protocol is very efficient it allows the selection of new key pairs for each transaction even in applications with very high number of transactions. Selecting the size of protocol's global parameters is very important to maintain the security level of the construction at high enough level. The main reason for this is that it determines the level of difficulty required to brute force private key pairs. This is described in details in chapter 3.2. Guidelines provided in that chapter are used for the construction of the proposed protocol and are implemented in the calculation of global parameters.

Challenge-response interaction between communicating parties within the authorization subsystem is replaced with the random oracle implemented using the secure hash function as explained in chapter 4. The current widely adopted standard for implementation of secure hash functions is based on the set of secure hash algorithms (SHA-2), based on the elliptic curve digital signature algorithm, and published as a U.S. Federal Information Processing Standard (FIPS) 180-4 [25]. This standard specifies how to satisfy preimage resistance requirement. This requirement stipulates that it is computationally infeasible to find the original message when the message digest is only known. It also ensures collision resistance, or how to avoid that two messages produce

the same message digest. Four hash algorithms specified in this standard produce message digest of 224, 256, 384 or 512 bits. SHA-512 algorithm with truncation can be used when shorter message digest is required. That algorithm variant is designated as SHA-512/t (t being the length of the message digest measured in bits). Gueron et al [26] showed that using SHA-512 on 64 bit systems is significantly faster than SHA-256. As a result of this it is more beneficial on 64-bit platforms to use SHA-512/t to produce 256 bit message digest than the original SHA-256. Selection of the adequate output size for the message digest depends on the security requirements for the application. If above described requirements are not satisfied the risk is that a cheating prover convinces the verifier to accept a false proof. The probability that this actually happens is determined by the size of the message digest. This error is also called soundness in the formal definition of sigma-protocols. It equals 2^{-t} where t is the challenge length as explained in Damgard [19]. The problem of cheating verifier is mitigated with the usage of the secure hash function. This results from the random selection of challenge values. SHA-1 does not provide sufficient collision resistance as demonstrated in NIST SP 800-107 [27]. With less than 80 bits it is not strong enough for commercial digital signatures. For secure commercial implementations only SHA-256 or SHA-512 should be used. Collision resistance is respectively 128 bits for SHA-256, and 256 bits for SHA-512. Preimage resistance for SHA-256 is 256 bits, and 512 bits for SHA-512. Collisions can occur with higher probability when messages are selected from larger sets and the size of digest is short. Cryptanalysis considers two types of collision attacks on hash functions. One attack type is classical collision attack. The time to break the hash function in this attack is equal to $2^{n/2}$ where n is the hash length. This is due to the problem known as the birthday problem. Chosen-prefix collision attack is another form considered in cryptanalysis. MD5 algorithm was successfully broken using this type of attack. The approach is to calculate prefixes that produce equal hash values and to concatenate them to distinct messages. For illustration, the analysis of malware called “Flame” detected in 2012 discovered that chosen-prefix collision attack on MD5 algorithm was used to forge code-signing certificates used in Microsoft Windows operating system¹¹. This resulted in unauthorized installation of operating system components such as Terminal Service software developed by hackers. Interestingly, to prevent further attacks the vulnerable MD5 algorithm was replaced with also vulnerable SHA-1 as already described. Cryptanalysis further considers two types of preimage attacks on hash functions as described in Schneier [28]. In the first method the attacker attempts to find a message that produces expected digest in less than 2^n attempts (n represents length of the digest in bits). The alternative approach is to attempt finding another message that has the same digest in less than 2^n attempts when knowing one message and the corresponding digest. All hash algorithms considered to become industry standards are analyzed for their resistance to these types of attacks. This process is described in details in Fleischmann, Christian Forler, and Michael Gorski [29]. The research of Seurin [30] shows that the security of Schnorr’s signature scheme in the random oracle model mainly depends on the security of selected hash function. This is of a critical importance for the secure construction of the proposed cryptographic protocol. Taking into account results of this analysis of hash algorithm security aspects, SHA-512 was selected for construction of the proposed cryptographic protocol. For development of software applications using Python programming language, *hashlib* module

¹¹ <http://blogs.technet.com/b/srd/archive/2012/06/06/more-information-about-the-digital-certificates-used-to-sign-the-flame-malware.aspx>

represents a common interface to secure hash functions implemented in OpenSSL library. This module is used for the prototyping and simulations of the proposed cryptographic protocol and the source code is presented in Annex 1.

Pseudo-random generation function is another basic component of the proposed protocol whose weakness may significantly impact protocol's overall security. To ensure adequate security level of the protocol an appropriate cryptographically strong pseudo-random generator must be used. The measure of uncertainty in a random variable called entropy was already referenced in chapter 2.1. The entropy of randomly selected data variables in software applications depends on the implementation of the random generation function. There are many practical implementations that use deterministic algorithms such as middle-square method or Mersenne-twister. They are not cryptographically secure. Cryptographically secure implementations are based on probabilistic algorithms that use entropy source provided by the operating system and the underlying hardware. Those implementations typically combine an electronic signal from a data input device such as mouse or a keyboard as a source of randomness. Alternatively they may use the outcome of quantum-mechanical events at the sub-atomic level as high entropy source of randomness¹². Data captured is then combined with the time stamp and passed through the secure hash function in an attempt to create cryptographically secure pseudo random generator. Such a method for example is implemented in the OpenSSL library mentioned above¹³. The security of such a generator entirely relies on the SHA algorithm selected. SHA-1 algorithm is used for implementation of the *rand_method* in the OpenSSL. As stated earlier SHA-1 is vulnerable and should not be used for commercial cryptographic protocols. For the purpose of prototyping and simulation of the cryptographic protocol in this research the *rand_method* is adequate. To improve its accuracy the state of the generator is reset at the beginning of each protocol iteration. Industry standards such as FIPS 186-2 and NIST SP 800-90A define some cryptographically secure pseudo random number generator implementations. However, cryptanalyst community raised warnings already back in 2007 on the existence of certain undocumented variables predefined in proposed implementations¹⁴. This could significantly reduce the entropy of the generator. Non-controversial implementations were subsequently added. For commercial cryptographic implementations some safe alternatives such as Fortuna algorithm could be used. *Pycrypto* library in Python programming language offers implementation of the Fortuna algorithm¹⁵. Additional security analysis for the selection of a secure pseudo random number generation algorithm is required for the commercial implementation of the proposed protocol.

Cryptanalysis attacks on the proposed protocol could be mitigated with standard construction techniques for public key cryptography. Lets consider cryptanalysis attacks classified in relation to the type of information available to the attacker. In a chosen message attack, also called chosen plaintext attack, attacker has a possibility to select a

¹² <http://www.idquantique.com/images/stories/PDF/quantis-random-generator/quantis-whitepaper.pdf>

¹³ <http://www.openssl.org/docs/crypto/rand.html>

¹⁴

http://www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115

¹⁵ <https://github.com/dlitz/pycrypto/tree/master/lib/Crypto/Random/Fortuna>

plaintext to be encrypted and to obtain the corresponding ciphertext. By repeating such an attack with sufficient amount of data attacker may significantly reduce the level of protocol's security and eventually may discover the secret key. However, as stated in Goldreich [4], such attacks do not bring advantage in case of public key schemes. Implementation of sigma-protocols in both authentication and authorization subsystems would ensure security against eavesdropper attempting to compromise the encryption key. Moreover, an efficient cryptographic protocol implementation would permit frequent change of keys and thus reduce the time available to attackers for breaching the security of keys.

In a chosen ciphertext attack a cryptanalyst may choose a ciphertext and obtain the corresponding decrypted plaintext. Multiple repetitions of the attack may gather enough information for the discovery of a secret key. There are two forms of chosen ciphertext attacks as described in Goldreich [4]. One form is an a-priori-chosen ciphertext attack in which the attacker is given access to the public key used to encrypt the plaintext and is given the resulting ciphertext. The second attack form is an a-posteriori-chosen ciphertext attack in which the attacker has not been given access to the public key used to encrypt the particular ciphertext. In both forms attacker may chose an arbitrary text and key and apply encryption scheme on it. As demonstrated in Blum, Micali and Feldman [8] chosen ciphertext attacks on cryptographic protocols could be effectively mitigated by using non-interactive zero-knowledge proofs. In described protocol construction a prover sends to a verifier an encrypted message together with a non-interactive zero-knowledge proof that she knows the decryption of the message. A verifier would produce the plaintext only if the proof is valid, in other words, only if the prover knows the corresponding decrypted message. Such a construction of sigma-protocol is proposed in the authorization subsystem.

In an adaptive chosen ciphertext attack cryptanalyst could modify a ciphertext and obtain a decrypted plaintext that is similar to the original plaintext without knowing neither the secret key nor the original plaintext. This is also called ciphertext malleability. Attacker must have interactive access to the cryptographic protocol and perform a large number of repetitions in order to obtain the secret key. In 1998 Bleichenbacher [53] of Bell Labs demonstrated the first practical attack of this kind against the Public Key Cryptographic Standard (PKCS) version 1 of RSA Laboratories. Non-malleability or security against adaptive chosen ciphertext attacks could be ensured in cryptographic protocols with implementation of non-interactive zero-knowledge proofs. The encryption scheme proposed in Sang and Shen [14] applies non-interactive zero-knowledge proofs based on bilinear maps to ensure non-malleability. It is demonstrated that if a random oracle is added to the encryption scheme the probability that a cheating prover successfully guesses a proof becomes negligible. The authorization subsystem implemented with non-interactive sigma-protocol is therefore secure against this type of attacks.

Signature schemes constructed from sigma-protocols are secure against tampering with the secret key and are secure from tampering with the prover's state as demonstrated in Damgard et al [54]. Changing the private key and observing the effect of a change on the resulting ciphertext is known in cryptanalysis as a related key attack. Tampering with the prover's state may result in information leakage and facilitate cryptanalysis. A construction called floppy model is proposed to ensure tamper resilience. In this model each user has a hardware token with the update key. This key is

used only to refresh the private key stored and used in the cryptodevice that is exposed to potential tampering. Although related key attacks were traditionally targeting only symmetric encryption and specifically block ciphers, public key encryption security against these attacks is studied to ensure the security of digital signatures. Attacks on public keys signed with a certificate may be significant only if the attacker may tamper with certificate's parameters. It is demonstrated in Bellare, Cash, and Miller [55] that this type of attack is impractical that the attack would be confined only to the private key. Furthermore, it is concluded that public key related high-level cryptographic primitives used in digital signature schemes could be effectively secured against related key attacks.

Security analysis of OR-proof form of sigma-protocols is presented in Keller et al [33]. The proposed construction uses additional keys to ensure deniability characteristics of the protocol. In addition it concludes that the state of randomness should be reset after every protocol transaction to ensure the sufficient level of entropy. An efficient practical construction for shared electronic cash wallet is proposed. In essence, a private secret is shared among the group of a single e-wallet users that interact with a third party as if they were a single user without compromising their identity. The construction differs from other related work in the area of secure multi-party communication in demonstrating improved efficiency by using OR-form of sigma-protocols.

Non-interactive deniable protocols are sensitive to replay attacks as pointed out in Haibo et al [32]. In this form of attacks an eavesdropper records conversation that takes place within the protocol and retransmits at later time in order to impersonate a valid user. If successful this type of attack could result in the breach of access controls and unauthorized authentication to the information system. Usual replay attack mitigation includes adding a nonce to the message in the form of a random or pseudo-random number. Another technique involves adding a time-stamp but the practical implementation is more complex as it requires time synchronization between a prover and a verifier. Since in the proposed protocol construction a non-interactive sigma-protocol is used in the authorization and not in the authentication sub-system, adding a pseudo-random nonce would provide a satisfactory level of security against replay attacks.

Side channel attacks represent attacks on the implementation of the cryptosystem. Above-mentioned tampering with prover's state is one example of side channel attacks. These attacks examine variations in physical characteristics of the system that can provide additional information about overall cryptographic system operation and eventually reduce the amount of information required to compromise its security. Such physical characteristics may include information on power consumption variation, variations in time required for computation, variation in electromagnetic radiation used to write to input-output sub-systems of the computer system, acoustic variations in power transformation. While such low-level physical effects may not be considered critical for applications such as proposed electronic voting, other side channel attacks at software level should be considered.

Computer system security controls have been classified in already mentioned ISO/IEC 27002:2005 standard. For secure software implementation of cryptographic protocols it is also important to consider certain coding rules. An attempt to outline

cryptographic coding standard was presented at the Internet Crypto workshop¹⁶ in January 2013 by the Virtual Applications and Implementations Research Lab¹⁷ as part of the European Network of Excellence in Cryptology II¹⁸. The proposed standard present programming language independent set of rules¹⁹. Some rules address timing attacks on secret data for example in conditional branching or variable comparison. Certain rules address vulnerabilities introduced in the binary code by compilers through the code optimization phase. Other areas involve addressing vulnerabilities resulting from insecure use of Application Programming Interface (API) layer, particularly when calling external cryptographic primitives like pseudo-random number generators. Selection of certain data types could also be significant to avoid software vulnerabilities. For example using signed bytes to represent binary data may lead to memory heap corruption. Recommendations are also made to use different data types for private and public keys and how to ensure that memory used to store private keys is cleared when the value is no more needed for computing.

Electronic voting maybe implemented in the form of a Web based application. In that case it may be vulnerable to specific types of attacks such as various code injections, memory overflows, cross-site scripting, and other. The Open Web Application Security Project (OWASP)²⁰ focuses on improving the security of software through analysis of vulnerabilities, identification of threats, and presentation of mitigation measures. Various OWASP projects focus specifically on certain programming languages and development frameworks and related vulnerabilities.

Complete post-implementation security analysis may cover areas typically used during penetration testing. These are outlined in the Penetration Testing Execution Standard²¹ and include information gathering, technical and procedural vulnerability assessment, exploitation proof of concept through direct and indirect attacks, and reporting. Application of penetration testing on newly designed systems is particularly useful to compensate on the absence of the history of events such as security breaches. This information is necessary to estimate the likelihood of risk materializing. In reporting vulnerabilities it is important to use Common Vulnerabilities and Exposure (CVE) enumeration standard²². It provides measurable and comparable set of software weaknesses as well as the overview of tools and services to ensure secure architecture and design. The Common Vulnerability Scoring System (CVSS) provides a standard method for rating vulnerabilities²³. It takes into account metrics such as vulnerability exploitability that includes access vector and complexity, and availability of countermeasures. It also includes metrics of impact on confidentiality, integrity and availability estimated by expert assessment of the CVSS Special Interest Group. The impact level maybe used as a baseline from the industry best practice, but it maybe customized for specific information security business context.

¹⁶ <http://hyperelliptic.org/internetcrypto/>

¹⁷ <http://hyperelliptic.org/ECRYPTII/vampire/>

¹⁸ <http://www.ecrypt.eu.org/>

¹⁹ https://cryptocoding.net/index.php/Coding_rules

²⁰ <https://www.owasp.org>

²¹ <http://www.pentest-standard.org>

²² <http://cve.mitre.org/>

²³ <http://www.first.org/cvss>

As stated in the beginning of the chapter, a holistic approach to the risk analysis must be taken into account to evaluate business impact on critical information and each transaction before the practical protocol implementation. Each component of both subsystems must be assessed from the aspect of potential threats and known vulnerabilities and adequate protection measures, reviewed in this chapter, must be put in place. As security management is the ongoing process, regular periodic assessments must be performed to identify any new vulnerability and evaluate adequacy of technical and procedural control measures.

6 Privacy protection in e-Government applications

6.1 Introduction to e-Government

On the 21st December 2001 at its 56th session the General Assembly of the United Nations [37] adopted resolution on the World Summit on Information Society. It recognized the importance of Information and Communication technology (ICT) in the development of all countries. It has tasked International Telecommunication Union (ITU) to convene the summit on which governments, relevant United Nations bodies, intergovernmental organizations, non-governmental organizations, civil society, and the private sector would adopt a declaration and a plan of action for implementation. A declaration would voice the global consensus and commitment to promote access of all countries to information, knowledge and communication technologies.

At the summit held in December 2003 in Geneva 175 countries were represented at the high level with over 11'000 participants in total²⁴. The declaration of principles [38] was adopted recognizing that education, knowledge, information and communication are at the core of human progress, endeavor and well-being. One of the key principles highlights the role of governments, private sectors, civil society and United Nations and other international organizations in the decision-making process for building a people-centered Information Society. The importance of building confidence and security in the use of ICTs was recognized among other key principles. The development of Information Society would be impossible without protection of privacy, information security and network security. It has also highlighted that local authorities should implement applications for the benefit of their populations in the areas such as government services, health care and health information, education and training, employment, job creation, business, agriculture, transport, protection of environment and management of natural resources, disaster prevention, culture, and other.

Participants at the summit endorsed the action plan [39] that sets up time-bound targets for development of the Information Society. The summit recognized that the evolution of the Information Society is uneven across the World and that the development has to be adapted to particular needs of regions and individual countries. Specific targets have to be set at national level in the framework of national e-strategies and in accordance with national development strategies. Internationally agreed development goals would serve as benchmark targets for measuring the development progress. Among the action lines important focus is given to building confidence and security in the use of ICTs. Cooperation among the governments at the United Nations and other forums is essential to achieve global results within this action line and notably in enhancing user confidence in ICTs, building trust and protecting data and network integrity. Governments together with the private sector should develop guidelines and legislation to prevent, detect and respond to cybercrime and other misuse of ICTs. Governments also play the central role in user education and awareness for protecting online privacy. National legislation is vital to overcome obstacles to the use of authenticated electronic documents and transactions. In order to strengthen trust in using ICTs it is important to develop guidelines for protection of privacy, data and consumers. Sharing good practices and information on security incidents among countries is vital for effective cooperation. Development of reliable and secure

²⁴ <http://www.itu.int/wsis/geneva/newsroom/index.html>

applications should be encouraged in the area of e-government, e-business, e-learning, e-health, e-employment, e-environment, e-agriculture, and e-science. To achieve these goals Official Development Assistance (ODA) to developing countries is established with 0.7 per cent of gross national product from developed countries and donations through the voluntary Digital Solidarity Fund. A Composite ICT Development (Digital Opportunity) Index would be developed with each country and published annually, or every two years to follow-up and evaluate progress.

The second phase of the World Summit on Information Society took place in Tunis in November 2005 with over 19'000 participants reaffirming commitment [40] from Geneva to build people-centered and development-oriented Information Society based on the Charter of United Nations respecting the Universal Declaration of Human Rights. The summit endorsed Tunis Agenda [41] further developing financial mechanisms for meeting challenges of ICT for development. The summit recognized that Internet governance is one of central pillars for people-centric non-discriminatory Information Society. Participants committed to stability and security of Internet as a global facility and its governance based on full participation of all stakeholders. It supported the creation of the Working Group for Internet Governance (WGIG) by the UN Secretary General. The report of the WGIG²⁵ was presented that defined Internet Governance and related public policy issues. The lack of national legislation and global standards on data protection and privacy rights was identified among issues for Internet Governance. The summit in Tunis called upon the UN Secretary General to convene another Internet Governance Forum in 2006 and establish the regular forum meetings to ensure effective addressing of identified policy issues. The summit also called upon the UN Secretary General to establish a UN group on Information Society (UNGIS) within the UN system Chief Executives Board for coordination (CEB) consisting of the relevant UN bodies and organizations. This group would have a mandate to facilitate the implementation of WSIS outcomes. The summit designated the United Nations Economic and Social Council (ECOSOC) to oversee the system-wide follow-up of the Geneva and Tunis outcomes of WSIS. The ITU was tasked to maintain the Report on the Stocktaking of WSIS-related activities as a tool for assisting with the follow-up beyond the Tunis phase of the Summit. The summit identified possible facilitators for action lines defined in the plan of action adopted in Geneva. For the action line on building confidence and security in the use of ICT it assigned the ITU as facilitator. United Nations Department for Economic and Social affairs (UNDESA) together with United Nations Conference on Trade and Development (UNCTAD) were assigned to facilitate actions related to ICT applications in the area of e-government.

Division for Public Administration and Development Management of UNDESA focuses on e-government as part of its services offered to governments to improve their public administration and finance systems. It has developed and implemented a program called United Nations Public Administration Network (UNPAN). The objective of UNPAN is to establish an Internet-based network linking public administration institutions at regional and global levels. To achieve this mission UNPAN has developed a number of tools such as the United Nations E-Government Development Database (UNeGovDD) and the United Nations Global E-Readiness Reports and Survey.

²⁵ <http://www.wgig.org/docs/WGIGREPORT.pdf>

E-government is defined as the use of ICT and its application by the government for the provision of information and public services to the people. The aim of e-government therefore is to provide efficient government management of information to the citizen; better service delivery to citizens; and empowerment of the people through access to information and participation in public policy decision-making.²⁶

The Global E-Readiness Reports and Survey present assessment of how governments use ICTs to provide access to information and facilitate participation in public administration for all citizens. The aim of the survey is to identify countries as leaders in particular areas of e-government activities and those countries in need on further development of those activities. This way the survey provides valuable information for public administration practitioners on identifying gaps and methods for addressing them. Main features of e-government reviewed by the survey are: information dissemination and outreach, access and usability, service delivery capability, and citizen participation and interconnectedness of national and ministerial websites of United Nations member countries.²⁷ E-government development index and e-participation index are defined for measuring progress of each country.

E-government development index is a weighted average of three normalized scores of the most important aspects of e-government.²⁸ These are: scope and quality of online services, development status of telecommunications infrastructure, human capital. Each of these components can be analyzed independently. As technology evolves and consequently electronic services for public administration, different components of e-government are evaluated in every survey to reflect better these changes.

The key findings of the 2012 survey [42] have yet again placed Asia on the leading position in e-government development, followed by Europe and North America. African region is the least developed with on average 30% of North American index of development. The lack of ICT infrastructure is still the main reason for slow development. Another important finding is the trend of centralizing e-government model rather than silos single-purpose approach. This unified portal like model offers to citizen a single point for all e-government offered services and increases effectiveness and efficiency of public administration. While digital-divide is still very present, the progress in infrastructure development continues. The outreach of mobile communications to broader population is of a particular importance in rural areas. Many governments have started to deploy mobile applications for e-government, sometimes referred to as m-government. In those area with limited or no broadband access to the Internet applications even permit payments over mobile applications as the only available mean of citizen online participation in e-government. Privacy and security matters play particularly important roles in this unified approach to e-government. The importance of the legal framework to protect privacy of citizens' data is highlighted. Creation of the mutual transparency between public administration and citizen strengthen the confidence in privacy measures. Citizen must have access to its personal

²⁶ UN Public Administration Programme

http://unpan3.un.org/egovkb/egovernment_overview/ereadiness.htm

²⁷ <http://unpan1.un.org/intradoc/groups/public/documents/un/unpan029361.pdf>

²⁸ <http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan048590.pdf>

data in order to verify its use, accuracy and authenticity. A number of organizational and technical controls are identified to protect personal data, for example:

- Protecting premises and ICT assets;
- Protecting software applications used to process personal data;
- Protecting data in transfer over communication channels;
- Ensuring effective blocking, anonymization, erasing, and destruction of personal data;
- Recording and tracking data entry, access and processing time.

To ensure the integrity of online transactions it is essential to develop a framework for digital authentication. Digital signatures are recognized as an accepted way of identification and authentication in e-government. Some other advanced authentication and identification measures include using banking cards or ID cards. Centralizing e-government applications increases the importance of scalability as top security issue. Only about 20 per cent of national portals clearly indicate the presence of security controls. In 2012 survey findings, this was the case of almost half of countries in Europe, while only one portal in Africa.

The importance of cloud computing is highlighted with many governments putting pressure to consider it prior to putting in place any new ICT systems for public administration. Cloud computing with its processing and data storage virtualization significantly cuts IT operational costs and reduces the size of hardware used thus reducing the carbon footprint and energy consumption. Assurance of privacy protection and compliance with regulation is major challenge when adopting cloud computing. Outsourcing IT functions and services is still a strong trend also putting high expectation to security and privacy protection.

The progress of e-government in Serbia is particularly recognized in this survey as it advanced 30 positions in the global ranking to arrive at the 51st. E-government development index of Serbia in 2012 is 0.6312. For the matter of comparison, Switzerland with index 0.8134 occupies the 15th position in the global ranking. The republic of Korea with its index value of 0.9283 maintains the world leader position. It offers 87% of e-government services as listed by the UN. The main new offering represent mobile services with e-training and e-employment. Their portal is unified across national and local level authorities allowing more efficient finding of services and creating of preference profiles for users based on their age and other parameters. The Digital Agenda Authority in Serbia created e-government portal, based on the unified principle, integrating information from over 27 authorities at national and local levels.²⁹ This improvement enabled significant progress in the global ranking.

Confidence and trust of using e-governance applications have been mentioned as success factors in implementing them and achieving citizen participation. Transparency for governments as well as for citizen is important component in increasing confidence. Transparency in use of personal information is of a particular importance and it is regulated within privacy policy and related procedural and technical controls to enforce it. The right to privacy is essential human right in the modern information society, as well as the right to information. These two rights complement each other in holding

²⁹ <http://www.euprava.gov.rs/>

governments accountable to individuals. Mechanisms to identify and limit conflicts between these two rights have to be developed by governments. Main international instruments that define and regulate these two rights and mechanisms to address potential conflicts are reviewed in Banisar [43]. Right to information represents a fundamental right for citizen to access information held by government. It has to be applicable without having to show a legal interest in that information. Mechanisms for handling requests and time limits to respond have to be defined. Mechanisms for external review of information withholding have also to be implemented. Right to privacy grant individuals a right to control the collection of, access to, and use of personal information about them that is held by governments and other entities. Although the definition of privacy varies among countries some fundamental elements are common and defined at various levels of international and national legislation even within the Universal Declaration of Human Rights. Within the context of ICT its scope is to address issues relating to the collection, use, and dissemination of personal data. The most influential international instrument regulating protection of personal data is European Union Data Protection Directive [44].

6.2 European Union Data Protection Directive

European Union Data Protection Directive defines personal data as “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. Although very comprehensive in setting legal instruments as well as main protection principles, the directive is becoming obsolete. To overcome the obsolescence the European Commission has proposed in 2012 a reform of the Data Protection Directive.³⁰ Some key newly proposed changes are:

- The right to be “forgotten” that regulates personal data deletion;
- Consent for personal data processing that should be explicitly requested, not assumed;
- The right of data portability to facilitate transfer of data from one provider to another;
- Companies will have to notify on serious data breaches immediately;
- The single set of protection rules implemented across all EU member countries;
- Companies will have to deal with one single data protection authority within the member country of their establishment;
- Individuals could refer all cases to one single data protection authority of their establishment no matter in which country is their personal data processed;
- EU rules will apply to companies not established within the EU if they offer goods or services, or monitor the online behavior of citizens within the EU;
- Increasing responsibility and accountability of those processing data;
- Unnecessary administrative burdens will be removed;
- National data protection authorities will be strengthened.

³⁰ http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

The reform would adapt data protection rules to new development in technology and particularly for cloud computing, social networks, and other. Before it could be adopted it would have to be considered by the Council of Europe and the European Parliament. It is not expected to be adopted before 2016. Nevertheless it has already gained a lot of attention in media, trade and political debates. “Big data” companies, providers of principle social networks and cloud computing providers mostly those incorporated outside of the European Union strongly criticize the proposed reform claiming that it would favor EU based companies. Their main argument is that certain provisions are difficult to implement, incompatible with their business models and would significantly increase their operational costs. On the other hand, political lobbies of privacy defending groups are strongly supporting the reform claiming that it would protect fundamental rights of citizens already jeopardized by marketing-centric business models of Internet services companies that capture data on citizens and their online behavior and sell it without consent. Certain are even predicting trade wars with EU if the reform is adopted.³¹

In order to comply with the current EU directive and prevent US companies of losing overseas business the US Department of Commerce after the consultation with the European commission have put in place US-EU Safe Harbor Framework back in 1998.³² Under this framework US companies could certify compliance with the EU Privacy Protection Directive if they demonstrate due diligence with directive’s key principles such as clear and visible privacy policy, recourse mechanism, and verification mechanism. What is the root for the difference in the approach to privacy protection between the US and the EU? The EU has opted for strong legal and regulatory instruments for privacy protection. The reason for this is that the right for privacy, as stated earlier, is one of fundamental human rights in the EU. In the US approach to privacy protection is voluntary for companies in data processing business. It is their internal business decision to define and enforce privacy policy and protection rules and publicize on their Websites or elsewhere. Their customers may decide whether to use their services and products if they agree with privacy protection rules of the company. In certain areas of privacy protection like healthcare (HIPAA) and protection of children under the age of thirteen (COPPA) particular legal instruments have been put in place to reinforce privacy protection.³³ Nevertheless, consumer protection associations even from non-EU countries are supporting the reform of the EU Data Protection Directive.³⁴

Consequences for non-compliance with the EU privacy protection directive could be serious for companies ranging from such undertakings as ordering the company or institution to organize mandatory data protection training for all their staff, to monetary penalties. For example after the breach of millions of customers’ records of Sony Playstation Network in 2011, Sony Computer Entertainment Europe was fined with 250’000£.³⁵ Another example is a penalty of 100’000€ attributed to Google Inc in France

³¹ <http://www.wired.co.uk/news/archive/2013-02/01/eu-data-protection-us-trade-war>

³² <http://export.gov/safeharbor/>

³³ http://export.gov/safeharbor/eu/eg_main_018474.asp

³⁴ http://epic.org/privacy/intl/eu_data_protection_directive.html

³⁵

http://www.ico.org.uk/enforcement/~/_media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx

for violating privacy protection by collecting mobile users' personal data through GSM and WiFi networks while capturing data for its StreetView application.³⁶ Furthermore, a coordinated action of privacy protection authorities from EU member countries could raise the level of monetary fines to a company that neglected the privacy protection. As an illustration, Google Inc. was charged in Germany to pay a fine of 145'000€ for the same breach of privacy as it was charged in France.³⁷ Other EU member countries consider the similar process. In the United States coordinated actions of multiple states could raise levels of penalties to significant levels. For example, following the coordinated action of 38 states, Google Inc. have settled an investigation into Street View related data breach by payment of 7 million US\$.³⁸ Lobbyists for privacy protection in Europe claim that maximum level of monetary penalties defined by the current EU directive are not high enough to serve as deterrent measures against breaches of privacy. Google's annual revenues for 2012 were over 50 billion US\$.³⁹ Amount of fines for privacy breach mentioned above are insignificant compared to their total revenues. As a result of this, within the newly proposed EU privacy protection directive companies could be fined for the breach of privacy protection up to 2 per cent of their global annual turnover.⁴⁰

According to the Schengen agreement on transit of persons and goods without checks at interior borders among EU member states, a centralized Information System has been created to facilitate such transfers.⁴¹ The Schengen Information System (SIS) consists of national SIS subsystems interconnected to the central SIS located in Strasbourg in France. A disaster recovery site is located in Sankt Johann im Pongau in Austria. The system is managed by the EU Agency for large-scale IT systems.⁴² The system is vital tool for borderless transfers of person and goods as it allows registration only at the entrance at the Union's exterior border. The system has alerting functionality for missing persons and certain goods. It is used by border guards, customs, police, visa and judicial authorities throughout the Union and other countries that have joined the Schengen agreement but are not EU members (Iceland, Norway, and Switzerland). An updated version of the system (SIS II) has been implemented and went in production in April 2013.⁴³ This updated system has ability to process biometric data and has improved data protection controls. Personal data is protected in accordance with European Data Protection Act. Personal data is kept within the system maximum for 48 hours. All accesses to data are logged and citizens have rights to obtain information on

³⁶

<http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000023733987&fastReqId=1081573599&fastPos=4>

³⁷ <http://www.bloomberg.com/news/2013-04-22/google-fined-145-000-euros-over-wi-fi-data-collection-in-germany.html>

³⁸ <http://www.reuters.com/article/2013/03/12/us-google-wifi-fine-idUSBRE92B0VX20130312>

³⁹ <http://investor.google.com/financial/tables.html>

⁴⁰ http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en

⁴¹ <http://www.consilium.europa.eu/policies/council-configurations/justice-et-affaires-interieures-%28jai%29/sirene-schengen-information-system.aspx?lang=en/#?lang=en>

⁴² http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/agency/index_en.htm

⁴³ http://ec.europa.eu/dgs/home-affairs/what-is-new/news/news/2013/20130409_01_en.htm

their personal data usage. Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and data concerning health or sex life are prohibited to be stored within the system. The European Data Protection Supervisor verifies the application of data protection act. The system is audited every 4 years and audit reports submitted to the Council of Europe.⁴⁴ Although this system represents a good example of the application of the data protection act, its size in terms of the amount of data stored and processed and its importance for national and individual safety and security requires maintaining the level of information security risk as high in risk assessments. Consequently technical and procedural controls for data protection must be regularly assessed for their adequacy against new emerging threats.

6.3 Swiss Federal Act on Data Protection

In Switzerland the approach to privacy protection is similar to that in the European Union. It is formalized within the Swiss Federal Act of 19 June 1992 on Data Protection [45]. The emphasis is on data protection assessments and control by companies that store and process personal data. In addition it regulates cross-boarder data transfer and related protection by companies established outside Swiss confederation. Other principles cover data accuracy, access control, consent requirement, and other. The federal act assigns controlling authority and penalties for non-compliance. Due to its similarity with the EU Privacy Protection Directive it has resulted in the similar agreement with the US authority to certify US based companies for compliance with principles for privacy protection defined within the Safe Harbor Framework.

The Swiss Federal Act was updated in 2006 to strengthen certain elements of privacy protection that reflect evolution of technology and evolution of business models for ICT operation.⁴⁵ In particular this covers national and international ICT outsourcing. Stricter requirements for consent of individuals are defined in case of international data transfers of personal data. Assessments of data protection controls are recognized only when performed by accredited independent auditors in accordance with international audit standards. All companies and individuals that store and process personal data and communicate them regularly with third parties must be registered in the federal register for data protection. Federal data protection office oversees and manages this register. The updated act also defines pilot tests and projects with new technologies that would process personal data and that may eventually require new laws and regulations. This particular article gives authority to the Federal Council to permits such pilot project in case it judges that adequate data protection measures are put in place. Certain exceptions for data exchange regulation are defined in legal and investigative cases of national or international character and are published within the act update of 2010. That most recent update is defined in accordance with the Schengen agreement.⁴⁶

⁴⁴

http://europa.eu/legislation_summaries/justice_freedom_security/free_movement_of_persons_asylum_immigration/l14544_en.htm

⁴⁵ <http://www.admin.ch/ch/f/as/2007/4983.pdf>

⁴⁶ <http://www.admin.ch/ch/f/as/2010/3387.pdf>

In addition to the Act on Data Protection Switzerland has adopted the Freedom of Information Act⁴⁷ that regulates transparency in public administration. This act gives right to every citizen to inspect any public document with some exceptions related to national security.

Federal commissioner for data protection⁴⁸ ensures the implementation of federal transparency act. Its role is advisory and is related to the cases at the federal level. The commissioner also serves as the mediator in case of disputes. In its annual report for 2011/2012 the commissioner proposed several improvement measures for data protection to the Swiss Federal Council.⁴⁹ Among those proposed measure is the recommendation to promote the use of technical data protection.

Data protection supervisor at the cantonal level oversees data protection and transparency implemented by public administration authorities, provides counseling and mediation in case of conflicts. In the canton of Geneva this function has been established in 2010.⁵⁰ It provides template documents for citizens to facilitate their request for personal data information, modification or erasure from private and public registries. It also coordinates awareness training for citizen and private sector companies. In its report of activities for 2012 data protection supervisor listed 865 public and private entities registered for personal data processing in Geneva.⁵¹ 446 public administration institutions are listed in the registry as of 9 April 2013.⁵²

In January 2013 a potential breach of data confidentiality by fiscal authorities of Geneva was revealed in media.⁵³ The authorities were accused of unlawfully contracting a French company to process confidential tax related citizens' data. The government denied that data were sent across the border. Outsourcing company processed data locally in Switzerland. However, the government admitted that data were not anonymized or encrypted and therefore were accessed by employees of the company in question. Data protection controls in place were purely contractual and relied on employees' background checks that were performed by the outsourcing company. Those checks included reviews of staffs' legal records. The government recognized that these controls were not sufficient to ensure adequate data protection and committed to undertake system audit and to consider implementing encryption as immediate risk mitigation action. Tax declaration system in Geneva is digitized in all its phases starting from data capture.⁵⁴ Citizens and companies have a possibility to complete tax declaration forms electronically on their personal computers and to submit them over the Internet. It is not possible to sign them electronically due to legal gaps in electronic digital signature system. Nevertheless, the only page from the declaration that has to be mailed traditionally is the cover page containing hand signature and the bar code linking

⁴⁷ http://www.admin.ch/ch/e/rs/152_3/index.html

⁴⁸ <http://www.edoeb.admin.ch/index.html?lang=fr>

⁴⁹

<http://www.edoeb.admin.ch/dokumentation/00153/00154/00178/index.html?lang=fr>

⁵⁰ <http://www.ge.ch/ppdt/bureau/presentation.asp>

⁵¹ http://www.ge.ch/ppdt/doc/documentations/PPDT_rapport_activite_2012.pdf

⁵² www.ge.ch/ppdt/doc/Institutions_soumises_a_la_LIPAD-site_PPDt.xls

⁵³ <http://www.tdg.ch/geneve/actu-genevoise/donnees-fiscales-etat-avoue-faille-securite/story/29857219>

⁵⁴ <http://www.getax.ch/>

it to the electronic tax declaration. This is yet another example where despite the existence of adequate legislation, technical and procedural data protection controls in place do not effectively serve their purpose.

6.4 Russian Federal Law on Personal Data

Russian Federation has adopted the Federal law on personal data in July 2006. [46]. This law regulates protection of personal data in compliance with the constitutional right to dignity and privacy of citizens.

Personal data are defined as data about individuals that allow their identification. This includes:

- last name, first name, and middle name;
- day, month, and year of birth;
- address;
- family, social, and property situation;
- education;
- profession;
- revenue, and other.

Actions on personal data that are regulated within the scope of this law include:

- collection,
- systematization,
- storage,
- modification,
- use,
- access,
- transfer,
- blocking,
- and destruction.

Requirement for data correctness and authenticity is one of main principles for personal data processing. Another important principle is timeliness. This principle related to the time period that data is need. Upon expiration of this time period data must be destroyed from the file. Personal data may be processed only by authorized subjects who have to demonstrate due diligence in data protection. Personal data cannot be collected without consent of concerned individual except under a few defined circumstances such as for statistical and research purposes, for investigative professional journalism, for safety and security, for legal investigation, and for protection of national interests. All above provisions must also be assured in case of personal data transfer to a third party. The law emphasizes the principle that all personal data must be treated as confidential.

The law defines procedures for written consent that concerned individuals have to provide prior of their data being collected, stored and processed. This includes providing consent on behalf of those concerned individuals that are unable to provide it for themselves, or providing consent in relation to personal data about deceased people. Particular importance is given to biometric data that could only be collected and

processed with the consent of related subjects. The sole exception is in judicial cases, and in cases where protection of national safety and security must be ensured.

International data transfers are permitted only in cases when adequate measures of data protection could be verified and assured. This requirement could be waived in cases when the written consent of concerned individuals is provided, when the transfer is performed in the interest for safety and security of a concerned individual, and in cases of national security importance.

Concerned individual has right to access its own personal data. Procedures for this access are defined within the law.

Entities authorized to process personal data are obliged to notify concerned individuals on their data usage. In addition, the law defines technical and procedural controls that have to be put in place to ensure adequate data protection. These controls include cryptographic protection, access control, information system protection and storage media protection.

The law defines the supervisory role and related responsibilities that are assigned to the authorized federal agency for personal data protection⁵⁵. The main role of this agency is to protect rights of data subjects. This includes inspection of protection measures implemented by authorized data processing entities, providing opinion to data subjects on compliance issues, and acting in cases of non-compliance with this law. The agency reports to the president of the Russian Federation, to the Government, and to the National Assembly. Reports on its work are published in media on the annual basis.

In May 2013 the law was updated to comply with the European Union directive on personal data protection.⁵⁶ This update regulates particularly sensitive categories of personal data such as data on political, religious and union association. In addition it defines simplified procedures for data transfer to external entities and related protection.

The agency for personal data protection is responsible for maintaining the register of entities certified for personal data processing. These entities, also called personal data operators, could be private and individual companies, public companies, local, regional and federal authorities. The registry, that is publicly available, listed 274'647 certified entities as of 11 May 2013.⁵⁷ To illustrate the growth of the number of registered personal data operators, the registry listed 170'000 entities at the end of 2010.⁵⁸ Private companies represented 69.9% of registered data operators. In 2010, the agency estimated that in the Russian federation there were between 2 and 2.5 million personal data operators. Therefore, despite the growth of the number of registered operators, it still represents approximately only 10% of all operators.

In 2010, the agency inspected 1253 personal data operators. This resulted in 1908 reports on non-compliance with the law and 2996 legal proceedings. The total

⁵⁵ <http://www.rsoc.ru>

⁵⁶ http://minsvyaz.ru/ru/news/index.php?id_4=43756

⁵⁷ <http://www.pd.rsoc.ru/>

⁵⁸ http://www.pd.rsoc.ru/docs/Otchet_Upolnomochennogo_organov_za_2010_g.pdf

amount of monetary penalties was 4.48 million Rubles (109'980€⁵⁹) compared to only 75 thousands Rubles (1'841€) a year earlier. Individual complaints to the agency almost quadrupled compared to the previous year from 465 to 1829 cases. Most of the cases were related to the processing of data without written consent of concerned subjects, for unauthorized data transfer to third parties, and for the breach of confidentiality. In most of the cases data operators were credit companies, media companies, and local authorities. According to its 2012 report on work⁶⁰ the agency performed inspection on 951 private entities and 175 public authorities certified for personal data processing.

In 2011, the agency inspected 2231 personal data operators resulting in 2250 reports on non-compliance with the law and 4315 legal proceedings.⁶¹ The amount of monetary penalties almost doubled compared to the previous year totaling 7.9 million Rubles (193'939€). 3920 individual complaints were recorded, almost double more than the previous year.

Similarly to the situation in European Union, Russian Federation is facing the situation where breaches of legislation are present and are statistically increasing with the increase of the sample size. Obviously monetary fines for non-compliance are not adequately high to motivate companies to implement expensive data protection measures.

6.5 Serbian Law on Personal Data Protection

Law on personal data protection of the Republic of Serbia was published on the 27th of October 2008 [47]. The law defines personal data as any information relating to a natural person, regardless of its form of presentation or the medium used, and regardless of the date of its creation or the place of its storage. Natural person is defined as any individual identified or identifiable on the basis of his/her proper name, unique personal identification number, address code or any other distinguishing feature of his/her physical, psychological, spiritual, economic, cultural or social identity. The purpose of this law is to enable every natural person to exercise and have recourse to protection of their right to privacy and other rights and freedoms in the context of personal data protection. The law defines some exception to its scope such as data collected in publicly accessible official archives or museum, data collected by families for their own purposes and not available to third parties, data collected with the full consent of the subject person, and data published on oneself by a person capable of taking care of its own interests. In addition, data collected for statistical or historical research and not used in decision-making or against the person concerned is exempted from this law providing that it is adequately protected with safeguards. The law puts an emphasis on the requirements to provide full consent for any authorization to store and process personal data, including those of deceased persons. The consent could be given only in written or recorded form by concerned individual or individual with the power of attorney. Exceptions to this are only covered in cases of legal nature, national interest or for the protection of concerned person. The law defines details on the modalities of

⁵⁹

http://www.cbr.ru/eng/currency_base/daily.aspx?C_month=05&C_year=2013&date_req=14.05.2013

⁶⁰ <http://www.rsoc.ru/docstore/doc1209.htm?print=1>

⁶¹ http://www.rsoc.ru/docs/Otchet_Upolnomochennogo_organa_za_2011_g.doc

data collection and of obligations to notify concerned persons on data processing. Data relating to ethnicity, race, gender, language, religion, political party affiliation, trade union membership, health status, receipt of social support, victims of violence, criminal record and sexual life are defined as particularly sensitive and its processing is restricted even with the subject's consent.

To enforce transparency in personal data usage, the law protects the right of citizens to be informed on all aspects of data usage. This includes what data types are used, by whom, where, for what purpose, under what legal ground, when, for how long, and what was the source for collection. Citizens have the right to access and copy data relating to themselves. Citizens also have rights to request deletion, correction, modification or update of their personal data in case that data protection requirements by this law are not met. In relation to this right concerned data subject may request suspension of data processing from the moment they have challenged the correctness until a decision is made. Monetary penalties are defined for infringements of this law.

The law on personal data protection defines the role and responsibilities of the Commissioner for Information of Public Importance and Personal Data Protection as an autonomous public authority who exercises his/her powers independently.⁶² The role of the commissioner is to supervise the enforcement of data protection, to decide on appeals, to point out on cases of abuse, to give opinion on data protection aspects defined by this law, to monitor the implementation and suggest improvements, to maintain the list of countries and international organizations with adequate provisions on data protection, to maintain the central register of data controllers, and any other related duties. The commissioner provides his/her reports to the National Assembly, to the President of the Republic, to the Government and to the Ombudsperson, as well as to the general public. The commissioner maintains the central register of files that contain personal data.⁶³ Processing entities have a duty to provide information on data files they maintain to the commissioner within 15 days of data file creation or modification. The register contains details on types of data, processing activities, time, purpose, legal grounds, methods, transfers, safeguards, and business names and contact details. The register is publicly available.

Trans-border transfer of data is permitted only to countries that have ratified the Convention for the protection of individuals of the Council of Europe, or countries and organizations that comply with provisions set forth by this convention as designated by the commissioner.

According to the commissioners report on activities for 2012⁶⁴ the register of data controllers listed only 849 entities. The commissioner estimated that in Serbia there are approximately 350'000 controllers of personal data each operating multiple data files with personal data. In overall it is estimated that there are more than one million data files with personal data. Registered data controllers submitted information on 4'637 data files they keep, most of which are kept by private companies (2'200), followed by public authorities (1'408). Despite commissioner efforts through media

⁶² <http://www.poverenik.org.rs/>

⁶³ <http://www.poverenik.org.rs/registar/>

⁶⁴ <http://www.poverenik.org.rs/images/stories/dokumentacija-nova/izvestajiPoverenika/2012/enizvestaj2012.pdf>

campaigns and direct notifications to data controllers the number of registered data files is extremely low.

In the field of personal data protection the commissioner received 1'405 cases. As a result of 184 preliminary checks irregularities were found in 118 cases. The commissioner carried out 365 inspections and found 223 violations of the law in 103 cases. That signifies multiple violations by certain individual data controllers. In majority of cases (23.65%) the reason for inspection was data processing without consent by the data subject. It is followed by the excessive processing of personal data (15.27% of cases), and the processing of Unique Personal Identification Number as an unnecessary piece of information. In 39.91% of cases the violation of the law was due to the failure to create records of data processing and to submit them to the Commissioner. It is followed by the excessive processing of personal data (19.28% of cases) and the processing of data without proper legal basis (15.70% of cases). In 55.37% of cases the commissioner issued a warning against irregularities. In 28.93% of cases the commissioner issued petitions for initiation of infringement. Other measures include proceedings for violation of law, decisions for ordering controllers to implement various measures, and criminal reports for committed criminal offences. By 31 December 2012 no judgments were passed by Magistrates' Courts for any of petitions issued by the commissioner. The commissioner reported of serious difficulties in enforcing its decisions that are largely ignored by data controllers that not only refuse to act upon decisions, but also refuse to pay fines for violation of the law. To illustrate the level of effectiveness of penalties, in 2013 one judgment was passed pursuant a petition of the Commissioner filed in 2012. The defendants, a health institution and its responsible person, received fines of 100'000 Dinars (894.5€⁶⁵) and 30'000 Dinars (268.4€) respectively. The commissioner appealed to the Government to enforce the application of law by adequate measures.

This illustrates that the situation in the domain of personal data protection in Republic of Serbia is not different than in the European Union or in Russian Federation and that it requires serious attention not only by authorities but also by professional experts in information security to raise the importance of information systems auditing, information security assessments and improve technical and procedural protection controls in place.

6.6 e-Government framework for assessing privacy readiness

Despite the existence of legal base for personal data protection and the existence of national authorities to supervise enforcement of protective measures defined by law, it could be concluded from reviews earlier in this chapter, that the legal framework alone is ineffective to ensure data protection. Enforcement of the application of law is fundamental in order to achieve its objective and provide adequate data protection. Penalties have certain effect on companies to follow due diligence in data protection and to put in place procedural and technical controls. Penalties however have to be strong enough to dissuade data controllers from accepting risks for being fined for law infringements. The ineffectiveness of legal protection reflects negatively on building of trust in using e-Government applications that involve processing of personal data.

⁶⁵ <http://www.nbs.rs/internet/cirilica/scripts/ondate.html>

In the framework for assessing privacy readiness of e-government, proposed by Kessler et al [48], e-government systems are evaluated from three requirement aspects: policy, technology, and citizen. Their level of privacy readiness could be mapped into one of five maturity stages. The first stage designated as information stage, represents one-way government to citizen information. The next stage, communication, represents two-way flow of electronic information between a government and citizens. The following, transaction stage, corresponds to service delivery oriented integrated communication. It is further developed into integration stage that breaks departmental silos into sharing transactional information across multiple government departments. The highest maturity level, participation stage, reflects ability for political participation such as electronic voting. Policy requirements mapped into each maturity level are as follow:

- Basic policies for information collection,
- Policies defining how data is used,
- Policies on Government accountability,
- Policies detailing roles and responsibilities of the information handler and cross-departmental information sharing,
- And finally policies that govern how a citizen can obtain control over the data a government has collected.

Technology requirements in the first maturity level focus on methods of collection of information in the transparent manner. In the further stage encryption and secured storage are defined to protect two-way communication. The following stage ensures protection and completeness of transactional information. Highly granular role based access control management is in the focus of the fourth stage. At the highest stage informational self-determination allows citizen to define which government departments have access to which personal data.

Citizen requirements in the most basic form represent citizen awareness of privacy issues. The second stage focuses on building trust by citizens in e-government privacy. Once the trust is established the decision on transactions is evaluated in the third stage. Empowering citizens to decide on which data is collected and how it is used is defined within the fourth stage. Finally at the fifth stage of maturity, high level of granularity gives further rights to the citizen to have full control over its own information.

The study examines two cases and concludes that meeting two of three requirements does not lead to higher maturity levels. For example, policy and technology alone, without meeting citizen expectations, cannot lead to the success of e-government application. The proposed framework could be used to identify issues in successful implementation of e-government systems as well as to compare systems from the aspect of privacy protection.

Security is as strong as the weakest link in the protection chain. What are the guarantees to a citizen that its personal data will be sufficiently protected throughout all e-government systems so that she actively uses them with confidence? Encryption is certainly very efficient among technical preventive measures. However, it is complex and carries out new risks that could result in a false sense of security, or even in abuse of control measures for committing unlawful acts. Is it worth investing in the development and implementation of complex encryption protocols to protect personal data in e-

government systems? Who should lead such a project? Who and how should oversee its implementation and measure its effectiveness over time?

Trust in society is defined in Fukuyama [49] as the expectation that arises within a community of regular, honest, and cooperative behavior, based on commonly shared norms, on the part of other members of that community. The scope of norms at the scale of society varies from deep moral and ethical values to professional standards and codes of practice.

In Schneier [50] societal pressures, as systems through which a society induces trustworthiness, are divided in four categories. These four categories are: moral pressure, reputational pressure, institutional pressure and security systems. These categories operate at different scales. Moral pressures work best in small groups. Reputational pressures are effective in small to medium-sized groups. Institutional pressures are mostly effective in large-scale groups. Security systems, however, can be effective at different scales. They may range from personal protection measures to global interconnected security systems. In addition of representing an individual category, security systems can enhance other three categories to scale better. The main objective of societal pressures is to reduce defection. Because e-government applications scale to large groups, institutional pressures should be enhanced with security systems to ensure personal data protection at all scales. Ideally individuals should be able to control the use of their own data in order to fully trust e-government applications. In addition, defection of both e-government users and data operators should be reduced to maintain collective trust in systems.

6.7 Auditing e-Government applications

An audit is an independent, systematic and repeatable evaluation of controls, processes, and records, to assess their compliance with organizational and/or regulatory requirements, standards, or to assess effectiveness of controls. In addition to financial audits there are audits of other business processes, or integrated audits of organizational governance. Specific types of audits are quality audits, operations audits, performance audits, and other. Therefore an information systems audit is an audit of IS and the processes that support them including service delivery, change and configuration management, security management, systems development life cycle, business relationship and supplier management, and incident and problem management. An IS auditor interviews personnel, gathers and analyzes evidence, and delivers a written opinion on the effectiveness of controls assessed.

Formal planning precedes every audit and includes following steps:

- Defining the audit purpose: In this phase audited organization and auditor define the purpose why an audit is conducted, for example to determine the level of compliance to a particular policy, or to assess if previously identified vulnerabilities have been effectively addressed.
- Establishing the scope of audit: The scope of audit could cover a single information system, specific period, one single subsidiary within the organization, or other aspect limiting the focus of the audit.
- Estimating the level of risk: The auditor has to estimate the level of risk relevant for the system being audited in order to estimate required resources for the audit. Two aspects of risk have to be taken into account.

The absolute level of risk that could affect the audited domain, and the relative risk level compared to previously identified deficiencies.

- Defining the audit procedures: Based on established purpose and scope auditors would define procedures to select adequate audit techniques, tools and skills.

ISACA⁶⁶ is an international professional association that publishes IS auditing standards, guidelines and procedures. It maintains the certification process for IS auditors which requires compliance with the code of ethics, passing the certification exam, and continuous training.

An audit of information systems security may have an objective to assess compliance with information security standards. International Standardization Organization (ISO) published a series of standards on information security techniques. These standards are known as 27000 series standards. ISO/IEC 27001:2005 [51] is an international standard on Information security management systems. It is applicable to all types and sizes of organizations, including governments. Organizations may obtain certification against this standard to demonstrate that their information security programs are aligned with industry best practices. According to this standard, the information security management process is based on the assessment and prioritization of information security risks in line with organizational strategic risk management, organizational information classification policy and any other organizational and legal requirements. An information security risk treatment plan is central to the information security management process. Control objectives and controls for risk treatment are defined within the complementary ISO/IEC 27002:2005 [52] standard for the code of practice for information security management. This standard contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development and maintenance;
- Information security incident management;
- Business continuity management;
- Compliance.

ISO/IEC 27000 series of standards are frequently used by internal and external auditors to determine the degree of compliance with policies adopted by an organization.

Different sets of audit standards are issued by associations of accountants. The American Institute of Certified Public Accountants (AICPA) issued the Statement on

⁶⁶ <https://www.isaca.org>

Standards for Attestation Engagements (SSAE) No. 16⁶⁷ including the Service Organization Control (SOC) reporting framework (SOC 1, 2, 3). The International Federation of Accountants (IFAC) issued the International Standard On Assurance Engagements (ISAE) No. 3402 - Assurance Reports On Controls At A Service Organization⁶⁸. Both standards are based on the former U.S. Statement on Auditing Standards No. 70 (SAS 70). The main difference is that SSAE 16 is an "attestation" standard while ISAE 3402 is an "assurance" standard. The former is more widely used in the United States while the latter is commonly used in the rest of the world. While both standards require the management to provide a description of systems and controls, there are some fundamental differences related to the audit process. The most important difference is that SSAE 16 requires an auditor to investigate all relevant details when detecting a deviation that may be the result of an intentional act by an employee. There are two types of audit reports based on above standards. Type I reports focus on the design of controls while type II reports focus on the effectiveness of controls.

The principal difference between ISO 27000 series of standards and ISAE/SSAE standards are in the scope of applicability. Certification against ISO 27000 standards ensures that all categories of controls defined by these standards are implemented within an organization. For audits based on ISAE/SSAE standards it is audited organization that defines the scope of audit. Consequently these audits do not necessarily cover all areas of controls defined by ISO 27000 standards.

Although proprietary, Payment Card Industry Data Security Standard (PCI DSS) is important assurance standard for organizations that process, store, and transmit credit card data. Credit card companies such as Visa and MasterCard require merchants and service providers to be validated annually for compliance with this standard. Small merchants have to implement all controls specified by this standard but are not required to validate it annually. The standard specifies protection requirements in the following areas:

- Securing networks;
- Protecting card holder data;
- Maintain a vulnerability management program;
- Implement access control measures;
- Monitor and test networks;
- Maintain an information security policy.

In addition to the standard, the PCI Security Standards Council⁶⁹ released information supplements such as Cloud Computing Guidelines, Wireless Guidelines, eCommerce Guidelines, and other. Cloud Computing Guidelines for example provide clarifications on responsibility delineation between Cloud Service Providers and client organizations. At the time when cloud computing becomes wider adopted among corporate IT organizations the importance of security compliance becomes a vital requirement. Given the complexity of data flow depending on the cloud architecture

⁶⁷ <http://www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx>

⁶⁸ <http://www.ifac.org/sites/default/files/downloads/b014-2010-iaasb-handbook-isae-3402.pdf>

⁶⁹ https://www.pcisecuritystandards.org/security_standards/

precise scope of responsibilities for ensuring maintenance of adequate security controls in the above categories is of a paramount importance. Credit card companies require their business partners not to take security for granted when subcontracting cloud computing services. Therefore it is important for organizations seeking PCI DSS compliance to verify regularly that cloud service providers are validated for compliance with this standard and that they maintain this compliance annually.

We will examine the auditing of an e-government application taking as an example the electronic voting in the Swiss canton of Geneva. Switzerland has a long experience of voting at distance. Voting by mail is possible since 1990. Three cantons including Geneva have started pilot voting over the Internet in 2000. The first e-voting was tested in the small commune of Anières with the voting eligible population of not more than 2000 people at that time. As of 2009 people of Geneva voted to change the cantonal constitution and to include e-voting as one of the fundamental methods for exercising the right to vote. Statistics in Geneva show that the turnout of voters that use e-voting over the Internet is stable at around 20% of all eligible voters⁷⁰. Only 5% of voters vote in person at voting stations. Initially the main reason for introducing voting at distance was to enable Swiss citizens abroad to vote, as well as those that for medical reasons are not in the capacity to physically vote. With over 85% of population that have access to the Internet⁷¹, Switzerland is among European countries with the highest Internet usage rate. Therefore e-government applications play an important role in facilitating access to public services. Switzerland was among the first countries to pilot Internet-based voting to further expand participation of voters and to overcome obstacles with slow international postal services. As already stated, the Federal government authorized three cantons to develop Internet-based voting systems. Recently the canton of Geneva has even started to offer the e-voting as a service to other cantons.

The government of Geneva defined eleven principles that serve as a basis for the e-voting system:

1. Votes submitted electronically cannot be intercepted, modified, or diverted.
2. The contents of votes submitted electronically must not be accessible to third parties prior to counting.
3. Only individuals eligible to vote could participate in ballot.
4. Each voter has right to one vote and cannot vote more than once.
5. Under no circumstances should be possible to link a voter to his/her vote, neither during the ballot nor after counting of votes.
6. The system should be robust against a denial of service attack that could saturate the server.
7. A voter must be protected against identity theft attempts
8. The number of votes counted must correspond to the number of votes received; any difference must be explained and corrected.
9. A proof that a voter has voted must be established.

⁷⁰ <http://www.ge.ch/evoting/faq/vote-internet/>

⁷¹ <http://www.itu.int/en/ITU->

[D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls](http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2013/Individuals_Internet_2000-2012.xls)

10. The system must not accept votes outside of electronic ballot opening period.
11. A well-functioning of the system must be verifiable by designated authorities.

Security and transparency are principal challenges with distance voting. New provisions in Geneva constitution as of 2009 require auditing electronic voting system every three years. The government has identified three areas to be audited:

1. An intrusion test should be performed to ensure that the base infrastructure (network, firewalls, systems and middleware) that supports e-voting applications is adequately protected against intrusions.
2. An audit of the source code should be performed of vital system functions: of the identification of voters, of the vote storage (voters authentication; reception, decryption, and control of the voting cards, and encryption and storage of validated voting cards in the electronic ballot box), counting of the electronic ballot box (decryption, accounting and consolidation of voting cards, and editing results).
3. Perform an evaluation of readiness for ISO 9001 standard certification of e-voting procedures. As the standard certification is assigned to an entity and not to a project, it should be assigned to the government.

The last audit was performed at the end of 2012 and the report published in April 2013 by the State Council [58].

The intrusion test was performed on the production infrastructure of the e-voting system. The audit scope included the computer network, systems and services, as well as applications. The test was performed from two aspects:

- Test of the e-voting infrastructure accessible from the Internet (network edge routers, firewall, and publicly accessible systems and services).
- Test of the e-voting infrastructure accessible from the standard workstation connected on the main internal network.

The chosen audit method was “greybox” approach. Auditor was given a voting right, a voting card, and a voter’s ID so that the voting application could be used and underlying infrastructure tested during the fictive ballot process. During the first test phase, auditor was given the same amount of information that is available to voters during the real ballot. During the second phase, auditor was provided access to the internal network from the standard production workstation. The audit objectives were to measure the effectiveness of protection controls in place against intrusion to the application server. The level of risk was estimated for each individual infrastructure component. Client workstations of voters were not in the scope of the audit. Auditor has summarized in their findings that no negative aspects were identified. It has highlighted following positive findings:

- The surface of attacks from the Internet is properly restricted.
- Voter’s entries are correctly processed at the application entry and could not be modified.
- The Internet exposed services are up-to-date against vulnerabilities known at the time of the audit.

- Network segregation and traffic filtering to the e-voting system network are excellent. Data exchange between a voter and the system is appropriately encrypted.
- Although certain non-critical vulnerabilities were identified on the internal workstation and servers, it was not possible to access e-voting systems neither directly nor through rebound.

Auditor concluded that the protection level is very good. In addition it concluded that neither the infrastructure nor the applications are vulnerable to the Internet-based intrusions. Similarly, it concluded that the system is not vulnerable to intrusions from the internal network. Lastly, the auditor concluded that the virtual private network (VPN) used for the maintenance of the e-voting system is not vulnerable to intrusions from the internal network.

The e-voting application consists of approximately 200 000 lines of code and modules covered in the scope of the audit of about 75 000 lines. It is developed in Java programming language. The audit of the source code focused on the above listed most critical functionalities of the application. The following application modules were subject of the audit: ballot procedure management module, e-voting end-user interface, e-voting administration application, and the administration console used by ballot monitoring authorities. International standard for quality evaluation of software products (ISO 25000) was selected as the audit baseline. The Open Web Application Security Project (OWASP) code review method was used. It was decided that two of eleven main principles for e-voting could not be taken into account during the audit. Those were:

Principle 6: The system should be robust against a denial of service attack that could saturate the server.

Principle 11: A well functioning of the system must be verifiable by designated authorities.

The quality level was measured as the ratio of the number of functionalities implemented according to specifications and the number of initially specified functionalities. The static code analysis was used as the evaluation methodology. The assessment was performed from two aspects. The first aspect was to assess the source code compliance with the security requirements. The second aspect was to identify the most critical parts of the source code and to assess if they have been implement in accordance with security best practices. Two types of audit activities were performed from both aspects:

- Firstly, the syntax analysis was performed evaluating the behavior of the application without executing it. It is based on using automated tools and manual intervention in ensuring the accuracy and criticality of automatically detected vulnerabilities.
- Secondly, the manual analysis of the most critical source code parts was performed focusing on the context, and on the application logic and objectives.

The auditor concluded that seven out of nine base principles were followed fully with 100% functionalities implemented as specified following good security practices.

Four vulnerabilities were identified in the area of remaining two e-voting principles. One of those principles is that votes submitted electronically cannot be intercepted, modified, or diverted. The second principle is that a voter must be protected against identity theft attempts. None of two vulnerabilities identified in relation to the first principle diminish the security of e-voting application. A vulnerability associated with the principle seven was identified but designated as hardly exploitable. Recommendations to mitigate identified risk were made by the auditor and fully implemented ahead of ballots performed in 2013. The auditor reported in its conclusion that all audited modules satisfy security requirements and are in-line with security standard ISO 25000.

The third audit aspect covering the area of conformity with the international standard ISO 9001 for management quality focused on management of the ballot process. In addition, the objective of this audit aspect was to identify risks for voters and the overall security. Following processes were included in the audit scope:

- Governance
 - Administration
 - Management system
 - Communication
- Resource management
 - Finance
 - Infrastructure and equipment
 - Human resources
 - Purchasing and contracting
- Operations
 - Prospecting
 - Project feasibility
 - Preparing a ballot
 - Receiving and processing votes
 - Counting votes
 - Terminating ballot
- Continuous improvements
 - Measuring satisfaction
 - Internal audit
 - Incident management
 - Improvement activities

The auditor concluded that the process maturity level required for ISO 9001 certification is high and that certification could be easily achieved.

In overall the executive summary in all three audit areas concluded that the security level of e-voting system is satisfactory and conforms to the defined requirements. However, certain vulnerabilities with potentially significant impact have been identified. Although the published audit report did not present any technical details on those vulnerabilities it is important to analyze risks in more details.

The application source code audit identified two vulnerabilities in the domain of the security principle 1 (Votes submitted electronically cannot be intercepted, modified, or diverted). These two vulnerabilities are related to the validation of data entry and to the cryptographic controls. Two more vulnerabilities were identified in the domain of

the security principle 7 (A voter must be protected against identity theft attempts). These vulnerabilities are related to the error management and to the storing of voting data in the application logs. The auditor evaluated the second vulnerability as hardly exploitable so the likelihood was estimated as low. The exploit requires high privileged access to two internal resources distinct from the e-voting system. However, if such an access is obtained during the ballot it could compromise voter's identity. Security principles 5 and 7 relate to the security of voters' identity while other principles are related to the security and the quality of the ballot process. In the context of such a risk the questions arises if voters are ready to accept estimated risk likelihood. In the process of voting by postal correspondence and voting in person, the controlling commission at the ballot point consists of randomly selected individuals eligible for voting. Their role is to supervise the ballot process, to verify the validity of voting cards, and to count the votes upon closure of the ballot period. Randomly selected assistants sort voting material sent by the post. They validate the voting cards and place unopened envelopes with votes in the box corresponding to the voters geographical location. Boxes are transported to the corresponding voting points to be opened and counted together with votes made in person. A team of several representatives of authorities control the process of electronic voting. In the next chapter this process will be described in more details. They open the process by generating the encryption keys. They are physically present at the system administration point during the ballot. They start votes counting by using the encryption keys generated at the opening of the ballot⁷². However, electronic threats and vulnerabilities would remain highly invisible to the human supervision during the ballot and during votes counting.

The infrastructure audit of the internal administrative network identified several vulnerabilities. Physical access to the personal computer connected to the administrative network permitted auditors to modify the booting sequence and start the machine with the modified operating system from the removable memory. As the local disk of the PC was not encrypted they managed to recover the password storage and obtain the access to certain local user accounts. The password selection and usage policy was not following the best practice. That opened the way to certain servers on the network and access to their contents. Auditors identified one particularly vulnerable server that is connected to the administrative network and managed to take the full control of it. That JBoss⁷³ application server permitted auditors to install their own Java application with the goal to intercept unencrypted network traffic and to attempt rebound to other servers. They have also managed to obtain the individual password of one administrator from the local password storage on the server. Auditors have not succeeded in rebound attacks on other servers but it was not reported on how much time and what techniques were spent for those attempts. The physical presence of the representatives of the voting commission and system administrators during the real ballot would certainly make such an exploit highly unlikely by the external malicious intruders. However, it would be difficult to identify and prevent an internal malicious activity. Moreover, all attacks performed by the auditors were targeted at the vulnerabilities known at the time of the audit. New vulnerabilities and malicious software that can exploit them are discovered every day. Just one anti-virus research

⁷² http://www.geneve.ch/legislation/rsg/f/rsg_a5_05p01.html

⁷³ <http://www.jboss.org/overview/>

company reported that they discover more than 200 000 new viruses every day⁷⁴. Therefore, the likelihood of an unpatched vulnerability and a “zero-day” virus that can exploit it is quite high at the time of a future ballot. Even if administrators ensure that all systems are maintained up-to-date with the latest security patches ahead of the ballot it cannot guarantee the complete protection against new threats. Furthermore, a determined attacker with malicious intent could deploy significant resources to prepare and perform attack. Recently published information of cyberattacks of nation states illustrate usage of advanced techniques in interception of encrypted traffic and usage of Remote Access Trojans (RAT) and rootkits as backdoors to targeted systems. Conventional information security controls have moderate effectiveness against that kind of attacks. In addition, the audit did not cover social engineering, which represents techniques of tricking authorized users to share their credentials, and other relevant information that may permit system access to attackers. Security of voters’ personal computers is another important area that was not within the audit scope. Exploit of local vulnerabilities during the ballot participation could expose voters’ identity to risk as well as their casting of votes.

To conclude, the protocol that enforces the protection of identity on the voters’ personal computer, as the point of participation in the ballot process, can significantly reduce potential breach of privacy risk in other components of the e-voting system. In this chapter we have given the review of the information system audit process from the industry standard aspect and on the concrete example of the security audit of the e-voting system of the canton of Geneva. The review audit was performed on the production system using test data. The audit may be performed using the production data as well. Such an IS audits are commonly performed on systems for critical business processes such as financial or human resources information systems and Enterprise Resources Planning (ERP) systems. During these audits confidential data are accessible to auditors but audited companies usually accept this exposure risk because auditors are bound to non-disclosure contractually and through the ethical aspect of their professional certification. This risk however should not be acceptable for e-voting systems. The freedom of vote is one of the fundamental political rights. The Swiss federal law on political rights stipulates in its article 5 that the secrecy of vote should be guaranteed⁷⁵. Therefore under no circumstances even during the audit should voting decisions of a citizen be disclosed to anyone. The e-voting system should be designed in such a way that under no circumstances could voting decisions be linked to the identity of the voter.

6.8 Applicability of the proposed cryptographic protocol in e-Government applications

We will take the e-voting system of the canton of Geneva as an example of the e-Government application in order to analyze the applicability of the proposed cryptographic protocol. The Internet voting system of the canton of Geneva is the intellectual property of the cantonal government and is continuously being developed and improved since its first practical usage in 2003. The infrastructure of the current

⁷⁴

http://www.kaspersky.com/about/news/virus/2012/2012_by_the_numbers_kaspersky_lab_now_detects_200000_new_malicious_programs_every_day

⁷⁵ <http://www.admin.ch/opc/fr/classified-compilation/19760323/index.html>

version as of December 2013 is described in details on the official cantonal Web site⁷⁶. Since privacy protection is the main objective of our research, we will analyze the applicability of the proposed protocol in the context of protecting the privacy of voters in all phases of the ballot. The special emphasis will be made on the privacy protection during and after the ballot process including eventual audit of the production system with real voters' data.

Personally identifiable information of each voter used in the Internet voting system of Geneva consists of name, surname, date of birth, and domiciliation. The Cantonal Population Office (CPO) collects and maintains this information in the register of inhabitants independently from the voting system. The personal information of eligible voters is transferred from the CPO to the Internet voting system ahead of the ballot in order to prepare and print voting cards. This personal information except for the date of birth is already available in many other commercial and public registers including public telephone directories (unless individuals explicitly requested not to be listed). Many individuals opt-in for commercial fidelity cards and other marketing tools and voluntarily provide those same pieces of information. Therefore, we assume that this information is not highly critical since the breach of its confidentiality could not have a significant impact neither on the ballot process nor on the security of voters. However, the identity information combined with the voting information could have a significant impact on the privacy of voters and their civil rights. Therefore ensuring the confidentiality of individual votes and that they cannot be linked to the identity of the voter is of an utmost importance.

The Central Electoral Commission (CEC) of Geneva established by the parliament is in charge of managing the ballot. The Voting and Elections Department (VED) of the government is in charge of administering the ballot process. At the beginning of the ballot process following individuals are involved in cryptographically sealing the ballot box so that votes could not be cast before the ballot process has officially started:

- A representative of the cantonal government as the chairperson of the ballot session,
- The chairperson of the CEC,
- Four CEC members in groups of two,
- A representative of the VED,
- A notary,
- Information Security Officer of the cantonal police,
- The system administrator of the internet voting system.

The system administrator manages the process using the administrative application from the standalone PC connected to the internet voting system over the secure Virtual Private Network (VPN). The PC is not connected simultaneously to any other computer network. The administrator initiates generation of the asymmetric key pair used to encrypt votes in the ballot box, and initiates generation of the symmetric key used to encrypt the integrity counter for votes. The private key from the asymmetric key pair is protected by two passwords each consisting of two combined words. These four words are selected by each of four CEC representatives who write them on the paper sealed in envelopes and given to the notary. These envelopes are opened in case

⁷⁶ http://www.ge.ch/evoting/english/Uncovering_the_veil_a.asp

any of four members forgets the preselected word. Encryption keys are not stored on the administrative PC. Immediately upon the generation they are saved on the removable memory and backed up on a CD. These storage media are handed to the Information Security Officer. The ballot box integrity counter is set to 0 and encrypted.

The functioning of the system is tested with two test votes performed and verified by the four CEC representatives. All ballot process phases are verified including the functioning of the integrity counter, decryption and counting of votes. The administrative PC is sealed in the bag that is kept in the custody of the VED representative during the ballot process. The integrity of the ballot box is ensured through the split custody of the secret information. Only all secrets gathered could be used to unlock the ballot box. They could be gathered by the notary and the Information Security Officer, or by the four CEC members. They could be used only from the PC with the IP address of the sealed administration PC and through the VPN protected by the password known only by the system administrator. Therefore only collusion of these parties could represent the threat to the integrity of the ballot box. However, it is not unheard of such situations through the history of non-electronic voting. Therefore it should be taken into consideration for the risk analysis particularly in cases of highly sensitive voting decisions and in environments with elevated likelihood of political struggles.

Voters receive voting cards by the post ahead of the ballot.

7

Chancellerie d'Etat
Service des votations et élections

CAN-COM

CARTE DE VOTE

Tout changement d'adresse annoncé à l'Office cantonal de la population (OCP) après le 20 MARS 2011 est enregistré mais ne peut figurer sur votre carte de vote, qui atteste de votre domicile à cette date. Une photocopie de cette carte de vote équivaut à l'attestation de résidence officielle délivrée par l'OCP pour 25 F.

VOTE PAR INTERNET

<https://www.evoting.ch/ga>

Numéro de carte de vote : 1351-5865-2696-4214

Codé de contrôle : WBPF

Mot de passe :

Empreintes numériques du certificat (certificate fingerprint) :
75:E9:D8:63:FS:DA:13:06:BB:F7:13:36:34:3E:05:42:6C:79:EC:73
ou
1E:78:0D:4E:74:62:ED:A1:1D:66:AC:D7:15:A8:D3:7C

Pour être pris en considération, votre vote par internet doit être effectué avant 12h00, le samedi 14 mai 2011

A REMPLIR ET SIGNER OBLIGATOIREMENT POUR VOTER PAR CORRESPONDANCE OU AU LOCAL DE VOTE

Date de naissance complète

JOUR	MOIS	ANNEE

Signature: _____

1000072

15 mai 2011
VOTATION POPULAIRE
Local fictif Electeurs de Test

6699-9901

PP 1211 Genève 2

Monsieur
CYBER Citoyen
Route Cyberadministration 1
1200 Genève 3

Figure 10: Sample voting card

Voting cards contain the Uniform Resource Locator (URL), the Internet address of the e-voting site, the unique voting card number, the control code, the password protected with the tamper-proof film, and Web site certificate fingerprints. When the official ballot is opened voters connect to the Web site using the secure Hypertext Transfer Protocol (HTTPS). They can verify Web site authenticity comparing fingerprints of the Secure Socket Layer (SSL) certificate. SwissSign AG certificate authority issued the current Extended Validation (EV) SSL certificate. It is cryptographically signed using Public Key Cryptographic Standard (PKCS #1) with Secure Hash Algorithm (SHA-1), and using RSA Encryption. The client voting application written in Java is downloaded and executed as applet in the local Internet browser on the voter's personal computer. The voter enters the unique voting card number to start voting. This number replaces voter's name and surname. Although communication between the voter's browser and the Web server is encrypted using the industry standard 128 bits strong Transport Layer Security (TLS), to reduce the likelihood of the man-in-the-middle attack on the TLS the voting card number is further protected using the keyed-hash message authentication code (HMAC). The key for HMAC is derived from the unique code of the voting card. It is combined with the Diffie-Hellman (DH) key exchange deployed between the client applet and the server. This also reduces the risk of brute force attack on the unique key with rainbow tables. Rainbow tables are pre-calculated hash tables that reduce the entropy of the code to shorten the time for attack. The voter is then reminded of the legal obligations and penalties. After acknowledging the acceptance of the legal disclaimer, voting options are displayed and the voter may cast its decisions. The four letters control code is displayed upon the completion of voting. It must correspond to the code printed on the voting card. Finally the voter authenticates and validates its vote entering the password from the voting card, the date of birth and the place of origin. Therefore, except for name and surname replaced by the unique number of the voting card, personal identification information together with voting decisions are stored temporarily in the cache of the Internet browser. It is recommended on the official online voting instructions that voters clear the cache after voting⁷⁷. There are numerous known Java and browser vulnerabilities that are exploited by thousands of computer viruses and other malicious software. Even if the voter follows best practice and maintains its software up-to-date with security patches and has an anti-virus protection active and up-to-date a "zero-day" virus or other malicious software could be specifically developed to exploit a newly discovered vulnerability and to collect information on the voter and its vote. Furthermore, certain client-side application vulnerabilities were identified during the source code audit as described in the previous chapter.

Once the information cast by the voter is received the server performs a "syntax check" to verify the validity of the vote before storing it in the ballot box. This check ensures the integrity of the vote and prevents manipulation of the voting decisions or prevents against SQL injection attack, for example if the virus infects the voter's PC. Upon successful syntax verification the server sends the control code to the voter's Java applet for verification. This code is generated ahead of the ballot process and imported in the system together with other information on voters. The system verifies voter's authentication information against the voting card register and if successful it encrypts

⁷⁷ <http://www.ge.ch/evoting/faq/comment-voter/welcome.asp>

the vote and voter's polling station information with the ballot box public key and stores it in the ballot box. The integrity counter is decrypted, incremented, and encrypted again. All these activities are performed in the single transaction to satisfy Atomicity, Consistency, Isolation and Durability (ACID) properties for transaction reliability. The voting card register and the ballot box are two distinct databases. However, the votes are stored in the order of reception so there is a possibility to establish the relationship between the vote and the voter's identity.

Once the ballot process is formally closed members of the team who sealed the ballot box gather all secret information and prepare the administration PC to decrypt the ballot box and start counting votes. Before decryption takes place, the votes in the ballot box are mixed twice in the server's memory using the quantum random number generator to prevent the risk of linking to voters' identities. Once votes are decrypted they are counted and the total compared with the integrity counter. The numbers must be equal. As stated earlier the collusion between team members who possess ballot encryption secrets may lead to the breach of voters' privacy. In addition, malicious activity during the opening of the ballot box that tampers with mixing of votes could also be a threat to voters' privacy. Although difficult given the presence of the voting supervision team and network segregation of the e-voting system it is not impossible for highly determined attacker with enough resources. For example a rootkit planted deeply in one of e-voting servers or the administration PC could be a vector of such an attack. Moreover, the audit described in the previous chapter identified certain vulnerabilities both in the server-side application and the infrastructure that could have been exploited to breach voters' privacy. Although these vulnerabilities have been supposedly remediated new vulnerabilities can be discovered in the future.

While a lot of efforts have been put in implementing the secure communication channel between the client application and the e-voting server, attacks on voters' privacy are still possible on the client and/or on the server side. Therefore the proposed protocol that ensures cryptographically strong externalization of identity verification from the e-voting transaction would significantly reduce such a risk. The construction described in chapter 5.1 can be implemented in such a way that the authentication subsystem is developed as a separate client application that communicates to the authentication database to verify the identity of voters and their eligibility to vote. Once this is verified and confirmed a different voting application can be used to cast the vote. This application can be implemented as part of the authorization subsystem of the proposed protocol and can communicate to the ballot box database to store encrypted votes. Therefore there would be no link ever maintained on the single server between votes and voters' identities. The team supervising e-voting couldn't breach voters' privacy even if all team members decide or are forced to collude. Even two distinct teams could supervise two subsystems. Targeted attack on the voter's PC could still represent a risk to the voter's privacy. However, carefully coded authentication application following the best practices for application security as described in chapter 5.3 would ensure minimum exposure of critical privacy related information. Even more complex architecture could be envisaged for example with authentication application executed from the mobile device like a smart mobile phone or tablet PC. The voting application may be running on a different client device, for example a personal computer as illustrated in Figure 11. In this scenario, if the mobile device is connecting to the authentication subsystem over the mobile telephone network, and the personal computer is connected to the authorization subsystem via the Internet Service Provider

there would be two different Internet Protocol (IP) addresses registered with each subsystem and different timestamps associated with two transactions. It would be much more difficult to correlate accurately time and locations in attempt to reveal identity of a voter. Even the audit of the production environment with real voters' data would have to include separate assessments of two subsystems and would not be able to recreate links between votes and voters' identities.

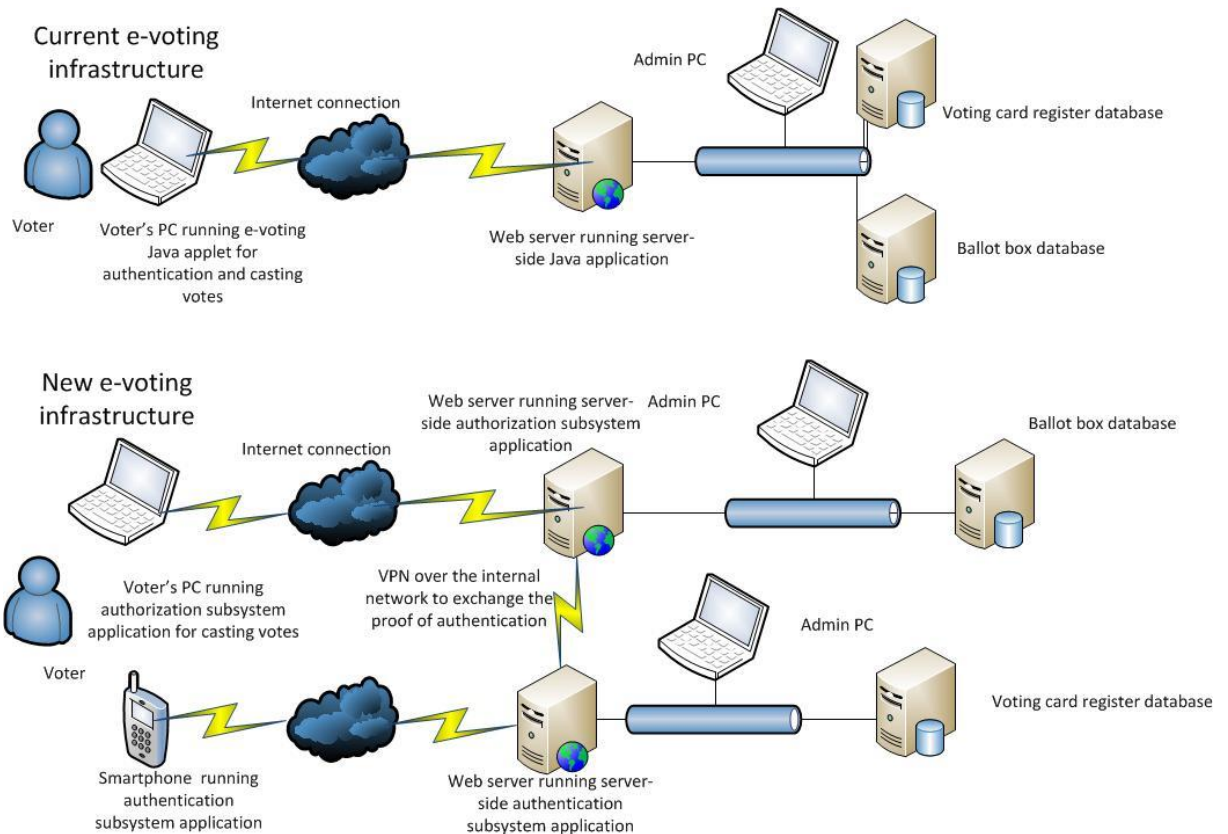


Figure 11: Infrastructure comparison of the current and newly proposed e-voting system based on the privacy protection protocol

7 Conclusion

7.1 Contribution

The main objective of this research is to develop the secure and efficient cryptographic protocol that can ensure users identity protection in transaction oriented business applications. The practical implementation of the proposed construction is adapted to the security requirements of the Internet based voting system. Particular objective of such a system is to improve the level of confidence that its users, voters in this case, may place in the system.

One of main research hypothesis is that there is a direct relation between the level of confidence in the security of an information system and the level of identity protection of its users, and consequently this relation influences business success of the system. In chapter 6.1 we have analyzed results of the United Nations Global E-Readiness Reports and Survey and concluded that protection of personal identity and privacy is one of main success factors for e-government applications. This is of a particular importance for such e-government applications as Internet based voting systems. We have illustrated in the analysis of regulatory measures in chapters 6.2 to 6.5 that their effectiveness has limited effect in increasing the level of trust that users place in information systems. Furthermore relation between policy and technology and users' expectations for identity protection are highlighted in chapter 6.6. In addition in chapter 6.7 we have illustrated that control and audit measures may have an adverse effect on the level of confidence since they may unnecessarily expose privacy of users to information systems auditors. In addition to supporting the above hypothesis our conclusion is that technical measures that enable end-users, voters in the reviewed online voting example, to have control on their own personal data would increase the perception of security and thus the level of confidence.

Contribution of the proposed cryptographic protocol in increasing the level of identity protection in e-voting systems is highlighted in chapter 6.8. This highlight supports the second general hypothesis that externalization of users' identification from the transaction data storage increases the level of identity protection. The proposed protocol efficiently enables such externalization and its modularity and scalability permits its applicability in various business scenarios with large amounts of data and high transaction rates.

The third general hypothesis states that cryptographic zero-knowledge proofs could be used to construct information systems that could be audited while identity of users is preserved. The research concludes in chapter 6.8 that cryptographic sigma-protocols maintain the same security attributes as zero-knowledge proofs. These security attributes are witness-hiding, deniability, honest prover and honest verifier. The review of IT audit process in the same chapter concludes that separate audit of the externalized identification system and of the transaction data storage system preserves identity of transaction users and unnecessary exposures personal data to auditors.

One particular hypothesis states that two separate data protection subsystems could be unified through the implementation of common cryptographic protocols based on Schnorr's cryptographic scheme. This is proven in chapter 5.1 where construction of such a protocol is described in details and supported by the practical implementation in SAGE mathematics.

The second particular hypothesis states that efficient and secure construction of cryptographic sigma-protocols could be based on the computational complexity of solving discrete logarithm problems. Simulations of generating as much as 1 million cryptographic key pairs and performing 100'000 cryptographic transactions in chapter 5.2 illustrated that the proposed protocol construction is efficient even for large-scale implementations. Security aspects of the protocol are analyzed in chapter 5.3 and the most critical cryptographic primitives identified such as secure hash function and cryptographically secure pseudo-random number generator. The review of existing frameworks for the secure coding and the review of methods for security assessments permit holistic approach to detailed risk analysis of the protocol construction and represent the basis for further development and security improvements.

7.2 Further work

The future work on a practical implementation of the proposed construction would consist of analyzing the current trends in cryptanalysis and advancement in such technologies as quantum computing that may increase security requirements of the implementation. The analysis process is described in chapter 5.3. Possible security improvements within individual protocol modules were also mentioned in the same chapter. For example, implementing elliptic curve based cryptographic primitives would make the proposed construction more robust against certain known vulnerabilities of cryptographic schemes based on the problem of computing discrete logarithms. Other possibility would be to use the quantum source of randomness such as the solution used within the Internet voting system of the canton of Geneva described in chapter 6.8. However, the core structure of the proposed protocol with two distinct subsystems based on sigma-protocols joined only through the global common cryptographic parameters would last over time and provide security attributes required to protect privacy in the long term.

The progress of interconnecting sensors that capture data such as air temperature in apartments, personal weight, blood pressure, heart rate, sport activities, eating habits, and many other become trendy, bring convenience to our lives, but carry tremendous risks to privacy. Tracking and storing massive amounts of data from such sensors and linking that data to personally identifiable information would create an irreversible risk for privacy. It already does, as reported by Gartner who predicts that 26 billion units will be interconnected in so cold the Internet of things by 2020⁷⁸. Implementation of privacy protection through technological solutions such as the proposed protocol would enable us to benefit from the evolution of technology while preserving individual freedoms. While it may be useful to have annual statistical analysis on our physical activities, eating habits and health parameters, it is not necessary to provide direct link to personally identifiable information and store those in online interconnected databases accessible to others. Personal information should remain personal and its usage must be directly controllable by data owners, us.

In the closing words of this thesis I would refer to the book "From Immigrant to Inventor" written in 1923 by Mihajlo Pupin (Michael Pupin). With his inventions Pupin contributed to the progress of telecommunications and to what he called in the last chapter of the book "the ideal democracy". Pupin stated that progress means more

⁷⁸ <http://www.gartner.com/newsroom/id/2636073>

coordination of all natural activities. In the 21st century when the World has truly become the global communication village, instrumentalities of coordination of information sharing must protect the individual nature of each one of us so that we perceive the global connectivity as the benefit and not a hazard.

Annex I - SAGE Mathematics source code for the cryptographic protocol for information systems audit with users' identity protection

```
# Construction of combined OR-proof form and non-interactive form of sigma protocol
# based on discrete logarithm problem
# Reference: Damgard, On Sigma-protocols, CPT2010 v.2
#
# Global public key components common for both protocol sub-systems
# Generates a 512 bits q and 2048 bits p, both prime
# such that q divides p-1
#  $2^{511} < q < 2^{512}$ 
#  $1 < k < (p-1)$ 
#  $g = (k^{(p-1)/q}) \bmod p$ 
# Reference for global components calculations: Stallings, Cryptography and Network
# Security, 5th edition, 2011
#
from time import time
set_random_seed()
t1 = cputime(t=0,subprocesses=True)
q = random_prime(2^512,2^511)
p = 1
while (not is_prime(p)):
    p = (2^2048 + randint(1,2^2048)*2)*q + 1
k=ZZ.random_element(q)
F = GF(p)
g = (F(k)^((p-1)/q))
t2 = cputime(subprocesses=True)

# Print size of global variables and time to calculate them
# Word size in bits depends on the computing platform architecture
#
import platform
print "Word size on this platform =", platform.architecture()
print "Size of global variables:"
print "q =", pari(q).sizeword(),"words"
print "p =", pari(p).sizeword(),"words"
print "g =", pari(g).sizeword(),"words"
print "q =", pari(q).sizebyte(),"bytes"
print "p =", pari(p).sizebyte(),"bytes"
print "g =", pari(g).sizebyte(),"bytes"
print "Time to calculate all global variables =", t2 - t1,"sec"

# Prover P chooses randomly a private key w
#  $0 < w < q$ 
#
t1 = cputime(t=0,subprocesses=True)
set_random_seed()
w=ZZ.random_element(q)
```

```

# Prover P calculates and publishes corresponding public key h
#  $h = g^w \bmod p$ 
#
h=F(g)^w
t2 = cputime(subprocesses=True)

# Print size of private variables
#
print "Size of private variables:"
print "Private key w =", pari(w).sizeword(),"words"
print "Private key w =", pari(w).sizebyte(),"bytes"
print "Public key h =", pari(h).sizeword(),"words"
print "Public key h =", pari(h).sizebyte(),"bytes"
print "Time to calculate private variables =",t2 - t1,"sec"

# Authentication sub-system
# Authenticate user without disclosure of identity
# OR-proof form of Sigma protocol based on Schnorr's scheme
#
# Prover P chooses r at random in  $\mathbb{Z}_q$ 
# and calculates  $a_0 = g^r \bmod p$ 
#  $0 < r < q$ 
#
t1 = cputime(t=0,subprocesses=True)
set_random_seed()
r=ZZ.random_element(q)
a0=F(g)^r
t2 = cputime(subprocesses=True)
print "Size of message a0:"
print "a0 =", pari(a0).sizeword(),"words"
print "a0 =", pari(a0).sizebyte(),"bytes"
print "Time to calculate message a0 =",t2 - t1,"sec"

# Prover P chooses e1 at random in  $\mathbb{Z}_q$ , chooses z1 at random in  $\mathbb{Z}_q$ 
# and runs simulator M on e1 and z1 to calculate a1 as  $a_1 = g^{z_1} h^{(-e_1)} \bmod p$ 
#
t1 = cputime(t=0,subprocesses=True)
set_random_seed()
e1=ZZ.random_element(q)
z1=ZZ.random_element(q)
a1=F(g)^z1*F(h)^(-e1)
t2 = cputime(subprocesses=True)
print "Size of message a1:"
print "a1 =", pari(a1).sizeword(),"words"
print "a1 =", pari(a1).sizebyte(),"bytes"
print "e1 =", pari(e1).sizeword(),"words"
print "e1 =", pari(e1).sizebyte(),"bytes"
print "z1 =", pari(z1).sizeword(),"words"
print "z1 =", pari(z1).sizebyte(),"bytes"

```

```

print "Time to run simulator M =",t2 - t1,"sec"

# Verifier V chooses random t-bit string s in  $\mathbb{Z}_2^t$  such that  $2^t < q$  but still exponentially
large.
# Verifier V sends s to prover P.
#
set_random_seed()
s=randint(2^510,2^511)
print "s =", pari(s).sizeword(),"words"
print "s =", pari(s).sizebyte(),"bytes"

# Prover P calculates  $e_0 = s \text{ XOR } e_1$ ,
# and calculates corresponding  $z_0 = r + e_0w \bmod q$ 
#
e0=pari(s).bitxor(e1)
z0=(r + e0*w) % q
print "Size of message z0:"
print "z0 =", pari(z0).sizeword(),"words"
print "z0 =", pari(z0).sizebyte(),"bytes"
print "e0 =", pari(e0).sizeword(),"words"
print "e0 =", pari(e0).sizebyte(),"bytes"

# Verification
# Upon receiving  $a_0, e_0, z_0$  and  $a_1, e_1, z_1$  from the prover P, verifier V checks that  $s = e_0$ 
XOR  $e_1$ .
# Also, taking into account prover's public key h, verifier tests if the following formula
holds for both sets of received messages:
# Is  $g^z = ah^e \bmod p$  ?
#
t1 = cputime(t=0,subprocesses=True)
s2=pari(e0).bitxor(e1)
print "Verification of the challenge =",s==s2
v1=g^z0
v2=F(a0)*F(h)^e0
print "Verification of the conversation 1 =",v1==v2
u1=g^z1
u2=F(a1)*F(h)^e1
print "Verification of the conversation 2 =",u1==u2
t2 = cputime(subprocesses=True)
print "Time to calculate verification =",t2 - t1,"sec"

# Authorization sub-system
# Prove correct participation in a transaction without linking to identity
# Non-interactive form of Sigma protocol based on Schnorr's scheme
#

# Schnorr's protocol convinces verifier that prover has the right private key
#

```

```

# Prover P chooses r at random in  $\mathbb{Z}_q$ 
# and sends  $a = g^r \bmod p$  to verifier V
#  $0 < r < q$ 
#
t1 = cputime(t=0,subprocesses=True)
r=random_prime(q-1)
a=F(g)^r
t2 = cputime(subprocesses=True)
print "Size of message a:"
print "a =", pari(a).sizeword(),"words"
print "a =", pari(a).sizebyte(),"bytes"
print "Time to calculate message a =",t2 - t1,"sec"

# Prover P calculates challenge e by applying hash function as a random oracle to the
message a.
# Integer a has to be converted to string.
# Hexadecimal output of hash is converted to long integer.
#
import hashlib
t1 = cputime(t=0,subprocesses=True)
e=int(hashlib.sha512(str(a)).hexdigest(),16)
t2 = cputime(subprocesses=True)
print "Size of challenge e:"
print "e =", pari(e).sizeword(),"words"
print "e =", pari(e).sizebyte(),"bytes"
print "Time to calculate challenge e =",t2 - t1,"sec"

# Prover P calculates z and sends it to verifier V.
#  $z = r + ew \bmod q$ 
#
t1 = cputime(t=0,subprocesses=True)
z=(r + e*w) % q
t2 = cputime(subprocesses=True)
print "Size of message z:"
print "z =", pari(z).sizeword(),"words"
print "z =", pari(z).sizebyte(),"bytes"
print "Time to calculate message z =",t2 - t1,"sec"

# Verification
# Upon receiving a and z from the prover P, verifier V calls random oracle to calculate e1
# Taking into account prover's public key h, verifier tests the following:
# Is  $g^z = ah^{e1} \bmod p$  ?
#
t1 = cputime(t=0,subprocesses=True)
v1=g^z
e1=int(hashlib.sha512(str(a)).hexdigest(),16)
v2=F(a)*F(h^e1)
print "Verification =",v1==v2
t2 = cputime(subprocesses=True)

```

```
print "Time to calculate verification =",t2 - t1,"sec"
```

Bibliography

- [1] David J.C. MacKey: *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, ISBN-13: 978-0521642989, October 2003
- [2] Gideon Samid: *Shannon Revisited: Considering a More Tractable Expression to Measure and Manage Intractability, Uncertainty, Risk, Ignorance, and Entropy*, Cornell University Library, CLN: 10-500, arXiv:1006.1055v1, June 2010
- [3] Shafi Goldwasser, Silvio Micali and Charles Rackoff: *The Knowledge Complexity of Interactive Proof-Systems*. In: STOC '85 Proceedings of the seventeenth annual ACM symposium on Theory of computing, Association for Computing Machinery, ISBN:0-89791-151-2, 1985
- [4] Oded Goldreich: *Foundations of Cryptography – Basic Techniques*, Cambridge University Press, ISBN 0-511-04120-9 eBook (netLibrary), 2004
- [5] Mihir Bellare and Oded Goldreich: *On Probabilistic versus Deterministic Provers in the Definition of Proofs Of Knowledge*, Lecture Notes in Computer Science, Vol.6650, Springer, p. 114-123, DOI 10.1007/978-3-642-22670-0_14, 2011
- [6] Oded Goldreich, Silvio Micali and Avi Wigderson: *Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems*, In: Journal of the Association for Computing Machinery, Vol.38, Issue 3, p.690-728, DOI 10.1145/116825.116852, July1991
- [7] Amos Fiat and Adi Shamir: *How to Prove Yourself: Practical Solutions to Identification and Signature Problems*, In: Proceedings of Advances in Cryptology (CRYPTO 1986) (Odlyzko, A.M., ed.), Lecture Notes in Computer Science, Vol.263, Springer, p.186–194, DOI 10.1007/3-540-47721-7_12, 1987
- [8] Manuel Blum, Paul Feldman, and Silvio Micali: *Non-interactive zero knowledge and its application*, In: Proceeding STOC '88 Proceedings of the twentieth annual ACM symposium on Theory of computing, Association for Computing Machinery, ISBN:0-89791-264-0, 1988
- [9] Jens Groth and Rafail Ostrovsky: *Cryptography in the multi-string model*, In: Proceeding CRYPTO'07 Proceedings of the 27th annual international cryptology conference on Advances in cryptology, Association for Computing Machinery, ISBN: 3-540-74142-9, 2007
- [10] Jens Groth, Rafail Ostrovsky, and Amit Sahai: *Perfect Non-Interactive Zero Knowledge for NP*, In: Proceedings of Eurocrypt 2006, volume 4004 of LNCS, Issue: 0430254, Springer, p. 339-358, DOI 10.1007/11761679_21, 2006
- [11] Jens Groth, Rafail Ostrovsky, and Amit Sahai: *Non-interactive Zaps and New Techniques for NIZK*, In: Proceedings of Crypto 2006, volume 4117 of LNCS, Issue: 0430254, Springer, p. 97-111, DOI 10.1007/11818175_6, 2006
- [12] Jens Groth: *Minimizing Non-interactive Zero-Knowledge Proofs Using Fully Homomorphic Encryption*, Cryptology ePrint Archive, <http://eprint.iacr.org/2011/012.pdf>, January 2011
- [13] Stefan G. Weber and Max Mühlhäuser: *Multilaterally Secure Ubiquitous Auditing*, In: *Intelligent Networking, Collaborative Systems and Applications*, vol. Studies in Computational Intelligence, Springer, p. 207-233, ISBN 978-3-642-16792-8, December 2010
- [14] Yingpeng Sang and Hong Shen: *Efficient and secure protocols for privacy-preserving set operations*, In: Journal ACM Transactions on Information and System Security (TISSEC), Association for Computing Machinery, Volume 13, Issue 1, DOI 10.1145/1609956.1609965, October 2009
- [15] Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, Christophe Geuens: *PrETP: Privacy-Preserving Electronic Toll Pricing*, In: Proceedings of

the 19th USENIX conference on Security, USENIX Association, ISBN: 888-7-6666-5555-4, August 2010

[16] Michael T. Goodrich and Florian Kerschbaum: *Privacy-Enhanced Reputation-Feedback Methods to Reduce Feedback Extortion in Online Auctions*, In: CODASPY '11 Proceedings of the first ACM conference on Data and application security and privacy, Association for Computing Machinery, ISBN: 978-1-4503-0466-5, 2011

[17] Ivan Damgard: *Efficient Concurrent Zero-Knowledge in the Auxiliary String Model*, In: EUROCRYPT '00 Proceedings of the 19th international conference on Theory and application of cryptographic techniques, Association for Computing Machinery, p.418-430, Springer, ISBN: 3-540-67517-5, Heidelberg, 2000

[18] Claus-Peter Schnorr: *Efficient Signature Generation by Smart Cards*, In : Journal of Cryptology, Vol.4, No.3, p.161-174, Springer, DOI: 10.1007/BF00196725, 1991

[19] Ivan Damgard: *On Sigma-Protocols*, Lecture notes, Faculty of Science Aarhus University, Department of Computer Science, <https://services.brics.dk/java/courseadmin/CPT/documents/getDocument/Sigma.pdf?d=53899>, 2011

[21] Bruce Schneier and Niels Ferguson: *Practical Cryptography*, Wiley Publishing, ISBN: 0-471-22357-3, Indianapolis, 2003

[22] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter: *Ron was wrong, Whit is right*, Cryptology ePrint Archive, Report 2012/064, Version: 20120217:134904, <http://eprint.iacr.org/2012/064.pdf>, February 2012

[23] Viktor D. Polic: *Non-Interactive Σ -Protocol Construction*, In: Metalurgia International, Vol. 17, No. 12-2012, p.81, ISSN: 1582-2214, Bucharest, 2012

[24] William A. Stein et al.: *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2009, <http://www.sagemath.org>.

[25] National Institute of Standards and Technology: *FIPS PUB 180-4 Secure Hash Standard (SHS)*, Federal Information Processing Standards Publication, MD 20899-8900, Gaithersburg, February 2011

[26] Shay Gueron, Simon Johnson, Jesse Walker: *SHA-512/256*, Cryptology ePrint Archive: Report 2010/548, Version: 20101118:153903, <http://eprint.iacr.org/2010/548.pdf>, November 2010

[27] Quynh Dang, National Institute of Standards and Technology: *NIST SP 800-107 Recommendation for Applications Using Approved Hash Algorithms*, Federal Information Processing Standards Publication, Gaithersburg, February 2009

[28] Bruce Schneier: *Attacks on Cryptographic Hashes in Internet Protocols*, Request for Comments: 4270, The Internet Engineering Task Force (IETF), November 2005

[29] Ewan Fleischmann, Christian Forler, and Michael Gorski: *Classification of the SHA-3 Candidates*, Cryptology ePrint Archive, Report 2008/511, Version: 20090419:140227, <http://eprint.iacr.org/2008/511.pdf>, April 2009

[30] Yannick Seurin: *On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model*, Lecture Notes in Computer Science Volume 7237, p. 554-571, Advances in Cryptology – EUROCRYPT 2012, Springer, 2012

[31] Viktor D. Polic: Construction of Σ - Protocol for guarding privacy, In: Metalurgia International, Vol. 18, No. 5-2013, p.131, ISSN: 1582-2214, Bucharest, 2013

[32] Haibo Tian, Fangguo Zhang, Xiaofeng Chen and Baodian Wei: *Selectively unforgeable but existentially forgeable signature schemes and applications*, Accepted for publishing by China Science: Information Sciences, <http://www.cs.sysu.edu.cn/~thb/papers/scs-accepted.pdf>, 2012

- [33] Marcel Keller, Gert Læssøe Mikkelsen, Andy Rupp: *Efficient Threshold Zero-Knowledge with Applications to User-Centric Protocols*, Will be published at "6th International Conference on Information-Theoretic Security (ICITS) 2012, version: 20120603:213734, Cryptology ePrint Archive: Report 2012/306, <http://eprint.iacr.org/2012/306>
- [34] Peter W. Shor: *Algorithms for quantum computation: Discrete logarithms and factoring*, Proceedings of the 35nd Annual Symposium on Foundations of Computer Science (Shafi Goldwasser, ed.), p. 124-134, IEEE Computer Society Press, 1994
- [35] Erik Lucero, R. Barends, Y. Chen, J. Kelly, M. Mariantoni, A. Megrant, P. O'Malley, D. Sank, A. Vainsencher, J. Wenner, T. White, Y. Yin, A. N. Cleland and John M. Martinis: *Computing prime factors with a Josephson phase qubit quantum processor*, Nature Physics, Vol. 8, No. 10, p. 719-723, ISSN: 1745-2473, 2012
- [36] Nanyang Xu, Jing Zhu, Dawei Lu, Xianyi Zhou, Xinhua Peng, Jiangfeng Du: *Quantum Factorization of 143 on a Dipolar-Coupling NMR system*, Cornell University Library, CLN: 10-500, arXiv:1111.3726, November 2011
- [37] United Nations General Assembly: *Resolution on World Summit on the Information Society*, A/RES/56/183, New York, 21 December 2001
- [38] World Summit on the Information Society: *Declaration of Principles*, WSIS-03/GENEVA/DOC/4-E, Geneva, 12 December 2003
- [39] World Summit on the Information Society: *Plan of Action*, WSIS-03/GENEVA/DOC/5-E, Geneva, 12 December 2003
- [40] World Summit on the Information Society: *Tunis Commitment*, WSIS-05/TUNIS/DOC/7, Tunis, 18 November 2005
- [41] World Summit on the Information Society: *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6 (Rev. 1), Tunis, 18 November 2005
- [42] United Nations Public Administration Network: *E-Government Survey 2012*, ST/ESA/PAD/SER.E/150, ISBN: 978 -92 -1-12319 0 -8, New York, 2012
- [43] David Banisar: *The Right to Information and Privacy: Balancing Rights and Managing Conflicts*, The International Bank for Reconstruction and Development / The World Bank, SSRN: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1786473, Washington DC, 2011
- [44] European Parliament and Council: *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM/95/375 COM/92/422 COM/90/314-2, Luxemburg, 24 October 1995
- [45] Assemblée fédérale de la Confédération suisse: *Loi fédérale sur la protection des données*, RS 235.1, Bern, 19 juin 1992 (Etat le 1^{er} janvier 2011)
- [46] Государственная дума: *Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ О персональных данных*, Российская газета № 4131, Москва, 29 июля 2006
- [47] Народна Скупштина Републике Србије: *Закон о заштити података о личности*, Службени гласник РС, бр. 97/08, Beograd, 27.10.2008. године
- [48] Kristof Kessler, Nils Hettich, Chadley Parsons, Craig Richardson and Anny Triana: *A Framework for Assessing Privacy Readiness of e- Government*, Centre for Development Informatics, Institute for Development Policy and Management, University of Manchester, ISBN: 978-1-905469-15-4, Manchester, 2011
- [49] Francis Fukuyama: *Trust: The Social Virtues and The Creation of Prosperity*, Free press, ISBN: 978-0684825250, New York, 1996
- [50] Bruce Schneier: *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, Wiley, ISBN: 978-1118143308, New York, 2012
- [51] International Standardization Organization: *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems --*

Requirements, Geneva, 2005

[52] International Standardization Organization: *ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management*, Geneva, 2005

[53] Daniel Bleichenbacher: *Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1*, Advances in Cryptology — CRYPTO '98, Lecture Notes in Computer Science Volume 1462, 1998, pp 1-12, ISBN: 978-3-540-64892-5, Heidelberg, 1998

[54] Ivan Damgard, Sebastian Faust, Pratyay Mukherjee and Daniele Ventur: *Bounded Tamper Resilience: How to go beyond the Algebraic Barrier*, In: ASIACRYPT 2013, Proceedings of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security, Cryptology ePrint Archive: Report 2013/677, Version: 20131024:092422, 23.10.2013

[55] Mihir Bellare and David Cash and Rachel Miller: *Cryptography Secure Against Related-Key Attacks and Tampering*, In: ASIACRYPT 2011, Cryptology ePrint Archive: Report 2011/252, Version: 20110906:203150, 06.09.2011

[56] Claude Elwood Shannon: *A Mathematical Theory of Communication*, The Bell System Technical Journal, vol. 27, pp. 379–423, 623–656, July, October, 1948

[57] Viktor D. Polic: *Implementing Auditability with Non-Interactive Zero Knowledge Proofs*, In: Metalurgia International, Vol. 17, No. 11-2012, p.106, ISSN: 1582-2214, Bucharest, 2012

[58] **République et Canton de Genève, Conseil d'Etat**: *Rapport du Conseil d'Etat au Grand Conseil sur l'audit triennal du système genevois de vote électronique*, http://www.ge.ch/evoting/doc/rapports/RD_983.pdf, RD 983, Genève, 2 avril 2013