Summary of professional achievements

1. Name: Tomasz Hyla, PhD

2. Diplomas, degrees

10.2007 – 09-2011 West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, Informatics, doctoral studies, with a doctoral degree in technical sciences, specialisation: data cryptography

- PhD thesis title: "*Long-term storage of electronic health records in distributed medical registries*"
- chair of the Faculty of Computer Science and Information Technology PhD students council
- the thesis has been recognised as an innovative work by Voivodeship Labour Office in Szczecin in the project "An investment in knowledge is an engine of innovation growth in the region."
- distinction in the category of doctoral thesis in the 5th edition of the competition (2012) for the best thesis organized by the Regional Centre for Innovation and Technology Transfer of the West Pomeranian University of Technology in Szczecin, with the support of the Polish Entrepreneurship Foundation, Zachodniopomorska Grupa Doradcza Sp. z o.o. and INVESTIN Sp. z o.o.

10.2002 – 06.2007 Szczecin University of Technology, Faculty of Computer Science and Information Technology

- field of study*: Informatics - Computer and Telecommunication Networks*
- specialisation*: Information systems security*
- master thesis: "*Smart card implementation of a Fingerprint Feature Extraction and Matching Algorithm compliant with ISO/IEC 19794-8 standard"*, ordered by Giesecke & Devrient www.gi-de.com, grade: very good

3. Information on previous employment in scientific institutions

10.2016 – today Head of Information Security Research Team and Representative of the Dean responsible for R&D project management, West Pomeranian University of Technology in Szczecin

10.2012 – today Assistant professor, West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, Department of Software Engineering, Information Security Research Team

10.2011 – 09.2012	Research assistant, West Pomeranian University of Technology, Faculty of Computer Science and Information Technology, Department of Software Engineering, Information Security Research Team
02.2012 – 07.2012	Lecturer, West Pomeranian Business School, Szczecin

4. Indication of achievement* resulting from Article 16(2) of the Act of 14 March 2003 on scientific degrees and academic title and degrees and title in art (Journal of Laws 2016, item 882, as amended in Journal of Laws 2016, item 1311):

a) Title of the scientific achievement

New methods for ensuring the security of electronic documents

b) (author / authors, title / titles of the publication, year of publication, name of the publishing house, publishing reviewers)

1. Tomasz Hyla, Jerzy Pejaś, **2012**, *Certificate-Based Encryption Scheme with General Access Structure*, A. Cortesi, N. Chaki, K. Saeed, S. Wierzchoń (editors), Computer Information Systems and Industrial Management CISIM 2012, Lecture Notes in Computer Science, vol. 7564, Springer, Berlin, Heidelberg, pp. 41-55. https://link.springer.com/content/pdf/10.1007/978-3-642-33260-9_3.pdf
2. Tomasz Hyla, Imed El Fray, Witold Maćków, Jerzy Pejaś, **2012**, *Long-term preservation of digital signatures for multiple groups of related documents*, IET Information Security, vol. 6, no. 3, pp. 219–227. http://dx.doi.org/10.1049/iet-ifs.2011.0344
3. Tomasz Hyla, Witold Maćków, Jerzy Pejaś, **2014**, *Implicit and Explicit Certificates-Based Encryption Scheme*, K. Saeed, V. Snasel (editors), Computer Information Systems and Industrial Management CISIM 2014, Lecture Notes in Computer Science, vol. 8838, Springer, Berlin, Heidelberg, pp. 651–666. https://doi.org/10.1007/978-3-662-45237-0_59
4. Tomasz Hyla, Jerzy Pejaś, **2016**, *Secure Outsourced Bilinear Pairings Computation for Mobile Devices*, J. Chen, V. Piuri, C. Su, M. Yung (editors) Network and System Security NSS 2016, Lecture Notes in Computer Science, vol. 9955, Springer, Cham, pp. 519-529. https://doi.org/10.1007/978-3-319-46298-1_34
5. Tomasz Hyla, Jerzy Pejaś, **2017**, *A Hess-like Signature Scheme based on Implicit and Explicit Certificates*, The Computer Journal, vol. 60, nr 4, pp. 457-475. https://doi.org/10.1093/comjnl/bxw052
6. Tomasz Hyla, Jerzy Pejaś, **2018,** *Demonstrably Secure Signature Scheme Resistant to k-Traitor Collusion Attack*, IEEE Access, vol. 6, pp. 50154-50168. https://doi.org/10.1109/ACCESS.2018.2868512
7. Tomasz Hyla, **2019**, *Local and Outsourced Simultaneous Verification of Pairing-based Signatures,* Journal of Internet Technology, no. 4/2019. (*article in press)*

c) A discussion of the scientific objective of the above mentioned work and the results achieved, together with a discussion of their possible use

I. Introduction

The subject of the research presented as the scientific achievement concerns new methods in the field of security of electronic documents. The research belongs to the field of technical sciences to the discipline of computer science (according to the new Polish classification of fields: the field of engineering sciences, technical computer science and telecommunications) and it concerns cyber security, information protection and cryptography.

Cyber security is one of the most important aspects of state security, as well as the security of individual organisations and companies. An increasing number of different attacks on information systems makes the security of information systems an inherent element related to the defence of the state. My research concerns mainly the development of new security mechanisms for information systems, which will enable protection against new cyber-attacks. The detection and blocking of cyber-attacks is insufficient, hence it is important to ensure the information system are secure by design.

Information systems should be designed in a way that a large number of cyber-attacks are impossible to carry out. This requires the constant development of new security mechanisms. The basic security risks associated with electronic documents include identity forgery of the author or addressee of the document, access by unauthorized entities, loss of authenticity or loss of legal value over a longer retention period. These threats make it necessary to constantly develop new security mechanisms adapted to newer and newer technologies.

In Poland, the problem of cyberspace protection is addressed by the *Strategy of the Cyber Security of the Republic of Poland for the years 2016-2020*, where in chapter 6 states that it is necessary to intensify research and development activities concerning new threats related to the development of the digital services market. This is related to the constantly growing number of cyber-attacks. In recent years, more and more attacks have come from organisations that are part of the services of various countries. Such organisations have much larger resources and are able to carry out much more advanced attacks, which increases security requirements for information systems, and in particular for systems supporting critical infrastructure.

In this report, the document is understood, in accordance with the Polish Act of 17 February 2005 on computerisation of the activities of entities performing public tasks (Polish Journal of Laws 2017, item 570), as "an individual set of semantic data arranged in a particular internal structure and recorded on an information storage medium". In such an understanding, it may be a pdf file, a text file, an xml file or a file of a different defined format. A document stored in various databases, archives or electronic registers must have basic security attributes. Another similar definition of an electronic document, provided by the International Council on Archives (MRA), explicitly mentions the need for an electronic document to have security attributes. The MRA states that an electronic document is “a specific piece of information generated by computer input, which can also be inserted or supplemented by action, and that this piece of information must contain sufficient content, context and structure to demonstrate the authenticity of the electronic document”.

The best known general models describing basic security features are CIA triad and Parker's hexad [8]. The CIA triad has the following attributes: confidentiality, integrity, availability and is

often extended by authenticity and non-repudiation, and the Parker's hexad has: confidentiality, integrity, availability, authenticity, possession or control, and usefulness.

The research presented in the set of publications submitted for evaluation concern methods in the field of electronic document security. Research problems mainly concern the confidentiality, authenticity, and integrity of documents and groups of documents. The technologies described in the publication set can also be used to ensure non-repudiation (in particular, non-repudiation of origin, time of creation or time of receipt by the system).

Security attributes must be preserved throughout the lifecycle of the document. In the case of long-term document storage, there are additional attributes that should be provided. A digital signature is as important as a qualified certificate associated with it, and therefore it is usually valid for a period of 2 years. After this period, additional measures should be taken to ensure that the documents still have the attributes of authenticity and non-repudiation.

The research covered topics belonging to the four following groups of problems:

1. The first topic concerns the use of blockchains to ensure the non-repudiation of documents. As part of the work related to this topic, the problem related to the integrity and non-repudiation of a large number of grouped documents stored in the long term was addressed.
2. The second topic concerns the problem of group encryption of documents based on access structures enabling any definition of entities that have the right to decrypt the document, as well as enabling the withdrawal of this right.
3. The third topic concerns the problem of certificates, which are considered by many experts as a source of disadvantages of Public Key Infrastructure (PKI). Therefore, it is well-known fact that their lack is a source of many advantages in certificateless and identity-based systems that are based on bilinear pairings. However, the problem of secure distribution of the public key remains open in these systems and requires a good solution to authenticate any copy of the public key used by the signatory or encryption person. As part of the work on this topic, signature and encryption schemes have been developed which combine the advantages of PKI with certificateless schemes or schemes that are using implicit certificates.
4. The last topic concerns problems with the encryption and signing speeds in the schemes based on bilinear pairings. Bilinear pairing calculation, as well as some operations on elliptical curves, are computationally intensive and in case of insufficient computing power of the devices performing them, it is necessary to delegate these computations to other more efficient devices. The aim of the research on this topics was to check the possibilities and propose a way to safely delegate these computations to untrusted servers (clouds). The untrusted servers cannot learn the arguments of the computations. It must also be possible to verify the correctness of the obtained results.

The results of scientific research included in the set of publication may be used in the construction of modern IT systems managing electronic documents and in systems ensuring the security of electronic documents and transactions, i.e. the public key infrastructure. PKI enables practical use of electronic signatures in the economy. In Poland, the digitalization process is progressing in practically all areas of the economy, starting with tax systems and ending with health care. At the same time, the increasing requirements for PKI make it necessary to constantly modernize it. The modernization of PKI is moving towards the use of new algorithms and

signature schemes, as well as new certificate management schemes. That will reduce trust in organisational measures and increase resistance to a larger range of cyber-attacks, while optimizing the use of resources in order to reduce operating costs.

Currently, confidentiality in IT systems is mainly provided through access control. One of the most popular methods of access control is the so-called cryptographic access control, where in order to gain access to the resource you need to have an appropriate decryption key. Such an approach increases security, as it limits the number of system components that must have access to resources. However, cryptographic access control is much more difficult to implement when there are many entities having access to a selected resource. Therefore, there is a need to develop new encryption schemes that could be used in the development of such systems.

In the following part of the report the following are presented: a description of the solved research problems, the most important scientific achievements, a detailed description of scientific achievements divided into four topics, and other scientific accomplishment that are not part of the publication set. A glossary of abbreviations and references to scientific literature are provided at the end of this report.

II. Research problems and scientific achievements

The work on the security of electronic documents is focused on solving a number of scientific problems relating to: the long-term storage of electronic documents, their encryption for user groups, the resistance of signature and encryption schemes to denial of verification and denial of decryption attacks, as well as the use of digital signature schemes and encryption in systems with limited computing power.

The first research problem concerns the long-term storage of digitally signed documents [2], as more and more documents are stored in digital archives. In many cases documents are digitally signed. Unlike handwritten signatures, digital signatures are not valid indefinitely. They expire at the end of the validity of a qualified certificate linking the user's identity with a public key, which usually does not exceed a period of 2-3 years. In the case of long-term archives, e.g. storing medical data, it is necessary to take steps that will extend the validity of the signature. In the case of a large number of signed documents, the efficiency of the system should be taken into account when planning the method of renewing signatures. In the case of multiple long-term archives, many documents often concern one person or entity. There is also the problem of durability of stored information. At the level of a single document, the integrity, authenticity and non-repudiation of a document can be ensured by digital signatures and trusted time stamps. However, providing the technical possibility to verify that all documents belong to the same entity are present, including the possibility to prove that no document has been removed or added to the archive in an unauthorized manner, requires additional security mechanisms.

Another problem concerns document encryption for many users belonging to multiple groups [1]. Currently, user' mobility must be taken into account when designing IT systems, like users process sensitive information, i.e. personal data or a file with valuable content (contracts, projects, etc.). Data is often stored in clouds managed by third parties. Such an approach is convenient, but creates risks related to the information security that are mainly related to unauthorized access and lack of actual control over the data. One way to reduce these risks is to store files in am encrypted form. When organization stores multiple files and has multiple users, encrypting everything with a single key stored e.g. inside an application is not a very secure approach. Users should have access to information in accordance with their access rights, where the right of access is equivalent to possessing an encryption key. The encryption mechanism should allow encryption at such a level as it is required to reflect the granted access rights, including group membership. Nor should the mechanism require the encryption operator to identify specific users, but only groups.

The next research problems are related to new signature and encryption schemes based on bilinear mappings [3, 5, 6]. Bilinear mapping has made it possible to implement many new ideas, e.g. signature schemes and identity-based encryption. The main goal of identity-based schemes, certificateless schemes and schemes based on implicit certificates was to avoid the problem of certificate management. However, in practice this problem was transferred to the problems related to identity management. An implicit certificate is called a numerical value linking the user's identity with a public key and it is a secret; sometimes the word "implicit" is omitted, which may at first glance mislead the reader by suggesting that the certificates are the same as certificates currently used in PKI. In addition, these solutions generate problems related to the distribution of public keys (susceptibility to public key substitution attacks) and create vulnerability to Denial of Decryption (DoD) or Denial of Signature Verification (DoSV) attacks. In

case of a DoSV attack, an adversary cannot forge a signature, but also an authorized user cannot verify it correctly.

Certificateless encryption does not require the user to download a certificate to encrypt the message, but the lack of a certificate also prevents verification of the public key assignment to the identity. As a result, the message encrypter may choose an incorrect public key or even use another one that has never been associated with the right person and the recipient will not be able to decrypt the message. The DoD attack was described for the first time by Liu et al. [9]. In this attack, the adversary cannot get any secret information, but the authorized user is also unable to read this information and use the service normally. DoD and DoSV attacks are attacks on service availability and they can block the system. An adversary is able to carry out these attacks because there is no verification of whether or not a key is actually assigned to a person.

The last group of research problems is related to the often insufficient computing power of mobile devices or application servers [4, 7]. Cloud can be used to delegate data storage or calculations. Delegating calculations enables transferring computationally intensive operations outside the mobile device. Many schemes based on bilinear mapping allow encryption of documents. Due to the widespread use of mobile devices, it is also necessary to implement client applications for mobile devices, whose computing capabilities are much smaller than desktop computers. Therefore, advanced cryptographic operations may be performed too slow to ensure a positive user experience. In particular, in cryptography based on bilinear mappings, there are several operations (calculation of bilinear mapping, operations on points of elliptical curves), the which execution time is measured in milliseconds or tens or even hundreds of milliseconds. Therefore, methods are necessary to safely delegate the calculations to the cloud. Public clouds are the most accessible, which means that the data sent for calculation to the cloud must be processed in such a way that the cloud is not able to know the original values, and there must be a way of verifying the result obtained from the cloud.

A similar problem but related to a very large number of signature verification operations occurs in many server applications. This is especially true for systems processing a large number of documents at the same time, e.g. financial systems or health care systems. Simultaneous verification of a large number of signatures, i.e. even 100,000 signatures, is a computational challenge. This situation occurs mainly when the number of required signature verifications per second changes over time and it is not worthwhile to maintain an infrastructure that would be used only a few days a year.

My research was aimed at solving the above research problems.

I consider the following scientific results (achievements) to be the most important:

1) The GER (Group Evidence Record) scheme, which is a solution extending the functions of the ERS (Evidence Record Syntax) specification [9] and making it possible to proof the existence of a group of documents in the long term as proposed in the paper [2].
2) A new group encryption scheme based on general access structures, allowing flexible selection of groups of users with the right to read information, without the requirement to know the composition of the groups and enabling the user, among other things, to verify whether he or she is a member of an authorised group as proposed in the paper [1].
3) A new paradigm called Public Key Cryptography (based on Implicit and Explicit Certificates IEC-PKC), whose main advantage is protection against denial of decryption attack, and the scheme implementing this paradigm (IE-CBE), proposed in the paper [3].
4) A new digital signature scheme based on implicit and explicit certificates (Implicit and Explicit Certificates-Based Hess's Signature, IE-CBHS), which is resistant to denial of signature verification (DoSV) attacks. Additionally, for the TA it is impossible to reconstruct a partial private key even in cooperation with the signatory. The scheme was proposed in the paper [5].
5) The first signature scheme (IE-CBS-kCAA) based on explicit and classified certificates, using a key construction based on the Sakai-Kasahara key construction method, whose security depends on *k*-mCAA hard computational problem, proposed in the paper [6].
6) Analysis of three models of computation outsourcing to the cloud from mobile devices and a proposal for a modified version of the IE-CBE scheme that allows delegating computations to the cloud, which are described in the paper [4].
7) Proposals of modified verification algorithms for three signature schemes (CLS scheme [11], CBS scheme II [12], IE-CBHS [4]) enabling secure delegation of bilinear pairings and multiplications of a point on an elliptic curve by a scalar. As part of the research, a number of computational experiments were carried out, taking into account different variants of simultaneous verification of 100,000 signatures, taking into account local verifications, batch verification and delegating calculations to a trusted cloud, as well as secure delegation of calculations to an untrusted cloud.

In the next section of the report, the results achieved are described in detail.

III. Description of scientific achievements

a. The use of blockchains to ensure the non-repudiation of documents

Related works

The simplest solution for extending the validity of digital signatures is the application of the XADES-A specification [13], which describes how to sign the document again before the expiration of the signature. Due to the need to generate a timestamp for each document separately, ERS (Evidence Record Syntax) [10] specifications were created, in which Merkel trees [14] are used to reduce the number of required time stamps. Proposals for a digital archive using ERS were presented by Blazic, et al. [15]. Pharow and Blobel [16] presented other solution to reduce the required number of time stamps during the renewal operation. Methods for detecting missing documents are mainly based on different methods based on hash chains (block chains), or more advanced methods, e.g. Haber-Stornett [17, 18] or Benaloh de Mare [19] schemes.

Contribution

In the paper [2] a GER (Group Evidence Record) scheme has been proposed, which is a solution extending the ERS and allows to prove the existence of a group of documents in the long term. GER, similarly to ERS, uses Merkel trees to calculate the hash from the round for which a timestamp is created. On the other hand, unlike in ERS, GER links hashes from a documents in a round and from a group of documents, in a way that allows to obtain new, additional properties:

a) ensuring the non-repudiation of a group of documents in the long term, where the non-repudiation of a group of documents is achieved when the requirement concerning the integrity of a group of documents is met and each of the documents in the group has non-repudiation property; the integrity of a group of documents means that all documents in the group are present and the order in which they have been added is preserved,
b) optimisation of re-time-stamping operations.

Main results

The proposed Signature Preservation Algorithm (SPA) algorithm consists of two phases. In phase one, the documents inside each group are linked together using a one-way cryptographic hash function. Each document is linked with the previous one. The first document in a round is linked with the last document from the previous round and with the previous archive timestamp chain. In phase two, the hashes linking the last document of the round from each group are gathered. The hashes are used as the leaves of a binary hash tree. The root of the hash tree is sent to a trusted timestamp service. The time-stamped hash is stored, together with additional information, in the evidence records of each group to which documents were added in that round. This action finishes the evidence update.

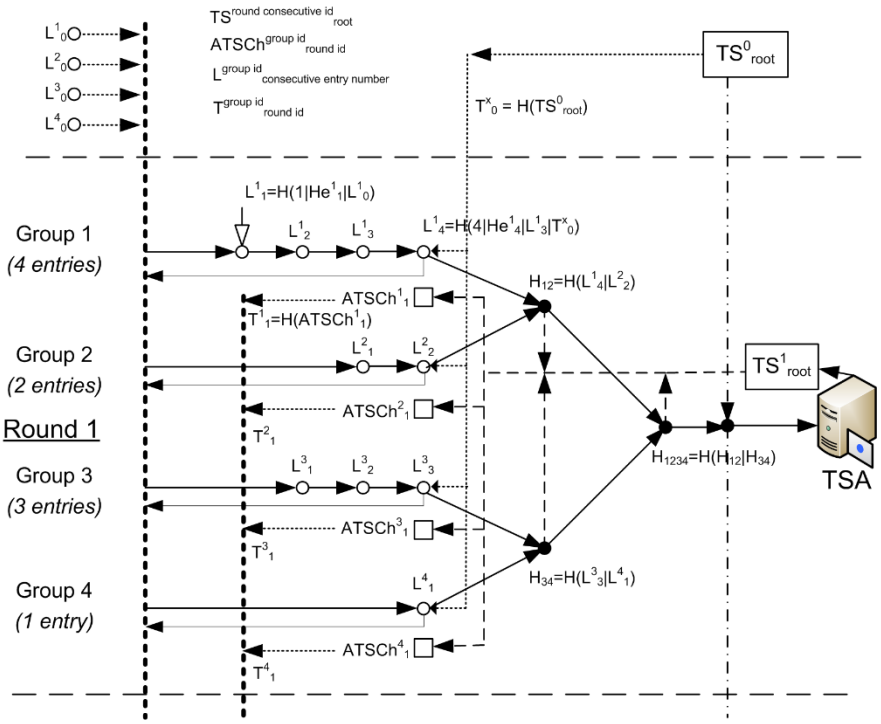

Figure 1. Computation of an archival timestamp in GER (source: Fig. 2 [2])

The security of the solution is based on the security of one-way cryptographic functions, digital signatures and trusted timestamps. The group's non-repudiation verification is threefold and is based on evidence stored in separate evidence records for each group. First, the linking of documents inside the group is verified. Second, the timestamps are verified and finally, the digital signatures are verified.

b. Group encryption using an access structure

Related works

The concept of group-oriented cryptosystems was for the first time proposed by Desmedt [20] and is based on the cooperation of the indicated set of authorized users, creating the so-called access structures.

Many group encryption schemes are based on a traditional public key infrastructure (PKI) based on certificates. However, due to the problems related to the maintenance of the certificate infrastructure, solutions using Identity-based Public Key Cryptography (ID-PKC), Certificateless Public Key Cryptography (CL-PKC), and solution proposed be Gentry [21] that uses (implicit) certificates were proposed. In Gentry's solutions the certificate is a number used when encrypting or calculating the signature and is implicit in contrast to the traditional PKI, where the certificate is a file (data structure) that binds the user's identity to the public key. Many threshold schemes based on identity-based cryptography have been proposed, e.g. [22, 23]. Threshold schemes are less flexible compared to those based on access structures (it can be said informally that the access structure allows to describe any combination of users who have the right to access the resource). One of the proposals for such schemes were proposed by Chang et al. [24] and Xu et al. [25].

Contribution

In the paper [1] a certificate-based encryption scheme with general access structure (CIBE-GAS) was proposed that combines three different ideas: the secret sharing scheme [26], publicly

available evidence of being a member of a particular group [27] and Sakai-Kasahara IBE (SK-IBE) scheme [28] with technique introduced by Fujisaki and Okamoto [29]. Such approach allows achieving the new group encryption scheme with following features:

a) the originator is not required to know the structure of qualified subsets, whose members are authorised to decrypt the information;
b) there is no need to designate a specific recipient of encrypted information - each member within a qualified subset can decrypt it;
c) the scheme is the certificate and ID-based encryption scheme; it means, compared to the certificateless schemes, that partial key created by TA is published as a certificate and it allows simplifying the user's identity verification;
d) The construction of the public component $k_{i,j}$ protects the scheme from dishonest shareholders and from unauthorised changes of the secret values being in possession of all users. This component allows also any member of qualified subset to verify if he or she is a member of an authorised set.

Main results

The CIBE-GAS scheme consists of eight algorithms: *Setup*, *SetSecretValue*, *CertGen*, *SetPublicKey*, *ShareDistribution, Encryption*, *SubDecrytpion,* and *Decryption*. Assume that are given: *n*–element set containing all shareholders $U = \{u_1, u_2, \dots, u_n\}$, dealer $D \notin U$, and combiner $Com \in U$. The algorithms work as follows:

1. *Setup* - the algorithm is run by a trusted authority (TA), which randomly selects the private key s_i and the public key P, P_0, and then publishes the public parameters.
2. *SetSecretValue* - the algorithm is run by each shareholder and the dealer, who selects a random number $s_i \in_R Z_q^*$ and calculates their public keys $Pk_i = (X_i, Y_i)$.
3. *CertGen* - The TA calculates and publishes certificate $Cert_i$ for each user.
4. *SetPublicKey* - each shareholder publishes its public key after the certificate has been validated.
5. *ShareDistribution* - the algorithm is executed by the dealer, who generates shares according to the general access structure and evidence for each shareholder and then publishes a public part of the data.
6. *Encryption* - the algorithm is executed by the dealer who, for the message $M \in \{0,1\}^p$, calculates the cryptogram $C = (C_1, C_2, C_3, C_4, C_5, C_6)$.
7. *SubDecryption* - the algorithm is executed by each shareholder from the privileged subset $u_{ij} \in A_j \in \Gamma$, who partially decrypts the message using his share $s_{i,j}$ and returns it to the combiner.
8. *Decryption* - the algorithm is executed by the combiner (usually one of the users of the privileged set), who decrypts the message *M* based on partial values and checks if it has been decrypted correctly.

The presented CIBE-GAS scheme is secure against attacks with chosen plain text (IND-CID-GO-CPA) in the random oracle model.

The CIB-GAS scheme was additionally implemented and tested within the MobInfoSec project [89]. A cloud-based demo application was created, which consists of two logical servers providing two sets of services (see Figure 2). The *sTA* (Trusted Authority server) located on the S1 server is responsible for managing system parameters, users and certificates and uses the mPBC library.

The mPBC library contains, among others, implemented CIBE-GAS algorithms. The second *sP* (secret Protection server) provides services of Internet sockets, which contain cryptographic operations from the CIBE-GAS scheme (e.g. encryption and partial decryption), which typically would be run on a mobile device.

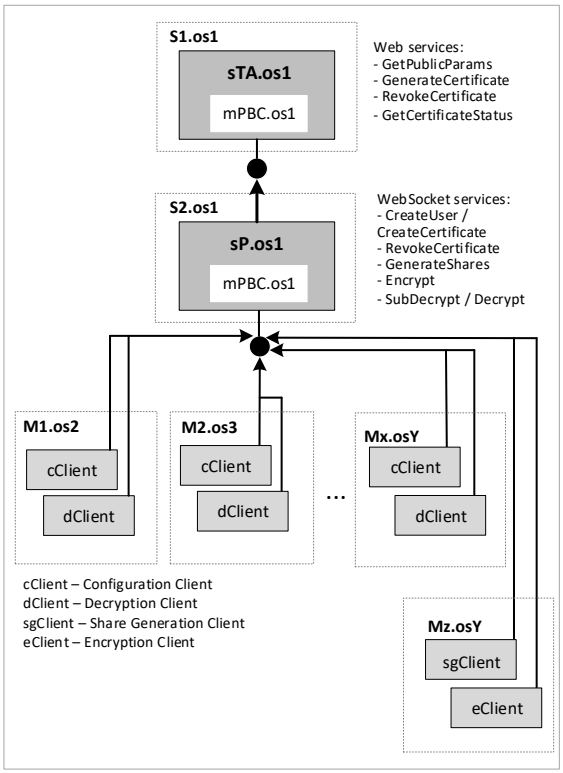

Figure 2. The architecture of demo application using a cloud architecture (source: [89])

Transferring cryptographic operations to *sP* server eliminates the need to port mPBC library for every mobile operating system, but requires creating secure communication channels to mobile devices. It also requires that *sP* server is trusted and provides the same level of security as *sTA* server. This might be seen as drawback, but it also simplifies the development of client applications for mobile devices. Particularly, reducing the number of security issues which must be considered.

c. Signature and encryption schemes based on implicit and explicit certificates

Related works

One of the main drawbacks associated with the public key infrastructure is the need to manage the issued certificates. To solve this problem Shamir [30] proposed Identity-based Public Key Cryptography (ID-PKC). In ID-PKC, the public key is the user's identity. However, the main disadvantage of ID-PKC is the so-called key escrow problem, which is that the Trusted Authority (TA) knows the private keys of all users.

This problem was solved in the cetificateless cryptography (CL-PKC) proposed by Al-Riyami and Paterson [31]. In the CL-PKC, a trusted authority is involved in issuing partial private keys calculated using the user's main secret. In addition, the user independently generates a secret value, which is part of the private key. Therefore, even if TA knows a part of the private key, it is not able to impersonate the user. The TA's ability to retrieve the key is one of the main drawbacks of identity-based encryption. However, due to the lack of explicit verification of public keys, some CL-PKC schemes are susceptible to key replacement attack, as demonstrated by Huang et al. [32]. The solution to this attack was a solution with the use of (implicit) certificates proposed by Gentry [21, 33] concerning the encryption scheme, which was quickly generalized to the certificate signature schemes (Kang et al. [34], Li et al. [35], Li et al. [36], and Wu et al. [12]). In the proposed schemes, the certificate is in practice a part of a private key and is secret. Certificate confidentiality means that the verifier of the signature may indirectly check the authenticity of the certificate and identity, but it can no longer check the validity of the certificate.

Certificateless encryption (CLE) does not require from the user to download a certificate to encrypt the message, but the lack of a certificate also makes it impossible to verify the assignment of a public key to users' identity. As a result, the entity encrypting the message may choose the wrong public key. This attack was described for the first time by Liu et al. [9] and called a Denial of Decryption (DoD) attack. Unfortunately, Certificate-Based Encryption (CBE), introduced by Gentry in 2003 [21], is also not resistant to DoD attack. This is mainly due to the fact that the issued certificate is part of a private key and is a secret certificate, which must remain a secret. This certificate binds the public key to identity, but cannot be used to verify the public key.

In the literature a few solutions of the DoD problem exist (e.g. Liu et al. [9, 37, 38]), but there are no solution for DoSV problem. However, it is well known that the solution of DoD and DoSV problems is natural for the traditional PKC schemes, where the explicit certificate is generated by the TA and directly authenticates the user's public key.

One of the first solutions to the DoD problem was presented by Liu et al. [9], who proposed the idea of Self-Generated Certificate Public Key Encryption (SGC-PKE), which requires the existence of two private keys. In these schemes, the sender can first authenticate the encryption key. This procedure is similar to traditional PKI-based systems, where the sender of the message must download and verify its auto-generated certificate. The difference comes down to a different certification process. In SGC-PKE certificate is generated and managed by the user, and in PKI by a trusted certification authority. However, in the case of global systems this is not an advantage.

IE-CBHS scheme is based on the Hess's signature scheme [31, 39, 40] that according to the techniques shown in [41, 42] is secure in a random oracle model with assumption that Diffie–Hellman problem is a hard computational problem. The Hess's signature scheme was later adopted in the ISO/IEC 14888-3 standard under name ISO/IEC 14888-3 IBS-1 [43] and in Al-Riyami and Paterson's certificateless signature (AP-CLS) scheme [31]. Unfortunately, AP-CLS

scheme in a security model defined in [44] is vulnerable to attacks described in [32, 45]. Due to the improvements based on ideas proposed in [12, 46-48] these attacks on the certificateless signature schemes can be eliminated.

The IE-CBS-kCAA scheme, on the other hand, is based on the wariant of *k*-CAA hard computational problem, which was proposed by Mitsunari et al. [49]. One of the first practical examples of using the *k*-CAA problem is the encryption scheme proposed in 2003 by Sakai and Kasahara [50] and simplified later by Zhang et al. [51] and Scott [52]. The Sakai-Kasahara key construction is also used in signature schemes. One of the first schemes of this type is the ID-based short signature scheme (ZSS), proposed in 2004 by Zhang et al. [51]. Hu et al. [53] demonstrated that the scheme is vulnerable to message-and-key replacement attacks. Nevertheless, this scheme is a basic element of many new signature schemes (e.g.: Barreto et al. [54], Du and Wen [55]).

One of the first certificateless signature schemes based on the *k*-CAA problem was the scheme proposed by Du and Wen [56]. However, in 2011, Fan et al. [57] and Choi et al. [58] independently showed that the scheme cannot be protected from Super Type I adversaries and hence does not allow Girault's level-3 security specifications to be achieved. The improved version of the Du and Wen scheme [56], proposed by Fan et al. [57], also does not allow to achieve this level of security. Examples of cryptanalysis of the signature scheme proposed by Fan et al. can be found in the works [59]-[61]. The Du-Wen's short CLS scheme is vulnerable to Type-I adversaries because this signature scheme is not randomized, i.e. multiple queries of the signature algorithm for the same message always generates a signature with the same value.

c.1 IE-CBE encryption scheme

Contribution

The paper [3] introduced a new paradigm called Implicit and Explicit Certificates-Based Public Key Cryptography (IEC-PKC) to defend against the DoD attack and proposed a concrete encryption scheme (IE-CBE). This scheme preserves all advantages of Certificate-Based Public Key Cryptography (CB-PKC), i.e., every user is given, by the TA, an implicit certificate as a part of a private key and generates his own secret key as well as corresponding public key. In addition, in the IE-CBE scheme the TA has to generate an explicit certificate for a user with some identity and a public key. The purpose of this explicit certificate is similar both to the self-generated certificate in SGC-PKE and the one in traditional PKC. However, the main difference is that in SGC-PKE schemes two secret keys are randomly generated, while in IE-SK-CBE only one. The implicit and explicit certificates should be related with each other in such a way that no one, even the entity of those certificates and their issuer (TA authority) should not be able to recreate an implicit certificate using the explicit certificate.

Main results

The paper [3] proposes an IE-CBE scheme consisting of 8 algorithms: *Setup*, *Create-User*, *Extract-Partial-Private-Key*, *Certificate-Generate, Set-Public-Key*, *Set-Private-Key*, *Encrypt* and *Decrypt.* The structure of the scheme is based on identity-based encryption proposed by Sakai-Kasahara [27, 61] and certificate-based encryption proposed by Y. Lu and J. Li [62]. The functions of the algorithms are as follows:

1. *Setup* - TA initiates and publishes common parameters and randomly selects its private key and calculates the public key.

2. *Create-User* - user *R* generates a key material containing the private key *R* and a partial public key.
3. *Extract-Partial-Private-Key* - The TA calculates a blinded partial private key for entity *R*.
4. *Certificate-Generate* - The TA, using the parameters received from *R* and the values calculated during execution of the *Extract-Partial-Private-Key* algorithm, generates an explicit for *R*.
5. *Set-Private-Key* – an entity *R* calculates the full private key.
6. *Encrypt* - Sender *S,* to encrypt the message *m,* first checks the authenticity of the certificate, selects a random number and calculates the cryptogram *C=(U,V,W).*
7. *Decrypt* - user *R* reconstructs the message *m* using cryptogram *C*.

The IE-CBE scheme is IND-CCA2− and DoD-Free secure in the random oracle model when it is hard to solve *p*-BDHI and *k*-CCA problems. In the IE-CBE construction, the implicit and explicit certificates are based on a short signature scheme given in [65, 66] that security depends on a *k*-CAA hard problem. It means that when adversary is not able to counterfeit an explicit certificate, then it is not possible to execute a DoD attack. The IE-CBE scheme is secure when *k*-CCA problem is a hard computational problem. Because IE-CBE scheme depends on the underlying I-CBE scheme complemented with algorithm *Certificate-Generate*, hence it is natural to divide its security proof into two phases (similar to approach used in [9, 37, 38]): in the first it must be shown that I-CBE scheme is IND-CCA2− secure and in the second that IE-CBE scheme is DoD free.

c.2 IE-CBHS and IE-CBS-kCAA signature schemes

Contribution

The first signature scheme resistant to DoSV attack and based on explicit and implicit certificates has been proposed in the paper [5] (IE-CBHS). The use of explicit and implicit certificates combines the features of traditional public key cryptography with those of systems based on implicit certificates. The scheme is an extension of the signature schemes proposed by Hess [39], Wu et al. [12], Huang et al. [46], and is the first application of the IEC-PKC paradigm for signature schemes. The most important features of the scheme are:

a) verification of the signature may be performed in two modes: with the use of an explicit certificate or with the use of only an implicit certificate;
b) both elements of a two-component private key are known only to a signer;
c) binding between hash functions H_1, H_2, and H_3 that induce a dependence , $H_1 \prec H_2 \prec H_3$, such logical order enforces simplification of the security proofs of the signature schemes [64];
d) the signatory's explicit certificate is public; verification of the certificate before verifying the signature is a similar approach as in PKI systems and makes the scheme resistant to DoSV attacks. Unlike traditional PKI systems, an explicit certificate is a Z_p^* number that is used directly in signature verification equations, simplifying the certificate verification algorithm.

Subsequent research led to the development of the IE-CBS-kCAA scheme (*Implicit and Explicit Certificate-Based Signature Scheme using Sakai-Kasahara's type keys*). The scheme is included in the paper [6]. Compared to the IE-CBHS scheme, it has a different structure. The key construction method is based on the method proposed by Sakai-Kasahara and its security depends on the *k*-mCAA difficult computational problem, which can be reduced to the *k*-CAA problem and to the discrete logarithm problem. It is also constructed on the basis of asymmetric bilinear pairings.

This design results in a scheme that has better performance parameters, especially signing does not contains bilinear pairing operation, what is the most time-consuming operation.

Main results

The IE-CBHS scheme involves three players: the Trusted Authority (TA), which issues explicit and implicit certificates, the signer S who creates signatures, and the message recipient R who verifies the messages. The scheme consists of 7 polynomial time algorithms: *Setup, Create-User*, *Implicit-Cert-Gen*, *Explicit-Cert-Gen*, *Set-Private-Key*, *Sign,* and *Verify*, which work as follows:

1. *Setup* – TA establishes public parameters and its private and public key;
2. *Create*-User – S selects secret number $s_{ID_S}$and creates public key $Pk_S = s_{ID_S}P$;
3. *Implicit-Cert-Gen* – TA based on identity S and its public key Pk_s, generates a partial private key $\overline{Sk}_{ID_S}$ (implicit certificate), which sends secretly to S together with additional parameters*;*
4. *Explicit-Cert-Gen* – TA, using parameters received from S and calculated during the execution of algorithm *Implicit-Cert-Gen,* generates explicit certificate $cert_{ID_S}$;
5. *Set-Private-Key* – S verifies $\overline{Sk}_{ID_S}$ and formulates his private key $Sk_{ID_S} = \left(\overline{Sk}_{ID_S}, s_{ID_s}\right)$;
6. *Sign* – S sign message m, using his private key; two random numbers are selected for each signature;
7. *Verify* – R verifies a signature using an explicit certificate and a public keys.

In the paper [5], only one kind of security notion, EUF under chosen-message attack (CMA) in the random oracle model (EUF-CMA) was considered. In this attack, an adversary allowed to ask the signer to sign any message of its choice adaptively according to previous answers, should not be able to generate a new valid message-signature pair. Similar to notation used by Kanga et al. [34] Gentry et al. [21] and others, two types of adversaries were considered. The adversary A_1 models the role of a dishonest user (anyone except TA). The adversary A_2 models a malicious TA who knows the master key but cannot replace public keys.

The IE-CBS-kCAA scheme is defined by seven polynomial-time algorithms. Its construction is similar to IE-CBHS scheme, because both schemes implement the same paradigm IE-PKC. The Fig. 3 shows data flow when each algorithm from the scheme is executed. The algorithms work as follows:

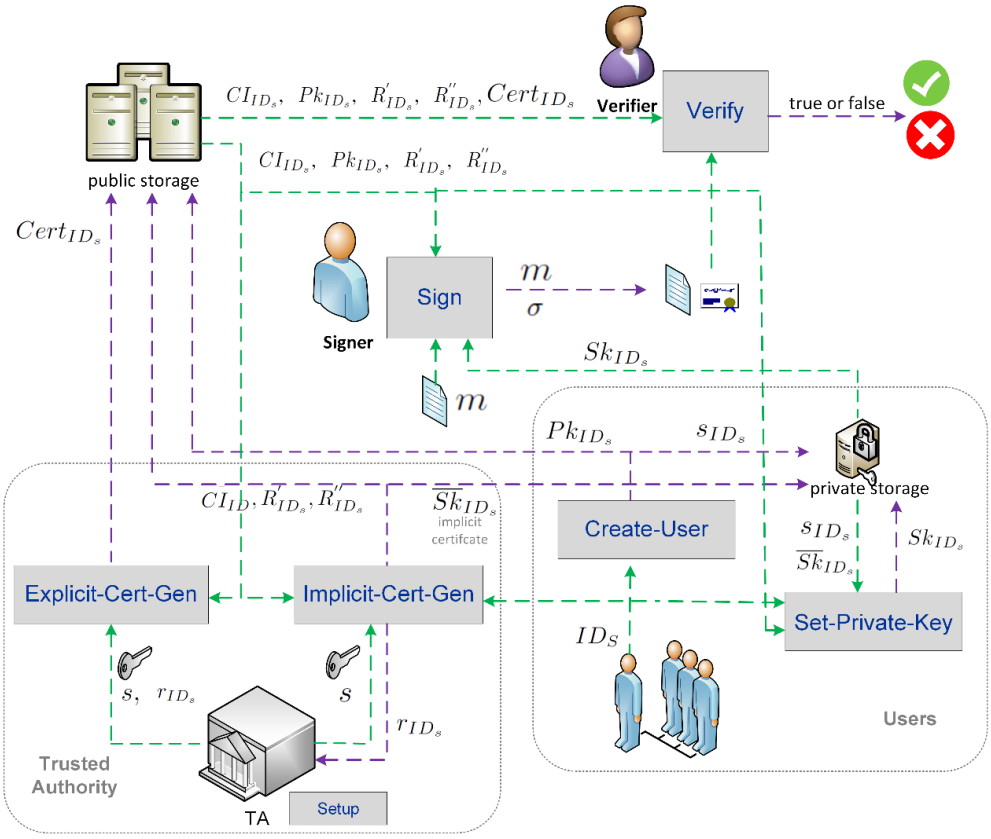

Figure 3. Data flow in IE-CBS-kCAA scheme (source: [6], graphical abstract available online)

1. *Setup* – TA establishes public parameters and its private and public key;
2. *Create*-User – a user selects secret number s_{ID_S} and creates public key $Pk_s = s_{ID_S}P$;
3. *Implicit-Cert-Gen* – TA based on identity S and its public key Pk_s, generates a partial private key $\overline{Sk}_{ID_S}$ (an implicit certificate), information about user's certificate CI_{ID_S} and two components (R'_{ID_S}, R''_{ID_S}), that includes a secret key r_{ID_S} of implicit and explicit certificates;
4. *Explicit-Cert-Gen* – *TA* using its master private key *s,* information about user's certificate CI_{ID_S}, and secret key r_{ID_S}, generates explicit certificate $Cert_{ID_S}$.
5. *Set-Private-Key* – a user based on data received after execution of *Implicit-Cert-Gen* algorithm verifies $\overline{Sk}_{ID_S}$ and formulates his private key $Sk_{ID_S} = (\overline{Sk}_{ID_S}, s_{ID_S})$.
6. *Sign* – a user sign message *m*, using his private key; two random numbers are selected for each signature;
7. *Verify* – a verifier checks the signature using information about user's certificate CI_{ID_S}, explicit certificate $Cert_{ID_S}$, components (R'_{ID_S}, R''_{ID_S}), and public key Pk_s.

The paper [6] includes, similar to IE-CBHS scheme, a formal proof of security. The security model is defined by two games played by the challenger *C* and the adversary *A*, assuming that the adversary chooses which game to play. In both cases, the adversary $A=(A_1, A_2)$ tries to break the EUF-CMA security barriers of the IE-CBS-kCAA scheme, i.e. a formal model describing existential unforgeability.

Table 1 compares the IE-CBHS and IE-CBS-kCAA schemes to schemes based on (implicit) certificates. The table shows the number of most time-consuming operations (M_G stands for scalar

multiplication,), $\hat{e}$ for bilinear pairing, P_{GT} for power in G_T group). Due to a similar design, it is interesting to compare the IE-CBHS scheme to the WMSH Scheme II (W. Wu et al. [12]). Assuming that an explicit certificate is not attached to the signature (this is consistent with the approach used in the PKI), the length of the signature in both schemes is the same. Calculation of the signature is faster in the IE-CBHS scheme, with slower verification. The IE-CBS-kCAA scheme, on the other hand, requires a similar number of time-consuming operations and is slightly more efficient than the IE-CBHS scheme, especially the calculation of the signature is faster (the multiplication in G_T is faster than the calculation of the bilinear pairing).

Table 1. Performance and security comparison (source: [5, 6])

Scheme	Type	Public Key Size	Signature Size	*Sign*	*Verify*	Security level (adversary type)
LHMSW (J. Li *et al.* [60])	I-CBS	$\|G_1\|$	$2\|G_1\|$	$3 M_G$	$3 \hat{e}$	Normal A_1 and Normal A_2
LHZX (J. Li *et al.* [72])	I-CBS	$2\|G_1\|$	$\|G_1\|$	M_G	$\hat{e}+ M_G$	Normal A_1 and Super A_2
CBSa (Kang *et al.* [58])	I-CBS	$\|G_1\|$	$3\|G_1\|$	$3 M_G$	$3\hat{e}+2 M_G$	Strong A_1 and Strong A_2
WMSH Scheme II (Wu, W., *et al.* [73])	I-CBS	$\|G_1\|$	$\|G_1\| +2\|Z_p\|$	$\hat{e}+4 M_G$	$2\hat{e}+3 M_G$	Super A_1 and Super A_2
IE-CBHS	IE-CBS	$\|G_1\|$	$\|G_1\| +2\|Z_p\|$	$\hat{e}+3 M_G$	$2\hat{e}+7 M_G$	Super A_1 and Super A_2
IE-CBS-kCAA	IE-CBS	$\|G_1\|$	$\|G_2\| +3\|Z_p\|$	$2 M_G + P_{GT}$	$2\hat{e}+6M_G$	Super A_1 and Super A_2

d) Accelerating signature creation and verification

The work on speeding up verification and signature creation operations using delegation of calculations was divided into two parts. The first part is concerned the acceleration of signing operations on mobile devices and the second part is concerned on the simultaneous verification of a very large number of signatures on a server.

Related works

Data computation outsourcing enables to move computationally expensive operations outside a mobile device. When outsourcing computation to third party servers, one must consider two questions. Firstly, is it required that data sent to be computed should remain secret? Secondly, is it required to have a tool enabling results' verification? Several techniques that enable verifying outsourced computation results done by untrusted servers have been proposed in the literature (e.g., Gennaro et al. [67]). Formal security definitions, models and notations for secure outsourcing of cryptographic computations can be found in [68]. Earlier in 2005, Girault and Lefranc [58] introduced a Server-Aided Verification (SAV) concept, which allows delegating a substantial part of computations to an untrusted powerful server (a cloud).

One of the first works regarding secure bilinear pairing delegation algorithms was presented by Chevallier-Mames et al. [70]. However, the total computation time of those algorithms is longer than local pairing calculation. One of the algorithms achieves unconditional security, i.e. it is not based on any security assumptions. Conard et al. [71] proposed more efficient versions of a pairing delegation algorithm. Next, Chen et al. [72] presented algorithm *Pair*, which does not require computationally expensive operations. Algorithm *Pair* is secure in the one-malicious version of two untrusted program (OMTUP) model [68]. In this model computations must be split into two parts, which are sent to two different servers U_1 and U_2. One of these servers must be honest for the algorithm to be secure. Later, Tian et al. [73] proposed two improved algorithms comparing to Pair, i.e., *Algorithm A* and *Algorithm B*. Further improved versions of these algorithms have been proposed by Dong et al. [74] and Dong together with the Ren [75].

Other computationally complex operations in pairing-based cryptography are scalar multiplication and modular exponentiation. Hohenberger and Lysyanskaya [68] proposed secure outsourcing schemes for scalar multiplication in the one-malicious version of two untrusted program model. More efficient scheme *Exp* in that security model with higher verifiability was proposed by Chen et al. [75] [77]. Later, Wang et al. [78] proposed an efficient scheme for securely outsourcing modular exponentiations in single untrusted program model, but it is difficult to translate this scheme into an elliptic curve scalar multiplication problem (in some of the other schemes it is a trivial task). Other papers on the secure delegation of modular exponentiation were published by Ding et al. [79], Nguyen et al. [80], Dijk et al. [81], and Zhou and Rhou [82].

Signatures can also be verified using batch processing. The batch verification algorithm returns truth when all signatures are correct and false otherwise. However, not for every signature verification algorithm it is possible to create a batch verification algorithm due to security reasons. The first algorithm was proposed by Fiat [83] followed by works of Harn [84]. Batch verification algorithms for identity-based schemes were proposed by Yoon et al. [85] and Shi et al. [86], and certificateless schemes were proposed by Geng and Zhang [87] and Fan et al. [88].

Contribution

The paper [5] analyses various options for secure outsourcing of bilinear pairing calculations to probably dishonest servers. Three models of delegating calculations were described, a modified version of the IE-CBE scheme was proposed, and a number of experiments were carried out, which showed that delegating the calculations to the cloud speeds up the total calculation time under certain conditions.

In the paper [7], the verification algorithms from three signature schemes (CLS scheme [11], CBS scheme II [12], IE-CBHS [5]) were modified in a way to enable secure delegation of bilinear pairing calculations and calculations of multiplication of a point on an elliptical curve by a scalar. A number of computational experiments have been carried out, taking into account different variants of simultaneous verification of 100,000 signatures, including local verification, using batch verification and delegating calculations to a trusted cloud, as well as secure delegation of calculations to an untrusted cloud.

Main results

The computation of pairing $\propto= \hat{e}(A, B)$ can be outsourced from a mobile device T to a server U using the following models:

- *Model 0 – No Outsourcing*: calculations are done solely on a mobile device;
- *Model 1 – Semi-Secure Outsourcing*: U does not know A and B. If U is dishonest, no mechanism exist that enables T to verify if α is correct.
- *Model 2 – Secure Outsourcing*: U does not know A and B. T can verify if α is correct. U can be dishonest.
- *Model 3 – Full Outsourcing*: a mobile device is only a thin client (provides only an interface), requires a fully trusted and honest U. A and B are send to U in an overt form.

The SO-IE-CBE scheme is a modified version of the IE-CBE scheme that uses secure outsource algorithm for pairing calculation (*Model 2*). The IE-CBE scheme, involves three entities: a trusted authority TA, an encrypter *S*, and a decrypter *R*. The *S* and *R* entities use four algorithms from the IE-CBE scheme: two from setup phase (*Create-User*, *Set-Private-Key*) – executed only once per entity and two algorithms (*Encrypt*, *Decrypt*) that can be used many times. However, algorithm *Create-User* does not involve pairing calculations. In the paper [4], two outsourced versions of IE-CBE scheme are proposed:

- *SO-IE-CBE*: SO-IE-CBE is IE-CBE scheme with three modified algorithms (*SO-Set-Private-Key, SO-Encrypt, SO-Decrypt*). The scheme uses a secure outsourcing algorithm *SO-PAR* for pairing calculation. The *SO-PAR* algorithm is a secure outsourcing algorithm for a symmetric pairing calculation that takes as an input $A, B \in G_1$ and returns $\hat{e}(A, B) \in G_2$.
- *O-IE-CBE*: O-IE-CBE is also IE-CBE scheme with three modified algorithms (*O-Set-Private-Key, O-Encrypt, O-Decrypt*), but the scheme uses a semi-secure outsourcing algorithm *O-PAR* for pairing calculation that not verifies if returned value from U is correct.

SO-IE-CBE and O-IE-CBE schemes are similar. They use different algorithm for outsourced pairing calculation. Also, the *O-Encrypt* algorithm has an additional optional step that is able to detect potentials pairing error. In terms of security, using a secure delegation algorithm should not change the security of the scheme. In particular, if an unconditionally secure delegation algorithm is used.

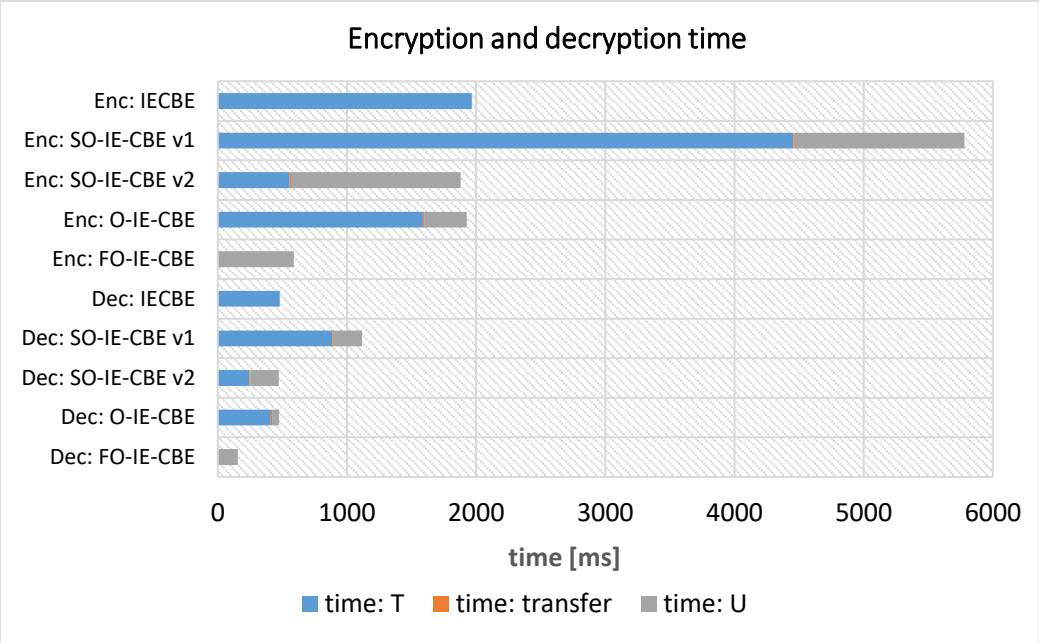

Figure 4. Comparison of encryption and decryption time for various options (source: Fig. 1 [4])

The Figure 4 shows the calculation times in the test environment of IE-CBE encryption and decryption operations and a modified version of the algorithm using different models of calculations' delegation. The version of the algorithm with calculations' secure delegation requires the same total time or is faster (it depends on the time of data transmission to *U* and the difference in performance between *T* and *U*).

The simultaneous verification of a large number of signatures requires a lot of processing power. The total time could be decreased tenfold by using more powerful processors with ten or more processor cores. The same acceleration was achieved in test environment using secure outsourcing of BP (bilinear pairing) and SM (scalar multiplication) operations, which can accelerate computation around 10 to 40 times depending on the signature scheme and cloud configuration. Using the same cloud configuration, it is possible to achieve 100 acceleration ratio when the local server is 2-3 times more powerful.

The batch verification is an easy method to implement solution for verification of many signatures at the same time in cases where all verified signatures are expected to be correct. In tested cases, it allows to calculate a scalar multiplication instead of a bilinear pairing for each signature and to reduce the total computation time up to three times. However, in practice to create a batch verification algorithm, a signature verification algorithm must have a linear structure of an equitation that contains a bilinear pairing or a scalar multiplication computations. Outsourcing only the most time-intensive operations simplifies the creation process of outsourced versions of verification algorithms. In comparison to SAV protocols designed especially for each scheme, the security of outsourced scheme depends on the security model used for computations outsourcing. Table 3 contains general comparison of different methods of signatures' simultaneous verification.

Even with outsourcing expensive operations(BP, SM) to a trusted cloud, it will be still difficult to reduce total time for verification of 100k signatures to a few seconds, because of other non-intensive computations that must be done locally and data transfer times. Even when entire verification algorithms is outsourced to a cloud, it will be difficult to decrease total verification

time to a few seconds when signed files are large. However, it should be possible to slightly change the schemes (i.e. replace a message with a hash of a message), what will reduce the total transfer time, but requires to calculate hashes locally. After such modifications the schemes will be similar to signatures schemes used currently in a public key infrastructure, where in most of the cases it is only required to send a hash of a file to the cloud for outsourced verification.

Table 3. Comparison of different verification methods (source: Tab. 4 [7])

Method	Computations		Total implementation complexity	Cloud implementation requirements	Cloud security requirements
	local	remote			
local verification	Yes	No	low	N/A	N/A
batch verification	Yes	No	medium	N/A	N/A
generic outsourcing	No	Yes	low	complete verification algorithm	high
outsourcing of computationally intensive operations	Yes	Yes	medium	only some computations: BP, SM	high
secure outsourcing of computationally intensive operations	Yes	Yes	high	only some computations: BP, SM	low
secure outsourcing of computationally intensive operations using *OMTUP model*	Yes	Yes	high	only some computations: BP, SM	medium

The experiments show that using secure outsourcing (in one-malicious version of two untrusted program model) is only around 1.8 to 3.3 times slower (depending on the scheme) than outsourcing to a trusted cloud. The further acceleration of secure outsourcing algorithms would require secure outsourcing algorithms with minimal time for a local verification that includes obfuscation of calculation arguments and verification of the result. Existing algorithms with efficiency ratio around 0.30 require many hours to verify of 100k signatures.

5. Discussion of other scientific and research achievements

5.1 MobInfoSec project

In years 2012-2015, I participated in the project entitled "Mobile device for protection of classified information" (MobInfoSec) financed by the NCBR (National Centre for Research and Development) under the Applied Research Program, carried out by West Pomeranian University of Technology in Szczecin, Military University of Technology of Warsaw and Unizeto Technologies SA (currently Asseco Data Systems SA). My achievements, within this project, included participation in the development of MobInfoSec system and the development of the mPBC library [89] as one of the tasks. The mPBC library was described earlier within the description of scientific achievements.

The problem solved by MobInfoSec system is a problem resulting from lack of an offer on the market concerning the transparently enforced protection of sensitive information collected from various sources and stored on mobile devices and preventing it from being passed on to third parties without the consent of the information administrator. It applies to users of mobile devices, both private individuals and employees of companies and organizations who store sensitive information on mobile devices.

MobInfoSec is aimed at users (individuals and legal persons) who use (or want to use) cryptographic systems for the protection of sensitive data by means of mobile devices. MobInfoSec is a distributed, modular and configurable cryptographic access control system for sensitive information, operating in a public environment, with a uniform interface allowing the use of functions built into the system. The basic features of the system are:

- cryptographic protection of sensitive information in accordance with the ORCON principles according to the access policy;
- protecting mobile information and relieving the user from the obligation to supervise any information (in particular against unauthorized copying of protected data);
- enabling the creation of a reliable mobile device that will implement the principles of access control to classified information in accordance with the ORCON model;
- enabling building trust in hardware and software components of a mobile device and trust in other devices.

As result of the project, a system design and its demo version were developed. MobInfoSec received a silver medal at the international fair in Paris - 113th International Exhibition of Innovation "Concours Lépine" and an award for innovative achievements in 2014 in the international arena "Inventory Exchange 2015" organized by the Minister of Science and Higher Education in Poland.

5.2. MOBINAV project

In 2012-2015, I participated in the project entitled "Mobile inland navigation (MOBINAV)" financed by NCBR under the Lider programme and implemented by Marine Technology Ltd. Within this project my two main achievements were the development of a decision support system for safety isobath designation [90] (together with N. Wawrzyniak) and the creation of a MOBINAV technology demonstrator, where I was the main person responsible for programming.

The paper [90] proposes a decision support system for automatic determination of the safety isobath, which determines non-navigable areas on the basis of bathymetric spatial data and other data like: geographical position, age of data, type of water body and water level. Due to the high

uncertainty of data, the solution uses the rough set theory to create decision-making rules. The decision-making rules were created with the use of experimental data (real depth measurements by means of an echo sounder) taken in the waters near Szczecin.

The demonstrator of MOBINAV technology is a universal Windows 10 application built using Microsoft Visual Studio. This approach allows to create a single application that can be run on all mobile devices with Windows 10. At the same time, the application has an interface that changes and adapts depending on the type of device. For example, on a tablet in a vertical position, part of the information fields is displayed on the right (Fig. 5), and on a smartphone in a vertical position, the same fields are displayed at the top of the screen.

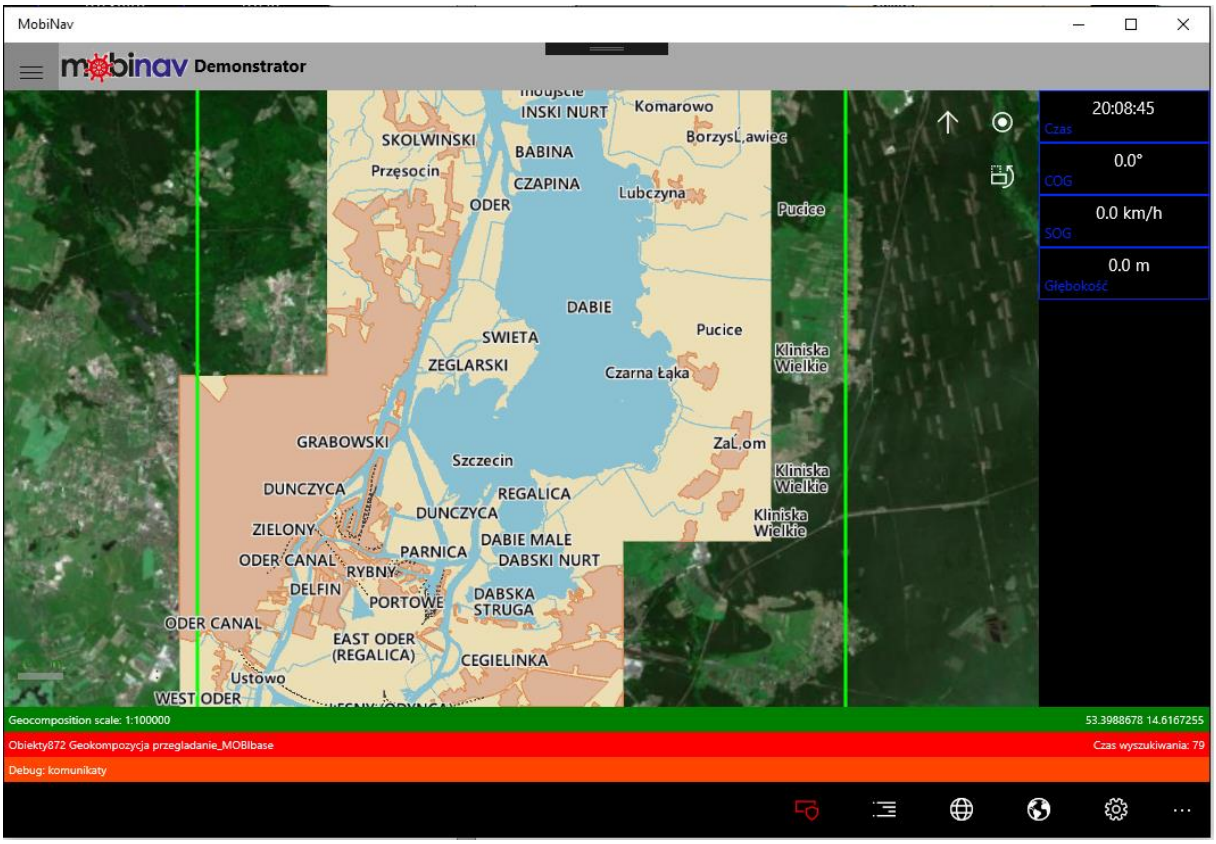

Figure 5: A screenshot of a MOBINAV demonstrator running on the tablet

The most important functions implemented as part of the system demonstrator are:

- support for a gml file (MODEF) with a cell containing a map encoded according to a format developed within the project, together with support for generalized geometry in case of its occurrence in a cell with a map;
- support for json-type file (MONAKO) containing: model of displaying individual cartographic presentation units in different styles, description of contents of individual geocompositions and geocompositions of components;
- algorithm for displaying objects read from the gml MODEF file and from the MONAKO file according and the algorithm for automatic selection of geocompositions, as well as WMS support;
- handling alarms such as: man overboard, approaching a navigation obstacle, approaching dangerous depths, approaching dangerous depths, approaching dangerous areas and information messages;
- handling of functions related to spatial analyses;

- sensor-related functions: integration and display of data from the device's internal sensors (position, speed, course) and from external sensors (e.g. AIS, depth) acquired through WiFi.

5.3 Papers in review

5.3.1 Certificate-based Group Signature Scheme with Publicly Verifiable General Access Structure

The paper was written jointly with J. Pejaś and has been in review in the Journal of Computer and System Sciences (IF = 1,497) since September 2017. My contribution to this work consists of: preparation of the analysis of related works, participation in the development of the scheme and preparation of the safety proof, as well as the implementation of the scheme and the execution of tests. I estimate my share at 50%.

The article proposes a group signature scheme based on access structures. The scheme is based on the division of the secret (Sang et al. [26]) and the signature scheme (Zhang et al. [91]). The proposed scheme is a generalized group signature scheme based on certificates, which meets the requirements for generalized signature schemes, the most relevant of which are:

- forward security, which causes the person leaving the group (authorized collection) to no longer create signatures;
- user shares can be publicly verified;
- the scheme ensures the anonymity of the members of the authorised set;
- in the event of a dispute, the identity of the members of the collection can be publicly verified;
- authorised set can be dynamically modified.

The scheme meets the requirements for correctness, anonymity, unlinkability, exculpability, traceability, coalition-resistance, forward security and is existentially unforgeable under chosen message attack (EUF-CMA) in the random oracle model assuming that the CDH (Computational Diffie-Hellman) problem is a hard computational problem.

5.3.2 Long-term Verification of Signatures Based on a Blockchain

The paper was written jointly with J. Pejaś and has been in review in Computers & Electrical Engineering magazine (IF = 1,747) since October 2018. My contribution to this work consists of: preparation of the introduction, development of the RBTS scheme and participation in the security analysis. I estimate my share at 60%.

The paper proposes the Round-based Blockchain Time-stamping Scheme (RBTS), which makes it possible to maintain the validity of a large number of digital signatures using blockchain-based cryptocurrency and presents an analysis of its security. The scheme does not require the use of time stamps from trusted third parties. It is based on the Haber-Stornett scheme [17] and OpenTimestamps [92]. Compared to OpenTiemstamps, the scheme contains a new algorithm for verifying signatures according to the *modified shell model* [93], and other algorithms have been adapted to support digital signatures.

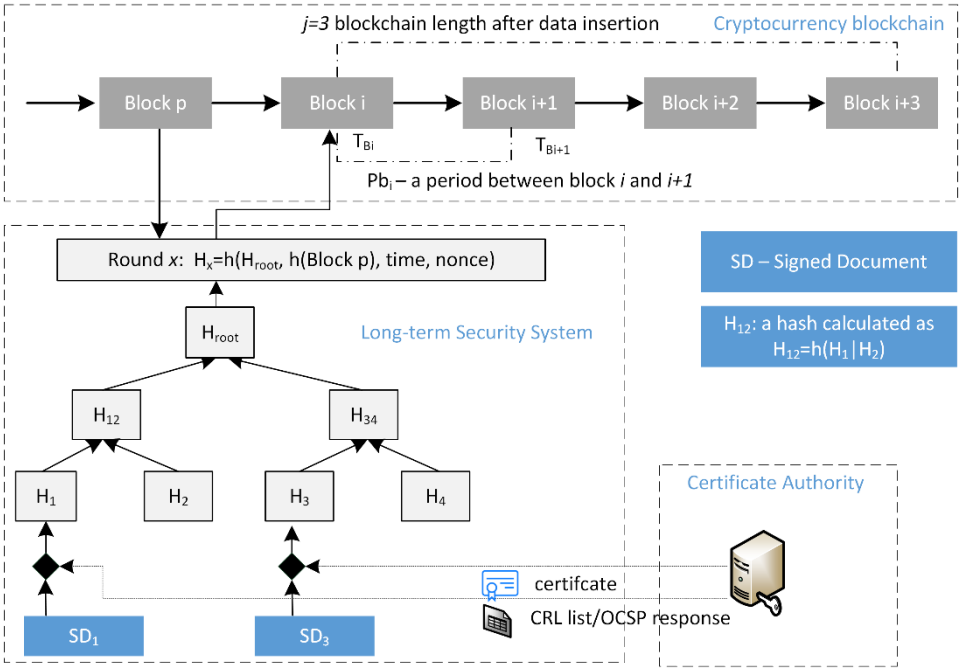

Figure 6: Illustration of adding documents in the RBTS scheme.

The main advantage of the RBTS scheme is that after adding documents to the cryptocurrency, the user can store the signed document in his archive without the need to perform maintenance activities in the future, which is contrary to the current PKI (apart from monitoring of the security of cryptographic algorithms, which should also be monitored in the current PKI). The scheme is scalable, it requires embeding a fixed number of bytes into the blockchain regardless of the number of input documents. Fig. 6 shows a diagram showing the process of inserting documents according to RBTS.

5.3.3 eHealth Integrity Model Based on a Permissioned Blockchain

The paper was written jointly with J. Pejaś and has been in review in Future Internet Journal since January 2019. It is an extended version of the paper from ICCSCS conference 2018 [94]. My contribution to this work consists of: preparation of the concept of the paper, participation in the development of the model and its analysis, preparation of the initial version of the article. I estimate my share at 60%.

The paper presents a blockchain-based eHealth Integrity Model (BEIM). The model uses a private blockchain (a permissioned blockchain) and off-chain storage of information. Unlike the existing solutions, the model allows to remove information from the e-Health system (medical data or other logs). Usually, a new record is added to e-Health systems and the old record is marked as outdated and preserved, but there are rare cases obligatory by law requiring the deletion of records.

The paper also includes a discussion of security issues related to blockchain technology, which must be considered when using it in e-Health systems. The proposed model can be easily integrated with systems using service-oriented architecture. The main research question was whether it was possible to design a model that would allow for transactional transparency in eHealth systems, which does not require trusted third parties and supports the removal of documents.

Blockchain technology can be used to store complete medical data or to store security-related data only. In BEIM, blockchain is mainly used to implement data integrity service. This service can be implemented using other mechanisms, but blockchain provides a solution that does not require trusted third parties. In addition, it allows combining patient records that are produced simultaneously in multiple healthcare facilities.

Glossary of abbreviations

BEIM	Blockchain based eHealth Integrity Model
BP	Bilinear Pairing
CBE	Certificate-Based Encryption
CDH	Computational Diffie-Hellman (problem)
CIBE-GAS	Certificate and ID-based Group Oriented Decryption Scheme with General Access Structure
CL-PKC	Certificateless Public Key Cryptography
CLE	Certificateless Encryption
DoD	Denial of Decryption (atack)
DoSV	Denial of Signature Verification (atack)
ERS	Evidence Record Syntax
GER	Group Evidence Record
ID-PKC	ID-based Public Key Cryptography
IEC-PKC	Implicit and Explicit Certificates-Based Public Key Cryptography
IE-CBE	Implicit and Explicit Certificates-Based Encryption
IE-CBHS	Implicit and Explicit Certificates-Based Hess's Signature
IE-CBS-kCAA	Implicit and Explicit Certificate-Based Signature Scheme using Sakai-Kasahara's type keys
O-IE-CBE	Outsourcing-Implicit and Explicit Certificates-Based Encryption
OMTUP	One-Malicious version of Two Untrusted Program model
PKI	Public Key Infrastructure, infrastruktura klucza publicznego
RBTS	Round-based Blockchain Time-stamping Scheme
SAV	Server-Aided Verification
SK-IBE	Sakai-Kasahara Identity-Based Encryption
SM	Scalar Multiplication
SO-IE-CBE	Secure Outsourcing-Implicit and Explicit Certificates-Based Encryption
sP	secret Protection server
SPA	Signature Preservation Algorithm
sTA	Trusted Authority server
TA	Trusted Authority

References

References 1-7 are references to publications from the publication set, presented on page 2.

8. Parker, D. B.: *Fighting Computer Crime*, New York, NY, John Wiley & Sons, ISBN 0-471-16378-3, 1998.
9. Liu, J., Au, K., Susilo, W.: *Self-Generated-Certificate Public Key Cryptography and certificateless signature/encryption scheme in the standard model: Extended abstract*. In: Bao, F., Miller, S. (eds.) ASIACCS 2007, pp. 273–283. ACM Press, 2007.
10. Gondrom, T., Brandner, R., Pordesch, U.: *RFC 4998 evidence record syntax (ERS*), 2007.
11. Zhang, L., Zhang, F.: *A New Provably Secure Certificateless Signature Scheme*, 2008 IEEE International Conference on Communications, Beijing, China, pp. 1685-1689, 2008.
12. Wu, W., Mu, Y., Susilo, W., Huang, X.: *Certificate-based signatures revisited*, Journal of Universal Computer Science, Vol. 15, No. 8, pp. 1659-1684, April, 2009.
13. ETSI, TS 101 903, *XML advanced electronic signatures (XAdES),* v1.4, 2009.
14. Merkle, R.C.: *Method of providing digital signatures*, US patent number 4309569, 1982
15. Blazic, A.J., Klobucar, T., Jerman, B.D.: *Long-term trusted preservation service using service interaction protocol and evidence records,* Comput. Stand. Interfaces, 29, pp. 398–412, 2007.
16. Pharow, P., Blobel, B.: *Electronic signatures for long-lasting storage purposes in electronic archives*, Int. J. Med. Inform., 74, pp. 279–287, 2005.
17. Haber, S., Stornetta, W.S.: *How to time-stamp a digital document*, J. Cryptol., 3, (2), pp. 99–111, 1991.
18. Bayer, D., Haber, S., Stornetta, W.S.: *Improving the efficiency and reliability of digital time-stamping*, in Capocelli, R.M., DeSantis, A., Vaccaro, U. (Eds.): 'Sequences'91: methods in Communication, Security, and Computer Science', Springer-Verlag, pp. 329–334, 1992.
19. Benaloh, J., de Mare, M.: *Efficient broadcast time-stamping,* Technical report 1, Department of Mathematics and Computer Science, Clarkson University, August 1991.
20. Desmedt, Y.: *Society and Group Oriented Cryptography: A New Concept*. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 120–127. Springer, Heidelberg, 1988.
21. Gentry, C.: *Certificate-based Encryption and the Certificate Revocation Problem*. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 272–293. Springer, Heidelberg, 2003.
22. Baek, J., Zheng, Y.: *Identity-Based Threshold Decryption*. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 262–276. Springer, Heidelberg, 2004.
23. Long, Y., Chen, K., Liu, S.: *ID-based threshold decryption secure against adaptive chosen ciphertext attack*. Computers and Electrical Engineering 33(3), 166–176, 2007.
24. Chang, T.-Y.: *An ID-based group-oriented decryption scheme secure against adaptive chosen-ciphertext attacks*. Computer Communications 32(17), 1829–1836, 2009.
25. Xu, C., Zhou, J., Xiao, G.: *General Group Oriented ID-Based Cryptosystems with Chosen Plaintext Security*. International Journal of Network Security 6(1), 1–5, 2008.
26. Sang, Y., Zeng, J., Li, Z., You, L.: *A Secret Sharing Scheme with General Access Structures and its Applications*. International Journal of Advancements in Computing Technology 3(4), 121–128, 2011.
27. Long, Y., Chen, K.-F.: *Construction of Dynamic Threshold Decryption Scheme from Pairing*. International Journal of Network Security 2(2), 111–113, 2006.
28. Sakai, R., Kasahara, M.: *ID based cryptosystems with pairing on elliptic curve*. Cryptology ePrint Archive, Report 2003/054, 2003.
29. Fujisaki, E., Okamoto, T.: *Secure Integration of Asymmetric and Symmetric Encryption Schemes*. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg, 1999.
30. Shamir, A.: *Identity-Based Cryptosystems And Signature Schemes.* Advances in Cryptology: Proc. Of Crypto'84 A Workshop on the Theory and Application of Cryptographic Techniques, University of California, Santa Barbara, USA, August 19–22, 1984, LNCS , vol. 196, pp. 47–53. Springer-Verlag, Berlin, 1984.
31. Al-Riyami, S.S., Paterson, K.G.: *Certificateless Public Key Cryptography.* Advances in Cryptology – ASIACRYPT 2003, 9th Int. Conf. on the Theory and Application of Cryptology and Information Security, Taipei, 2003.
32. Huang, X., Susilo, W., Mu, Y. , Zhang, F. : *On the Security of Certificateless Signature Schemes from Asiacrypt 2003*. Cryptology and Network Security, 4th Int. Conf., CANS 2005, Xiamen, China, December 14–16, Lecture Notes in Computer Science 3810, pp. 13–25. Springer, Berlin, 2005.
33. Lu, Y. , *Efficient certificate-based proxy re-encryption scheme for data sharing in public clouds*. KSII Trans. Internet Inf. Syst., 9(7), 2703–2718, 2015.
34. Kang, G., Park, J. H. and Hahn, S. G., *A Certificate-Based Signature Scheme*. Topics in Cryptology – CT-RSA 2004, The Cryptographers' Track at the RSA Conf. 2004, San Francisco, CA, USA, February 23–27, Lecture Notes in Computer Science 2964, pp. 99–111, Springer-Verlag, Berlin, 2004.
35. Li, J., Xu, L., Zhang, Y.: Provably secure certificate based proxy signature schemes. J. Comput., 4, 444–452, 2009.

36. Li, J., Huang, X., Mu, Y., Susilo, W. , Wu, Q.: *Certificate-Based Signature: Security Model and Efficient Construction*. Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice, EuroPKI 2007, Palma de Mallorca, Spain, June 28-30, Lecture Notes in Computer Science 4582, pp. 110–125. Springer-Verlag, Berlin, 2007.
37. Lai, J., Kou, W.: *Self-generated-certificate public key encryption without pairing*. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 476–489. Springer, Heidelberg, 2007.
38. Dent, A.W.: *A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures*. In: Martinelli, F., Preneel, B. (eds.) EuroPKI 2009. LNCS, vol. 6391, pp. 1–16. Springer, Heidelberg, 2010.
39. Hess, F.: *Efficient Identity Based Signature Schemes Based on Pairings. Selected Areas in Cryptography*, 9th Annual Int. Workshop, SAC 2002 St. John's, Newfoundland, Canada, August 15–16, 2002, Lecture Notes in Computer Science 2595, pp. 310–324, Springer, Berlin, 2002.
40. Barreto, P.S.L.M., Libert, B., McCullagh, N. and Quisquater, J. J.:*Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps*. Advances in Cryptology - ASIACRYPT 2005, 11th Int. Conf. on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, Lecture Notes in Computer Science 3788, pp. 515–532. Springer-Verlag, Berlin, 2005.
41. Pointcheval, D., Stern, J.: *Security Proofs for Signature Schemes.* Advances in Cryptology — EUROCRYPT'96, Int. Conf. on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, Lecture Notes in Computer Science 1070, pp. 387–398. Springer, Berlin, 1996.
42. Pointcheval, D. , Stern, J. :Security arguments for digital signatures and blind signatures. J. Cryptol., 13, 361–396, 2000.
43. ISO/IEC 14888-3 Information Technology – Security Techniques – Digital Signatures with Appendix – Part 3: Discrete Logarithm Based Mechanisms, International Organization for Standardization, Geneva, Switzerland, 2006.
44. Dent, A.W.: *A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures*. Public Key Infrastructures, Services and Applications, 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10–11, Lecture Notes in Computer Science 6391, pp. 1–16. Springer, Berlin, 2010.
45. Au, M.H., Chen, J., Liu, J.K., Mu, Y., Wong, D.S., Yang, G.: *Malicious KGC Attacks in Certificateless Cryptography.* 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), Singapore, March 20–22, 2007, pp. 302–311. ACM Press, New York, 2007.
46. Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W.: *Certificateless signatures: new schemes and security models.* Comput. J., 55, 457–474, 2011.
47. Cheng, Z.H. and Comley, R. (2005) *Efficient certificateless public key encryption*. Cryptology ePrint Archive, Report 2005/012. http://eprint.iacr.org/2005/012.
48. Libert, B. and Quisquater, J.J. (2006) *On Constructing Certificateless Cryptosystems from Identity Based Encryption*. Public Key Cryptography - PKC 2006, 9th Int. Conf. on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24–26, Lecture Notes in Computer Science 3958, pp.474–490. Springer, Berlin.
49. Mitsunari, S., Sakai, R., Kasahara, M.: *A new traitor tracing*, IEICE Trans. Fundam. Electron., Commun. Comput. Sci., vol. E85-A, no. 2, pp. 481-484, [Online]. Available: http://ci.nii.ac.jp/naid/110003216755/en/, 2002.
50. Sakai, R, Kasahara, M.: *Id based cryptosystems with pairing on elliptic curve*, IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2003/054, [Online]. Available: http://eprint.iacr.org/2003/054, 2003.
51. Zhang, F., Safavi-Naini, R., Susilo, W.: *An efficient signature scheme from bilinear pairings and its applications*, in Proc. Int. Workshop Public Key Cryptogr., F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, pp. 277-290.
52. Scott, M.: *Computing the Tate pairing*, in Proc. Cryptographers' Track RSA Conf., A. Menezes, Ed. Berlin, Germany: Springer, 2005,pp. 293-304.
53. Hu, B. C., Wong, D. S., Zhang, Z., Deng, X.: *Certicateless signature: A new security model and an improved generic construction* Des., Codes Cryptogr., vol. 42, no. 2, pp. 109-126, 2007.
54. Barreto, P. S. L. M. , Libert, B., McCullagh, N., Quisquater, J.-J.: *Efficient and provably-secure identity-based signatures and signcryption from bilinear maps*, in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., B. Roy, Ed. Berlin, Germany: Springer, pp. 515-532, 2005.
55. Du, H., Wen, Q.: *An efficient identity-based short signature scheme from bilinear pairings*, in Proc. Int. Conf. Comput. Intell. Secur. (CIS), pp. 725-729, Dec. 2007.
56. Du, H., Wen, Q.: *Efficient and provably-secure certificateless short signature scheme from bilinear pairings,* Comput. Standards Inter., vol. 31, no. 2, pp. 390-394, 2009.
57. Fan, C.-I., Hsu, R.-H., Ho, P.-H.: *Truly non-repudiation certificateless short signature scheme from bilinear pairings*, J. Inf. Sci. Eng., vol. 27, no. 3, pp. 969-982, 2011.
58. K. Y. Choi, J. H. Park, and D. H. Lee, ``A new provably secure certificateless short signature scheme,'' Comput. Math. Appl., vol. 61, no. 7, pp. 1760-1768, 2011. [Online].
59. Chen, Y. C., Horng, G.: *On the security models for certificateless signature schemes achieving level 3 security*, IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 554, 2011.
60. Sharma, G., Bala, S., Verma, A. K.: *On the security of certificateless signature schemes*,' Int. J. Distrib. Sensor Netw., vol. 9, no. 6, p. 102508, 2013.
61. Chen, Y.-C., Tso, R., Horng, G., Fan, C.-I., Hsu, R.-H.: *Strongly secure certificateless signature: Cryptanalysis and improvement of two schemes*, J. Inf. Sci. Eng., vol. 31, no. 1, pp. 297314, 2015.
62. Chen, L., Cheng, Z.: *Security proof of Sakai-Kasahar's identity-based encryption scheme*. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 442–459. Springer, Heidelberg, 2005.

63. Lu, Y., Li, J.: *Constructing Efficient Certificate-based Encryption with Paring*. Journal of Computers 4(1), January 2009.
64. Chatterjee, S. and Kamath, Ch., A closer look at multiple forking: leveraging (In)dependence for a tighter bound. Algorithmica, 74, 1321–1362 , 2016.
65. Huang, X., Mu, Y., Susilo, W., Wong, D. S. , Wu, W.: *Certificateless signatures: New schemes and security models*, Comput. J., vol. 55, no. 4, pp. 457474, Apr. 2012.
66. Girault, M.: *Self-certified public keys,* in Proc. Workshop Theory Appl. Cryptograph. Techn., D. W. Davies, Ed. Berlin, Germany: Springer, pp. 490-497, 1991.
67. Gennaro, R., Gentry, C., Parno, B.: *Non-interactive verifiable computing: Outsourcing computation to untrusted workers*. In: Rabin, T., (ed.) CRYPTO 2010. LNCS 6223, pp. 465–482, Springer, Heidelberg, 2010.
68. Hohenberger, S., Lysyanskaya, A.: *How To Securely Outsource Cryptographic Computations*. In: Kilian, J. (ed.) TCC 2005. LNCS 3378, pp. 264–282, Springer, Heidelberg, 2005.
69. Girault, M., Lefranc, D.: *Server-Aided Verification*: Theory and Practice, in: B. Roy (Ed.) ASIA CRYPT 2005, Chennai (Madras), India, Lecture Notes in Computer Science, Vol. 3788, pp. 605–623, IACR, 2005.
70. Chevallier-Mames, B., Coron, J.S., McCullagh, N., Naccache, D., Scott, M.: *Secure delegation of elliptic-curve pairing*. In: Gollmann, D., Lanet, J.-L., Iguchi-Cartigny, J., (eds.) CARDIS 2010. LNCS 6035, pp. 24–35, Springer, Heidelberg, 2010.
71. Canard, S.: *Delegating a Pairing Can Be Both Secure and Efficient*, in: I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.) International Conference on Applied Cryptography and Network Security 2014, Lausanne, Switzerland, Lecture Notes in Computer Science, Vol. 8479, pp. 549-565, Springer International Publishing, Switzerland, 2014.
72. Chen, X., Susilo, W., Li, J., Wong, D.S., Ma, J., Tang, S., Tang, Q.: *Efficient algorithms for secure outsourcing of bilinear pairings*. Theor. Comput. Sci. 562, 112–121, 2015.
73. Tian, H. , Zhang, F., Ren, K.: *Secure Bilinear Pairing Outsourcing Made More Efficient and Flexible*, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, Republic of Singapore, pp. 417-426, 2015.
74. Dong, M., Ren, Y., Zhang X.*, Fully Verifiable Algorithm for Secure Outsourcing of Bilinear Pairing in Cloud Computing*, KSII Transactions on Internet and Information Systems, Vol. 11, No. 7, pp. 3648-3663, July, 2017.
75. Dong, M., Ren, Y. L.: *Efficient and secure outsourcing of bilinear pairings with single server*, Science China Information Sciences, vol. 61(3): 039104, 2018.
76. Chen, X., Li, J., Ma, J., Tang, Q., Lou, W.: *New Algorithms for Secure Outsourcing of Modular Exponentiations*, in: S. Foresti, M. Yung, and F. Martinelli (Eds.) European Symposium on Research in Computer Security 2012, Pisa, Italy, Lecture Notes in Computer Science, Vol. 7459, pp. 541–556, Springer, Heidelberg, 2012.
77. Chen, X., Li, J., Ma, J., Tang, Q., Lou, W.: *New algorithms for secure outsourcing of modular exponentiations*, IEEE Transactions on Parallel and Distributed Systems, Vol. 25(9), pp. 2386-2396, September, 2014.
78. Wang, Y., et al.: *Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage*, in: M. Kutyłowski and J. Waidya (Eds.): European Symposium on Research in Computer Security 2014, Wroclaw, Poland, Lecture Notes in Computer Science, Vol. 8712, pp. 326-343, Springer International Publishing, Switzerland, 2014.
79. Ding, Y., et al.: *Secure outsourcing of modular exponentiations under single untrusted programme model*, Journal of Computer and System Sciences, Vol. 90, pp. 1-13, December, 2017.
80. Nguyen, P. Q., Shparlinski, I. E., Stern, J.: *Distribution of Modular Sums and the Security of the Server Aided Exponentiation*, in: K. Y. Lam, I. Shparlinski, H. Wang, C. Xing (Eds.), Cryptography and Computational Number Theory. Progress in Computer Science and Applied Logic, Vol. 20, pp. 331-342, Birkhauser Verlag, Basel, Switzerland, 2001.
81. Dijk, M.V., Clarke, D., Gassend, B., Suh, G. E., Devadas*,* S.: *Speeding up Exponentiation using an Untrusted Computational Resource*, Designs, Codes and Cryptography, Vol. 39, No. 2, pp. 253–273, Springer Science+Business Media, May, 2006.
82. Zhou, K., Ren, J.: *Secure Outsourcing of Scalar Multiplication on Elliptic Curves*, IEEE ICC 2016 Communication and Information Systems Security Symposium, Kuala Lumpur, Malaysia, pp. 1-5, 2016.
83. Fiat, A., *Batch RSA*, Journal of Cryptology, Vol. 10, No. 2, pp. 75–88, March, 1997.
84. Harn, L., *Batch verifying multiple RSA digital signatures*, Electronics Letters, Vol. 34, No. 12, pp. 1219–1220, June, 1998.
85. Yoon, H., Cheon, J. H., Kim, Y.: *Batch verifications with ID-based signatures*, in Proceedings of International Conference on Information Security and Cryptology 2004, Seoul, Korea, pp. 233–248, 2004.
86. Shi, C., Pu, D., Choong, W. C.: *An efficient identity-based signature scheme with batch verifications*, in InfoScale '06 Proceedings of the 1st international conference on Scalable information systems, Hong Kong, pp. 1–6, 2006.
87. Geng, M., Zhang, F.: *Batch verification for certificateless signature schemes*, in Proceedings of the International Conference on Computational Intelligence and Security 2009, Beijing, China, pp. 288–292, 2009.
88. Fan, C.-I., Ho, P.-H., Tseng, Y.-F.: *Strongly Secure Certificateless Signature Scheme Supporting Batch Verification*, Mathematical Problems in Engineering, vol. 2014, Article ID 854135, doi:10.1155/2014/854135, 2014.
89. Hyla, T., *Implementation of a Group Encryption System in a Cloud-based Environment*, IARIA XPS Press, ThinkMindTM Digital Library, ICONS2015, ISBN 978-1-61208-399-5, str. 14-18, 2015.
90. Wawrzyniak, N., Hyla, T., *Managing Depth Information Uncertainty in Inland Mobile Navigation Systems,* M. Kryszkiewicz, C. Cornelis, D. Ciucci, J. Medina-Moreno, H. Motoda, Z.W. Raś (edyt.), Rough Sets and Intelligent Systems Paradigms RSEISP 2014, Lecture Notes in Computer Science, tom 8537, Springer, Cham, str. 343-350, 2014.
91. Zhang, Y., Li, J., Wang, Z., Yao, W.: *A New Efficient Certificate-Based Signature Scheme.* Chinese J. Electron. 24, 776–78, 2015.
92. Todd, P.: *Opentimestamps: Scalable, trust-minimized, distributed timestamping with bitcoin*, https://petertodd.org/2016/opentimestampsannouncement, 2016.

93. Baier, H., Karatsiolis, V.: *Validity models of electronic signatures and their enforcement in practice*, in: F. Martinelli, B. Preneel (Eds.), Public Key Infrastructures, Services and Applications: 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10-11, 2009, Revised Selected Papers, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 255-270, 2010.
94. Hyla, T.; Pejaś, J., *eHealth Integrity Model Based on a Permissioned Blockchain*, Intern. Conf. on Cyber Security & Communication Systems, Dec. 10-12 2018, Melbourne, Australia; Agbinya, J.I., Ed. Melbourne Institute of Technology, pp. 238–247, 2018.

Tomasz Hyla 08.03.2019