A security mechanism based on anonymous signature schemes as a method to reduce the consumption of consumable materials

N F Antonie, C Răcuciu, D Glăvan and F Medeleanu

1Faculty of Military Electronic and Information Systems, Military Technical Academy, Bulevardul George Coșbuc 81-83, București 050141, Bucharest, Romania
2Department of Computer Science, Titu Maiorescu University, 22 Strada Dâmbovnicului Tineretului, București 040441, Bucharest, Romania
3Author to whom any correspondence should be addressed

Abstract. In an effort to reduce bureaucracy and the consumption of consumable materials Romania introduced a few years ago the “Single Integrated Information System” which ensures the collection, consolidation and processing of data from the entire Romanian health insurance system. Like any IT system the “Single Integrated Information System”, may also pose some concerns regarding the confidentiality of personal data and information. In this respect, the present paper explores the possibility of mitigating these concerns by introducing anonymous signature schemes into the Romanian “Single Integrated Information System”. Following their research, the authors concluded that this change can improve security and increase citizens’ confidence in the system, without significantly increasing the implementation costs of the existing system. The authors are also confident that if implementing this method will result in a further reduction of the quantity of consumable materials, like paper and printer ink, used in the healthcare system. This will have a positive impact on the environment and on Earth in general.

1. Introduction
Nowadays the process of automation and the switching from physical to electronic means of data storage encompasses almost all sectors of society. Besides the great advantage of lowering bureaucracy, this transition also leads to reduced usage of consumables, especially paper, mainly used to store and manage data in a physical form. This advantage is even more relevant when it comes to protecting the environment and reducing pollution.

In Romania, a relatively new sector that has made this transition is the healthcare sector which previously relied on handwritten paper documents to maintain an archive, to issue medical documents or prescriptions, etc. By using a large amount of paper and toxic ink, the healthcare insurance system was generating a significant impact on the environment. This sector introduced a few years ago the “Single Integrated Information System” which ensures the collection, consolidation and processing of data from the entire Romanian health insurance system. This system’s main purpose is to help the national health insurance providers to perform their specific tasks of managing the health insurance budget.

Like any IT system the “Single Integrated Information System”, SIIS for short, may also pose some concerns regarding the confidentiality of personal data and information. There are also legal
considerations that need to be taken into account when thinking about the protection of private data and information.

In this respect, the present paper explores the possibility of mitigating these concerns by introducing anonymous signature schemes into the SIIS. These types of schemes can provide the same security services as standard signature schemes, but in addition they can hide the identity of the signer until such time when that identity needs to be proven.

After considering this possibility, the authors believe that adding anonymous signature schemes to the SIIS can improve security and increase citizens' confidence in the system, without significantly increasing the implementation costs to the already existing system.

2. Standard signatures and anonymous signatures
Digital signatures have become a standard element for many suites of cryptographic protocols available worldwide. They are mostly used to detect and/or to prevent the forgery or manipulation of digital messages. The most common examples of digital signatures usage are in software distribution, contract management software, in financial transactions or wherever there is a need to prevent forgery or manipulation.

2.1. Standard signatures
Standard digital signature schemes are mathematical schemes which are used to prove the authenticity of a digital message or document. A valid digital signature gives motives to a recipient to trust that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

RSA cryptosystem (Rivest-Shamir-Adleman) is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem [8].

The users of RSA algorithm create and then publish a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message. In order to verify the origin of a message, RSA can also be used to sign a message.

2.2. Anonymous signatures
The first formalization of anonymous signatures notion was presented by Yang et al. in [1]. It was further explored by Fischlin in [2] and revisited by Saraswat et al. in [3]. This paper tries to make another proposal of the possible practical usage of these signature schemes in the Romanian national health insurance system.

Anonymous signature schemes use standard signature algorithms, but instead of proving the signer identity of the message \(m\) at any moment, the signature \(\sigma\) conceals the identity of the signer up to a specific moment in time. Anonymous signatures are used in many applications where the identity of the signer needs to be protected, e.g. key exchange protocols, electronic auction systems, electronic paper review systems or electronic voting systems like in [4].

There are several anonymous signature schemes, but most important and prevalent schemes are Yang [1], [5] and Saraswat [3]. Yang’s scheme for anonymous signature guarantees the anonymity of the signer when the adversary obtains only the signature but not the message, or when the message contains a random string, called security parameter, which is kept hidden until the verification phase. To keep secret a part of the message may be not appropriate in some applications, but there are also enough applications which require not revealing the complete message.

Saraswat’s scheme for anonymous signature splits the digital signature \(\sigma'\) in two segments of data, \(\sigma' = (\sigma, \tau)\). The first part of digital signature \(\sigma\) is called anonymous signature or simply signature, and the second part of the digital signature \(\tau\) is called verification token or simply token. The generation of signature \(\sigma\) and token \(\tau\) makes use of signature generation algorithm which uses as inputs the signer’s secret key and the message \(m\). Verification phase occurs when anonymous signer
decides to prove publicly the anonymous signed message $m$ belongs to him. At this moment, the signer has to make public $m$, $\sigma$ and $\tau$, and then the validity of the signature can be verified by everybody making use of the public key of the signer. During that time, $\tau$ is hidden, nobody can determine who the signer is, so the anonymity of the signer cannot be broken only from the message $m$ and the signature $\sigma$.

An anonymous signature scheme $\Sigma$ is a triple of algorithms, $\Sigma = (Gen, Sig, Vf)$, where the key generation algorithm $Gen()$ produces a key pair $(pk, sk) \leftarrow Gen()$. The signature generation algorithm $Sig()$ produces a pair of a signature and a verification token $\sigma^* = (\sigma, \tau) \rightarrow Sig(sk, m)$ using the secret key $sk$ and a message $m \in \{0, 1\}^*$. And the deterministic signature verification algorithm $Vf(pk, m, Sig(sk, m))$ produces an output „true” or „false”. In the case that the signature, token or the message was not tampered, the following relation holds:

$$Vf(pk, m, Sig(sk, m)) = true$$

(1)

for $(pk, sk) \leftarrow Gen()$, and for any $m \in \{0, 1\}^*$.

3. The Romanian electronic health insurance system

After an executive ministry order (645/2007) the plan for an electronic health insurance system in Romania was approved. It took some years to reach a functional solution and in 2015 the system became operational and available to the public at large.

The system has the following main components, the “Single Integrated Information System” (SIIS), the “Electronic Prescription” (EP), the “Electronic Health Insurance Card” (EHIC), the health service providers (HSP) and the electronic reporting applications (RA).

The most important component of the electronic health insurance system is the SIIS which has the role of collecting, consolidating and efficient processing of data from the entire national health insurance system. Its main purpose is to help the national health insurance providers to perform their specific tasks of managing the health insurance budget. It has a hierarchical structure distributed on three main levels, national, county level and health service providers – HSP level (figure 1).

![Figure 1: The hierarchical structure of the Single Integrated Information System.](image)

The main functions of SIIS are, managing health insurance funds, managing the insured people, keeping an evidence of health service providers (medical and pharmaceutical), keeping the evidence of contributors and providing quality control for health services. The data from HSP is collected and analyzed locally by the level two of the hierarchical structure (figure 1) at the county level and afterwards is aggregated and maintained at the central level.
In the development of this system seven main objectives have been pursued, the collection and management of the economical and medical information required for an efficient operation of the Health Insurance System, transparency in the usage and management of health insurance budget by the National Health Insurance Provider, keeping a record of the insured people and of the health service providers by creating and administrating the National Registries for the insured people and for the health service providers, the simplification of data reporting by HSP, the standardization in the application of norms and laws at a national level, the highlight and the control of the costs for each insured person and the interfacing of other entities residing outside the system besides the HSPs, in online and/or offline modes.

The benefits of implementing such a system are obvious and intuitive.

3.1. The interfacing of the SIIS

The SIIS provides interfaces for the communication with the exterior through which electronic data transfer is being made. These interfaces are of two main categories:
- Interfaces with the health service providers (medical and pharmaceutical);
- Interfaces with other entities.

The main purpose of the interfaces with the HSPs is to report the provided services so that the health insurance provider can pay the HSPs for those services. On the other hand these interfaces are also used to exchange information related to the released medical prescriptions, sick leaves or other documents that a physician may issue. There are also other types of data exchanged on these interfaces, but that information depends on the specific contract each HSP has with the insurance provider.

The user (whoever it is, HSP, institution, etc.), does the reporting or receives details from the SIIS via the electronic reporting applications – the RAs. The RAs connect to the resources of the SIIS using https/SSL protocol (figure 2).

The SIIS also has the option to validate the prescriptions online or to check in real time if a client is really insured, in order to avoid the possibility that a prescribed service, medical device or pharmaceutical product may not be covered under the insurance.

The interfaces of SIIS with other entities are defined according to some protocols between governmental institutions and are used to obtain or to provide data for the proper operation of the system. Some of these entities may be institutions that keep a population record, antifraud institutions, financial institutions, ministries, treasury departments, city halls, etc. (figure 1).
3.2. Information security in the Single Integrated Information System

To ensure data security for the exchange between the reporting applications and the System (i.e. SIIS), this project implements a public key infrastructure (PKI) designed to use digital certificates generated by well-known and approved certificate authorities.

The PKI infrastructure (figure 3), the technics, the practices and procedures that contributes collectively to the proper implementation and operation of the public key cryptosystems consists of hardware, software, databases, network resources, security procedures and legal obligations. These elements are linked together and are collaborating in order to provide and implement both certification services and other associated infrastructure services, like timestamps.

![SIIS Security architecture](image)

Figure 3: The security architecture of the Single Integrated Information System.

The digital certificates are permanently maintained and verified. The process of verification is done periodically by the certificate authority through the method of certificate revocation. The authority generates and uploads periodically or as needed a “Certificate Revocation List” – CRL, which contains a list with the serial numbers of the certificates that are revoked due to any justified reason (the certificate was compromised, the owned is no longer eligible, etc.). The verification of a digital certificate can also be done via the Online Certificate Status Protocol – OCSP (in accord with RFC2560). Using this method the applications do not have to download and check the long CRL file, but simply send a request to an OSCP service and check only the certificate of interest (figure 3).

The digital certificates will be handled using a dedicated database administered at the county level of the hierarchical structure of the SIIS (figure 1). The reporting applications will use the digital certificate to authenticate and to authorize its online requests to the SIIS by using the https/SSL suite of protocols (figures 2 and 3).

In order to access the resources of the SIIS, all HSPs will require the digital certificates generated by the certificate authorities mentioned earlier. Also those certificates must be registered in the SIIS in order for the HSP’s reporting applications to work. For every operator of a specific HSP user accounts will be created which will give authorization to that operator. This will provide further accountability of the actions taken by each operator.

The access gateway into the SIIS is protected by a hardware firewall which also acts as a SSL Accelerator and load balancer. At the same time this equipment checks the integrity and validity of the digital certificates presented by the reporting applications when a new https/SSL session is initiated.

After integrity and validity verification the SSL accelerator forwards the request by http to the authorization and authentication servers (figure 3 – Auth. Servers). In the http header the SSL accelerator also includes data related to the digital certificate in question, information which will be used by the following servers for a further evaluation of the certificate revocation status by OCSP. The
auth. servers are checking the dedicated database if the digital certificate was registered by an authorized user of the system. If it checks out the server forwards an OCSP request via the “Special Telecommunication Service” - STS, which provides this service, to the public certificate authorities in order to verify the revocation status of the certificate.

The STS offers as a part of the system a component that allows for simultaneous interrogation of all public certificate authorities in Romania. In this way the consequences when a certain certificate authority changes its structure or becomes unavailable are prevented.

If the OCSP request reveals that the digital certificate is not revoked, the auth. servers will check in a buffer database the status of the user’s contract. If that will also check out the server will send a software token to the reporting application. The token is called session-id-hash and will be used by the application to announce that the session has already been approved. This will prevent next requests in the same SSL session to undergo the same process of authorization. This way will accelerate the operation of the application and will not overwhelm the auth. servers with verification requests which can result in slow operation and long waiting times.

3.2.1. Digital Signatures in the Single Integrated Information System. A digital signature represents additional electronic information attached (or logically attached) to an electronic document and has the same significance as the handwritten signature on a paper document. The signer is that person or entity that has the proper device or software to create the signature and is acting either in its own name or representing a third party.

Like the handwritten signature, the digital signature proves the ownership of an electronic document and in addition it offers the recipient the possibility to check if the document suffered alterations or tampering, either intentional or accidental.

For generating a digital signature the signer needs a digital certificate which follows the criteria presented earlier. The certificate links the digital signature to the person or entity that generated that signature.

In order to ensure non-repudiation of the data reported to the SIIS, all reporting files need to be signed with the signer’s digital signature. Electronically signing these files leads to the possibility to fully automate the health insurance system and to simplify the procedures by eliminating paperwork.

The system keeps a record of all reported files, no matter if the digital signature was validated or not. The reasoning behind this behavior is to always have the proof for the revocation of a specific request, if the need to justify a decision made by the system arises.

4. Possible security concerns regarding the confidentiality of personal information in the Single Integrated Information System

Like any IT system, the SIIS is posing some concerns regarding information security. By using mainly proven security protocols and cryptographic means, the system can be considered to have a good security level when it comes to well-known methods of attack. The most obvious vulnerability of the system derives from the fact that the connection between the reporting applications and the SIIS is achieved via the Internet. Even though the employed security protocols provide good protection against attacks like packet sniffing, man-in-the middle, attempts to decrypt the traffic or to impersonate a legitimate user, the system is still vulnerable to attacks such as denial of service. The main reason behind this vulnerability is the fact that the Internet is opened to the whole world and any ill intended person or entity can perform a denial of service attack like the bandwidth attack for example. The attacker cannot penetrate the system or alter/read the traffic, but he or she can still be able to successfully prevent the reporting applications from establishing the SSL sessions with the system by occupying all available bandwidth.

The bandwidth attacks are usually successful attacks against most IT systems that run over the Internet and there are very few ways to protect against them. The most efficient method to mitigate these kinds of attacks is to have the system connected to more than one Internet Service Providers. This method is not an assurance that bandwidth attacks will fail, but doing so will substantially raise the cost of the attack, because the attacker will have to employ significantly more resources to perform the attack.
After analyzing the Single Integrated Information System, the authors of this paper manage to identify another possible vulnerability of this system. The data that is stored in the SIIS contains a lot of personal information regarding its users. This information might be medical information, general health insurance information, identification information and other type of information that may fall under the “Processing of personal data” laws.

When stored inside the system this sensitive data is well protected, but as it was shown in figure 1, the SIIS is connected to other entities through external interfaces. For instance one institution that requires a connection with the system is the “National Statistics Institute”. This institute requires the data to compute detailed statistics regarding many characteristics of the national health system. These statistics may include statistics about the usage of different types of medication, about medical leaves, about types of diseases and their prevalence, etc.. In order to compute these statistics this institution requires the data generated by the reporting applications, like prescriptions, medical reports, etc.. These reports also contain data that may be used to identify the individual for which the reports were generated. And under the aforementioned laws this information is protected and access to it must be limited. Besides that, “The National Statistics Institute” doesn’t need the identification information in order to achieve its objective of generating those statistics.

Due to security best practices any outside system connected to one’s own system should be considered untrusted, as it is implied in [6]. And so, the identification data must be protected, even more so when it leaves the SIIS. But there must also be a way to retrieve the identification data when such need arises.

That is why the authors of this paper are proposing the introduction of anonymous signature schemes in the Single Integrated Information System.

5. The proposed solution

The proposed solution implies the implementation of anonymous signatures in the report generating process of the system.

In order to generate a report or to search a report in the system, the reporting applications use different identifications markers. These markers are the beneficiary’s personal identification number, the serial and number of the report and the physician’s stamp number. After the physician fills up a report, like a medical prescription, with the prescribed treatment and the aforementioned identification markers, he validates it in the system and digitally signs it. After that the system stores it. In order to access the user’s health insurance information the physician is using the user’s Electronic Health Insurance Card, the EHIC, which contains the user’s keys and digital certificate. When the user goes to a pharmacy to get his prescription drugs, the pharmacist either scans the code on the paper prescription (which the doctor prints out after it was validated and stored in the system) or searches the prescription by introducing the same identification markers. The pharmacist also checks the user’s health insurance status by using the data stored on the user’s EHIC.

The possible vulnerability derives from the fact that the electronic prescription is stored with the name and personal identification number of the user alongside the prescribed drugs and diagnosis. The problem is even more noticeable when sending this kind of reports to other systems or institutions like the “National Statistics Institute”.

It is the authors’ opinion that the implementation of anonymous signature schemes is a way to eliminate this vulnerability.

The idea is to have an electronic dossier for each beneficiary of health insurance. This dossier will contain all documents released on that beneficiary’s name and all its medical record. Each medical document released for that beneficiary will be added to this dossier. The dossier won’t have any identification markers; instead it will be anonymously signed with a Saraswat anonymous signature generated using the data stored on the personal EHIC. This will also prove, if necessary, the identity of the owner.

At the reporting applications side (which are responsible for the generation of the documents that will be added to the dossier) all electronic documents generated (e.g. electronic prescriptions) will have the name and the personal identification number fields removed or encrypted (using the user’s public key) by the application. Each document will be released and added to the person’s dossier after
the validation from an insurance point of view. After adding the document to the dossier, the system will remove the previous signature and regenerate it including the latest modifications to the dossier (i.e. the addition of the newly generated documents). As it was expected the signature will be generated using the data from the personal EHIC.

The removal or the encryption of the name and the personal identification number from the generated documents is crucial because the other data on the document will be used to generate statistics and to be sent to other institutions or entities outside the system. And for that reason that data needs to be in the clear and the name and the personal identification number (i.e. the person that belongs to) needs to be protected.

Applying the anonymous signature scheme will result in the generation of the signature and the verification token, which will be used to verify the signature and to prove, if such need arises, the identity of the owner of the dossier. The verification token will be stored on the personal EHIC and it will be updated each time a modification to its dossier will be performed.

The dossiers for each insured person will be stored on the database servers (figure 2). The signature needs to be in the clear and the verification token, which will be used to verify the signature and to prove, if such need arises, the identity of the owner of the dossier. The verification token will be stored on the personal EHIC and it will be updated each time a modification to its dossier will be performed.

The dossiers for each insured person will be stored on the database servers (figure 2). The signature needs to be in the clear and the verification token, which will be used to verify the signature and to prove, if such need arises, the identity of the owner of the dossier. The verification token will be stored on the personal EHIC and it will be updated each time a modification to its dossier will be performed.

By adding anonymous signatures the operation of the system will not change drastically. It will follow the operations presented in chapter 3 with the addition of this new functionality (figure 4).

Figure 4: Anonymous signatures flow chart: (a) Signing flow chart; (b) Verification flow chart.
For example in order to release a prescription, the pharmacist (i.e. the reporting application of the pharmacist) will search the database for that prescription using the serial and number of the prescription. After finding it, the pharmacist app will check the validity of the dossier containing that prescription, by using the token from the user’s personal EHIC. If the validation passes the pharmacist will be able to release the prescribed drugs to the client. The reporting app of the pharmacist will also have to make changes to the client’s dossier in order to mark the prescription as being released. The resigning process will have to be repeated and the new token will replace the old one on the EHIC.

From a mathematical point of view we will denote \( D \in \{0,1\}^* \) to be the user’s dossier. Thus we can write \( D = \sum_{i=1}^{n+1} r_i \), where \( r_i \in \{0,1\}^* \) is the report number \( i \) that was added to the dossier. We also have the key pair \((pk, sk)\) generated by the key generation algorithm, where \( pk \) is the user’s public key and \( sk \) is the secret key. The key pair is stored on the personal EHIC. Applying the anonymous signature will generate \( \sigma^* = (\sigma, \tau) \rightarrow Sig(sk, D) \), where \( \sigma \) is the part of the signature that will be added to the dossier \( D \) and \( \tau \) is the token stored on the EHIC used for verification. Thereby we will get \( D' = \sigma + D = \sigma + \sum_{i=1}^{n+1} r_i \) which will be the signed dossier stored on the system.

In the verification phase the system will have to compute \( Vf(pk,D,\sigma,\tau) \) which is:

\[
Vf(pk, D, Sig(sk, D))
\]  

(2)

If the result of (2) is true for any \( D \in \{0,1\}^* \) and for \((pk, sk)\) the initially generated key pair, we can judge that the dossier belongs to the claimer and has not been modified in the meantime.

A step by step flow chart example of the proposed solution is given in figure 4.

5.1. Security analysis
The anonymous signature scheme proposed by the authors uses a Saraswat scheme which can be combined with and asymmetric encryption scheme. The anonymous signature scheme is used to protect owner identity and to sign a user document dossier. It also provides non-repudiation and integrity protection for the dossier. The encryption scheme is not mandatory but it can provide encrypted identity markers (name and personal identification number) for each individual document in the user dossier thus allowing for more options and furthering security. It is also worth mention that for the anonymous signature verification there is no need for the asymmetric decryption of the documents contained in the user dossier (figure 4 - b).

In the signing phase (figure 4 - a), a dossier parser removes the old signature and adds the new document to the dossier. The new dossier is passed through the anonymous signature processor and a new signature is generated which is added to the dossier by a parser. The signature \( \sigma^* \) it is then split by the signature processor into two parts \((\sigma, \tau)\). \( \sigma \) will be used to sign the dossier and \( \tau \) will be stored on the electronic health insurance card – EHIC and used in the verification process. In the final step the newly signed dossier is then stored on the database servers, which ends the signing process.

In the verification phase (figure 4 - b), the dossier parser will separate the signature \( \sigma \) from the user dossier. The dossier will be passed through the anonymous signing process again and the signature \( \sigma \) will be combined with the stored verification token \( \tau \) from the user’s EHIC in order to form the original full signature \( \sigma^* \). The new signing process will generate a new \( \sigma'' = (\sigma', \tau') \) pair which will be compared to the original \( \sigma^* \). If they are identical (i.e. \( \sigma^* = \sigma'' \)), we can assess that the dossier belongs to the claimer and it was not tempered or modified.

The implementation of anonymous signature schemes into the Single Integrated Information System will also allow the user dossiers to be securely passed to other entities outside of the system. The outside recipients will not be able to uncover the identity of the dossier owner but can still read and process the medical data contained within.

6. Conclusions
Anonymous signature schemes can provide the functionalities of standard signature schemes but will keep the identity of the signer hidden until such time that the signer decides to reveal it.
This paper provides a practical example scenario where an anonymous signature scheme can be implemented and the benefits and improvements it adds to that scenario.

The Single Integrated Information System – SIIS, is the Romanian national health insurance system. It was recently implemented in Romania and provides electronic administration of citizens’ medical data and health insurance information.

As any IT system, the SIIS, can be affected by security vulnerabilities, like, for instance, denial-of-service attacks or the illicit acquiring of user medical information. Proposing a solution to mitigate or eliminate the latter form of attack is this paper’s purpose because that kind of information is also protected by Romanian laws. Thus the authors proposed the implementation of anonymous signature schemes into the SIIS. This solution will allow the system to securely disseminate the medical and pharmaceutical data for statistics or other purposes without linking that data to specific individuals or entities. Beside anonymity and signing it also provides non-repudiation and integrity services. And if the need arises the solution provides a verification mechanism of the identity of the signer.

It is the authors’ opinion that the implementation cost of this solution will be small in comparison with the whole implementation cost of the system. The reasoning behind this assumption is that the system hardware has already been deployed and paid for and the authors’ solution will consist only in software development and implementation.

The implementation of such a security scheme to the health insurance system will also lead to the reduction of consumables like paper and the ink associated with the printing process of that paper. The reasoning behind this statement is that by properly securing electronic data and communications will no longer be required to generate and store hard paper copies of medical documents and records. This will lead to a better environmental footprint and a lower impact on planet Earth.

The authors of this paper also proposed an anonymity-based fair e-lottery system [7]. In that paper the proposal was made to use a hybrid anonymous signature scheme in order to restore people’s faith in the lottery and increase the number of players thus increasing also the earnings for the lottery organizer. The downside of that proposal, compared with the proposal in this paper, was that the implementation cost would be quite large because a national-wide e-lottery system is not yet implemented.

7. References
[1] Yang G, Wong D S, Deng X and Wang H 2005 Anonymous signature schemes PKC 2006 3958 (Berlin, Heidelberg: Springer) pp 347 – 63
[2] Fischlin M Anonymous signatures made easy PKC 2007 4450, ed T Okamoto and X Wang (Berlin, Heidelberg: Springer) pp 31 – 42
[3] Saraswat V and Yun A Anonymous Signatures Revisited ProvSec 2009 5848, ed J Pieprzyk and P Zhang (Berlin, Heidelberg: Springer) pp 140 – 53
[4] Gang C An Electronic Voting Based on Multi-Party Computation ISCSCT ’08 10.1109/ISCSCT.2008.80 (Shanghai: IEEE)
[5] Yang G, Wong D S and Deng X Efficient anonymous roaming and its security analysis ACNS 2005 3531, ed J Ioannidis et al (Berlin, Heidelberg: Springer) pp 334 – 49
[6] Lehtinem R, Russell D and Gangemi G T Sr 2006 Computer security basics 2nd edition, ed T Apandi et al (Sebastopol CA: O’Reilly)
[7] Medeleanu F, Racuciu C and Antonie N F 2017 Anonymous signature schemes applied for a fair e-lottery system The international conference “Education and creativity for a knowledge-based society” 11th edition ISBN 978-3-9503145-5-7 (Vienna: Österreichish Rumanischer Akademischer Verein) pp 32 – 7
[8] Stinson D R 1995 Cryptography: Theory and practice third edition, ed K Osen (Boca Raton: Chapman & Hall/CRC Press)