"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2014
Brasov, 22-24 May 2014

IDENTITY-BASED CHRYPTOGRAPHY: FROM PROPOSALS TO EVERYDAY USE

Mihai Lica PURA, Victor Valeriu PATRICIU

Faculty of Military Electronic and Information Systems, Military Technical Academy, Bucharest, Romania

Abstract: *Since the invention of public key cryptographic algorithms, researchers have also proposed what will later be known as identity based cryptography: the use of identities as public keys. Over the years, different identity based encryption and signature algorithms were developed, making possible what others only predicted some 30 years ago. This paper is a survey over what identity based cryptography is, what advantages it has over classical PKI, what success stories of its use already exists, and on how can one benefit from it, in different civilian and even military scenarios. The purpose of the paper is to set a background for latter research on developing an identity base cryptographic scheme for military use.*

Keywords: *identity based encryption, identity based cryptography, public key cryptography*

1. INTRODUCTION

Identity-based cryptography is a particular case of public key cryptography that in certain conditions offers implementation and utilization advantages, without reducing the security degree. In a conventional public key security scheme, the generation of the two keys (the private key and the public key) starts from an unpredictable randomly chose large number. This leads to two random keys mathematically bounded. Given the random character of the public key, it cannot be given as is to the interested users because it would be very difficult to store and to use. That is why the certificates are use to bind the key to the user and to the issuing certification authority. The necessity of the certificates determines, prior to any communication, the need to search for the qualified certificate of the person someone would like to securely communicate with and to validate this certificate in order to make sure that it belongs to the other party.

But what if the public key can be chosen? This is the determinant characteristic of identity-based cryptography (IBC): the public key is no longer random, but a piece of information regarding the identity of the user ([1]). For example, the whole name, the e-mail address or the home address can all be use as a public key. The chosen information should comply with some rules like: the information should be uniquely bound to a user, the information should be bound in such a way that the users cannot later deny, and, of course, this information should be publicly available.

In this paper we will present the general problematic of identity based cryptography, with an emphasis on its possible applications, especially in military organizations. The rest of the paper is organized as follows. The second section presents the mathematical backgrounds of identity based cryptography.

In the third section the current state of the art of IBC is described, based on the published RFCs. The fourth section presents the costs of using such schemes, demonstrating the superiority of IBC over classical PKI. The fifth section discuses the security of the IBC schemes, taking into consideration the possible attacks and countermeasures. The sixth section presents some possible applications of IBC, and also the military relevance of such schemes. The last section contains some conclusions and future work directions.

2. CHARACTERISTICS OF IDENTITY-BASED CRYPTOGRAPHY

The users of an identity-based cryptography scheme can derive their public key starting from the value of an identity element, which, most of the time, is an ASCII value ([1]). After the public key is chosen, the corresponding private key must be generated. If a user could generate they own private key for the public key they have chosen, then they could generate the private key for any other user of the same security scheme, because the public keys are public. If this would happen, the security would be compromised. That is why the private key can only be generated by a specially designated key generation centre (KGC). The KGC has also a pair of keys: a public and a private one. Starting from the identity of a user (which is also the user's public key) and using its private key, the KGC computes the private key of every user.

From a mathematical point of view, identity-based cryptography is a particular form of pairing based cryptography. The IBC cryptosystem is build based on pairing between elements of a group to a second group. The pairing can be regarded also as a mapping from elements from the first group to elements from the second group. This way, a hard problem in one group is reduced to an easier problem in the other.

An identity-based cryptographic scheme consists out of four algorithms ([2]):

- Setup algorithm is run only one time by the KGC. In this step the private and public key pair of the KGC is created along with the others parameters of the scheme.
- Key generation algorithm is run by the KGC for every user that asks for its private key. The result is the private key of this user and it is transmitted to it.
- Encryption algorithm uses the identity of a node (its public key) to encrypt a message for this node.
- Decryption step is performed at the receiving node: using its private key the node decrypts the encrypted message and obtains the clear message.

Besides these four algorithms, others aspects should be taken into consideration. When a user asks for a private key, the KGC must authenticate the user to be sure that they are not impersonating another one in order to find out they private key. If the authentication succeeds, the private key must be transmitted to the user on a secure channel in order to avoid eavesdropping by a malicious user ([3]). Such secure side channels can be Bluetooth of Infrared channels.

We will now present the advantages of IBC schemes. The first and the most obvious advantage of this security scheme is that the users can securely communicate by encrypting and/or signing messages without the prior need of exchanging public keys through the exchange of certificates ([4]). This way, there is no longer need for a certificate distribution infrastructure (PKI). Another advantage is that if the certificates are no longer needed, the certificate validation step is also missing because there is no need to check if the public key really belongs to the user by checking the signature of the certification authority ([4]). This is an important advantage because the validation of the user's certificate would imply the validation of the whole certificate path.

IBC schemes have also some disadvantages. We will briefly present them in the following paragraphs.

The main disadvantage of the scheme is that the KGC knows (can compute) the private keys of all de users ([5]). If it is compromised, the security of communications can be questioned. This means that the users should trust the KGC that their keys will not be made available to others. This disadvantage can be eliminated in many manners. If all the users are known prior to the start of the communication and no other user will be

joining after, than the KGC is no longer needed. If there is no need for a private key revocation mechanism than the KGC can be destroyed and the private keys of the users will be safe. Another way of solving this problem is to replace a centralized KGC with several KGC in such a way that all are needed to participate in order to generate private keys ([5]).

3. CURRENT STATE OF THE ART IN THE FIELD

In this moment there are over 400 scientific publications on IBC. IBC mathematics is being standardized in IEEE 1363.3 (6). The interest of the Internet Community in this matter and thus the belief of the specialists in identity-based cryptography can be also seen from the RFCs published. The total number of RFCs that handle aspects of identity-based cryptography is four.

The first one dates from August 1995 and proposes "An identity-based Cryptographic Protocol for Authenticated Key Exchange" (RFC1824) ([7]). The authors of this RFC describe "the basic mechanisms and functions of an identity-based system for the secure authenticated exchange of cryptographic keys, the generation of signatures, and the authentic distribution of public key".

The second RFC is named "Identity-based cryptography standard (IBCS) #1: supersingular curve implementations of the BF and BB1 cryptosystems" (RFC5091) ([8]). It was published in December 2007 and was a proposal for an Identity-Based Cryptographic Standard (IBCS#1). It describes the algorithms that implement two kinds of identity-based encryption: Boneh-Franklin (BF) and Boneh-Boyen (BB1).

The third RFC is "Identity-Based Encryption Architecture and Supporting Data Structures" (RFC5408) ([9]) and it was published in January 2009 and describes a security architecture required to implement identity-based encryption and defines the data structures that can be used to implement the technology.

The forth RFC "Using the Boneh-Franklin and Boneh-Boyen Identity-Based Encryption Algorithms with the Cryptographic Message Syntax (CMS)" (RFC5409) ([10]) was published in January 2009. It describes the conventions for using identity-based encryption algorithms (BF and BB1) in the Cryptographic Message Syntax (CMS) to encrypt content encryption keys. It also defines the object identifiers (OIDs) and the convention for encoding a recipient's identity.

By analyzing these RFCs one can see that although identity-based encryption was not shown that much attention, lately it became a relative debated subject. It is interesting to observe that the last three RFCs was published by employees of Voltage Security, a corporation that has implemented and now offers security solutions based on identity-based encryption. These identity-based encryption solutions focus on information encryption for e-mails, files, documents and databases.

Another corporation that invested into identity-based cryptography is Gemalto which developed the first smartcard implementation of identity-based encryption. The implementation is based on the Boneh-Franklin algorithm. From the advantages of this new solution the most important aspects are that the encryption of the confidential messages is more secure, more user-friendly and more manageable by large corporations and telecom operators. Of course, the

smartcard solution was developed in collaboration with Voltage. The advantages that identity-based encryption brings to the smartcards are: more protection for the private keys, strong authentication for the end-users, and simplicity of the encryption process for users and also for telecom operators.

4. COSTS CONSIDERATION

Ferris Research conducted an analysis of IBC at the end of 2008 and observes that the interest for identity-based cryptosystems is growing. Ferris looked on the cost of the security solution proposed by Voltage and concluded that the total cost of ownership of a typical identity-based cryptographic system is one third of a typical public key system. In the same research other interesting results emerged. We will briefly present some of them ([11]).

The infrastructure required by an identity-based encryption system is far simpler than the one needed by a PKI solution. This means that fewer servers are required and the installations are much easier. The operating costs of the Voltage IBC system were one-fifth of those of public key systems, and the users of identity-based encryption systems were more productive that the users of typical cryptographic systems.

These consideration suggest that identity based cryptography is a good candidate for extending its use because not only that it leads to higher profit for the providing companies, but it also determines higher productivity for the users. We believe that this win-win situation will conduct to a high spread f IBC cryptosystems. The only difficulty so far is the lack of regulations on this matter.

5. SECURITY CONSIDERATIONS

Boneh and Franklin gave the first formal definition of security for identity-based encryption ([12, 13]). In an attack defined by them, the malicious user can choose the target identity in an adaptive manner, based on the master public key and any other keys that they had already obtained. These schemes are called “fully secure”. Another notion was introduced by Canetti. It is called selective-identity security because it requires for the malicious user to specify the target identity in advanced, before the master public key is published. This last scheme is considered weaker by the research community ([13]). Based on these definitions of security as countermeasures for different kinds of attacks, the researchers proposed satisfying identity-based encryption schemes.

Another way to formalize notions of security for the cryptographic schemes in general and for the identity-based cryptography in particular is considering the combinations between various security goals and possible attack models ([13, 14]). There are four essential security goals and three important attacks that should be taken into consideration:

- The security goals are: “one-wayness”, “indistinguishability”, semantic security and non-malleability.
- The attack models are: chosen plaintext attack, non-adaptive chosen cipher text attack and adaptive chosen cipher text attack.

From the relations between all these security objectives and attack models raise different security scenarios that were studied by the researchers.

If the algorithms are implemented on cryptographic devices there are a number of specific attacks like the power analysis attack ([15]). This kind of attack consists in two phases: data acquisition phase and data analysis phase. In the first phase the attacker collects data of the power consumption of the devices while it operates. The second phase consists in analyzing the collected data in order to retrieve secret information. Another attack specific when using cryptographic devices is fault attack ([15]). In this attack the malicious user disrupts in some way the normal execution of the device in order to obtain faulty output.

An aspect more closely related to the identity-based cryptography is the efficient implementation of pairings ([16, 17]). This is important both from the point of view of security (pairing being a central part of identity-based related algorithms) and applications (pairing should be efficiently

computable on resource constrained devices). Attackers can adapt the used attacks to pairing ([15]). Research showed that it is possible to obtain important information this way, but has also showed specific countermeasures. Researchers have also highlight some open problems is this field: curve parameterization attacks, special point attacks and high-order power attacks. They were called open problems because they were not sufficiently researched or were not researched at all. So their real destructive potential is unknown.

6. APPLICATIONS OF IBC

6.1 General applications. From a practical and scientific point of view, there are some special applications of identity-based cryptography. The most common one is the identity-based encryption. All of the previous examples were based on it. The possible applications of identity-based encryption would have to be in domains that can profit out of its advantages over public key systems and do not mind or can overcome the disadvantages. The most obvious systems that can be secure with the help of identity-based encryption are the systems in with communication are based on identity. In an e-mail system the messages target a single recipient. The e-mail address is unique and its owner should be the only one that receives the message. So, using it as a public key in an identity-based encryption scheme would be a natural thing to do. The message is sent directly (the sender does not have to look for or validate the certificate of the recipient) the software does the encryption in a user transparent manner. The same discussion can be applied to GSM communication systems. The telephone number of each user is unique in the whole world. So it can be used as a public key in order to reach end-to-end user security. The solution implementation would naturally dress the existing infrastructure. All the communication between devices can be encrypted this way too, using as public key the IP address of the device.

Relatively recently researchers showed that identity-based cryptography can also be used for e-signature in a scheme based on error-correcting codes, thus providing means for identification ([18]).

There is another application that takes identity-based encryption one step further: Fuzzy Identity-based Encryption ([19]). The idea is to replace the identity ASCII value used as public keys with a set of descriptive attributes (of a certain biometric: fingerprint, iris, voice, face, etc). This attributes are used as a public key in order to encrypt messages for the respective user. The main difference of this solution is that the private key is derived from that biometric too. The error-tolerance property of Fuzzy-Identity-based encryption allows for a private key (derived from a measurement of the same biometric) to decrypt that message even if it was encrypted with a slightly different measurement of the biometric.

Another interesting concept is attribute-based encryption ([20]). In this scheme the users' keys and the cipher text are labeled with sets of descriptive attributes. So a particular key can decrypt a particular cipher text only if the attributes of the key match the attributes of the cipher text. This attributes take the form of an access structure that specifies what type of text the key can decrypt. From the attribute-based encryption point of view, identity-based encryption is only a particular case.

6.2 Military relevance. Identity-based cryptography is a new emerging technology

that promises to reduce costs and overhead time and to provide security in a more natural way (for the users). Benefits of IBC - high system usability, highly scalable architecture, low operational impact, fully stateless operation- are all very important in military applications. Military communications can also benefit from it, if used in proper scenarios, where its few important disadvantages can be cancelled.

Here is an enumeration of other possible military applications of identity based cryptosystems.

- Encryption applications using hybrid (symmetric-asymmetric) schemes but without the complex aspects of PKI.
- E-Signature schemes without huge problems of certificates generation, distribution, revocation (no CRLs), validation ([4]).
- Possible mixing cryptography schemes and biometric attributes, in so-called biocryptography ([19]).
- Large applications in MANET's, where dynamic coalition-forming environments are very envisaged in future military networking; in this case, for example, two Trusted Authorities from different coalition forces may wish to (temporarily or permanently) generate a common set of public parameters and a common master secret, and to issue new private keys to all entities under their joint command only for this context ([21]).
- Identity-based cryptography can be used to enable strong security with reduced bandwidth consumption and latency, because the security associations between nodes can be established without the need to exchange any other information ([22]).
- The advantages of identity-based cryptography can be combined with methods of assuring compatibility with current public key infrastructures (like IB-mRSA Identity-Based-Mediated RSA). This way, one can assure interoperability without decreasing security ([23]).
- If the initial identity-based cryptosystem is enriched with a hierarchical approach to KGC problem, than the new cryptosystem will comply with the hierarchical characteristics of the military organization. An advantage is that in this way the key escrow is allowed at different levels ([21]).
- Several key agreement protocols based on identity-based cryptography had been developed and can be successfully used to secure communications.
- ID-based group signature schemes can be relatively easy converted into Group Signature schemes.
- Zero knowledge proof of identity: proving your identity not with a piece of information you have (for example by sending a password to a server), but with prove of your knowledge ([24]).

7. CONCLUSIONS

In this paper we have made a general introduction in identity based cryptography's problematic. We have presented the key differences between it and classical PKI, highlighting its advantages and disadvantages. Based on these considerations, we have given a non exhaustive list with possible applications of IBC.

Researching over these aspects, made possible to better understand in which scenarios the user could really benefit from using an identity based cryptosystem, and not a classical PKI scheme. So based on this survey we will continue our work by researching over the use of IBC schemes in the communication inside the Romanian army, as a backup or even as an alternative to the PKI infrastructure proposed and implemented so far.

REFERENCES

1. Adi Shamir, *Identity-Based Cryptosystems and Signatures Schemes*, Advances in Cryptology: Proceedings of CRYPTO'84, Lecture Notes in Computer Science, 7:47-53, 1984.
2. Shane Balfe, Kent D. Boklan, Zev Klagsbrun, Kenneth G. Paterson, *Key Refreshing in Identity-Based Cryptography and its Applications in MANETS*, Proceedings of the Military

Communications Conference MILCOM '07, 2007.
3. Leonardo B. Oliviera, Diego Aranha, Eduardo Morais, Felipe Daguano, Julio Lopez, Ricardo Dahab, *TinyTate: Identity-Based Encryption for Sensor Networks*, [online]. Available: http://eprint.iacr.org/2007/020.pdf (2007).
4. Sherman S.M. Chow, *Certificateless Encryption*, Identity-Based Cryptography, IOS Press, pp. 207-225, 2009.
5. Antoine Joux, *Introduction to Identity-Based Cryptography*, Identity- Based Cryptography, IOS Press, 2009.
6. IEEE 1363.3 Standard, [online]. Available: http://grouper.ieee.org/groups/1363/IBC/index.html (2006).
7. RFC 1824, [online]. Available: http://ietfreport.isoc.org/idref/rfc1824/ (1995).
8. RFC 5091, [online]. Available: http://www.rfc-editor.org/pipermail/rfc-dist/2007-December/001834.html (2007).
9. RFC 5408, [online]. Available: http://tools.ietf.org/html/rfc5408/ (2009).
10. RFC 5409, [online]. Available: http://www.ietf.org/rfc/rfc5409.txt (2009).
11. Ferris Research, *Report 586 – The total Cost of Ownership for Voltage Identity-Based Encryption Solution*, [online]. Available: http://www.ferris.com/2006/05/30/the-total-cost-of-ownership-for-voltage-identity-based-encryption-solutions/ (2006).
12. Dan Boneh, Matthew K. Franklin, *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology: Proceedings of CRYPTO '01, 2001.
13. Dan Boneh, Xavier Boyen, *Efficient Selective Identity-Based Encryption Without Random Oracles*, Advances in Cryptology (EUROCRYPT 2004), Lecture Notes in Computer Science, vol. 3027, Springer, 2004.
14. David Galindo, Marina Gavrilova, Osvaldo Gervasi, Vipin Kumar, Chih Jeng Tan, David Taniar, Antonio Lagana, Youngsong Mun, Hyunseung Choo, *A Separation Between Selective and Full-Identity Security Notions for Identity-Based Encryption*, Proceedings of ICCSA International Conference on Computer Science and its Applications, Lecture Notes for Computer Science, vol. 3982, Springer, pp. 318-326, 2006.
15. Claire Whelan, Dan Page, Frederik Vercauteren, Michael Scott, William Marnane, *Implementation Attacks and Countermeasures*, Identity-Based Cryptography, IOS Press, pp. 226-243, 2009.
16. Darrel Hankerson, Alfred Menezes, Michael Scott, *Software Implementation of Pairings*, Identity-Based Cryptography, IOS Press, pp. 188-206, 2009.
17. Maurice Keller, Robert Ronan, Andrew Byrne, Colin Murphy, William Marnane, *Hardware Implementation of Pairings*, Identity-Based Cryptography, IOS Press, pp. 207-225, 2009.
18. Pierre-Louis Cayrel, Philippe Gaborit, Marc Girault, *Identity-Based Identification and Signature Schemes using Error Correcting Codes*, Identity-Based Cryptography, IOS Press, pp. 207-225, 2009.
19. Amit Sahai, Brent Waters, *Fuzzy Identity-Based Encryption*, [online]. Available: http://eprint.iacr.org (2004).
20. Amit Sahai, Brent Waters, Steve Lu, *Attribute-Based Encryption*, Identity-Based Cryptography, IOS Press, pp. 156-168, 2009.

21. Shushan Zhao, *Application of Identity-Based Cryptography in Mobile Ad Hoc Networks*, ACM Transactions on Computational Logic, 2007.
22. D. W. Carman, G. H. Cirincione, *Identity-Based Ramdom Key Predistribution for Army MANETS*, [online]. Available: http://www.dtic.mil/dtic/ (2004).
23. Dan Boneh, Xuhua Ding, Gene Tsudik, *Identity-Based Mediated RSA*, Dow Jones & Company, Inc., 2002.
24. Jonathan Katz, Rafail Ostrovsky, Michael O. Rabin, *Identity-Based Zero-Knowledge*, Security in Communication Networks, Lecture Notes for Computer Science, vol. 3352, Springer, pp. 180-192, 2002.