A COMPATIBLE IMPLEMENTATION BETWEEN IDENTITY-BASED AND CERTIFICATELESS ENCRYPTION SCHEMES

Antigoni Polychroniadou[1], Konstantinos Chalkias[2] and George Stepanides[2]
[1]*Royal Holloway, University of London, Egham, Surrey TW20 0EX, U.K.*
[2]*University of Macedonia, Egnatia 156, 54006, Thessaloniki, Greece*

Keywords: Compatibility, Identity-based Encryption, Certificateless Encryption, Protocol Classification, Efficiency Comparison, Compatible Implementation.

Abstract: In this paper we put into practice the concept of compatibility and we present a classification of two IBE-related schemes, the Identity-Based Encryption (IBE) and the Certificate-Less Encryption (CLE). An innovative implementation of a compatible IBE and CLE system was developed in order to support different encryptions on-the-fly based on the user's needs at a specific moment. Motivated from the fact that there are numerous theoretically efficient IBE-related schemes in the literature overshadowing the benefits of traditional public key encryption (PKI) schemes, they did not, in any important way implemented into practice, as the widely-used PKI. The question is why this is the case since IBE solves a number of problems associated with PKI. Therefore, the controversial issue concerning the widespread use of IBE schemes into practice and the issue of compatibility between IBE and CLE are discussed in this paper. These real problems hinder the wide use of IBE. However, it cannot be denied that IBE, which can be extended to support a plethora of encryption models, gains widespread adoption day by day as it solves problems within conventional public key schemes and it results in a simplified key management, making it much more lightweight to deploy. Based on the fact that a number of different encryption schemes stemmed from IBE, an implementation of an IBE-related compatible system is important. Our approach categorizes known concrete constructions from two IBE-related types into classes and analyzes similarities concerning public settings, used keys, protocol structures and provided model of provable security.

1 INTRODUCTION

Traditional RSA (or similar) encryption is still considered the first option for e-commerce transactions and key exchange. This is based on the fact that current security infrastructure in the web is mainly based on RSA digital certificates. On the other hand, elliptic curve cryptography (ECC) is considered to offer the same level of security with RSA but with smaller key-sizes. Unfortunately, although ECC has been proposed years ago as an RSA alternative, currently, ECC is mostly used in constrained devices and thus actual web transactions are mostly based on RSA encryption and signatures. Moreover, there is no doubt that for a new product or an idea to be applied in the real world, compatibility with already established approaches plays the most important role, as history has shown in the case of passing from DES to 3DES (before moving to AES) for backward compatibility reasons. Therefore, we issue the compatibility between schemes stemmed from ECC such as the flexible as well as versatile IBE schemes.

To circumvent some of the problems of conventional asymmetric encryption, including the complexity and the maintenance cost arised from the use of digital certificates, the concept of IBE was proposed by Shamir (Shamir, 1985) in 1984. However, it took almost twenty years for an IBE scheme to be proposed by Boneh and Franklin (Boneh and Franklin, 2003) in 2001. Since then, a couple of breakthroughs have been achieved leading to new asymmetric encryption schemes. IBE can be extended to support a plethora of encryption models and applications including Hirerachical IBE (HIBE), Certificateless Encryption (CLE) (Al-riyami and Paterson, 2003), Certificate-Based Encryption (CBE), Fuzzy IBE (FIBE), Timed-Release Encryption (TRE) to name just a few. Hence, there are numerous theoretically efficient IBE-related models in the literature which offer different advantages and properties. On the other hand, the commercial use of IBE is not 'growing' as fast as someone would expect and we

Polychroniadou A., Chalkias K. and Stephanides G..
A COMPATIBLE IMPLEMENTATION BETWEEN IDENTITY-BASED AND CERTIFICATELESS ENCRYPTION SCHEMES.
DOI: 10.5220/0003975302250230
In *Proceedings of the 8th International Conference on Web Information Systems and Technologies* (WEBIST-2012), pages 225-230
ISBN: 978-989-8565-08-2

suppose that both the compatibility issue and the lack of a complete ECC parameter standardization (including pairing-friendly curves) are the main reasons hindering the wide use of IBE. The latter is due to the fact that the most efficient and practical IBE schemes are currently based on bilinear pairings over elliptic curve groups for which pairing-friendly elliptic curve groups have been proposed. The first companies have already started to exploit IBE commercially. Some of them are Voltage, Trend Micro, Mitsubishi and Noretech Microsoft etc. All in all, due to the challenges that appear in asymmetric encryption, the issue of moving from one model to another requires much more attention in order for new schemes, with various interesting properties, to be widely adopted.

From the aforementioned encryption models, CLE owns some interesting properties making it a strong candidate to be the ‘connector’ between traditional public key encryption and IBE. In fact, a CLE scheme could be characterized as a mixed scheme which shares properties from both encryption models, conventional and IBE. As far as CLE and IBE are concerned, after a thorough research we found that there are currently at least 35 different concrete IBE schemes and 30 concrete CLE schemes in the literature. There are also generic CLE schemes that can be derived from IBE. Moreover, some of the existing protocols are independent (Sun et al., 2007), (Cocks, 2001), but some of them share certain features which allow us to put the concept of compatibility into practice. So in the following sections, we propose specific protocols exploring IBE and CLE concepts.

We focus on practicality issues rather than technical and security details. We identified eight, competitive or not, classes of IBE and eight classes of CLE. A plethora of CLE frameworks are found to be compatible with IBE frameworks. As a result, the concept of compatibility is easier to be deployed. On the other hand, there are classes from one model (e.g. (Baek et al., 2005) in CLE) for which a related compatible class does not seem to exist. Moreover, we recommend the best combination of IBE and CLE for the concept of compatibility and we offer an implementation. However, we emphasize on the fact that a key relation and a similar construction between IBE and CLE schemes does not automatically implies a fully secure compatible system between them and in some cases further security proofs are required in order to implement a parallel encryption system with both IBE and CLE support. Under some circumstances, the coexistence of IBE and CLE gives an adversary more capabilities than in a single-mode CLE.

1.1 IBE and CLE Concepts

The concept of an IBE scheme simplifies the key management, because the receiver’s unique identity, such as an email address or a phone number, is used to easily construct the receiver’s public key without contacting the KGC or the receiver. When a sender sends an encrypted message he/she merely derives receiver’s public key $PK1$ directly from receiver’s identity ID (usually $PK1 = H(ID)$), where H is a Map-to-Point hash function. Thus, the automatic generation of public keys by everyone is considered to be the main advantage of IBE. According to this, there is no need for public key queries, explicit certificates and transition of public keys. However, the receiver’s private key d_{ID} is not generated by the receiver as in conventional cryptography, but it is securely provided by the KGC. The KGC owns a master secret key and using an algorithm that takes as input a user’s ID it outputs a private keys d_{ID} for each user. As for IBE implementations, current IBE approaches either rely on bilinear pairings over elliptic curve groups or on the quadratic residue assumption and recently on Lattices’ problems.

Regarding the disadvantages of IBE, they are arisen by the fact that KGCs can generate the private keys for each of their users. As a result, a KGC is capable of decrypting any messages. Accordingly, the private key escrow becomes an inherent problem in IBE. Another important problem is that IBE private keys must be sent to the users over secure channels, which is solved in practice using RSA-based SSL.

In order to overcome the drawback of IBE, the essence of CLE was proposed by Al-Riyami and Paterson (Al-riyami and Paterson, 2003) in 2003. CLE retains the desirable properties of IBE without the inherent key escrow problem. In such a scheme the receiver independently generates his public key $PK2$ and secret key x as in the case of conventional Public Key Infrastracrure (PKI). Similarly to IBE, the KGC computes the partial private key d_{ID} using its master secret key and the receiver’s ID. Contrary to IBE’s private key, receiver’s private key is a combination of his/her secret key x and d_{ID}. As a result, the key escrow problem is solved since messages can only be decrypted by the receiver (both private key parts are required). Under some circumstances, the full private key is just the pair (x, d_{ID}) while, in some other cases, a more complex combination is used. When it comes to the sender, he/she has to generate $PK1$ from receiver’s ID and ask for receiver’s public key $PK2$ in order to encrypt a message. Bearing in mind the communication between the KGC and the user during the key generation, some classes of CLE extend IBE schemes. Current CLE schemes that evolved from IBE depend on Bilinear Pairings. However some others do not derive from an existing IBE scheme, such as (Baek et al., 2005) and (Lai et al., 2009).

2 COMPATIBILITY ISSUES

This article focuses on CLE schemes derived from an IBE variant, because our aim is to combine both technologies. What appears to be interesting when considering the above schemes is how we can connect or modify the keys in order to make compatible implementations using a single KGC. In both schemes the KGC provides the receiver with the d_{ID} which is used as the receiver's private key in IBE and as a part of the receiver's private key in CLE. Secondly, the public key $PK1 = H(ID)$ is computed in the same way in both schemes. Hence, the partial private and the public key of IBE schemes are generated in the same way as in CLE. Generally speaking, all pairing-based IBE-related schemes (CLE, TRE, HIBE) indirectly include the 'pure' IBE scheme. This fact can be used in order to achieve compatibility.

In our approach, one scenario we need to solve is the case when a user, who uses CLE, receives a message from a sender who used IBE for encryption. Is it possible for a CLE-capable receiver to decrypt a message derived from an IBE scheme? This can be achieved by decrypting the message with the compatible IBE part of the CLE, using the partial private key. Furthermore, in case where CLE and IBE schemes are compatible, the user is provided with the opportunity to use different IBE-related schemes in parallel. More specifically, the user can choose which encryption to use depending on the features that he expects from a scheme (need more privacy against KGC or not?). Emphasizing on the fact that the concept of compatibility can be implemented in a company, it can be 'somehow' compared to a HIBE scheme. More specifically, using only one KGC with a compatible system we offer two categories per user. The first category enables the KGC to check/decrypt a user's message decrypted using IBE encryption. The second category achieves user's privacy due to the fact that the message can be encrypted using CLE encryption. Therefore, in a company if a user needs more privacy he/she can encrypt a message using CLE. On the other hand, in some circumstances where the administration (KGC) needs to decrypt messages from specific users, it allows them to encrypt using IBE encryption. Contrary to a HIBE scheme, the proposed compatible systems do not offer hierarchy and the user can select which of the above aforementioned categories needs to implement any time. Contrary to our approach, in a Hierarchical HIBE scheme the top level user (e.g. KGC) can decrypt all the messages from all the users due to the hierarchy. Moreover, such a scheme demands more complex keys, contrary to our compatible systems. We are currently dealing with the concept of a scalable compatible system without significant additional cost. In order to achieve compatibility between IBE and CLE, we studied the key generation algorithms of the majority of IBE and CLE concrete schemes. Needless to say that we had to pay attention to the mathematical problems on which the security of every scheme depends on. Bearing in mind that if two schemes have closely similar keys, but the problems that they depend on are different, the transfer of a key from one scheme to another may lead to the disclosure of the key. Furthermore, we considered the communication between the KGC and the user during the key generation phase. The only compatible schemes that we underline are based on the concept that the user's public key is independent of the partial private key generation (e.g. BF and AP classes etc.). The CLE schemes that are not compatible with any IBE class are those in which the user's public key can only be generated after receiving the partial private key or after a protocol interaction with the KGC (e.g. BSS (Baek et al., 2005) class and (Lai and Kou, 2007)). Regarding the security models, as CLE implies IBE, probably the security proofs are included in the security model of CLE. Therefore, almost all security models for CLE protect against a disclosure of the IBE-part of the CLE private key. However, in some cases further security proofs are required to implement a parallel encryption system for both IBE and CLE support[1] as the co-existence of IBE and CLE gives an adversary more capabilities than in a single-mode CLE. For example, the partial private key cannot be divulged if the CLE attacker has replaced the public key.

2.1 Classification

Taking into consideration the similarities, as well as the differences of numerous IBE and CLE proposals, we tried to organize them into classes. As a result, eight IBE classes have been modeled which are the BF(Boneh and Franklin, 2003), the COCKS(Cocks, 2001), the SK(Kasahara, 2003), the KW(Katz and Wang, 2003), the Waters(Waters, 2005), the Gentry(Gentry, 2006), the BB1(Boneh and Boyen, 2004)(a) and the BB2(Boneh and Boyen, 2004)(b) classes. Note that the classes can be

[1] In fact, changes in the security proofs of CLE are required as they typically extend IBE, but not vice versa.

generalized into less classes since Gentry, SK and BB2 classes belong to the Exponent-inversion family. Moreover, Waters and BB1 classes derive from the commutative-blinding framework and KW class stems from a full-domain-hash IBE. We pointed out which of them are useful or not. The representative scheme of each class is the first proposed scheme in the literature. Therefore, the names of the classes derived from the corresponding authors' names of the initial paper of each approach which does not automatically mean that these schemes are or are not the best performed paradigms in their class. This classification depends on the structure of the keys. Furthermore, we had to pay attention to the mathematical problems (security assumptions) on which the security of every scheme depends on. In addition, in an attempt to standardize the closely related CLE with IBE proposals we classify the CLE schemes into eight classes which are the AP03(Al-riyami and Paterson, 2003), the AP05(Al-riyami and Paterson, 2005), the LQ(Libert and jacques Quisquater, 2006), the CCLC(Cheng et al., 2007)(a), the BSS(Baek et al., 2005), the PCHL(Park et al., 2007), the DLP(Dent et al., 2008) and the LDLK(Lai et al., 2009) classes.

In Tables 1 and 2, we can see the representative classes of schemes belonged to BF or AP05 classes where *Msk* is the master secret key of KGC, *Pub* is the user's public key, *Priv* is the user's private key and *Gener* is a specified generator. Our implementation is a compact compatible system based on these two classes. We will see later why we chose these two compatible classes.

Table 1: CLE Classes.

AP05(Al-riyami and Paterson, 2005)	
KEYS	
Msk:	$s \overset{R}{\longleftarrow} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$
Secret:	$x \in \mathbb{Z}_q$
Pub:	$P_A = xP \in \mathbb{G}_1, ID \in \{0,1\}^*$
Partial:	$d_{ID} = sQ_{ID} \in \mathbb{G}_1$ *where* $Q_{ID} = H_1(ID) \in \mathbb{G}_1$
Priv:	$s_{ID} = (d_{ID}, x) \in \mathbb{G}_1 \times \mathbb{Z}_q$
Gener:	$P \in \mathbb{G}_1$

Table 2: IBE Classes.

BF(Boneh and Franklin, 2003)	
KEYS	
Msk:	$s \overset{R}{\longleftarrow} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$
Pub:	$ID \in \{0,1\}^*$
Priv:	$d_{ID} = sQ_{ID} \in \mathbb{G}_1$ $Q_{ID} = H_1(ID) \in \mathbb{G}_1$
Gener:	$P \in \mathbb{G}_1$

The used hash function is modeled as: $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$.

2.2 Compatibility

Considering the structure of the keys derived from CLE classes we set the IBE compatible classes. Table 3 shows the CLE classes corresponding to their IBE compatible class. By taking into consideration the competitive and compatible useful classes, the compatibility can be put into practice. If the Random Oracle Model and of course the Weak-Types of Adversarial Security Models are considered practically secure, according to our performance analysis, the SK (Kasahara, 2003) class has the best efficiency performance, followed by BB2 and Gentry classes which are proven secure in the standard model. In CLE, among the useful classes, the best performed class is the LQ(Libert and jacques Quisquater, 2006) class, followed by AP05 and CCLC classes. The LQ(Libert and jacques Quisquater, 2006) class is compatible with SK-IBE class. Depending on their keys and on the security assumptions they lead to a mixed CLE-IBE system. Both classes support the simplest implementations. A drawback of these classes is that the security depends on a strongest q-BDHI assumption compared to other classes. We highlight though that our measurements took under consideration the case of a single KGC, otherwise some other pairing-based classes could be benefited from the bilinearity property when multiple KGCs are to be used. We are currently investigate the case of multiple KGCs and its effect on the compatibility and on the performance of IBE and CLE schemes. In a multiple KGCs approach, we need to split the master secret key into additive or polynomial shares to avoid single points of failure. On the other hand, a less time efficient commutative blinding BB1 scheme is extremely flexible as well as versatile to implement extensions of IBE followed by BF schemes. Thus, another mixed CLE-IBE system could be derived from BB1 and CCLC classes sacrificing some of its efficiency. The combi-

Table 3: Compatible Classes.

CLE Classes	***compatible with***	**IBE Classes**
AP03 and AP05	$\longrightarrow$	BF
LQ	$\longrightarrow$	SK
DLP	$\longrightarrow$	Waters
PCHL	$\longrightarrow$	Gentry
CCLC	$\longrightarrow$	BB1
BSS		-
LDLK		-
-		BB2
-		COCKS
-		KW

nation of BF and AP classes are quiet efficient but a practical drawback in terms of security is their high dependency on random hash functions. Therefore, based on the fact that the majority of companies that use IBE, such as Voltage, implement the BF scheme, we constructed compatible systems companying BF and AP05 compatible classes. Using the IBECrypto library(Anastasios Kihidis, 2010) which is an open source implementation of BF scheme we can successfully implement a compatible scheme in which users as well as administrators choose whether they want to use IBE or CLE on-the-fly.

3 CONCLUSIONS

This article raises the importance of compatibility between IBE-related schemes in order to exploit all aspects from each IBE-related scheme (CLE, Time-released, hierarchical IBE, etc) since IBE can offer a lot of extensions. More specifically, we consider compatibility as the ability to use different asymmetric encryption constructions in parallel. If someone uses an IBE scheme and someone else uses another scheme (e.g. CLE) derived from this specific IBE scheme, under certain circumstances, they can communicate to each other. Our focus is on CLE due to the fact that it is theoretically the most general scheme, in which the structure of its keys shares properties from both IBE and conventional PKI. For this reason we conducted an extended and analytical survey of the majority, if not all, existing concrete IBE as well as CLE schemes. We constructed eight, compatible or not, classes of IBE and CLE in order to achieve compatibility. Then we identified the compatible classes, from which we can benefit from utilizing IBE and CLE in a whole compatible system with a single KGC. The categorization in classes allowed us to specify a compatible system for example in a company where the users are provided with the opportunity to select between CLE(privacy) and IBE(no privacy) encryptions depending on the needs of the company. With the concept of compatibility and its implementation we can achieve some intresting properties. We can use only one KGC for both encryptions, increase the security of an IBE scheme at any time by using a secret key as in CLE. In addition, we can decrypt an IBE message using the IBE part of CLE, bearing in mind that it is impossible to achieve this if the user's public key in CLE is certified in the partial private key. The concept of a compatible system firstly reduces the problems of PKI avoiding the use of digital certificates, and secondly it offers the best aspects of both CLE and IBE schemes. Even better, although it comes in contrast with the characterization *certificateless*, the user's public key $PK2$ could in some schemes be signed, for backward compatibility with traditional PKI. Under this assumption, a CLE user would be able to encrypt in IBE, CLE and traditional PKI settings in an ideal system. In addition, considering other IBE-related encryptions such as the TRE, the Role-based Access, the HIBE, the Fuzzy IBE and the Attribute-based Encryption, we can develop a 'global' compatible system supported numerous IBE-related concepts in which a user will be provided with the opportunity to choose between the desired IBE-related encryption on-the-fly.

REFERENCES

Al-riyami, S. S. and Paterson, K. G. (2003). Certificateless public key cryptography. In *Asiacrypt2003*, pages 452–473. Springer-Verlag.

Al-riyami, S. S. and Paterson, K. G. (2005). CBE from CL-PKE: A generic construction and efficient schemes. In *Public Key Cryptography - PKC 2005, Lecture Notes in Comput. Sci*, pages 398–415. Springer.

Anastasios Kihidis, Chalkias Konstantinos, S. G. (2010). Practical implementation of identity based encryption for secure e-mail communication. In *In 14th Panhellenic Conferenceon Informatics*, PCI 2010. IEEE CS.

Baek, J., Safavi-Naini, R., and Susilo, W. (2005). Certificateless public key encryption without pairing. In *ISC*, pages 134–148.

Boneh, D. and Boyen, X. (2004). Efficient selective-id secure identity based encryption without random oracles. In *Proceedings of Eurocrypt 2004, volume 3027 of LNCS*, pages 223–238. Springer-Verlag.

Boneh, D. and Franklin, M. (2003). Identity-based encryption from the weil pairing. *SIAM J. of Computing*, 32:586–615.

Cheng, Z., Chen, L., Ling, L., and Comley, R. (2007). General and efficient certificateless public key encryption constructions. In *Pairing*, pages 83–107.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *Proceedings of the 8th IMA Int. Conf.*, pages 360–363. Springer-Verlag.

Dent, A. W., Libert, B., and Paterson, K. G. (2008). Certificateless encryption schemes strongly secure in the standard model. In *11th international conference on Public key cryptography*, PKC'08, pages 344–359. Springer-Verlag.

Gentry, C. (2006). Practical identity-based encryption without random oracles. In *EUROCRYPT*, pages 445–464.

Kasahara, R. S. M. (2003). ID based cryptosystems with pairing on elliptic curve. *Cryptology ePrint Archive*.

Katz, J. and Wang, N. (2003). Efficiency improvements for signature schemes with tight security reductions. In *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, pages 155–164.

Lai, J., Deng, R. H., Liu, S., and Kou, W. (2009). RSA-Based certificateless public key encryption. In *Proceedings of the 5th International Conference on Information Security Practice and Experience*, ISPEC '09, pages 24–34. Springer-Verlag.

Lai, J. and Kou, W. (2007). Self-generated-certificate public key encryption without pairing. In *10th international conference on Practice and theory in public-key cryptography*, PKC'07, pages 476–489. Springer-Verlag.

Libert, B. and jacques Quisquater, J. (2006). On constructing certificateless cryptosystems from identity based encryption. In *In PKC 2006*, pages 474–490. Springer-Verlag.

Park, J. H., Choi, K. Y., Hwang, J. Y., and Lee, D. H. (2007). Certificateless public key encryption in the selective-ID security model (without random oracles). In *Pairing*, pages 60–82.

Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 47–53. Springer-Verlag New York, Inc.

Sun, Y., Zhang, F., and Baek, J. (2007). Strongly secure certificateless public key encryption without pairing. In *CANS*, pages 194–208.

Waters, B. (2005). Efficient identity-based encryption without random oracles. In *EUROCRYPT 2005*, pages 114–127. Springer-Verlag.