The Concept of Compatibility 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.

Abstract: This paper introduces the concept of compatibility and presents an extended classification of two IBE-related schemes, the Identity-Based Encryption (IBE) and the Certificate-Less Encryption (CLE) in order to implement compatible systems. 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 enables a number of different encryptions on-the-fly based on the user's needs at a specific moment. 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. Therefore, we consider compatibility issues between CLE and IBE and we conclude that a significant number of them are closely related. Therefore, the concept of compatibility can be put into practice.

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 the 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 and applications. Undoubtedly, IBE gains widespread adoption day by day as it solves problems within conventional public key schemes based on the fact that it results in simplified key management, making it much more lightweight to deploy. 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 suppose that both the compatibility issue and the lack of a complete ECC parameter standardization (includ-

Polychroniadou A., Chalkias K. and Stephanides G..
The Concept of Compatibility between Identity-based and Certificateless Encryption Schemes.
DOI: 10.5220/0004076704030407
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 403-407
ISBN: 978-989-8565-24-2

ing 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 spread.

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.

1.1 Classes of IBE

Taking into consideration the similarities, as well as the differences of numerous IBE proposals, we tried to organize them into classes. As a result, eight IBE classes have been modeled in Table 1. Note that the classes can be generalize into less classes since Gentry, Sakai-Kashara and BB2 classes belong to the Exponent-inversion family. Moreover, Waters and BB1 classes both 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 for 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 Table 1, *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. The differences of the keys are obvious.

1.2 Classes of CLE

In an attempt to standardize the closely related CLE with IBE proposals we classify the CLE schemes into eight classes. As in the IBE classification, this classification depends on the structure of the keys and the security assumptions on which every scheme depends. The eight different classes are depicted in Table 2. We emphasize on which of them are useful or not for comparison and compatibility testing.

1.3 Compatibility

Considering the structure of the keys derived from CLE classes we set the 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 ROM 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 combination of BF and AP classes

Table 1: IBE Classes.

IBE CLASSES			
	BF (Boneh and Franklin, 2003)	COCKS (Cocks, 2001)	SK (Kasahara, 2003)
KEYS			
Msk:	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$	$q, p : q \equiv p \equiv 3(mod4)$	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$
Pub:	$ID \in \{0,1\}^*$	$ID \in \{0,1\}^*$	$ID \in \{0,1\}^*$
Priv:	$d_{ID} = sQ_{ID} \in \mathbb{G}_1$ *where* $Q_{ID} = H_1(ID) \in \mathbb{G}_1$ *where*	$r = \alpha^{\frac{n+5-(p+q)}{8}} modn \in \mathbb{Z}_n^*$ *where* $\alpha = H_2(H_2(H_2...(ID))) \in \mathbb{Z}_n^*$ such that $\left(\frac{a}{n}\right) = 1, n = pq$ $a = \pm r^2 modn$ depending on whether $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = \pm 1$	$d_{ID} = \frac{1}{s+H_3(ID)} Q \in \hat{\mathbb{G}}_1$
Gener:	$P \in \mathbb{G}_1$		$P \in \mathbb{G}_1$,$Q \in \hat{\mathbb{G}}_1$
	KW (Katz and Wang, 2003)	Waters (Waters, 2005)	Gentry (Gentry, 2006)
KEYS			
Msk:	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$	$s \in \xleftarrow{R} \mathbb{Z}_q, sP_2 \in \mathbb{G}_1$	$s \in \xleftarrow{R} \mathbb{Z}_q, P_{pub} = sP \in \mathbb{G}_1$
Pub:	$ID \in \{0,1\}^*$	$ID \in \{0,1\}^n$	$ID \in \mathbb{Z}_q$
Priv:	$d_{ID} = (sQ_{ID}, b_{ID})$ *where* $b_{ID} \in \{0,1\}$, $Q_{ID} = (H_1(ID, b_{ID})) \in \mathbb{G}_1$	$d_{ID} = (sP_2 \cdot r(u' \prod_{i \in \nu} u_i), rP)$ *where* $\nu \subseteq \{1,..n\}$ where $ID_i = 1$ $\vec{U} = (u_i), u_i \in \xleftarrow{R} \mathbb{G}_1$, $r \in \mathbb{Z}_q, u' \in \mathbb{G}_1$	$d_{ID} = (r_i, h_{ID,i}) : i \in \{1,2,3\}$ *where* $h_{ID} = \frac{1}{s-ID}(h_i P^{-r_i}) \in \mathbb{G}_1^3$, $r_i \in \mathbb{Z}_q$
Gener:	$P \in \mathbb{G}_1$	$P \in \mathbb{G}_1$	$P, h1, h2, h3 \in \mathbb{G}_1$

	BB1 (Boneh and Boyen, 2004)(a)	BB2 (Boneh and Boyen, 2004)(b)
KEYS		
Msk:	$(Q, \alpha, \beta, \gamma) \in \hat{\mathbb{G}}_1 \times \in \mathbb{Z}_q^3$	$s_1, s_2 \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub1} = s_1 P$, $P_{pub2} = s_2 P \in \mathbb{G}_1$
Pub:	$ID \in \{0,1\}^*$	$ID \in \mathbb{Z}_q$
Priv:	$d_{ID} = (rQ,$ $(\alpha\beta + (\alpha H_6(ID) + \gamma)r)Q) \in \hat{\mathbb{G}}_1^2$ *where* $r \in \mathbb{Z}_q$,	$d_{ID} = (r, \frac{1}{ID+s_1+rs_2} Q) \in$ $\mathbb{Z}_q \times \mathbb{G}_1$ *where* $r \in \mathbb{Z}_q$
Gener:	$Q \in \hat{\mathbb{G}}_1$	$P \in \mathbb{G}_1, Q \in \hat{\mathbb{G}}_1$

• The schemes use bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2)$ of prime order q for which there exists a bilinear map $\hat{e} : \mathbb{G}_1 \times \hat{\mathbb{G}}_1 \rightarrow \mathbb{G}_2$ satisfying the following properties:
1. Bilinearity: $\forall P, Q \in \mathbb{G}_1, \forall a, b \in \mathbb{Z}$, we have $\hat{e} = (aP, bQ) = \hat{e}(P,Q)^{ab}$.
2. Non-degeneracy: $\hat{e}(P,Q) \neq 1 \in \mathbb{G}_2$.
3. Computability: $\forall P, Q \in \mathbb{G}_1$, the pairing $\hat{e} = (P,Q)$ can be efficiently computed.
• In addition, type-1 ($\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$) pairings are symmetric, type-2 ($\hat{e} : \mathbb{G}_1 \times \hat{\mathbb{G}}_1 \rightarrow \mathbb{G}_2$) asymmetric pairings include a one-way mapping from $\hat{\mathbb{G}}_1$ to $\mathbb{G}_1$ and also there are the type-3 asymmetric pairings in which the groups are not mapped efficiently to each other.
•The used hash functions are modeled as: $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1^*$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_n^*$, $H_3 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_4 : \{0,1\}^* \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_p^*$ and $H_5 : \{0,1\}^* \times \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^{odd}$
•We use additive notation for ECC protocols to denote a scalar multiplication
• The RO Model is a security model in which all parties get black-box access to a random function H. The ROM implies simplicity and practicality in a scheme. However, a security proof in ROM is only a heuristic indication of the scheme's security. On the other hand, a model that do not use idealized oracles is the Standard Model in which the security is proven using only standard complexity assumptions. Thus, a security proof of a scheme in the standard model is preferred rather than a proof in the ROM.

Table 2: CLE Classes.

CLE CLASSES			
	AP03 (Al-riyami and Paterson, 2003)	AP05 (Al-riyami and Paterson, 2005)	LQ (Libert and jacques Quisquater, 2006)
KEYS			
Msk:	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$	$s \in \xleftarrow{R} \mathbb{Z}_q$, $P_{pub} = sP \in \mathbb{G}_1$
Secret:	$x \in \mathbb{Z}_q$	$x \in \mathbb{Z}_q$	$x \in \mathbb{Z}_q$
Pub:	$P_A = (X,Y)$,$ID \in \{0,1\}^*$ *where* $X = xP \in \mathbb{G}_1, Y = xP_{pub} \in \mathbb{G}_1$	$P_A = xP \in \mathbb{G}_1$,$ID \in \{0,1\}^*$	$P_A = g^x$,$ID \in \{0,1\}^*$ *where* $g = \hat{e}(P,Q) \in \mathbb{G}_2$
Partial:	$d_{ID} = sQ_{ID} \in \mathbb{G}_1$ *where* $Q_{ID} = H_1(ID) \in \mathbb{G}_1$	$d_{ID} = sQ_{ID} \in \mathbb{G}_1$ *where* $Q_{ID} = H_1(ID) \in \mathbb{G}_1$	$d_{ID} = \frac{1}{H_3(ID)+s} Q \in \hat{\mathbb{G}}_1$
Priv:	$s_{ID} = xd_{ID} \in \mathbb{G}_1$	$s_{ID} = (d_{ID}, x) \in \mathbb{G}_1 \times \mathbb{Z}_q$	$s_{ID} = (d_{ID}, x) \in \mathbb{G}_1 \times \mathbb{Z}_q$
Gener:	$P \in \mathbb{G}_1$	$P \in \mathbb{G}_1$	$P \in \mathbb{G}_1, Q \in \hat{\mathbb{G}}_1$

	CCLC (Cheng et al., 2007)(a)	BSS (Baek et al., 2005)	PCHL (Park et al., 2007)
KEYS			
Msk:	$(Q, \alpha, \beta, \gamma) \in \hat{\mathbb{G}}_1 \times \in \mathbb{Z}_q^3$	$s \in \xleftarrow{R} \mathbb{Z}_p^*$, $g^s \in \mathbb{Z}_q^*$	$s \in \xleftarrow{R} \mathbb{Z}_q, P_{pub} = sP \in \mathbb{G}_1$ $h, u \xleftarrow{R} \mathbb{G}_1$
Secret:	$x \in \mathbb{Z}_q$	$x \in \mathbb{Z}_p$	$x \in \mathbb{Z}_q$
Pub:	$P_A = xP \in \mathbb{G}_1$,$ID \in \{0,1\}^*$	$P_A = (w,u) \in \mathbb{Z}_q^* \times \mathbb{Z}_q^*$, $ID \in \{0,1\}^*$ *where* $u = g^x \in \mathbb{Z}_q^*, w = g^a \in \mathbb{Z}_q^*$, $a \in \mathbb{Z}_p^*$	$P_A = (X,Y)$,$ID \in \mathbb{Z}_q$ *where* $X = x(P_{pub}P^{-ID}) \in \mathbb{G}_1$, $Y = x \cdot u \in \mathbb{G}_1$
Partial:	$d_{ID} = (rQ$, $(\alpha\beta + (\alpha H_3(ID) + \gamma)r)Q) \in \hat{\mathbb{G}}_1^2$ *where* $r \in \mathbb{Z}_q$	$d_{ID} = (w, d_0) \in \mathbb{Z}_q^* \times \mathbb{Z}_q^*$ *where* $d_0 = a + sH_4(ID, w) \in \mathbb{Z}_q^*$	$d_{ID} = (r, h_{ID}) \in \mathbb{Z}_q \times \mathbb{G}_1$ *where* $h_{ID} = \frac{1}{(s-ID)}(hP^{-r})$,
Priv:	$s_{ID} = (d_{ID}, x) \in \mathbb{G}_1 \times \mathbb{Z}_q$	$s_{ID} = (x, d_0) \in \mathbb{Z}_p^* \times \mathbb{Z}_q^*$	$s_{ID} = (x, r, h_{ID})$
Gener:	$P \in \mathbb{G}_1$,$Q \in \hat{\mathbb{G}}_1$	$g \in \mathbb{Z}_p^*$	$P \in \mathbb{G}_1$

	DLP (Dent et al., 2008)	LDLK (Lai et al., 2009)
KEYS		
Msk:	$s \in \xleftarrow{R} \mathbb{Z}_q^{;} sP_2, P_{pub} = sP$, $P_2 \in_R \mathbb{G}_1$	$d, RsaGroup < p, q, e, d, g >$
Secret:	$x \in \mathbb{Z}_q$	$x \in \mathbb{Z}_q$
Pub:	$P_A = (X,Y)$, $ID \in \{0,1\}^n$ *where* $X = xP \in \mathbb{G}_1, Y = xP_{pub} \in \mathbb{G}_1$,	$P_A = H_2(ID)^{x+d}$, $ID \in \{0,1\}^*$
Partial:	$d_{ID} = (d_0, d_1) =$ $(sP_2 \cdot rF_u(ID), rP) \in \mathbb{G}_1{}^2$ *where* $F_u(ID) = u' \prod_{i=1}^{n} u_i^{ID_i}$ $\vec{U} = (u', u_i), u_i \in \xleftarrow{R} \mathbb{G}_1$, $r, r' \in \mathbb{Z}_q$	$d_{ID} = H_2(ID)^d$
Priv:	$s_{ID} = (xd_0 \cdot r'F_u(ID)$, $xd_1 \cdot r'P)$	$s_{ID} = (d_{ID}, x) \in \mathbb{Z}_n \times \mathbb{Z}_q$
Gener:	$P \in \mathbb{G}_1$	

Table 3: Compatible Classes.

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

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. We successfully implemented a compatible scheme in which users/administrators choose whether they want to use IBE or CLE 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.

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.

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.