Security-Mediated Certificateless Cryptography

Sherman S.M. Chow[1⋆], Colin Boyd[2], and Juan Manuel González Nieto[2]

[1] Department of Computer Science
Courant Institute of Mathematical Sciences
New York University, NY 10012, USA
schow@cs.nyu.edu

[2] Information Security Institute
Queensland University of Technology
GPO Box 2434, Brisbane, QLD 4001, Australia
{c.boyd, j.gonzaleznieto}@qut.edu.au

Abstract. We introduce the notion of security-mediated certificateless (SMC) cryptography. This allows more lightweight versions of mediated cryptography while maintaining the ability for instantaneous revocation of keys. Moreover, our solutions avoid key escrow, which has been used in all previous mediated cryptography algorithms. We provide a model of security against a fully-adaptive chosen ciphertext attacker, who may be a rogue key generation centre or any coalition of rogue users. We present a generic construction and also a concrete algorithm based on bilinear pairings. Our concrete scheme is more efficient than the identity-based mediated encryption scheme of Baek and Zheng in PKC 2004 which is provably secure in a comparable security model. In addition, our proposals can be easily extended to support distributed security mediators.

Keywords: security-mediated cryptography, certificateless cryptography

1 Introduction

During the 1980s and 1990s elaborate schemes for certification of public keys, including many standardised solutions, seemed to be moving towards a world-wide public key infrastructure (PKI). However, in recent years it has been widely recognised that this infrastructure has more problems than was at first realised. Business confidence in public key infrastructure has faltered. Apart from the many commercial, legal and political issues, a recurring dilemma has been how best to manage the processing, storage and revocation of public key certificates.

Public key revocation. The need to be able to revoke public keys was recognised early in the development of public key infrastructure. It seems inevitable that on occasions some private keys will become compromised and in such a case

⋆ Major part of the research is done while the author was a visiting scholar of the Information Security Institute (ISI), Queensland University of Technology (QUT). His visit is sponsored by Endeavour Australia Cheung Kong Award 2005.

it is no longer safe to use the corresponding public key. Initial solutions relied on certificate revocation lists (CRLs) similar to the idea of black lists for credit cards. The difficulty of managing CRLs has led to alternative revocation solutions [7, 12], many of which rely on some on-line checking. As modern networks become more widely available and reliable, use of on-line servers becomes much more realistic than it was several years ago.

Mediated cryptography was designed by Boneh, Ding and Tsudik [7] as a method to allow immediate revocation of public keys. They suggest that such a scheme is particularly useful in government, corporate or military environments, where there may be an unexpected and immediate requirement to revoke a key when a user suspects key compromise, or when a user is removed from a position of authority. Previous revocation techniques cannot satisfy this requirement. The basic idea of mediated cryptography is to use an on-line mediator for every transaction. This on-line mediator is referred to as a SEM (SEcurity Mediator) since it provides a control of security capabilities. If the SEM does not cooperate then no transactions with the public key are possible any longer. Once the SEM is notified that a user's key is to be revoked its use can be immediately stopped.

Identity-based cryptography. Many recent research proposals have focussed on developing public key systems that avoid the use of certificates altogether. The impetus for this trend has largely come from the realisation that the use of pairings on elliptic curves opens up many new options that were not available before. The primary step in this direction was taken by Boneh and Franklin [8] who showed that identity-based cryptography could be practically achieved through use of pairings. Instead of using public keys and certificates, any identity string can take the place of both. Anyone can encrypt a message intended for the entity described by the identity string.

Identity-based cryptography does not solve the revocation problem. Indeed, in some sense it can be argued to make the situation worse since how can a person revoke his own identity? A pragmatic way to deal with this problem is to notice that the identity string can include any additional information, including a validity period. To manage revocation in identity-based cryptosystems, short validity periods may be encoded into the identity string. However, this does not fit an environment where immediate revocation may be required. Ding and Tsudik [10] therefore proposed a combined scheme providing both identity-based key and security-mediated feature.

Escrow problem. A major drawback of all identity-based and security-mediated cryptosystems so far proposed is that they require a trusted third party to generate keys for all entities. This is widely known as the *escrow problem*. Absolute trust is placed in the third party, who could decrypt any message or sign on behalf of any entity. Partial solutions have been proposed to the escrow problem, particularly by distributing the power of the third party over several entities. The problem is present in a particularly acute way in Ding and Tsudik's identity-based mediated cryptography; compromise of the SEM gives away all messages ever encrypted for every party.

Recently there have been schemes proposed to overcome the escrow problem in a more complete way. Certificateless cryptography proposed by Al-Riyami and Paterson [2] is a hybrid between identity-based schemes and traditional schemes using public key certificates. Entities have public keys but they do not have certificates. Instead the identity string is used to ensure that only the correct entity can be in possession of the private key corresponding to the public key. The scheme is attractive, but does not address how to provide instant revocation when desired. This is the problem that we solve in this paper.

CONTRIBUTIONS. We introduce the notion of *Security-Mediated Certificateless (SMC) cryptography.* The major properties that the proposed notion achieve are:

- no certificates are used (in contrast with PKI-based schemes).
- user private keys are not escrowed (in contrast with identity-based schemes).
- instant revocation is provided (in contrast with certificateless schemes).

No previously proposed cryptosystem can provide all these properties together. We first provide a generic construction for security-mediated certificateless encryption. Then we provide a concrete scheme for security-mediated certificateless encryption with better efficiency (and also signature schemes) based on pairings. Security proof in the random oracle model is given. Our concrete scheme has the following properties:

- it is secure in a powerful security model against a fully adaptive rogue key generation centre, or any coalition of fully adaptive rogue users, which can replace the public key of any user and ask for decryption oracle queries even when the public key is replaced.
- it is more efficient[3] than the known identity-based mediated scheme in a similar security model.
- it can be extended to support distributed SEMs, essential for availability.

PAPER STRUCTURE. In the following section we compare related proposals' properties with our proposal. Section 3 discusses the building blocks used by our proposals. The security model for our proposed notion of security-mediated certificateless encryption is discussed in Section 4. Section 5 details our generic construction. In Section 6 a concrete scheme from pairings achieving a higher efficiency than the generic construction is proposed. Finally we conclude our work and discuss some future work of SMC cryptography.

2 Related Work

Our new cryptographic model has strong similarities to a number of previous proposals. It is important to understand our contribution in the context of this previous work. Before discussing each of these in turn we consider a number of prominent features which can be used to differentiate the various models.

[3] Our concrete scheme is *not* a trivial extension from existing identity-based medicated scheme and existing certificateless public key encryption scheme.

SEM free. We use this term to indicate that a scheme does *not* use a security mediator. Generally we may regard this feature as an advantage.

Predefined keys. In traditional public key systems, public and private keys generally need to be generated together. An attractive feature of identity-based and related schemes is that encryption can be done before the corresponding private key has been generated. As discussed in [2], this allows "cryptographic work-flow", such that one must satisfy some condition in order to perform a certain cryptographic function (e.g. encryption). We say a system has predefined keys if part of the key can be predefined, which is sufficient for the interesting applications based on control of work-flow.

Instant revoke. As already discussed, in some applications it is important to have the feature to instantly revoke public keys.

Escrow free. Escrow freeness means the user's secret is not (completely) computable by a certain party other than the user. As discussed previously, identity-based cryptography and some related schemes do not achieve this property since they require some (possibly distributed) third party to compute all entities' secrets. The scheme in [7] is also not escrow free since the private key is not generated by the user (a single party generates the RSA modulus for all users).

Implicit certificates. Explicit certificates are required for conventional public key systems. We say that a scheme has *implicit certificates* if there is no need for users of public keys (e.g. the sender of the message being encrypted) to use an explicit certified string. An implication is that there is no need for on-line verification of certificates. Another advantage of implicit certificates is a saving in storage and bandwidth.

We will consider the relevant previous work next in the context of these important features. Table 1 summarises which schemes provide which features. Notice that no scheme can satisfy all features at once, and therefore our security-mediated certificateless cryptography can be considered as a new compromise between the various desirable features.

	SEM Free	Predefined Keys	Instant Revoke	Escrow Free	Implicit Certificates
Identity-based (ID-based) [8]	✓	✓	✘	✘	✓
Certificateless [2]	✓	✓	✘	✓	✓
Certificate-based [12]	✓	✓	✘	✓	✓
Security-mediated [7]	✘	✘	✓	✘	✘
ID-based security-mediated [10, 16]	✘	✓	✓	✘	✓
Security-mediated Certificateless	✘	✓	✓	✓	✓

Table 1. Properties of related paradigms

Certificateless cryptography. Al-Riyami and Paterson [2] proved that their encryption scheme provides a strong form of chosen ciphertext security. They also provide a key agreement protocol, and a hierarchical encryption scheme in the same model, although none of these extras comes with a formal security analysis. The signature scheme they proposed is later found to be insecure by [14]. More efficient constructions of certificateless public key encryption were proposed subsequently [1,3,9,18]. The improved encryption scheme by Al-Riyami and Paterson [3] is broken and fixed by Zhang and Feng [21].

It is possible to extend certificateless public key encryption (CL-PKE) to a security-mediated one which entails keeping the public key constant while requiring the encryption algorithm to append a changing information such as the current time period to the identifier of the recipient. The corresponding partial private key can then be issued instead of the partial decryption as used in our scheme. This has similar interaction to our scheme. However, an important limitation of this solution is that the key generation centre needs to remain virtually permanently on-line. The point is that the master secret is needed for the creation of a huge number of partial private keys associated with the fine-grained time intervals. Moreover, this requires every sender to know what "changing information" should be used for each recipient every time, which is not a trivial assumption. In contrast, the mediators in our scheme do not use the master secret and so compromise of one mediator does not affect other mediators or the master secret. Besides, the identifier in our scheme remains unchanged.

The PhD thesis of Al-Riyami [1, Section 4.6.1] suggested a way to provide revocation in certificateless cryptography which entails changing the private key (and hence the public key) of the system at regular time intervals. The encryption algorithm must then retrieve the latest system parameters. Again, an important limitation of this solution is that the key generation centre needs to go on-line at the start of each time period. We also remark that Al-Riyami provides no formal model or proof for such a scenario.

Distributed SEM. In any security-mediated schemes, every decryption must involve the help of an on-line SEM, distributing SEM-key across multiple SEMs is essential to ensure availability. Distributing duplicated copies of SEM-key may not be desirable since it introduces more sites for attacker to compromise. One of the standard solutions is to apply threshold cryptography to distribute the SEM-key. In [20], apart from assigning one of the SEMs to hold the original SEM-key, the SEM-key is replicated in the form of a number of shares across multiple SEMs. However, their solution have not considered obtaining partial token from the SEMs holding a share of the SEM-key. Instead, once the initial SEM (holding the original SEM-key) is temporary unavailable, SEM-key migration occurs. The SEM-key is reconstructed from the shares, resulting in an extra copy of a SEM-key. We will show how distributing of SEM-keys is possible for all our proposal.

3 Preliminaries

We review some general notions about public key encryption, one-time signature and identity-based encryption, which will be used in our generic construction. The cryptographic primitive used by our concrete scheme will also be discussed.

3.1 Public key encryption

Let $\mathcal{PKE}$ = (PKE.Gen, PKE.Enc, PKE.Dec) be a (standard) public key encryption scheme consists of the key generation algorithm PKE.Gen, the encryption algorithm PKE.Enc and the decryption algorithm PKE.Dec. PKE.Gen takes as an input security parameter 1^k and outputs a encryption/decryption key pair (EK, DK). PKE.Enc is a randomized algorithm taking EK, a label ℓ and a message m as input, outputs a ciphertext C. PKE.Dec is a deterministic algorithm taking DK, a ciphertext C and a label ℓ, outputs a message m or $\perp$ if C is invalid. We require $\mathcal{E}$ to be correct, i.e. $\mathsf{PKE.Dec}^{\ell}_{\mathsf{DK}}(\mathsf{PKE.Enc}^{\ell}_{\mathsf{EK}}(m)) = m$ for all message m and for all $(\mathsf{EK}, \mathsf{DK})$ generated by PKE.Gen. We also require $\mathcal{PKE}$ to be secure against adaptive chosen ciphertext attack, adapted to deal with labels [19].

3.2 One-time signature

Let $\mathcal{S}$ = (SGen, Sig, Vfy) be a public key signature scheme consists of the key generation algorithm SGen, the signing algorithm Sig and the verification algorithm Vfy. SGen takes as an input security parameter 1^k and outputs a signing/verification key pair (SK, VK). Sig takes SK and a message m as input, outputs a signature σ. Vfy is a deterministic algorithm taking VK, a message m and a signature σ, outputs $\top$ or $\perp$ depending whether the signature is valid. $\mathcal{S}$ should be correct such that $\mathsf{Vfy}_{\mathsf{VK}}(\mathsf{Sig}_{\mathsf{SK}}(m)) = \top$ for all message m and for all $(\mathsf{SK}, \mathsf{VK})$ generated by SGen. For security, we assume $\mathcal{S}$ is strongly unforgeable (cannot create a new valid signature even for previously-signed messages) under adaptive chosen-message attacks. We refer *one-time signature schemes* as a class of signature schemes with a slightly modified security model that an adversary can only request a signature on a single message.

3.3 Identity-based encryption

In 1984, Shamir [17] introduced the idea of identity-based cryptosystem. An identity-based encryption $\mathcal{IBE}$ consists of four algorithms: IBE.Set, IBE.Gen, IBE.Enc and IBE.Dec. In essence, IBE.Set takes as an input security parameter 1^k, outputs common public parameters params and master secret master-key. For simplicity we omit the inclusion of params in the description of the remaining algorithm. IBE.Gen takes user's identity ID, and master-key as input and generates the private key D_{ID} for each user; IBE.Enc produces the ciphertext C by taking the recipient's identity ID, and the message m as input. Finally, IBE.Dec recovers the original message by taking the recipient's private key D_{ID}, and the ciphertext C as input. We require the scheme to be correct, i.e. $\mathsf{IBE.Dec}_{\mathsf{D}_{\mathsf{ID}}}(\mathsf{IBE.Enc}_{\mathsf{ID}}(m)) = m$ for all messages m and all ID such that $\mathsf{D}_{\mathsf{ID}} = \mathsf{IBE.Gen}_{\mathsf{master-key}}(\mathsf{ID})$. We assume $\mathcal{IBE}$ is secure against chosen-ciphertext-and-identity attack. By chosen-identity attack we mean the adversary can ask for the private key of any chosen identities except the one in the challenge.

3.4 Bilinear pairings and related problems

We provide a brief overview of the main definitions and notation for bilinear maps based on elliptic curve pairings. More details and implementation options can be found in many recent papers [6, 8]. We also provide definitions for the BDH problem used by Al-Riyami and Paterson [2]. Using the notation of Boneh and Franklin [8], we let $\mathbb{G}_1$ be an additive group of prime order q and $\mathbb{G}_2$ be a multiplicative group also of order q. We assume the existence of an efficiently computable bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$. Typically, $\mathbb{G}_1$ will be a subgroup of the group of points on an elliptic curve over a finite field, $\mathbb{G}_2$ will be a subgroup of the multiplicative group of a related finite field, and $\hat{e}$ will be derived from the Weil or Tate pairing on the elliptic curve. We assume that an element $P \in \mathbb{G}_1$ satisfying $\hat{e}(P, P) \neq 1_{\mathbb{G}_2}$ is known. By $\hat{e}$ being bilinear, we mean that for $Q, W, Z \in \mathbb{G}_1$, both $\hat{e}(Q, W + Z) = \hat{e}(Q, W) \cdot \hat{e}(Q, Z)$ and $\hat{e}(Q + W, Z) = \hat{e}(Q, Z) \cdot \hat{e}(W, Z)$. When $a \in \mathbb{Z}_q$ and $Q \in \mathbb{G}_1$, we write aQ for Q added to itself $a - 1$ times, also called scalar multiplication of Q by a. As a consequence of bilinearity, for any $Q, W \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q$: $\hat{e}(aQ, bW) = \hat{e}(Q, W)^{ab} = \hat{e}(abQ, W)$.

Throughout this paper we assume that suitable groups $\mathbb{G}_1$ and $\mathbb{G}_2$, a map $\hat{e}$ and an element $P \in \mathbb{G}_1$ have been chosen, and that elements of $\mathbb{G}_1$ and $\mathbb{G}_2$ can be represented by bit strings of the appropriate lengths.

Bilinear Diffie-Hellman(BDH) Problem: Let $\mathbb{G}_1$, $\mathbb{G}_2$, P and $\hat{e}$ be as above. The BDH problem in $\langle \mathbb{G}_1, \mathbb{G}_2, e \rangle$ is as follows: Given $\langle P, aP, bP, cP \rangle$ with $a, b, c \in \mathbb{Z}_q^*$, compute $\hat{e}(P, P)^{abc} \in \mathbb{G}_2$. An algorithm $\mathcal{A}$ has advantage ϵ in solving the BDH problem if $\Pr\left[\mathcal{A}(\langle P, aP, bP, cP \rangle) = \hat{e}(P, P)^{abc}\right] = \epsilon$. Here the probability is measured over random choices of a, b, c in $\mathbb{Z}_q^*$ and the random bits of $\mathcal{A}$.

4 Security-Mediated Certificateless Cryptography

Security-mediated certificateless encryption is a seven-tuple (Setup, Set-Private-Key, Set-Public-Key, Register-Public-Key, Encrypt, SEM-Decrypt, User-Decrypt). The players are the key generation centre (KGC), security mediators (SEMs) and a set of users. The KGC runs the setup phase. It takes a security parameter k as input and generates system parameters (we omit the inclusion of system parameters as the input of the rest of the algorithms). A master-key s that is used to generate a SEM-key is randomly selected.

Following this users can generate their private and public key pairs, using Set-Private-Key and Set-Public-Key. Users need to register their identities and the public keys with the KGC by Register-Public-Key, which is a protocol initiated by the user. This requires the KGC to identify the user and receive an authentic version of the public key. At the same time the user must prove knowledge of the private key corresponding to its public key, although the value of the private key remains secret to the user. The KGC then uses the master secret s to generate the SEM-key required during decryption time by the SEM. This key needs to be authentically and confidentially transferred to the SEM. It is quite possible for one user to register different public keys (or even the same one) with multiple SEMs. Notice that SEMs are not given access to the master secret s at any time.

$\mathsf{Encrypt}$ takes a message, an identity and a registered public key to produce the corresponding ciphertext. $\mathsf{SEM\text{-}Decrypt}$ is executed by the SEM using the SEM-key to do the partial decryption for the user. Finally $\mathsf{User\text{-}Decrypt}$ takes the partial decryption results and the user's private key to get back the message.

4.1 Security model

Existing security-mediated schemes are of different security levels. The identity-based scheme of Ding and Tsudik [10] uses a common RSA modulus for all users, and hence a collusion between a user and the SEM would result in a total break of the scheme. So the security of the scheme requires a strong assumption that the SEM is totally trusted or remains secure throughout the life of the system.

The security model used by Libert and Quisquater [16] has the restriction that the adversary cannot ask for the private key (i.e. the adversary can still ask for the SEM-key) of the target user in the challenge phase of the game. Although their scheme do not have the drawback of Ding and Tsudik's [10], trust is moved to the user as the scheme is insecure against chosen-ciphertext attack by the attacker who possesses the user part of the private key. Since it is assumed that the adversary do not equipped with the user part of the private key, the notion is termed as *weak semantic security against insider attacks*. Generally speaking, it is easier for an attacker to compromise the key for users' side than the SEM's one. The assumption is still a strong one.

We use a similar security model to that used by the identity-based scheme of Baek and Zheng [5], which is secure against chosen-ciphertext attack by insiders. However, a more powerful adversary should be considered in our scenario. The differences are firstly that we allow the adversary access to the master secret s, and secondly that we provide extra queries which allow the adversary to extract and replace public keys. No such queries are relevant to schemes in [5, 16] since identities are used in place of public keys.

The security model also reflects the similarity with Al-Riyami and Paterson's certificateless encryption [2]. An adversary against our scheme should be allowed to make a number of queries. Some of these are the same as those used in the CL-PKE model but we also need to allow queries for partial and complete decryption. The following are the queries available to the adversary. There are some restrictions on when these can be used which will be detailed below.

1. **Extract SEM-key:** On input an identity ID_A the adversary is returned with D_A, which is the key held by SEM for doing the partial decryption on behalf of the user A.
2. **Request public key:** On input an identity ID_A the adversary obtains user A's public key P_A
3. **Replace public key:** On input an identity ID_A and a valid public key P_A, the public key of A is replaced by this new one (and the SEM-key is also updated if the system bundles the public key with the identifier for SEM-key

creation). The replaced version will be used in the rest of the game (unless replaced again), e.g. the **User decrypt** query to be described below.

4. **Extract private key:** On input an identity ID_A, the adversary gets user A's private key x_A. This query is reasonably disallowed if the public key of A has already been replaced by the adversary.
5. **SEM decrypt:** On input a ciphertext C and identity ID_A, the adversary is returned with the partial decryption result C' by using the SEM-key D_A.
6. **User decrypt:** On input a ciphertext C' and an identity ID_A, the adversary is returned with the decryption of C' (which could, of course, be simply $\perp$). Similar to the proof of security for CL-PKE in [2], we have the luxury of allowing this query even in the case that the public key of A has been replaced by the adversary.
7. **Complete decrypt:** It can be done by executing the above two queries in sequence, subject to the restriction (if any) imposed to either one of them.

As in the CL-PKE model, the adversary is forbidden from both making an **Extract SEM-key** query and making a **Replace public key** query for the same identity. We consider two types of adversary, modelling a rogue key generation centre or any coalition of rogue users.

Type-I adversaries do not have access to the master secret s, but are allowed to choose any public key to be used for the challenge ciphertext.

Type-II adversaries have access to the master secret s, but only a registered public key can be used for the challenge ciphertext. (We do not consider a rogue SEM explicitly since it is weaker than the Type-II adversary.)

4.2 Definition of security

The definition of security follows a well-known pattern in which the adversary plays a game in two phases against a challenger. In each phase the adversary is allowed to make queries to the challenger subject to any restrictions. At the end of the first stage the adversary outputs a pair of plaintexts and an ID, and the challenger returns the encryption of one of these. At the end of the second phase the adversary has to output a bit predicting which plaintext was chosen. It wins the game if it gets the bit correctly. The scheme is secure if no efficient adversary exists which can win the game with probability significantly bigger than 1/2. More formally the game proceeds as follows.

Setup: System parameters are generated using the setup procedure of the cryptosystem. The parameters are given to $\mathcal{A}$.

Phase 1: The adversary $\mathcal{A}$ is allowed to make any of the queries detailed above. These queries may be made adaptively.

Challenge phase: The adversary outputs an identity ID_{ch} and a pair of plaintexts m_0, m_1. If $\mathcal{A}$ is a Type-I adversary, it also chooses a public key P_{ch} (by the last **Replace public key** query); otherwise, the public key of identity ID_{ch} cannot be replaced. Important restrictions on key extractions include disallowing **Extract private key** query for ID_{ch} if $\mathcal{A}$ is a Type-II adversary, and disallowing making both of the **Extract SEM-key** query and **Extract private key** query (which is assumed to be issued implicitly if $\mathcal{A}$ has issued a **Replace public key** query) for ID_{ch} if $\mathcal{A}$ is a Type-I adversary. A ciphertext C_{ch}, which is the encryption of m_b (where b is a random bit) under the public key P_{ch} for ID_{ch}, is generated and passed to $\mathcal{A}$.

Phase 2: $\mathcal{A}$ can continue to make queries but cannot make both **Extract SEM-key** query and **Extract private key** query for ID_{ch}. If $\mathcal{A}$ has requested the private key corresponding to the public key P_{ch}, which is registered as the public key of ID_{ch} at the challenge phase, then **SEM decrypt** of the challenge ciphertext by the SEM-key corresponding to ID_{ch} is not allowed. On the other hand, $\mathcal{A}$ cannot ask a **User decrypt** query for C'_{ch} where C'_{ch} is the result of **SEM decrypt** of C_{ch}, if $\mathcal{A}$ has requested the SEM-key corresponding to ID_{ch} (which is assumed to be requested implicitly if $\mathcal{A}$ is a Type-II adversary).

Guess: When it has finished with Phase 2, $\mathcal{A}$ must output a guess bit b'. $\mathcal{A}$ wins the game if $b' = b$ and $\mathcal{A}$'s advantage is defined as $2 \times |\Pr[b' = b] - 1/2|$.

Definition 1. *A security-mediated certificateless encryption scheme is* IND-CCA secure *if there is no efficient adversary in the above game with non-negligible advantage in the security parameter k.*

5 Generic Construction from Multiple Encryption

Multiple encryption refers to the encryption of the same piece of data using multiple and independent encryption schemes. Dodis and Katz [11] proposed a strong chosen-ciphertext secure multiple encryption (refer to [11] for the security definition). We follow their construction and explain our generic security-mediated certificateless encryption scheme. In essence, the multiple encryption includes one instance of identity-based encryption (for SEM side) and one instance of public key encryption (for user side). We illustrate our construction by a bitwise-OR operator instead of the (t, n) threshold secret sharing[4] in their settings. Here the (t, n) notation means at least $t + 1$ decryption keys out of the set of n decryptions keys can recover the ciphertext from the n-times-encryption. In the rest of the paper, we will abuse this notation to refer to a similar meaning that t is the confidentiality threshold of different threshold schemes.

5.1 Encryption algorithm

Setup:

1. On input a security parameter k, execute $\mathsf{IBE.Set}$ to generate system parameters params and the $\mathsf{master\text{-}key}$.
2. Sample H from a family of collision-resistant hash functions.

[4] Dodis and Katz's scheme actually offers four parameters: (t_p, t_f, t_r, t_f), referring to the threshold for privacy (confidentiality), fault-tolerance, robustness and soundness.

$\mathsf{Set\text{-}Private\text{-}Key}$ and $\mathsf{Set\text{-}Public\text{-}Key}$: In this generic construction, this two algorithm may be necessary to combined into one if we treat $\mathsf{PKE.Gen}$ as a black-box. On input a security parameter k, execute $\mathsf{PKE.Gen}$ to generate the user's public/private key pair $(\mathsf{EK}, \mathsf{DK})$.

$\mathsf{Register\text{-}Public\text{-}Key}$: Inputs are the public key EK and an identity ID_A and the master secret $\mathsf{master\text{-}key}$. The $\mathsf{SEM} - \mathsf{key}$ for A is set as $D_A = \mathsf{IBE.Extract}_{\mathsf{params}}(\mathsf{ID}_A)$. As part of the registration process we assume that A proves the knowledge of the private key DK corresponding to the registered public key EK.

$\mathsf{Encrypt}$: Inputs are a message $M \in \{0,1\}^n$, an identity ID_A and public key EK.

1. Generate one-time signature keys $(\mathsf{SK}, \mathsf{VK})$ using SGen.
2. Choose a random label ℓ.
3. Choose random $s_1 \in \{0,1\}^n$ and set $s_2 = M \oplus s_1$.
4. Compute $C_1 = \mathsf{IBE.Enc}_{\mathsf{params}}(\mathsf{ID}_A, s_1)$.
5. Compute $C_2 = \mathsf{PKE.Enc}^{\ell}_{\mathsf{EK}}(s_2)$.
6. Compute $\alpha = H(C_1, C_2, \ell)$.
7. Compute the one-time signature $\sigma = \mathsf{Sig}_{\mathsf{SK}}(\alpha)$.
8. Output the ciphertext $C = \langle C_1, C_2, \mathsf{VK}, \sigma, \ell \rangle$.

$\mathsf{SEM\text{-}Decrypt}$: Inputs are a ciphertext $\langle C_1, C_2, \mathsf{VK}, \sigma, \ell \rangle$, an identity ID_A, a public key DK and $\mathsf{SEM\text{-}key}$ D_A.

1. Check that ID_A is a legitimate user whose key is not revoked.
2. Compute $\alpha = H(C_1, C_2, \ell)$.
3. Check that σ is a valid one-time signature on α by $\mathsf{Vfy}_{\mathsf{VK}}(\alpha, \sigma)$.
4. Output $\perp$ if verification fails.
5. Otherwise, compute $V_1' = \mathsf{IBE.Dec}_{\mathsf{D_A}}(C_1)$ and output V_1'.

$\mathsf{User\text{-}Decrypt}$: Inputs are a ciphertext $\langle C_1, C_2, \mathsf{VK}, \sigma, \ell \rangle$, the token V_1' from the SEM, and a secret DK.

1. Compute α and check σ similar to $\mathsf{SEM\text{-}Decrypt}$.
2. Output $\perp$ if verification fails.
3. Otherwise, compute $V_2' = \mathsf{PKE.Dec}^{\ell}_{\mathsf{DK}}(C_2)$
4. Output $M' = V_1' \oplus V_2'$.

5.2 Efficiency and security analysis

Encryption takes the time for an invocation of identity-based encryption and a public key encryption, together with one signature generation. Decryption by SEM and the user, apart from signature verification, takes one identity-based decryption and one public key decryption respectively. The resulting ciphertext's length is the total length of the ciphertext produced by identity-based encryption and public key encryption, together with the verification key of the signature algorithm, a hash value and a label employed by the public key encryption. Note that the use of one-time signature offers fast signature generation/verification.

Due to the page limit we only outline how simulations in the security proof can be done. From the strong-multiple chosen-ciphertext (SM-CCA) security of the multiple-encryption scheme [11], it is easy to see that partial decryption by the SEM and the complete decryption can be supported in the simulation by querying the decryption oracle of $\mathcal{IBE}$ and $\mathcal{PKE}$ respectively. Type-I adversary's **Extract SEM-key** and **Extract private key** queries can be simulated by the corresponding corruption oracle of $\mathcal{IBE}$ and $\mathcal{PKE}$. The success of a Type-I adversary means breaking the security of either $\mathcal{IBE}$ or $\mathcal{PKE}$. For Type-II adversary, the simulator is only given with $\mathcal{PKE}$ and executes $\mathsf{IBE.Set}$ itself instead of relying on any $\mathcal{IBE}$'s oracles. Simulating in this way makes it possible to answer the queries revealing the $\mathsf{master\text{-}key}$. Since our generic construction is a $(1, 2)$ instantiation of Dodis and Katz's scheme, winning the game in the security proof means the adversary made a successful $\mathcal{IBE}$ decryption and a successful $\mathcal{PKE}$ decryption, implying the security of the underlying $\mathcal{PKE}$ is broken.

5.3 Distributing the SEMs

Our proposed generic construction can be extended to support distributed SEMs in two ways. Suppose t out of n shares of SEM-key is needed for a successful SEM decryption for a particular user. Instead of the above $(1, 2)$ instantiation, the first method is to instantiate $(t, n+1)$ Dodis-Katz multiple encryption, which includes n instances of IBE and one instance of PKE, i.e. the ciphertext contains n ciphertext from IBE and one ciphertext from PKE. Let $\{\mathsf{ID}_A\}$ be $\{(\mathsf{ID}_A||i), i \in \{0 \cdots 0, 0 \cdots 1, 0 \cdots 10, \cdots, 1 \cdots 1\}\}$, i.e. the identity string ID_A concatenated by the binary representations of the integers $\{1, n\}$. For the n instances of IBE, we encrypt n shares produced by a $(t, n + 1)$ secret sharing[5], (instead of a $(1, 2)$ secret-sharing used above) of the message m by the n identities $\{\mathsf{ID}_A\}$ and the remaining share by EK. There are n SEM-keys corresponding to each user, generated by the KGC according to the identity set $\{\mathsf{ID}_A\}$. Each of n SEMs holds one of them. For SEM decryption, t SEMs perform decryption of the corresponding part of the ciphertext, without interacting with other SEMs. After obtaining these partial decryption results, the user executes $\mathsf{PKE.Dec}$ and gets the final message by the recover algorithm of the $(t, n + 1)$ secret sharing.

However, this method inherits the linear ciphertext size and the linear number of encryption from Dodis-Katz's construction. Hereafter we describe our second extension to avoid these linear dependencies. Instead of using n identity-based encryption, we employ a (t, n) identity-based threshold decryption [5], so essentially we are using something similar to the $(1, 2)$ instantiation of the above generic method again. Notice that the threshold decryption scheme employed should spilt the *user*'s key instead of *KGC*'s key, in order to support different threshold settings for different users.

[5] Again, four threshold parameters instead of one can be set in the original construction [11], we only include the confidentiality threshold for the sake of brevity.

By this approach, we achieve a constant size ciphertext, but the efficiency of the resulting scheme is still linearly with (and hence highly dependent on) the decryption efficiency of the underlying identity-based threshold decryption. This shortcoming motivates our concrete construction in the next section.

6 Our Concrete Scheme from Bilinear Pairings

This section explains our concrete security-mediated certificateless encryption scheme, followed by discussion on its efficiency and threshold extension.

6.1 Encryption algorithm

Setup:

1. On input a security parameter k, generate system parameters $(\mathbb{G}_1, \mathbb{G}_2, \hat{e})$ where $\mathbb{G}_1$ and $\mathbb{G}_2$ are groups of prime order q and $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a pairing. Also choose five hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1$, $H_2 : \{0,1\}^n \to \mathbb{Z}_q^*$, $H_3 : \mathbb{G}_1 \to \{0,1\}^n$, $H_4 : \mathbb{G}_2 \to \{0,1\}^n$, and $H_5 : \mathbb{G}_1 \times \mathbb{G}_1 \times \{0,1\}^n \to \mathbb{G}_1$, where n is the length of plaintexts. These hash functions will be modelled as random oracles in order to provide the security proof.
2. Choose an arbitrary generator $P \in \mathbb{G}_1$.
3. Select a master-key s uniformly at random from $\mathbb{Z}_q^*$ and set $P_{pub} = sP$.
4. Return the master-key and the public system parameters given by

$$\mathsf{params} = \langle \mathbb{G}_1, \mathbb{G}_2, \hat{e}, n, P, P_{pub}, H_1, H_2, H_3, H_4, H_5 \rangle.$$

Set-Private-Key: Choose a secret value $x_A \in_R \mathbb{Z}_q^*$ as the private key of entity A.

Set-Public-Key: Given the private key x_A of entity A, set the public key of A to $P_A = x_A P$.

Register-Public-Key: Inputs are the public key P_A and an identity ID_A and the master secret s. The SEM-key for A is set as $D_A = s \cdot H_1(\mathsf{ID}_A)$. As part of the registration process we assume that A proves the knowledge of the value x_A such that $P_A = x_A P$.

Encrypt: Inputs are a message $M \in \{0,1\}^{n-k_0}$, an identity ID_A and public key P_A.

1. Compute $Q_A = H_1(\mathsf{ID}_A)$.
2. Choose random $\sigma \in \{0,1\}^{k_0}$ and set $r = H_2(M \parallel \sigma)$.
3. Compute $k = \hat{e}(Q_A, P_{pub})^r$, $U = rP$ and $U' = rP_A$.
4. Compute $V = (M \parallel \sigma) \oplus H_3(U') \oplus H_4(k)$ [6].
5. Compute $S = rH_5(P_A, U, V)$.
6. Compute the ciphertext $C = \langle S, U, V \rangle \in \mathbb{G}_1 \times \mathbb{G}_1 \times \{0,1\}^n$.

[6] CL-PKE in [3] employs a similar "exclusive-or structure" in the ciphertext, which is exploited by the attack in [21]. However, the non-malleability provided by the S component protects our scheme from their attack.

SEM-Decrypt: Inputs are a ciphertext $\langle S, U, V \rangle$, an identity ID_A, a public key P_A and SEM-key D_A.

1. Check that ID_A is a legitimate user whose key is not revoked.
2. Check that $\hat{e}(P, S) = \hat{e}(U, H_5(P_A, U, V))$.
3. Compute $V' = V \oplus H_4(\hat{e}(D_A, U))$ and output V'.

User-Decrypt: Inputs are a partial ciphertext U, the token V' from the SEM, and a secret x_A.

1. Parse M' and σ' from $M' \parallel \sigma' = H_3(x_A U) \oplus V'$.
2. Verify whether $H_2(M' \parallel \sigma') \cdot P = U$.
3. If the verification succeeds then output M'. Else output $\perp$.

It is easy to see that the proposed scheme is correct. Consider a valid ciphertext produced by our scheme; from the bilinearity of pairings, the checking done in SEM-Decrypt must pass. Consider the decryption step in SEM-Decrypt, we have $\hat{e}(D_A, U)) = \hat{e}(sQ_A, rP) = \hat{e}(Q_A, sP)^r = \hat{e}(Q_A, P_{pub})^r$. For the decryption step in User-Decrypt, $x_A U = x_A rP = rP_A$. Again, the checking in User-Decrypt must pass for a valid ciphertext since $U = rP$. The correctness thus follows.

6.2 Efficiency and security analysis

We make the focus of our comparison on the efficiency of identity-based threshold decryption by Baek and Zheng [5] for the following reasons. First, the second threshold extension of the generic scheme described in previous section requires the use of identity-based threshold decryption. To the best of authors' knowledge, Baek and Zheng [5]'s scheme is the only scheme that separating the private key of each user into shares instead of the private key of the KGC. Second, a $(1, 2)$ threshold decryption can be used as an identity-based medicated encryption (IDME) by delegating one share to the SEM and another to the user. Since their threshold decryption scheme is chosen-ciphertext secure, the resulting IDME offering a similar level of security as ours, in the sense that partial SEM decryption queries are allowed.

From the Table 2, we can see that our scheme offers a more efficient solution. In IDME, the checking on the SEM's decryption is not included as part of the protocol. As a consequence, the user will not notice if there is something wrong in the SEM's decryption. Yet, a zero knowledge proof for the equality of two discrete logarithms based on bilinear pairings [5, 16] can be used to ensure the consistency of SEM's decryption result. The notation $(+y)$ in Table 2 represents the number of additional operations required if such a proof is employed. In our proposed scheme, such a zero knowledge proof is not necessary since a mechanism of consistency checking is already incorporated.

The following theorem summarises the security of our proposed scheme. The proof can be found in the full version of this paper.

Theorem 1 *Our proposed scheme is IND-CCA secure against Type I and Type II adversary in the random oracle model, under the assumption that the BDH problem is intractable.*

	Encryption			Decryption (SEM)			Decryption (User)		
	$\hat{e}(\cdot,\cdot)$	Exp	Hash	$\hat{e}(\cdot,\cdot)$	Exp	Hash	$\hat{e}(\cdot,\cdot)$	Exp	Hash
IDME	1	3	1	3 (+2)	0 (+1)	1	3 (+2)	0 (+2)	1
Proposed Scheme	1	3	1	3	0	1	0	2	0

Table 2. Efficiency Analysis of Security-Mediated Encryption Schemes

6.3 Distributing SEMs

Since our proposed scheme is built on top of a variant of the identity-based threshold decryption scheme which is proven to be IND-CCA secure, the extension of our scheme to support distributed SEMs can be proven to be IND-CCA secure too. The idea of the extension is as follows. Instead of delegating a single SEM-key, the SEMs got a (t, n) share $D_A^{(i)}$ of the SEM-key D_A (by employing the sharing a point on $\mathbb{G}$ sub-routine in [5], which is a simple twist of the Shamir's polynomial secret sharing). The partial decryption result to be returned by the SEMs is no longer the hash value $H_4(\hat{e}(D_A^{(i)}, U))$ but $\hat{e}(D_A^{(i)}, U)$.[7] And the user reconstructs all these partial decryption results and performs the final decryption. As a result, the extended scheme offers higher availability without explicit replication of SEM-key. Indeed, the major portion of the pairing operations in our proposed scheme comes from the checking of the validity of ciphertext before SEM decryption, which is an essential step for the chosen-ciphertext security of distributed SEMs. Similar to our second extension of our generic construction, constant size ciphertext is achieved. Moreover, our concrete scheme has a higher efficiency as shown in Table 2.

7 Conclusion and Future Work

We introduce the notion of security-mediated certificateless (SMC) cryptography, which has instantiated one more of the set of compromises within the various desirable properties for solving the certification problem in public key cryptography. We have provided a generic construction and also a concrete encryption scheme. An attractive feature of our proposal is that it can use the same parameters used for most other identity-based and share the same key generation centre (KGC). Our scheme also supports distributed security mediators (SEMs).

A limitation of certificateless encryption (both ours and the original) is that in its basic form it fails to reach Girault's level 3 [13]. This means that although there is less trust placed in the authority than for identity-based schemes (users do not reveal their private keys to the KGC), there is more trust placed in the KGC than in traditional public key schemes. This is because if a malicious KGC distributes a bogus public key for a user, the KGC can obtain secrets intended for that user even though there is no evidence that can be used to prove that

[7] Note that there is no special handling for the simulation of H_4 in the security proof.

the KGC misbehaved. There are ways to achieve level 3 as discussed by Al-Riyami [1]. One way is to provide a proof of possession of the private key, which in turn provides the evidence of malicious behaviour if more than one is found. This can be achieved by providing a signature using the same key.

We discuss some of our future work in SMC cryptography. Naturally it would be nice to provide a complementary signature scheme with similar properties. We have a set of candidate signature schemes, including a variant of blind signature scheme that SEM can blindly issue a partial signature to users. Another challenge is to design a scheme with all the properties of ours but can achieve the level 3 of trust refined by Al-Riyami [1]. His work [1] also refined the CBE model [12], and generic construction of CBE in this new model from CL-PKE is proposed [1, 3]. However, their security evidence is questioned recently [15]. It is interesting to identify the relation between SMC encryption and CBE. Another related problem is to design SMC encryption without pairing [4].

Acknowledgement

This paper is an outgrowth of a short-term research project sponsored by Endeavour Australia Cheung Kong Award 2005. Sherman Chow would like to thank Australian Government Department of Education, Science and Training for the assistantship. He is grateful to his coauthors for offering this on-going project, and anonymous reviewers for helpful comments and the suggestion about generic construction in particular. He is also indebted to all the staff and students of ISI, QUT for their continuing support and kind hospitality during his visit there.

References

1. Sattam S. Al-Riyami. *Cryptographic Schemes Based on Elliptic Curve Pairings.* PhD thesis, Royal Holloway, University of London, 2004.
2. Sattam S. Al-Riyami and Kenneth G. Paterson. Certificateless Public Key Cryptography. In *Advances in Cryptology - ASIACRYPT 2003, 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30 - December 4, 2003*, volume 2894 of *LNCS*, pages 452–473. Springer, 2003. Full version at `http://eprint.iacr.org/2003/126`.
3. Sattam S. Al-Riyami and Kenneth G. Paterson. CBE from CL-PKE: A Generic Construction and Efficient Schemes. In *Public Key Cryptography - PKC 2005, 8th International Workshop on Theory and Practice in Public Key Cryptography, Les Diablerets, Switzerland, January 23-26, 2005*, volume 3386 of *LNCS*, pages 398–415. Springer, 2005.
4. Joonsang Baek, Reihaneh Safavi-Naini, and Willy Susilo. Certificateless Public Key Encryption Without Pairing. In *Information Security, 8th International Conference, ISC 2005, Singapore, September 20-23, 2005*, volume 3650 of *LNCS*, pages 134–148. Springer, 2005.
5. Joonsang Baek and Yuliang Zheng. Identity-based Threshold Decryption. In *Public Key Cryptography - PKC 2004, 7th International Workshop on Theory and Practice in Public Key Cryptography, Singapore, March 1-4, 2004*, volume 2947 of *LNCS*, pages 262–276. Springer, 2004.

6. Paulo S. L. M. Barreto, Hae Yong Kim, Ben Lynn, and Michael Scott. Efficient Algorithms for Pairing-based Cryptosystems. In *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002*, volume 2442 of *LNCS*, pages 354–368. Springer.
7. Dan Boneh, Xuhua Ding, and Gene Tsudik. Fine-grained control of security capabilities. *ACM Transactions on Internet Technology*, 4(1):60–82, February 2004.
8. Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.
9. Zhaohui Cheng and Richard Comley. Efficient Certificateless Public Key Encryption. Cryptology ePrint Archive, Report 2005/012, 2005.
10. Xuhua Ding and Gene Tsudik. Simple Identity-Based Cryptography with Mediated RSA. In *Topics in Cryptology - CT-RSA 2003, The Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, April 13-17, 2003*, volume 2612 of *LNCS*, pages 193–210. Springer, 2003.
11. Yevgeniy Dodis and Jonathan Katz. Chosen-Ciphertext Security of Multiple Encryption. In *Theory of Cryptography, Second Theory of Cryptography Conference, TCC 2005, Cambridge, MA, USA, February 10-12, 2005, Proceedings*, volume 3378 of *LNCS*, pages 188–209. Springer, 2005.
12. Craig Gentry. Certificate-Based Encryption and the Certificate Revocation Problem. In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003*, volume 2656 of *LNCS*, pages 272–293. Springer, 2003.
13. Marc Girault. Self-certified Public Keys. In *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of Cryptographic Techniques, Brighton, UK, April 8-11, 1991*, volume 547 of *LNCS*, pages 490–497.
14. Xinyi Huang, Willy Susilo, Yi Mu, and Futai Zhang. On the Security of Certificateless Signature Schemes from Asiacrypt 2003. In *Cryptology and Network Security, 4th International Conference, CANS 2005, Fujian, China, December 14-16, 2005*, volume 3810 of *LNCS*, pages 13-25. Springer, 2005.
15. Bo Gyeong Kang and Je Hong Park. Is it possible to have CBE from CL-PKE?. Cryptology ePrint Archive, Report 2005/431, 2005.
16. Benoît Libert and Jean-Jacques Quisquater. Efficient Revocation and Threshold Pairing based Cryptosystems. In *PODC 2003 of the Twenty-Second ACM Symposium on Principles of Distributed Computing (PODC 2003), July 13-16, 2003, Boston, Massachusetts, USA. ACM*, pages 163–171. ACM Press, 2003.
17. Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In *Advances in Cryptology of CRYPTO 1984, Santa Barbara, California, USA, August 19-22, 1984*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, 1985.
18. Yijuan Shi and Jianhua Li. Provable Efficient Certificateless Public Key Encryption. Cryptology ePrint Archive, Report 2005/287, 2005.
19. Victor Shoup. A Proposal for an ISO Standard for Public Key Encryption (Version 2.1). Cryptology ePrint Archive, Report 2001/112, 2001.
20. Gabriel Vanrenen and Sean Smith. Distributing Security-Mediated PKI. In *Public Key Infrastructure, First European PKI Workshop: Research and Applications, EuroPKI 2004, Samos Island, Greece, June 25-26, 2004, Proceedings*, volume 3093 of *LNCS*, pages 218–231. Springer, 2004.
21. Zhenfeng Zhang and Dengguo Feng. On the Security of a Certificateless Public-Key Encryption. Cryptology ePrint Archive, Report 2005/426, 2005.