Efficient revocation and threshold pairing based cryptosystems

Benoît Libert Jean-Jacques Quisquater

UCL Crypto group, Microelectronics Laboratory
Place du Levant, 3, 1348 Louvain-la-Neuve, Belgium
{libert,quisquater}@dice.ucl.ac.be

ABSTRACT

Boneh, Ding, Tsudik and Wong recently proposed a way for obtaining fast revocation of RSA keys. Their method consists in using security mediators that keep a piece of each user's private key in such a way that every decrytion or signature operation requires the help of the mediator for the user. Revocation is achieved by instructing the mediator to stop helping the user to sign or decrypt messages. This security architecture, called SEM, gave rise to an identity based mediated RSA scheme (IB-mRSA) that combines the advantages of fast revocation and identity based public keys. We show that, in opposition to what was stated in [9], this revocation method can be applied to several existing public key encryption and signature schemes (all those for which a secure practical threshold adaptation exists) including the Boneh-Franklin identity based encryption scheme and a pairing based digital signature schemes. We first describe a threshold adaptation of the Boneh-Franklin identity based encryption scheme and, then, we compare the mediated versions of these schemes with IB-mRSA from security and efficiency points of view.

Keywords

Public key cryptosystems, bilinear maps, revocation

1. INTRODUCTION

Efficient revocation of public key certificates has always been a critical issue in public key infrastuctures (PKIs). In 2001, Boneh et al. introduced a method for obtaining instantaneous revocation of a user's public key privileges ([4]) in RSA-type cryptosystems. Their idea was to give an online security mediator (SEM) a piece of each user's private key exponent while users have the second piece of their respective decryption/signature exponent. In such a setting, a user is unable to decrypt/sign a message without first receiving a message-specific token from the security mediator that is assumed to be a semi-trusted entity. Public key revocation is achieved by instructing the SEM to stop issuing tokens for the user's public key. The scheme described in [4] is built using threshold RSA (the private key is shared between two parties) and is called mediated RSA (mRSA). The SEM architecture is transparent to the sender of a message and to the verifier of a signature because the encryption and verification operations remain the same as in classical RSA. Furthermore, the use of a SEM architecture removes the need to enquire about the status of a public key before using it. Before encrypting a message with Bob's key, Alice does not have to worry about any certificate's validity: Bob will simply not be able to decrypt the message if his public key is revoked since the SEM has been instructed not to give him the necessary token. Similarly, when receiving a signed message from Bob, Alice can be sure the verification public key is valid since the SEM does not help any user whose public key is revoked in a signature process.

Key management can also be simplified by using identity based cryptosystems. This is a concept introduced by Shamir in 1984 ([25]) to eliminate as much as possible the need for public key certificates by allowing a public key to be uniquely derived from the user's identity information (e-mail address, telephone number, social security number,...). It also simplifies key management since there is no need to maintain a great database containing a list of public keys and their respective owner. Many identity based cryptosystems have been proposed since 1984 ([15], [5], [19], [7],[16], [28],...) but none of these provides an efficient solution to revoke identities. It is their inherent drawback since their goal is to avoid the use of public key certificates which usually indicate the validity of their corresponding keys. Boneh et al. recently described ([3]) how to transform mRSA into an identity based mediated RSA scheme (IB-mRSA). In this paper, we will first review their scheme and we discuss about its security against inside attackers (i.e. dishonest users of the system). We point out that the provable security of mediated cryptosystems against insider attacks can be hampered by the same obstacles as those to the provable security of threshold cryptosystems. Next, we will show that a SEM architecture can also be introduced in existing identity based ([5]) and other pairing based or ordinary cryptosystems ([6],[24]) for which a threshold adaptation exists. We discuss about the security of a threshold adaptation of the Boneh-Franklin IBE before describing how to turn its original version into a mediated cryptosystem that satisfies the same security notion as IB-mRSA and that is more robust

PODC '03 Boston, Massachusetts USA

to a compromise of the SEM. Finally, we show that it exists an interesting alternative to the mediated RSA signature scheme.

2. THE IB-MRSA SCHEME AND ITS SECURITY

As told above, the idea of mediated RSA is to split the private key in two parts. One part is given to the user while the other one is given to the SEM in such a way that the user has to cooperate with the SEM to be able to decrypt or sign messages. The scheme of course uses the OAEP padding to achieve the IND-CCA2 security. Formally, IB-mRSA is made of four algorithms as usual identity based cryptosystems.

Setup: given a security parameter k, the PKG chooses $k/2-$bits primes p', q' such that $p = 2p' + 1$ and $q = 2q' + 1$ are also prime. Then it computes the $k-$bit Blum integer $n = pq$ and chooses a hash function $H : \{0, 1\}^* \rightarrow \{0, 1\}^l$ for a parameter l depending on k. The public parameters are $\mathcal{P} := (n, H)$ (and must be certified).

Keygen: For Alice's identity ID_A,

1. Let $s = k - l - 1$.
2. The PKG computes $e_{Alice} = 0^s||H(ID_A)||1$. [1]
3. It computes $d_{Alice} = e_{Alice}^{-1} \mod \phi(n)$.
4. It chooses $d_u \leftarrow_R \mathbb{Z}_n^*$ and computes $d_{sem} = d_{Alice} - d_u \mod \phi(n)$.

The PKG gives d_{sem} to the SEM and d_u to Alice.

Encrypt: is the same as in classical RSA-OAEP.

Decrypt: when receiving an encrypted message $c \in \mathbb{Z}_n^*$, Alice transmits c to the SEM. They perform the following tasks in parallel.

SEM:
1. Check if Alice's identity ID_A is revoked. If it is, return "Error".
2. Compute $m_{sem} = c^{d_{sem}} \mod n$ and send it to Alice

USER:
1. Alice computes $m_u = c^{d_u} \mod n$.
2. When receiving m_{sem} from the SEM, she computes $m = m_{sem}m_u \mod n$.

In the key generation algorithm, we notice that the output of the hash function is padded with a 1 to the right in order to obtain an odd e_{Alice} and increase the probability for it to be prime with $\phi(n)$. Notice that the SEM is not able to decrypt messages intended to Alice since Alice never sends it her partial decryption m_u in the decryption protocol.

In the corresponding signature scheme, we have a similar protocol for the signing algorithm. We thus have identity based encryption and signature schemes where it is possible to efficiently revoke identities.

We recall that it is completely insecure to have a common modulus for several users in classical RSA-OAEP since the knowledge of a single private-public pair of exponents allows to factor the modulus. It is not the case in IB-mRSA since no user completely knows his key pair. Therefore, unlike the non identity based mRSA, the SEM is here assumed to be a totally trusted and secure entity. A collusion between a user and the SEM would result in a total break of the scheme. As explained in [4], we must assume that no user is able to compromise the SEM.

From another security point of view, it is claimed in [9] (proposition 1) that IB-mRSA-OAEP offers equivalent semantic security to classical RSA-OAEP against chosen ciphertext attacks in the random oracle model provided the Keygen algorithm has negligible probability to produce exponents e_a and e_b satisfying a multiplicative relation from identities ID_a and ID_b. We point out there is a flaw in the security proof provided in [9]. In lemma 1, when an attacker $\mathcal{B}$ against IB-mRSA performs a SEM query on a ciphertext c, the attacker $\mathcal{F}$ against RSA-OAEP (in the single user setting) has to simulate the behavior of the SEM. It is claimed in [9] that $\mathcal{F}$ just has to forward c in a decryption query to its challenger. Once, $\mathcal{F}$ receives the decryption c^d, it just has to compute c^d/c^r, where r is the user piece of private exponent given to the adversary, and to return it as an answer to $\mathcal{B}$'s decryption query. This works for RSA without padding but not for RSA-OAEP. Indeed, recall that in RSA-OAEP, the encryption $\mathcal{E}(m, r)$ of m with the random string r is given by $\mathcal{E}(m, r) = (s||t)^e \mod n$ with

$$s = (m||\mathbf{0}^{k_1}) \oplus G(r), \quad \text{and} \quad t = r \oplus H(s)$$

where G and H are suitable hash functions. It is not considered in the proof of lemma 1 of [9] that, when $\mathcal{F}$ asks its challenger for the decryption of c, it receives a plaintext m (or the symbol $\perp$ if c is not a valid ciphertext) instead of the e^{th} root of c. $\mathcal{F}$ can of course try to recover which random string r was used to encrypt m into c (and then s, t and $(s||t) = c^d$) by looking at the hash queries made by $\mathcal{B}$ and the answers given by $\mathcal{F}$'s challenger. But what happens if $\mathcal{B}$ did not ask the appropriate hash queries on G and H ? $\mathcal{F}$ cannot simply reject the ciphertext because it is expected to output a partial computation on c. More generally, when $\mathcal{F}$'s challenger answers that c is not a valid ciphertext, $\mathcal{F}$ cannot return "?" to $\mathcal{B}$ as an answer to the SEM query nor return a random quantity (because this would provide $\mathcal{B}$ with an inconsistent view since $\mathcal{B}$ is assumed to know the user part of the decryption exponent). It turns out that $\mathcal{F}$ cannot simulate the behavior of the SEM when the attacker $\mathcal{B}$ asks a decryption token for an invalid ciphertext. As a result, IB-mRSA/OAEP does not seem to be provably semantically secure against insider attacks (i.e. attacks made by dishonest users in the system). Even worse, for any mediated cryptosystem it seems that a correct simulation of the SEM's behavior could only be made if the SEM was able to check the validity of the ciphertext at the beginning of the decryption process (just like for a threshold cryptosystem to be secure against chosen ciphertext attacks as explained in [10], [27]). Whereas, the IB-mRSA signature scheme does not suffer from this problem, the provable security against insider attacks for mediated encryption schemes turns out to be not so easy. We do not provide a solution in this paper

[1] The padding with zeros on the left side allows to avoid the constraint to use a hash function with a too wide range

but we describe an alternative to IB-mRSA that is provably secure against inside attacks in a weaker sense. This weaker security notion is also achievable by IB-mRSA/OAEP but, unlike this latter, the new mediated identity based cryptosystem does not completely crumble if a dishonest user corrupts the SEM. It is based on the Boneh-Franklin identity based encryption scheme.

About revocation issues in identity based cryptosystems, it is claimed in [4] and [3] that the only way to obtain revocation in the Boneh-Franklin IBE ([5]) is to concatenate a validity period to the identifying strings. Senders do not use identities outside their validity period to encrypt messages and revocation is achieved by instructing the PKG to stop issuing new private keys for revoked identities. This involves the need to periodically re-issue all private keys in the system and the PKG must be online most of the time. We show that it is not true and that a SEM architecture can also be combined to the pairing based IBE to obtain fine grain revocation without creating security flaws. In fact, a mediated cryptosystem can be built from any threshold cryptosystem. Let us now describe an IND-CPA threshold adaptation of the Boneh-Franklin cryptosystem.

3. A (T, N) IND-ID-CPA THRESHOLD IBE

We first give a basic overview of the properties of bilinear maps which have been very useful tools to build the Boneh-Franklin IBE and some other interesting schemes ([19], [7], [28], [6],...).

3.1 Bilinear pairings

Let us consider an additive group $\mathbb{G}_1$ and a multiplicative group $\mathbb{G}_2$ of the same prime order q. We assume the discrete logarithm problem is hard in both groups. We need a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfying the following properties:

1. Bilinearity: $\forall\ P, Q \in \mathbb{G}_1,\ \forall\ a, b \in \mathbb{F}_q^*$, we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
2. Non-degeneracy: for any point $P \in \mathbb{G}_1$, $\hat{e}(P, Q) = 1$ for all $Q \in \mathbb{G}_1$ iff $P = \mathcal{O}$.
3. Computability: there exists an efficient algorithm to compute $\hat{e}(P, Q)\ \ \forall\ P, Q \in \mathbb{G}_1$.

The modified Weil pairing and the Tate pairing are admissible maps satisfying these properties (see [20] for a description of these pairings). $\mathbb{G}_1$ is a cyclic subgroup of the additive group of points of a supersingular elliptic curve $E(\mathbb{F}_p)$ over a finite field while $\mathbb{G}_2$ is a cyclic subgroup of the multiplicative group associated to a finite extension of $\mathbb{F}_p$.

Definition 1. *Given two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q, a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and a generator P of $\mathbb{G}_1$, the **Bilinear Diffie-Hellman problem** (BDHP) in $(\mathbb{G}_1,\mathbb{G}_2,\hat{e})$ is to compute $\hat{e}(P, P)^{abc}$ given (P, aP, bP, cP).*

3.2 The threshold IBE

We refer to [5] for a detailed description of the Boneh-Franklin identity based encryption scheme. The threshold version works like this.

Setup: Given a security parameter k, the PKG chooses two groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q (with $q \approx 2^k$), a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, a generator $P \in \mathbb{G}_1$, a secret master key $s \in_R \mathbb{F}_q$. After that, it chooses a polynomial of degree t

$$f(x) = s + a_1 x + \cdots + a_{t-1} x^{t-1}$$

for random $a_1, \ldots, a_{t-1} \in \mathbb{F}_q$. For $i = 1, \ldots, n$, it computes $P_{pub}^{(i)} = f(i)P \in \mathbb{G}_1$. Finally, it computes $P_{pub} = sP \in \mathbb{G}_1$ and chooses cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^n$. The public parameters are

$$\mathcal{P} := \{\mathbb{G}_1, \mathbb{G}_2, \hat{e}, H_1, H_2, P, P_{pub}^{(1)}, \ldots, P_{pub}^{(n)}, P_{pub}\}.$$

Before requesting his private share, each player can check that

$$\sum_{i \in S} L_i P_{pub}^{(i)} = P_{pub}$$

for any subset $S \in \{1, \ldots, n\}$ such that $|S| = t$ where L_i denotes the appropriate Lagrange coefficient.

Keygen: given a user's identity ID, the PKG plays the role of the trusted dealer. It first computes $Q_{ID} = H_1(ID) \in \mathbb{G}_1$. For $i = 1, \ldots, n$, it delivers $d_{ID_i} = f(i)Q_{ID} \in \mathbb{G}_1$ to player i. When receiving d_{ID_i}, player i checks that $\hat{e}(P_{pub}^{(i)}, Q_{ID}) = \hat{e}(P, d_{ID_i})$. If the verification fails, he complains to the PKG that issues a new share.

Encrypt: to encrypt a message m, Alice has to code it as an element of $\mathbb{G}_2$. Given the receiver's identity ID, compute $Q_{ID} = H_1(ID)$.

1. Choose a random $r \in_R \mathbb{F}_q$.
2. The ciphertext is given by

$$< U, V > \ = \ < rP,\ m \oplus H_2(\hat{e}(P_{pub}, Q_{ID})^r) > .$$

Decrypt: when receiving $< U, V >$, player i computes his decryption share $\hat{e}(U, d_{ID_i})$ and gives it to the recombiner who is a designated player .

Recombination: the recombiner selects a set $S \subset \{1, \ldots, n\}$ of t acceptable shares $\hat{e}(U, d_{ID_i})$ and computes

$$g = \prod_{i \in S} \hat{e}(U, d_{ID_i})^{L_i}.$$

Once he has g, he recovers the plaintext

$$m = V \oplus H_2(g).$$

The correctness of the scheme is easy to verify since

$$g = \hat{e}(rP, \sum_{i \in S} L_i d_{ID_i}) = \hat{e}(rP, sQ_{ID}) = \hat{e}(P_{pub}, Q_{ID})^r.$$

It is possible to add the robustness [2] feature to the scheme. Every player just has to prove (in a non-interactive way) the equality of two inverses of the isomorphism $f_P(.) = \hat{e}(P, .)$ induced by the bilinear map $\hat{e}$. To do this, each player

[2]That is to allow the honest players (we must assume that $n \geq 2t - 1$ in such a way that at least t players are honest) to perform the decryption even if some other players do not broadcast admissible shares.

chooses a random $R \in \mathbb{G}_1$ and computes $w_1 = \hat{e}(P, R) \in \mathbb{G}_2$, $w_2 = \hat{e}(U, R) \in \mathbb{G}_1$ and then a hash e of the tuple $(\hat{e}(U, d_{ID_i}), \hat{e}(P_{pub}, Q_{ID}), w_1, w_2)$. After that, player i computes $V = R + ed_{ID_i} \in \mathbb{G}_1$ and joins the tuple (w_1, w_2, e, V) to his share. The other players can check that

$$\hat{e}(P, V) = \hat{e}(P, R)\hat{e}(P_{pub}^{(i)}, Q_{ID})^e$$

and

$$\hat{e}(U, V) = \hat{e}(U, R)\hat{e}(U, d_{ID_i})^e.$$

The soundness of this proof is easy to be verified. When dishonest players are detected, t among the others can combine their shares to find the one of the dishonest ones and find their decryption share.

This cryptosystem looks like the threshold adaptation of the El Gamal cryptosystem. Whereas this latter scheme is known to resist to chosen-plaintext attacks under the decisional Diffie-Hellman assumption over a multiplicative cyclic group, the above threshold IBE is provably secure against chosen plaintext attacks in the identity based setting under the computational bilinear Diffie-Hellman assumption.

3.3 Security

We first describe formally the IND-ID-TCPA security notion satisfied by the threshold IBE.

DEFINITION 2. *We say that a threshold identity based encryption scheme is secure against chosen-plaintext attacks (we denote by IND-ID-TCPA2 this security notion) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. *The adversary $\mathcal{A}$ first chooses a set S of $t-1$ players it wants to corrupt. It receives from the challenger the partial private keys d_{ID_i} (with $i \in S$) of the corrupted users.*

2. *The challenger runs the Setup algorithm with a security parameter k and sends the system parameters to the adversary.*

3. *The adversary $\mathcal{A}$ performs a polynomially bounded number of full key extraction queries: $\mathcal{A}$ produces an identity ID and receives the complete decryption key d_{ID} (as in the classical BF scheme). $\mathcal{A}$ can present its requests adaptively: every request may depend on the answer to the previous ones.*

4. *$\mathcal{A}$ chooses two plaintexts $m_0, m_1 \in \mathcal{M}$ and an identity ID on which it wishes to be challenged. It is not allowed to choose an identity for which it made a full key extraction query during the first stage.*

5. *The challenger takes a random bit $b \in_R \{0, 1\}$ and computes $C = Encrypt(m_b, ID)$ that is sent to $\mathcal{A}$.*

6. *$\mathcal{A}$ performs a second series of queries just like in the first stage. This time, it cannot ask the complete private key corresponding to ID.*

6. *Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.*

The adversary's advantage is defined to be

$$Adv(\mathcal{A}) := \big|2Pr[b' = b] - 1\big|.$$

In the corresponding IND-ID-TCCA security notion (that is against adaptive chosen ciphertext attacks), the attacker is allowed to ask decryption shares for messages and identities of its choice (other than those corresponding to the challenge). The following theorem states the IND-ID-TCPA security of the threshold IBE in the random oracle model.

THEOREM 3.1. *In the random oracle model, if an attacker $\mathcal{A}$ has a non negligible advantage ϵ in a chosen plaintext attack against the threshold IBE in a time t_1, there exists an algorithm $\mathcal{B}$ that can solve the bilinear Diffie-Hellman problem in a time $O(t_1)$ with an advantage $\epsilon/q_{H_1}q_{H_2}$ where q_{H_1} denotes the number of H_1 queries made by $\mathcal{A}$ and q_{H_2} is the number of H_2 queries.*

Proof. $\mathcal{B}$ receives a random instance (P, aP, bP, cP) of the bilinear Diffie-Hellman problem and has to compute $\hat{e}(P, P)^{abc}$. It will run the adversary $\mathcal{A}$ and use it to achieve its goal.

Let us first recall an important property of a (t, n)-secret sharing schemes: given shares $\{c_1, \ldots, c_n\}$ of a secret c and any ordered subset $S = \{i_1, \ldots, i_t\} \subset \{0, \ldots, n\}$, for any $i \in \{0, \ldots, n\} \backslash S$, there are easy to compute coefficients $\lambda_{i1}, \ldots, \lambda_{it} \in \mathbb{F}_q$ such that $c_i = \sum_{j=1}^{t} \lambda_{ij} c_{i_j}$.

Before the game begins, $\mathcal{A}$ first chooses a set S of $t-1$ servers it wants to corrupt. Without loss of generality, we can assume it chooses $S = \{1, \ldots, t-1\}$. $\mathcal{B}$ then generates the public parameters like this. It sets $P_{pub} = cP$ (but it does not know c). It chooses random values $c_1, \ldots, c_{t-1} \in \mathbb{F}_q$, finds the appropriate λ_{ij} coefficients and computes $P_{pub}^{(i)} = \lambda_{i0} P_{pub} + \sum_{j=1}^{t-1} \lambda_{ij} c_j P$ for $i = t, \ldots, n$ and $P_{pub}^{(i)} = c_i P$ for $i = 1, \ldots, t-1$. The condition

$$\sum_{i \in T} L_i P_{pub}^{(i)} = P_{pub} \quad \text{for any } T \subset \{1, \ldots, n\} \text{ with } |T| = t$$

then holds. At the first stage of the game, $\mathcal{B}$ first chooses a random integer $\mu \in \{1, \ldots, q_{H_1}\}$ and $\mathcal{A}$ then performs a polynomially bounded number of hash and full key extraction queries and $\mathcal{B}$ will simulate the hash and key extraction oracles using a list L_1 that is initially empty to keep track of answers to hash queries. Without loss of generality, we can assume that any key extraction query on an identity is preceded by a hash query on that identity. $\mathcal{A}$ then asks hash values of identities ID_e that are indexed by $e = 1, \ldots, q_{H_1}$ (we can assume that these hash queries are distinct) and asks the full private keys corresponding to identities of its choice. $\mathcal{B}$ responds to these queries using the hash simulation and key extraction simulation algorithms described below.

$\mathbf{H_1}$-simulate($\mathbf{ID}_e$)
If $e = \mu$ then answers by $H_1(ID_e) = bP$,
for $i \in S$ give $d_{ID_i} = c_i(bP)$
to the attacker
else choose $d_e \in_R \mathbb{F}_q$, answer by
$H_1(ID_e) = d_e P$ and put the
entry (ID_e, d_e) into L_1.
for $i \in S$ give $d_{ID_i} = c_i(d_e P)$
to the attacker

Keygen-simulate(ID)

If $ID = ID_\mu$ [3] then stop and output "failure"

Otherwise, scan L_1 in order to find a tuple (ID, d) and return dP_{pub} as a full private key

In order to simulate the H_2 oracle, $\mathcal{B}$ maintains a list L_2 that is initially empty. At every time H_2 is queried at a point g_i, $\mathcal{B}$ checks if L_2 already contains an entry (g_i, R_i). If it does, R_i is returned to $\mathcal{A}$. Otherwise, $\mathcal{B}$ chooses a random bitstring $R_i \in \{0,1\}^n$, puts (g_i, R_i) into L_2 and returns R_i to $\mathcal{A}$. At the end of the first stage, $\mathcal{A}$ outputs a pair of plaintexts (m_0,m_1) and an identity ID on which it wishes to be challenged. If the target identity ID is not ID_μ then $\mathcal{B}$ stops and output "failure" (it is assumed that $\mathcal{A}$ chooses to be challenged on an identity of which it asked the hash value). Otherwise, $\mathcal{B}$ takes a random bitstring $R \in_R \{0,1\}^n$ and sends the challenge ciphertext $\sigma =< aP,\ R >$ to $\mathcal{A}$. At the second stage, $\mathcal{A}$ performs a second series of queries which is treated by $\mathcal{B}$ as the first one. At the end of the game, the output of $\mathcal{A}$ is ignored by $\mathcal{B}$. If we denote by $\mathcal{H}$ the event that $\mathcal{A}$ asks the hash value $H_2(\hat{e}(P,P)^{abc})$ during the simulation, one can easily see that $Pr[\mathcal{H}] \geq \epsilon$. Indeed, as explained in [5], we have

$$\begin{aligned} Pr[b = b'] &= Pr[b = b'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] + Pr[b = b'|\mathcal{H}]Pr[\mathcal{H}] \\ &\leq Pr[b = b'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] + Pr[\mathcal{H}] \\ &= \frac{1}{2} + \frac{1}{2}Pr[\mathcal{H}] \end{aligned}$$

since $Pr[b' = b|\neg\mathcal{H}] = 1/2$. On the other side, we also have $Pr[b' = b] \geq Pr[b = b'|\neg\mathcal{H}]Pr[\neg\mathcal{H}] = \frac{1}{2} - \frac{1}{2}Pr[\mathcal{H}]$ and this implies that $\epsilon = |2Pr[b' = b] - 1| \leq Pr[\mathcal{H}]$. Thus, if the simulation does not fail (that is if $\mathcal{A}$ actually chooses to be challenged on ID_μ), the solution of the BDH problem lies on the list L_2 at the end of the simulation and $\mathcal{B}$ just chooses a random element of L_2 as a result. It is easy to see that $\mathcal{B}$'s probability of success is given by $\epsilon/q_{H_1}q_{H_2}$.

□

The scheme presented in this section is a threshold adaptation of the BasicIdent scheme described in [5]. This scheme is malleable and does not resist to adaptive chosen-ciphertext attacks. If we consider a threshold adaptation of the corresponding FullIdent scheme (see [5]), it seems to be impossible to prove its security against chosen-ciphertext attacks because the validity of the ciphertext is checked at the end of the decryption process as pointed out in [10] and [27]. Nevertheless, it is possible to transform it into a threshold identity based cryptosystem achieving the highest level of security in the random oracle model. It is too long to be explained here. A possible method is slightly modifiy the scheme to apply to it the Fouque-Pointcheval generic technique described in [10] in the identity based security model. Another method is more efficient and allows to obtain shorter ciphertexts than in the latter one. This method will be the object of a future paper. The purpose of this one was just to show the relationship between threshold schemes and mediated ones.

4. A MEDIATED PAIRING BASED IDENTITY BASED ENCRYPTION SCHEME

Although we cannot prove the security of the threshold IBE against chosen ciphertext attacks even if the Fujisaki-Okamoto ([11]) transform is applied to it, we can prove that the corresponding mediated scheme is secure against adaptive chosen-ciphertext attacks performed by inside adversaries that do not have access to the user part of private key corresponding to the identity they want to attack. This is a weaker security notion than the semantic security against any inside attack but a stronger one than the security against outside adversaries. This mediated IBE is obtained from the IND-ID-CCA version of the Boneh-Franklin scheme. It consists of four algorithms.

Setup: given a security parameter k, the PKG chooses groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q, a generator P of $\mathbb{G}_1$, a bilinear map $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ and a master-key $s \in \mathbb{F}_q^*$. It then computes $P_{pub} = sP$ and chooses hash functions

$$\begin{aligned} H_1 &: \{0,1\}^* \to \mathbb{G}_1, & H_2 : \mathbb{G}_2 \to \{0,1\}^n \\ H_3 &: \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*, & H_4 : \{0,1\}^n \to \{0,1\}^n \end{aligned}$$

where n denotes the size of plaintexts. The system's public parameters are

$$\mathcal{P} = (P, n, P_{pub}, H_1, H_2, H_3, H_4)$$

(and must be certified by a CA) while the master-key s is kept secret by the PKG.

Keygen: given a user of identity ID, the PKG computes the hash value $Q_{ID} = H_1(ID)$ and $d_{ID} = sQ_{ID}$. Then it chooses a random point $d_{ID,user} \leftarrow_R \mathbb{G}_1^*$ and computes $d_{ID,sem} = d_{ID} - d_{ID,user} \in \mathbb{G}_1$. The PKG gives the partial private key $d_{ID,user}$ to the user and $d_{ID,sem}$ is given to the security mediator.

Encrypt: is the same as in the original scheme ([5]). Given a plaintext M and the recipient's identity ID

1. Compute $Q_{ID} = H_1(ID) \in \mathbb{G}_1$.
2. Choose a binary string $\sigma \leftarrow_R \{0,1\}^n$ and compute $r = H_3(\sigma, M)$.
3. Compute $U = rP \in \mathbb{G}_1$, $g = \hat{e}(P_{pub}, Q_{ID})^r \in \mathbb{G}_2$.
4. The ciphertext is

   $$C =< U, V, W >=< rP, \sigma \oplus H_2(g), M \oplus H_4(\sigma) > .$$

Decrypt: when receiving $C =< U, V, W >$, the recipient forwards it to the SEM. They perform the following tasks in parallel.

SEM:
1. Check if the recipient's identity ID is revoked. If it is, return "Error".
2. Compute $g_{sem} = \hat{e}(U, d_{ID,sem})$ and send it to the user

USER:
1. He computes $g_{user} = \hat{e}(U, d_{ID,user})$.
2. When receiving g_{sem} from the SEM, he computes $g = g_{sem}g_{user}$.
3. He computes $\sigma = V \oplus H_3(g)$ and then $M = W \oplus H_4(\sigma)$.
4. He checks the ciphertext's validity: $U = r'P$ with $r' = H_3(\sigma, M)$.

The consistency is easy to verify from the bilinearity of $\hat{e}$:

$$g = g_{sem} g_{user} = \hat{e}(U, d_{ID,sem} + d_{ID,user}) = \hat{e}(P_{pub}, Q_{ID})^r.$$

As in IB-mRSA, the SEM never sees the user's partial computations (i.e. $\hat{e}(U, d_{ID,user})$) and cannot decrypt messages intended to him. Users never see the SEM's pieces of private key and have no mean to compute them from the tokens $\hat{e}(U, d_{ID_i,sem})$ they receive (since given $c \in \mathbb{G}_2$ and $P \in \mathbb{G}_1$, it is hard to find $R \in \mathbb{G}_1$ such that $\hat{e}(P, R) = c$ if the computational Diffie-Hellman problem is hard in $\mathbb{G}_1$).

Note that the PKG and the SEM are two distinct entities. The SEM remains online all the system's lifetime while the PKG can be put offline once it has delivered private keys to all users of the system.

We also note that the user cannot use the same decryption token $\hat{e}(U, d_{ID,sem})$ twice provided H_3 is a collision-free hash function. Indeed, he could only re-use it for a second message with the same U component and we have $U = rP$ with $r = H_3(\sigma, M)$. Finally, note that the token $\hat{e}(U, d_{ID,sem})$ is useless to any user other than Alice and it does not bring any information about Alice's full private key to anyone since it is a random element of $\mathbb{G}_2$.

It is pointed out in [4] and [3] that the Boneh-Franklin IBE is significantly less efficient than IB-mRSA. It is true but, from a security point of view, IB-mRSA is completely broken if a user can corrupt a SEM. This is not the case for the mediated Boneh-Franklin IBE. Unlike IB-mRSA, a dishonest user who corrupts the SEM cannot decrypt ciphertexts intended to other users (we formally prove it in the security analysis). He is just able to unrevoke previously revoked identities and to revoke other unrevoked ones. The only way for attackers to completely break the scheme is to take control of the PKG. Although less efficient, the mediated pairing based IBE scheme has a significant advantage against IB-mRSA: only one entity is assumed to be completely trusted.

If we compare this revocation method with the built-in revocation method of the Boneh-Franklin IBE (the one consisting in concatenating validity periods to identities), it is clear that the SEM method provides finer grain revocation (since the private key privileges of the user are instantaneously removed) and it does not compell the PKG to periodically re-issue new private keys (this was already pointed out in [9] and [3]).

We will now show that the mediated Boneh-Franklin IBE is weakly semantically secure. That means it is semantically secure against inside attackers that do not have the user part of the private key corresponding to the attacked public key. That is the same level of security as the one achievable by IB-mRSA.

4.1 Security

For the mediated pairing based IBE, we will slightly modifiy the notion of semantic security given in [5].

DEFINITION 3. *We say that a mediated identity based encryption scheme is weakly semantically secure against insider attacks (we can denote by IND-mID-wCCA this security notion: Indistinguishability against weak Chosen-Ciphertext Attacks in the mediated Identity based setting) if no polynomially bounded adversary can have a non-negligible advantage in the following game.*

1. *The challenger runs the Setup algorithm with a security parameter k and sends the system parameters to the adversary.*

2. *The adversary $\mathcal{A}$ performs a polynomially bounded number of queries:*
   - *Decryption query: $\mathcal{A}$ produces an identity ID_i and a ciphertext C_i. The challenger generates both pieces of the private key corresponding to ID_i and sends the result of the decryption of C_i to $\mathcal{A}$.*
   - *User key extraction query: $\mathcal{A}$ produces an identity ID_i and receives the user part of the extracted private key $d_{ID_i,user}$.*
   - *SEM query: $\mathcal{A}$ produces an identity ID_i and a ciphertext C. It receives the token allowing the user of identity ID_i to decrypt the ciphertext.*
   - *SEM key extraction query: $\mathcal{A}$ produces an identity ID and receives the part of the private key d_{ID} corresponding to ID that belongs to the SEM.*

   $\mathcal{A}$ can present its requests adaptively: every request may depend on the answer to the previous ones.

3. *$\mathcal{A}$ chooses two plaintexts $m_0, m_1 \in \mathcal{M}$ and an identity ID on which it wishes to be challenged. It is not allowed to choose an identity for which it made a user key extraction query during the first stage.*

4. *The challenger takes a random bit $b \in_R \{0,1\}$ and computes $C = Encrypt(m_b, ID)$ that is sent to $\mathcal{A}$.*

5. *$\mathcal{A}$ performs a second series of queries just like at the first stage. This time, it cannot ask the plaintext corresponding to C nor the partial private key corresponding to ID. It is allowed to make a SEM request on C for the identity ID.*

6. *Finally, $\mathcal{A}$ produces a bit b' and wins the game if $b' = b$.*

The adversary's advantage is defined to be

$$Adv(\mathcal{A}) := \left|2Pr[b' = b] - 1\right|.$$

This is a weak notion of semantic security against inside attackers (attackers that have access the user part of the private key corresponding to any identity but the one on which they are challenged): we do not prove that a user is completely unable to find any information about a plaintext intended to him without the help of the SEM but we prove that no coalition of dishonest users with the SEM can allow them to find any information about a ciphertext intended to a honest user (that is the reason why the attacker is allowed to ask the user part of private keys associated to other identities than the attacked one and to ask the SEM's pieces of private key for any identity). This is a slightly stronger security notion than the mere security against outsider attacks but it is a weaker one than the strong semantic security against insider attacks (attacks where the adversary has access to the user part of private key for any identity). It seems to be impossible to prove the semantic security against this latter kind of attacks for this version of the mediated Boneh-Franklin IBE. We just prove the weak semantic security against inside attackers.

THEOREM 4.1. *In the random oracle model, assume we have an attacker $\mathcal{A}$ against the mediated pairing based IBE scheme. We assume this attacker is able to win the IND-mID-wCCA2 game with a non negligible advantage ϵ when running in a time t and asking at most q_E user key extraction queries and q_S SEM queries. We then have an adversary $\mathcal{B}$ that is able to win the IND-ID-CCA2 game against the classical Boneh-Franklin scheme with the same advantage ϵ in a time $t' = t + q_E t_A + q_S t_{\mathcal{E}}$ where t_A denotes the time to add two elements of $\mathbb{G}_1$ and $t_{\mathcal{E}}$ is the computation time of the pairing $\hat{e}$.*

Proof. We will use the attacker $\mathcal{A}$ to build an algorithm $\mathcal{B}$ that is able to distinguish ciphertexts produced by the classical Boneh-Franklin IBE. At the beginning of the game, $\mathcal{B}$ receives the BF system parameters from its challenger. It is allowed to ask a polynomially bounded number of key extraction, decryption and random oracle queries to its challenger but it first initializes the IND-mID-CCA2 game it plays with $\mathcal{A}$ by giving him the same system parameters it received from its challenger. $\mathcal{B}$ will act as $\mathcal{A}$'s challenger in the IND-mID-CCA2 game and control the SEM. It maintains a list L_{sem} to store information about the answers to key generation queries (more precisely, L_{sem} will contain the piece of key given to the SEM for each identity). $\mathcal{A}$ performs a first series of queries. $\mathcal{B}$ answers to these queries like this.

- For every query made by $\mathcal{A}$ to random oracles H_1, H_2 and H_3, $\mathcal{B}$ simply forwards them to its challenger and sends the answers back to $\mathcal{A}$.
- Every decryption query is forwarded by $\mathcal{B}$ to its challenger and the answer is sent back to $\mathcal{A}$.
- For a user key extraction query on an identity ID_i, $\mathcal{B}$ first forwards it to its challenger. When it receives the private key d_{ID_i}, it checks whether the list L_{sem} already contains an entry for ID_i. If it does, $\mathcal{B}$ recovers $d_{ID_i,sem}$ from the list and computes $d_{ID_i,user} = d_{ID_i} - d_{ID_i,sem}$ which is sent to $\mathcal{A}$. If no such entry is found in L_{sem}, $\mathcal{B}$ chooses a random point $d_{ID_i,user} \in_R \mathbb{G}_1$ and computes $d_{ID_i,sem} = d_{ID_i} - d_{ID_i,user}$. It gives $d_{ID,user}$ to $\mathcal{A}$ and puts the entry $(ID_i, d_{ID_i,sem})$ into the list L_{sem}.
- For a SEM query on a ciphertext $C_i = (U, V, W)$ and an identity ID_i, $\mathcal{B}$ first searches in the list L_{sem} for an entry containing ID_i. If such an entry is found, it recovers the SEM part of the private key $d_{ID_i,sem}$ and computes the pairing $\hat{e}(U, d_{ID_i,sem})$ which is sent to $\mathcal{A}$ as a decryption token. If no such entry exists, $\mathcal{B}$ chooses a random point $d_{ID_i,sem} \in_R \mathbb{G}_1$, sends $\hat{e}(U, d_{ID_i,sem})$ to $\mathcal{A}$ and puts the entry $(ID_i, d_{ID_i,sem})$ into the list L_{sem}.
- For a SEM key extraction query on an identity ID_i, $\mathcal{B}$ first searches in the list L_{sem} for an entry containing ID_i. If such an entry is found, it recovers the SEM part of the private key $d_{ID_i,sem}$ and returns it to $\mathcal{A}$. Otherwise, $\mathcal{B}$ chooses a random $d_{ID_i,sem} \in_R \mathbb{G}_1$, puts $(ID_i, d_{ID_i,sem})$ into L_{sem} and returns $d_{ID_i,sem}$ to $\mathcal{A}$.

After the first stage, $\mathcal{A}$ produces two plaintexts m_0 and m_1 and an identity ID on which it wishes to be challenged. At this moment, $\mathcal{B}$ forwards m_0 and m_1 to its challenger and chooses ID as challenge identity. It then receives a challenge ciphertext C from its challenger (C is the encryption of m_0 or m_1) and forwards it as a challenge to $\mathcal{A}$.

$\mathcal{A}$ then performs a second series of requests that is treated by $\mathcal{B}$ in the same way as the first one. At the end of the game, $\mathcal{A}$ produces a bit b' for which it believes that C is the encryption of $m_{b'}$ and $\mathcal{B}$ produces the same result b' as $\mathcal{A}$. It is clear that $\mathcal{B}$ wins its IND-ID-CCA2 game if and only if $\mathcal{A}$ wins the game it plays with $\mathcal{B}$. Our new turing machine $\mathcal{B}$ has thus the same advantage as $\mathcal{A}$. The reduction costs are q_S pairing computations and q_E additions in $\mathbb{G}_1$.

□

It is shown in [5] that the Boneh-Franklin scheme is semantically secure in the random oracle model provided the Bilinear Diffie-Hellman problem is hard. The mediated pairing based IBE scheme is thus also semantically secure against outside attackers in the random oracle model. We notice that, although we could not formally prove the security against inside attakcers (and that a user is unable to find any information about a plaintext intended to him without the help of the SEM), we did not find any attack that could help a dishonest user to decrypt a ciphertext alone and bypass the decryption protocol. On the other hand, the mediated IBE can be considered as less sensitive to a key compromise than IB-mRSA as far as a collusion between a user and the SEM does not allow them to break the scheme (they just break the revocation process) while, in IB-mRSA, the system is completely broken if an attacker learns the full public/private key pair of a user. Another advantage of mediated IBE is the shorter size of private keys. Using point compression techniques (that is representing a point by its x-coordinate and a single bit), one can currently have 512 or even 160 bits private keys (by using the same parameters as in [6]) against 1024 for IB-mRSA. The ciphertexts produced by the mediated IBE can also be shorter than those produced by its RSA counterpart if we use 160 bits private keys.

We now have a method to immediately revoke the public key privileges of users in the Boneh-Franklin scheme. This method can be used in some other systems but it does not work for every pairing based cryptosystems. It is easy to see that any public key encryption scheme supporting a two-out-of-two threshold decryption mechanism can be turned into a scheme allowing SEM-aided decryption. The Goldwasser-Micali probabilistic encryption and the modified-Rabin encryption scheme (padded with SAEP) are examples of such systems (see [18] for a description of the threshold adaptations). Since these threshold cryptosystems are provably secure (see [18]) against chosen-ciphertext attacks, it can be shown that, in the corresponding mediated schemes, an attacker that corrupts either the SEM or a user of the system cannot find any information about a ciphertext. Nevertheless, we point out that the underlying threshold cryptosystems are not required to be provably secure against chosen-ciphertext attacks in order for the corresponding mediated schemes to be weakly semantically secure against inside attackers: for example the El Gamal cryptosystem (that is known to be secure against chosen-plaintext attacks under the decisional Diffie-Hellman assumption), when padded with the Fujisaki-Okamoto ([11]) transform (that turns it into an IND-CCA cryptosystem according to [11]), can also support a security mediator that turns it into a weakly semantically secure mediated cryptosystem (it can be shown using an approach similar to the one in this paper).

For signature schemes, we will show that a SEM architecture can be used for the GDH signature described in [6] that produces short signatures using the computational-decisional Diffie-Hellman separation.

5. THE MEDIATED GDH SIGNATURE

Just like encryption schemes, it is easy to see that a SEM architecture can be built into any signature scheme for which a secure threshold version exists (since signature shares are combined into a full signature without any user disclosing his/her share): a threshold signature scheme can be used for setting up a scheme with a security mediator (which is seen as a honest signing player). Unfortunately, only a few signature schemes, such as the RSA or GDH signatures, support a threshold adaptation that could allow the integration of a practical SEM architecture. Probabilistic threshold signatures have the drawback to involve all the signing parties into the random number generation process and this would induce a communication overhead between the user and the SEM at every signature computation.

In this section we describe a mediated version of the GDH signature. The original GDH scheme was devised by Boneh, Lynn and Shacham ([6]) and is based on groups where the computational Diffie-Hellman problem is hard while the decisional one is easy (see [22] and [17]: GDH stands for Gap-Diffie-Hellman and usually denotes this kind of group). These separation groups are built on supersingular elliptic curves and allow to design a 160 bit signature. A threshold version of this scheme has been described in [2] and it clearly allows to build a mediated version of the GDH signature. This adaptation involves a trusted authority (TA) which has to perform the system's key setup. The public parameters are an additive group $\mathbb{G}_1$ of prime order q, and a generator P of $\mathbb{G}_1$.

Keygen: to generate user U_i's key pair, the TA picks random numbers $x_{i,sem}, x_{i,user} \in_R \mathbb{F}_q^*$. He gives the partial private key $x_{i,user}$ to the user and the other piece $x_{i,sem}$ to the SEM. It then computes $R_i = (x_{i,sem} + x_{i,user})P \in \mathbb{G}_1$. U_i's public key is (q, P, R_i).

Sign: to sign a message M, user U_i contacts the SEM and sends it a hash $h(M) \in \mathbb{G}_1$ [4] of the message. They perform the following protocol in parallel.

SEM:
1. Check if user U_i is revoked. If he is, return "Error".
2. Compute $S_{M,sem} = x_{i,sem}h(M)$ and send it to user U_i.

USER:
1. He computes $S_{M,user} = x_{i,user}h(M)$.
2. When receiving $S_{M,sem}$ from the SEM, he computes $S_M = S_{M,sem} + S_{M,user}$.
3. He verifies that S_M is a valid signature on M. If it is, he returns the pair message-signature (M, S_M).

[4]See [6] for an explanation of how to hash onto such a group $\mathbb{G}_1$

Verify: it is exactly as in [6]: compute $h(M)$ and check if $(P, R, h(M), S_M)$ is a valid Diffie-Hellman tuple (i.e. by checking if $e(P, S_M) = e(R, h(M))$).

It is shown in [6] that the original scheme is secure in the random oracle model for any Gap-Diffie-Hellman group (i.e. a group where the decisional Diffie-Hellman problem is easy while the computational one is hard). It is shown in [2] that the threshold version is as secure as the original one since a forgery on the threshold scheme allows to build a forgery on the orginal GDH signature. The unforgeability of the mediated GDH scheme follows directly the threshold signature's one. This allows to prove that a user is unable to create a signature on a message without the help of the SEM.

From an efficiency point of view, we can see that the SEM and the user only have to perform a scalar multiplication in $\mathbb{G}_1$ when generating a signature while the verification still requires two pairing evaluations (this computation overhead is the only disadvantage of mediated GDH when compared to the mRSA signature). If we consider the size of transmitted data, we can see that the SEM only has to send 160 bits to the user with respect to 1024 bits for the mRSA signature: while the mediated pairing based IBE does not offer a reduction of communication cost (since about 1000 bits have to be sent by the SEM to the user) when compared with IB-mRSA, the mediated GDH signature does when it is compared with the mRSA signature.

6. CONCLUSIONS

We have discussed about the provable security of IB-mRSA against inside adversaries and we have shown that the method of [4] to allow fast revocation of RSA keys can also be used by some other public key systems including two pairing based cryptosystems. This results in interesting alternatives to IB-mRSA that is more efficient but can be less secure even though it is provably secure against the same kind of adversaries as mediated IBE.

It is possible to apply this method to any secure threshold cryptosystem to obtain "revokable" asymmetric schemes. Indeed, threshold-RSA schemes ([26]) gave rise to mRSA and the threshold-GDH signature ([2]) is the building block for the mediated-GDH signature. Unfortunately, most of the known secure threshold signature schemes are probabilistic ([23],[29]) and require all the signing parties to collaborate in random number generation operations. This would result in increasing the number of communications between the users and the SEM.

In this paper, we also raised an open question which is the possible existence of a semantically secure threshold adaptation of the Boneh-Franklin cryptosystem. We showed that the existing underlying threshold decryption mechanism in this latter scheme can be used to build a pairing based mediated IBE that is weakly secure against adaptive chosen ciphertext attacks run by insiders even if the corresponding threshold cryptosystem is not. We leave for future research to find a threshold identity based cryptosystem secure against chosen ciphertext attacks.

Finally, we conjecture the SEM method can also be integrated into many other existing public key cryptosystems including the Goldwasser-Micali probabilistic encryption ([14]) and the modified Rabin signature and encryption schemes ([24]) for which efficient threshold adaptations have been described in [18]. Another possible goal for future research is to find signcryption scheme where both the capabilities of the sender and those of the receiver can be removed using this kind of architecture.

7. REFERENCES

[1] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. of the* 1^{st} *ACM Conference on Computer and Communications Secrurity*, pages 62–73. ACM Press, 1993.

[2] A. Boldyreva. Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme. In *Proceedings of PKC'03*, Lecture Notes in Computer Science. Springer, 2003.

[3] D. Boneh, X. Ding, and G. Tsudik. Identity based encryption using mediated RSA. In *proceedings of the* 3^{rd} *Workshop on Information Security Application*, 2002.

[4] D. Boneh, X. Ding, G. Tsudik, and C. Wong. A method for fast revocation of public key certificates and security capabilities. In *proceedings of the* 10^{th} *USENIX Security Symposium*, USENIX, 2001.

[5] D. Boneh and M. Franklin. Identity Based Encryption From the Weil Pairing. In *Advances in Cryptology - Proceedings of Crypto'01*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer, 2001.

[6] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In *Advances in Cryptology - Proceedings of Asiacrypt'01*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.

[7] J. Cha and J. Cheon. An Identity-Based Signature from Gap Diffie-Hellman Groups. In *Proceedings of PKC'03*, Lecture Notes in Computer Science. Springer, 2003.

[8] C.-K. Chu, L. Liu, and W.-G. Tzeng. A Threshold GQ Signature Scheme, 2002. available at http://eprint.iacr.org/2003/016/.

[9] X. Ding and G. Tsudik. Simple Identity-Based Cryptography with Mediated RSA. In *Proceedings of CT-RSA'03*, Lecture Notes in Computer Science. Springer, 2003.

[10] P. Fouque and D. Pointcheval. Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks. In *Advances in Cryptology - Proceedings of Asiacrypt'01*, volume 2248 of *Lecture Notes in Computer Science*, pages 351–368. Springer, 2001.

[11] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology - Proceedings of CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 537–554. Springer, 1999.

[12] E. Fujisaki, T. Okamoto, D. Pointcheval, and J. Stern. RSA-OAEP Is Secure under the RSA Assumption. In *Advances in Cryptology - Proceedings of CRYPTO'01*, volume 2139 of *Lecture Notes in Computer Science*, pages 260 – 274. Springer, 2001.

[13] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. Robust Threshold DSS Signatures. In *Advances in Cryptology - Eurocrypt'96*, volume 1070 of *Lecture Notes in Computer Science*, pages 354–371. Springer, 1996.

[14] S. Goldwasser and S. Micali. Probabilistic Encryption. JCSS 28(2): 270-299 (1984).

[15] L. Guillou and J.-J. Quisquater. A "Paradoxical" Identity-Based Signature Scheme Resulting From Zero-Knowledge. In *Advances in Cryptology - Crypto'88*, volume 0403 of *Lecture Notes in Computer Science*, pages 216–231. Springer, 1988.

[16] F. Hess. Efficient identity based signature schemes based on pairings. In *proceedings of SAC'02*, Lecture Notes in Computer Science. Springer, 2002.

[17] A. Joux and K. Nguyen. Separating Decision Diffie-Hellman from Diffie-Hellman in cryptographic groups, 2001. available at http://eprint.iacr.org/2001/003/.

[18] J. Katz and M. Yung. Threshold Cryptosystems Based on Factoring. In *Advances in Cryptology - proceedings of Asiacrypt 2002*, Lecture Notes in Computer Science. Springer, 2002.

[19] B. Lynn. Authenticated Identity-Based Encryption, 2002. available at http://eprint.iacr.org/2002/072/.

[20] A. Menezes. *Elliptic curve public key cryptosystems.* Kluwer Academic Publishers, 1995.

[21] M. Naor and M. Yung. Public-Key Cryptosystems Provably Secure against Chosen Ciphertext Attacks. In *Proc. of the* 22^{nd} *STOC*, pages 427–437. ACM Press, New York,, 1990.

[22] T. Okamoto and D. Pointcheval. The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes. In *Proc. of of PKC'01*, volume 1992 of *Lecture Notes in Computer Science.* Springer, 2001.

[23] C. Park and K. Kurosawa. New el gamal type threshold digital signature scheme. IEICE Trans., Vol.E79-A, No. 1 (1996) 86-93.

[24] M. Rabin. Digital Signatures and Public Key Functions as Intractable as Factoring. Technical Memo TM-212, Lab. for Computer Science, MIT, 1979.

[25] A. Shamir. Identity Based Cryptosystems and Signature Schemes. In *Advances in Cryptology - Crypto' 84*, volume 0196 of *Lecture Notes in Computer Science.* Springer, 1984.

[26] V. Shoup. Practical threshold Signatures. In *Advances in Cryptology - Eurocrypt'00*, volume 1807 of *Lecture Notes in Computer Science*, pages 208–220. Springer, 2000.

[27] V. Shoup and R. Gennaro. Securing Threshold Cryptosystems against Chosen Ciphertext Attack. In *Advances in Cryptology - Eurocrypt'98*, volume 1403 of *Lecture Notes in Computer Science*, pages 1–16. Springer, 1998.

[28] N. Smart. An identity based authenticated key agreement protocol based on the weil pairing. Electronic Letters, 38(13): 630-632, 2002.

[29] D. Stinson and R. Strobl. Provably Secure Distributed Schnorr Signatures and a (t, n) Threshold scheme for Implicit Certificates. In *proc. of ACISP'01,*, volume 2119 of *Lecture Notes in Computer Science*, pages 417–434. Springer, 2001.