Identity Based Encryption Without Redundancy

Benoît Libert* and Jean-Jacques Quisquater

UCL Crypto Group
Place du Levant, 3, B-1348 Louvain-La-Neuve, Belgium
{libert,jjq}@dice.ucl.ac.be

Abstract. This paper presents a first example of secure identity based encryption scheme (IBE) without redundancy in the sense of Phan and Pointcheval. This modification of the Boneh-Franklin IBE is an hybrid construction that is proved to be secure (using proof techniques borrowed from those for KEM-DEM constructions) in the random oracle model under a slightly stronger assumption than the original IBE and turns out to be more efficient at decryption than the latter. A second contribution of this work is to show how to shorten ciphertexts in a recently proposed multiple-recipient IBE scheme. Our modification of the latter scheme spares about 1180 bits from a bandwidth point of view as, somewhat surprisingly, redundancies are not needed although all elements of the ciphertext space are not reachable by the encryption mapping. This shows that in public key encryption schemes, redundancies may be useless even when the encryption mapping is not a surjection.

Keywords: ID-based encryption, provable security, redundancies.

1 Introduction

Identity based cryptosystems were introduced by Shamir in 1984 [35] in order to simplify key management and avoid the use of digital certificates by letting a public key be publicly derivable from a human-memorizable information on its owner (e-mail address, IP address combined to a user name,...) while the associated private keys must be computed by a trusted Private Key Generator (PKG) thanks to a master secret. This paradigm avoids key management problems arising in traditional public key infrastructures: as long as a public key "is" its owner's identity, nothing must be certified except the PKG's public key and a single public key per domain is thus needed.

Finding a practical identity based encryption scheme (IBE) remained an long-standing open challenge until two independent works of Boneh-Franklin [10] and Cocks [14] which appeared in 2001. Among those solutions, Boneh and Franklin's one happens to be the most practical one.

In provable security purposes, motivated by the design of public key encryption schemes that provably reach the widely admitted required level of security against adaptive chosen-ciphertext attacks [34] in the random oracle model [6],

* This author is supported by the DGTRE's First Europe Program.

J. Ioannidis, A. Keromytis, and M.Yung (Eds.): ACNS 2005, LNCS 3531, pp. 285–300, 2005.

Bellare and Rogaway introduced the notion of plaintext-awareness [7] that captures the general idea to render a decryption oracle useless by making impossible the creation of valid ciphertexts by the adversary. As mentioned in [21], several works [2, 13, 20, 31, 33], gave (knowingly or not) evidence that chosen-ciphertext security is achievable without plaintext-awareness in the random oracle model. Among them, salient results of Phan and Pointcheval [31, 33] showed designs of strongly secure [34] public key encryption schemes for which all ciphertexts are valid and have a corresponding plaintext. Those results were very recently extended by a work [13] exhibiting a 'redundancy-optimal' generic construction of IND-CCA secure public key encryption.

Meanwhile, Kurosawa and Matsuo [28] showed how to turn the DHIES [1] hybrid construction into a redundancy-free encryption scheme in the standard model (but under the non-standard oracle Diffie-Hellman assumption that actually looks as strong as the random oracle model) by removing the message authentication code (MAC) and replacing the IND-CPA symmetric encryption scheme with an IND-CCA one. Their approach is actually a KEM-DEM [17, 18, 36] construction that can also be proved secure in the random oracle model under a more standard assumption in the same way as the oracle Diffie-Hellman assumption was shown [1] to imply the Gap Diffie-Hellman assumption [30] in the random oracle model.

The contribution of the present paper is two-fold. We first extend the technique of Kurosawa and Matsuo to the identity based setting in the random oracle model and show a hybrid variant of the Boneh-Franklin IBE [10] that reaches the IND-ID-CCA2 security level (under a slightly stronger assumption) without introducing redundancies in ciphertexts that are thus shorter than in the $\mathsf{FullIdent}$ scheme of [10]. As a side effect, the decryption operation is more efficient in the resulting scheme than its counterpart in the fully secure original IBE [10]. We mention that an independent work [8] of ours recently considered identity based and certificateless [3] extensions of KEMs. When combined to a suitable symmetric encryption scheme, the first identity based KEM proposed in [8] provides a hybrid IBE that is quite similar to ours. However, as explained in section 3, our variant enjoys a better security reduction in the random oracle model.

The second contribution of the paper is a method to shorten ciphertexts produced by a recently proposed [5] multiple-receiver IBE by the size of an RSA modulus. The modified scheme has the particulary that, although the encryption function is not surjective, no validity checking must be performed at decryption and the decryption algorithm never returns any error message.

2 Preliminaries

2.1 Admissible Bilinear Maps

Let k be a security parameter and q be a $k-$bit prime number. Let us consider groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of the same prime order q. For our purposes, we need a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ satisfying the following properties:

1. Bilinearity: $\forall\ P,Q \in \mathbb{G}_1,\ \forall\ a,b \in \mathbb{Z}_q^*$, we have $e(aP,bQ) = e(P,Q)^{ab}$.
2. Non-degeneracy: $\forall\ P \in \mathbb{G}_1,\ e(P,Q) = 1$ for all $Q \in \mathbb{G}_1$ iff $P = \mathcal{O}$.
3. Computability: $\forall\ P,Q \in \mathbb{G}_1,\ e(P,Q)$ can be efficiently computed.

As shown in [10], such non-degenerate admissible maps over cyclic groups can be obtained from the Weil or the Tate pairing over algebraic curves.

2.2 Underlying Hard Problems

This section recalls definitions of underlying hard problems on which the security of our scheme is shown to rely.

Definition 1. *Given groups $\mathbb{G}_1$ and $\mathbb{G}_2$ of prime order q, a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and a generator P of $\mathbb{G}_1$,*

- *The* ***Bilinear Diffie-Hellman Problem*** *(BDH) in $(\mathbb{G}_1, \mathbb{G}_2)$ is, given elements $\langle P, aP, bP, cP\rangle$ for unknown $a,b,c \in \mathbb{Z}_q$, to compute $e(P,P)^{abc} \in \mathbb{G}_2$.*
- *The* ***Decision Bilinear Diffie-Hellman Problem*** *(DBDH) is to distinguish the distributions $D_1 := \{(P, aP, bP, cP, e(P,P)^{abc}) | a,b,c \overset{R}{\leftarrow} \mathbb{Z}_q^*\}$ and $D_2 := \{(P, aP, bP, cP, h) | a,b,c \overset{R}{\leftarrow} \mathbb{Z}_q^*,\ h \overset{R}{\leftarrow} \mathbb{G}_2\}$. Tuples from D_1 are denoted as "BDH tuples" in the sequel in contrast to those from D_2 which will be called "random tuples" .*
- *The* ***Gap Bilinear Diffie-Hellman Problem*** *(Gap-BDH) in $(\mathbb{G}_1, \mathbb{G}_2)$ consists of, given $\langle P, aP, bP, cP\rangle$, to compute $e(P,P)^{abc}$ with the help of a DBDH oracle.*

The security of the schemes presented in this paper relies on the Gap-BDH assumption which is the intractability of the latter problem.

2.3 Definition of IBE

We recall here the formalism introduced in [10] for identity based encryption. Such a primitive consists of the following algorithms.

Setup: is a probabilistic algorithm run by a private key generator (PKG) that takes as input a security parameter to output a public/private key pair (P_{pub}, mk) for the PKG (P_{pub} is its public key and mk is its master key that is kept secret).

Keygen: is a key generation algorithm run by the PKG on input of a master key mk and a user's identity ID to return the user's private key d_{ID}.

Encrypt: this probabilistic algorithm takes as input a plaintext M, a recipient's identity ID and the PKG's public key P_{pub} to output a ciphertext C.

Decrypt: is a deterministic decryption algorithm that takes as input a ciphertext C and the private decryption key d_{ID} to return a plaintext M or a distinguished symbol $\perp$ if C is not a valid ciphertext.

In sections 3 and 4, we shall use the above definition with the restriction that the decryption algorithm never outputs a rejection message.

2.4 Security Notions

Definition 2. *An identity based encryption scheme (IBE) is said to be* ***adaptively chosen-ciphertext secure*** *(IND-ID-CCA2) if no probabilistic polynomial time (PPT) adversary has a non-negligible advantage in the following game.*

1. *The challenger runs the Setup algorithm on input of a security parameter k and sends the domain-wide parameters to the cca-adversary $\mathcal{A}$.*
2. *In a find stage, $\mathcal{A}$ starts probing the following oracles:*
   - *Key extraction oracle: given an identity ID, it returns the extracted private key associated to it.*
   - *Decryption oracle: given an identity $\mathsf{ID} \in \{0,1\}^*$ and a ciphertext C, it generates the private key d_{ID} associated to ID and returns a plaintext $M \in \mathcal{M}$ or (optionally, in schemes where ciphertexts may be invalid) a distinguished symbol $\perp$ indicating an ill-formed ciphertext.*

   $\mathcal{A}$ can present her queries adaptively in the sense that each query may depend on the answer to previous ones.
3. *$\mathcal{A}$ produces two equal-length plaintexts $M_0, M_1 \in \mathcal{M}$ and a target identity ID^* for which she has not corrupted the private key in stage 2.*
4. *The challenger computes $C = \mathsf{Encrypt}(M_b, \mathsf{ID}^*)$, for a random hidden bit $b \overset{R}{\leftarrow} \{0,1\}$, which is sent to $\mathcal{A}$.*
5. *In the guess stage, $\mathcal{A}$ asks new queries as in the find stage but is restricted not to issue a key extraction request on the target identity ID^* and cannot submit C to the decryption/verification oracle for the identity ID^*.*
6. *$\mathcal{A}$ eventually outputs a bit b' and wins if $b' = b$.*

$\mathcal{A}$'s advantage is defined as $Adv(\mathcal{A}) := |2 \times Pr[b' = b] - 1|$.

As the modification of DHIES presented in [28], our hybrid modification of the Boneh-Franklin IBE [10] makes use of a symmetric cipher (i.e. a deterministic length-preserving symmetric encryption scheme) that is chosen-ciphertext secure in the find-then-guess sense instead of one that only withstands passive attacks as required by the Fujisaki-Okamoto transform [23].

Recall that a symmetric encryption scheme is a triple of algorithms $SE = (K, E, D)$. The key generation algorithm K generates a key $k \overset{R}{\leftarrow} \{0,1\}^\lambda$ for a security parameter λ. The encryption algorithm E takes a key k and a plaintext m to produce a ciphertext $c = E(k, m)$ while the decryption algorithm takes a key k and a ciphertext c to return $m/reject = D(k, c)$. In the definition of chosen-ciphertext security for symmetric encryption schemes, the adversary can query a decryption oracle $D(k, .)$ as well as an encryption oracle $E(k, .)$. We recall below a security notion for ciphers that is considered in [32] and [28].

Definition 3. *A symmetric cipher (E, D) is secure in the IND-CCA sense if no PPT adversary $\mathcal{A}$ has a non negligible advantage in the following game:*

1. *The challenger chooses a key $k \overset{R}{\leftarrow} \{0,1\}^\lambda$.*
2. *$\mathcal{A}$ queries the encryption oracle $E(k, .)$ and the decryption oracle $D(k, .)$.*
2. *$\mathcal{A}$ outputs (m_0, m_1) that were not submitted to $E(k, .)$ (which is deterministic) or obtained from $D(k, .)$ and gets $c^* = E(k, m_b)$ for $b \overset{R}{\leftarrow} \{0,1\}$.*

3. $\mathcal{A}$ issues new queries[1] *as in step 2 but is disallowed to ask for the decryption of c^* and the encryptions of m_0 and m_1.*
4. $\mathcal{A}$ eventually outputs a guess b' for b.

As usual, her advantage is $Adv^{\mathsf{sym}}(\mathcal{A}) := |2 \times Pr[b' = b] - 1|$.

The modes of operations CMC [25] and EME [26] are both length preserving and they were shown to be secure in the sense of IND-CCA if the underlying block cipher is a strong pseudo-random permutation.

3 A Modification of the Boneh-Franklin IBE

This section presents a secure modification of the Boneh-Franklin IBE that is (almost) as efficient as its basic version (that is only secure against chosen-plaintext attacks and was called BasicIdent in [10]) while the original fully secure version of IBE (that was called FullIdent) has computational and bandwidth overheads induced by the application of the Fujisaki-Okamoto transform [23]. The new scheme, that we call Hybrid-IBE, produces shorter ciphertexts than the original FullIdent while it is slightly more efficient for the receiver who does not have to compute a scalar multiplication in $\mathbb{G}_1$ upon decryption.

We have to mention that other transformations such as REACT [29] or GEM [16] could be applied to BasicIdent or to some of its variants to turn them into fully secure identity based encryption schemes without requiring the receiver to

Setup: given security parameters k and λ so that λ is polynomial in k, this algorithm chooses a k-bit prime number q, groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, a generator $P \in \mathbb{G}_1$, a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : {\mathbb{G}_1}^2 \times \mathbb{G}_2 \rightarrow \{0,1\}^\lambda$, as well as a chosen-ciphertext secure cipher (E, D) of keylength λ. It finally picks a master key $\mathsf{mk} := s \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$ and the corresponding public key $P_{pub} := sP \in \mathbb{G}_1$. The system-wide public key is

$$\mathsf{params} := \{q, \mathbb{G}_1, \mathbb{G}_2, P, P_{pub}, e, H_1, H_2, G, n, E, D, \lambda, l\}$$

where n denotes a bound on the size of plaintexts.

Keygen: given an user's identity $\mathsf{ID} \in \{0,1\}^*$, the PKG computes $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in \mathbb{G}_1$ and returns a private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}} \in \mathbb{G}_1$.

Encrypt: to encrypt a message M using P_{pub} and an identity $\mathsf{ID} \in \{0,1\}^*$, compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in \mathbb{G}_1$, pick a random $r \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$ and output the ciphertext

$$C = \langle rP, E_{SK}(M) \rangle$$

where $SK = H_2(Q_{\mathsf{ID}}, rP, e(P_{pub}, Q_{\mathsf{ID}})^r) \in \{0,1\}^\lambda$

Decrypt: upon receiving a ciphertext $C = \langle A, B \rangle \in \mathbb{G}_1 \times \{0,1\}^n$, the recipient returns $M = D_{SK}(B)$ where $SK = H_2(Q_{\mathsf{ID}}, A, e(A, d_{\mathsf{ID}})) \in \{0,1\}^\lambda$.

Fig. 1. Hybrid-IBE

[1] Phan and Pointcheval showed in [32] that post-challenge queries are not of a significant additional help to adversaries.

perform a re-encryption in validity checking concerns. Unfortunately, these transformations should be applied to a OW-PCA[2] variant of BasicIdent for which a part of the ciphertext is obtained by multiplying the message with a $\mathbb{G}_2$ element. As those elements have a representation of at least 1024 bits for recommended parameters (see [10] or [11] for details), ciphertexts would be significantly longer than in our scheme. On the other hand, redundancy-free IBE schemes may also be obtained with the OAEP 3-round generic construction [33] but the security could only be proved in a relaxation of the security model of definition 2 and ciphertexts would also be longer than those of Hybrid-IBE. The security of the latter is claimed by the theorem below.

Theorem 1. *Let us assume that an IND-ID-CCA2 adversary $\mathcal{A}$ has an advantage ϵ against Hybrid-IBE when running in a time τ, asking q_{h_i} queries to oracles h_i ($i = 1, 2$), q_D decryption queries and q_{KE} key extraction queries. Then, for any $0 \leq \nu \leq \epsilon$, there either exists*

- *a PPT algorithm $\mathcal{B}$ to solve the Gap-BDH problem with an advantage*
$$\epsilon' \geq \frac{1}{e(q_{KE}+1)}\big(\epsilon - \frac{q_D}{2^k} - \nu\big)$$
within time $\tau' \leq \tau + (q_{h_1} + q_{KE})\tau_{mult} + q_D \tau_{sym} + q_{h_2}\Phi$
- *an attacker that breaks the IND-CCA security of the symmetric encryption scheme (E, D) with advantage ν within a time τ'*

where e is the base of the natural logarithm, τ_{mult} is the cost of a multiplication in $\mathbb{G}_1$ while τ_{sym} and Φ respectively denote the complexity of a symmetric decryption and the one of a call to the decision oracle.

Proof. Let $(aP, bP, cP, \mathcal{O}_{DBDH})$ be an instance of the Gap-BDH problem where $\mathcal{O}_{DBDH}(.)$ is a decision[3] oracle that, on input (P, aP, bP, cP, ω), answers 1 if $\omega = e(P,P)^{abc}$ and 0 otherwise. We describe an algorithm $\mathcal{B}$ using $\mathcal{A}$ and the latter oracle to compute $e(P,P)^{abc}$.

Algorithm $\mathcal{B}$ initializes $\mathcal{A}$ with the system-wide public key $P_{pub} = aP$ and simulates the adversary's view as explained below. Wlog, we assume that H_1 queries on identities are distinct (otherwise, a list may be used to store inputs and responses) and that any key extraction, decryption or H_2 query involving an identity is preceded by a H_1 query on the same identity.

- H_1 queries: for such a query on an identity ID, $\mathcal{B}$ flips a bit $coin \in \{0, 1\}$ taking the value 0 with probability ξ and the value 1 with probability $1 - \xi$. If $coin = 0$, $\mathcal{B}$ returns $uP \in \mathbb{G}_1$ for some $u \overset{R}{\leftarrow} \mathbb{Z}_q^*$ and it answers $u(bP) \in \mathbb{G}_1$ if $coin = 1$. In both cases, a triple $(\mathsf{ID}, u, coin)$ is stored in a list L_1.

[2] More precisely, this notion would be an identity based flavored extension of the One-Wayness against Plaintext-Checking Attacks characterizing schemes that remain computationally one-way even in the presence of an oracle deciding whether a given ciphertext encrypts a given message. See [29] for a more formal definition.

[3] In fact, it is a restricted decision oracle as some of its inputs (namely P and $aP \in \mathbb{G}_1$) do not change between all queries. The actual assumption is thus slightly weaker than the Gap-BDH one for which additional degrees of freedom are enabled in queries to the DBDH oracle.

- Private key queries: when the private key associated to an identity $\mathsf{ID} \in \{0,1\}^*$ is requested, $\mathcal{B}$ recovers the entry $(\mathsf{ID}, u, coin)$ from L_1. If $coin = 1$, $\mathcal{B}$ aborts since it is unable to coherently answer the query. Otherwise, it returns uP_{pub} as a private key.
- Queries to $H_2(.)$: according to a proof technique already used in [17, 18, 36] for KEMs, these queries are processed using three lists $L_{2,a}$, $L_{2,b}$ and $L_{2,c}$ which are initially empty:
  - $L_{2,a}$ contains triples $(Q_{\mathsf{ID}_i}, A_i, \omega_i)$ to which a hash value was previously assigned and the corresponding digest $h_{2,i} \in \{0,1\}^\lambda$.
  - $L_{2,b}$ contains triples $(Q_{\mathsf{ID}_i}, A_i, \omega_i)$ such that $(Q_{\mathsf{ID}_i}, A_i, \omega_i, h_{2,i})$ exists in $L_{2,a}$ for $h_{2,i} \in_R \{0,1\}^\lambda$ and $\mathcal{O}_{DBDH}(P, Q_{\mathsf{ID}_i}, A_i, P_{pub}, \omega_i) = 1$.
  - $L_{2,c}$ will contain triples $(Q_{\mathsf{ID}_i}, A_i, h_{2,i})$ for which $\mathcal{B}$ has implicitly assigned a value $h_{2,i} \xleftarrow{R} \{0,1\}^\lambda$ to $H_2(Q_{\mathsf{ID}_i}, A_i, \omega_i)$ although the value ω_i such that $\mathcal{O}_{DBDH}(P, Q_{\mathsf{ID}_i}, A_i, P_{pub}, \omega_i) = 1$ is unknown.

  More precisely, when $\mathcal{A}$ submits a triple $(Q_{\mathsf{ID}}, A, \omega)$ to $H_2(.)$,
  - $\mathcal{B}$ first checks if $L_{2,a}$ contains a tuple $(Q_{\mathsf{ID}}, A, \omega, h_2)$ for some $h_2 \in \{0,1\}^\lambda$ (meaning the a hash value was previously assigned to the same input). If it does, h_2 is returned to $\mathcal{A}$.
  - Otherwise, $\mathcal{B}$ submits $(P, Q_{\mathsf{ID}}, A, P_{pub}, \omega)$ to the $\mathcal{O}_{DBDH}(.)$ oracle which decides whether it is a valid BDH tuple.
    - ∗ If it is, then:
      - · If $A = cP$ and $coin = 1$ (i.e. $H_1(\mathsf{ID})$ was defined to be $u(bP)$), $\mathcal{B}$ halts and outputs $\omega^{1/u}$ which is the searched solution. We denote by AskH_2 the event that such a hash query is made .
      - · Otherwise, $\mathcal{B}$ continues and adds $(Q_{\mathsf{ID}}, A, \omega)$ in $L_{2,b}$.
      - · If $L_{2,c}$ contains an entry $(Q_{\mathsf{ID}}, A, h_2)$ for some $h_2 \in \{0,1\}^\lambda$, the tuple $(Q_{\mathsf{ID}}, A, \omega, h_2)$ is stored in $L_{2,a}$ and h_2 is returned to $\mathcal{A}$. Otherwise, $\mathcal{B}$ continues.
    - ∗ It selects a string $h_2 \xleftarrow{R} \{0,1\}^\lambda$, inserts the tuple $(Q_{\mathsf{ID}}, A, \omega, h_2)$ into $L_{2,a}$ and answers h_2 to $\mathcal{A}$.
- Decryption queries: upon receiving a ciphertext $C = \langle A, B \rangle \in \mathbb{G}_1 \times \{0,1\}^n$ and an identity ID, the simulator $\mathcal{B}$ does the following:
  - it checks if $(Q_{\mathsf{ID}}, A, \omega)$ exists in $L_{2,b}$ for some $\omega \in \mathbb{G}_2$. If it does, $\mathcal{B}$ retrieves the tuple $(Q_{\mathsf{ID}}, A, \omega, h_2)$ that must be in $L_{2,a}$ and returns the symmetric decryption $D_{h_2}(B)$ of B using $h_2 \in \{0,1\}^\lambda$ as a symmetric key. Otherwise, it continues.
  - It tests whether $L_{2,c}$ contains a triple $(Q_{\mathsf{ID}}, A, h_2)$ for some string $h_2 \in \{0,1\}^\lambda$. In this case, the latter is used to compute a symmetric decryption $D_{h_2}(B)$ that is returned as a result. Otherwise, a random $h_2 \xleftarrow{R} \{0,1\}^\lambda$ is chosen and $(Q_{\mathsf{ID}}, A, h_2)$ is inserted into $L_{2,c}$ ($\mathcal{B}$ thereby implicitly assigns the hash value h_2 to the oracle H_2 on the unique input $(Q_{\mathsf{ID}}, A, \omega)$ for which $\mathcal{O}_{DBDH}(P, Q_{\mathsf{ID}}, A, P_{pub}, \omega) = 1$ although the relevant $\omega \in \mathbb{G}_2$ is still unknown) while $D_{h_2}(B)$ is returned to $\mathcal{A}$.

After the find stage, $\mathcal{A}$ comes with messages $M_0, M_1 \in \{0,1\}^n$ and a target identity ID^*. Let $(\mathsf{ID}^*, u^*, coin^*)$ be the corresponding entry in L_1. If $coin^* = 0$,

$\mathcal{B}$ aborts and reports "failure" because, in such a situation, $\mathcal{A}$ is of no help in $\mathcal{B}$'s endeavour. Otherwise, it sets $A^* = cP \in \mathbb{G}_1$, checks whether $L_{2,c}$ contains an entry $(Q_{\mathsf{ID}^*}, A^*, h_2^*)$ for $Q_{\mathsf{ID}^*} = h_1(\mathsf{ID}^*)$ and some $h_2^* \in \{0,1\}^\lambda$ (if not, $\mathcal{B}$ inserts it for a string $h_2 \overset{R}{\leftarrow} \{0,1\}^\lambda$ of its choice) to compute a symmetric encryption $B^* = E_{h_2^*}(M_d)$, for $d \overset{R}{\leftarrow} \{0,1\}$, and return the challenge $C^* = \langle A^*, B^* \rangle$. In the unlikely event (its probability is less than $q_D/2^k$) that C^* was previously submitted to the decryption oracle for the identity ID^*, $\mathcal{B}$ aborts.

At the second stage, $\mathcal{B}$ processes all queries as above and $\mathcal{A}$ eventually produces a bit d'. In a real game, we have $\Pr[d' = d] = (\epsilon + 1)/2$ and, provided the simulation is perfect, the latter equality still holds as $\mathcal{A}$'s view is indistinguishable from a real environment. It can be showed that the simulation is imperfect with a probability smaller than $e^{-1}(q_{KE}+1)^{-1}(1-q_D/2^k)$. Indeed, let us define the following events:

E_1: $\mathcal{B}$ does not abort as a result of a private key extraction query.
E_2: $\mathcal{B}$ does not abort during the challenge phase because $\mathcal{A}$ chooses a target identity ID^* for which $coin^* = 0$.
E_3: $\mathcal{B}$ does not fail because the constructed challenge C^* was previously queried to the decryption oracle for the identity ID^*.

Those events are independent. We observed that $\Pr[E_3] \geq 1 - q_D/2^k$. We also have $\Pr[E_1] = (1 - 1/(q_{KE}+1))^{q_{KE}} \geq 1/e$ (as shown in the proof technique of [15]) and $\Pr[E_2] = 1/(q_{KE}+1)$. It comes that if $\mathsf{Fail} = \neg E_1 \vee \neg E_2 \vee \neg E_3$, we have $\Pr[\neg\mathsf{Fail}] = e^{-1}(q_{KE}+1)^{-1}(1-q_D/2^k)$.

On the other hand, if AskH_2 does not occur and thus if $\mathcal{A}$ never makes the relevant $h_2(Q_{\mathsf{ID}^*}, A^*, \omega^*)$ query during the game, the only way for her to produce a correct guess for d is to succeed in a chosen-ciphertext attack against the symmetric cipher (E, D): indeed, in the latter case, each decryption query on a ciphertext $C' = (A^*, B)$, with $B \neq B^*$, for the target identity ID^* corresponds to a symmetric decryption request for a completely random key SK^*. It follows that, if (E, D) is a chosen-ciphertext secure symmetric encryption scheme, the event AskH_2 is very likely to happen and $\mathcal{B}$ is able to extract the Gap-BDH solution.

More formally, for any event E, if we denote by $\mathrm{pr}[E]$ the conditional probability $\Pr[E|\neg\mathsf{Fail}]$, we have

$$\begin{aligned}\mathrm{pr}[d' = d] &= \mathrm{pr}[d' = d|\mathsf{AskH}_2]\mathrm{pr}[\mathsf{AskH}_2] + \mathrm{pr}[d' = d|\neg\mathsf{AskH}_2]\mathrm{pr}[\neg\mathsf{AskH}_2] \\ &\leq \mathrm{pr}[\mathsf{AskH}_2] + \mathrm{pr}[d' = d|\neg\mathsf{AskH}_2](1 - \mathrm{pr}[\mathsf{AskH}_2])\end{aligned}$$

and, since $\mathrm{pr}[d' = d] = (\epsilon + 1)/2$ and $\mathrm{pr}[d' = d|\neg\mathsf{AskH}_2] \leq (\nu + 1)/2$, it comes that

$$\frac{\epsilon+1}{2} \leq \frac{\nu+1}{2} + \frac{1-\nu}{2}\mathrm{pr}[\mathsf{AskH}_2] \leq \frac{\nu+1}{2} + \frac{1}{2}\mathrm{pr}[\mathsf{AskH}_2]$$

and hence $\mathrm{pr}[\mathsf{AskH}_2] \geq \epsilon - \nu$. When going back to non-conditional probabilities, we find the announced lower bound

$$\Pr[\mathsf{AskH}_2 \wedge \neg\mathsf{Fail}] \geq \frac{1}{e(q_{KE}+1)}\big(1 - q_D 2^{-k}\big)\big(\epsilon - \nu\big) > \frac{1}{e(q_{KE}+1)}\big(\epsilon - \frac{q_D}{2^k} - \nu\big)$$

on $\mathcal{B}$'s probability of success. □

The reason for which the symmetric encryption key is computed using a hash function taking U and Q_{ID} among its input is that it provides us with a more efficient reduction: the security of the scheme can still be proved if the symmetric key is derived from the sole bilinear Diffie-Hellman key but the reduction then involves $q_D q_{H_2}$ calls to the decision oracle. A similar observation was made by Cramer and Shoup [17] in their security proof of the Hashed El Gamal KEM.

The reduction given in theorem 1 is more efficient than the one obtained from the BDH assumption through the Fujisaki-Okamoto tranform [23] in the original IBE. Although our proof relies on a stronger assumption, we believe that this is a fact of interest because a tight reduction from a given assumption should always be preferred to a loose reduction from a potentially weaker assumption as argued in [27]. On the other hand, the Gap-BDH assumption does not appear as a much stronger assumption than the (already non-standard) BDH assumption.

Interestingly, if we compare our security reduction for Hybrid-IBE with the one of Galindo [24] for another variant of the Boneh-Franklin IBE obtained through the first Fujisaki-Okamoto transform [22], we find that ours is as efficient as Galindo's one (which relies on the DBDH assumption) but our Hybrid construction happens to be more efficient (as no re-encryption is needed for the receiver) and produces shorter ciphertexts thanks to the absence of redundancy.

As for Galindo's variant [24], an essentially optimal reduction can be obtained for Hybrid-IBE by applying a trick suggested in [27] at the cost of an additional pairing computation at encryption. We also mention that a similar technique can be applied to a variant of a certificateless encryption scheme [3] proposed in [4].

4 Shortening Ciphertexts in the Multiple-Receiver Case

A recent result [5] of Baek, Safavi-Naini and Susilo showed how to efficiently encrypt a message intended to N distinct recipients from their identities without having to compute more than one pairing. The security of their scheme in the selective-ID model considered in [12] and [9] (that is, the attacker has to announce the set of identities it intends to attack at the beginning of the game even before seeing the master-key of the scheme) was shown to rely on the Gap-BDH assumption and was obtained through the REACT transformation.

It is not hard to see that the construction we used in the previous section can also help to shorten the ciphertexts produced by the single-recipient version of the latter scheme since, in the same way as the use of an IND-CCA cipher instead of an IND-CPA one allows removing the message authentication code (MAC) from the DHIES construction [1] as shown in [28], it also allows removing the checksum from REACT (so that the resulting construction produces as short ciphertexts as the GEM conversion).

Interestingly, the same trick applies to the multiple-receiver case considered in [5] if we accept a loss of efficiency in the security reduction. The latter then involves a number of calls to the decision oracle that depends on the square of the number of adversarial queries. We thus believe the resulting hybrid multiple-recipient scheme (called Hybrid-IBE2 and depicted on figure 2) to be of interest because of its ciphertexts which are about 1184 bits shorter than in [5] as no checksum is needed and there is no need to encode a part of ciphertext as a $\mathbb{G}_2$ element.

4.1 The Selective-ID Security Model for Multiple-Receiver Schemes

The formal definition [5] of a multiple-receiver IBE scheme is identical to the definition of section 2.3 with two essential syntactic differences. First, the encryption algorithm takes as inputs a message M, system-wide parameters params and several identities $(\mathsf{ID}_1, \ldots, \mathsf{ID}_t)$ to produce an encryption C of M under $(\mathsf{ID}_1, \ldots, \mathsf{ID}_t)$. Secondly, the decryption algorithm is given a ciphertext C together with a receiver number $i \in \{1, \ldots, t\}$ and the associated private key d_{ID_i} and returns either a plaintext or a rejection message $\perp$. In the scheme described in this section, a ciphertext is never rejected.

Similarly to the authors of [5], we establish the security of our multiple-receiver construction in the selective-ID model recalled in the next definition. The reason for this is that, as in [5], a security reduction in the strongest model (where target identities are adaptively chosen) involves a loss of concrete security which is exponential in the number of receivers.

Definition 4 ([5]). *A multiple-receiver IBE scheme is said to be selective-ID secure against chosen-ciphertext attacks (or IND-sMID-CCA secure) if no PPT adversary has a non-negligible advantage in the game below.*

1. *The attacker $\mathcal{A}$ outputs a set of target identities* $(\mathsf{ID}_1^*, \ldots, \mathsf{ID}_t^*)$.
2. *The challenger $\mathcal{CH}$ runs the setup algorithm, transmits the public parameters* params *to $\mathcal{A}$ and keeps the master key* mk *to itself.*
3. *$\mathcal{A}$ issues a number of key extraction queries (as in definition 2) for identities* $\mathsf{ID} \neq \mathsf{ID}_1^*, \ldots, \mathsf{ID}_t^*$ *and decryption queries, each of which is denoted by* (C, ID_i) *for some* $i \in \{1, \ldots, t\}$.
4. *$\mathcal{A}$ produces messages (M_0, M_1) and obtains a challenge ciphertext* $C^* = \mathsf{Encrypt}(M_b, \mathsf{params}, \mathsf{ID}_1^*, \ldots, \mathsf{ID}_t^*)$, *for a random bit* $b \overset{R}{\leftarrow} \{0, 1\}$, *from $\mathcal{CH}$.*
5. *$\mathcal{A}$ issues new queries with the same restriction as in step 3. Additionally, she is disallowed to ask for the decryption of C^* for any one of the target identities* $(\mathsf{ID}_1^*, \ldots, \mathsf{ID}_t^*)$.
6. *$\mathcal{A}$ outputs a bit $b' \in \{0, 1\}$ and wins if $b' = b$. Her advantage is again* $Adv(\mathcal{A}) = |2 \times Pr[b' = b] - 1|$.

4.2 The Scheme

A strange feature of Hybrid-IBE2 is that, unlike Hybrid-IBE, it is not a public key encryption scheme without redundancy in the strict sense of [31] and [33]. Indeed, in the simplest single-recipient scenario, elements $\langle U, V, W\rangle$ of the ciphertext space for which $\log_P(U) \neq \log_{Q_{\mathsf{ID}}+Q}(V)$ can never be reached by a correct application of the encryption function and thus do not correspond to

Setup: given security parameters k and λ, this algorithm selects a k-bit prime q, groups $\mathbb{G}_1, \mathbb{G}_2$ of order q, a generator $P \in \mathbb{G}_1$, a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^\lambda$ and an IND-CCA cipher (E, D) of keylength λ. It also picks $Q \overset{R}{\leftarrow} \mathbb{G}_1$, a master key $\mathsf{mk} := s \overset{R}{\leftarrow} \mathbb{Z}_q^*$ and the public key is $(P_{pub} := sP, Q)$. The public parameters are

$$\mathsf{params} := \{q, \mathbb{G}_1, \mathbb{G}_2, P, Q, P_{pub}, e, H_1, H_2, n, E, D, \lambda\}$$

where n denotes a bound on the size of plaintexts.

Keygen is the same as in Hybrid-IBE.

Encrypt: to encrypt a message M under the system-wide public key P_{pub} for identities $\mathsf{ID}_1, \ldots, \mathsf{ID}_t \in \{0,1\}^*$, compute $Q_{\mathsf{ID}_i} = H_1(\mathsf{ID}_i) \in \mathbb{G}_1$ for $i = 1, \ldots, t$, pick a random $r \overset{R}{\leftarrow} \mathbb{Z}_q^*$ and output the ciphertext

$$C = \langle U, V_1, \ldots, V_t, W, \mathcal{L} \rangle = \langle rP, rQ_{\mathsf{ID}_1} + rQ, \ldots, rQ_{\mathsf{ID}_t} + rQ, E_{SK}(M), \mathcal{L} \rangle$$

where $SK = H_2(U, V_1, \ldots, V_t, \mathcal{L}, \omega) \in \{0,1\}^\lambda$ with $\omega = e(P_{pub}, Q)^r$ and $\mathcal{L}$ is a label indicating how each part of ciphertext is associated to each receiver.

Decrypt: given $C = \langle U, V_1, \ldots, V_t, W, \mathcal{L} \rangle \in {\mathbb{G}_1}^{t+1} \times \{0,1\}^n$ and his private key $d_{\mathsf{ID}_i} = sQ_{\mathsf{ID}_i}$, receiver $i \in \{1, \ldots, t\}$ computes $\omega = e(P_{pub}, V_i)/e(U, d_{\mathsf{ID}_i})$ and returns $M = D_{SK}(W)$ where $SK = H_2(U, V_1, \ldots, V_t, \mathcal{L}, \omega) \in \{0,1\}^\lambda$.

Fig. 2. Hybrid-IBE2

any plaintext. Nevertheless, the decryption oracle never returns an error message indicating a badly formed ciphertext and the receiver does not have to perform a validity checking (that could be made here by solving a DDH problem in $\mathbb{G}_1$) when decrypting a ciphertext. In any case, for an input $\langle U, V, W \rangle$, the decryption algorithm returns a symmetric decryption of W using a hash value of $e(P_{pub}, V)/e(U, d_{\mathsf{ID}})$ and other ciphertext components (it is essential to include them among the inputs of H_2 to prevent the scheme from being malleable) as a symmetric key so that inconsistent ciphertexts are decrypted into random messages but consistently encrypted messages are always correctly decrypted.

From a security point of view, theorem 2 shows that ill-formed ciphertexts do not have to be detected and that their existence does not induce security concerns: in the security proof, the simulator is always able to provide an attacker with a perfectly consistent emulation of the decryption oracle thanks to the power of the decision oracle. This result shows that the existence of incorrectly formed ciphertexts does not necessarily require the recipient to perform a validity checking for chosen-ciphertext security purposes.

Theorem 2. *Let $\mathcal{A}$ be an adversary having an advantage ϵ against the IND-sMID-CCA2 security of Hybrid-IBE2 when running in a time τ, making q_{H_i} queries to random oracles H_i $(i = 1, 2)$, q_D decryption queries and q_{KE} private key extraction queries. Then, for any $0 \leq \nu \leq \epsilon$, there either exists*

– *a PPT algorithm $\mathcal{B}$ to solve the Gap-BDH problem with an advantage*

$$\epsilon' \geq \epsilon - \nu - \frac{q_D}{2^k}$$

within time $\tau' \leq \tau + (q_{H_1} + q_{KE})\tau_{mult} + (2q_D + 1)q_{H_2}\Phi + q_D(\tau_{sym} + \tau_p)$

- *an attacker that breaks the IND-CCA security of the symmetric encryption scheme (E, D) with an advantage ν within a time τ'*

where τ_{mult} is the time to perform a multiplication in $\mathbb{G}_1$, τ_{sym} denotes the cost of a symmetric decryption, τ_p the cost of a pairing evaluation and Φ the complexity of a call to the decision oracle.

Proof. Given an instance $(aP, bP, cP, \mathcal{O}_{DBDH})$ of the Gap-BDH problem, $\mathcal{B}$ launches the adversary $\mathcal{A}$ who first announces the set of identities $(\mathsf{ID}_1^*, \ldots, \mathsf{ID}_t^*)$ that she intends to attack. She then obtains the domain-public key $(P_{pub} = aP, Q = bP)$ from $\mathcal{B}$ that simulates her view as follows.

- queries $H_1(\mathsf{ID}_i)$: $\mathcal{B}$ draws $l_i \stackrel{R}{\leftarrow} \mathbb{Z}_q^*$. If $\mathsf{ID}_i = \mathsf{ID}_j^*$ for some $j \in \{1, \ldots, t\}$, $\mathcal{B}$ returns $l_i P - Q$. Otherwise, it responds with $l_i P$ (so that the associated private key $d_{\mathsf{ID}_i} = l_i(aP)$ is always computable).

$H_2(.)$ queries and decryption queries are handled using two lists L_2 and L_2' which are initially empty.

- For decryption queries on a ciphertext $C = \langle U, V_1, \ldots, V_t, W, \mathcal{L} \rangle$ for an identity ID_i and a receiver number $i \in \{1, \ldots, t\}$, the simulator's strategy is to always return a symmetric decryption of W under a symmetric key that appears (or will subsequently appear) to $\mathcal{A}$ as a hash value of the tuple

  $$(U, V_1, \ldots, V_t, \mathcal{L}, e(P_{pub}, V_i)/e(U, d_{\mathsf{ID}_i}))$$

  according to the specification of the decryption algorithm under recipient i's private key d_{ID_i}. To do so, $\mathcal{B}$ first retrieves $Q_{\mathsf{ID}_i} = H_1(\mathsf{ID}_i) \in \mathbb{G}_1$ and then searches list L_2 for entries of the form $(U, V_1, \ldots, V_t, \mathcal{L}, \omega_j, \kappa_j)$ for pairs $(\omega_j, \kappa_j) \in \mathbb{G}_2 \times \{0,1\}^\lambda$ indexed by $j \in \{1, \ldots, q_{h_2}\}$.
  - For each one of such entries, $\mathcal{B}$ checks whether

    $$\mathcal{O}_{DBDH}(P, Q_{\mathsf{ID}}, U, P_{pub}, e(P_{pub}, V_i)/\omega_j) = 1$$

    (meaning that $\omega_j = e(P_{pub}, V_i)/e(U, d_{\mathsf{ID}_i})$). If the unique $\omega \in \mathbb{G}_2$ satisfying the latter relation is found, $\mathcal{B}$ uses the corresponding κ to compute $M = D_\kappa(W)$ and return the result to $\mathcal{A}$.
  - If no entry of L_2 satisfies the above condition, $\mathcal{B}$ draws $\kappa \stackrel{R}{\leftarrow} \{0,1\}^\lambda$, stores the information $(U, V_1, \ldots, V_t, \mathcal{L}, ?, \kappa, e(P_{pub}, V_i), Q_{\mathsf{ID}_i})$, where ? denotes an unknown $\mathbb{G}_2$ element, into L_2' and returns $M = D_\kappa(W)$ as a plaintext.
- $H_2(.)$ queries: for such a query on an input $(U, V_1, \ldots, V_t, \mathcal{L}, \omega)$, $\mathcal{B}$ halts and outputs ω as a result if $\mathcal{O}_{DBDH}(P, aP, bP, cP, \omega) = 1$. Otherwise, it first checks whether H_2 was previously defined for that input. If so, the previously defined value is returned. Otherwise, $\mathcal{B}$ checks if the auxiliary list L_2' contains an entry of the form $(U, V_1, \ldots, V_t, \mathcal{L}, ?, \kappa, \gamma, Q_{\mathsf{ID}_i})$ for some pair $(\kappa, \gamma) \in \{0,1\}^\lambda \times \mathbb{G}_2$ and some $Q_{\mathsf{ID}_i} \in \mathbb{G}_1$.

- If it does, $\mathcal{B}$ checks if $\mathcal{O}_{DBDH}(P, Q_{\mathsf{ID}_i}, U, P_{pub}, \gamma/\omega) = 1$ for each one of such triples $(\kappa, \gamma, Q_{\mathsf{ID}_i})$. If the decision oracle positively answers for one of them, the corresponding κ is returned as a hash value.
- Otherwise, $\mathcal{B}$ returns a randomly sampled string $\kappa \overset{R}{\leftarrow} \{0,1\}^\lambda$

In both case, $\mathcal{B}$ stores the information $(U, V_1, \ldots, V_t, \mathcal{L}, \omega, \kappa)$ in L_2.

In the challenge step, $\mathcal{A}$ produces messages $M_0, M_1 \in \{0,1\}^n$. The simulator $\mathcal{B}$ computes $U^* = cP, V_1^* = l_1^*(cP), \ldots, V_t^* = l_t^*(cP)$ and the corresponding label $\mathcal{L}^*$ where $l_1^*, \ldots, l_t^* \in \mathbb{Z}_q^*$ are finite field elements for which $H_1(\mathsf{ID}_j^*) = l_j^* P - Q$ for $j \in \{1, \ldots, t\}$. It then chooses a random $\kappa^* \overset{R}{\leftarrow} \{0,1\}^\lambda$ and computes $W^* = E_{\kappa^*}(M_d)$ for $d \overset{R}{\leftarrow} \{0,1\}$. The challenge ciphertext is set to $C^* = \langle U^*, V_1^*, \ldots, V_t^*, W^*, \mathcal{L}^* \rangle$. In the unlikely event (its probability is less than $q_D/2^k$) that C^* was queried to the decryption oracle at the find stage, $\mathcal{B}$ aborts.

All queries of the guess stage are processed as in the find stage and $\mathcal{A}$ eventually produces a bit d'. From a similar analysis to the one of theorem 1, we find that the relevant query $H_2(U^*, V_1^*, \ldots, V_t^*, \mathcal{L}^*, \omega^*)$, where $\omega^* = e(P,P)^{abc}$ is very likely to be made by $\mathcal{A}$ during the simulation. The Gap-BDH solution can thus be detected when handling $H_2(.)$ queries. □

5 Another Way to Avoid the Re-encryption in IBE

This section presents an alternative method to achieve the chosen-ciphertext security in the original IBE system [10] without requiring a re-encryption for validity checking upon decryption and without having to encode of piece of ciphertext as a long $\mathbb{G}_2$ element. This method introduces a minimal amount of redundancies in ciphertexts (only 160 additional bits are needed w.r.t to BasicIdent) and is actually an extension of a construction originally designed by Bellare and Rogaway [6] for trapdoor permutations. Recall that this construction produces ciphertexts of the form $E(m,r) = \langle f(r), m \oplus G(r), H(m,r) \rangle$, where r denotes a random coin, f is a trapdoor permutation and G, H are random oracles. Actually, this construction (that was previously generalized into a generic conversion in [29]) can be instantiated with more general number theoretic primitives. For example, it can be applied to the El Gamal [19] cryptosystem and to the Boneh-Franklin identity based encryption scheme. The resulting scheme is called XBR-IBE (as a shorthand for eXtended Bellare-Rogaway like IBE) and depicted on figure 3.

As for the schemes described in the previous sections, the security relies on the Gap-BDH assumption. The security proof is omitted here because of space limitation but will be given in the full version of this paper.

Theorem 3. *If an IND-ID-CCA2 adversary $\mathcal{A}$ has advantage ϵ against XBR-IBE in a time τ when asking q_{h_i} queries to oracles h_i ($i = 1,2,3$), q_D decryption queries and q_{KE} private key queries, then a PPT algorithm $\mathcal{B}$ can solve the Gap-BDH problem with an advantage $\epsilon' \geq (e(q_{KE}+1))^{-1}(\epsilon - \frac{q_D}{2^{k-1}})$ within time $\tau' \leq \tau + (q_{h_1} + q_{KE})\tau_{mult} + 2(q_{h_2} + q_{h_3})\Phi$ where τ_{mult} is the cost of a scalar*

Setup: is the same as in Hybrid-IBE except that no cipher is needed and hash functions are $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \{0,1\}^* \rightarrow \{0,1\}^{k_1}$ and $H_3 : \mathbb{G}_2 \rightarrow \{0,1\}^n$ where n still denotes the size of plaintexts and k_1 is a security parameter which is polynomial in $k = \log(|\mathbb{G}_1|)$.

Keygen is the same as in Hybrid-IBE and Hybrid-IBE2.

Encrypt: to encrypt a message M using an identity $\mathsf{ID} \in \{0,1\}^*$, compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in \mathbb{G}_1$, pick a random $r \overset{R}{\leftarrow} \mathbb{Z}_q^*$ and output the ciphertext

$$C = \left\langle rP, m \oplus H_3(g_{\mathsf{ID}}^r), H_2(m||rP||\mathsf{ID}||g_{\mathsf{ID}}^r)\right\rangle$$

where $g_{\mathsf{ID}} = e(P_{pub}, Q_{\mathsf{ID}}) \in \mathbb{G}_2$.

Decrypt: given $C = \langle U, V, W\rangle$, compute $\omega = e(U, d_{\mathsf{ID}})$ and $m = V \oplus H_3(\omega) \in \{0,1\}^n$. Output $m \in \{0,1\}^n$ if $W = H_2(m||U||\mathsf{ID}||\omega)$ and $\perp$ otherwise.

Fig. 3. XBR-IBE

multiplication in $\mathbb{G}_1$, Φ denotes the cost of a call to the DBDH oralce and e is the base of the natural logarithm.

Interestingly, a similar method also applies to Baek et al.'s multiple-receiver scheme [5] and yields shorter ciphertexts (about 1024 bits are spared) which have the form $\langle rP, V_1, \ldots, V_t, m \oplus H_3(\omega), H_2(m, rP, V_1, \ldots, V_t, \mathcal{L}, \omega), \mathcal{L}\rangle$ where $V_i = rH_1(\mathsf{ID}_i) + rQ$ for $i = 1, \ldots, t$, $\omega = e(P_{pub}, Q)^r$ and the label $\mathcal{L}$ contains receivers'identities $\mathsf{ID}_1, \ldots, \mathsf{ID}_t$. The security of this second multiple-receiver scheme still relies the Gap-BDH assumption.

6 Conclusion

We presented two methods to avoid the re-encryption in chosen-ciphertext secure IBE systems. Among those methods, the hybrid construction yields more compact ciphertexts thanks to the absence of redundancies. We also explained how to shorten ciphertexts produced by a multiple-receiver IBE scheme. We finally gave an example of secure public key encryption scheme for which no validity checking is needed at decryption although the encryption mapping is not surjective.

Acknowledgements

Thanks to Damien Vergnaud for his helpful comments and to the anonymous referees for their useful feedback.

References

1. M. Abdalla, M. Bellare, P. Rogaway, *The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES*, in Topics in Cryptology – CT-RSA'01, LNCS 2020, pp. 143–158, Springer, 2001.

2. M. Abe, *Combining Encryption and Proof of Knowledge in the Random Oracle Model*, Topics in Cryptology – CT-RSA'02, LNCS 2271, Springer, pp. 277–289, 2002.
3. S.-S. Al-Riyami , K.G. Paterson, *Certificateless Public Key Cryptography*, in Advances in Cryptology – Asiacrypt'03, LNCS 2894, pp. 452–473, 2003.
4. S.S. Al-Riyami , K.G. Paterson, *CBE from CL-PKE: A Generic Construction and Efficient Schemes* , in proc. of PKC'05, LNCS 3386, pp. 398–415, Springer, 2005.
5. J. Baek, R. Safavi-Naini, W. Susilo, *Efficient Mutli-Receiver Identity-Based Encryption and Its Application to Broadcast Encryption,* in proc. of PKC'05, LNCS 3386, pp. 380–397, Springer, 2005.
6. M. Bellare, P. Rogaway, *Random oracles are practical: A paradigm for designing efficient protocols*, in proc. of the 1^{st} ACM Conference on Computer and Communications Security, pp. 62-73, 1993.
7. M. Bellare, P. Rogaway, *Optimal asymmetric encryption – How to encrypt with RSA*, in Advances in Cryptology – Eurocrypt 94, LNCS 950, Springer, pp. 92–111, 1995.
8. K. Bentahar, P. Farshim, J. Malone-Lee, N.P. Smart, *Generic Constructions of Identity-Based and Certificateless KEMs*, Cryptology ePrint Archive Report, available from http://eprint.iacr.org/2005/058.
9. D. Boneh, X. Boyen, *Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles*, in Advances in Cryptology – Eurocrypt'04, LNCS 3027, Springer,pp. 223–238, 2004.
10. D. Boneh, M. Franklin, *Identity Based Encryption From the Weil Pairing*, in Advances in Cryptology – Crypto'01, LNCS 2139, pp. 213–229, Springer, 2001.
11. D. Boneh, B. Lynn, H. Shacham, *Short signatures from the Weil pairing*, in Advances in Cryptology – Asiacrypt'01, LNCS 2248, pp. 514–532. Springer, 2001.
12. R. Canetti, S. Halevi, J. Katz, *A Forward Secure Public Key Encryption Scheme*, in Advances in Cryptology – Eurocrypt'03, LNCS 2656, pp. 254–271, Springer, 2003.
13. Y. Chui, K. Kobara, H. Imai, *A Generic Conversion with Optimal Redundancy*, in Topics in Cryptology – CT-RSA'05, LNCS 3376, Springer, pp. 104–117, 2005.
14. C. Cocks, *An Identity Based Encryption Scheme Based on Quadratic Residues*, 8th IMA International Conference, LNCS 2260, Springer, pp. 360-363, 2001.
15. J.-S. Coron. *On the Exact Security of Full Domain Hash*, in Advances in Cryptology – Crypto'00, LNCS 1880, pp. 229–235, 2000.
16. J.-S. Coron, H. Handschuh, M. Joye, P. Paillier, D. Pointcheval, C. Tymen, *GEM: a Generic Chosen-Ciphertext Secure Encryption Method*, in Topics in Cryptology – CT-RSA'02, LNCS 2271, pp. 263–276, Springer, 2002.
17. R. Cramer, V. Shoup, *Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack*, in SIAM Journal of Computing 33:167-226, 2003.
18. A. Dent, *A Designer's Guide to KEMs*, in Cryptography and Coding, 9th IMA International Conference, pp. 133–151, Springer, 2003.
19. T. El Gamal, *A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms* , Advances in Cryptology – Crypto'84, LNCS 0196, pp. 10–18, Springer, 1984.
20. P.A. Fouque, D. Pointcheval, *Threshold Cryptosystems Secure against Chosen-Ciphertext Attacks*, Advances in Cryptology – Asiacrypt'01, LNCS 2248, Springer, pp. 351–368, 2001.
21. E. Fujisaki, *Plaintext Simulatability*, Cryptology ePrint Archive Report, available from http://eprint.iacr.org/2004/218.

22. E. Fujisaki, T. Okamoto, *How to Enhance the Security of Public-Key Encryption at Minimum Cost*, in proc. of PKC'99, LNCS 1560, pp. 53–68. Springer, 1999.
23. E. Fujisaki and T. Okamoto, *Secure integration of asymmetric and symmetric encryption schemes*, in Advances in Cryptology – Crypto'99, LNCS 1666, pp. 537–554. Springer, 1999.
24. D. Galindo, *The Exact Security of Pairing Based Encryption and Signature Schemes*, talk at INRIA Workshop on Provable Security, 2004.
25. S. Halevi, P. Rogaway, *A tweakable enciphering mode*, in Advances in Cryptology – Crypto'03, LNCS 2729, pp. 482–499, Springer, 2003.
26. S. Halevi, P. Rogaway, *A parallelizable enciphering mode*, in Topics in Cryptology – CT-RSA'04, LNCS 2964, pp. 292–304, Springer, 2004
27. J. Katz, N. Wang, *Efficiency improvements for signature schemes with tight security reductions*, in 10^{th} ACM Conference on Computer and Communications Security, pp. 155–164, 2003.
28. K. Kurosawa, T. Matsuo, *How to Remove MAC from DHIES*, in proc. of ACISP 2004, LNCS 3108, pp. 236–247, Springer, 2004.
29. T. Okamoto, D. Pointcheval, *REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform*, in Topics in Cryptology – CT-RSA'01, LNCS 2020, pp. 159–174, Springer, 2001.
30. T. Okamoto, D. Pointcheval, *The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes*, in proc. of PKC'01, LNCS 1992, pp. 104–118, Springer, 2001.
31. D.H. Phan, D. Pointcheval, *Chosen-Ciphertext Security without Redundancy*, in Advances in Cryptology – Asiacrypt'03, LNCS 2894, pp. 1–18, Springer, 2003.
32. D.H. Phan, D. Pointcheval, *About the Security of Ciphers (Semantic Security and Pseudo-Random Permutations)*, Selected Areas in Cryptography (SAC'04), pp. 185–200, LNCS 3357, Springer, 2005.
33. D.H. Phan, D. Pointcheval, *OAEP 3-Round: A Generic and Secure Asymmetric Encryption Padding*, in Advances in Cryptology – Asiacrypt'04, LNCS 3329, pp. 63–78, Springer, 2004.
34. C. Rackoff, D. Simon, *Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack*, in Advances in Cryptology – Crypto'91, LNCS 576, Springer, pp. 433–444, 1991.
35. A. Shamir, *Identity Based Cryptosystems and Signature Schemes*, in Advances in Cryptology – Crypto' 84, LNCS 196, pp. 47-53, Springer, 1984.
36. V. Shoup, *A proposal for the ISO standard for public-key encryption (version 2.1)*, manuscript available from http://shoup.net/, 2001.