CCA2 Secure IBE: Standard Model Efficiency through Authenticated Symmetric Encryption

Eike Kiltz[1,⋆] and Yevgeniy Vahlis[2]

[1] Cryptology and Information Security Theme
CWI Amsterdam
The Netherlands
kiltz@cwi.nl
[2] University of Toronto
Canada
evahlis@cs.toronto.edu

Abstract. We propose two constructions of chosen-ciphertext secure identity-based encryption (IBE) schemes. Our schemes have a security proof in the standard model, yet they offer performance competitive with all known random-oracle based schemes. The efficiency improvement is obtained by combining modifications of the IBE schemes by Waters [38] and Gentry [21] with authenticated symmetric encryption.

1 Introduction

An Identity-Based Encryption (IBE) scheme is a public-key encryption scheme where any string is a valid public key. In particular, email addresses and dates can be public keys. The ability to use identities as public keys avoids the need to distribute public key certificates — which is one of the main technical difficulties when setting up a public-key infrastructure. An efficient construction of an IBE was not given until almost two decades after Shamir posed the initial open question in [35] regarding the existence of such cryptographic primitives. The first efficient IBEs appeared in 2001, given separately by Boneh and Franklin [10, 11], and Sakai et al. [33]. In particular, Boneh and Franklin [10, 11] proposed formal security notions for IBE systems and designed a fully functional secure IBE scheme using bilinear maps. This scheme and the tools developed in its design have been successfully applied in numerous cryptographic settings, transcending by far the identity based cryptography framework.

Despite its only recent invention, IBE is already used extensively in practice. Two companies — Voltage security and Identum — are specialized in identity-based security solutions. This is one of the reasons why IBE is currently in the process of getting standardized — the new IEEE P1363.3 standard for "Identity-Based Cryptographic Techniques using Pairings" is currently in preparation [25].

⋆ Supported by the research program Sentinels (http://www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

T. Malkin (Ed.): CT-RSA 2008, LNCS 4964, pp. 221–238, 2008.

The schemes that are currently in consideration are the one by Boneh and Franklin [11]; the one by Boneh and Boyen [7, 12]; and the one by Kasahara and Sakai [33, 16].

All the above IBE schemes provide security against *chosen-ciphertext attacks*. In a chosen ciphertext attack [32, 11], the adversary is given access to a decryption oracle that allows to obtain the decryptions of ciphertexts of his choosing. Intuitively, security in this setting means that an adversary obtains (effectively) no information about encrypted messages, provided the corresponding ciphertexts are never submitted to the decryption oracle. Since the dramatic attack by Bleichenbacher [5], the notion of chosen-ciphertext security is commonly agreed as the "right" notion of security for encryption schemes [37]. We stress that, in general, chosen-ciphertext security is a much stronger security requirement than semantic security, where in the latter an attacker is not given access to the decryption oracle.

Random Oracles. The drawback of all the IBE schemes [11, 7, 33, 16] that are currently under submission to the new IEEE P1363.3 standard is that their security can only be guaranteed in the *random oracle* model [3], i.e. in an idealized world where all parties get black-box access to a truly random function. Unfortunately a proof in the random oracle model can only serve as a heuristic argument and, admittedly using quite contrived constructions, has been shown to possibly lead to insecure schemes when the random oracles are implemented in the standard model (see, e.g., [14]). More importantly, there exist results [20] indicating that even certain standardized cryptographic schemes (such as full-domain hash signatures) will always remain in the grey area of schemes having a proof in the random oracle yet are "provably unprovable" in the standard model.

IBE Without Random Oracles. Waters [38] presents the first practical IBE that is chosen-plaintext secure without random oracles. It fits the category of "commutative-blinding" IBE schemes from Boneh and Boyen [7] and its chosen-plaintext security can be reduced to the Bilinear Decisional Diffie-Hellman (BDDH) assumption. Based on Waters scheme several chosen-ciphertext secure IBE schemes were proposed starting with generic constructions [9] whose specific instantiations were later improved [13, 28]. Today's most efficient variant is due to Kiltz and Galindo who successfully applied "direct chosen-ciphertext" techniques from [13, 27] to Waters' IBE scheme. More recently, Gentry [21] proposed yet another practical chosen-ciphertext secure IBE scheme based on the class of "inversion-based" IBE schemes from [7], offering interesting efficiency trade-offs compared to the commutative-blinding schemes [28].

Random Oracles: Theory vs. Practice. The above mentioned drawbacks of the random oracle model readily leads to the question why random-oracle based schemes are sometimes chosen over schemes with a rigorous proof in the standard model. The answer is straight-forward: it is common knowledge that schemes in the random-oracle model are usually much more efficient than schemes in the standard model. As long as the "theoretical problems" from [14, 20] do not lead to an actual break of a non-artificial scheme, using random-oracle

schemes seems justifiable in practice. On the other hand it is in the belief of the authors that this general perception about random oracles will change when alternative random-oracle free schemes become available that offer competitive performance.

1.1 Our Contributions

In this paper we demonstrate that there exist identity-based encryption schemes that are provably secure in the standard model, yet their performance is competitive with the best schemes in the random oracle model. We propose two constructions of chosen-ciphertext secure IBE schemes which outperform all such existing standard-model schemes, and have performance comparable to the random-oracle based schemes that were described above.

Scheme I. Our first IBE scheme is based on Waters' semantically secure IBE. Our approach to protecting a ciphertext against chosen ciphertext attacks bears some resemblance to the one used by Cramer and Shoup [18, 19] to obtain chosen ciphertext secure public key encryption. More precisely, we use the more efficient "encrypt-then-mac" or "authenticated symmetric encryption" variant proposed by Kurosawa and Desmedt [30]. More precisely, in our construction decryption of ill-formed ciphertexts (i.e. ciphertexts that could not have been generated by the encryption algorithm) uses randomness which is built into the user private key (and is independent of the master public key). Such ill-Formed ciphertexts can be detected using extra-information that is algebraically encoded into the "identity-carrying" part of the ciphertext (similar to the HIBE construction from [8]). Overall this allows us to obtain a CCA secure IBE scheme by only adding *one exponentiation* to the encryption/decryption algorithm of Waters' scheme, which is secure only against chosen plaintext attacks. We give a standard-model security proof reducing the intractability of the *modified Bilinear Decisional Diffie-Hellman* (mBDDH) problem (a problem closely related to BDDH) to breaking the CCA security of our scheme.

Scheme II. Our second construction is a variant of Gentry's chosen-ciphertext secure IBE scheme. Here our new contribution is to use authenticated symmetric encryption [30, 23] to reduce ciphertext expansion and encryption/decryption cost compared to Gentry's original schemes. We prove chosen-ciphertext security of our scheme with respect to the decisional augmented bilinear Diffie-Hellman exponent (q-ABDHE) assumption [21] in the standard model. We remark that the proof technique is different from the one used for the first scheme.

1.2 Comparison

We carefully review all known chosen-ciphertext secure IBE constructions and make an extensive comparison with our schemes. Our studies also incorporate all relevant practical issues when making a comparison, including the tightness of the security reduction with respect to different assumptions and instantiating the schemes in asymmetric pairing groups. To obtain concrete comparison

	Size (bits)		Cost (relative)	
Scheme	Ciphertext	Public Key	Encrypt	Decrypt
Standard model				
Ours: IBE_1 (§4)	422	2376	39	216
Ours: IBE_2 (§5)	1277	2223	110	222
KG [28]	513	2565	40	360
Gentry [21]	2223	3249	146	408
Random Oracle model				
BF [10]	331	171	187	151
BB_1 [7]	502	1386	39	217
KS [16]	331	171	38	152

Fig. 1. Efficiency comparison for CCA-secure IBE schemes in the standard/random oracle model for MNT/80-bit security level. Timings are relative to one exponentiation in group $\mathbb{G}$.

values we estimate ciphertext expansion and encryption/decryption cost when implemented in different pairing groups using recent (independent) timing data from [12]. This includes pairing groups based on super-singular curves and MNT curves.

The numerical results of our comparison for 80 bits MNT curves are given in Fig. 1 (For 80 bits super-singular curves the results are similar. We refer the reader to Fig. 5 in Section 6.) The figure shows that our schemes outperform all known IBE schemes in the standard model. Most notably, compared to the standard-model scheme KG from [28] decryption cost and ciphertext expansion is reduced by approximately one third, whereas encryption cost is the same. More importantly, in comparison with the random-oracle based schemes BF from [11], BB_1 from [7, 12], and KS from [33, 16] our schemes offer competitive performance in all parameters, yet are provably secure in the standard model.

1.3 Related Work

A special class of authenticated symmetric encryption schemes which is obtained using the "encrypt-then-mac" primitive was recently successfully applied to public-key encryption schemes by Kurosawa and Desmedt [30, 2] who greatly improved efficiency of the original Cramer-Shoup encryption scheme [19]. Their result was generalized to cover arbitrary authenticated encryption schemes [23]. In fact, our second IBE scheme can be seen as the "Kurosawa-Desmedt variant" of the original CCA secure scheme by Gentry. A variant of it was also sketched in independent work by Boneh, Gentry and Hamburg [6] using their general framework of "hash proof systems". In connection with IBE, authenticated encryption was first used in [34]. This paper is an extended version of an unpublished manuscript [26] by the first author.

2 Preliminaries

2.1 Notation

If x is a string, then $|x|$ denotes its length, while if S is a set then $|S|$ denotes its size. If $k \in \mathbb{N}$ then 1^k denotes the string of k ones. If S is a set then $s \leftarrow_{\mathrm{R}} S$ denotes the operation of picking an element s of S uniformly at random. Unless otherwise indicated, algorithms are randomized and polynomial time. By $z \leftarrow_{\mathrm{R}} \mathsf{A}^{\mathcal{O}_1,\mathcal{O}_2,\cdots}(x, y, \ldots)$ we denote the operation of running algorithm A with inputs $x, y, \ldots$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, and letting z be the output. An adversary is an algorithm or a tuple of algorithms.

2.2 Identity Based Encryption

An IBE scheme consists of four algorithms: Setup, KeyGen, Enc, and Dec. Setup generates the global public and private keys; KeyGen uses the global private key to generate an individual private key PRI_{id} for a given identity; Enc uses the global public key to encrypt a message to a given identity; and Dec uses the individual private key to decrypt ciphertexts.

The strongest and commonly accepted notion of security for an identity-based key encryption is that of indistinguishability against an adaptive chosen ciphertext attack [11]. This notion, denoted IND-ID-CCA (or simply CCA), is captured by defining the following advantage function for an adversary $\mathsf{A} = (\mathsf{A}_1, \mathsf{A}_2)$, and for an IBE scheme IBE:

$$\mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(k) \;=\; \left|\Pr[\mathsf{Exp}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(k) = 1] - 1/2\right|$$

where $\mathsf{Exp}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(k)$ is defined by the following experiment.

Experiment $\mathsf{Exp}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(k)$
$(\mathsf{PUB}, \mathsf{PRI}) \leftarrow_{\mathrm{R}} \mathsf{Setup}(1^k)$
$(id^*, m_0, m_1, St) \leftarrow_{\mathrm{R}} \mathsf{A}_1^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot,\cdot)}(\mathsf{PUB})$
$b \leftarrow_{\mathrm{R}} \{0,1\}; \quad C^* \leftarrow_{\mathrm{R}} \mathsf{Enc}(\mathsf{PUB}, id^*, m_b)$
$b' \leftarrow_{\mathrm{R}} \mathsf{A}_2^{\mathsf{KeyGen}(\cdot),\mathsf{Dec}(\cdot,\cdot)}(C^*, St)$
If $b = b'$ Return 1 else return 0

The oracle $\mathsf{KeyGen}(\cdot)$ on input id generates a new private key for the identity id and returns it. The oracle $\mathsf{Dec}(\cdot,\cdot)$ on input id and C first generates a new private key for id and then uses it to decrypt C. When A_1 outputs id^* it must not be any of the identities that the adversary queried to the $\mathsf{KeyGen}(\cdot)$ oracle. Furthermore, A_2 is not allowed to query the KeyGen$(\cdot)$ oracle on id^*, and is not allowed to query the $\mathsf{Dec}(\cdot,\cdot)$ oracle on (id^*, C^*). The variable St represents some internal state information of adversary A and can be any (polynomially bounded) string.

Definition 1. *An IBE scheme* IBE *is secure against chosen-ciphertext attacks (CCA secure) if for all adversaries* A *the advantage function* $\mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(\cdot)$ *is negligible.*

For a more precise analysis of the tightness of reduction we will sometimes use the following more detailed notation. For integers k, t, q_x, q_d, $\mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE},t,q_x,q_d}(k) = \max_{\mathsf{A}} \mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE},\mathsf{A}}(k)$, where the maximum is over all adversaries A that make at most t computational steps, q_x key-derivation, and q_d decryption queries. Here we make the convention to count all decryption queries for $id \neq id^*$ as a key-derivation query.

2.3 Symmetric Encryption

A symmetric encryption scheme $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ is specified by its encryption algorithm E (encrypting $m \in \mathit{MsgSp}(k)$ with keys $K \in \mathcal{K}(k)$) and decryption algorithm D (returning $m \in \mathit{MsgSp}(k)$ or $\perp$). Here we restrict ourselves to deterministic algorithms E and D.

The most common notion of security for symmetric encryption is that of ciphertext indistinguishability, which requires that all efficient adversaries fail to distinguish between the encryptions of two messages of their choice. Another common security requirement is *ciphertext authenticity*. Ciphertext authenticity requires that no efficient adversary can produce a new valid ciphertext under some key when given one encryption of a message of his choice under the same key. A symmetric encryption scheme which satisfies *both* requirements simultaneously is called secure in the sense of authenticated encryption (AE-OT secure). Note that AE-OT security is a stronger notion than chosen-ciphertext security. Formal definitions and constructions are provided in the full version [29].

3 Intractability Assumptions

3.1 Bilinear Groups

Our schemes will be parameterized by a *pairing parameter generator*. This is an algorithm $\mathcal{G}$ that on input 1^k returns the description of an multiplicative cyclic group $\mathbb{G}$ of prime order p, where $2^k < p < 2^{k+1}$, the description of a multiplicative cyclic group $\mathbb{G}_T$ of the same order, and a non-degenerate bilinear pairing $\hat{e} : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. See [11] for a description of the properties of such pairings. We use $\mathbb{G}^*$ to denote $\mathbb{G} \setminus \{1\}$, i.e. the set of all group elements except the neutral element. Throughout the paper we use $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g, g_T)$ as shorthand for the description of bilinear groups, where g is a generator of $\mathbb{G}$ and $g_T = \hat{e}(g, g) \in \mathbb{G}_T$.

3.2 The Modified BDDH Assumption

Let $\mathbb{PG}$ be the description of pairing groups. The Bilinear Decisional Diffie-Hellman (BDDH) assumption [11] states that the two distributions $(g^x, g^y, g^z, \hat{e}(g, g)^{xyz})$ and $(g^x, g^y, g^z, \hat{e}(g, g)^r)$, for $x, y, z, r \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ are indistinguishable for any adversary. For the modified BDDH assumption we furthermore provide the

adversary with the element $g^{(y^2)}$. More formally we define the advantage function $\mathsf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathsf{B}}(k)$ of an adversary B as

$$\left| \begin{array}{l} \Pr[\mathsf{B}(\mathbb{PG}, g^x, g^y, g^{y^2}, g^z, \hat{e}(g,g)^{xyz}) = 1] \\ \quad - \Pr[\mathsf{B}(\mathbb{PG}, g^x, g^y, g^{y^2}, g^z, \hat{e}(g,g)^r) = 1] \end{array} \right| ,$$

where $x, y, z, r \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ and $\mathbb{PG} \leftarrow_{\mathrm{R}} \mathcal{G}(1^k)$. We say that the *modified Bilinear Decision Diffie-Hellman (mBDDH) assumption relative to generator* $\mathcal{G}$ holds if $\mathsf{Adv}^{\mathrm{mbddh}}_{\mathcal{G},\mathsf{B}}(\cdot)$ is negligible for all adversaries B.

3.3 The Truncated q-ABDHE Assumption

Let $q = q(k)$ be a polynomial. The q-BDDHI assumption [7] states that the two distributions $(g^x, \ldots, g^{x^q}, \hat{e}(g,g)^{1/x})$ and $(g^x, \ldots, g^{x^q}, \hat{e}(g,g)^r)$, for $x, r \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ are indistinguishable for any adversary. In [21] Gentry proposed the related truncated decisional augmented bilinear Diffie-Hellman exponent (truncated q-ABDHE) assumption which augments the q-BDDHI assumption with additional information to the adversary. We define the advantage function $\mathsf{Adv}^{\text{q-abdhe}}_{\mathcal{G},\mathsf{B}}(k)$ of an adversary B as

$$\left| \begin{array}{l} \Pr[\mathsf{B}(\mathbb{PG}, g^x, \ldots, g^{x^q}, g^z, g^{zx^{q+2}}, \hat{e}(g,g)^{zx^{q+1}}) = 1] \\ \quad - \Pr[\mathsf{B}(\mathbb{PG}, g^x, \ldots, g^{x^q}, g^z, g^{zx^{q+2}}, \hat{e}(g,g)^r) = 1] \end{array} \right| ,$$

where $x, z, r \leftarrow_{\mathrm{R}} \mathbb{Z}_p$ and $\mathbb{PG} \leftarrow_{\mathrm{R}} \mathcal{G}(1^k)$. We say that the *truncated q-ABDHE assumption relative to generator* $\mathcal{G}$ holds if $\mathsf{Adv}^{\text{q-abdhe}}_{\mathcal{G},\mathsf{B}}(\cdot)$ is negligible for all B.

3.4 Relations

The next lemma classifies the strength of the modified BDDH assumption we introduced between the well known *standard pairing-based assumptions* BDDH and 2-BDDHI. Here "A $\leq$ B" means that assumption B implies assumption A (in a generic sense), i.e. assumption B is a stronger assumption than A.

Lemma 1. *BDDH* $\leq$ *mBDDH* $\leq$ 2-*BDDHI* $\leq \ldots \leq$ *q-BDDHI* $\leq$ *truncated q-ABDHE*

The simple proof will be given in the full version [29]. We remark that the complexity of q-BDDHI (as well as truncated q-ABDHE) in the in the generic-group model [36] is roughly $\Omega(\sqrt{p/q})$ [7, 21] which matches the recent attack due to Cheon [17].

4 IBE Scheme I

In this section we present our first CCA secure IBE scheme. It is based on the Boneh-Boyen "commutative-blinding" IBE scheme [7] in its full-identity secure variant of Waters [38] which is chosen-plaintext secure. We construct a CCA

secure IBE by adding a redundant group element to the ciphertext, and authenticating the two group elements both explicitly, using target collision resistant hash function, and implicitly by using the same randomness to generate both elements.

A similar technique was already used by Cramer and Shoup to obtain chosen-ciphertext secure public-key encryption and later also successfully applied in [13, 27, 28]. All the above works make a distinction between ciphertexts that can be generated by the encryption algorithm (well-formed ciphertexts), and strings that the encryption algorithm would never output (ill-formed ciphertexts) in their security analysis. The first CCA secure IBE that applies this methodology is [28]. The IBE of [28] handles ill-formed ciphertexts by decrypting them to a fresh random value chosen by the decryption algorithm ("implicit rejection"). This approach is sufficient for obtaining CCA security, but is prohibitively expensive as it requires the decryption algorithm to be randomized, and to compute several exponentiations of group elements to handle ill-formed ciphertexts.

We avoid this additional computation by exploiting the fact that in our IBE the decryption of an ill-formed ciphertext depends on the randomness of the private key that was used for the decryption. In other words, we decrypt ill-formed ciphertexts in the same way as we would decrypt well-formed ciphertext, but for a well formed ciphertext the outcome of the decryption is independent of the randomness in the private key. As a result our decryption algorithm is deterministic and significantly faster than [28]. Furthermore, our scheme also has one group element less in the ciphertext than [28]. This is achieved by algebraically integrating the implicit ciphertext consistency check into the part of the ciphertext that carries the information about the recipient's identity.

4.1 The IBE Construction

We assume that $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g, g_T)$ are public system parameters obtained by running the group parameter algorithm $\mathcal{G}(1^k)$ (that may be shared among multiple systems).

We review the hash function $H : \{0,1\}^n \to \mathbb{G}$ used in Waters' identity based encryption schemes [38]. On input of $\mathbb{G}$ and an integer n, the randomized hash key generator $\mathsf{HGen}(\mathbb{G}; n)$ chooses $n+1$ random group elements $h_0, \ldots, h_n \in \mathbb{G}$ and returns $h = (h_0, h_1, \ldots, h_n) \in \mathbb{G}^{n+1}$ as the public description of the hash function. The algebraic hash function $H : \{0,1\}^n \to \mathbb{G}$ is evaluated on a string $id = (id_1, \ldots, id_n) \in \{0,1\}^n$ as the product

$$H(id) = h_0 \prod_{i=1}^{n} h_i^{id_i} \in \mathbb{G}.$$

Let $TCR : \mathbb{G} \to$ be a target collision-resistant hash function and $\mathsf{SE} = (\mathsf{E}, \mathsf{D})$ be a symmetric encryption scheme with key-space $\mathcal{K} = \mathbb{G}_T$. Our IBE scheme IBE_1 with identity space $IDSp = \{0,1\}^n$ is described in Fig. 2. Here it is understood that decryption rejects if the ciphertext C does not parse to (c_1, c_2, c_3) with $c_1 \in \mathbb{G}$ and $c_2 \in \mathbb{G}^*$. An IBE scheme with arbitrary identity space $IDSp = \{0,1\}^*$

can be obtained by applying a collision-resistant hash function to the identities. (The choice of $n = 2k$ is due to the birthday paradox.)

$\mathsf{Setup}(1^k)$	$\mathsf{KeyGen}(\mathsf{PRI}, id)$
$\alpha, u \leftarrow_{\mathrm{R}} \mathbb{G};\ z \leftarrow \hat{e}(g, \alpha)$	$s \leftarrow_{\mathrm{R}} \mathbb{Z}_p$
$H \leftarrow_{\mathrm{R}} \mathsf{HGen}(\mathbb{G}; n)$	$\mathsf{PRI}_{id} \leftarrow (\alpha \cdot H(id)^s, g^{-s}, u^s) \in \mathbb{G}^3$
$\mathsf{PUB} \leftarrow (H, u, z)\ ;\ \mathsf{PRI} \leftarrow \alpha$	Return PRI_{id}
Return $(\mathsf{PUB}, \mathsf{PRI})$	
$\mathsf{Enc}(\mathsf{PUB}, id, m)$	$\mathsf{Dec}(\mathsf{PUB}, id, \mathsf{PRI}_{id}, C)$
$r \leftarrow_{\mathrm{R}} \mathbb{Z}_p;\ c_1 \leftarrow g^r$	Parse C as $(c_1, c_2, c_3) \in \mathbb{G} \times \mathbb{G}^* \times \{0,1\}^*$
$t \leftarrow TCR(c_1);\ c_2 \leftarrow (H(id) \cdot u^t)^r$	Parse PRI_{id} as $(d_1, d_2, d_3) \in \mathbb{G}^3$
$K \leftarrow z^r \in \mathbb{G}_T;\ c_3 \leftarrow \mathsf{E}_K(m)$	$t \leftarrow TCR(c_1);\ K \leftarrow \hat{e}(c_1, d_1 \cdot d_3^t) \cdot \hat{e}(c_2, d_2)$
Return ciphertext $C = (c_1, c_2, c_3)$	Return $m \leftarrow \mathsf{D}_K(c_3)$

Fig. 2. Our first CCA-secure IBE scheme IBE_1

We now show correctness of the scheme, i.e. that the symmetric key K computed in the encryption algorithm matches the key K computed in the decryption algorithm.[1] A correctly generated secret key for identity id has the form $\mathsf{PRI}_{id} = (d_1, d_2, d_3) = (\alpha \cdot H(id)^s, g^{-s}, u^s)$ for some $s \in \mathbb{Z}_p$. Therefore the decryption algorithm computes the symmetric key K as

$$\begin{aligned} K &= \hat{e}(c_1, d_1 \cdot d_3^t) \cdot \hat{e}(c_2, d_2) \\ &= \hat{e}(g^r, \alpha \cdot H(id)^s \cdot (u^s)^t) \cdot \hat{e}((H(id) \cdot u^t)^r, g^{-s}) \\ &= \hat{e}(g^r, \alpha) \cdot \hat{e}(g^r, H(id)^s \cdot (u^s)^t) \cdot \hat{e}((H(id) \cdot u^t)^r, g^{-s}) \\ &= z^r \cdot \hat{e}(g^r, (H(id) \cdot u^t)^s) \cdot \hat{e}((H(id) \cdot u^t)^{-s}, g^r) \\ &= z^r, \end{aligned}$$

which is the same as the key computed in the encryption algorithm. Now correctness of the scheme is implied by correctness of SE.

4.2 Security

Theorem 1. *Assume TCR is a target collision resistant hash function and* (E, D) *is a* AE-OT*-secure symmetric scheme. Under the modified Bilinear Decisional Diffie-Hellman (mBDDH) assumption relative to generator* $\mathcal{G}$*, the IBE scheme* IBE_1 *is* CCA *secure. In particular, for* $\varepsilon(k) = \mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE}_1, t, q_x, q_d}(k)$ *and* $\tilde{\varepsilon}(k) = \mathsf{Adv}^{\mathrm{mbddh}}_{\mathcal{G}, \tilde{t}}(k)$ *we have*

$$\varepsilon(k) \leq (\mathsf{Adv}^{\mathsf{IND}}_{\mathsf{SE}, \tilde{t}}(k) + \tilde{\varepsilon}(k)) \cdot 10nq + \mathsf{Adv}^{\mathsf{TCR}}_{TCR, t}(k) + q_d \cdot \mathsf{Adv}^{\mathsf{CT\text{-}INT}}_{\mathsf{SE}, t}(k) + 2q_d^2/p;$$

$$t \geq \tilde{t} - \mathcal{O}(\tilde{\varepsilon}^{-2}(k) \cdot \ln(\tilde{\varepsilon}^{-1}(k)) + q_d + q_x)\ .$$

[1] Decryption rejects all ciphertexts with $c_2 = 1 \in \mathbb{G}$. We can assume that encryption does not generate ciphertexts with $c_2 = 1$. In case it does encryption can pick fresh randomness r.

The full proof is given in the full version [29]. We give a brief overview here. Our proof for this system has many similarities with [28] (which in turn is based on [38]). The key difference between the two proofs is the treatment of ill-formed ciphertexts. [28] use the fact that anyone that has the global public key can check whether a ciphertext is well-formed. Then, if the ciphertext is ill-formed the decryption algorithm chooses a random value for K, and uses it to attempt and decrypt the symmetric ciphertext. Thus, the adversary himself could have decrypted any ill-formed ciphertext, and does not gain any information from querying the decryption oracle on such ciphertexts.

Our approach to dealing with ill-formed ciphertexts is different. We do not rely on the ability of anyone who has the global public key to check whether a ciphertext is well-formed. Instead, we make the observation that an ill-formed ciphertext, i.e. a ciphertext of the form $C = (g^r, (H(id) \cdot u^t)^{r'}, c_3)$, where $r \neq r'$, decrypts in the following way:

1. The intermediate key K is computed: $K = z^r \cdot \hat{e}(g, H(id) \cdot u^t)^{(r-r')s}$, where s is the random value that was used to generate the private key.
2. K is used to attempt and decrypt the AE ciphertext.

Now, the adversary makes a polynomial number of decryption queries with ill-formed ciphertexts. We show that the first such query is likely to decrypt as "reject", and each query after the first is likely to decrypt as "reject" given that all previous ill-formed queries decrypted as reject, which completes the proof. The idea is that the value s remains random in the view of the adversary as he makes decryption queries with valid ciphertexts, or ciphertexts that decrypt as "reject". Since s is random, K is also a random element of $\mathbb{G}_T$. Thus, by the authenticity property of the AE encryption, c_3 will be decrypted to "reject" when the random element K is used as the key.

4.3 Extensions

Trading Public Key Size and Security Reduction. As independently discovered in [15, 31], there exists an interesting trade-off between key-size of Waters' hash H and the security reduction of the IBE schemes. The construction modifies Waters hash H as follows: Let the integer $l = l(k)$ be a new parameter of the scheme. In particular, we represent an identity $id \in \{0,1\}^n$ as an n/l-dimensional vector $id = (id_1, \ldots, id_{n/l})$, where each id_i is an l bit string. Waters hash is then redefined to $H : \{0,1\}^n \to \mathbb{G}$, with $H(id) = h_0 \prod_{i=1}^{n/l} h_i^{id_i}$ for random public elements $h_0, h_1, \ldots, h_{n/l} \in \mathbb{G}$. Waters' original hash function is obtained as the special case $l = 1$. It is easy to see that using this modification in our IBE scheme (i) reduces the size of the public key from $n+2$ to $n/l+2$ elements in $\mathbb{G}$, whereas (ii) it adds another multiplicative factor of 2^l to the security reduction of the IBE scheme (Theorem 1).

For concreteness we propose the following value for l (our choice will become clear in Section 6). For a scheme implemented in groups offering 80 bits of

security we have $n = 2 \cdot 80 = 160$ bits and use 128. This shrinks the public-key size to reasonable $n/l + 2 \approx 10$ elements in $\mathbb{G}$ (plus one element in $\mathbb{G}_T$).

We further remark that in the random-oracle model we can replace Waters' hash $H : \{0,1\}^* \to \mathbb{G}$ with $H(id) = h_0 \cdot h_1^{RO(id)}$, where $RO : \{0,1\}^* \to \mathbb{Z}_p$ is a cryptographic hash function which is modeled as a random oracle [3] in the security analysis.

Hierarchical Identities. Hierarchical identity-based encryption (HIBE) is a generalization of IBE to identities supporting hierarchical structures [24]. In a HIBE, identities are hierarchical and take the form $id = [id_1.id_2.id_3]$. This particular hierarchical identity has depth 3, and is subordinate to $[id_1]$, $[id_1.id_2]$, but not to $[id_1.id_2.id_3']$. Each user in the hierarchy may act as a local key-generation authority for all subordinate hierarchical identities.

By the relation to Waters IBE scheme it is easy to see that our technique can also be used to obtain a chosen-ciphertext secure HIBE. Using a technique from [8] it is furthermore possible to reduce the HIBE ciphertext size to three elements, i.e. it is independent of the hierarchy's depth. To be more precise, the IBE from Section 4.1 is modified to a HIBE supporting maximal d hierarchies as follows. The setup algorithm chooses d different and independent hash functions $H_i \leftarrow_R \mathsf{HGen}(\mathbb{G}; n)$, for $1 \leq i \leq d$. The user secret key for the hierarchical identity $id = [id_1. \cdots .id_\mu]$ of depth $\mu \leq d$ is defined as $\mathsf{PRI}_{id} = (d_1, d_2, d_3, (d_{ij})_{\mu+i \leq j \leq d, 0 \leq i \leq n}) \in \mathbb{G}^{3+(n+1)\cdot(d-\mu-1)}$, where $d_1 = \alpha \cdot (\prod_{j=1}^{\mu} H_i(id^{(j)}))^r$, $d_2 = g^{-r}$, $d_3 = u^r$, and $d_{ij} = ((h_i^{(j)})^r)$. We remark that the latter $(n+1) \cdot (d-\mu-1)$ elements d_{ij} are only needed for hierarchical key delegation (and may be not included in PRI_{id} if such a feature is not wanted). Encryption of m with respect to id computes the two ciphertext elements $c_1 = g^r$ and $c_2 = (u^t \prod_{j=1}^{\mu} H_i(id^{(j)}))^r$ and uses the key $K = z^r$ to compute the symmetric ciphertext (using an AE-OT-secure scheme). Decryption uses $K = \hat{e}(d_1 \cdot d_3^t, c_1) \cdot \hat{e}(d_2, c_2)$ to reconstruct the plaintext from the symmetric ciphertext. Note that this only needs two pairing operations, independent of the depth of the hierarchy d. (In contrast the HIBE from [28] needs $d+1$ pairings.)

Security can be proved with respect to the *d-modified BDDH assumption*, where compared to the mBDDH assumption the adversary gets the values g^y, $g^{y^2}, \ldots, g^{y^{d+1}}$ (instead of just g^y, g^{y^2}). As in [22, 38] the security reduction is exponential in the depth d of the hierarchy, i.e. it introduces, roughly, a multiplicative factor of $(nq)^d$. Hence the scheme can only be considered practical for small hierarchies, say of depth $d = 4$.

Trading ciphertext size for efficiency. A variant of our IBE scheme can be combined with CCA-secure symmetric encryption. CCA-secure symmetric encryption is less demanding than authenticated encryption and, in particular, strong pseudorandom permutations imply CCA-secure symmetric encryption without any redundancy. This has the advantage of more compact ciphertexts while decryption has to perform some algebraic consistency checks and is therefore less efficient.

5 IBE Scheme II

In this section we present our second chosen-ciphertext secure IBE scheme from the q-ABDHE assumption. It is based on the Boneh-Boyen "exponent inversion" IBE scheme [7] in its full-identity secure variant of Gentry [21]. Gentry also presents a chosen-ciphertext secure variant of his basic chosen-plaintext secure scheme. Our main improvement is to combine it with a strongly secure symmetric encryption scheme to considerably reduce ciphertext size and encryption/decryption cost.

5.1 The IBE Construction

Let $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g, g_T = \hat{e}(g,g))$ be a pairing group. Let $TCR : \mathbb{G}\times\mathbb{G} \to \mathbb{Z}_p$ be a target collision-resistant hash function. Let (E, D) be a symmetric cipher. Our IBE scheme $\mathsf{IBE}_2 = (\mathsf{Setup}, \mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with identity space $IDSp = \mathbb{Z}_p$ is depicted in Fig. 3.

$\mathsf{Setup}(1^k)$
$x, y_1, y_2 \leftarrow_{\mathrm{R}} \mathbb{Z}_p$
$u \leftarrow g^x;\ v_1 \leftarrow g_T^{y_1};\ v_2 \leftarrow g_T^{y_2}$
$\mathsf{PUB} \leftarrow (u, v_1, v_2);\ \mathsf{PRI} \leftarrow (x, y_1, y_2)$
Return $(\mathsf{PUB}, \mathsf{PRI})$

$\mathsf{KeyGen}(\mathsf{PRI}, id)$
$s_1, s_2 \leftarrow_{\mathrm{R}} \mathbb{Z}_p$
$d_1 \leftarrow g^{\frac{y_1 - s_1}{x - id}};\ d_2 \leftarrow g^{\frac{y_2 - s_2}{x - id}}$
$\mathsf{PRI}_{id} \leftarrow (d_1, s_1, d_2, s_2)$
Return user secret-key PRI_{id}

$\mathsf{Enc}(\mathsf{PUB}, id, m)$
$r \leftarrow_{\mathrm{R}} \mathbb{Z}_p\ c_1 \leftarrow (ug^{-id})^r;\ c_2 \leftarrow g_T^r$
$t \leftarrow TCR(c_1, c_2);\ K \leftarrow (v_1^t v_2)^r$
$c_3 \leftarrow \mathsf{E}_K(m)$
Return ciphertext $C = (c_1, c_2, c_3)$

$\mathsf{Decaps}(\mathsf{PUB}, id, \mathsf{PRI}_{id}, C)$
Parse C as $(c_1, c_2, c_3) \in \mathbb{G} \times \mathbb{G}_T \times \{0,1\}^*$
Parse PRI_{id} as (d_1, s_1, d_2, s_2)
$t \leftarrow TCR(c_1, c_2)\ ;\ K \leftarrow \hat{e}(c_1, d_1^t d_2) \cdot c_2^{s_1 t + s_2}$
Return $m \leftarrow \mathsf{D}_K(c_3)$

Fig. 3. Our CCA-secure IBE scheme IBE_2

To show correctness consider a ciphertext (c_1, c_2, c_3) generated for identity id that gets decrypted with a valid user secret key $\mathsf{PRI}_{id} = (d_1, d_2, s_1, s_2)$ by computing the symmetric key K as follows

$$\begin{aligned} K &= \hat{e}(c_1, d_1^t d_2) \cdot c_2^{s_1 t + s_2} \\ &= \hat{e}(g^{(x-id)r}, g^{\frac{(y_1 - s_1)t + (y_2 - s_2)}{x - id}}) \cdot \hat{e}(g,g)^{(s_1 t + s_2) r} \\ &= \hat{e}(g^r, g^{y_1 t + y_2}) \\ &= (v_1^t v_2)^r, \end{aligned}$$

as in the encryption algorithm.

Theorem 2. *Assume TCR is a target collision resistant hash function and (E, D) is a* AE-OT*-secure symmetric scheme. Let $q = q_x + 1$, where q_x is the*

number of key-derivation queries. Under the truncated q-ABDHE assumption relative to generator $\mathcal{G}$, the IBE scheme IBE_2 is IND-CCA *secure. In particular, we have*

$$\mathsf{Adv}^{\mathsf{CCA}}_{\mathsf{IBE}_2,t,q_x,q_d}(k) \leq \mathsf{Adv}^{\text{q-abdhe}}_{\mathcal{G},t}(k) + \mathsf{Adv}^{\mathsf{TCR}}_{TCR,t}(k) + 2q_d \cdot \mathsf{Adv}^{\mathsf{CT\text{-}INT}}_{\mathsf{SE},t}(k) + \mathsf{Adv}^{\mathsf{IND}}_{\mathsf{SE},t}(k) + \frac{q_d}{p} .$$

The proof of Theorem 2 will be given in the full version [29]. We give some intuition why the scheme is IND-CCA secure. First, the proof of Gentry [21] can be used to show that user secret-key queries, as well as *consistent* decryption queries for the challenge identity id^* are basically useless for an adversary attacking the scheme (unless it can efficiently solve the q-ABDHE problem). However, inconsistent decryption queries with respect to the challenge identity id^* may leak information about the hidden bit b. Here we use a Cramer-Shoup argument. The idea is that the user secret-key $\mathsf{PRI}_{id^*} = (d_1^*, s_1^*, d_2^*, s_2^*)$ used to answer such decryption queries contains some internal randomness $(s_1, s_2) \in \mathbb{Z}_p^2$ that is initially hidden from the adversary's view. During the simulation of the IND-CCA environment the challenge ciphertext will leak (in an information-theoretic sense) one linear equation on the hidden randomness (s_1^*, s_2^*). Decryption queries of inconsistent ciphertexts will use a key K for symmetric decryption that is computed as a linear equation in s_1^*, s_2^* which is linearly independent from the equation the adversary knows. Hence, one single key K is uniformly distributed over $\mathbb{G}_T$. By the ciphertext authenticity property of SE the adversary will not be able to come up with an inconsistent ciphertext (c_1, c_2, c_3) such that $\mathsf{D}_K(c_3)$ does not reject. Consequently, all inconsistent ciphertext will get rejected by the scheme.

5.2 Extensions

Using techniques from [1] it is further possible to prove IBE_2 anonymous in the sense that the ciphertext does not leak any information about the sender's identity. This property has recently proved useful in the area of public-key encryption with keyword search [1].

We remark that in contrast to the IBE construction from Section 4 it is not possible to trade algebraic consistency checks for a weaker symmetric encryption scheme. In general, the class of inversion-based IBE schemes are less versatile than the commutative-blinding IBE schemes; for example, adding extensions like hierarchical key delegation to inversion-based IBE schemes seems a difficult task.

6 Comparison

6.1 Considered Schemes

For our comparison we consider the following standard-model IBE schemes.

IBE_1: Our scheme from Section 4 with the shorter public-parameters. See Section 4.3 for details.

IBE_2: Our scheme from Section 5.
KG: The scheme from Kiltz and Galindo [28].
Gentry: The scheme from Gentry [21] (IND-CCA variant).

We furthermore consider the following three IBE schemes that only have a proof in the random-oracle model. All of them are currently in submission for the IEEE1363.3 standardization project [25].

BF: The (FullIdent) scheme from Boneh and Franklin [11].
BB_1: The scheme from Boneh and Boyen [7] in its "hashed identities" variant [12].
KS: The scheme from Kasahara and Sakai [33] as described in [16].

We remark that when assuming the interactive *gap Bilinear Diffie-Hellman* (gap-BDH) assumption efficiency of BF and BB_1 can be further improved [12]. Due to the strong assumption we will not consider those schemes.

6.2 Security Reductions

For determining the parameters of the compared schemes, we make the following assumptions, most of the are conservative towards the efficiency of our new schemes. For $k = 80$ bit security we estimate (following Bellare and Rogaway [4]) the number of (random oracle) hash queries as $q_H = 2^{50}$. This seems reasonable since a hash function is in the hand of an adversary and can be attacked offline. Similar to signatures schemes we think that a reasonable estimate for the number of key-derivation queries is $q_x \approx 2^{25}$. This is much smaller than the number of hash queries since key-derivation queries can only be made online, in interaction with the system. In practice it is easy to limit the number of key-derivation queries.

The IBE schemes IBE_1 and KG have two additional integer parameters: n, l. Parameter $n = 2k$ resembles the bit size $n = 160 \approx 2^7$ of the identity space and $l(k)$ defines the tradeoff between public parameters and security-reduction (cf. Section 4.3). We choose $l = 18$ to obtain a security loss of $2^{18+7+25} = 2^{50} = q_H$. This explains our choice of $l(k)$: it is chosen such that the security loss of the above schemes matches the one of all random-oracle schemes.

The concrete security reductions are given in Fig. 4. For a fair comparison the security reductions of the random-oracle based schemes are given relative to the respective decisional assumption (e.g., BDDH instead of BCDH for BB_1). We note that the two schemes IBE_2 and Gentry have a tight security reduction to a much stronger security assumption. Due to the recent attacks by Cheon [17] it seems reasonable that the q-xxxx assumption are $\sqrt{q}$ times "less secure" than the BDDH assumption. This in particular implies (by Lemma 1) that we can treat the mBDDH assumption as "as secure" as the BDDH assumption. To simplify the comparison we make the conservative assumption that all the above schemes with the given parameters have the same security loss with respect to the BDDH assumption.

Scheme	Standard Model?	Assumption	Security reduction Bounds concrete ($k = 80$)	
IBE_1	$\surd$	mBDDH	$2^l nq_x$	2^{50}
IBE_2	$\surd$	q-ABDHE	1	1
KG	$\surd$	BDDH	$2^l nq_x$	2^{50}
Gentry	$\surd$	q-ABDHE	1	1
BF	—	BDDH	$> q_H$	2^{50}
BB_1	—	BDDH	q_H	2^{50}
KS	—	q-BDDHI	q_H^3	$\gg 2^{50}$

Fig. 4. Security assumptions and (concrete) reduction factors for IBE schemes

6.3 Results

A comparison with concrete timing values from Boyen [12] is carried out in Fig. 1 (Section 1) and Fig. 5. Ciphertext overhead represents the difference (in bits) between the ciphertext length and the message length. All timings are given in multiplicative factors relative to one exponentiation in $\mathbb{G}$. As usual, all symmetric operations (cryptographic hash function, symmetric encryption, etc) are ignored. All schemes come with a security proof based on different security assumption, furthermore introducing a different loss of security in the reduction, depending on several system parameters. A high loss in the security reduction reduces the real-world efficiency of the scheme by making it necessary to increase the size of the groups for any given security level. In order not to compare apples with pears, attempted to pick the parameters (in particular the parameter l for IBE_1 and KG) such that we obtain the *same concrete security reduction* for all schemes. We refer to the full version [29] for more details of the comparison.

We conclude that our schemes are the most efficient chosen-ciphertext secure IBE schemes in the standard model. Furthermore its performance and

	Size (bits)		Cost (relative)	
Scheme	Ciphertext	Public Key	Encrypt	Decrypt
Standard model				
Ours: IBE_1 (§4)	1104	6144	8	25
Ours: IBE_2 (§5)	1616	2560	14	25
KG [28]	1536	5632	9	29
Gentry [21]	2560	3584	18	49
Random Oracle model				
BF [10]	672	512	22	21
BB_1 [7]	1184	2048	7	29
KS [16]	672	512	6	22

Fig. 5. Efficiency comparison for CCA-secure IBE schemes in the standard/random oracle model for SS/80-bit security level. Timings are relative to one exponentiation in group $\mathbb{G}$.

ciphertext expansion seems comparable to the known random-oracle based schemes, in particular to the one by Boneh and Franklin which is intensively used in practice (see, e.g., `http://www.voltage.com`).

Acknowledgement

We thank Charles Rackoff, Ian Blake, and the anonymous CT-RSA reviewers for useful comments.

References

[1] Abdalla, M., Bellare, M., Catalano, D., Kiltz, E., Kohno, T., Lange, T., Malone-Lee, J., Neven, G., Paillier, P., Shi, H.: Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 205–222. Springer, Heidelberg (2005)

[2] Abe, M., Gennaro, R., Kurosawa, K., Shoup, V.: Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 128–146. Springer, Heidelberg (2005)

[3] Bellare, M., Rogaway, P.: Random oracles are practical: A paradigm for designing efficient protocols. In: Ashby, V. (ed.) ACM CCS 1993, pp. 62–73. ACM Press, New York (1993)

[4] Bellare, M., Rogaway, P.: The exact security of digital signatures: How to sign with RSA and Rabin. In: Maurer, U.M. (ed.) EUROCRYPT 1996. LNCS, vol. 1070, pp. 399–416. Springer, Heidelberg (1996)

[5] Bleichenbacher, D.: Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS #1. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 1–12. Springer, Heidelberg (1998)

[6] Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: Proceedings of FOCS 2007, pp. 647–657. IEEE, Los Alamitos (2007)

[7] Boneh, D., Boyen, X.: Efficient selective-ID secure identity based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)

[8] Boneh, D., Boyen, X., Goh, E.-J.: Hierarchical identity based encryption with constant size ciphertext. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 440–456. Springer, Heidelberg (2005)

[9] Boneh, D., Canetti, R., Halevi, S., Katz, J.: Chosen-ciphertext security from identity-based encryption. SIAM Journal on Computing 5(36), 1301–1328 (2006)

[10] Boneh, D., Franklin, M.K.: Identity-based encryption from the Weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)

[11] Boneh, D., Franklin, M.K.: Identity based encryption from the Weil pairing. SIAM Journal on Computing 32(3), 586–615 (2003)

[12] Boyen, X.: The BB1 identity-based cryptosystem: A standard for encryption and key encapsulation. Submitted to IEEE 1363.3, (August 2006), `http://grouper.ieee.org/groups/1363/`

[13] Boyen, X., Mei, Q., Waters, B.: Direct chosen ciphertext security from identity-based techniques. In: Atluri, V., Meadows, C., Juels, A. (eds.) ACM CCS 2005, pp. 320–329. ACM Press, New York (2005)

[14] Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. In: 30th ACM STOC, pp. 209–218. ACM Press, New York (1998)

[15] Chatterjee, S., Sarkar, P.: Trading time for space: Towards an efficient IBE scheme with short(er) public parameters in the standard model. In: Won, D.H., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 424–440. Springer, Heidelberg (2006)

[16] Chen, L., Cheng, Z., Malone-Lee, J., Smart, N.P.: An efficient ID-KEM based on the Sakai-Kasahara key construction. IEE Proceedings Information Security 152, 19–26 (2006)

[17] Cheon, J.H.: Security analysis of the strong Diffie-Hellman problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 1–11. Springer, Heidelberg (2006)

[18] Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13–25. Springer, Heidelberg (1998)

[19] Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing 33(1), 167–226 (2003)

[20] Dodis, Y., Oliveira, R., Pietrzak, K.: On the generic insecurity of the full domain hash. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 449–466. Springer, Heidelberg (2005)

[21] Gentry, C.: Practical identity-based encryption without random oracles. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 445–464. Springer, Heidelberg (2006)

[22] Gentry, C., Silverberg, A.: Hierarchical ID-based cryptography. In: Zheng, Y. (ed.) ASIACRYPT 2002. LNCS, vol. 2501, pp. 548–566. Springer, Heidelberg (2002)

[23] Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer, Heidelberg (2007)

[24] Horwitz, J., Lynn, B.: Toward hierarchical identity-based encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 466–481. Springer, Heidelberg (2002)

[25] IEEE P1363.3 Committee. IEEE 1363.3 — standard for identity-based cryptographic techniques using pairings (April 2007), `http://grouper.ieee.org/groups/1363/`

[26] Kiltz, E.: Chosen-ciphertext secure identity-based encryption in the standard model with short ciphertexts. Cryptology ePrint Archive, Report 2006/122 (2006), `http://eprint.iacr.org/`

[27] Kiltz, E.: Chosen-ciphertext security from tag-based encryption. In: Halevi, S., Rabin, T. (eds.) TCC 2006. LNCS, vol. 3876, pp. 581–600. Springer, Heidelberg (2006)

[28] Kiltz, E., Galindo, D.: Direct chosen-ciphertext secure identity-based key encapsulation without random oracles. In: Batten, L.M., Safavi-Naini, R. (eds.) ACISP 2006. LNCS, vol. 4058. Springer, Heidelberg (2006)

[29] Kiltz, E., Vahlis, Y.: CCA2 Secure IBE: standard model efficiency through authenticated symmetric encryption. Cryptology ePrint Archive, Report 2008 (2008), `http://eprint.iacr.org/`

[30] Kurosawa, K., Desmedt, Y.: A new paradigm of hybrid encryption scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426–442. Springer, Heidelberg (2004)
[31] Naccache, D.: Secure and *practical* identity-based encryption. Cryptology ePrint Archive, Report 2005/369 (2005), `http://eprint.iacr.org/`
[32] Rackoff, C., Simon, D.R.: Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In: Feigenbaum, J. (ed.) CRYPTO 1991. LNCS, vol. 576, pp. 433–444. Springer, Heidelberg (1992)
[33] Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing over elliptic curve (in japanese). In: Proceedings of the Symposium on Cryptography and Information Security — SCIS 2001 (Janurary 2001)
[34] Sarkar, P., Chatterjee, S.: Transforming a CPA-secure HIBE protocol into a CCA-secure hibe protocol without loss of security. Cryptology ePrint Archive, Report 2006/362 (2006), `http://eprint.iacr.org/`
[35] Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
[36] Shoup, V.: Lower bounds for discrete logarithms and related problems. In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 256–266. Springer, Heidelberg (1997)
[37] Shoup, V.: Why chosen ciphertext security matters. IBM Research Report RZ 3076 (November 1998)
[38] Waters, B.R.: Efficient identity-based encryption without random oracles. In: Cramer, R.J.F. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)