Direct Chosen-Ciphertext Secure Identity-Based Key Encapsulation Without Random Oracles

Eike Kiltz[1] and David Galindo[2]

[1] CWI Amsterdam
The Netherlands
kiltz@cwi.nl
[2] Radboud University Nijmegen
The Netherlands
d.galindo@cs.ru.nl

Abstract. We describe a new and practical identity-based key encapsulation mechanism that is secure in the standard model against chosen-ciphertext (CCA2) attacks. Since our construction is direct and not based on generic transformations from hierarchical identity-based encryption, it is more efficient than all previously proposed schemes.

1 Introduction

Identity-Based Encryption and Key Encapsulation. 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.

Instead of providing the full functionality of an IBE scheme, in many applications it is sufficient to let sender and receiver agree on a common random session key. This can be accomplished with an *identity-based key encapsulation mechanism* (IB-KEM) as formalized in [5]. Any IB-KEM can be updated to a full IBE scheme by adding a symmetric encryption scheme with appropriate security properties.

After Shamir proposed the concept of IBE in 1984 [27] it remained an open problem for almost two decades to come up with a satisfying construction for it. In 2001, Boneh and Franklin [8] 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. IBE is currently in the process of getting standardized — from February 2006 on the new IEEE P1363.3 standard for "Identity-Based Cryptographic Techniques using Pairings" [19] accepts submissions.

An alternative but less efficient IBE construction was proposed by Cocks [14] based on quadratic residues. Both IBE schemes (Cocks' scheme only through Fujisaki-Okamoto [15]) provide security against *chosen-ciphertext attacks*. In

L. Batten and R. Safavi-Naini (Eds.): ACISP 2006, LNCS 4058, pp. 336–347, 2006.

a chosen ciphertext attack, the adversary is given access to a decryption oracle that allows him 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. For different reasons, the notion of chosen-ciphertext security has emerged as the "right" notion of security for encryption schemes. We stress that, in general, chosen-ciphertext security is a much stronger security requirement than chosen-plaintext attacks [3, 16], where in the latter an attacker is not given access to the decryption oracle.

The drawback of the IBE scheme from Boneh-Franklin and Cocks is that security can only be guaranteed in the *random oracle* model [4], i.e. in an idealized world where all parties magically 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 has proved to possibly lead to insecure schemes when the random oracles are implemented in the standard model (see, e.g., [12]).

Waters' IBE. To fill this gap Waters [29] presents the first efficient Identity-Based Encryption scheme that is chosen-plaintext secure without random oracles. The proof of his scheme makes use of an algebraic method first used by Boneh and Boyen [6] and security of the scheme is based on the Bilinear Decisional Diffie-Hellman (BDDH) assumption. However, Waters' plain IBE scheme only guarantees chosen-plaintext security.

From 2-level Hierarchical IBE to chosen-ciphertext secure IBE. Hierarchical identity-based encryption (HIBE) [18, 17] is a generalization of IBE allowing for hierarchical delegation of decryption keys.

Recent results from Canetti, Halevi, and Katz, further improved upon by Boneh and Katz [10] show a generic and practical transformation from any chosen-plaintext secure 2-level HIBE scheme to a chosen-ciphertext secure IBE scheme. Since Waters' IBE scheme can naturally be extended to a 2-level HIBE this implies the first chosen-ciphertext secure IBE in the standard model. Key size, as well as the security reduction of the resulting scheme are comparable to the ones from Waters' IBE. However, the transformation involves some symmetric overhead to the ciphertext in form of a one-time signature or a MAC with their respective keys.

1.1 Our Contributions

Our two main contributions can be summarized as follows.

A direct chosen-ciphertext secure IB-KEM based on Waters' IBE. Our main idea is to enhance (the IB-KEM version of) Waters *chosen-plaintext* secure IBE by adding some redundant information to the ciphertext (consisting of a single group element) to make it *chosen-ciphertext* secure. This information is used to check whether a given IB-KEM ciphertext was "properly

generated" by the encryption algorithm or not; if so decryption is done as before, otherwise the ciphertext is simply rejected. Intuitively, this "consistency check" is what gives us the necessary leverage to deal with the stronger chosen-ciphertext attacks. Unfortunately implementing the consistency check is relatively expensive and an equivalent "implicit rejection" method is used to improve efficiency.

This provides the first direct construction of a chosen-ciphertext secure IB-KEM that is not explicitly derived from hierarchical techniques. No exogenous consistency test relying on a symmetric primitive like one-time signatures or MACs is required. Our scheme can be proved secure under the Bilinear Decisional Diffie-Hellman (BDDH) assumption in pairing groups. Chosen-ciphertext security is obtained at sheer minimal cost. Compared to Waters' IB-KEM our scheme comes with a ciphertext overhead of only one single element whereas computational overhead is one more exponentiation for encryption and one pairing plus two exponentiations for decryption. The security reduction is comparable to the one for Waters' scheme, i.e. it introduces only a small additive component.

Using a chosen-ciphertext secure symmetric encryption scheme (also called a data-encapsulation mechanism DEM) our IB-KEM can be extended to a chosen-ciphertext secure IBE scheme [5]. From a theoretical point of view IB-KEM and IBE are equivalent. However, there are a numerous practical reasons to prefer a IB-KEM over an IBE scheme. The biggest advantage is its flexibility, i.e. an IB-KEM completely decouples the key encapsulation from the asymmetric part. So when performing encryption one is free to pick whatever security parameter necessary without changing the size of the message space. For (standard) public-key encryption the same modular approach is incorporated in many standards due to his simplicity and flexibility (see, e.g., [28, 2]). The same is expected to happen in the new IEEE P1363.3 standard for "Identity-Based Cryptographic Techniques using Pairings" [19].

Our IB-KEM scheme can be extended in a natural way to obtain a chosen-ciphertext secure HIB-KEM with only one additional element in the ciphertext compared to Waters' chosen-plaintext secure HIB-KEM.

A RIGOROUS GAME-BASED PROOF. The proof of Waters' IBE is already quite complex and has many technical parts that we found pretty hard to verify. Additionally, many recent results [11, 13, 23] already use ingredients of Waters' IBE, some more or less in a "black-box" manner which makes verification nearly impossible without having completely understood the original work. This goes along with a general movement in our field to produce proofs that are increasingly hard to verifyour opinion this situation has been getting worse and worse. Our additional components to make Waters IB-KEM chosen-ciphertext secure add even more complexity to the proof.

Motivated by this we give a rigorous, games-based proof of our result that can be easily understood and verified. As an immediate benefit our security reduction achieves some slight improvements over Waters bounds [29]. Unfortunately our proof extends by far the page limit of this extended abstract. The interested reader is referred to [22] for the full details.

1.2 Related Work and Comparison

In this paper we extract the "IB-KEM part" of our pre-print [22] where we furthermore show how our IB-KEM can be extended to the first chosen-ciphertext secure threshold IB-KEM in the standard model. Our technique to obtain the chosen-ciphertext secure IB-KEM is somewhat reminiscent of the method used in [11, 21] to obtain chosen-ciphertext secure *standard encryption*. Interestingly our scheme can be seen as a generalization of the standard public-key encryption scheme from [11], i.e. ignoring all "identity-based components" (and applying some optimizations in the decapsulation algorithm) our scheme can be simplified to exactly their scheme.

In the same work [11] a technique is sketched how to avoid the CHK transformation to get a direct chosen-ciphertext secure IB-KEM construction based on Waters' 2-level HIB-KEM. Compared to our IB-KEM, however, this construction has a weaker (quadratic) security reduction and nearly doubles the public key size. In [22] we carefully review all known chosen-ciphertext secure IB-KEM constructions, including the above proposal, and make an extensive comparison with our scheme.

It turns out that, to the best of our knowledge, our IB-KEM is the most efficient chosen-ciphertext secure IB-KEM scheme in the standard model based on a standard complexity-theoretic assumption.

2 Definitions

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 $s \xleftarrow{\$} S$ denotes the operation of picking an element s of S uniformly at random. We write $\mathcal{A}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and by $z \xleftarrow{\$} \mathcal{A}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and letting z be the output. We write $\mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ to indicate that $\mathcal{A}$ is an algorithm with inputs $x, y, \ldots$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$ and by $z \xleftarrow{\$} \mathcal{A}^{\mathcal{O}_1, \mathcal{O}_2, \cdots}(x, y, \ldots)$ we denote the operation of running $\mathcal{A}$ with inputs $(x, y, \ldots)$ and access to oracles $\mathcal{O}_1, \mathcal{O}_2, \ldots$, and letting z be the output.

2.2 Identity Based Key Encapsulation

An *identity-based key-encapsulation mechanism* (IB-KEM) scheme $\mathcal{IBKEM} = (\mathsf{IBKEMkg}, \mathsf{IBKEMkeyder}, \mathsf{IBKEMenc}, \mathsf{IBKEMdec})$ consists of four polynomial-time algorithms. Via $(pk, msk) \xleftarrow{\$} \mathsf{IBKEMkg}(1^k)$ the randomized key-generation algorithm produces master keys for security parameter $k \in \mathbb{N}$; via $sk[id] \xleftarrow{\$} \mathsf{IBKEMkeyder}(msk, id)$ the master computes the secret key for identity id; via $(C, K) \xleftarrow{\$} \mathsf{IBKEMenc}(pk, id)$ a sender creates a random session key K and a corresponding ciphertext C with respect to identity id; via $K \leftarrow \mathsf{IBKEMdec}(sk, C)$

the possessor of secret key sk decapsulates ciphertext C to get back a the session key K. Associated to the scheme is a key space KeySp. For consistency, we require that for all $k \in \mathbb{N}$, all identities id, and all $(C, K) \xleftarrow{\$} \mathsf{IBKEMenc}(pk, id)$, we have $\Pr[\mathsf{IBKEMdec}(\mathsf{IBKEMkeyder}(msk, id), C) = K] = 1$, where the probability is taken over the choice of $(pk, msk) \xleftarrow{\$} \mathsf{IBKEMkg}(1^k)$, and the coins of all the algorithms in the expression above.

Let $\mathcal{IBKEM} = (\mathsf{IBKEMkg}, \mathsf{IBKEMkeyder}, \mathsf{IBKEMenc}, \mathsf{IBKEMdec})$ be an IB-KEM with associated key space KeySp. To an adversary $\mathcal{A}$ we associate the following experiment:

Experiment $\mathbf{Exp}^{\text{ib-kem-cca}}_{\mathcal{IBKEM},\mathcal{A}}(k)$
$(pk, msk) \xleftarrow{\$} \mathsf{IBKEMkg}(1^k)$
$(id^*, st) \xleftarrow{\$} \mathcal{A}^{\textsc{KeyDer}(\cdot),\textsc{Dec}(\cdot,\cdot)}(\mathtt{find}, pk)$
$K_0^* \xleftarrow{\$} \mathsf{KeySp}\,;\ (C^*, K_1^*) \xleftarrow{\$} \mathsf{IBKEMenc}(pk, id)$
$\gamma \xleftarrow{\$} \{0,1\}\,;\ K^* \leftarrow K_\gamma^*$
$\gamma' \xleftarrow{\$} \mathcal{A}^{\textsc{KeyDer},\textsc{Dec}}(\mathtt{guess}, K^*, C^*, st)$
If $\gamma \neq \gamma'$ then return 0 else return 1

The oracle $\textsc{KeyDer}(id)$ returns $sk[id] \xleftarrow{\$} \textsc{KeyDer}(msk, id)$ with the restriction that $\mathcal{A}$ is not allowed to query oracle $\textsc{KeyDer}(\cdot)$ for the target identity id^*. The oracle $\textsc{Dec}(id, C)$ first computes $sk[id] \xleftarrow{\$} \textsc{KeyDer}(msk, id)$ as above and then returns $K \leftarrow \mathsf{IBKEMdec}(sk[id], id, C)$ with the restriction that in the guess stage $\mathcal{A}$ is not allowed to query oracle $\textsc{Dec}(\cdot,\cdot)$ for the tuple (id^*, C^*). st is some internal state information of adversary $\mathcal{A}$ and can be any (polynomially bounded) string. We define the advantage of $\mathcal{A}$ in the IND-CCA experiment as

$$\mathbf{Adv}^{\text{ib-kem-cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) \;=\; \left|\Pr\left[\,\mathbf{Exp}^{\text{ib-kem-cca}}_{\mathcal{IBKEM},\mathcal{A}}(k) = 1\,\right] - \frac{1}{2}\right| .$$

An IB-KEM $\mathcal{IBKEM}$ is said to be *secure against adaptively-chosen ciphertext attacks* if the advantage functions $\mathbf{Adv}^{\text{ib-kem-cca}}_{\mathcal{IBKEM},\mathcal{A}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{A}$.

We remark that our security definition is given with respect to "full-identity" attacks, as opposed to the much weaker variant of "selective-identity" attacks where the adversary has to commit to its target identity id^* in advance, even before seeing the public key.

2.3 Target Collision Resistant Hash Functions

Let $\mathcal{F} = (\mathsf{TCR}_s)_{s \in S}$ be a family of hash functions for security parameter k and with seed $s \in S = S(k)$. $\mathcal{F}$ is said to be *collision resistant* if, for a hash function $\mathsf{TCR} = \mathsf{TCR}_s$ (where the seed is chosen at random from S), it is infeasible for an efficient adversary to find two distinct values $x \neq y$ such that $\mathsf{TCR}(x) = \mathsf{TCR}(y)$.

A weaker notion is that of *target collision resistant hash functions*. Here it should be infeasible for an efficient adversary to find, given a randomly chosen

element x and a randomly drawn hash function $\mathsf{TCR} = \mathsf{TCR}_s$, a distinct element $y \neq x$ such that $\mathsf{TCR}(x) = \mathsf{TCR}(y)$. (In collision resistant hash functions the value x may be chosen by the adversary.) Such hash functions are also called *universal one-way hash functions* [24] and can be built from arbitrary one-way functions [24, 25]. We define (slightly informal)

$$\mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k) = \Pr[\mathcal{H} \text{ finds a collision in } \mathsf{TCR}].$$

Hash function family TCR is said to be a *target collision resistant* if the advantage function $\mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}$ is a negligible function in k for all polynomial-time adversaries $\mathcal{H}$.

In practice, to build a target collision resistant hash function TCR, one can use a dedicated cryptographic hash function, like SHA-1 [26]. For that reason and to simplify our presentation, in what follows we will consider the hash function TCR to be a fixed function.

3 Assumptions

3.1 Parameter Generation Algorithms for Bilinear Groups

All pairing based schemes will be parameterized by a *pairing parameter generator*. This is a PTA $\mathcal{G}$ that on input 1^k returns the description of an multiplicative cyclic group $\mathbb{G}_1$ 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 $\hat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$. See [9] for a description of the properties of such pairings. We use $\mathbb{G}_1^*$ to denote $\mathbb{G}_1 \setminus \{0\}$, i.e. the set of all group elements except the neutral element. Throughout the paper we use $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_T, p, \hat{e})$ as shorthand for the description of bilinear groups.

3.2 The BDDH Assumption

Let $\mathcal{PG}$ be the description of pairing groups. Consider the following problem first considered by Joux [20] and later formalized by Boneh and Franklin [9]: Given $(g, g^a, g^b, g^c, W) \in \mathbb{G}_1^4 \times \mathbb{G}_T$ as input, output yes if $W = \hat{e}(g,g)^{abc}$ and no otherwise. More formally, to a parameter generation algorithm for pairing-groups $\mathcal{G}$ and an adversary $\mathcal{B}$ we assotiate the following experiment.

Experiment $\mathbf{Exp}^{\text{bddh}}_{\mathcal{G},\mathcal{B}}(k)$
$\mathcal{PG} \xleftarrow{\$} \mathcal{G}(1^k)$
$a, b, c, w \xleftarrow{\$} \mathbb{Z}_p^*$
$\beta \xleftarrow{\$} \{0,1\}$
If $\beta = 1$ then $W \leftarrow \hat{e}(g,g)^{abc}$ else $W \leftarrow \hat{e}(g,g)^{w}$
$\beta' \xleftarrow{\$} \mathcal{B}(1^k, \mathcal{PG}, g, g^a, g^b, g^c, W)$
If $\beta \neq \beta'$ then return 0 else return 1

We define the advantage of $\mathcal{B}$ in the above experiment as

$$\mathbf{Adv}^{\mathrm{bddh}}_{\mathcal{G},\mathcal{B}}(k) \;=\; \left|\Pr\left[\,\mathbf{Exp}^{\mathrm{bddh}}_{\mathcal{G},\mathcal{B}}(k)=1\,\right]-\frac{1}{2}\right| .$$

We say that the *Bilinear Decision Diffie-Hellman (BDDH) assumption relative to generator* $\mathcal{G}$ holds if $\mathbf{Adv}^{\mathrm{bddh}}_{\mathcal{G},\mathcal{B}}$ is a negligible function in k for all PTAs $\mathcal{B}$. The BDDH assumption was shown to hold in the generic group model in [7].

4 A Chosen-Ciphertext Secure IB-KEM Based on BDDH

In this section we present our new chosen-ciphertext secure IB-KEM. From now on let $\mathcal{PG} = (\mathbb{G}_1, \mathbb{G}_T, p, \hat{e}, g)$ be public system parameters obtained by running the group parameter algorithm $\mathcal{G}(1^k)$.

4.1 Waters' Hash Function

We review the hash function $\mathsf{H} : \{0,1\}^n \to \mathbb{G}_1$ used in Waters' identity based encryption schemes [29]. On input of an integer n, the randomized hash key generator $\mathsf{HGen}(\mathbb{G}_1)$ chooses $n+1$ random groups elements $h_0, \ldots, h_n \in \mathbb{G}_1$ and returns $h = (h_0, h_1, \ldots, h_n)$ as the public description of the hash function. The hash function $\mathsf{H} : \{0,1\}^n \to \mathbb{G}_1^*$ is evaluated on a string $id = (id_1, \ldots, id_n) \in \{0,1\}^n$ as the product

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

4.2 The IB-KEM Construction

Let $\mathsf{TCR} : \mathbb{G}_1 \to \mathbb{Z}_p$ be a target collision-resistant hash function (which we assume to be included in the system parameters). Our IB-KEM with identity space $\mathsf{IDSp} = \{0,1\}^n$ ($n = n(k)$) and key space $\mathsf{KeySp} = \mathbb{G}_T$ is depicted in Fig. 1.

A tuple $(g, c_1, u_1^t u_2, c_3)$ is a Diffie-Hellman tuple[1] if $\hat{e}(g, c_3) = \hat{e}(u_1^t u_2, c_1)$. Analogously, $(g, c_1, \mathsf{H}(id), c_2)$ is a Diffie-Hellman tuple if $\hat{e}(g, c_2) = \hat{e}(\mathsf{H}(id), c_1)$. Therefore the check in the decapsulation algorithm $\mathsf{IBKEMdec}$ can be implemented by evaluating the bilinear map four times.

We now show correctness of the scheme, i.e. that the session key K computed in the encapsulation algorithm matches the K computed in the decapsulation algorithm. A correctly generated ciphertext for identity id has the form $C = (c_1, c_2, c_3) = (g^r, \mathsf{H}(id)^r, (u_1^t u_2)^r)$ and therefore $(g, c_1, u_1^t u_2, c_3) = (g, g^r, u_1^t u_2, (u_1^t u_2)^r)$ is always a DH tuple. A correctly generated secret key for identity id has the form $sk[id] = (d_1, d_2) = (\alpha \cdot \mathsf{H}(id)^s, g^s)$. Therefore the decapsulation algorithm computes the session key K as

[1] A tuple $(h, h^a, h^b, h^c) \in \mathbb{G}_1^4$ is said to be a *Diffie-Hellman tuple* if $ab = c \bmod p$.

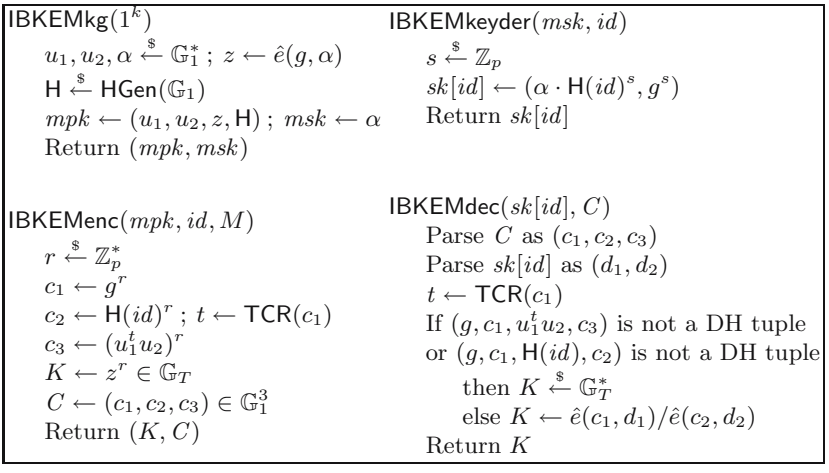

Fig. 1. Our chosen-ciphertext secure IB-KEM

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

as the key computed in the encapsulation algorithm. This shows correctness.

Let $C = (c_1, c_2, c_3) \in \mathbb{G}_1^3$ be a (possibly malformed) ciphertext. Ciphertext C is called *consistent* (w.r.t the public key pk and identity id) if $(g, c_1, u_1^t u_2, c_3)$ and $(g, c_1, \mathsf{H}(id), c_2)$ are Diffie-Hellman tuples, where $t = \mathsf{TCR}(c_1)$. Note that any ciphertext properly generated by the encapsulation algorithm is always consistent. The decapsulation algorithm tests for consistency of the ciphertext. Note that this consistency test can be performed by anybody knowing the public-key. We call this property "public verification" of the ciphertext. In the words of [1] the IB-KEM ciphertext is not *anonymous*.

4.3 More Efficient Decapsulation

We now describe an alternative decapsulation algorithm which is more efficient (but less intuitive). The idea is to make the Diffie-Hellman consistency check implicit in the computation of the key K. This is done by choosing a random values $r_1, r_2 \in \mathbb{Z}_p^*$ and computing the session key as

$$K \leftarrow \frac{\hat{e}(c_1, d_1 \cdot (u_1^t u_2)^{r_1} \cdot \mathsf{H}(id)^{r_2})}{\hat{e}(c_2, d_2 \cdot g^{r_2}) \cdot \hat{e}(g^{r_1}, c_3)} .$$

We claim that this is equivalent to first checking for consistency and then computing the key as $K \leftarrow \hat{e}(c_1, d_1)/\hat{e}(c_2, d_2)$ as in the original decapsulation algorithm.

To prove this claim we define the functions $\Delta_1(C) = \hat{e}(c_1, u_1^t u_2)/\hat{e}(g, c_3)$ and $\Delta_2(C) = \hat{e}(\mathsf{H}(id), c_1)/\hat{e}(g, c_2)$. Then $\Delta_1(C) = \Delta_2(C) = 1$ if and only if C is consistent. Consequently, for random $r_1, r_2 \in \mathbb{Z}_p^*$, $K = \hat{e}(c_1, d_1)/\hat{e}(c_2, d_2) \cdot (\Delta_1(C))^{r_1} \cdot (\Delta_2(C))^{r_2} \in \mathbb{G}_T^*$ evaluates to $\hat{e}(c_1, d_1)/\hat{e}(c_2, d_2) \in \mathbb{G}_T$ if C is consistent and to a random group element otherwise. As in the original decapsulation algorithm. The claim then follows by

$$\begin{aligned} K &= \hat{e}(c_1, d_1)/\hat{e}(c_2, d_2) \cdot \Delta_1(C)^{r_1} \cdot (\Delta_2(C))^{r_2} \\ &= \hat{e}(c_1, d_1)/\hat{e}(c_2, d_2) \cdot (\hat{e}(c_1, u_1^t u_2)/\hat{e}(g, c_3))^{r_1} \cdot (\hat{e}(\mathsf{H}(id), c_1)/\hat{e}(g, c_2))^{r_2} \\ &= \frac{\hat{e}(c_1, d_1 (u_1^t u_2)^{r_1} \mathsf{H}(id)^{r_2})}{\hat{e}(c_2, d_2 \cdot g^{r_2}) \cdot \hat{e}(g^{r_1}, c_3)} \, . \end{aligned}$$

We remark that the alternative decapsulation algorithm roughly saves two pairing operation (for the cost of a couple of exponentiations).

4.4 Security

Theorem 1. *Assume* TCR *is a target collision resistant hash function. Under the Bilinear Decisional Diffie-Hellman (BDDH) assumption relative to generator* $\mathcal{G}$*, the IB-KEM from Section 4.2 is secure against chosen-ciphertext attacks. In particular, we have*

$$\mathbf{Adv}^{\text{ib-kem-cca}}_{\mathcal{IBKEM},\mathcal{A}} = \mathcal{O}(nq \cdot (\epsilon + q/p) + \mathbf{Adv}^{\text{hash-tcr}}_{\mathsf{TCR},\mathcal{H}}(k)) \, ,$$

for any IBE adversary $\mathcal{A}$ *running for time* $\mathbf{Time}_{\mathcal{A}}(k) = \mathbf{Time}_{\mathcal{B}} - \Omega(\epsilon^{-2} \cdot \ln(\epsilon^{-1}) + q)$*, where* $\epsilon = \mathbf{Adv}^{\text{bddh}}_{\mathcal{G},\mathcal{B}}(k)$ *and* q *is an upper bound on the number of key derivation/decapsulation queries made by adversary* $\mathcal{A}$*.*

A game-based proof of Theorem 1 can be found in [22]. The proof is mainly based on the one given by Waters [29]. However, we have to do some important modifications to be able to deal with chosen-ciphertext attacks. Furthermore, compared to Waters proof we can achieve a slightly improved security reduction.

Intuitively, security can be best understood by observing that our scheme is a generalization of Waters' (chosen-plaintext secure) IBE scheme, as well as of the chosen-ciphertext secure *public-key* encapsulation scheme from [11]. We remark that unfortunately, there does not seem to be a way to derive security of our IBE scheme directly from security of either of the two schemes and hence details of the whole proof have to be worked out from scratch.

Relation to Waters' IBE scheme. The ciphertext in our scheme is basically identical to the ciphertext from Waters' IBE scheme [29] plus one redundant element (the element c_3) used to check for consistency of the ciphertext. Hence Waters' IBE scheme is obtained by ignoring the computation of c_3 in encapsulation as well as the consistency check in decapsulation.

Relation to the Encryption Scheme from BMW. Clearly, IB-KEM implies (standard) public-key encapsulation by simply ignoring all operations related to the identity. We remark that viewed in this light (i.e. ignoring the

element c_2 in encapsulation/decapsulation and ignoring the key derivation algorithm) our IB-KEM can be simplified to the chosen-ciphertext secure encryption scheme recently proposed by Boyen, Mei, and Waters [11].

5 Extensions

5.1 Chosen-Ciphertext Secure Hierarchical Identity-Based Key Encapsulation

Hierarchical identity-based key encapsulation (HIB-KEM) is a generalization of IB-KEM to identities supporting hierarchical structures [18, 17]. By the relation to Waters IBE scheme it is easy to see that our technique can also be used to make (the KEM variant of) Waters' HIBE chosen-ciphertext secure. To be more precise, we modify Waters' HIB-KEM and add one more element $h_1^{rt}h_2^r$ to the the ciphertext, where t was computed by applying a target-collision hash function to g^r (here r is the randomness used to create the ciphertext). The additional element is used for a consistency check at decryption. The security reduction is exponential in the depth d of the hierarchy, i.e. it introduces, roughly, a multiplicative factor of $(nq)^d$.

5.2 Identity-Based Encryption

Given a IB-KEM and a symmetric encryption scheme, a hybrid identity-based encryption scheme can be obtained by using the IB-KEM to securely transport a random session key that is fed into the symmetric encryption scheme to encrypt the plaintext message. It was recently shown in [5] that if both the IB-KEM and the symmetric encryption scheme are chosen-ciphertext secure, then the resulting hybrid encryption is also chosen-ciphertext secure. The security reduction is tight.

5.3 A Tradeoff Between Public Key Size and Security Reduction

As independently discovered in [13, 23], there exists an interesting trade-off between key-size of Waters' hash H and the security reduction of the IBE scheme.

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 $\mathsf{H} : \{0,1\}^n \to \mathbb{G}_1$, with $\mathsf{H}(id) = h_0 \prod_{i=1}^{n/l} h_i^{id_i}$ for random public elements $h_0, h_1, \ldots, h_{n/l} \in \mathbb{G}_1$. 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 $n+4$ to $n/l+4$ group elements, whereas (ii) it adds another multiplicative factor of 2^l to the security reduction of the IBE scheme (Theorem 1).

5.4 Selective-Identity Chosen-Ciphertext Secure IB-KEM

For the definition of a selective-identity chosen-ciphertext secure IB-KEM we change the security experiment such that the adversary has to commit to the

target idenity id^* before seeing the public key. Clearly, this is a weaker security requirement. We quickly note that (using an algebraic technique from [6]) by replacing Waters' hash H with $\mathsf{H}(id) = h_0 \cdot h_1^{id}$ (for $id \in \mathbb{Z}_p$) we get a selective-id chosen-ciphertext secure IB-KEM. Note that the size of the public-key of this scheme drops to 3 elements.

5.5 Implementing the Collision Resistant Hash Function TCR

In practice, to build a target collision resistant hash function, one can use a dedicated cryptographic hash function, like SHA-1 [26].

Every injective function $\mathsf{TCR} : \mathbb{G}_1 \to \mathbb{Z}_p$ trivially also is (target) collision resistant (with zero advantage). Boyen, Mei and Waters [11] note that for bilinear maps defined on elliptic curves there exists a very efficient way to implement such injective mappings. We refer to [11] for more details.

References

1. M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange, J. Malone-Lee, G. Neven, P. Paillier, and H. Shi. Searchable encryption revisited: Consistency properties, relation to anonymous ibe, and extensions. In V. Shoup, editor, *CRYPTO 2005*, LNCS. Springer-Verlag, Aug. 2005.
2. American National Standards Institute (ANSI) X9.F1 subcommittee. ANSI X9.63 Public key cryptography for the Financial Services Industry: Elliptic curve key agreement and key transport schemes, July 5, 1998. Working draft version 2.0.
3. M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, *CRYPTO'98*, volume 1462 of *LNCS*, pages 26–45. Springer-Verlag, Aug. 1998.
4. M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM CCS 93*, pages 62–73. ACM Press, Nov. 1993.
5. K. Bentahar, P. Farshim, J. Malone-Lee, and N. Smart. Generic constructions of identity-based and certificateless KEMs. Cryptology ePrint Archive, Report 2005/058, 2005. `http://eprint.iacr.org/`.
6. D. Boneh and X. Boyen. Efficient selective-id secure identity based encryption without random oracles. In C. Cachin and J. Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *LNCS*, pages 223–238. Springer-Verlag, May 2004.
7. D. Boneh, X. Boyen, and E.-J. Goh. Hierarchical identity based encryption with constant size ciphertext. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 440–456. Springer-Verlag, May 2005.
8. D. Boneh and M. K. Franklin. Identity-based encryption from the Weil pairing. In J. Kilian, editor, *CRYPTO 2001*, volume 2139 of *LNCS*, pages 213–229. Springer-Verlag, Aug. 2001.
9. D. Boneh and M. K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003.
10. D. Boneh and J. Katz. Improved efficiency for CCA-secure cryptosystems built using identity-based encryption. In A. Menezes, editor, *CT-RSA 2005*, volume 3376 of *LNCS*, pages 87–103. Springer-Verlag, Feb. 2005.

11. X. Boyen, Q. Mei, and B. Waters. Simple and efficient CCA2 security from IBE techniques. In *ACM Conference on Computer and Communications Security—CCS 2005*, pages 320–329. New-York: ACM Press, 2005. Available at `http://eprint.iacr.org/2005/288/`, August 2005.
12. R. Canetti, O. Goldreich, and S. Halevi. The random oracle methodology, revisited. In *30th ACM STOC*, pages 209–218. ACM Press, May 1998.
13. S. Chatterjee and P. Sarkar. Trading time for space: Towards an efficient ibe scheme with short(er) public parameters in the standard model. Proceedings of ICISC, to appear, 2005.
14. C. Cocks. An identity based encryption scheme based on quadratic residues. In B. Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *LNCS*, pages 360–363, Cirencester, UK, Dec. 17–19, 2001. Springer-Verlag.
15. E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 537–554. Springer-Verlag, Aug. 1999.
16. D. Galindo and I. Hasuo. Security notions for identity based encryption. Cryptology ePrint Archive, Report 2005/253, 2005. `http://eprint.iacr.org/`.
17. C. Gentry and A. Silverberg. Hierarchical ID-based cryptography. In Y. Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 548–566. Springer-Verlag, Dec. 2002.
18. J. Horwitz and B. Lynn. Toward hierarchical identity-based encryption. In L. R. Knudsen, editor, *EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 466–481. Springer-Verlag, Apr. 2002.
19. IEEE P1363.3 Committee. IEEE 1363.3 / CfS — standard for identity-based cryptographic techniques using pairings. `http://grouper.ieee.org/groups/1363/index.html/`, Feb. 2006. Call for submissions.
20. A. Joux. A one round protocol for tripartite diffie-hellman. In *Algorithmic Number Theory – ANTS IV*, volume 1838 of *LNCS*, pages 385–394. Springer-Verlag, 2000.
21. E. Kiltz. Chosen-ciphertext security from tag-based encryption. In S. Halevi and T. Rabin, editors, *TCC 2006*, LNCS, pages 581–600. Springer-Verlag, Mar. 2006.
22. E. Kiltz and D. Galindo. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles, Jan. 2006. Available at `http://eprint.iacr.org/2006/034/`.
23. D. Naccache. Secure and *practical* identity-based encryption. Cryptology ePrint Archive, Report 2005/369, 2005. `http://eprint.iacr.org/`.
24. M. Naor and M. Yung. Universal one-way hash functions and their cryptographic applications. In *21st ACM STOC*, pages 33–43. ACM Press, May 1989.
25. J. Rompel. One-way functions are necessary and sufficient for secure signatures. In *22nd ACM STOC*, pages 387–394. ACM Press, May 1990.
26. Secure hash standard. National Institute of Standards and Technology, NIST FIPS PUB 180-1, U.S. Department of Commerce, Apr. 1995.
27. A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO'84*, volume 196 of *LNCS*, pages 47–53. Springer-Verlag, Aug. 1985.
28. V. Shoup. A proposal for an ISO standard for public key encryption (version 2.1). manuscript, 2001. Available on `http://shoup.net/papers/`.
29. B. R. Waters. Efficient identity-based encryption without random oracles. In R. Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *LNCS*, pages 114–127. Springer-Verlag, May 2005.