From Selective-ID to Full Security: The Case of the Inversion-Based Boneh-Boyen IBE Scheme

Eike Kiltz

CWI Amsterdam, The Netherlands
kiltz@cwi.nl
http://kiltz.net

Abstract

In this note we remark that the inversion-based selective-ID secure identity-based encryption (IBE) scheme from Boneh and Boyen can be bootstrapped to full-ID security using a technique by Waters.

Keywords: Identity-based Encryption, full-ID security.

1 Introduction

An Identity-Based Encryption (IBE) scheme is a public-key (asymmetric) encryption scheme where any string such as email addresses, server names or phone numbers, can be used as public keys. The ability to use identities as public keys largely reduces the need for public key certificates and certificate authorities to distribute public key certificates.

After Shamir proposed the concept of IBE in 1984 [Sha85] it remained an open problem for almost two decades to come up with a satisfying construction for it. In 2001, Boneh and Franklin [BF03] proposed an IBE scheme using bilinear maps and proved its security in the idealized random oracle model. Boneh and Boyen proposed two IBE schemes without random oracles [BB04a]. However, security could only be proved in the restricted selective-ID security model where an adversary has to commit to the "attack-identity" before even seeing the public key. Waters [Wat05] modified the first (BDDH-based) scheme of Boneh and Boyen to obtain a practical IBE scheme which is secure in the full-ID model.

In this paper we remark that Waters' technique can also be applied to the second (inversion-based) IBE scheme of Boneh and Boyen to obtain an alternative IBE scheme secure in the full-ID model. A second IBE scheme is obtained by applying a different randomization technique due to Gentry [Gen06]. The resulting IBE schemes are slightly more efficient than Waters' IBE whereas security is based on a stronger security assumption, the q-BDDHI assumption.

Even though we mostly combine known results from [BB04a, Wat05, Gen06] to obtain our schemes we hope our exposition helps understanding available "inversion-based" IBE techniques.

2 Preliminaries

2.1 Identity Based Encryption

An *identity-based encryption* (IBE) scheme [Sha85, BF03] $\mathcal{IBE} = (\mathsf{Kg}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ consists of four polynomial-time algorithms. Via $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$ the randomized key-generation algorithm produces master keys for security parameter $k \in \mathbb{N}$; via $usk[id] \overset{\$}{\leftarrow} \mathsf{Extract}(sk, id)$ the master computes the secret key for identity id; via $C \overset{\$}{\leftarrow} \mathsf{Enc}(pk, id, m)$ a sender creates a ciphertext C with respect to message m and identity id; via $m \leftarrow \mathsf{Dec}(sk, C)$ the possessor of secret key sk decrypts ciphertext C to get back a message m. For consistency, we require that for all $k \in \mathbb{N}$, all identities id, all messages m and all $C \overset{\$}{\leftarrow} \mathsf{Enc}(pk, id)$, we have $\Pr[\mathsf{Dec}(\mathsf{Extract}(sk, id), C) = K] = 1$, where the probability is taken over the choice of $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$, and the coins of all the algorithms in the expression above.

We now define security against chosen-plaintext attacks (IND-CPA) by associating to an adversary $\mathcal{A}$ the following experiment.

```
Experiment $\mathbf{Exp}^{\text{ind-cpa}}_{\mathcal{IBE},\mathcal{A}}(k)$
  $(pk, sk) \overset{\$}{\leftarrow} \mathsf{Kg}(1^k)$
  $(id^*, m_0, m_1, St) \overset{\$}{\leftarrow} \mathcal{A}^{\mathsf{Extract}(sk,\cdot)}(\mathit{find}, pk)$
  $b \overset{\$}{\leftarrow} \{0,1\}$ ; $C^* \overset{\$}{\leftarrow} \mathsf{Enc}(pk, id^*, m_b)$
  $b' \overset{\$}{\leftarrow} \mathcal{A}^{\mathsf{Extract}(sk,\cdot)}(\mathit{guess}, C^*, St)$
  If $b \neq b'$ then return 0 else return 1
```

The oracle $\mathsf{Extract}(sk, id)$ returns $sk[id] \overset{\$}{\leftarrow} \mathsf{Extract}(sk, id)$ with the restriction that $\mathcal{A}$ is not allowed to query oracle $\mathsf{Extract}(sk, \cdot)$ for the target identity id^*. The variable St represents some internal state information of adversary $\mathcal{A}$ and can be any (polynomially bounded) string. We define the advantage of $\mathcal{A}$ in the chosen-plaintext experiment as

$$\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{IBE},\mathcal{A}}(k) = \left| \Pr\left[\mathbf{Exp}^{\text{ind-cpa}}_{\mathcal{IBE},\mathcal{A}}(k) = 1 \right] - \frac{1}{2} \right| .$$

An IBE scheme $\mathcal{IBE}$ is said to be indistinguishable against chosen-plaintext attacks (IND-CPA secure) if the advantage functions $\mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{IBE},\mathcal{A}}(k)$ 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.

2.2 Pairings and complexity assumption

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 $\mathbb{G}$ 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 $\hat{e}\colon \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$. See [BF03] 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 $\mathbb{PG} = (\mathbb{G}, \mathbb{G}_T, p, \hat{e}, g)$ as shorthand for the description of bilinear groups, where g is a generator of $\mathbb{G}$.

We require that in $\mathbb{PG}$ the q-BDDHI (q-Bilinear Decisional Diffie-Hellman Inversion) [BB04a] problem is computationally hard which is captured by defining the q-bddhi-advantage of an adversary $\mathcal{B}$ as

$$\mathbf{Adv}^{\text{q-bddhi}}_{\mathbb{PG},\mathcal{B}}(k) = \Pr[\mathcal{B}(g, g^x, \ldots, g^{x^q}, \hat{e}(g,g)^{1/x}) = 1] - \Pr[\mathcal{B}(g, g^x, \ldots, g^{x^q}, W) = 1],$$

where $g, W \overset{\$}{\leftarrow} \mathbb{G}_T$ and $x \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. We say that the q-BDDHI assumption holds in $\mathbb{PG}$ if the advantage functions $\mathbf{Adv}^{\text{q-bddhi}}_{\mathbb{PG},\mathcal{B}}(k)$ is a negligible function in k for all polynomial-time adversaries $\mathcal{B}$.

3 Identity-Based Encryption

3.1 The IBE scheme

Our starting point is the second IBE scheme from Boneh and Boyen [BB04a] which can only proved to be selective-ID IND-CPA secure. We apply a hashing technique (or "implicit Chameleon hash") due to Waters [Wat05] to make it full-ID IND-CPA secure.

Let $\mathbb{PG}$ be a bilinear group. The following IBE scheme $\mathcal{IBE} = (\mathsf{Kg}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ encrypts messages $m \in \mathbb{G}_T$ to arbtrary identities $id = (id_1, \ldots, id_n) \in \{0,1\}^n$.

```
$\mathsf{Kg}(\mathbb{PG}, 1^k)$
    For $0 \le i \le n$: $x_i \xleftarrow{\$} \mathbb{Z}_p$ ; $X_i \leftarrow g^{x_i}$
    $y \xleftarrow{\$} \mathbb{Z}_p$ ; $Y \leftarrow g^y$
    $pk = (X_0, \ldots, X_n, Y)$ ; $sk = (x_0, \ldots, x_n, y)$
    Return $(sk, pk)$
```

```
$\mathsf{Extract}(sk, id)$
    $s \xleftarrow{\$} \mathbb{Z}_p$
    $d \leftarrow g^{\frac{1}{x_0 + \sum x_i id_i + ys}}$
    $sk[id] \leftarrow (d, s)$
    Return $sk[id]$
```

```
$\mathsf{Enc}(pk, id, M)$
    $r \xleftarrow{\$} \mathbb{Z}_p$
    $c_1 \leftarrow (X_0 \prod_{i=1}^n X_i^{id_i})^r$ ; $c_2 \leftarrow Y^r$
    $K \leftarrow \hat{e}(g, g)^r$ ; $e \leftarrow K \cdot m$
    Return $C = (c_1, c_2, e) \in \mathbb{G} \times \mathbb{G} \times \mathbb{G}_T$
```

```
$\mathsf{Dec}(usk[id], id, C)$
    Parse $C = (c_1, c_2, e)$
    Parse $usk[id] = (d, s)$
    $K \leftarrow \hat{e}(c_1 c_2^s, d)$
    Return $m \leftarrow e \cdot K^{-1}$
```

We remark that in practice one would hash key $K \in \mathbb{G}_T$ to a bit string and use it as a binary key to perform symmetric encryption. To allow arbitrary identities $id \in \{0,1\}^*$ one can apply a collision-resistant hash function.

To show correctness consider the KEM part $(c_1 = (X_0 \prod_{i=1}^n X_i^{id_i})^r, c_2 = Y^r)$ of a correctly generated ciphertext. Decryption with respect to a correct user secret key $(d = g^{\frac{1}{x_0 + \sum x_i id_i + ys}}, s)$ yield the symmetric key

$$\begin{aligned} K &= \hat{e}(c_1 c_2^s, d) \\ &= \hat{e}((X_0 \prod_{i=1}^n X_i^{id_i})^r \cdot Y^s, g^{\frac{1}{x_0 + \sum x_i id_i + ys}}) \\ &= \hat{e}(g^{(x_0 + \sum_{i=1}^n x_i id_i + ys)r}, g^{\frac{1}{x_0 + \sum x_i id_i + ys}}) \\ &= \hat{e}(g, g)^r , \end{aligned}$$

as in encryption.

3.2 Security

Theorem 3.1 The IBE scheme is IND-CPA secure under the q-BDDHI assumption. In particular, given an adversary $\mathcal{A}$ attacking the chosen-plaintext security of the IBE scheme with advantage $\varepsilon_{\mathcal{A}} = \mathbf{Adv}^{\text{ind-cpa}}_{\mathcal{IBE}, \mathcal{A}}$ and running time $\mathbf{Time}_{\mathcal{A}}(k)$ we construct an adversary $\mathcal{B}$ breaking the $q+1$-BDDHI assumption with advantage $\varepsilon_{\mathcal{B}} = \mathbf{Adv}^{\text{q-bddhi}}_{\mathbb{PG}, \mathcal{B}}(k)$ and running time $\mathbf{Time}_{\mathcal{B}}(k)$

with

$$\begin{aligned}\varepsilon_{\mathcal{B}}(k) &\geq \frac{\varepsilon_{\mathcal{A}}(k)}{8(n+1)q} \\ \mathbf{Time}_{\mathcal{B}}(k) &\leq \mathbf{Time}_{\mathcal{A}} + \tilde{\mathcal{O}}(nq \cdot \varepsilon_{\mathcal{A}}^{-2}(k)),\end{aligned}$$

where q is an upper bound on the number of key derivation queries made by adversary $\mathcal{A}$.

A proofsketch will be given in Section 3.5.

3.3 Another IBE variant

We present yet another IBE variant that uses a different "randomization technique" for generating the user secret key which is due to Gentry [Gen06]. Like Gentry's scheme [Gen06] it has the advantage that it is anonymous in the sense that a ciphertext does not leak any information about the recipients' identitiy [ABC$^+$05].

Let $\mathbb{PG}$ be a bilinear group. The following IBE scheme $\mathcal{IBE} = (\mathsf{Kg}, \mathsf{Extract}, \mathsf{Enc}, \mathsf{Dec})$ encrypts messages $m \in \mathbb{G}_T$ to arbtrary identities $id = (id_1, \dots, id_n) \in \{0,1\}^n$.

```
$\mathsf{Kg}(\mathbb{PG}, 1^k)$
    For $0 \leq i \leq n$: $x_i \xleftarrow{\$} \mathbb{Z}_p$ ; $X_i \leftarrow g^{x_i}$
    $z \xleftarrow{\$} \mathbb{Z}_p$ ; $Z \leftarrow \hat{e}(g,g)^z$
    $pk = (X_0, \dots, X_n, Z)$ ; $sk = (x_0, \dots, x_n, z)$
    Return $(sk, pk)$

$\mathsf{Extract}(sk, id)$
    $s \xleftarrow{\$} \mathbb{Z}_p$
    $d \leftarrow g^{\frac{z-s}{x_0 + \sum x_i id_i}}$
    $sk[id] \leftarrow (d, s)$
    Return $sk[id]$

$\mathsf{Enc}(pk, id, M)$
    $r \xleftarrow{\$} \mathbb{Z}_p$
    $c_1 \leftarrow (X_0 \prod_{i=1}^{n} X_i^{id_i})^r$ ; $c_2 \leftarrow Z^r$
    $K \leftarrow \hat{e}(g,g)^r$ ; $e \leftarrow K \cdot m$
    Return $C = (c_1, c_2, e) \in \mathbb{G} \times \mathbb{G}_T \times \mathbb{G}_T$

$\mathsf{Dec}(usk[id], id, C)$
    Parse $C = (c_1, c_2, e)$
    Parse $usk[id] = (d, s)$
    $K \leftarrow \hat{e}(c_1, d) \cdot c_2^s$
    Return $m \leftarrow e \cdot K^{-1}$
```

Under the q-BDDHI assumption the IBE scheme is IND-CPA secure and anonymous. The proof (which is omitted here) uses Cramer-Shoup techniques and combines ideas from the proof of Theorem 3.1 with techniques from [Gen06].

Unfortunately the scheme is not very practical since in practice the element in $c_2 \in \mathbb{G}_T$ ($\mathbb{G}_T$ is usually an order p subgroups of $\mathbb{Z}_{q^\alpha}$ and hence vulnarable to sub-exponential discrete log attacks) needs very large representation. For example, for for 128 bits security one element in $\mathbb{G}_T$ requires *at least* 3072 bits.

3.4 Comparison

We compare our IBE schemes with the ones from Waters [Wat05] and Gentry [Gen06].

Scheme	Enc	Dec	Delegation	Ciphertext		pk	Assumption	Anon?
	#pairings + #exps			Overhead	(bits)			
Waters	$0+3$	$2+0$	$0+2$	$2\lvert\mathbb{G}\rvert$	(512)	$n+2$	BDDH	—
Gentry	$0+3$	$1+1$	$0+1$	$\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	(3.328)	3	q-ABDHE	$\surd$
Ours §3.1	$0+3$	$1+1$	$0+1$	$2\lvert\mathbb{G}\rvert$	(512)	$n+2$	q-BDDHI	—
Ours §3.3	$0+3$	$1+1$	$0+1$	$\lvert\mathbb{G}\rvert + \lvert\mathbb{G}_T\rvert$	(3.328)	$n+2$	q-BDDHI	$\surd$

We remark that the term $(X_0 \prod_{i=1}^n X_i^{id_i})^r$ can be computed as efficient as one (multi-)exponentiation. In terms of security assumptions, we remark that q-ABDHE implies q-BDDHI implies BDDH, i.e. q-ABDHE is the strongest and BDDH is the weakest security assumption.

3.5 Proof of Theorem 3.1

As a technical tool we first introduce the following complexity assumption which is implied by the q-BDDHI assumption but already closer to the proposed IBE scheme. The q-RBDDH (q-Randomized Bilinear Decisional Diffie-Hellman) assumption in $\mathbb{PG}$ is captured by defining the q-rbddh-advantage of an adversary $\mathcal{B}$ as

$$\begin{aligned}\mathbf{Adv}^{\mathrm{q-rbddh}}_{\mathbb{PG},\mathcal{B}}(k) \;&=\; \Pr[\mathcal{B}(g, g^x, t_1, g^{1/(x+t_1)}, \ldots, t_q, g^{1/(x+t_q)}, g^y, \hat{e}(g,g)^{y/x}) = 1] \\ &\quad - \Pr[\mathcal{B}(g, g^x, t_1, g^{1/(x+t_1)}, \ldots, t_q, g^{1/(x+t_q)}, g^y, W) = 1],\end{aligned}$$

where $g, W \overset{\$}{\leftarrow} \mathbb{G}$ and $x, y, t_1, \ldots, t_q \overset{\$}{\leftarrow} \mathbb{Z}_p^*$. The proof of the following simple implication is postponed to Appendix A.

Lemma 3.2 For any polynomial $q(k) \geq 1$, $q+1$-BDDHI $\Rightarrow$ q-RBDDH

Proof of Theorem 3.1: (Sketch) Suppose there exists a polynomial time adversary $\mathcal{A}$ that breaks the IND-CPA security of the IBE scheme and makes at most q key derivation queries. We use the following notation. For a given secret key, we define the function $h : \{0,1\}^n \to \mathbb{Z}_p$ as $h(id) = x_0 + \sum_{i=1}^n x_i id_i$. That means user secret keys are of the form $usk[id] = (g^{\frac{1}{h(id)+ys}}, s)$ and correctly generated IBE ciphertexts of the form $C = (c_1, c_2, e) = ((g^{h(id)})^r, (g^y)^r, \hat{e}(g,g)^r \cdot m)$.

Let $\mathcal{B}$ be an adversary against the q-RBDDH problem, i.e. $\mathcal{B}$ inputs $(g, X = g^x, t_1, T_1 = g^{1/(x+t_1)}, \ldots, t_q, T_q = g^{1/(x+t_q)}, Z = g^z, T)$. $\mathcal{B}$'s goal is to decide if $T = \hat{e}(g,g)^{z/x}$ or if $T \in \mathbb{G}_T$ is random. We show now how $\mathcal{B}$ can use $\mathcal{A}$ as a subroutine to successfully break the q-RBDDH assumption. By Lemma 3.2 this proves the theorem.

Adversary $\mathcal{B}$ is defined as follows.

Setup Adversary $\mathcal{B}$ picks $b_0, \ldots, b_n \overset{\$}{\leftarrow} \mathbb{Z}_p$ and the values $a_0, \ldots, a_n$ according to the following probability distribution $\mathbf{A}$ on $(a_0, \ldots, a_n)$.

$$k \overset{\$}{\leftarrow} \{0, \ldots, n\} \; ; \; a_0', a_1, \ldots, a_n \overset{\$}{\leftarrow} \{0, \ldots, 2q-1\} \; ; \; a_0 \leftarrow -k2q + a_0' \; . \tag{1}$$

Furthermore, a random $c \in \mathbb{Z}_p$ is picked and the public key $pk = (X_0, \ldots, X_n, Y)$ is computed as

$$X_0 = g^{a_0} X^{b_0}, \ldots, X_n \leftarrow g^{a_n} X^{b_n}, Y \leftarrow X^c.$$

Note that this does not change the distribution of pk. Since this implicitly defines the secret values x_i as $x_i = a_i + b_i x$, for each identity $id \in \{0,1\}^n$ we have

$$h(id) = a(id) + b(id)x, \tag{2}$$

with $b(id) = b_0 + \sum_{i=1}^n id_i b_i$ and $a(id) = a_0 + \sum_{i=1}^n id_i a_i$ only known to the simulator.

$\mathcal{B}$ runs $\mathcal{A}$ on pk answering $\mathcal{A}$'s key derivation queries as follows.

Key Derivation Queries. Suppose $\mathcal{A}$ makes a user secret key query for identity $id \in \{0,1\}^n$ and $id = id^{(i)}$ is the ith distinct identity $\mathcal{A}$ has queried, for $i \in \{1,\ldots,q\}$. Adversary $\mathcal{B}$ hopes that

$$a(id) \neq 0 \bmod p \; . \tag{3}$$

Using the tuple (T_i, t_i) from it's input, adversary $\mathcal{B}$ returns a user secret key $usk[id] = (d, s)$ for identity id as

$$d = T_i^{\frac{t_i}{a(id)}}, s = \frac{a(id)/t_i - b(id)}{c},$$

This is a correct user secret key since $s \in \mathbb{Z}_p$ is a uniform random element (since t_i is) and by $t_i/a(id) = 1/(b(id)+cs)$ we have

$$d = T_i^{\frac{t_i}{a(id)}} = (g^{\frac{1}{t_i+x}})^{\frac{1}{b(id)+cs}} = (g^{\frac{1}{a(id)/(b(id)+cs)+x}})^{\frac{1}{b(id)+cs}} = g^{\frac{1}{a(id)+(b(id)+cs)x}} = g^{\frac{1}{h(id)+ys}}$$

If $a(id) = 0 \bmod p$ then adversary $\mathcal{B}$ terminates and returns a random bit b'.

Challenge Suppose $\mathcal{A}$ wants to be challenged on identity id^* and the two messages m_0, m_1. Adversary $\mathcal{B}$ hopes that

$$a(id^*) = 0 \bmod p \; . \tag{4}$$

In that case $\mathcal{B}$ creates that challenge ciphertext as

$$c_1^* = Z^{b(id)} \; ; \quad c_2^* = Z^c \; ; \quad e^* = T \cdot m_d,$$

where d is a random bit chosen by $\mathcal{B}$. We claim that if $T = \hat{e}(g,g)^{z/x}$, then (c_1^*, c_2^*, e^*) is a correct IBE ciphertext created with randomness $r = z/x \in \mathbb{Z}_p$. Since $a(id^*) = 0 \bmod p$, we have

$$\begin{aligned} c_1^* &= (u_0 \prod u_i^{id_i^*})^r = (g^{h(id^*)})^{z/x} = (g^{b(id)x})^{z/x} = Z^{b(id)}, \\ c_2^* &= (g^y)^r = (g^{cx})^{z/x} = Z^c \; . \end{aligned}$$

Furthermore, since $T = \hat{e}(g,g)^{z/x}$ the key $K^* = T$ is the correct key with randomness $r = z/x$. On the other hand, if T is a random element then the target ciphertext is clearly independent of the bit d.

If $a(id) \neq 0 \bmod p$ then adversary $\mathcal{B}$ terminates and returns a random bit b'.

Output Eventually $\mathcal{A}$ outputs a bit d' and $\mathcal{B}$ returns $b' = 1$ (meaning $T = \hat{e}(g,g)^{z/x}$) if $d = d'$ and $b' = 0$ (meaning T is random) otherwise, and terminates the game.

This completes the description of $\mathcal{B}$.

We now sketch an analysis of $\mathcal{B}$'s success probability. Let good be the event that Equation (3) and Equation (4) hold. In case good holds it is easy to see that $\mathcal{B}$ perfectly simulates the view of $\mathcal{A}$ and $\mathcal{B}$ can use $\mathcal{A}$'s output to break the q-RBDDH assumption.

Fix a public-key pk. The central argument in the proof is that for any possible set of appearing identities id^*, $id^{(1)}, \ldots, id^{(q)}$, the probability $\mu(id^*, id^{(1)}, \ldots, id^{(q)})$ that event good happens is lower bounded by $1/4(n+1)q$, where the probability space is $\mathbf{A}$, i.e, over all redundant randomness in the generation of the public-key. This claim will be formally proved in Lemma 3.3.

One technical problem that arises in the formal analysis is that adversary $\mathcal{B}$ aborts (and outputs a random bit b') in case good does not happen. Now it may happen that adversary $\mathcal{A}$'s output bit d' is correlated with $\mathcal{B}$'s abortion. To overcome this problem Waters used a technique called "artificial abort" in his original analysis [Wat05] to make $\mathcal{B}$'s abortion independent of $\mathcal{A}$'s output bit. The idea is that $\mathcal{B}$, after receiving $\mathcal{A}$'s output bit, tosses a coin. With some probability ν', $\mathcal{B}$ aborts, and with probability $1-\nu'$, $\mathcal{B}$ continues as before. It can be shown that for the right choice of ν' (depending on the queried identities) the output of adversary $\mathcal{B}$ can be made quasi independent of the event good. However, $\mathcal{B}$ needs about $\tilde{\mathcal{O}}(nq \cdot \varepsilon_{\mathcal{A}}^{-2}(k))$ time units to sample the right value ν'. For details we refer to the original proof by Waters [Wat05] or a game-based proof in [KG06]. ▮

It leaves to prove the following information-theoretic lemma that is implicitly contained in [Wat05].

Lemma 3.3 Fix integers n, q. For a string $id = (id_1, \dots, id_n) \in \{0,1\}^n$ and $(a_0, \dots a_n) \in \mathbb{Z}^{n+1}$ we define the function $a : \{0,1\}^n \to \mathbb{Z}$, $a(id) := a_0 + \sum_{i=1}^n a_i id_i$. Consider the probability distribution $\mathbf{A}$ on $(a_0, \dots, a_n)$ as defined in Equation (1). Then, for arbitrary $q+1$ pairwise distinct binary strings $id^{(i)} \in \{0,1\}^n$ $(0 \leq i \leq q)$, we have that for the probability μ over $\mathbf{A}$ that $a(id^{(0)}) = 0$, and $a(id^{(i)}) \neq 0$, for $i = 1, \dots, q$,

$$\mu \geq \frac{1}{4(n+1)q}.$$

Proof: Let $m = 2q$. Fix the strings $id^{(0)}, \dots, id^{(q)}$. We want to show that

$$\eta = \Pr_{\mathbf{A}}[\bigwedge_{i=1}^{q} \left(a(id^{(i)}) \neq 0 \right) \wedge a(id^{(0)}) = 0] \geq \frac{1}{4(n+1)q} \,. \tag{5}$$

We have that $a(id^{(0)}) = -km + a_0' + \sum_{i=1}^n id_i^{(0)} a_i$, where $0 \leq a_0' + \sum_{i=1}^n id_i^{(0)} a_i < (n+1)m$. This shows that if $a(id^{(0)}) = 0 \bmod m$, then there is a unique $0 \leq k < n+1$ such that $a(id^{(0)}) = 0$ over the integers. On the other hand, if $a(id^{(i)}) \neq 0 \bmod m$ then this in particular implies $a(id^{(i)}) \neq 0$ over the integers. Since k is uniformly and independently distributed between 0 and n, we have that :

$$\eta \quad \geq \quad \frac{1}{n+1} \cdot \Pr_{\mathbf{A}_k}[\bigwedge_{i=1}^{q} (a(id^{(i)}) \neq 0 \bmod m) \wedge a(id^{(0)}) = 0 \bmod m] \,,$$

where $\mathbf{A}_k$ is the distribution implied by Equation (1) for a fixed k.

Let $id \neq id'$ and $b, b' \in \mathbb{Z}$. We collect some simple observations on $a(\cdot)$ which essentially show that the $a(\cdot) \bmod m$ are pairwise independent.

$$\Pr_{\mathbf{A}_k}[a(id) = b \bmod m] \quad = \quad 1/m \tag{6}$$

$$\Pr_{\mathbf{A}_k}[a(id) = b \bmod m \mid a(id') = b' \bmod m] \quad = \quad 1/m \tag{7}$$

Equation (6) follows since for any choice of $a_1, ..., a_n$ there is a single choice of a_0' that will make the condition hold. To show Equation (7) assume there exists an index $1 \leq i \leq n$ such that $id_i = 1$ and $id_i' = 0$. Then fix all a_j's for $j \neq i$ except a_i so that $a(id') = b'$. Then there is a single choice of a_i such that $a(id) = b$ and therefore $\Pr[a(id) = b \mid a(id') = b'] = 1/m$. If there is no such i then we can use Bayes to reverse roles of id and id'.

We continue to bound η with

$$\begin{aligned}
\eta &\geq \frac{1}{n+1} \cdot \Pr_{\mathbf{A}_k}[\bigwedge_{i=1}^{q} a(id^{(i)}) \neq 0 \bmod m \mid a(id^{(0)}) = 0 \bmod m] \cdot \Pr[a(id^{(0)}) = 0 \bmod m] \\
&\overset{(6)}{=} \frac{1}{(n+1)m} \cdot \Pr_{\mathbf{A}_k}[\bigwedge_{i=1}^{q} a(id^{(i)}) \neq 0 \bmod m \mid a(id^{(0)}) = 0 \bmod m] \\
&= \frac{1}{(n+1)m} \cdot (1 - \Pr_{\mathbf{A}_k}[\bigvee_{i=1}^{q} a(id^{(i)}) = 0 \bmod m \mid a(id^{(0)}) = 0 \bmod m]) \\
&\geq \frac{1}{(n+1)m} \cdot (1 - \sum_{i=1}^{q} \Pr_{\mathbf{A}_k}[a(id^{(i)}) = 0 \bmod m \mid a(id^{(0)}) = 0 \bmod m]) \\
&\overset{(7)}{=} \frac{1}{(n+1)m} \cdot (1 - \sum_{i=1}^{q} \frac{1}{m}) \\
&= \frac{1}{(n+1)m} \cdot (1 - \frac{q}{m}) \\
&= \frac{1}{4(n+1)q} \ ,
\end{aligned}$$

where the last equation follows by our choice of $m = 2q$ which minimizes the term. ▮

4 Short signatures

4.1 The signature scheme

Moni Naor noted [BF03] that every IBE scheme directly implies a signature scheme unforgeable against adaptively chosen message attacks [GMR88]. Applying some simplifications we get the following signature scheme $\mathcal{SIG} = (\mathsf{Kg}, \mathsf{Sign}, \mathsf{Vfy})$, where Kg is the same as in the IBE scheme. The scheme sign arbitrary messages $m = (m_1, \ldots, m_n) \in \{0,1\}^n$, arbitrary bitstrings $m' \in \{0,1\}^*$ can be signed by applying a collission-resistant hash function.

```
Sign($sk, m$)
  $s \xleftarrow{\$} \mathbb{Z}_p$
  $d \leftarrow g^{\frac{1}{x_0 + \sum x_i m_i + ys}}$
  Return $sig \leftarrow (d, s)$

Vfy($pk, m, sig$)
  Parse $sig = (d, s)$
  If $\hat{e}(d, Y^s X_0 \prod_{i=1}^{n} X_i^{m_i}) \neq \hat{e}(g, g)$ then reject
    Else accept
```

For efficiency one may add the element $\hat{e}(g,g)$ to the public-key. The signature size is one group element plus one element in $\mathbb{Z}_p$. Using asymmetric pairings it is hence possible to get signatures with 256 bits (for 128 bits security).

4.2 Security

Analog to the proof of Theorem 3.1 security can be reduced to the q-Computational Diffie-Hellman Inversion (q-CDHI) assumption in pairing groups which states that given $g, g^x, \ldots, g^{x^q}$, it is infeasible to compute $g^{1/x}$.

Theorem 4.1 Under the $q+1$-CDHI assumption the signature scheme is (strongly) unforgeable against adaptively chosen message attacks.

4.3 Comparison

The short signature scheme from Boneh and Boyen [BB04b] (which is in fact the signature scheme implied by the second Boneh Boyen IBE scheme [BB04a]) is quite similar to ours, i.e. a message m is signed by computing (d, s) where $s \in \mathbb{Z}_p$ is a random element and $d = g^{1/(x_0+m+ys)}$. Whereas our scheme has a larger public/secret keys ($n + 2$ compared to 2 elements), security relies on a weaker assumption. To be more precise, the Boneh-Boyen signature scheme can only be proved under the q-strong CDHI assumption which states that (given the same imput as q-CDHI), it is infeasible to compute the tuple $(c, g^{1/(c+x)})$, where c is an arbitrary element from $\mathbb{Z}_p$.

Scheme	Sign	Verify	Signatures		pk	Assumption
	#pairings +	#exps	Size	(bits)		
Boneh/Boyen	$0+1$	$1+1$	$\lvert\mathbb{G}\rvert + \lvert p\rvert$	(512)	2	q-strong CDHI
Ours	$0+1$	$1+1$	$\lvert\mathbb{G}\rvert + \lvert p\rvert$	(512)	$n+2$	q-CDHI

References

[ABC$^+$05] Michel Abdalla, Mihir Bellare, Dario Catalano, Eike Kiltz, Tadayoshi Kohno, Tanja Lange, John Malone-Lee, Gregory Neven, Pascal Paillier, and Haixia Shi. Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions. In Victor Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621 of *Lecture Notes in Computer Science*, pages 205–222, Santa Barbara, CA, USA, August 14–18, 2005. Springer-Verlag, Berlin, Germany. (Cited on page 4.)

[BB04a] Dan Boneh and Xavier Boyen. Efficient selective-ID secure identity based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany. (Cited on page 1, 2, 3, 9.)

[BB04b] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In Christian Cachin and Jan Camenisch, editors, *Advances in Cryptology – EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 56–73, Interlaken, Switzerland, May 2–6, 2004. Springer-Verlag, Berlin, Germany. (Cited on page 9.)

[BF03] Dan Boneh and Matthew K. Franklin. Identity based encryption from the Weil pairing. *SIAM Journal on Computing*, 32(3):586–615, 2003. (Cited on page 1, 2, 8.)

[Gen06] Craig Gentry. Practical identity-based encryption without random oracles. In Serge Vaudenay, editor, *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *Lecture Notes in Computer Science*, pages 445–464, St. Petersburg, Russia, May 28 – June 1, 2006. Springer-Verlag, Berlin, Germany. (Cited on page 1, 4.)

[GMR88] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, April 1988. (Cited on page 8.)

[KG06] Eike Kiltz and David Galindo. Direct chosen-ciphertext secure identity-based key encapsulation without random oracles. In *ACISP 2006*, volume 4058, pages 336–347. Springer-Verlag, 2006. (Cited on page 7.)

[Sha85] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO'84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53, Santa Barbara, CA, USA, August 19–23, 1985. Springer-Verlag, Berlin, Germany. (Cited on page 1.)

[Wat05] Brent R. Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127, Aarhus, Denmark, May 22–26, 2005. Springer-Verlag, Berlin, Germany. (Cited on page 1, 3, 4, 7.)

A Proof of Lemma 3.2

Proof: We show q-BDDHI $\Rightarrow$ $q-1$-RBDDH. Suppose $\mathcal{A}$ is given the values $(g, g^x, \ldots, g^{x^q}, T)$. $\mathcal{A}$'s task is to decide if $T = \hat{e}(g,g)^{1/x}$ or if $T \in \mathbb{G}_T$ is random.

Note that $\mathcal{A}$ can efficiently compute all the values $g^{q(x)}$ for any explicily known polynomial $q(x)$ of degree at most q. For $1 \leq i \leq q-1$, $\mathcal{A}$ picks at random uniform values $t_i \in \mathbb{Z}_p$, defines the polynomial $p(x) = \prod_{i=1}^{q-1}(x - t_i) = \sum_{i=0}^{q-1} p_i x^i$ of degree $q-1$, and sets $h = g^{p(x)}$. Note that $\mathcal{A}$ can compute $h = g^{p(x)}$, $h^x = g^{xp(x)}$, and all the $x+t_i$th roots $h^{1/(x+t_i)} = g^{p(x)/(x+t_i)}$, for $1 \leq i \leq q-1$. Then $\mathcal{A}$ picks a random y and calls $\mathcal{B}$ on the values $(h, h^x, t_1, h^{1/(x+t_1)}, \ldots, t_{q-1}, h^{1/(x+t_{q-1})}, h^y, \tilde{T})$, where $\tilde{T} = \hat{e}(h,h)^{y/x} = \hat{e}(g^{p(x)/x}, g^{p(x)})^y = (\hat{e}(g,g)^{1/x} \cdot \hat{e}(g^{p'(x)}, g^{p''(x)}))^y$ for some polynomials p', p'' of degree $\leq q$. This value $\tilde{T}$ can be computed using the value $T = \hat{e}(g,g)^{1/x}$ from $\mathcal{A}$'s input. ▌