Provable Security of Pairing-Based Protocols: The Case of Public Key and Identity-Based Encryption

Benoît Libert

UCL Crypto Group, Belgium

benoit.libert@uclouvain.be

August 28th 2007

Overview

- Properties of pairings
- Boneh-Franklin Identity-Based Encryption (IBE)
  - Description, model, proof
  - IBE and signatures
  - Hierarchical IBE
- IBE schemes in the standard model
  - Boneh-Boyen
  - Waters
- CCA-secure public key encryption from IBE:
  - Canetti-Halevi-Katz, Boneh-Katz, Boyen-Mei-Waters, ...

1 Properties of pairings

Basic properties:

- Triple of groups $\mathbb{G}_1$, $\mathbb{G}_2$, $\mathbb{G}_T$, all of prime order p.
- A mapping $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$ such that:
  - $e(g \cdot g', h) = e(g, h) \cdot e(g', h)$
  - $e(g, h \cdot h') = e(g, h) \cdot e(g, h')$
  - Hence, for any $a, b \in \mathbb{Z}$,

$$e(g^a, h^b) = e(g, h)^{ab} = e(g^b, h^a) = \ldots$$

- Non-degeneracy: $e(g, h) \neq 1_{\mathbb{G}_T}$ if $g \neq 1_{\mathbb{G}_1}$ and $h \neq 1_{\mathbb{G}_2}$.
- Computability: $e(g, h)$ can be efficiently computed.

Pairings

- Typically, $\mathbb{G}_1$, $\mathbb{G}_2$ are subgroups of the group of p-torsion points on an elliptic curve E defined over a field $\mathbb{F}_q$.
- More precisely, $\mathbb{G}_1 \subset E(\mathbb{F}_q)[p]$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{q^k})[p]$.
- Then $\mathbb{G}_T$ is a subgroup of $\mathbb{F}^*_{q^k}$ where k is the least integer with $p|q^k - 1$.
- k is called the *embedding degree*.

Pairings

- If E is supersingular, then we can arrange $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$.
- Simplifies presentation of schemes and security analyzes.
- Allows "small" representations of group elements in both $\mathbb{G}_1$ and $\mathbb{G}_2$.
- But then we are limited to $k \leq 6$ with consequences for efficiency at higher security levels.
- Even generation of parameters may become difficult.

Pairings

- If E is ordinary, then a variety of constructions for pairing-friendly curves are known.
- But then certain trade-offs are involved:
  - Only elements of $\mathbb{G}_1$ may have short representations.
  - Although elements from $\mathbb{G}_2$ and $\mathbb{G}_T$ can be compressed.
- Most of the protocols discussed here are re-writable in the asymmetric setting.

Constructive Applications of Pairings

- At SCIS2000, Sakai, Ohgishi and Kasahara used pairings to construct:
  - An identity-based signature scheme (IBS); and
  - An identity-based non-interactive key sharing (NIKS).
- Tripartite Diffie-Hellman Key agreement (Joux, ANTS 2000).
- At SCIS2001, Sakai-Kasahara also used pairings to construct an efficient identity-based encryption scheme.

2 Boneh-Franklin IBE

- First practical IBE scheme with a security proof (Crypto 2001).
- (SK scheme at SCIS 2001, but no security proof, published in Japanese).
- Boneh-Franklin also give security model for IBE.
- Basic version provides CPA security, enhanced version gives CCA security.
- This paper was the main trigger for the flood of research in pairing-based cryptography.

Boneh-Franklin IBE

Setup:

1. On input a security parameter k, generate parameters $\langle \mathbb{G}, \mathbb{G}_T, e, p \rangle$ where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a pairing on groups of prime order p.
2. Select two hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G}_T \rightarrow \{0,1\}^n$, where n is the length of plaintexts.
3. Choose an arbitrary generator $g \in \mathbb{G}$.
4. Select a master-key $s \xleftarrow{R} \mathbb{Z}_p^*$ and set $g_1 = g^s$.
5. Return the public system parameters params $= \langle \mathbb{G}, \mathbb{G}_T, e, p, g, g_1, H_1, H_2 \rangle$ and the master-key s.

Boneh-Franklin IBE

Extract: Given an identity $\mathsf{ID} \in \{0,1\}^*$, set $d_{\mathsf{ID}} = H_1(\mathsf{ID})^s$ as the private decryption key.

Encrypt: Inputs are message M and an identity ID.

1. Choose random $t \overset{R}{\leftarrow} \mathbb{Z}_p$.
2. Compute the ciphertext $C = \langle g^t, M \oplus H_2\big(e(g_1, H_1(\mathsf{ID}))^{\mathsf{t}}\big)\rangle$.

Decrypt: Given a ciphertext $\langle c_1, c_2\rangle$ and a private key d_{ID}, compute:

$$M = c_2 \oplus H_2(e(c_1, d_{\mathsf{ID}})).$$

Boneh-Franklin IBE – What Makes it Tick?

- Can be seen as an extension of ElGamal where the sender uses the public key $g, g_1 = g^s$ to compute

$$\langle c_1, c_2 \rangle = \langle g^t, M \oplus H(g_1^t) \rangle$$

- Here, both sender (who has t) and receiver (who has d_{ID}) can compute $e(g, H_1(\mathsf{ID}))^{st}$:

$$\begin{aligned} e(g, H_1(\mathsf{ID}))^{st} &= e(g^s, H_1(\mathsf{ID}))^t = e(g_1, H_1(\mathsf{ID}))^t \\ e(g, H_1(\mathsf{ID}))^{st} &= e(g^t, H_1(\mathsf{ID})^s) = e(c_1, d_{\mathsf{ID}}) \end{aligned}$$

- Security relies on the hardness of computing $e(g, g)^{abc}$ given (g, g^a, g^b, g^c) (Bilinear Diffie-Hellman assumption).

Security of Boneh-Franklin IBE

Informally:

- Adversary sees message XORed with hash of $e(g_1, H_1(\mathsf{ID}))^t$.
- Adversary also sees $g_1 = g^s$ and $c_1 = g^t$.
- Write $H_1(\mathsf{ID}) = g^z$ for some (unknown) z.
- Then $e(g_1, H_1(\mathsf{ID}))^t = e(g, g)^{stz}$.
- Hence, an adversary needs to compute $e(g, g)^{stz}$ when given as inputs g^s, g^t, g^z.
- This is an instance of the **Bilinear Diffie-Hellman** problem.

Security Model for IBE

Reminder: IND-CCA security for public key encryption

- Challenger $\mathcal{C}$ generates (sk, pk) and gives pk to adversary $\mathcal{A}$.
- $\mathcal{A}$ accesses a Decrypt oracle.
- $\mathcal{A}$ outputs two messages m_0, m_1.
- $\mathcal{C}$ selects $b \xleftarrow{R} \{0,1\}$ and gives $\mathcal{A}$ an encryption c^* of m_b.
- $\mathcal{A}$ has further oracle access to Decrypt and finally outputs a guess b' for b.

$\mathcal{A}$ wins the game if $b' = b$. Define

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

Security Model for IBE

Similar game to standard security game for PKE:

- Challenger $\mathcal{C}$ runs Setup and adversary $\mathcal{A}$ is given the public parameters.
- $\mathcal{A}$ accesses $\mathsf{Extract}$ and $\mathsf{Decrypt}$ oracles.
- $\mathcal{A}$ outputs two messages m_0, m_1 and a challenge identity ID^*.
- $\mathcal{C}$ selects $b \stackrel{R}{\leftarrow} \{0,1\}$ and gives $\mathcal{A}$ an encryption of m_b under identity ID^*, denoted c^*.
- $\mathcal{A}$ has further oracle access and finally outputs a guess b' for b.

$\mathcal{A}$ wins the game if $b' = b$. Define

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

Security Model for IBE

Natural limitations on oracle access and selection of ID^*:

- No Extract query on ID^*.
- No Decrypt query on c^*, ID^*.

An IBE scheme is said to be IND-ID-CCA secure if there is no poly-time adversary $\mathcal{A}$ which wins the above game with non-negligible advantage.

An IBE scheme is said to be IND-ID-CPA secure if there is no poly-time adversary $\mathcal{A}$ having access only to the Extract oracle which wins the above game with non-negligible advantage.

Security of Boneh-Franklin IBE

- Boneh and Franklin prove that their encryption scheme is IND-ID-CPA secure, provided the BDH assumption holds.
- The proof is in the random oracle model.
- "Standard" techniques can be used to transform Boneh-Franklin IBE into an IND-ID-CCA secure scheme.
- These generally add complexity, require random oracles, and result in inefficient security reductions.

Security of Boneh-Franklin IBE (cont.)

Idea of the proof: use Coron's trick (Crypto'00) to answer random oracle queries and solve a BDH instance (g^a, g^b, g^c).

Set $g_1 = g^a$ as a master public key.

For each random oracle query $H_1(\mathsf{ID}_i)$:

- set $H_1(\mathsf{ID}_i) = g^{\omega}$ with $\omega \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ with probability $\delta = q_e/(q_e + 1)$.

  $\Rightarrow$ Private keys are computable $d_{\mathsf{ID}_i} = (g^a)^{\omega} = (g^{\omega})^a$

- return $H_1(\mathsf{ID}_i) = (g^b)^{\omega}$ where $\omega \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$ with probability $1 - \delta$.

Set the challenge as $C^{\star} = \langle g^c, R \rangle$ with $R \stackrel{R}{\leftarrow} \{0,1\}^n$.
If $H_1(\mathsf{ID}^{\star}) = (g^b)^{\omega^{\star}}$, $\mathcal{A}$ must query $e(g_1, H_1(\mathsf{ID}^{\star}))^c = e(g,g)^{abc\omega^{\star}}$ to random oracle $H_2(\cdot)$.

IBE and pairing-based signatures

- Naor: any IBE implies a signature.

  Keygen: Let $(PK, SK) = (\mathsf{PK}_{\mathsf{IBE}}, \mathsf{mk}_{\mathsf{IBE}})$ be the TA's key pair

  $\mathbf{Sign}_{SK}(M)$: return $d_M = \mathsf{Extract}^{\mathsf{IBE}}_{\mathsf{mk}_{\mathsf{IBE}}}(M)$

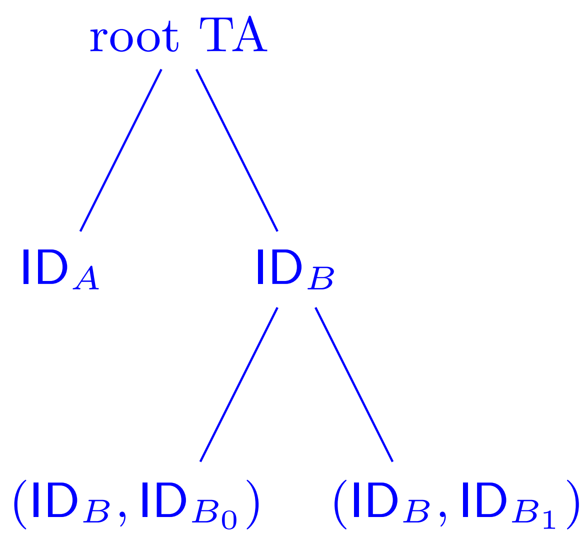
  $\mathbf{Verify}_{PK}(M, d_M)$: choose $M_{rand} \stackrel{R}{\leftarrow} \mathcal{M}^{\mathsf{IBE}}$, encrypt it as $C = \mathsf{Enc}^{\mathsf{IBE}}_{\mathsf{PK}_{\mathsf{IBE}}}(M_{rand}, M)$, accept if $M_{rand} = \mathsf{Dec}^{\mathsf{IBE}}_{\mathsf{mk}_{\mathsf{IBE}}}(C, d_M)$

- But not all signatures imply an IBE, only a handful of schemes. In all known IBE, a private key for ID is a signature on it.

  e.g. Boneh-Franklin : $e(d_{\mathsf{ID}}, g) = e(H_1(\mathsf{ID}), g_1)$

Hierarchical IBE

- Extension of IBE to provide hierarchy of TAs, each generating private keys for TA in level below.



- Encryption needs root's parameters and a vector of identities.
- First secure, multi-level scheme due to Gentry and Silverberg.
- Also an important theoretical tool (forward-secure encryption, CCA-secure IBE in the standard model,...).

3 IBE in the Standard Model

- Prior to 2004, most applications of pairings use the Random Oracle Model (Bellare-Rogaway, CCS'93) in security proofs.
- ROM provides a powerful and convenient tool for modeling hash functions in security proofs.
- But concern has been shed on how ROM accurately models the behavior of hash functions.
- Several examples in the literature of schemes secure in the ROM but insecure for every family of hash functions.
- General move towards "proofs in the standard model" in cryptography.

CHK, BB, and Waters

IBE in the standard model:

- Eurocrypt'03: Canetti-Halevi-Katz provide (fairly inefficient) selective-ID secure IBE scheme.
- Eurocrypt'04: Boneh-Boyen present efficient selective-ID secure (H)IBE scheme.
- Crypto'04: Boneh-Boyen present inefficient, but adaptive-ID secure IBE scheme.
- Eurocrypt'05: Waters presents efficient, adaptive-ID secure IBE by "tweaking" Boneh-Boyen the construction from Eurocrypt'04.

The Boneh-Boyen IBE

Setup:

1. On input a security parameter k, generate parameters $\langle \mathbb{G}, \mathbb{G}_T, e, p \rangle$ where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a pairing on groups of prime order p.
2. Select generators $g, h \stackrel{R}{\leftarrow} \mathbb{G}$.
3. Choose $s \stackrel{R}{\leftarrow} \mathbb{Z}_p$. Set $g_1 = g^s$ and pick $g_2 \stackrel{R}{\leftarrow} \mathbb{G}$.
4. The $\mathsf{master\text{-}key}$ is g_2^s.
5. Output $\mathsf{params} = \langle \mathbb{G}, \mathbb{G}_T, e, p, g, g_1, g_2, h \rangle$.

The Boneh-Boyen IBE

The Boneh-Boyen “Hash”: Given an identity string $\mathsf{ID} \in \mathbb{Z}_p^*$, define

$$H_{BB}(\mathsf{ID}) = g_1^{\mathsf{ID}} \cdot h.$$

Extract: given an identity $\mathsf{ID} \in \mathbb{Z}_p^*$, select $r \xleftarrow{R} \mathbb{Z}_p$ and set

$$d_{\mathsf{ID}} = \langle d_1, d_2 \rangle = \langle g_2^s \cdot H_{BB}(\mathsf{ID})^r, g^r \rangle \in \mathbb{G}^2$$

– randomized private key extraction.

– private key $\langle d_1, d_2 \rangle$ satisfies $e(d_1, g) = e(g_1, g_2) \cdot e(H_{BB}(\mathsf{ID}), d_2)$.

The Boneh-Boyen IBE

Encrypt: Inputs are a message $m \in \mathbb{G}_T$ and an identity ID.

1. Choose random $t \xleftarrow{R} \mathbb{Z}_p$.
2. Compute the ciphertext

$$c = \langle m \cdot e(g_1, g_2)^t, g^t, H_{BB}(\mathsf{ID})^t \rangle \in \mathbb{G}_T \times \mathbb{G}^2.$$

Decrypt: Given a ciphertext $c = \langle c_1, c_2, c_3 \rangle$ and a private key $d_{\mathsf{ID}} = \langle d_1, d_2 \rangle$, compute:

$$m = c_1 \cdot \frac{e(d_2, c_3)}{e(d_1, c_2)}.$$

Correctness of the Boneh-Boyen IBE

Private keys $\langle d_1, d_2 \rangle = \langle g_2^s \cdot H_{BB}(\mathsf{ID})^r, g^r \rangle$ satisfy:

$$\frac{e(d_1, g)}{e(d_2, H_{BB}(\mathsf{ID}))} = e(g_1, g_2).$$

If we raise both members to the power $t \in \mathbb{Z}_p$:

$$\frac{e(d_1, g)^t}{e(d_2, H_{BB}(\mathsf{ID}))^t} = e(g_1, g_2)^t$$

which yields

$$\frac{e(d_1, g^t)}{e(d_2, H_{BB}(\mathsf{ID})^t)} = e(g_1, g_2)^t.$$

Hence

$$\frac{e(d_1, c_2)}{e(d_2, c_3)} = e(g_1, g_2)^t.$$

Security for the Boneh-Boyen IBE

The scheme is IND-sID-CPA secure assuming the hardness of the decisional BDH problem:

> Given $\langle g, g^a, g^b, g^c, Z\rangle$ for $a, b, c \overset{R}{\leftarrow} \mathbb{Z}_p$, and $Z \in \mathbb{G}_T$, decide if $Z = e(g, g)^{abc}$.

c.f.: Proof of security for Boneh-Franklin IBE based on hardness of the computational BDH problem *in the Random Oracle Model*.

Sketch of Security Proof

- Assume $\mathcal{A}$ is an adversary against BB-IBE, and $\mathcal{B}$ is faced with a DBDH instance $\langle g, g^a, g^b, g^c, Z \rangle$.
- $\mathcal{B}$ simulates a challenger in $\mathcal{A}$'s security game.
- $\mathcal{B}$ sets $g_1 = g^a$, $g_2 = g^b$ and will put $g^t = g^c$ in the generation of the challenge ciphertext c^*.
- $\mathcal{B}$ also uses Z in place of $e(g_1, g_2)^z$ when creating c_1^* from m_b.
- If $Z = e(g, g)^{abc}$ then the challenge ciphertext will be a correct encryption of m_b. If $Z \neq e(g, g)^{abc}$ then the challenge ciphertext will be unrelated to m_b.
- From this, $\mathcal{B}$ can convert a successful $\mathcal{A}$ into an algorithm for solving DBDHP.

Sketch of Security Proof (ctd.)

How to handle private key extraction queries?

- $\mathcal{B}$ sets $h = {g_1}^{-\mathsf{ID}^\star} \cdot g^\omega$, for a random $\omega \stackrel{R}{\leftarrow} \mathbb{Z}_p^*$, so that

$$H_{BB}(\mathsf{ID}) = g_1^{\mathsf{ID}} \cdot h = {g_1}^{\mathsf{ID}-\mathsf{ID}^\star} \cdot g^\omega.$$

- Provided $\mathsf{ID} \neq \mathsf{ID}^\star$, $\mathcal{B}$ can construct a private key $\langle d_1, d_2 \rangle$ for ID via:

$$d_1 = {g_1}^{-\frac{1}{\mathsf{ID}-\mathsf{ID}^\star}} \cdot H_{BB}(\mathsf{ID})^r, \quad d_2 = {g_1}^{-\frac{1}{\mathsf{ID}-\mathsf{ID}^\star}} \cdot g^r.$$

  It can be checked that $\langle d_1, d_2 \rangle = \langle g_2^s \cdot H_{BB}(\mathsf{ID})^{\tilde{r}}, g^{\tilde{r}} \rangle$ with $\tilde{r} = r - \frac{a}{\mathsf{ID}-\mathsf{ID}^\star}$.

Sketch of Security Proof (concluded)

Challenge ciphertext should be an encryption of m_b:

$$\begin{array}{ccc} c_1 = m_b \cdot e(g_1, g_2)^t & c_2 = g^t & c_3 = H_{BB}(\mathsf{ID}^*)^t \\ \downarrow & \downarrow & \downarrow \\ c_1 = m_b \cdot Z & c_2 = g^c & c_3 = H_{BB}(\mathsf{ID}^*)^c \end{array}$$

Problem: how to compute c_3 knowing only g^c but not c?

Solution: in the selective-ID model, h can be chosen so as to "program" H_{BB} as $H_{BB}(\mathsf{ID}^*) = g^\omega$. So,

$$H_{BB}(\mathsf{ID}^*)^c = (g^c)^\omega$$

The Waters IBE

Setup:

1. On input a security parameter k, generate parameters $\langle \mathbb{G}, \mathbb{G}_T, e, p \rangle$ where $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$ is a pairing on groups of prime order p.
2. Select $u', u_1, \ldots, u_n \stackrel{R}{\leftarrow} \mathbb{G}^{n+1}$. Here n is the length of (hashed) identities.
3. Choose an arbitrary generator $g \in \mathbb{G}$ and $s \stackrel{R}{\leftarrow} \mathbb{Z}_p$. Set $g_1 = g^s$, $g_2 \stackrel{R}{\leftarrow} \mathbb{G}$.
4. The master-key is g_2^s.
5. Output params $= \langle \mathbb{G}, \mathbb{G}_T, e, p, g, g_1, g_2, u', u_1, \ldots, u_n \rangle$.

The Waters IBE

The Waters Hash: Given an n-bit string $\mathsf{ID} = i_1 i_2 \ldots i_n$, define

$$H_W(\mathsf{ID}) = u' \cdot u_1^{i_1} \cdots u_n^{i_n} = u' \cdot \prod_{i=1} u_i.$$

Extract: Given an identity $\mathsf{ID} \in \{0,1\}^*$, select $r \xleftarrow{R} \mathbb{Z}_p$ and set

$$d_{\mathsf{ID}} = \langle d_1, d_2 \rangle = \langle g_2^s \cdot H_W(\mathsf{ID})^r, g^r \rangle \in \mathbb{G}^2$$

– similar private key extraction to Boneh-Boyen.

– private key again satisfies $e(d_1, g) = e(g_1, g_2) \cdot e(H_W(\mathsf{ID}), d_2)$.

The Waters IBE

Encrypt: Inputs are a message $m \in \mathbb{G}_T$ and an identity ID.

1. Choose random $t \overset{R}{\leftarrow} \mathbb{Z}_p$.
2. Compute the ciphertext

$$c = \langle m \cdot e(g_1, g_2)^t, g^t, H_W(\mathsf{ID})^t \rangle \in \mathbb{G}_T \times \mathbb{G}^2.$$

Decrypt: Given a ciphertext $c = \langle c_1, c_2, c_3 \rangle$ and a private key $d_{\mathsf{ID}} = \langle d_1, d_2 \rangle$, compute:

$$m = c_1 \cdot \frac{e(d_2, c_3)}{e(d_1, c_2)}.$$

Sketch of Security Proof

To decide whether $Z \stackrel{?}{=} e(g,g)^{abc}$ given (g^a, g^b, g^c),

- Choose $u', u_1, \ldots, u_n$ so as to have

$$H_W(\mathsf{ID}) = u' \cdot \prod_{j=1}^{n} u_i^{i_j} = (g^b)^{F(\mathsf{ID})} \cdot g^{K(\mathsf{ID})}$$

  for some functions $K(.)$ and $F(.)$ where F is relatively small (i.e. $\ll p$) in absolute value.

- Handle private key extraction queries as in Boneh-Boyen whenever $F(\mathsf{ID}) \neq 0 \bmod p$.

- With non-negligible probability $F(\mathsf{ID}^\star) = 0$ and thus $c_3^\star = H_W(\mathsf{ID}^\star)^c = (g^c)^{K(\mathsf{ID}^\star)}$ is computable.

Efficiency of Waters' IBE

- Large public parameters: dominated by $n + 1$ group elements.
- Small private keys (2 group elements) and ciphertexts (3 group elements).
- Encryption: on average $n/2 + 1$ group operations in $\mathbb{G}$, two exponentiations in $\mathbb{G}$, one exponentiation in $\mathbb{G}_T$ (assuming $e(g_1, g_2)$ is pre-computed).
- Decryption: dominated by cost of two pairing computations.
- Size of public parameters can be reduced at the cost of a looser security reduction using ideas of Chatterjee-Sarkar/Naccache.

A Hierarchical Version of Waters' IBE

- A simple generalization of Waters' IBE yields a HIBE scheme that is IND-ID-CPA secure assuming DBDHP is hard.
- IND-ID-CCA security for $(\ell - 1)$-level HIBE can be attained by applying CHK/BK/BMW ideas to the ℓ-level IND-ID-CPA secure scheme.
- Quality of the security reduction declines exponentially with ℓ.
  - Recent scheme by Gentry (Eurocrypt'06) has a tight reduction, but under a less natural hardness assumption and does not scale into a HIBE.
  - A "million dollar problem": HIBE with polynomial security degradation in the depth of the hierarchy.

Other HIBE constructions and extensions

- With constant-size ciphertexts (Boneh-Boyen-Goh, Eurocrypt'05).
  - Provides selective-ID security.
  - Adaptive-ID security possible using the Waters "hashing" (again with exponential degradation of security bounds).
- With anonymous ciphertexts (Boyen-Waters, Crypto'06).
- IBE with "wildcards" (Abdalla *et al.* – ICALP'06).
- Attribute-based encryption (Sahai-Waters, Eurocrypt'05).

4 Applications of Secure IBE in the Standard Model

- A new paradigm of CCA-secure public key encryption:
  - Canetti-Halevi-Katz (Eurocrypt'04): IND-CCA secure public key encryption from any IND-ID-CPA selective-ID secure IBE scheme.
  - Improvement by Boneh-Katz (RSA-CT'05).
  - Can be applied to selective-ID secure IBE scheme of Boneh-Boyen scheme (don't need fully secure IBE).
  - Direct non-generic constructions by Boyen-Mei-Waters (ACM-CCS'05).

The CHK construction: PKE from IBE

Key generation: Public key of PKE set to params of IBE; private key is set to master-key.

Encrypt:

1. Generate a key-pair $\langle vk, sk \rangle$ for a strong one-time signature scheme;
2. IBE-encrypt m using as the identity the verification key vk to obtain c;
3. Sign c using signature key sk to obtain σ;
4. Output $C = \langle vk, c, \sigma \rangle$ as the encryption of m.

The CHK construction: PKE from IBE

Decrypt:

1. Check that σ is a valid signature on c given vk;
2. Generate the IBE private key for identity vk;
3. IBE-decrypt c to obtain m.

Informally: a decryption oracle is of no use to an attacker faced with $\langle vk^*, c^*, \sigma^* \rangle$:

- If oracle queried on $\langle vk, c, \sigma \rangle$ with $vk = vk^*$, then σ will be incorrect (unforgeability).
- If query with $vk \neq vk^*$, then IBE decryption will be done with a different "identity" so result won't help (IBE security).

Improvement on CHK

- Drawback of CHK: use of one-time signatures that imply long ciphertexts.
- Boneh-Katz (RSA-CT'05) replace the one-time signature with a MAC/commitment combination.
  - Significantly shorter ciphertexts.
  - But the "well-formedness" of ciphertexts is not publicly verifiable anymore (not suitable for threshold decryption).

The BMW construction: PKE from Waters' IBE

Boyen-Mei-Waters (ACM-CCS 2005) used a direct approach to produce an efficient PKE scheme from Waters' IBE (and from Boneh-Boyen).

Key generation:

- Public key:

$$\langle \mathbb{G}, \mathbb{G}_T, e, p, g, g_1, g_2, H, u' = g^{y'}, u_1 = g^{y_1}, \ldots, u_n = g^{y_n} \rangle$$

  with H is a collision-resistant hash function $H : \mathbb{G}_T \times \mathbb{G} \rightarrow \{0,1\}^n$ and $y', y_1, \ldots, y_n \stackrel{R}{\leftarrow} \mathbb{Z}_p$.

- Private key:

$$\langle g_2^s, y', y_1, \ldots, y_n \rangle$$

The BMW construction: PKE from Waters' IBE

Encrypt: Given a message $m \in \mathbb{G}_T$,

1. Choose random $t \stackrel{R}{\leftarrow} \mathbb{Z}_p$.
2. Compute the ciphertext

$$c = \langle m \cdot e(g_1, g_2)^t, g^t, H_W(w)^t \rangle \in \mathbb{G}_T \times \mathbb{G}^2$$

where

$$w = H(c_1, c_2).$$

The BMW construction: PKE from Waters' IBE

Decrypt: Given a ciphertext $c = \langle c_1, c_2, c_3 \rangle$ and the private key

1. Compute $w = H(c_1, c_2)$;
2. Test if $\langle g, c_2, H_W(w), c_3 \rangle$ is a DH quadruple by using the pairing (or more efficiently using knowledge of the values y', y_i).
3. Calculate

$$m = c_1 / e(c_2, g_2^s).$$

Idea of the Proof

To decide whether $Z \stackrel{?}{=} e(g,g)^{abc}$ given (g^a, g^b, g^c),

- Choose $u', u_1, \ldots, u_n$ so as to have

$$H_W(w) = u' \cdot \prod_{j=1}^{n} u_i^{w_j} = g_1^{F(w)} \cdot g^{K(w)}$$

  for some functions $K(.)$ and $F(.)$ where $|F(.)| \ll p$.

- Any valid ciphertext (c_1, c_2) satisfies

$$c_2 = g^t, \quad c_3 = \left(g_1^{F(w)} \cdot g^{K(w)}\right)^t$$

  and $g_1^t = \left(c_3 / c_2^{K(w)}\right)^{1/J(w)}$ is computable and yields $e(g_1, g_2)^t$.

- With non-negligible probability $F(w^\star) = 0$ and thus $c_3^\star = H_W(w^\star)^c = (g^c)^{K(w^\star)}$ is computable.

The BMW construction: PKE from Waters' IBE

- Scheme is similar to Waters' IBE, but with "identity" in c_3 being computed from components c_1, c_2.
- Scheme is more efficient than CHK/BK approach – no external one-time signature/MAC involved.
- A specific rather than generic transform from IBE to PKE (c.f. CHK approach).
- Security proof needs full security model for IBE (selective-ID security not enough).
- Specific selective-ID secure schemes yield CCA-secure hybrid encryption (via the KEM-DEM framework).

A relative of IBE-2-PKE transforms:

- At TCC'04, McKenzie-Reiter-Yang consider tag-based encryption.
- Kiltz (TCC'06) shows that selective-tag weakly CCA-secure tag-based encryption suffices to give CCA-security for public key encryption via CHK.
- Gives an efficient hybrid scheme based on the **Decision Linear Assumption** in the same vein as BMW:

  Given $(g_1, g_2, h, g_1^a, g_2^b, T)$, decide whether $T = h^{a+b}$.

- Must be implemented in pairing groups but does not require pairing operations to encrypt or decrypt.

Hybrid Encryption from the DLIN assumption

Key generation: pick $SK = (x, y) \xleftarrow{R} \mathbb{Z}_p^2$. Choose $h, u, v \xleftarrow{R} \mathbb{G}$ and set $g_1 = h^x, g_2 = h^y$. Define

$$F_1(t) = h^t u, \quad F_2(t) = h^t v.$$

Let $PK = (g_1, g_2, h, u, v)$.

Encrypt: pick $r, s \xleftarrow{R} \mathbb{Z}_p$ and set

$$A = g_1^r, \quad B = g_2^s, \quad C = F_1(t)^r, \quad D = F_2(t)^s$$

where $t = H(A, B)$. Use $K = h^{r+s}$ to perform a symmetric encryption of M.

Decrypt: check whether $(g_1, A, F_1(t), C)$ and $(g_2, B, F_2(t), D)$ form DH-tuples. If yes, let $K = A^x \cdot B^y$ and use it to decrypt.

Other Pairing-Based PKE schemes

- Key-updating cryptography (Anderson, ACM-CCS'97):
  - Canetti-Halevi-Katz (Eurocrypt'03): forward-secure public key encryption from selective-ID secure HIBE.

    ⇒ Boneh-Boyen-Goh gives fs-PKE with constant-size ciphertexts.
  - Key-insulated encryption (Dodis-Katz-Xu-Yung, Eurocrypt'02).
    - Generic construction from IBE (Bellare-Palacio).
    - "Parallel" extensions with multiple secure devices (Hanaoka-Hanaoka-Imai, Libert-Quisquater-Yung, PKC'06 and '07).
  - Intrusion-resilient PKE (Dodis *et al.* – RSA-CT'04).

Other Pairing-Based PKE schemes (ctd.)

- Public key encryption with keyword search (Boneh *et al.* – Eurocrypt'04).
  - Connection with anonymous IBE (Abdalla *et al.* – Crypto'05).
  - Efficient searchable PKE in the standard model thanks to Gentry (Eurocrypt'06) and Boyen-Waters (Crypto'06) IBE schemes.

Other Pairing-Based PKE schemes (ctd.)

- Certificate-Based Encryption (Gentry, Eurocrypt'03) (CBE) removes key escrow from IBE.
  - Standard model realizations using Dodis-Katz (TCC'05).
- Certificateless Encryption (Al-Riyami-Paterson, Asiacrypt'03) independently achieves the same goal.
  - Dent-Libert-Paterson (2006): CCA-secure CLE in standard model using full security definitions of Al-Riyami-Paterson.

Conclusions

- Pairings definitely enlarge the cryptographer's toolbox for public key encryption.
- Theoretical applications far beyond IBE.
- Recent focus on removing reliance on random oracle model – sometimes at the expense of less natural hardness assumptions.
- Open problems remain.