III – Pairing-based Cryptography

David Pointcheval

Ecole normale supérieure, CNRS & INRIA

ENS – Paris – 2018

Outline

Outline

Gap Groups

Definition (Pairing Setting)

- Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic groups of prime order p.
- Let g_1 and g_2 be generators of $\mathbb{G}_1$ and $\mathbb{G}_2$ respectively.
- Let $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}^T$, be a bilinear map.

Definition (Various Cases)

1. The symmetric case: $\mathbb{G}_1 = \mathbb{G}_2$.
2. There exists an isomorphism ψ, from $\mathbb{G}_2$ onto $\mathbb{G}_1$:
   1. ψ is efficiently computable; as well as ψ^{-1}
   2. ψ is efficiently computable; but no efficient isomorphism from $\mathbb{G}_1$ onto $\mathbb{G}_2$
   3. no efficiently computable isomorphism in any direction

Gap Groups

[Okamoto-Pointcheval – RSA '01]

Definition (co-Diffie-Hellman Problems)

Let $(p, \mathbb{G}_1, g_1, \mathbb{G}_2, g_2, \mathbb{G}^T, e)$ be a pairing setting

- **co-CDH** in $(\mathbb{G}_1, \mathbb{G}_2)$: Given $g, g^a \in \mathbb{G}_2$ and $h \in \mathbb{G}_1$, compute h^a
- **co-DDH** in $(\mathbb{G}_1, \mathbb{G}_2)$: Given $g, g^a \in \mathbb{G}_2$ and $h, h^b \in \mathbb{G}_1$, decide whether $a = b$ or not

Note: when $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$, **co-CDH** in $(\mathbb{G}_1, \mathbb{G}_2)$ is **CDH** in $\mathbb{G}$, and **co-DDH** in $(\mathbb{G}_1, \mathbb{G}_2)$ is **DDH** in $\mathbb{G}$

Definition (Gap Groups)

We say that a group $\mathbb{G}$ is a gap group if **CDH** in $\mathbb{G}$ is hard, whereas **DDH** in $\mathbb{G}$ is simple.

Outline

Admissible Bilinear Map

[Joux – ANTS '00]

Definition (Admissible Bilinear Map)

Let $(p, \mathbb{G}_1, g_1, \mathbb{G}_2, g_2, \mathbb{G}^T, e)$ be a pairing setting, with $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}^T$ a non-degenerated bilinear map

- Bilinear: for any $g \in \mathbb{G}_1$, $h \in \mathbb{G}_2$ and $u, v \in \mathbb{Z}$,
$$e(g^u, h^v) = e(g, h)^{uv}$$
- Non-degenerated: $e(g_1, g_2) \neq 1$

co-DDH in $(\mathbb{G}_1, \mathbb{G}_2)$ easy

Given $g, g^a \in \mathbb{G}_2$ and $h, h^b \in \mathbb{G}_1$
$$a = b \bmod p \iff e(h, g^a) = e(h^b, g)$$

Bilinear Diffie-Hellman Problems

We now focus on the symmetric case: $\mathbb{G}_1 = \mathbb{G}_2 = \mathbb{G}$.

Diffie-Hellman Problems

- **CDH** in $\mathbb{G}$: Given $g, g^a, g^b \in \mathbb{G}$, compute g^{ab}
- **DDH** in $\mathbb{G}$: Given $g, g^a, g^b, g^c \in \mathbb{G}$, decide whether $c = ab$ or not

CDH can be hard to solve, but **DDH** is easy in gap-groups.

Bilinear Diffie-Hellman Problems

- **CBDH** in $\mathbb{G}$: Given $g, g^a, g^b, g^c \in \mathbb{G}$, compute $e(g, g)^{abc}$
- **DBDH** in $\mathbb{G}$: Given $g, g^a, g^b, g^c \in \mathbb{G}$ and $h \in \mathbb{G}^T$, decide whether $h \stackrel{?}{=} e(g, g)^{abc}$

Outline

Signature in Gap Groups [Boneh-Lynn-Shacham – Asiacryp '01]

Let $\mathbb{G}$ be a gap-group of prime order p, with a generator g.

Signature Scheme

- Key generation: choose $x \in \mathbb{Z}_p$, and set $y = g^x$;
- Signature of $M \in \mathbb{G}$: $\sigma = M^x$;
- Verification of (M, σ): check $\mathbf{DDH}(g, y, M, \sigma)$.

Full-Domain Hash

$$\mathcal{H} : \{0,1\}^\star \to \mathbb{G}$$

- In order to sign m, one first computes $M = \mathcal{H}(m) \in \mathbb{G}$
- then $\sigma = M^x = \mathbf{CDH}(g, y, \mathcal{H}(m))$

The signature of a message m is thus an element $\sigma \in \mathbb{G}$.

Identity-Based Cryptography [Shamir – Crypto '84]

Public-Key Cryptography

Each user $\mathcal{ID}$ owns

- a public key *pk*
- a certificate that guarantees the link between $\mathcal{ID}$ and *pk*
- a private key *sk*, related to *pk*

One has to access a dictionary in order to get *pk*, the public key of $\mathcal{ID}$, together with the certificate, in order to encrypt a message to $\mathcal{ID}$.

Identity-Based Cryptography

Each user $\mathcal{ID}$ owns

- a private key *sk*, related to $\mathcal{ID}$
- the public key *pk* is indeed $\mathcal{ID}$ itself

Key Computation

Public-Key Cryptography

- User $\mathcal{ID}$ chooses his private key *sk*
- derives his public key *pk*
- asks a TTP for the certification of *pk* w.r.t. $\mathcal{ID}$

Identity-Based Cryptography

- Each user $\mathcal{ID}$ asks a TTP for the computation of the private key *sk*, related to $\mathcal{ID}$
  $\Rightarrow$ extraction

Note

For signature, the two scenarios are quite similar.

Identity-Based Encryption

Setup

The authority generates a master secret key msk,
and publishes the public parameters, PK

Extraction

Given an identity $\mathcal{ID}$, the authority computes
the private key *sk* granted the master secret key *sk*

Encryption

Any one can encrypt a message *m* to a user $\mathcal{ID}$
using only *m*, $\mathcal{ID}$ and the public parameters PK

Decryption

Given a ciphertext, user $\mathcal{ID}$ can recover the plaintext,
with his secret key *sk*

Outline

Security Model: $\mathbf{IND-ID-CCA}$

Definition ($\mathbf{IND-ID-CCA}$ Security)

The adversary
- receives the global parameters
- asks any extraction-query, and any decryption-query
- outputs a target identity $\mathcal{ID}^\star$
  and two messages (m_0, m_1)

The challenger flips a bit *b*, and encrypts m_b for $\mathcal{ID}^\star$ into $c^\star$,
then the adversary
- asks any extraction-query, and any decryption-query
- outputs its guess b' for *b*

$$\mathbf{Adv}^{\mathsf{ind-id-cca}} = 2 \times \Pr[b' = b] - 1$$

Restrictions

- $\mathbf{IND-ID-CCA}$: semantic security, full-identity, chosen-ciphertext attacks
  The adversary is just restricted not to ask:
  - the target identity $\mathcal{ID}^\star$ to the extraction-oracle,
  - nor the challenge ciphertext $c^\star$ to the decryption-oracle with $\mathcal{ID}^\star$
- $\mathbf{sID}$: selective-identity
  The adversary provides the target identity $\mathcal{ID}^\star$ before receiving the global parameters
- $\mathbf{CPA}$: chosen-plaintext attacks
  The adversary does not have access to the decryption-oracle

Identity-Based Encryption

[Boneh-Franklin – Crypto '01]

Setup

- The authority sets up a gap-group framework:
  a group $\mathbb{G}$ of prime order p, with a generator g,
  with an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}^T$
- It selects a master secret key msk $= s \in \mathbb{Z}_p$
- It publishes the public parameters: $\mathsf{PK} = (p, \mathbb{G}, e, g, P = g^s)$

Extraction

Given an identity $\mathcal{ID}$, the authority compute
the private key $sk = \mathcal{H}(\mathcal{ID})^s$

Note that sk is a BLS signature of $\mathcal{ID}$,
which can be checked by the user: $e(sk, g) \stackrel{?}{=} e(\mathcal{H}(\mathcal{ID}), P)$

BF IBE (Cont'd)

Encryption

In order to encrypt a message m to a user $\mathcal{ID}$

- one chooses a random $r \in \mathbb{Z}_p$
- computes $A = g^r$ and $K = e(P, \mathcal{H}(\mathcal{ID})^r)$
- sends $(A, B = K \times m)$

$$\begin{aligned} K &= e(P, \mathcal{H}(\mathcal{ID})^r) = e(g^s, \mathcal{H}(\mathcal{ID})^r) \\ &= e(g^r, \mathcal{H}(\mathcal{ID})^s) = e(A, sk) \end{aligned}$$

Decryption

Upon reception of (A, B), user $\mathcal{ID}$

- computes $K = e(A, sk)$
- gets $m = B/K$

BF IBE Security Analysis

Theorem

The BF IBE is $\mathbf{IND-ID-CPA}$ *secure*
under the ***DBDH*** *problem,*
in the random oracle model.

By masking m with $H(K)$: $B = m \oplus H(K)$,
the BF IBE is $\mathbf{IND-ID-CPA}$ *secure*
under the ***CBDH*** *problem,*
in the random oracle model

CCA Security

[Fujisaki-Okamoto – Crypto '01]

Usual tricks in the random oracle model to achieve $\mathbf{IND-ID-CCA}$.

- How to avoid the random oracle model?
- How to avoid a full-domain hash function onto $\mathbb{G}$?

Outline

Boneh-Boyen's Signature

[Boneh-Boyen – Eurocrypt '04]

Let $\mathbb{G}$ be a cyclic group of prime order p, with two independent generators g, h, equipped with an admissible bilinear map

$$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}^T$$

For any message $m \in \mathbb{Z}_p$ (output by a hash function), we define $F(m) = uv^m$, where u and v are independent public elements in $\mathbb{G}$.

Boneh-Boyen's Signature (Cont'd)

Signature Scheme

- Key generation: choose $x \in \mathbb{Z}_p$, and set $G = g^x$ as well as $H = h^x$; The public key is G, whereas H is kept private.
- Signature of $m \in \mathbb{Z}_p$: $\sigma = (H \times F(m)^r, g^r)$, for a random $r \in \mathbb{Z}_p$; Here, $F(m) = G^m \times u$
- Verification of $(m, (\sigma_1, \sigma_2))$: check whether

$$\begin{aligned} e(g, \sigma_1) &= e(g, h^x \times F(m)^r) \\ &= e(g, h^x) \times e(g, F(m)^r) = e(g^x, h) \times e(g^r, F(m)) \\ &\stackrel{?}{=} e(G, h) \times e(\sigma_2, F(m)) \end{aligned}$$

Boneh-Boyen's Signature: Security Analysis

Theorem (Selected-Message CMA)

*For a message $m^\star$ chosen ahead, before having seen the parameters and the public key, signing $m^\star$ under a chosen-message attack is intractable under the **CDH** problem in $\mathbb{G}$.*

Simulation: Selected-Message Forgery

Let us be given g, $G = g^a$ and $h = g^b$, we want to extract $H = h^a = g^{ab}$.
We set $u = G^{-m^\star} g^\beta$ for a random β:

$$F(m) = G^m u = G^{m-m^\star} g^\beta \qquad F(m^\star) = g^\beta$$

A forgery for $m^\star$: (σ_1, σ_2), such that

$$e(g, \sigma_1) = e(G, h) e(\sigma_2, g^\beta) \Longrightarrow e(G, h) = e(g, \sigma_1/\sigma_2^\beta)$$

$$\mathbf{CDH}(g, h, G) = \sigma_1/\sigma_2^\beta$$

Boneh-Boyen's Signature: Security Analysis

Simulation: CMA

For any query $m \neq m^\star$, we simulate a signature:
$\sigma_1 = h^{-\beta/(m-m^\star)} F(m)^r$ and $\sigma_2 = g^r h^{1/(m^\star - m)}$
Let us set $\rho = r - b/(m - m^\star)$:

$$\begin{aligned} \sigma_1 &= h^{-\beta/(m-m^\star)} \times F(m)^r \\ &= h^{-\beta/(m-m^\star)} \times (G^{m-m^\star} g^\beta)^{\rho + b/(m-m^\star)} \\ &= h^{-\beta/(m-m^\star)} \times G^{\rho(m-m^\star)} \times G^b \times g^{\beta\rho} \times h^{\beta/(m-m^\star)} \\ &= h^a \times G^{\rho(m-m^\star)} \times g^{\beta\rho} \\ &= h^a \times F(m)^\rho \\ \sigma_2 &= g^r \times h^{1/(m^\star - m)} = g^{r - b/(m-m^\star)} = g^\rho \end{aligned}$$

Identity-Based Encryption

[Boneh-Boyen – Eurocrypt '04]

Setup

- The authority sets up a gap-group framework:
  a group $\mathbb{G}$ of prime order p,
  with three independent generators g, h and u,
  with an admissible bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}^T$
- It selects a master secret key $s \in \mathbb{Z}_p$, and keeps $H = h^s$
- It publishes the parameters: $(p, \mathbb{G}, e, g, h, G = g^s)$

Extraction

Given an identity $\mathcal{ID}$, the authority computes the key
$sk = (sk_1 = H \times F(\mathcal{ID})^r, sk_2 = g^r)$, where $F(x) = uG^x$

Note that sk is a BB signature of $\mathcal{ID}$: $e(g, sk_1) \stackrel{?}{=} e(G, h) \times e(sk_2, F(\mathcal{ID}))$

BB IBE (Cont'd)

Encryption

In order to encrypt a message $m \in \mathbb{G}^T$ to a user $\mathcal{ID}$

- one chooses a random $t \in \mathbb{Z}_p$
- computes $A = F(\mathcal{ID})^t$, $B = g^t$ and $K = e(G, h)^t$
- sends $(A, B, C = K \times m)$

$$\begin{aligned} K &= e(G,h)^t = e(g^s,h)^t = e(g^t,h^s) = e(g^t,H) \\ &= e(g^t, sk_1/F(\mathcal{ID})^r) = e(g^t, sk_1)/e(g^t, F(\mathcal{ID})^r) \\ &= e(B, sk_1)/e(g^r, F(\mathcal{ID})^t) = e(B, sk_1)/e(sk_2, A) \end{aligned}$$

Decryption

Upon reception of (A, B, C),
user $\mathcal{ID}$ computes $K = e(B, sk_1)/e(A, sk_2)$ and gets $m = C/K$

BB IBE (Cont'd)

BB IBE Security Analysis

The BB IBE is $\mathbf{IND} - \mathbf{sID} - \mathbf{CPA}$ secure under the **DBDH** problem

Outline

Waters' Signature

[Waters – Eurocrypt '05]

Let $\mathbb{G}$ be a cyclic group of prime order p,
with two independent generators g, h,
equipped with an admissible bilinear map

$$e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}^T$$

For any message $m \in \{0,1\}^k$ (output by a hash function), we define

$$F(m) = u'(\prod u_i^{m_i}), \qquad m = m_1 \dots m_k,$$

where u' and $u_1, \dots, u_k$ are independent public elements in $\mathbb{G}$

Waters' Signature (Cont'd)

Signature Scheme

- Key generation: choose $x \in \mathbb{Z}_p$,
  and set $G = g^x$ as well as $H = h^x$;
  The public key is G, whereas H is kept private.
- Signature of $m \in \{0,1\}^k$: $\sigma = (H \times F(m)^r, g^r)$,
  for a random $r \in \mathbb{Z}_p$;
- Verification of $(m, (\sigma_1, \sigma_2))$: check whether

$$\begin{aligned} e(g, \sigma_1) &= e(g, h^x \times F(m)^r) \\ &= e(g, h^x) \times e(g, F(m)^r) = e(g^x, h) \times e(g^r, F(m)) \\ &\stackrel{?}{=} e(G, h) \times e(\sigma_2, F(m)) \end{aligned}$$

Waters' Signature (Cont'd)

Theorem

The Water's IBE is $\mathbf{IND-ID-CPA}$ *secure*
under the ***DBDH*** *problem*