Advanced Encryption: IBE and Pairings

CS 276: Introduction to Cryptography

Sanjam Garg

March 30, 2026

Overview

1. Diffie–Hellman and Bilinear Maps
2. Identity-Based Encryption (IBE)
3. Pairing-Based IBE

Diffie–Hellman Key Exchange

Classic DH

Public parameters: group G of prime order p with generator g.

- Alice: sample $a \leftarrow \mathbb{Z}_p$, send $A = g^a$.
- Bob: sample $b \leftarrow \mathbb{Z}_p$, send $B = g^b$.
- Shared key: $K = g^{ab}$, computed as $K = B^a = A^b$.

Eavesdropper sees (g, A, B) but (under CDH/DDH) cannot recover g^{ab}.

Diffie–Hellman Key Exchange

Classic DH

Public parameters: group G of prime order p with generator g.

- Alice: sample $a \leftarrow \mathbb{Z}_p$, send $A = g^a$.
- Bob: sample $b \leftarrow \mathbb{Z}_p$, send $B = g^b$.
- Shared key: $K = g^{ab}$, computed as $K = B^a = A^b$.

Eavesdropper sees (g, A, B) but (under CDH/DDH) cannot recover g^{ab}.

From DH to PKE (sketch)

One-bit ElGamal-style encryption:

- $\mathsf{pk} = A = g^a$, $\mathsf{sk} = a$.
- Encrypt $m \in \{0, 1\}$: sample $b, r \leftarrow \mathbb{Z}_p$, set $c_1 = g^b$, $c_2 = mA^b + (1 - m)g^r$.
- Decrypt: test whether $c_2 = c_1^a$ to recover m.

Bilinear Maps

Definition 1 (Bilinear map)

Let G, G_T be cyclic groups of prime order p with generator $g \in G$. A **bilinear map** is an efficiently computable $e : G \times G \to G_T$ such that:

- $e(g, g)$ generates G_T.
- For all $a, b \in \mathbb{Z}_p$: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

Bilinear Maps

Definition 1 (Bilinear map)

Let G, G_T be cyclic groups of prime order p with generator $g \in G$. A **bilinear map** is an efficiently computable $e : G \times G \to G_T$ such that:

- $e(g, g)$ generates G_T.
- For all $a, b \in \mathbb{Z}_p$: $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$.

DH via pairings

If $A = g^a$, $B = g^b$, $T = g^{ab}$, then $e(A, B) = e(g^a, g^b) = e(g, g)^{ab} = e(g, T)$.

Tripartite Diffie–Hellman

Three-party DH using pairings

Private keys: $a, b, c \leftarrow \mathbb{Z}_p$.

- Public keys: $A = g^a$, $B = g^b$, $C = g^c$.
- Shared key: $K = e(g, g)^{abc}$, computable by each party:
  - Alice: $K = e(B, C)^a$.
  - Bob: $K = e(A, C)^b$.
  - Carol: $K = e(A, B)^c$.

Motivation: Identity-Based Encryption

Why IBE?

In traditional PKI, senders must fetch and verify recipients' public keys (certificates, CAs, etc.). This is costly and error-prone.

Motivation: Identity-Based Encryption

Why IBE?

In traditional PKI, senders must fetch and verify recipients' public keys (certificates, CAs, etc.). This is costly and error-prone.

IBE idea

- Public key is an **identity string** (e.g. email address).
- A trusted **Private Key Generator** (PKG) runs setup, then issues secret keys for identities.
- Sender only needs the master public key and recipient ID to encrypt.

IBE is also a building block for CCA-secure PKE and signatures.

IBE Syntax

Definition 2 (Identity-Based Encryption)

An IBE scheme $\mathcal{E}_{id} = (G, K, E, D)$ has:

- $G(1^n)$: setup; outputs master public key mpk and master secret key msk.
- $K(msk, id)$: keygen; outputs secret key sk_{id} for identity id.
- $E(mpk, id, m)$: encrypts m under identity id, outputs ciphertext c.
- $D(sk_{id}, c)$: decrypts; outputs m or $\perp$.

IBE Correctness

Definition 3 (Correctness)

For all n, identities id, messages m:

$$\Pr\Big[(mpk, msk) \leftarrow G(1^n),\ sk_{id} \leftarrow K(msk, id),\ c \leftarrow E(mpk, id, m),\ m' \leftarrow D(sk_{id}, c)\Big] = 1 - \mathrm{negl}(n),$$

where the probability is over the randomness of G, K, E.

IBE Security: IBE-CPA Game

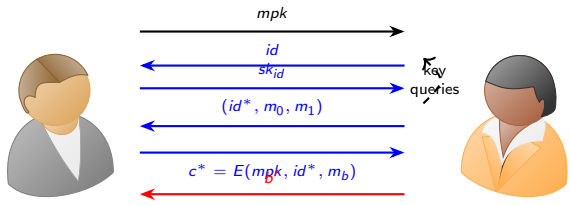
Game $\mathrm{Exp}^{\mathrm{IBE,CPA}}_{\Pi,\mathcal{A}}(n)$

1. Challenger runs $(mpk, msk) \leftarrow G(1^n)$, sends mpk to $\mathcal{A}$.
2. $\mathcal{A}$ may make **key queries** id and receive sk_{id} (for any $id \neq id^*$).
3. $\mathcal{A}$ outputs challenge identity id^* and messages (m_0, m_1).
4. Challenger samples $b \leftarrow \{0,1\}$, computes $c^* \leftarrow E(mpk, id^*, m_b)$, sends c^* to $\mathcal{A}$.
5. $\mathcal{A}$ may continue to make key queries for identities $id \neq id^*$.
6. Finally $\mathcal{A}$ outputs b'; output 1 if $b' = b$, else 0.

IBE-CPA: Challenger vs Adversary

$$\mathrm{Exp}^{\mathrm{IBE,CPA}}_{\Pi,\mathcal{A}}(n)$$

sample $(mpk, msk) \leftarrow G(1^n)$, $b \leftarrow \{0,1\}$



output 1 if $b' = b$; else 0

IBE Security Definition

Definition 4 (IBE-CPA security)

An IBE $\mathcal{E}_{id} = (G, K, E, D)$ is IBE-CPA secure if for every non-uniform PPT adversary $\mathcal{A}$:

$$\Pr[\mathrm{Exp}^{\mathrm{IBE,CPA}}_{\Pi,\mathcal{A}}(n) = 1] = \frac{1}{2} + \mathrm{negl}(n).$$

Equivalently, $\mathcal{A}$'s advantage over random guessing is negligible.

BDH Assumption

Definition 5 (Decisional Bilinear Diffie–Hellman (DBDH))

Let $e : \mathbb{G}_0 \times \mathbb{G}_1 \to \mathbb{G}_T$ be a pairing, with cyclic groups of prime order q and generators $g_0 \in \mathbb{G}_0$, $g_1 \in \mathbb{G}_1$. The DBDH assumption says that

$$(g_0^\alpha, g_1^\alpha, g_0^\beta, g_1^\gamma, e(g_0, g_1)^{\alpha\beta\gamma})$$

is computationally indistinguishable from

$$(g_0^\alpha, g_1^\alpha, g_0^\beta, g_1^\gamma, e(g_0, g_1)^\delta),$$

where $\alpha, \beta, \gamma, \delta \leftarrow \mathbb{Z}_q$.

IBE from Pairings: Construction

Setup and KeyGen

Let G be a group of order q with generator g, pairing $e : G \times G \to G_T$, and hash $H : \{0,1\}^* \to G$.

- $G(1^n)$: pick $\alpha \leftarrow \mathbb{Z}_q$; $mpk = g^\alpha$, $msk = \alpha$.
  Output (mpk, msk).
- $K(msk = \alpha, id)$: set $sk_{id} = H(id)^\alpha$.

IBE from Pairings: Construction

Setup and KeyGen

Let G be a group of order q with generator g, pairing $e : G \times G \to G_T$, and hash $H : \{0,1\}^* \to G$.

- $G(1^n)$: pick $\alpha \leftarrow \mathbb{Z}_q$; $mpk = g^\alpha$, $msk = \alpha$.
  Output (mpk, msk).
- $K(msk = \alpha, id)$: set $sk_{id} = H(id)^\alpha$.

Encrypt and Decrypt

- $E(mpk, id, m)$: pick $\beta \leftarrow \mathbb{Z}_q$; set

$$c_1 = g^\beta, \quad c_2 = e(mpk, H(id)^\beta) \cdot m,$$

  output $c = (c_1, c_2)$.
- $D(sk_{id}, c_1, c_2)$: output $m = \frac{c_2}{e(c_1, sk_{id})}$.

Correctness of Pairing-Based IBE

Check

$$
\begin{aligned}
m' &= \frac{c_2}{e(c_1, sk_{id})} \\
&= \frac{e(mpk, H(id)^{\beta}) \cdot m}{e(g^{\beta}, H(id)^{\alpha})} \\
&= \frac{e(g^{\alpha}, H(id)^{\beta})}{e(g^{\beta}, H(id)^{\alpha})} \cdot m \\
&= \frac{e(g, H(id))^{\alpha\beta}}{e(g, H(id))^{\alpha\beta}} \cdot m \\
&= m.
\end{aligned}
$$

Security Theorem (Sketch)

Theorem 6

If the DBDH assumption holds for e and H is modeled as a random oracle, then the above IBE scheme is IBE-CPA secure.

Security Theorem (Sketch)

Theorem 6

If the DBDH assumption holds for e and H is modeled as a random oracle, then the above IBE scheme is IBE-CPA secure.

Proof idea

Adversary $\mathcal{B}$ gets a DBDH challenge and must distinguish $e(g,g)^{\alpha\beta\gamma}$ from random. It simulates the IBE game for $\mathcal{A}$ by:

- Embedding g^{α} as mpk, programming $H(id)$ so that one special identity gets $H(id^*) = g^{\beta}$.
- Using the DBDH tuple to form the challenge ciphertext for id^* and (m_0, m_1).
- If $\mathcal{A}$ has non-negligible advantage, $\mathcal{B}$ distinguishes DBDH.

Full proof follows the notes (reduction + success probability bound). $\square$