Identity-Based Encryption and Pairings

Dan Boneh receives 2014 ACM-Infosys Foundation Award in the Computing Sciences

Dan Boneh’s work was central to establishing the field of pairing-based cryptography where pairings are used to construct new cryptographic capabilities and improve the performance of existing ones. Boneh, in joint work with Matt Franklin, constructed a novel pairing-based method for identity-based encryption (IBE), whereby a user’s public identity, such as an email address, can function as the user’s public key. Since then, Boneh’s contributions, together with those of others, have shown the power and versatility of pairings, which are now used as a mainstream tool in cryptography. The transfer of pairings from theory to practice has been rapid. Organizations now using pairings include healthcare, financial, and insurance institutions. Over a billion IBE-encrypted emails are sent each year.

The People

Identity-Based Encryption from the Weil Pairing

Abstract

We propose a fully practical identity-based encryption scheme (IBE). The scheme has a ciphertext size that is constant (regardless of the computation of the Boneh problem. Our system is based on bilinear maps between groups. The Weil pairing elliptic curve is an example of such a map. We give precise definitions for secure identity encryption schemes and give several applications for such systems.

The Awards

Example: I = bob@example.com

Receiver generates her own key pair (pk, sk)

Trusted authority (CA), given pk, provides receiver with a certificate cert

Sender needs Receiver’s certificate before she can encrypt

Receiver generates nothing a priori

Sender only needs receiver’s identity I before she can encrypt

Trusted authority (CA), given I, provides receiver with a decryption key
**Syntax of an IBE scheme**

\[ \text{IBE} = (P, K, E, D) \]

- \( P \) parameter generation
- \( K \) key generation
- \( E \) encryption
- \( D \) decryption

The correct decryption requirement for identity \( I \) and message \( M \) asks that

\[ \Pr[D(\text{mpk}, K(\text{mpk}, I), E(\text{mpk}, I, M)) = M] = 1 \]

**Security of an IBE scheme**

For any identity \( I' \neq I \)

- The master public key \( \text{mpk} \)
- The identity \( I \)
- The ciphertext \( C \)
- AND: Secret key \( \text{sk} \) for any identity \( I' \neq I \)

Adversary \( A \) should be unable to figure out a message \( M \) encrypted to identity \( I \), even given

- The master public key \( \text{mpk} \)
- The identity \( I \)
- The ciphertext \( C \)
- AND: Secret key \( \text{sk} \) for any identity \( I' \neq I \)

**Building an IBE scheme**

It is hard to find a way to build an IND-CPA-secure IBE scheme based on conventional number theory.

**Game IND-CPA_{\text{IBE}}**

\[ \text{Adv}_{\text{IND-CPA}_{\text{IBE}}}^\text{A}(\text{mpk, msk}) \]

Initialize

\( \{\text{mpk, msk}\} \leftarrow P; b \mapsto \{0, 1\} \)

Exd \( \leftarrow \emptyset \); Chl \( \leftarrow \emptyset \)

Return \( \text{mpk} \)

Expose(I)

If \( (I \in \text{Chl}) \) then return \( \bot \)

Exd \( \leftarrow \text{Exd} \cup \{I\} \)

\( \text{sk} \leftarrow K(\text{mpk}, \text{msk}, I) \)

Return \( \text{sk} \)

LR(I, M_0, M_1)

If \( (I \in \text{Exd}) \) then return \( \bot \)

Chl \( \leftarrow \text{Chl} \cup \{I\} \)

\( C \leftarrow E(\text{mpk}, I, M_0) \)

Return \( C \)

Finalize(b')

Return \( (b = b') \)

Security requires that adversary can't figure out whether left \( (b=0) \) or right \( (b=1) \) messages are encrypted for challenge identities.

Even when it is allowed to obtain the secret keys of non-challenge identities.

**With RSA, let**

- \( \text{mpk} = (N, e) \)
- \( \text{msk} = (N, d) \)
- \( \text{sk} = ? \)
- \( C = ? \)

\[ \text{IBE} = (P, K, E, D) \] is an IBE scheme.
Pairings

Let $e: G \times G \to G_T$ be a function, where $G, G_T$ are groups whose order $p$ is a prime. Let $g$ be a generator of $G$.

We say that $e$ is a pairing if the following are true:

- Bi-linearity: $e(g^x, g^y) = e(g, g)^{xy}$ for all $x, y \in \mathbb{Z}_p$
- Non-degeneracy: $e(g, g)$ is a generator of $G_T$.

Let $e: G \times G \to G_T$ be a function, where $G, G_T$ are groups whose order $p$ is a prime. Let $g$ be a generator of $G$.

Game $\text{BDH}_{e,g}$

Initialize $a, b, c \leftarrow \mathbb{Z}_p$
Return $g^a, g^b, g^c$

Finalize $(Z)$
Return $(Z = e(g, g)^{abc})$

Adv$_{\text{bdh}}(A) = \Pr[B \text{DH}_e, g \in A]$

Pairings that appear to be BDH-secure can be built from the Weil and Tate pairings over elliptic curves.

Boneh-Franklin IBE scheme

$e: G \times G \to G_T$ a BDH-secure pairing
$g$ a generator of $G$
$p$ the order of $G, G_T$
Identity $I \in \{0,1\}^*$
Message $M \in \{0,1\}^m$
Function $H: \{0,1\}^* \to G$
Function $G: G_T \to \{0,1\}^m$

Algorithm $\mathcal{P}$

$\text{msk} \leftarrow \mathbb{Z}_p$ ; $\text{mpk} \leftarrow g^\text{msk}$

Return $(\text{mpk}, \text{msk})$

Algorithm $\mathcal{K}(\text{mpk}, \text{msk}, I)$

$s_k \leftarrow H(I)^{\text{msk}}$ ; Return $s_k$

Algorithm $\mathcal{E}(\text{mpk}, I, M)$

$r \leftarrow \mathbb{Z}_p$ ; $R \leftarrow g^r$ ; $K \leftarrow e(\text{mpk}, H(I)^r)$

$W \leftarrow G(K) \oplus M$ ; Return $(R, W)$

Algorithm $\mathcal{D}(\text{mpk}, s_k, (R, W))$

$L \leftarrow e(R, s_k) ; M \leftarrow G(L) \oplus W ;$ Return $M$

Proof of correct decryption requirement:

Let $I \in \{0,1\}^*$ be an identity.
Let $M \in \{0,1\}^m$ be a message
Let $s_k = K(\text{mpk}, \text{msk}, I) = H(I)^{\text{msk}}$
Let $(R, W) \leftarrow \mathcal{E}(\text{mpk}, I, M)$
We show that $\mathcal{D}(\text{mpk}, s_k, (R, W)) = M$

Let $i$ be such that $H(I) = g^i$

Advantage of PBC Library

Subject to some assumptions, the PBC library can be used to build pairing-based cryptosystems that are secure against all known attacks.

IBE features

Sender only needs receiver’s identity / before she can encrypt
"Trusted" authority can decrypt all ciphertexts for all identities
Revocation is a pain

IBE issues

"Trusted" authority can decrypt all ciphertexts for all identities
Compromise of server storing $\text{msk}$ can result in adversary decrypting all ciphertexts for all identities
A secure channel is needed to communicate $\text{sk}$ from trusted authority to receiver
Revocation is a pain