

Boneh-Franklin Identity Based Encryption Revisited

David Galindo

d.galindo@cs.ru.nl

Security of Systems

Department of Computer Science

Radboud Universiteit Nijmegen

ICALP 2005

2005, July 13

Outline

- Definitions
 - Identity Based Encryption (IBE)
 - Secure IBEs
 - Bilinear maps and problems

Outline

- Definitions
 - Identity Based Encryption (IBE)
 - Secure IBEs
 - Bilinear maps and problems
- Boneh-Franklin IBE scheme revisited
 - A flaw in the security reduction
 - New security proof

Identity Based Encryption (IBE)

Identity Based Encryption (IBE)

Main idea The public key is an identity $id \in \{0, 1\}^*$

A Key Generation Center **KGC** issues private keys for id

Identity Based Encryption (IBE)

Main idea The public key is an identity $id \in \{0, 1\}^*$

A Key Generation Center **KGC** issues private keys for id

An IBE scheme consists of 4 algorithms:

Setup Takes a security parameter ℓ and outputs system parameters **params** and **master-key**.

Identity Based Encryption (IBE)

Main idea The public key is an identity $id \in \{0, 1\}^*$

A Key Generation Center **KGC** issues private keys for id

An IBE scheme consists of 4 algorithms:

Setup Takes a security parameter ℓ and outputs system parameters $params$ and **master-key**.

Encrypt Takes as inputs $params$, $id \in \{0, 1\}^*$ and message m and outputs a ciphertext C .

Identity Based Encryption (IBE)

Main idea The public key is an identity $id \in \{0, 1\}^*$

A Key Generation Center **KGC** issues private keys for id

An IBE scheme consists of 4 algorithms:

Setup Takes a security parameter ℓ and outputs system parameters $params$ and $master-key$.

Encrypt Takes as inputs $params$, $id \in \{0, 1\}^*$ and message m and outputs a ciphertext C .

ExtractPrivateKey Takes as inputs $params$, $master-key$ and $id \in \{0, 1\}^*$ and outputs a private decryption key d_{id} .

Identity Based Encryption (IBE)

Main idea The public key is an identity $id \in \{0, 1\}^*$

A Key Generation Center **KGC** issues private keys for id

An IBE scheme consists of 4 algorithms:

Setup Takes a security parameter ℓ and outputs system parameters $params$ and $master-key$.

Encrypt Takes as inputs $params$, $id \in \{0, 1\}^*$ and message m and outputs a ciphertext C .

ExtractPrivateKey Takes as inputs $params$, $master-key$ and $id \in \{0, 1\}^*$ and outputs a private decryption key d_{id} .

Decrypt Takes as inputs $params$, private key d_{id} and message C and outputs a message m .

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

Initialization The challenger runs **setup**, gives the adversary \mathcal{A} the description of \mathcal{E} , **params** and keeps **master-key** secret.

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

Initialization The challenger runs **setup**, gives the adversary \mathcal{A} the description of \mathcal{E} , **params** and keeps **master-key** secret.

Phase 1 \mathcal{A} issues adaptive queries of the type

- Extraction query $\langle \text{id}_i \rangle$
- Decryption query $\langle \text{id}_i, C_i \rangle$

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

Initialization The challenger runs `setup`, gives the adversary \mathcal{A} the description of \mathcal{E} , `params` and keeps `master-key` secret.

Phase 1 \mathcal{A} issues adaptive queries of the type

- Extraction query $\langle \text{id}_i \rangle$
- Decryption query $\langle \text{id}_i, C_i \rangle$

Challenge \mathcal{A} outputs two equal length m_0, m_1 and id_{ch} on which it wishes to be challenged. The challenger $\beta \leftarrow \{0, 1\}$ and sets $C = \text{Encrypt}(\text{params}, \text{id}_{ch}, m_\beta)$

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

Initialization The challenger runs **setup**, gives the adversary \mathcal{A} the description of \mathcal{E} , **params** and keeps **master-key** secret.

Phase 1 \mathcal{A} issues adaptive queries of the type

- Extraction query $\langle \text{id}_i \rangle$
- Decryption query $\langle \text{id}_i, C_i \rangle$

Challenge \mathcal{A} outputs two equal length m_0, m_1 and id_{ch} on which it wishes to be challenged. The challenger $\beta \leftarrow \{0, 1\}$ and sets $C = \text{Encrypt}(\text{params}, \text{id}_{ch}, m_\beta)$

Phase 2 As in Phase 1, except submitting id_{ch} or $\langle \text{id}_{ch}, C \rangle$

IBE chosen ciphertext security

IND-ID-CCA security for an IBE scheme \mathcal{E}

Initialization The challenger runs **setup**, gives the adversary \mathcal{A} the description of \mathcal{E} , **params** and keeps **master-key** secret.

Phase 1 \mathcal{A} issues adaptive queries of the type

- Extraction query $\langle \text{id}_i \rangle$
- Decryption query $\langle \text{id}_i, C_i \rangle$

Challenge \mathcal{A} outputs two equal length m_0, m_1 and id_{ch} on which it wishes to be challenged. The challenger $\beta \leftarrow \{0, 1\}$ and sets $C = \text{Encrypt}(\text{params}, \text{id}_{ch}, m_\beta)$

Phase 2 As in Phase 1, except submitting id_{ch} or $\langle \text{id}_{ch}, C \rangle$

Guess \mathcal{A} outputs a bit β' and wins if $\beta' = \beta$.

Bilinear maps and bilinear groups

Let \mathbb{G}, \mathbb{G}_1 be prime order p abelian groups in which the discrete logarithm is believed to be hard. Let $\mathbb{G} = \langle P \rangle$.

Bilinear maps and bilinear groups

Let \mathbb{G}, \mathbb{G}_1 be prime order p abelian groups in which the discrete logarithm is believed to be hard. Let $\mathbb{G} = \langle P \rangle$.
By a **bilinear map** we will refer to a non-degenerate bilinear function $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$.

- $e(aP, bP) = e(P, abP) = e(abP, P) = e(P, aP)^b = e(P, P)^{ab}$
- $e(P, P) \neq \mathbf{1}_{\mathbb{G}_1} \quad a, b \in \mathbb{Z}_p$

Bilinear maps and bilinear groups

Let \mathbb{G}, \mathbb{G}_1 be prime order p abelian groups in which the discrete logarithm is believed to be hard. Let $\mathbb{G} = \langle P \rangle$. By a bilinear map we will refer to a non-degenerate bilinear function $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$.

- $e(aP, bP) = e(P, abP) = e(abP, P) = e(P, aP)^b = e(P, P)^{ab}$
- $e(P, P) \neq \mathbf{1}_{\mathbb{G}_1} \quad a, b \in \mathbb{Z}_p$

Bilinear Diffie-Hellman (BDH) Problem on \mathbb{G} . Given $P, aP, bP, cP \in \mathbb{G}$ as input, where $a, b, c \leftarrow \mathbb{Z}_p$ compute $\hat{e}(P, P)^{abc} \in \mathbb{G}_1$.

Bilinear maps and bilinear groups

Let \mathbb{G}, \mathbb{G}_1 be prime order p abelian groups in which the discrete logarithm is believed to be hard. Let $\mathbb{G} = \langle P \rangle$. By a bilinear map we will refer to a non-degenerate bilinear function $\hat{e} : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_1$.

- $e(aP, bP) = e(P, abP) = e(abP, P) = e(P, aP)^b = e(P, P)^{ab}$
- $e(P, P) \neq \mathbf{1}_{\mathbb{G}_1} \quad a, b \in \mathbb{Z}_p$

Bilinear Diffie-Hellman (BDH) Problem on \mathbb{G} . Given $P, aP, bP, cP \in \mathbb{G}$ as input, where $a, b, c \leftarrow \mathbb{Z}_p$ compute $\hat{e}(P, P)^{abc} \in \mathbb{G}_1$.

Decision Bilinear Diffie-Hellman (DBDH) Problem on \mathbb{G} . Given $P, aP, bP, cP \leftarrow \mathbb{G}$, where $a, b, c \leftarrow \mathbb{Z}_p$, and $T \leftarrow \mathbb{G}_1$, as inputs; tell apart $(P, aP, bP, cP, \hat{e}(P, P)^{abc})$ from (P, aP, bP, cP, T) .

Concrete security

Security level A problem \mathcal{P} has security level 2^t when the minimal computational effort to solve \mathcal{P} is 2^t basic operations.

Concrete security

Security level A problem \mathcal{P} has security level 2^t when the minimal computational effort to solve \mathcal{P} is 2^t basic operations.

Currently, it is required $t \geq 80$.

Concrete security

Security level A problem \mathcal{P} has security level 2^t when the minimal computational effort to solve \mathcal{P} is 2^t basic operations.

Currently, it is required $t \geq 80$.

In the Random Oracle Model $q_{\text{RO}} \leq 2^t$, and it is often assumed that $q_D, q_E \leq 2^{30}$.

Boneh-Franklin IBE scheme (2001-03)

Setup.

- Choose $P \leftarrow \mathbb{G}$, $s \leftarrow \mathbb{Z}_p^*$ and set $P_{pub} = sP \in \mathbb{G}$.

Boneh-Franklin IBE scheme (2001-03)

Setup.

- Choose $P \leftarrow \mathbb{G}$, $s \leftarrow \mathbb{Z}_p^*$ and set $P_{pub} = sP \in \mathbb{G}$.
- Choose $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G}_1 \rightarrow \{0, 1\}^n$,
 $H_3 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0, 1\}^n \rightarrow \{0, 1\}^n$.

Boneh-Franklin IBE scheme (2001-03)

Setup.

- Choose $P \leftarrow \mathbb{G}$, $s \leftarrow \mathbb{Z}_p^*$ and set $P_{pub} = sP \in \mathbb{G}$.
- Choose $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G}_1 \rightarrow \{0, 1\}^n$,
 $H_3 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0, 1\}^n \rightarrow \{0, 1\}^n$.
- Set $\mathcal{M} = \{0, 1\}^n$ and $\mathcal{C} = \mathbb{G} \times \{0, 1\}^n \times \{0, 1\}^n$.

Boneh-Franklin IBE scheme (2001-03)

Setup.

- Choose $P \leftarrow \mathbb{G}$, $s \leftarrow \mathbb{Z}_p^*$ and set $P_{pub} = sP \in \mathbb{G}$.
- Choose $H_1 : \{0, 1\}^* \rightarrow \mathbb{G}$, $H_2 : \mathbb{G}_1 \rightarrow \{0, 1\}^n$,
 $H_3 : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \mathbb{Z}_p^*$, $H_4 : \{0, 1\}^n \rightarrow \{0, 1\}^n$.
- Set $\mathcal{M} = \{0, 1\}^n$ and $\mathcal{C} = \mathbb{G} \times \{0, 1\}^n \times \{0, 1\}^n$.
- $\text{params} = \langle P, P_{pub}, H_1, H_2, H_3, H_4 \rangle$.
- The master-key is $s \in \mathbb{Z}_p^*$.

Boneh-Franklin IBE scheme (ii)

Extract.

- $d_{\text{ID}} = sH_1(\text{id}) \in \mathbb{G}.$

Boneh-Franklin IBE scheme (ii)

Extract.

- $d_{\text{ID}} = sH_1(\text{id}) \in \mathbb{G}$.

Encrypt. To encrypt $M \in \{0, 1\}^n$ under the public key ID

- Compute $Q_{\text{ID}} = H_1(\text{ID}) \in \mathbb{G}$, choose $\sigma \leftarrow \{0, 1\}^n$.

- Set $C = \langle rP, \sigma \oplus H_2(g_{\text{ID}}^r), M \oplus H_4(\sigma) \rangle$ where $g_{\text{ID}} = \hat{e}(P_{\text{pub}}, Q_{\text{ID}}) \in \mathbb{G}_1$, and $r = H_3(\sigma, M)$.

Boneh-Franklin IBE scheme (ii)

Extract.

- $d_{\text{ID}} = sH_1(\text{id}) \in \mathbb{G}$.

Encrypt. To encrypt $M \in \{0, 1\}^n$ under the public key ID

- Compute $Q_{\text{ID}} = H_1(\text{ID}) \in \mathbb{G}$, choose $\sigma \leftarrow \{0, 1\}^n$.

- Set $C = \langle rP, \sigma \oplus H_2(g_{\text{ID}}^r), M \oplus H_4(\sigma) \rangle$ where $g_{\text{ID}} = \hat{e}(P_{\text{pub}}, Q_{\text{ID}}) \in \mathbb{G}_1$, and $r = H_3(\sigma, M)$.

Decrypt. To decrypt $C = \langle U, V, W \rangle \in \mathbb{G} \times \{0, 1\}^n \times \{0, 1\}^n$

- Compute $V \oplus H_2(\hat{e}(U, d_{\text{id}})) = \sigma$ and $W \oplus H_4(\sigma) = M$.

- Set $r = H_3(\sigma, M)$. Check that $U = rP$. If not **reject**.

Boneh-Franklin IBE scheme (ii)

Extract.

- $d_{\text{ID}} = sH_1(\text{id}) \in \mathbb{G}$.

Encrypt. To encrypt $M \in \{0, 1\}^n$ under the public key ID

- Compute $Q_{\text{ID}} = H_1(\text{ID}) \in \mathbb{G}$, choose $\sigma \leftarrow \{0, 1\}^n$.

- Set $C = \langle rP, \sigma \oplus H_2(g_{\text{ID}}^r), M \oplus H_4(\sigma) \rangle$ where $g_{\text{ID}} = \hat{e}(P_{\text{pub}}, Q_{\text{ID}}) \in \mathbb{G}_1$, and $r = H_3(\sigma, M)$.

Decrypt. To decrypt $C = \langle U, V, W \rangle \in \mathbb{G} \times \{0, 1\}^n \times \{0, 1\}^n$

- Compute $V \oplus H_2(\hat{e}(U, d_{\text{id}})) = \sigma$ and $W \oplus H_4(\sigma) = M$.

- Set $r = H_3(\sigma, M)$. Check that $U = rP$. If not **reject**.

$$\hat{e}(U, d_{\text{id}}) = \hat{e}(rP, sQ_{\text{id}}) = \hat{e}(sP, rQ_{\text{id}}) = \hat{e}(P_{\text{pub}}, Q_{\text{id}})^r = g_{\text{id}}^r$$

Security intuition/statement

Sender aP, bP, c \rightarrow $\hat{e}(P, P)^{abc} = \hat{e}(aP, bP)^c$

Receiver abP, cP \rightarrow $\hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$

Adversary aP, bP, cP \nrightarrow $\hat{e}(P, P)^{abc}$

Security intuition/statement

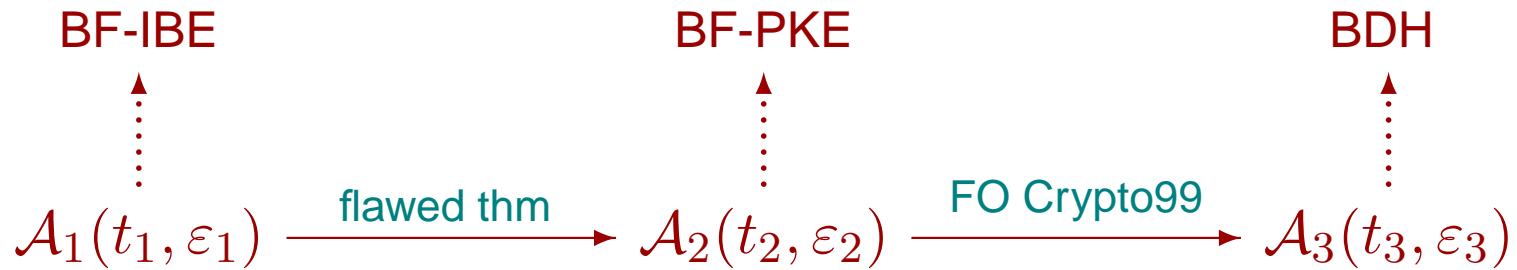
Sender aP, bP, c $\rightarrow \hat{e}(P, P)^{abc} = \hat{e}(aP, bP)^c$

Receiver abP, cP $\rightarrow \hat{e}(P, P)^{abc} = \hat{e}(abP, cP)$

Adversary aP, bP, cP $\nrightarrow \hat{e}(P, P)^{abc}$

Theorem Let \mathcal{A} an IND-ID-CCA adversary running in time t and with advantage ε against BF-IBE making at most q_E, q_D, q_H queries. Then there exists \mathcal{B} running in time roughly t with advantage at least $\frac{\varepsilon}{q_H^2 q_D}$ against BDH problem in \mathbb{G} .

Security reduction strategy



A flaw in the reduction

Theorem Let \mathcal{A} an **IND-ID-CCA** adversary that has advantage ε against **BF-IBE** making at most q_H, q_E, q_D queries. Then there is an **IND-CCA** adversary \mathcal{B} that has advantage at least $\frac{\varepsilon}{(1+q_E+q_D)}$ against **BF-PKE**.

A flaw in the reduction

Theorem Let \mathcal{A} an **IND-ID-CCA** adversary that has advantage ε against **BF-IBE** making at most q_H, q_E, q_D queries. Then there is an **IND-CCA** adversary \mathcal{B} that has advantage at least $\frac{\varepsilon}{(1+q_E+q_D)}$ against **BF-PKE**.

Let $C = \langle rP, \sigma \oplus H_2(e(P, Q)^r), M \oplus H_4(\sigma) \rangle$

A flaw in the reduction

Theorem Let \mathcal{A} an **IND-ID-CCA** adversary that has advantage ε against **BF-IBE** making at most q_H, q_E, q_D queries. Then there is an **IND-CCA** adversary \mathcal{B} that has advantage at least $\frac{\varepsilon}{(1+q_E+q_D)}$ against **BF-PKE**.

Let $C = \langle rP, \sigma \oplus H_2(e(P, Q)^r), M \oplus H_4(\sigma) \rangle$

Wrong claim: $C' = \langle b^{-1}rP, \sigma \oplus H_2(e(P, bQ)^{b^{-1}r}), M \oplus H_4(\sigma) \rangle$

BF-decrypts as C does, where $b \leftarrow \mathbb{Z}_p$ is known.

A flaw in the reduction

Theorem Let \mathcal{A} an **IND-ID-CCA** adversary that has advantage ε against **BF-IBE** making at most q_H, q_E, q_D queries. Then there is an **IND-CCA** adversary \mathcal{B} that has advantage at least $\frac{\varepsilon}{(1+q_E+q_D)}$ against **BF-PKE**.

Let $C = \langle rP, \sigma \oplus H_2(e(P, Q)^r), M \oplus H_4(\sigma) \rangle$

Wrong claim: $C' = \langle b^{-1}rP, \sigma \oplus H_2(e(P, bQ)^{b^{-1}r}), M \oplus H_4(\sigma) \rangle$

BF-decrypts as C does, where $b \leftarrow \mathbb{Z}_p$ is known.

But the checking $H_3(\sigma, m) = b^{-1}rP$ does (almost) never hold!.

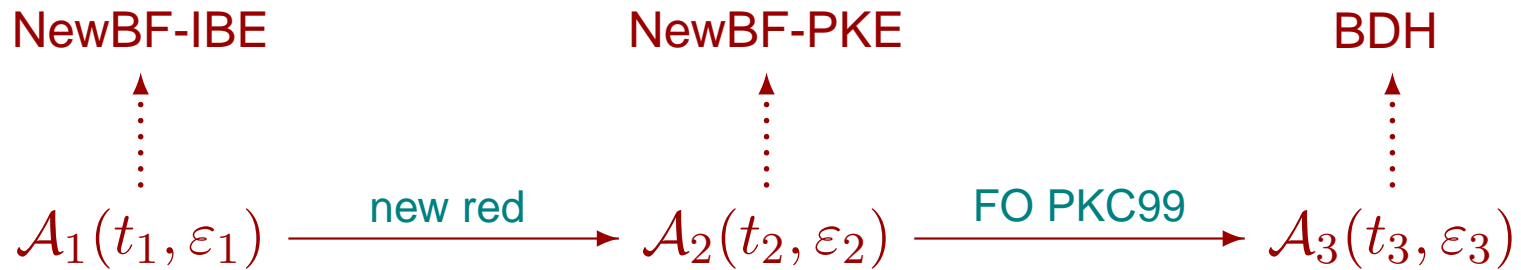
BF security reduction is not valid!

Fixing the reduction

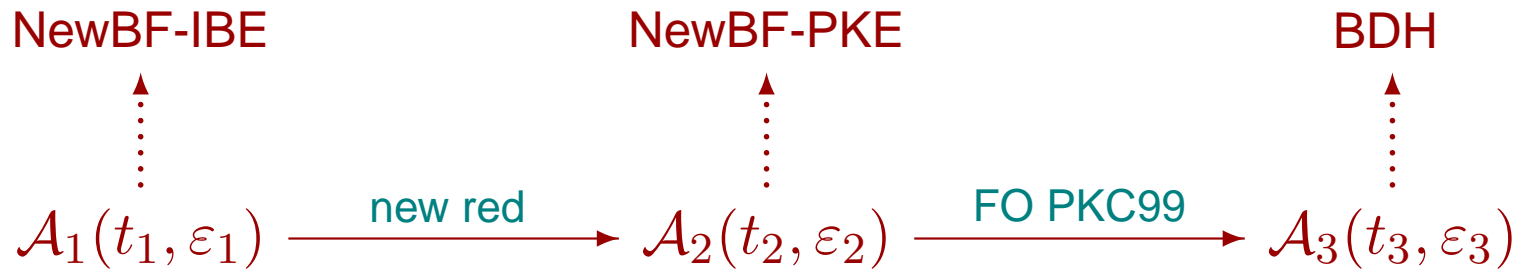
Theorem Let \mathcal{A} an IND-ID-CCA adversary running in time t and with advantage ε against BF-IBE making at most q_H queries. Then exists \mathcal{B} running in time roughly t with advantage at least $\frac{\varepsilon}{q_H^3}$ against BDH problem in \mathbb{G} .

Worse reduction :-)

IBE scheme with tighter reduction

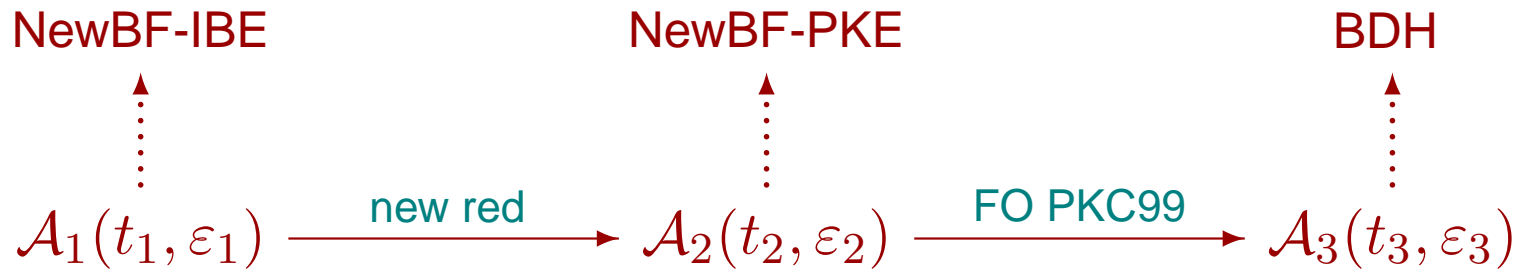


IBE scheme with tighter reduction



Theorem Let $\mathcal{A}(t, \varepsilon)$ breaking IND-ID-CCA security of NewBF-IBE making at most q_H queries. Then there exists $\mathcal{B}(t, \frac{\varepsilon}{q_H^2})$ against BDH problem in \mathbb{G} .

IBE scheme with tighter reduction



Theorem Let $\mathcal{A}(t, \varepsilon)$ breaking **IND-ID-CCA** security of **NewBF-IBE** making at most q_H queries. Then there exists $\mathcal{B}(t, \frac{\varepsilon}{q_H^2})$ against **BDH** problem in \mathbb{G} .

The new scheme has shorter and more compact ciphertexts, uses one less random oracle, has a tighter reduction ($\frac{\varepsilon}{q_H}$ with respect to decisional **BDH**.)

Conclusions

- A flaw in **BF** security reduction has been pointed out and solved.
- A **New-BF** scheme with better performance and security properties.
- These remarks can be applied to a considerable number of works in the literature.

This is the end...