ID-based encryption from bilinear pairings

Tatiana Issaeva

18 February 2003

Identity-based systems

- public-key encryption schemes, but users do not have explicit public keys.
- public key is derived from a user's publicly available identity (for example e-mail address)
- the services of trusted third party is required during set-up phase to generate user's private key.
- idea proposed in 1984 by Shamir
- Motivation: to stimulate the deployment of a public key infrastructure.

Identity-based systems: latest developments

- constructing a usable IBE was considered an open issue

- in 2001 [Boneh, Franklin] proposed a secure IBE system based on bilinear pairings

- security of [Boneh, Franklin] IBE system is based on hardness of Bilinear Diffie-Hellman (BDH) problem

- also in 2001 [Cocks] proposed a secure IBE system based on quadratic residues

The Bilinear Diffie-Hellman (BDH) problem.

- let G_1 and G_2 be two groups of prime order q.

- let $e : G_1 \times G_1 \to G_2$be a bilinear map

- let P be a generator of G_1.

The BDH problem in $\langle G_1, G_2, e\rangle$ is

- given $\langle P, aP, bP, cP\rangle$ compute $e = (P, P)^{abc}$ for some $a, b, c \in \mathbb{Z}_p^*$.

BDH parameter generator

Definition 1. A randomized algorithm $\mathcal{G}$ is a *BDH parameter generator* if (1) $\mathcal{G}$ takes a security parameter $k \in \mathbb{Z}^+$, (2) $\mathcal{G}$ runs in polynomial time in k, and (3) $\mathcal{G}$ outputs a prime number q, the description of two proups G_1, G_2 of order q, and the description of admissible bilinear map $e : G_1 \times G_1 \rightarrow G_2$.

Denote $\mathcal{G}\left(1^k\right) = \langle q, G_1, G_2, e\rangle$ as output of $\mathcal{G}$.

BDH assumption

Definition 2. An algorithm $\mathcal{A}$ has an advantage $\epsilon(k)$ in solving the BDH problem for $\mathcal{G}$ if for sufficiently large k: $\mathsf{adv}_{\mathcal{G},\mathcal{A}}(k) \geq \epsilon(k)$,

where $\mathsf{adv}_{\mathcal{G},\mathcal{A}}(k) =$

$$= \Pr\left[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc} \middle| a, b, c \leftarrow \mathbb{Z}_p^*\right]$$

BDH assumption (cont)

- BDH parameter generator $\mathcal{G}$ satisfies the BDH assumption if $\mathsf{adv}_{\mathcal{G},\mathcal{A}}(k) < 1/f\,(k)$ for any randomized polynomial time algorithm $\mathcal{A}$, for any polynomial $f \in \mathbb{Z}\,[x]$ and for sifficiently large k.

- when $\mathcal{G}$ satisfies the BDH assumption, it is said that BDH is hard in groups generated by $\mathcal{G}$.

Identity-Based encryption (IBE) definition.

An IBE scheme $\mathcal{E}$ is specified by 4 algorithms:

- Setup generates global system parametes params and a $\mathsf{master-key}$

- $\mathsf{Extract}$ uses the $\mathsf{master-key}$ and params to generate the private key d from public key $\mathsf{ID} \in \{0,1\}^*$

- Encryption: $C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, M)$

- Decryption: $M = \mathsf{Decrypt}(\mathsf{params}, C, d)$

Chosen ciphertext attack on IBE.

Let's build algorithm to break IBE by chosen ciphertext attack (CCA), consisting from five stages:

- **Setup**
- **Phase 1**
- **Challenge**
- **Phase 2**
- **Guess**

Chosen ciphertext attack on IBE: Setup.

- the challenger takes a security paramer k and runs the Setup algorithm.

- it gives the attacker the resulting system parameters params.

- it keeps the $\mathsf{master-key}$ to itself.

Chosen ciphertext attack on IBE: Phase 1

The attacker issues adaptive queries

$q_1, \ldots, q_m$ where query q_i is one of:

- Extraction query $\langle \mathsf{ID}_i \rangle$: the attacker receives the private key d_i for the public key ID_i.

- Decryption query $\langle \mathsf{ID}_i, C_i \rangle$: the attacker receives the private key d_i corresponding to the public key ID_i and plaintext as decrypted from the ciphertext C_i using the private key d_i.

Chosen ciphertext attack on IBE: Challenge

- the attacker produces two equal length plaintexts $M_0, M_1 \in \mathcal{M}$ and an identity ID to be challenged.

- Constraint: ID did not appear in any extraction query $\langle \mathsf{ID}_i \rangle$ in Phase 1.

- the challenger picks a random bit $b \in \{0, 1\}$ and sets $C = \mathsf{Encrypt}(\mathsf{params}, \mathsf{ID}, M_b)$.

- the challenger sends C as challenge to the attacker.

Chosen ciphertext attack on IBE: Phase 2

The attacker issues more adaptive queries

$q_{m+1}, \ldots, q_n$ the same way as in Phase 1:

- Extraction query $\langle \mathsf{ID}_i \rangle$, where $\mathsf{ID}_i \neq \mathsf{ID}$.

- Decryption query $\langle \mathsf{ID}_i, C_i \rangle \neq \langle \mathsf{ID}, C \rangle$.

Chosen ciphertext attack on IBE: Guess

- finally, the attacker outputs a guess $b^{'} \in \{0,1\}$.

- the attacker wins the game, if $b = b^{'}$.

We refer to such an attacker as $\mathsf{IND-ID-CCA}$ adversary.

Chosen ciphertext security of IBE

Definition 3. The advantage of $\mathsf{IND-ID-CCA}$ adversary $\mathcal{A}$ against the IBE scheme $\mathcal{E}$ is:

$$\mathsf{adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|.$$

Definition 4. The IBE scheme $\mathcal{E}$ is semantically secure against an adaptive chosen ciphertext attack if for any polynomial time $\mathsf{IND-ID-CCA}$ adversary $\mathcal{A}$ the function $\mathsf{adv}_{\mathcal{E},\mathcal{A}}(k)$ is negligible.

Chosen plaintext security of IBE

The attacker can issue only extraction queries $\langle \mathsf{ID}_i \rangle$ in Phase 1 and Phase 2 of $\mathsf{IND}-\mathsf{ID}-\mathsf{CCA}$ algorithm.

Definition 5. The advantage of $\mathsf{IND}-\mathsf{ID}-\mathsf{CPA}$ adversary $\mathcal{A}$ against the scheme $\mathcal{E}$ is:

$$\mathsf{adv}_{\mathcal{E},\mathcal{A}}(k) = \left|\Pr\left[b = b'\right] - \frac{1}{2}\right|.$$

Definition 6. We say that the IBE scheme $\mathcal{E}$ is semantically secure if for any polynomial time $\mathsf{IND}-\mathsf{ID}-\mathsf{CPA}$ adversary $\mathcal{A}$ the function $\mathsf{adv}_{\mathcal{E},\mathcal{A}}(k)$ is negligible.

IBE based on bilinear pairings: overview.

- IBE scheme from [Boneh, Franklin].

- First we consider basic IBE scheme, which is $\mathsf{IND}-\mathsf{ID}-\mathsf{CPA}$ secure only

- extend basic IBE to full IBE scheme to get security against an adaptive chosen ciphertext attack in the random oracle model.

- reliability of random oracle model is questionable.

Basic IBE scheme BasicIdent: Setup

Let $\mathcal{G}$ be some BDH parameter generator satisfying the BDH assumption.

- run $\mathcal{G}$ on input $k \in \mathbb{Z}^+$to generate $\mathcal{G}\left(1^k\right) = \langle q, G_1, G_2, e \rangle$. Choose generator $P \in G_1$.

- choose random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$.

- choose $H_1 : \{0,1\}^* \to G_1^*$, $H_2 : G_2 \to \{0,1\}^n$ for some n.

The system parameters are

$\mathsf{params} = \left\langle q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2 \right\rangle$.

The $\mathsf{master-key}$ is $s \in \mathbb{Z}_q^*$.

Basic IBE scheme BasicIdent: Extract

For a given $\mathsf{ID} \in \{0,1\}^*$

- compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID}) \in G_1^*$
- set private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$.

Basic IBE scheme BasicIdent: Encrypt

To encrypt message $m \in \{0, 1\}^n$

- compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID})$
- compute $g_{\mathsf{ID}} = e(Q_{\mathsf{ID}}, P_{pub})$
- choose random $r \in \mathbb{Z}_q^*$
- compute $U = rP$ and $V = m \oplus H_2(g_{\mathsf{ID}}^r)$.
- set cipher text to be $C = \langle U, V \rangle$.

Basic IBE scheme BasicIdent: Decrypt

To decrypt C

- compute $m = V \oplus H_2(e(d_{\mathsf{ID}}, U)$.

BasicIdent: security definition

Theorem 1: *Suppose the hash functions* H_1,H_2 *are random oracles. Then* BasicIdent *is* IND − ID − CPA *secure assuming BDH is hard in groups generated by* $\mathcal{G}$. *Concretely, suppose there is an adversary* $\mathcal{A}$ *that has advantage* $\epsilon(k)$*against scheme* BasicIdent. *Suppose* $\mathcal{A}$ *makes at most* $q_E > 0$ *private key extraction queries and* $q_{H_2} > 0$ *hash queries to* H_2. *Then there is algorithm* $\mathcal{B}$ *that solves BDH in groups generated by* $\mathcal{G}$ *with advantage at least:*

$$\mathsf{Adv}_{\mathcal{G},\mathcal{B}}(k) \geq \frac{2\epsilon(k)}{e(1+q_E)q_{H_2}}.$$

The running time of $\mathcal{B}$ *is* $\mathcal{O}$*(time(*$\mathcal{A}$*)).*

Security proof of BasicIdent: overview

Stage 1:

- build the public key encryption scheme BasicPub from BasicIdent

- show that $\mathsf{IND}-\mathsf{ID}-\mathsf{CPA}$ attack on BasicIdent can be converted to $\mathsf{IND}-\mathsf{CPA}$ attack on BasicPub

Stage 2

- show that BasicPub is $\mathsf{IND}-\mathsf{CPA}$ secure if BDH assumption holds.

Security proof of BasicIdent: Stage 1.

public key encryption scheme BasicPub:

- keygen produces the public key

$$K_{pub} = \left\langle q, G_1, G_2, e, n, P, P_{pub}, Q_{\mathsf{ID}}, H_2 \right\rangle$$

- all the parameters are the same as in Setup algorithm from BasicIdent, except Q_{ID}

- Q_{ID} is random element from G_1^*

- encrypt and decrypt - the same as in BasicIdent, but Q_{ID} is from keygen

Security proof of BasicIdent: Stage 1 (cont).

Lemma 1. *Let H_1 be a random oracle from $\{0,1\}^*$ to G_1^*. Let $\mathcal{A}$ be an* $\mathsf{IND}-\mathsf{ID}-\mathsf{CPA}$ *adversary that has advantage $\epsilon(k)$ against* BasicIdent. *Suppose $\mathcal{A}$ makes at most $q_E > 0$ private key extraction queries. Then there is a* $\mathsf{IND}-\mathsf{CPA}$ *adversary $\mathcal{B}$ that has advantage at least $\frac{\epsilon(k)}{e(1+q_E)}$ against* BasicPub. *Its running time is $O(\mathit{time}(\mathcal{A}))$.*

Proof of lemma 1.

- challenger generates public key K_{pub} and private key $d_{\mathsf{ID}} = sQ_{\mathsf{ID}}$.

- K_{pub} is given to algorithm $\mathcal{B}$

- $\mathcal{B}$ produces two messages m_0 and m_1 and expects encryption of m_b under K_{pub}, where $b \in \{0, 1\}$.

- then $\mathcal{B}$ guesses $b^{'} \in \{0, 1\}$ for b.

$\mathcal{B}$ works by interacting with IND – ID – CPA adversary $\mathcal{A}$

Proof of lemma 1. Setup:

- $\mathcal{B}$ gives $\mathcal{A}$ the $\mathsf{BasicIdent}$ system parameters $\left\langle q, G_1, G_2, e, n, P, P_{pub}, H_1, H_2 \right\rangle$

- H_1 is a random oracle controlled by $\mathcal{B}$

- the rest parameters are from K_{pub}

Proof of lemma 1. H_1-queries:

- $\mathcal{A}$ can query H_1 at any time.
- $\mathcal{B}$ maintains a list H_1^{list} of tuples $\left\langle \mathsf{ID}_j, Q_j, b_j, c_j \right\rangle$
- H_1^{list} is initially empty

Proof of lemma 1. H_1**-queries (cont):**

When $\mathcal{A}$ queries H_1 at a point ID_i:

- if ID_i is in H_1^{list} in a tuple $\langle \mathsf{ID}_i, Q_i, b_i, c_i \rangle$, then $\mathcal{B}$ responds with $H_1(I\mathsf{D}_i) = Q_i$.

- if ID_i is not in H_1^{list}, $\mathcal{B}$ generates random *coin* $\in \{0, 1\}$, $\Pr[coin = 0] = \delta$.

- $\mathcal{B}$ picks a random $b \in \mathbb{Z}_q^*$. If coin $= 0$, compute $Q_i = bP$, else compute $Q_i = bQ_{\mathsf{ID}}$.

- $\mathcal{B}$ adds a tuple $\langle \mathsf{ID}_i, Q_i, b_i, c_i \rangle$ to H_1^{list} and responds to $\mathcal{A}$ with $Q_i = H_1(\mathsf{ID}_i)$.

Proof of lemma 1. Phase 1:

- $\mathcal{A}$ issues private key extraction query ID_i to $\mathcal{B}$.

- $\mathcal{B}$ computes $Q_i = H_1(\mathsf{ID}_i)$.

- $\langle \mathsf{ID}_i, Q_i, b_i, coin_i \rangle$ is coresponding tuple in H_1^{list}.

- If *coin* $= 1$, then attack on BasicPub failed, $\mathcal{B}$ reports failure and terminates.

Proof of lemma 1. Phase 1 (cont):

- if *coin* $= 0$, hence $Q_i = b_i P$.

- define $d_i = b_i P_{pub} \in G_1^*$

- since $d_i = sQ_i$, d_i is a private key assosiated with public ID_i.

- $\mathcal{B}$ provides d_i to $\mathcal{A}$.

Proof of lemma 1. Challenge (step 1):

- $\mathcal{A}$ decides that Phase 1 is overand outputs public key ID_{ch} and two messages m_0 and m_1 to be challenged.

- $\mathcal{B}$ gives m_0 and m_1 to challenger as the messages to be challenged on

- the challenger responds ciphertext $C = \langle U, V \rangle$, such that C is encryption of m_c under K_{pub} for random $c \in \{0, 1\}$

Proof of lemma 1. Challenge (step 2):

- $\mathcal{B}$ runs algorithm of H_1-queries to compute $Q \in G_1^*$: $H_1(\mathsf{ID}_{ch}) = Q$.

- let $\langle \mathsf{ID}_{ch}, Q, b, coin \rangle$ be a coresponding tuple in H_1^{list}.

- if *coin* $= 0$, then attack on BasicPub failed, $\mathcal{B}$ reports failure and terminates.

Proof of lemma 1. Challenge (step 3):

- if *coin* $= 1$, hence $Q = bQ_{\mathsf{ID}}$.

- when $C = \langle U, V \rangle$, then $U \in G_1^*$.

- set $C^{'} = \left\langle b^{-1}U, V \right\rangle$, where $b^{-1}$is inverse of b mod q.

$C^{'}$ is a BasicIdent encryption of m_c under ID_{ch}, since $H_1(\mathsf{ID}_{ch}) = Q$ and private key corresponding to ID_{ch} is $d_{ch} = sQ$.

Proof of lemma 1. Challenge :

Note that

$$e(b^{-1}U, d_{ch}) = e(b^{-1}U, sQ) =$$

$$= e(U, sb^{-1}Q) = e(U, sQ_{\mathsf{ID}}) = e(U, d_{\mathsf{ID}})$$

Hence: BasicIdent decryption of C' using d_{ch} is the same as the BasicPub decryption of C using d_{ID}.

Proof of lemma 1. Phase 2:

- $\mathcal{A}$ issues more private key extraction queries
- $\mathcal{B}$ responds as in Phase 1

Proof of lemma 1. Guess:

- eventually $\mathcal{A}$ produces a guess $c^{'}$ for c.

- $\mathcal{B}$ outputs $c^{'}$ as its guess for c

Proof of lemma 1 (cont).

Claim 1: if $\mathcal{B}$ does not abort during the simulation then $\mathcal{A}$'s view is identical to its view of real attack.

- all responces to H_1 are uniformly distributed in and are valid.

Proof of lemma 1 (cont).

Claim 2: probability that $\mathcal{B}$ does not abort is $\left|\Pr\left[c = c'\right] - \frac{1}{2}\right| \geq \epsilon$

- the challenge C' given to $\mathcal{A}$ is the BasicIdent encryption of m_c for random $c \in \{0, 1\}$

- see definition of $\mathcal{A}$

Proof of lemma 1 (cont).

Pr[$\mathcal{B}$ does not abort during the simulations] is $\delta^{q_E}(1-\delta)$, where

- δ^{q_E} - Pr[$\mathcal{B}$ does not abort in phases 1,2]
- $(1-\delta)$ - Pr[$\mathcal{B}$ does not abort at challenge step]
- $\delta^{q_E}(1-\delta)$ maximized at $\delta = 1 - 1/(q_E + 1)$
- Pr[$\mathcal{B}$ does not abort] $\geq 1/e(q_E + 1)$.
- So $\mathcal{B}$'s advantage $\geq \epsilon/e(q_E + 1)$

$\square$

Security proof of BasicIdent: Stage 2.

Lemma 2. *Let H_2a random oracle from G_2 to $\{0,1\}^n$. Let $\mathcal{A}$ be an* $\mathsf{IND-CPA}$ *adversary that has advantage $\epsilon(k)$ against* BasicPub*. Suppose $\mathcal{A}$ makes a total $q_{H_2} > 0$ queries to H_2. Then there is an algorithm $\mathcal{B}$ that solves BDH problem for $\mathcal{G}$ with advantage at least $\frac{2\epsilon(k)}{q_{H_2}}$ and the running time is O(time($\mathcal{A}$)).*

Proof of lemma 2.

Let $D = (P, P)^{abc}$ is the solution to the BDH problem. $\mathcal{B}$ is given as input

- the BDH parameters $\langle q, G_1, G_2, e \rangle$
- random instance of the BDH problem $\langle P, aP, bP, cP \rangle = \langle P, P_1, P_2, P_3 \rangle$ for random $P \in G_1^*$and for random $a, b, c \in \mathbb{Z}_q^*$.

Let's build algorithm $\mathcal{B}$ to find D by interaction with $\mathcal{A}$.

Proof of lemma 2. Setup:

- $\mathcal{B}$ creates $K_{pub} = \left\langle q, G_1, G_2, e, n, P, P_{pub}, Q_{\mathsf{ID}}, H_2 \right\rangle$
- so that $P_{pub} = P_1$ and $Q_{\mathsf{ID}} = P_2$
- $\mathcal{B}$ gives $\mathcal{A}$ the K_{pub}
- unknown private key associated with K_{pub} is $d_{\mathsf{ID}} = aQ_{\mathsf{ID}} = abP$

Proof of lemma 2. H_2-queries:

- $\mathcal{A}$ can query H_2 at any time.
- $\mathcal{B}$ maintains a list H_2^{list} of tuples $\left\langle X_j, H_j \right\rangle$
- H_2^{list} is initially empty.

Proof of lemma 2. H_2**-queries:**

When $\mathcal{A}$ queries H_2 at a point X_i:

if X_i is in H_2^{list} in a tuple $\langle X_i, H_i \rangle$:

- then $\mathcal{B}$ responds with $H_2(X_i) = H_i$.

if X_i is not in H_2^{list}:

- $\mathcal{B}$ generates a random string $H_i \in \{0, 1\}^n$
- adds a tuple $\langle X_i, H_i \rangle$ to the H_2^{list}
- responds to $\mathcal{A}$ with $H_2(X_i) = H_i$.

Proof of lemma 2. Challenge:

- $\mathcal{A}$ outputs two messages m_0 and m_1 on which it wishes to be challenged.

- $\mathcal{B}$ picks a random string $R \in \{0,1\}^n$

- $\mathcal{B}$ defines C to be the ciphertext $C = \langle P_3, R \rangle$

- $\mathcal{B}$ gives it as a challenge to $\mathcal{A}$.

Note $C = R \oplus H_2(e(P_3, d_{\mathsf{ID}})) = R \oplus H_2(D)$.

Proof of lemma 2. Guess:

- $\mathcal{A}$ produces a guess $c^{'} \in \{0, 1\}$.

- $\mathcal{B}$ picks a random tuple $\left\langle X_j, H_j \right\rangle$ from H_2^{list}

- $\mathcal{B}$ outputs X_j as the solution to given instance of BDH.

Proof of lemma 2.

Pr[$\mathcal{B}$ outputs correct answer D to BDH] = ?

- event $\mathcal{H}$ = [$\mathcal{A}$ issues a query for $H_2(D)$ at some point during the simulation].

- Pr $[\mathcal{H}]$ in simulation is the same as in real attack.

- in real attack $\left|\Pr\left[c = c'\right] - \frac{1}{2}\right| \geq \epsilon$ (by definition of $\mathcal{A}$).

Proof of lemma 2.

$\Pr\left[c = c^{'}\right] =$

$= \Pr\left[\left|c = c^{'}\right| \neg\mathcal{H}\right] \Pr\left[\neg\mathcal{H}\right] + \Pr\left[\left|c = c^{'}\right| \mathcal{H}\right] \Pr\left[\mathcal{H}\right] \leq$

$\leq \Pr\left[\left|c = c^{'}\right| \neg\mathcal{H}\right] \Pr\left[\neg\mathcal{H}\right] + \Pr\left[\mathcal{H}\right] \leq$

$\leq \frac{1}{2}\Pr\left[\neg\mathcal{H}\right] + \Pr\left[\mathcal{H}\right] \leq \frac{1}{2} + \frac{1}{2}\Pr\left[\mathcal{H}\right]$

From latter,

$\Pr\left[c = c^{'}\right] \geq \Pr\left[\left|c = c^{'}\right| \neg\mathcal{H}\right] \Pr\left[\neg\mathcal{H}\right] = \frac{1}{2} - \frac{1}{2}\Pr\left[\mathcal{H}\right].$

Hence, $\epsilon \leq \left|\Pr\left[c = c^{'}\right] - \frac{1}{2}\right| \leq \frac{1}{2}\Pr\left[\mathcal{H}\right].$

Proof of lemma 2.

- in real attack $\Pr[\mathcal{H}] \geq 2\epsilon$.
- hence at the end of simulation D appears in some tuple with probability at least 2ϵ.
- hence $\mathcal{B}$ outputs correct answer D to BDH with probability at least $2\epsilon/q_{H_2}$. $\square$

BasicIdent: security proof

The proof of theorem 1 is followed from Lemma 1 and Lemma 2. $\square$

Full IBE scheme FullIdent

- We can convert BasicIdent to IND − ID − CCA secure IBE scheme

- transformation is from [Fujisaki-Okamoto]

Full IBE scheme FullIdent**:**

Setup:

- as in BasicIdent scheme,

- also we pick hash functions $H_3 : \{0,1\}^n \times \{0,1\}^n \to \mathbb{Z}_q^*$ and $H_4 : \{0,1\}^n \to \{0,1\}^n$for some n.

Extract (key-generation): As in BasicIdent scheme.

Full IBE scheme $\mathsf{FullIdent}$**:**

$\mathsf{Encrypt}$: To encrypt message $m \in \{0,1\}^n$ with public key ID:

- compute $Q_{\mathsf{ID}} = H_1(\mathsf{ID})$
- choose a random $\sigma \in \{0,1\}^n$
- set $r = H_3(\sigma, m)$
- compute $g_{\mathsf{ID}} = e(Q_{\mathsf{ID}}, P_{pub})$
- compute $U = rP$, $V = \sigma \oplus H_2(g_{\mathsf{ID}}^r)$, $W = m \oplus H_4(\sigma)$
- set cipher text to be $C = \langle U, V, W \rangle$.

Full IBE scheme FullIdent**:**

Decrypt: To decrypt C using private key d_{ID}:

- if $U \notin G_1^*$reject ciphertext, else:
- compute $V \oplus H_2(e(d_{\mathsf{ID}}, U) = \sigma$
- compute $W \oplus H_4(\sigma) = m$
- set $r = H_3(\sigma, m)$
- test $U = rP$, if not, reject ciphertext.
- if test is succeesful, then m is decrypttion of C.

FullIdent: **security definition**

- FullIdent scheme is IND – ID – CCA secure
- for security proof see [Boneh, Franklin]
- similar to security proof of BasicIdent

Conclusion

- IBE system FullIdent is build from bilinear pairings

- to build the concrete example of IBE, authors use the Weil pairings

- some implementation results available at http://crypto.stanford.edu/ibe/download.html

- security proof of IBE scheme FullIdent is based on random oracle model

- building a chosen ciphertext secure IBE in the standard model and not in random oracle is still an open problem.

References

D.Boneh, M.Franklin, "Identity-based encryption from the Weil pairing", In *Advances in Cryptology - Crypto 2001*, volume 2139 of LNCS, pages 213-229. Springer-Verlag, 2001.

C.Cocks, "An identity-based encryption scheme based on quadratic residues", Eighth IMA International Conference on Cryptography and Coding, Dec. 2001, Royal Agricultural College, Cirencester, UK.

E.Fujisaki, T.Okamoto, "Secure integration of asymmetric and symmetric encryption schemes", in *Advances in Cryptology - Crypto* '99, Lecture Notes in Computer Science, Vol. 1666, Springer-Verlag, pp. 537-554, 1999.