Gentry IBE Paper Reading

Y. Jiang[1]

[1] University of Wollongong

September 5, 2014

Literature

Craig Gentry.
Practical Identity-Based Encryption Without Random Oracles.
Advances in Cryptology - EUROCRYPT 2006, 445-464, 2006.

Outline

1. **Introduction of Identity-Based Encryption**
   - Background
   - Security Model

2. **Gentry IBE**
   - Gentry IBE's Contribution
   - Construction 1: Chosen-Paintext Security
   - Construction 2: Chosen-Ciphertext Security

3. **Conclusion**

UNIVERSITY OF WOLLONGONG

Outline

1 **Introduction of Identity-Based Encryption**
- Background
- Security Model

2 **Gentry IBE**
- Gentry IBE's Contribution
- Construction 1: Chosen-Paintext Security
- Construction 2: Chosen-Ciphertext Security

3 **Conclusion**

UNIVERSITY OF WOLLONGONG

Background of Identity-Based Encryption

Identity-Based Encryption system is a public key encryption system in which a user's public key may be an arbitrary string and the private key is generated by a trusted authority, called a Private Key Generator ($\mathcal{PKG}$), which applies its master key to the user's identity after the user authenticates it self.

Motivation To simplify public key and certificate management.[1]

Features
- disparate public keys → public identities
- public key certificates → eliminated

Definition of Identity-Based Encryption

An identity-based encryption scheme $\mathcal{E}$ is a tuple of four polynomial-time algorithms $(\mathbf{Setup}, \mathbf{Extract}, \mathbf{Encrypt}, \mathbf{Decrypt})$ satisfying the following:

- The *environment set-up algorithm* $\mathbf{Setup}$ takes as input a security parameter 1^k and returns $\mathbf{params}$ (system parameters) and a $\mathbf{master\text{-}key}$.
- The *key generation algorithm* $\mathbf{Extract}$ takes as input an arbitrary ID $\in \{0,1\}^*$ and $\mathbf{master\text{-}key}$, and returns a private key $d_{\mathsf{ID}} \leftarrow \mathsf{Extract}_{\mathsf{master\text{-}key}}(\mathsf{ID})$.

Definition of Identity-Based Encryption

- The encryption algorithm $\mathbf{Enc}$ takes as input an ID and a message $M \in \mathcal{M}$, and returns a ciphertext $C \leftarrow \mathsf{Enc}_{\mathsf{ID}}(M) \in \mathcal{C}$.
- The decryption algorithm $\mathbf{Dec}$ takes a private key d_{ID} and a ciphertext $C \in \mathcal{C}$, and returns $M \leftarrow \mathsf{Dec}_{d_{\mathsf{ID}}}(C) \in \mathcal{M}$.

It is required that

$$\Pr[\mathsf{Dec}_{\mathsf{Extract}_{\mathsf{master\text{-}key}}(\mathsf{ID})}(\mathsf{Enc}_{\mathsf{ID}}(M)) = M]$$

except with possibly negligible probability over master-key output by Setup(1^k), any M in $\mathcal{M}$, any ID $\in \{0,1\}^*$, and any randomness used by Enc and Extract.

Security Model of Identity-Based Encryption

	IND-CCA			IND-ID-CCA		
ST	Challenger KenGen(k) →(pk,sk)	 $\rightarrow$	Adversary pk	Challenger Setup(k) →(params,mk)	 $\rightarrow$	Adversary params
P 1		$\leftarrow$	c_i		$\leftarrow$	ID_i, c_i
	$\mathsf{Dec}_{sk}(c_i)$	$\rightarrow$	m_i	$\mathsf{Dec}_{\mathsf{Extract}}(c_i)$	$\rightarrow$	m_i
					$\leftarrow$	ID_i
				$\mathsf{Extract}_{mk}(\mathsf{ID}_i)$	$\rightarrow$	d_{ID_i}
P C		$\leftarrow$	m_0, m_1		$\leftarrow$	m_0, m_1, ID^*
	$\mathsf{Enc}_{pk}(m_b)$	$\rightarrow$	c^*	$\mathsf{Enc}(m_b, \mathsf{ID}^*)$	$\rightarrow$	c^*
P 2	Same as Phase 1 $c \neq c^*$			Same as Phase 1 $\mathsf{ID} \neq \mathsf{ID}^*, (c, \mathsf{ID}) \neq (c^*, \mathsf{ID}^*)$		
G	$b = b'?$	$\leftarrow$	b'	$b = b'?$	$\leftarrow$	b'

$$\mathsf{AdvIdCCA}_{\mathcal{S}_{\mathsf{IBE}},\mathcal{A}} = |\Pr[c = c'] - \frac{1}{2}|$$

Security Model of Identity-Based Encryption

Definition

An IBE system is $(t, q_{\mathsf{ID}}, q_C, \epsilon)$ IND-ID-CCA secure if all t-time IND-ID-CCA adversaries making at most q_{ID} private key queries and at most q_C chosen ciphertext queries have advantage at most ϵ in winning the above IND-ID-CCA game.

Definition

An IBE system is $(t, q_{\mathsf{ID}}, \epsilon)$ IND-ID-CPA secure if it is $(t, q_{\mathsf{ID}}, 0, \epsilon)$ IND-ID-CCA secure.

Outline

1 **Introduction of Identity-Based Encryption**

- Background
- Security Model

2 **Gentry IBE**

- Gentry IBE's Contribution
- Construction 1: Chosen-Paintext Security
- Construction 2: Chosen-Ciphertext Security

3 **Conclusion**

Gentry IBE's Contribution

- CCA secure without random oracles
- A tight reduction via Cramer-Shoup proof style on a stronger assumption
- Recipient-anonymity

Preliminaries

Bilinear Maps

- $\mathbb{G}$ and $\mathbb{G}_T$ are two multiplicative cyclic groups of prime order p;
- g is a generator of $\mathbb{G}$
- $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a bilinear map.

Properties

- Bilinear: for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
- Non-degenerate: $e(g, g) \neq 1$.

Definition

A group $\mathbb{G}$ is a bilinear group if the group action in $\mathbb{G}$ can be computed efficiently and there exists a group $\mathbb{G}_T$ and an efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ as above.

Reduction Proof

A top-level concept

In the simulation, we pack the hard problem in a fashion that adversary would accept, ask the adversary to do its job and study what the adversary has done.

For a decisional hard problem:

1. If the input of the decisional hard problem is *True*. The adversary should be able to attack with its full advantage if the adversary cannot notice it is a simulation rather than an actual attack.
2. If the input is *False*. The adversary should have no advantage to do its job whatsoever.

Reduction Proof

Now we have three tasks in the proof:

1. To provide the environment and the cryptanalysis training course so that the simulation is polynomially indistinguishable from an actual attack.
2. To encrypt a valid challenge ciphertext with the hard problem embedded so that if the input of hard problem is from random space it would also make the ciphertext into the same distribution so that in the adversary's view the ciphertext is independent of its message.
3. To answer the hard problem with the educated guess from the adversary.

Complexity Assumptions

q-BDHE Given a vector of $2q+1$ elements

$$\left(g', g, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}, g^{(\alpha^{q+2})}, \ldots, g^{(\alpha^{2q})}\right) \in \mathbb{G}^{2q+1}$$

as input, output $e(g, g')^{(\alpha^{q+1})}$.

Decisional q-ABDHE Given a vector of $q+4$ elements

$$\left(g', g'^{(\alpha^{q+2})}, g, g^{\alpha}, g^{(\alpha^2)}, \ldots, g^{(\alpha^q)}, Z\right) \in \mathbb{G}^{q+3} \times \mathbb{G}_T$$

as input, output 1 if $Z = e(g, g')^{(\alpha^{q+1})}$, otherwise output 0.

$*$ From now on, we use g_i and g'_i to denote $g^{(\alpha^i)}$ and $g'^{(\alpha^i)}$.

Construction 1

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map.

Setup generators $g, h \overset{R}{\leftarrow} \mathbb{G}$, $\alpha \overset{R}{\leftarrow} \mathbb{Z}_p$, $g_1 = g^{\alpha} \in \mathbb{G}$, outputs params $= (g, g_1, h)$, master-key $= \alpha$.

Extract(ID) $r_{\mathsf{ID}} \overset{R}{\leftarrow} \mathbb{Z}_p$, $h_{\mathsf{ID}} = (hg^{-r_{\mathsf{ID}}})^{\frac{1}{\alpha - \mathsf{ID}}}$ (ID $\neq \alpha$), outputs $d_{\mathsf{ID}} = (r_{\mathsf{ID}}, h_{\mathsf{ID}})$.

Encrypt(m, ID) $s \overset{R}{\leftarrow} \mathbb{Z}_p$, outputs $C = (g_1^s g^{-s \cdot \mathsf{ID}}, e(g,g)^s, m \cdot e(g,h)^{-s})$.

Decrypt(C, ID) Let $C = (u, v, w)$ with ID, outputs $m = w \cdot e(u, h_{\mathsf{ID}}) v^{r_{\mathsf{ID}}}$.

Reduction Proof for Construction 1 I

Suppose adversary $\mathcal{A}$ $(t', \epsilon', q_{\mathsf{ID}})$-breaks the IND-ID-CPA security of the construction 1, we construct simulator $\mathcal{B}(g', g'_{q+2}, g, g_1, \ldots, g_q, Z)$ where $q = q_{\mathsf{ID}} + 1$.

Setup polynomial $f(x) \overset{R}{\leftarrow} \mathbb{Z}_p[x]$ of degree q, $h = g^{f(\alpha)}$, outputs

$$params = (g, g_1, h).$$

Phase 1 Key query For $\mathsf{ID} \in \mathbb{Z}_p$, $F_{\mathsf{ID}}(x) = \frac{f(x) - f(\mathsf{ID})}{x - \mathsf{ID}}$, outputs

$$d_{\mathsf{ID}} = (r_{\mathsf{ID}}, h_{\mathsf{ID}}) = (f(\mathsf{ID}), g^{F_{\mathsf{ID}}(\alpha)}).$$

Validity: $g^{F_{\mathsf{ID}}(\alpha)} = g^{\frac{f(\alpha) - f(\mathsf{ID})}{\alpha - \mathsf{ID}}} = (hg^{-f(\mathsf{ID})})^{\frac{1}{\alpha - \mathsf{ID}}}$.

Reduction Proof for Construction 1 II

Challenge $\mathcal{A}$ outputs M_0, M_1, ID^*, $\mathcal{B}$ flips a fair coin $c \in \{0,1\}$, computes $d_{\mathsf{ID}^*} = (r_{\mathsf{ID}^*}, h_{\mathsf{ID}^*})$, let $F_{2,\mathsf{ID}^*}(x) = \frac{x^{q+2} - (\mathsf{ID}^*)^{q+2}}{x - \mathsf{ID}^*}$, sets

$$u = g'^{\alpha^{q+2} - (\mathsf{ID}^*)^{q+2}}$$

$$v = Z \cdot e(g', \prod_{i=0}^{q} g_i^{F_{2,\mathsf{ID}^*,i}})$$

$$w = M_c / e(u, h_{\mathsf{ID}^*}) v^{r_{\mathsf{ID}^*}}$$

and outputs the challenge ciphertext $C = (u, v, w)$.

Phase 2 $\mathcal{B}$ responds to queries the same way as in Phase 1.

Guess $\mathcal{A}$ outputs c'. If $c' = c$, $\mathcal{B}$ outputs 1; otherwise outputs 0.

Reduction Proof for Construction 1 III

Now we study the two cases:
Case 1: $Z = e(g_{q+1}, g')$ Goal: $\mathcal{A}$ cannot distinguish it is a simulation.

- The validity of the challenger ciphertext:
  Let $s = (\log_g g')F_{2,\mathsf{ID}^*}(\alpha)$.
  Since $Z = e(g_{q+1}, g')$,

$$
\begin{aligned}
u &= g^{s(\alpha-\mathsf{ID}^*)} = g_1^s g^{-s\cdot\mathsf{ID}} \\
v &= e(g_{q+1}, g')e(g', \prod_{i=0}^{q} g^{F_{2,\mathsf{ID}^*,i}\cdot\alpha^i}) \\
&= e(g', g^{\alpha^{q+1}+(\sum_{i=0}^{q} F_{2,\mathsf{ID}^*,i}\alpha^i)}) \\
&= e(g^{\log_g g'}, g^{F_{2,\mathsf{ID}^*}(\alpha)}) = e(g,g)^s \\
M_c/w &= e(g^{s(\alpha-\mathsf{ID}^*)}, (g^{f(\alpha)}g^{-f(\mathsf{ID}^*)})^{\frac{1}{\alpha-\mathsf{ID}^*}})e(g,g)^{sf(\mathsf{ID}^*)} \\
&= e(g^s, hg^{-f(\mathsf{ID}^*)})e(g^s, g^{f(\mathsf{ID}^*)}) \\
&= e(g,h)^s
\end{aligned}
$$

Reduction Proof for Construction 1 IV

- WARNING! Private key simulation (Different from PKE)
- Question: Could $\mathcal{A}$ distinguish the simulation from private key distribution?
  To prove the private keys issued by $\mathcal{B}$ are appropriately distributed. Let $\mathcal{ID} = \{\mathsf{ID}_1, \ldots, \mathsf{ID}_{q_{\mathsf{ID}}}, \alpha, \mathsf{ID}^*\}$, we have $|\mathcal{ID}| \leq q+1$. Since $f(x)$ is a uniformly random polynomial of degree q, in $\mathcal{A}$'s view private keys $d_{\mathsf{ID}} = (r_{\mathsf{ID}}, h_{\mathsf{ID}}), r_{\mathsf{ID}} = f(\mathsf{ID}), h_{\mathsf{ID}} = (hg^{-r_{\mathsf{ID}}})^{\frac{1}{\alpha - \mathsf{ID}}}$ are uniformly random and independent.

Reduction Proof for Construction 1 V

Case 2: Z is uniformly random

Goal: c is independent in $\mathcal{A}$'s view whatsoever.

Z is uniformly random $\Rightarrow (u, v)$ is uniformly random and independent $\Rightarrow v \neq e(u, g)^{\frac{1}{\alpha - \mathsf{ID}^*}}$ holds with $1 - 1/p$.

On the other hand, r_{ID^*} is uniformly random and independent in $\mathcal{A}$'s view

Therefore, $M_c/w = e(u, h_{\mathsf{ID}^*})v^{r_{\mathsf{ID}^*}} = e(u, h)^{\alpha - \mathsf{ID}^*}(\frac{v}{e(u,g)^{\frac{1}{\alpha - \mathsf{ID}^*}}})^{r_{\mathsf{ID}^*}}$ is uniformly random and independent in $\mathcal{A}$'s view

To summarize, $\mathcal{B}$ would have ϵ' advantage to solve the hard problem except with negligible probability.

□

Construction 2

Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p, and let $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ be the bilinear map.

Setup generators $g, h_1, h_2, h_3 \overset{R}{\leftarrow} \mathbb{G}$, $\alpha \overset{R}{\leftarrow} \mathbb{Z}_p, g_1 = g^\alpha \in \mathbb{G}$, a collision-resistant hash function H, outputs
params $= (g, g_1, h_1, h_2, h_3, H)$, master-key $= \alpha$.

Extract(ID) For $i = 1, 2, 3$, $r_{\mathsf{ID},i} \overset{R}{\leftarrow} \mathbb{Z}_p$, $h_{\mathsf{ID},i} = (hg^{-r_{\mathsf{ID},i}})^{\frac{1}{\alpha - \mathsf{ID}}}$
(ID $\neq \alpha$), outputs
$d_{\mathsf{ID}} = \{(r_{\mathsf{ID},i}, h_{\mathsf{ID},i}) : i \in \{1, 2, 3\}\}$.

Encrypt(M, ID) $s \overset{R}{\leftarrow} \mathbb{Z}_p, u = g_1^s g^{-s \cdot \mathsf{ID}}, v = e(g, g)^s$,
$w = m \cdot e(g, h_1)^{-s}, \beta = H(u, v, w)$,
$y = e(g, h_2)^s e(g, h_3)^{s\beta}$, outputs $C = (u, v, w, y)$.

Decrypt(C, ID) Let $C = (u, v, w, y)$. $\beta = H(u, v, w)$ and tests
$y \overset{?}{=} e(u, h_{\mathsf{ID},2} h_{\mathsf{ID},3}^{\beta}) v^{r_{\mathsf{ID},2} + r_{\mathsf{ID},3}\beta}$.
Yes, $m = w \cdot e(u, h_{\mathsf{ID},1}) v^{r_{\mathsf{ID},1}}$
Otherwise the recipient outputs $\perp$.

Reduction Proof for Construction 2 I

Suppose adversary $\mathcal{A}$ $(t', \epsilon', q_{\mathsf{ID}}, q_C)$-breaks the IND-ID-CCA security of the construction 2, we construct simulator $\mathcal{B}(g', g'_{q+2}, g, g_1, \ldots, g_q, Z)$ where $q = q_{\mathsf{ID}} + 2$.

Setup Three random polynomials $f_i(x) \overset{R}{\leftarrow} \mathbb{Z}_p[x]$ of degree q for $i = 1, 2, 3$, computes $h_i = g^{f_i(\alpha)}$ and outputs

$$params = (g, g_1, h_1, h_2, h_3).$$

Phase 1 [Private key queries]
For ID $\in \mathbb{Z}_p$, $\mathcal{B}$ uses $f_i(x)$ to generate $\{(r_{\mathsf{ID},i}, h_{\mathsf{ID},i}) : i = 1, 2, 3\}$ as before so that $(r_{\mathsf{ID},i}, h_{\mathsf{ID},i}) = (f_i(\mathsf{ID}), g^{F_{i,\mathsf{ID}}(\alpha)})$.
[Decryption queries]
For (C, ID), $\mathcal{B}$ check the data-integrity, generates a private key for ID as above and decrypts it.

Reduction Proof for Construction 2 II

Challenge After $\mathcal{A}$ outputs M_0, M_1, ID^*, $\mathcal{B}$ flips a fair coin $c \in \{0,1\}$, computes $d_{\mathsf{ID}^*} = \{(r_{\mathsf{ID}^*,i}, h_{\mathsf{ID}^*,i}) : i = 1,2,3\}$, (u,v,w) using $(r_{\mathsf{ID}^*,1}, h_{\mathsf{ID}^*,1})$, $\beta = H(u,v,w)$, $y = e(u, h_{\mathsf{ID},2} h_{\mathsf{ID},3}^{\beta}) v^{r_{\mathsf{ID},2} + r_{\mathsf{ID},3}\beta}$, outputs $C = (u,v,w,y)$.

Phase 2 $\mathcal{B}$ responds to queries the same way as in Phase 1.

Guess $\mathcal{A}$ outputs c'. If $c' = c$, $\mathcal{B}$ outputs 1; otherwise outputs 0.

Then we consider the two cases:
Case 1: $Z = e(g_{q+1}, g')$ Goal: $\mathcal{A}$ cannot distinguish it is a simulation.

- Key generation simulation is good as before.
- Decryption simulation Goal: Reject all invalid ciphertext
- Question: Have we leaked any information so that $\mathcal{A}$ could use to generate an invalid ciphertext that would pass the data-integrity check?

Reduction Proof for Construction 2 III

- What $\mathcal{A}$ wants to do: to make (u', v', w', y') for a not queried ID where $v' \neq e(u', g)^{\frac{1}{\alpha - \mathsf{ID}}}$ valid.
- $\mathcal{A}$ needs to find

$$a_{y'} = a_{u'}(\log_g h_{\mathsf{ID},2} + \beta' \log_g h_{\mathsf{ID},3}) + a_{v'}(r_{\mathsf{ID},2} + \beta' r_{\mathsf{ID},3}) \qquad (1)$$

where $a_{u'} = \log_g u', a_{y'} = \log_{e(g,g)} y', a_{v'} \log_{e(g,g)} v'$.
From the construction of the private key:

$$\log_g h_2 = (\alpha - \mathsf{ID}) \log_g h_{\mathsf{ID},2} + r_{\mathsf{ID},2} \qquad (2)$$

$$\log_g h_3 = (\alpha - \mathsf{ID}) \log_g h_{\mathsf{ID},3} + r_{\mathsf{ID},3} \qquad (3)$$

Then Equation (1) changes to:

$$a_{y'} = (\frac{a_{u'}}{\alpha - \mathsf{ID}})(\log_g h_2 + \beta' \log_g h_3) + (a_{v'} - \frac{a_{u'}}{\alpha - \mathsf{ID}})(r_{\mathsf{ID},2} + \beta' r_{\mathsf{ID},3}) \qquad (4)$$

Reduction Proof for Construction 2 IV

- WARNING! $r_{\mathsf{ID},i} = f_i(\mathsf{ID})$
  $\mathcal{A}$'s learning from $r_{\mathsf{ID}_1,2}, \ldots, r_{\mathsf{ID}_{q-2},2}, h_2, r_{\mathsf{ID}_1,3}, \cdots, r_{\mathsf{ID}_{q-2},3}, h_3$.

$$\underset{\mathbf{f}}{[\lambda_0^{(2)}, \lambda_1^{(2)}, \ldots, \lambda_q^{(2)}, \lambda_0^{(3)}, \lambda_1^{(3)}, \ldots, \lambda_q^{(3)}]} \underset{V}{\begin{bmatrix} 1 & 1 & \cdots & 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ \mathsf{ID}_1 & \mathsf{ID}_2 & \cdots & \mathsf{ID}_{q-2} & \alpha & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \mathsf{ID}_1^q & \mathsf{ID}_2^q & \cdots & \mathsf{ID}_{q-2}^q & \alpha^q & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & \mathsf{ID}_1 & \mathsf{ID}_2 & \cdots & \mathsf{ID}_{q-2} & \alpha \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \mathsf{ID}_1^q & \mathsf{ID}_2^q & \cdots & \mathsf{ID}_{q-2}^q & \alpha^q \end{bmatrix}}$$

$$a_{y'} = (\frac{a_{u'}}{\alpha - \mathsf{ID}})(\log_g h_2 + \beta' \log_g h_3) + (a_{v'} - \frac{a_{u'}}{\alpha - \mathsf{ID}})(\mathbf{f} \cdot \boldsymbol{\gamma}_{\mathsf{ID}} \| \beta' \boldsymbol{\gamma}_{\mathsf{ID}}) \tag{5}$$

where $\boldsymbol{\gamma}_{\mathsf{ID}} = (1, \mathsf{ID}, \ldots, \mathsf{ID}^q)$.

- SAFE! $\boldsymbol{\gamma}_{\mathsf{ID}} \| \beta' \boldsymbol{\gamma}_{\mathsf{ID}}$ is linear independent of V.
  $\mathcal{A}$ finds such a y' with negligible probability.

Reduction Proof for Construction 2 V

Case 2: Z is uniformly random.
Goal: c is independent in $\mathcal{A}$'s view whatsoever.
$\Rightarrow$ Unbounded computational power of $\mathcal{A}$.
From the challenge ciphertext$\psi = (u, v, w, y)$ for ID*:

$$\log_{e(g,g)}(M_c/w) = \frac{a_u}{\alpha - \mathsf{ID}^*} \log_g h_1 + (a_v - \frac{a_u}{\alpha - \mathsf{ID}^*}) r_{\mathsf{ID}^*,1} \qquad (6)$$

c should be independent in $\mathcal{A}$'s view as discussed in Construction 1.

- WARNING! the independence of $r_{\mathsf{ID}^*,1}$ is no longer guaranteed.
- Question: Is it possible for $\mathcal{A}$ to generate related invalid ciphertext which could pass the data-integrity so that it would be numerically decrypted?

Reduction Proof for Construction 2 VI

If $\mathcal{A}$ queries an invalid ciphertext $\psi' = (u', v', w', y')$ for unqueried identity ID, where $(u', v', w', y', \mathsf{ID}) \neq (u, v, w, y, \mathsf{ID}^*)$ and $\beta' = H(u', v', w')$.

There are three cases to consider:

1. $(u', v', w') = (u, v, w)$: Hashes are equal as well.
   - ID = ID* $y' \neq y$, reject.
   - ID ≠ ID* $\mathcal{A}$ must find a y' that satisfies Equation (5), but $\boldsymbol{\gamma}_{\mathsf{ID}} \| \beta \boldsymbol{\gamma}_{\mathsf{ID}}$ is independent of $[V_1, \ldots, V_{2q-2}, \boldsymbol{\gamma}_{\mathsf{ID}^*} \| \beta \boldsymbol{\gamma}_{\mathsf{ID}^*}]$.
2. $(u', v', w') \neq (u, v, w)$ and $\beta = \beta'$: Hash function!?
3. $(u', v', w') \neq (u, v, w)$ and $\beta \neq \beta'$:
   - ID ≠ ID* Negligible probability for essentially the same reason as Item 1.
   - ID = ID* Then $\boldsymbol{\gamma}_{\mathsf{ID}} \| \beta \boldsymbol{\gamma}_{\mathsf{ID}}$ and $\boldsymbol{\gamma}_{\mathsf{ID}} \| \beta' \boldsymbol{\gamma}_{\mathsf{ID}}$ are linearly independent to each other and the columns of V.

Reduction Proof for Construction 2 VII

- SAFE! No information about $r_{\mathsf{ID}^*,1}$ is leaked. c is independent in $\mathcal{A}$'s view.

Therefore, CCA Secure ✓. $\mathcal{B}$ would have ϵ' advantage to solve the hard problem except with negligible probability.

□

Outline

1. **Introduction of Identity-Based Encryption**
   - Background
   - Security Model

2. **Gentry IBE**
   - Gentry IBE's Contribution
   - Construction 1: Chosen-Paintext Security
   - Construction 2: Chosen-Ciphertext Security

3. **Conclusion**

Conclusion

- Guarded decryption! Data-integrity check with message information and extra random augments
- Add redundancy against more powerful attacks
- For CPA secure, one thing different in IBE system is it needs to prove the key generation simulation.
- For CCA secure, Cramer-Shoup security proof technique is very useful, but it needs thoroughness and carefulness.

Bibliography I

Adi Shamir.
Identity-based cryptosystems and signature schemes.
In GeorgeRobert Blakley and David Chaum, editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer Berlin Heidelberg, 1985.

Thankyou.