Efficient Ciphertext Policy Attribute Based Encryption Under Decisional Linear Assumption

PhD Candidate: Tran Viet Xuan Phuong

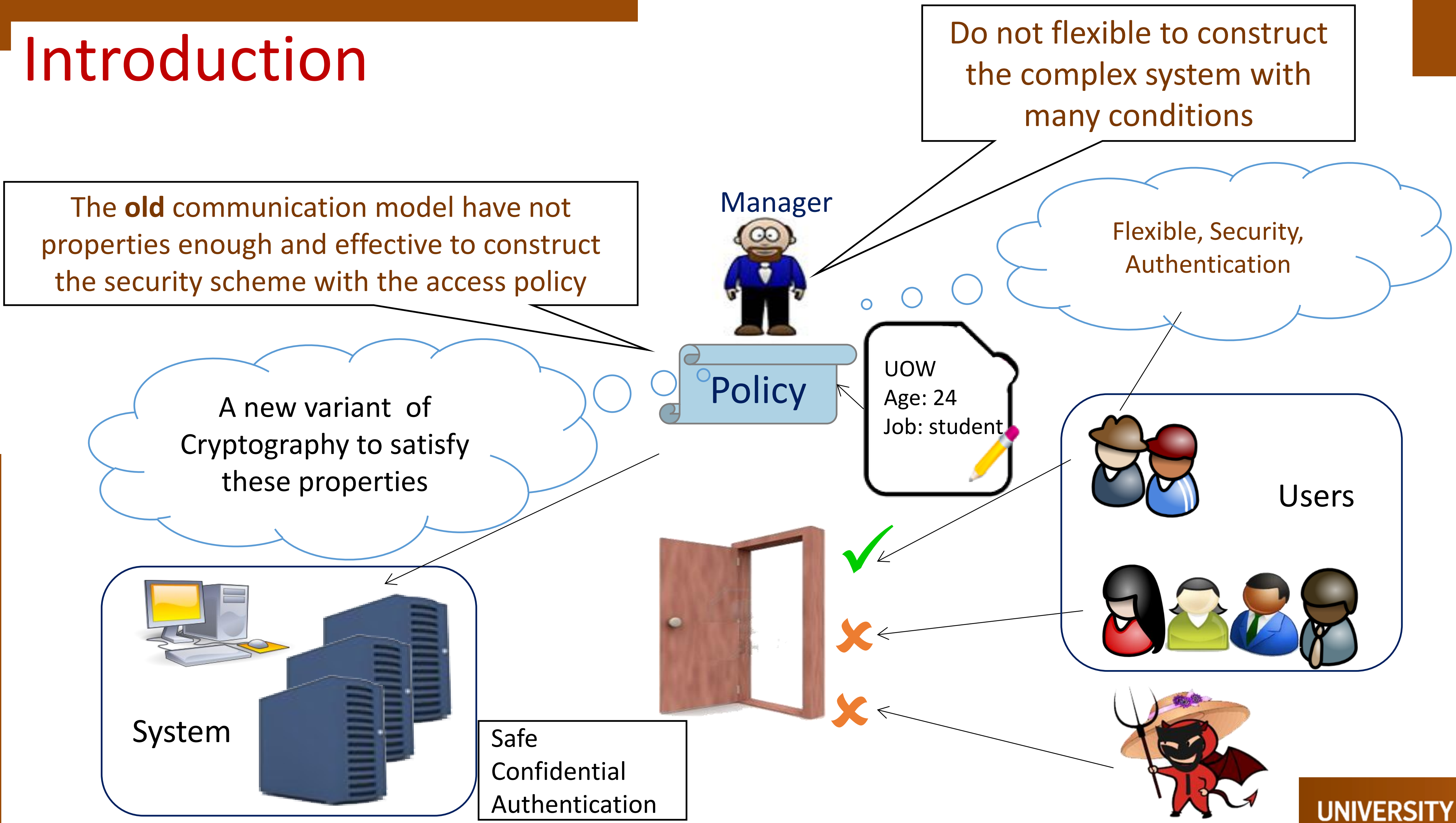
Supervision: Prof. Willy Susilo

Dr. Guomin Yang

Content

- Introduction
- Previous work
- Contribution
- Preliminaries
- Construction
- Conclusion

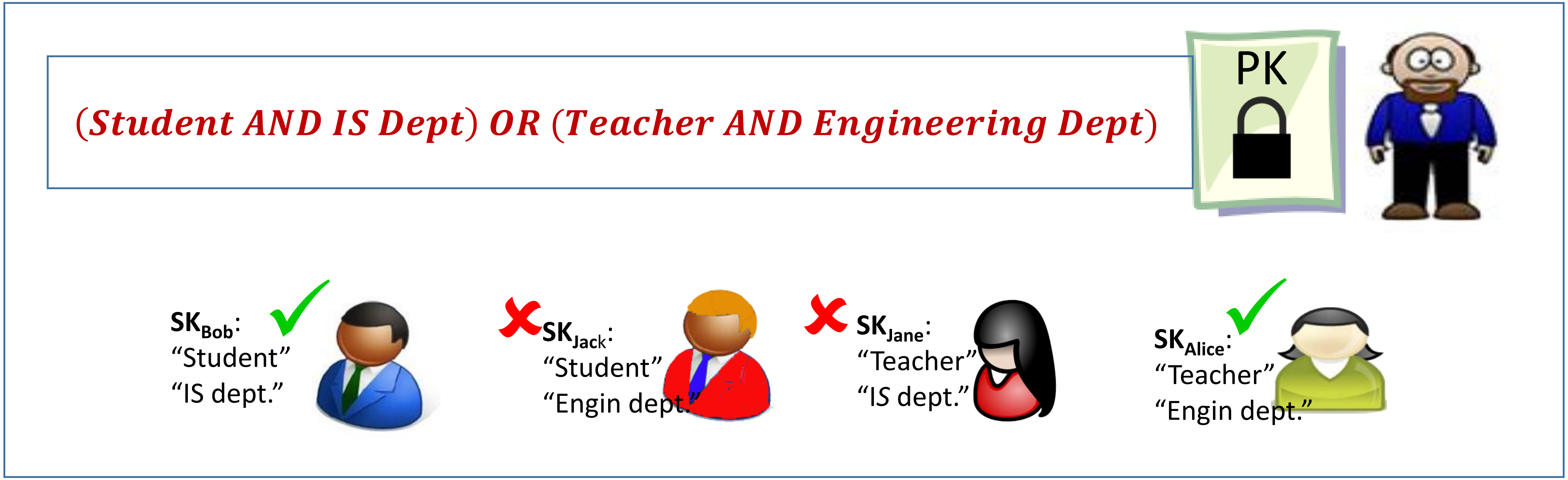
Introduction



Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [1]

An encryptor makes a ciphertext associated with an **access structure** W(***policy***).

A decryptor with a **set of attribute** S can decrypt a ciphertext if S **satisfies** W



[1] Bethencourt, John and Sahai, Amit and Waters, Brent Ciphertext-Policy Attribute-Based Encryption, IEEE Symposium on Security and Privacy, 2007.

Previous Work

- Most current CP-ABE schemes incur large ciphertext size and encryption/decryption operations
  - The length size depends on the number of attributes

	Encryption	Decryption	CTLength	Policy	Assumption
CN(CSS 2007)	$(n+2)\mathbf{ex}$	$(n+1)\mathbf{p}$	$\lvert\mathbb{G}_T\rvert+(n+1)\lvert\mathbb{G}\rvert$	Non-monotone AND gate	DBDH
BW(PKC, 2011)	$(2t+2)\mathbf{ex}$	$(2t+1)\mathbf{p}$	$\lvert\mathbb{G}_T\rvert+(2t+1)\lvert\mathbb{G}\rvert$	Linear Structure	n-BDHE
EM(IPSEC 2009)	$(\boldsymbol{t}+\mathbf{2})\mathbf{ex}$	$\mathbf{2p}+\mathbf{2ex}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	**Monotone(n,n) thresold scheme**	**DBDH**
ZH (CSS 2010)	$\mathbf{2ex}$	$\mathbf{2}\boldsymbol{tp}+\mathbf{1}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	**Non-monotone AND gate**	**n-DBDE**
HLR (PKC, 2010)	$(\boldsymbol{n}+\boldsymbol{t}+\mathbf{1})\mathbf{ex}$	$\mathbf{3p}+(\boldsymbol{t}^{\mathbf{2}})\mathbf{ex}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	**Monotone(n,n) thresold scheme**	**aMSE-BDH**
CZD(ProvSec 2011)	$\mathbf{3ex}$	$\mathbf{2p}$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	**Non-monotone AND gate**	**n-DBHE**

EM(IPSEC 2009)	$(t+2)$ex	$2p+2ex$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	Monotone(n,n) thresold scheme	DBDH

EM09 which admits only (n,n)-threshold policies

ZH (CSS 2010)	2ex	$2tp+1$	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	Non-monotone AND gate	n-DBDE

ZH10 using non-monotone AND gate access structure, but the cost of decryption depends on the number of attributes

HLR (PKC, 2010)	$(n+t+1)$ ex	$3p+(t^2)$ex	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	Monotone(n,n) thresold scheme	aMSE-BDH

HLR10 (t,n) threshold structure, but both the cost of encryption and decryption depend on the number of attributes

CZD(ProvSec 2011)	3ex	2p	$\lvert\mathbb{G}_T\rvert+2\lvert\mathbb{G}\rvert$	Non-monotone AND gate	n-DBDE

CZD11 Short ciphertext but applying n-BDHE is not a standard assumption to satisfy the security of PKC scheme compare with DBDH assumption

Contribution

- Proposed an efficient CP-ABE Scheme:
  - Constant ciphertext length with short size.
  - Constant computation costs.
  - Using non-monotone AND gates with wildcards to construct access structure.
  - Apply the standard assumption in security proof.

Preliminaries

Bilinear Map

p : $prime\ number$
$\mathbb{G}, \mathbb{G}_T$: groups with order p

A bilinear map $\boldsymbol{e}$: $\mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$

Bilinearity

For all $g \in \mathbb{G}, a, b \in \mathbb{Z}_p$,
$e(g^a, g^b) = e(g, g)^{ab}$

Non-degeneracy

$\mathrm{e}(g, g) \neq 1.$

Desicional Linear Assumption (DLIN)

Definition 1: *We say that the decisional Linear assumption holds if no polynomial time algorithm has a non-negligible advantage in solving the DLIN problem.*

$g, g^a, g^b, g^{ac}, g^d, T \in \mathbb{G}^6$

distinguish

$\boldsymbol{T} = \boldsymbol{g}^{\boldsymbol{b}(\boldsymbol{c}+\boldsymbol{d})}$

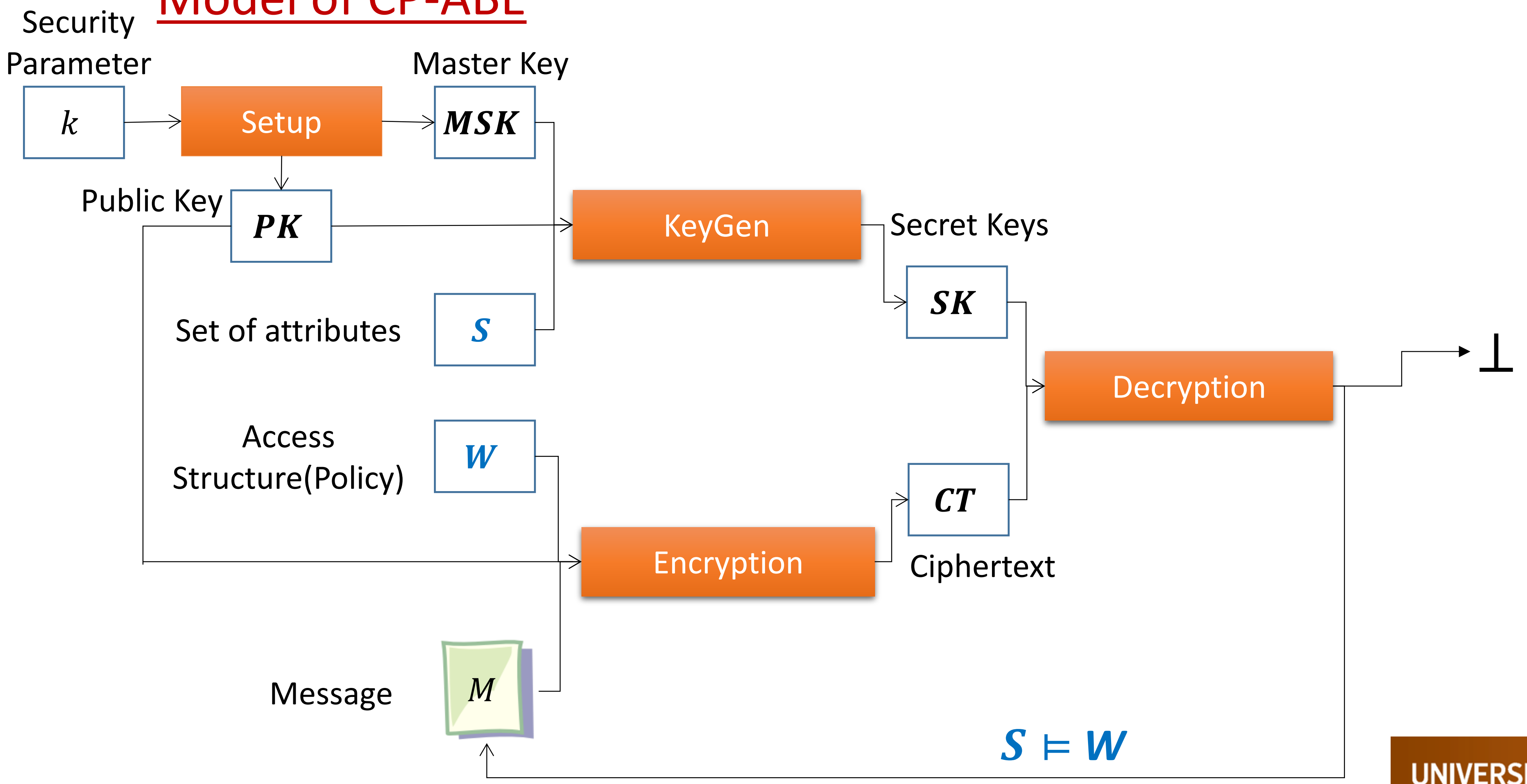
$\boldsymbol{T} \in \mathbb{G}$ (random element)

$\mathcal{B}$: polynomial time algorithm
$a, b, c, d, r \in_R \mathbb{Z}_p, \epsilon(k)$: negligible in security parameter k

$$\left|\mathbf{Pr}\left[\boldsymbol{\mathcal{B}}\left(\boldsymbol{g}, \boldsymbol{g}^{\boldsymbol{a}}, \boldsymbol{g}^{\boldsymbol{b}}, \boldsymbol{g}^{\boldsymbol{ac}}, \boldsymbol{g}^{\boldsymbol{d}}, \boldsymbol{T} = \boldsymbol{g}^{\boldsymbol{b}(\boldsymbol{c}+\boldsymbol{d})}\right) = \mathbf{1}\right] - \boldsymbol{Pr}\left[\boldsymbol{\mathcal{B}}\left(\boldsymbol{g}, \boldsymbol{g}^{\boldsymbol{a}}, \boldsymbol{g}^{\boldsymbol{b}}, \boldsymbol{g}^{\boldsymbol{ac}}, \boldsymbol{g}^{\boldsymbol{d}}, \boldsymbol{T} = \boldsymbol{r}\right)\right]\right| \leq \boldsymbol{\epsilon}(\boldsymbol{k})$$

Preliminaries

Model of CP-ABE



Preliminaries

AND gate structure with wildcards

Let $U = \{A_1, A_2, \dots, A_k\}$ be the Universe of attributes

Let $W = \{A_1, A_2, \dots, A_k\}$ be and AND-gate access policy.

Old expression

	Att_1	Att_2	Att_3	Att_4
Positive	A_1	A_2	A_3	A_4
Negative	A_5	A_6	A_7	A_8
Wildcard	A_9	A_{10}	A_{11}	A_{12}

Attributes	Att_1	Att_2	Att_3	Att_4
Description	CS	EE	Faculty	Student
Alice	+	−	−	+
Bob	−	+	+	−
Carol	+	+	+	−
W_1	+	−	−	+
W_2	+	−	*	*

Alice is a student in the CS department;

Bob is a faculty in the EE department;

Carol is a faculty holding a joint position in the EE and CS department

W_1 can be satisfied by all the CS students,
W_2 can be satisfied by all CS people.

Preliminaries

Viète's formulas

$$\vec{w} = (w_1, w_2, *, .., *, w_L)$$
$$\vec{z} = (z_1, z_2, \dots, z_L)$$

$J = \{j_1, j_2, .., j_n\} \subset \{1, \dots, L\}$ positions wildcard in $\vec{w}$

$w_i = z_i \vee w_i = *$ for $i = 1, \dots, L$ $\longrightarrow$ $\sum_{i=1, i \notin J}^{L} w_i \prod_{j \in J} (i-j) = \sum_{i=1}^{L} z_i \prod_{j \in J} (i-j)$

$\prod_{j \in J} (i-j) = \sum_{k=0}^{n} \lambda_k i^k$, λ_k coefficients of J $\longrightarrow$ $\sum_{i=1, i \notin J}^{L} w_i \prod_{j \in J} (i-j) = \sum_{k=0}^{n} \lambda_k \sum_{i=1}^{L} z_i i^k$

Hiding computation, $H_i \in_R G$ $\longrightarrow$ $\prod_{i=1, i \notin J}^{L} H_i^{w_i \prod_{j \in J}(i-j)} = \prod_{k=0}^{n} \left(\prod_{i=1,}^{L} H_i^{z_i i^k} \right)^{\lambda_k}$

Using Viète formulas, construct λ_k: $\lambda_k = (-1)^k \sum_{1 \le i_1 < i_2 < \cdots < i_k \le n} j_{i_1} j_{i_2} \dots j_{i_k}, 0 \le k \le n$

Construction

Setup(1^k)

Assume that we have L attributes in the universe, and each attribute has two possible values: positive and negative.
In addition, we also consider wildcard (meaning ``don't care'') in access structures.

Let N_1, N_2, N_3 be three upper bounds defined as follows:

- $N_1 \leq L$: the maximum number of wildcard in an access structure;
- $N_2 \leq L$: the maximum number of positive attribute in an attribute set S;
- $N_3 \leq L$: the maximum number of negative attribute in an attribute set S.

--Generates bilinear groups $\mathbb{G}, \mathbb{G}_T$ with order p,
--Selects two random generators $V_0, V_1, g \in \mathbb{G}$.
--Randomly choose $\alpha, \beta_1, \beta_2, a_1, \ldots, a_L \in_R \mathbb{Z}_p$,
-> Set $\boxed{\Omega_1 = e(g, V_0)^{\alpha\beta_1} e(g, V_1)^{\alpha\beta_1}, \Omega_2 = e(g, V_0)^{\alpha\beta_2} e(g, V_1)^{\alpha\beta_2}}$.
---Let $A_i = g^{a_i}$ for $i = 1, \ldots, L$.

$$\textbf{PK} = (e, g, \Omega_1, \Omega_2, g^{\alpha}, V_0, V_1, \boxed{A_1, \ldots, A_L})$$

$$\textbf{MSK} = (\alpha, \beta_1, \beta_2, a_1, \ldots, a_L)$$

Encryption(W, M,PK)

Suppose that the access structure W contains:

- $n_1 \leq N_1$ wildcards which occur at positions $J = \{w_1, \dots, w_{n_1}\}$;
- $n_2 \leq N_2$ positive attributes which occur at positions $V = \{v_1, \dots, v_{n_2}\}$;
- $n_3 \leq N_3$ negative attributes which occur at positions $Z = \{z_1, \dots, z_{n_3}\}$.

$$\lambda_k = (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} j_{i_1} j_{i_2} \dots j_{i_k}, 0 \leq k \leq n$$

Compute for the wildcard positions $\{w_j\}(j = 0, 1, 2, \cdots, n_1)\{\lambda_{w_j}\}$ and set $t_w = \sum_{j=0}^{n_1} \lambda_{w_j}$.

The encryption algorithm then chooses $r_1, r_2 \in_R \mathbb{Z}_p$, and create ciphertext as:

$$C_0 = M\, \Omega_1^{r_1} \Omega_2^{r_2}, \qquad C_1 = g^{\frac{a_1 r_1}{t_w}}, \qquad C_2 = g^{\frac{r_2}{t_w}},$$

$$\boxed{C_3 = \left(V_0 \prod_{i \in V} A_i^{\frac{\prod_{j=0}^{n_1}(i - w_j)}{t_w}}\right)^{r_1 + r_2}, C_4 = \left(V_0 \prod_{i \in Z} A_i^{\frac{\prod_{j=0}^{n_1}(i - w_j)}{t_w}}\right)^{r_1 + r_2}}$$

$$\textbf{CT} = (C_0, C_1, C_2, C_3, C_4, J = \{w_1, w_2, \dots, w_{n_1}\})$$

KeyGen(MSK, S)

Suppose that a user joins the system with the attribute list L, which contains:

- $n'_2 \leq N_2$ positive attributes which occur at positions $V' = \{v'_1, \dots, v'_{n'_2}\}$.
- $n'_3 \leq N_3$ negative attributes which occur at positions $Z' = \{z'_1, \dots, z'_{n'_3}\}$.

By means of the Viète's formulas,

- for all the positive positions $\{v'_k\}$ $(k = 0, 1, 2, \cdots, n'_2)$, calculate $\{\lambda_{v'_k}\}$ and set $t'_v = \sum_{k=0}^{n_2} \lambda_{v'_k}$;
- for all the negative positions $\{z'_\tau\}$ $(\tau = 0, 1, 2, \cdots, n'_3)$, calculate $\{\lambda_{z'_\tau}\}$\$ and set $t'_z = \sum_{\tau=0}^{n_3} \lambda_{z'_\tau}$.

Chooses $s \in_R \mathbb{Z}_p$ and computes $s_1 = \beta_1 + s$, $s_2 = \beta_2 + s$\$ and creates the secret key as:

$$L_1 = g^{\frac{\alpha s}{t'_v}}, \qquad L_2 = g^{\frac{\alpha s}{t'_z}},$$

$$K_1 = \{K_{1,0}, K_{1,1}, \dots, K_{1,N_1}\} = \{V_0^{s_1} \prod_{i \in V'} g^{s\, a_i}, V_0^{s_1} \prod_{i \in V'} g^{s\, a_i i}, \dots, V_0^{s_1} \prod_{i \in V'} g^{s\, a_i i^{N_1}}\}$$

$$K'_1 = \{K'_{1,0}, K'_{1,1}, \dots, K'_{1,N_1}\} = \{V_0^{\alpha s_2} \prod_{i \in V'} g^{s\alpha\, a_i}, V_0^{\alpha s_2} \prod_{i \in V'} g^{s\alpha\, a_i i}, \dots, V_0^{\alpha s_2} \prod_{i \in V'} g^{s\, \alpha a_i i^{N_1}}\}$$

$$K_2 = \{K_{2,0}, K_{2,1}, \dots, K_{2,N_1}\} = \{V_0^{s_1} \prod_{i \in Z'} g^{s\, a_i}, V_0^{s_1} \prod_{i \in Z'} g^{s\, a_i i}, \dots, V_0^{s_1} \prod_{i \in Z'} g^{s\, a_i i^{N_1}}\}$$

$$K'_2 = \{K'_{2,0}, K'_{2,1}, \dots, K'_{2,N_1}\} = \{V_0^{\alpha s_2} \prod_{i \in Z'} g^{s\alpha\, a_i}, V_0^{\alpha s_2} \prod_{i \in Z'} g^{s\alpha\, a_i i}, \dots, V_0^{\alpha s_2} \prod_{i \in Z'} g^{s\, \alpha a_i i^{N_1}}\}$$

SK = $(S, L_1, L_2, K_1, K'_1, K_2, K'_2)$

Decryption (SK,CT)

The algorithm first identifies the wildcard positions in $J = \{w_1, \ldots, w_{n_1}\}$ and computes $\{\lambda_{w_j}\}$. Then it returns:

$$M = \frac{e(L_1, C_3)^{t'_v} \cdot e(L_2, C_4)^{t'_z}}{e(\prod_{j=0}^{n_1} K_{1,j}^{\lambda_{w_j}}, C_1) \cdot e(\prod_{j=0}^{n_1} (K'_{1,j})^{\lambda_{w_j}}, C_2) \cdot e(\prod_{j=0}^{n_1} K_{2,j}^{\lambda_{w_j}}, C_1) \cdot e(\prod_{j=0}^{n_1} (K'_{2,j})^{\lambda_{w_j}}, C_2)} \cdot C_0.$$

$$\frac{e(L_1, C_3)^{t'_v} \cdot e(L_2, C_4)^{t'_z}}{e(\prod_{j=0}^{n_1} K_{1,j}^{\lambda_{w_j}}, C_1) \cdot e(\prod_{j=0}^{n_1} (K'_{1,j})^{\lambda_{w_j}}, C_2) \cdot e(\prod_{j=0}^{n_1} K_{2,j}^{\lambda_{w_j}}, C_1) \cdot e(\prod_{j=0}^{n_1} (K'_{2,j})^{\lambda_{w_j}}, C_2)} M\ \Omega_1^{r_1} \Omega_2^{r_2}$$

$$= e(g, V_0)^{-\alpha\beta_1 r_1} e(g, V_0)^{-\alpha\beta_2 r_2} e(g, V_1)^{-\alpha\beta_1 r_1} e(g, V_1)^{-\alpha\beta_2 r_2}\ M\ \Omega_1^{r_1} \Omega_2^{r_2}$$

$$= \Omega_1^{-r_1} \Omega_2^{-r_2}\ M\ \Omega_1^{r_1} \Omega_2^{r_2}$$

Security Proof

CPA Game for CP-ABE

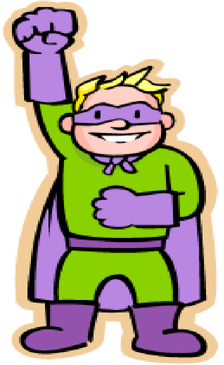
- Attacker $\mathcal{A}$ can fix the access structure W before joining system
- $\mathcal{A}$ can not get the secret key with the list of attributes not satisfy W

- Init : The attacker $\mathcal{A}$ send the access structure W the challenger.
- Setup: The challenger runs the algorithm $\mathcal{B}$, and sent PK to $\mathcal{A}$.
- Phase 1: $\mathcal{A}$ makes repeated private keys SK_i correponding to set of attributes $S \subseteq U$, with $S \nvDash W$ condition.
- Challenge :
  - $\mathcal{A}$ submits two equal length messages M_0 and M_1 to challenger.
  - The challenger chooses a random $\mu \in \{0,1\}$, and encrypts $CT^* = \left(PK, M_\mu, W\right)$ and sent back to $\mathcal{A}$.
- Phase 2 : Phase 1 repeated
- Guess : $\mathcal{A}$ outputs a guess $\mu' \in \{0,1\}$

$$Adv(\mathcal{A}) = |\Pr(\mu' = \mu) - \frac{1}{2}|$$

CPA Security Game for CP-ABE

Init


Simulator

the access structure $W^* = [W_1^*, \dots, W_L^*]$

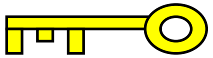

Attacker

$n_1 \leq N_1$ wildcards which occur at positions $J = \{w_1, \dots, w_{n_1}\}$;
$n_2 \leq N_2$ positive attributes which occur at positions $V = \{v_1, \dots, v_{n_2}\}$;
$n_3 \leq N_3$ negative attributes which occur at positions $Z = \{z_1, \dots, z_{n_3}\}$.

CPA Security Game for CP-ABE

Setup

Public Params



PK = $(e, g, \Omega_1, \Omega_2, g^{\alpha}, V_0, V_1, A_1, \dots, A_L)$

Selects $\sigma_1, \sigma_2, \sigma_3 \in_R \mathbb{Z}_p, \gamma_0, \gamma_1, \{a_i'\}_{\{1 \le i \le L\}} \in \mathbb{Z}_p$, using Viete formulas $\left\{\lambda_{w_j}\right\}_{\{w_j \in J\}}$.

and sets $t_w = \sum_{i=0}^{n_1} \lambda_{w_i}$. Then calculates:

$$V_0 = (g^b)^{\gamma_0} g^{-\sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i - w_j)}{t_w}}, V_1 = (g^b)^{\gamma_1} g^{-\sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i - w_j)}{t_w}}.$$

$$A_i = g^{a_i} = \begin{cases} g^{a_i'}, & att_i = W_i^* \\ g^{\frac{a_i'}{\sum_{att_m \in W_i^*} a_m' \prod_{j=1}^{n_1}(m - w_j)}}, & att_i \neq W_i^* \end{cases}$$

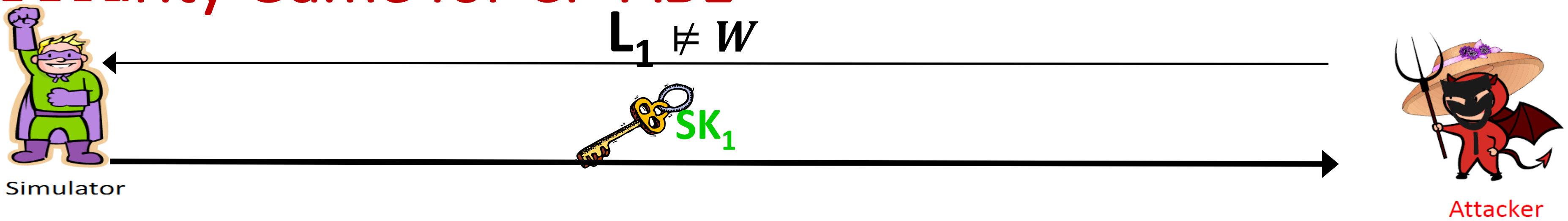
$$\Omega_1 = e(g^a, V_0)^{\sigma_1 - \sigma_2} e(g^a, V_1)^{\sigma_1 - \sigma_2}$$

$$\Omega_2 = e(g^{\sigma_3}(g^a)^{-\sigma_2}, V_0) e(g^{\sigma_3}(g^a)^{-\sigma_2}, V_1).$$

$$MSK = (\alpha = a, \beta_1 = \sigma_1 - \sigma_2, \beta_2 = \frac{\sigma_3}{a} - \sigma_2, a_1, \dots, a_L)$$

CPA Security Game for CP-ABE

Phase 1



Suppose that a user joins the system with the attribute list L, which contains:

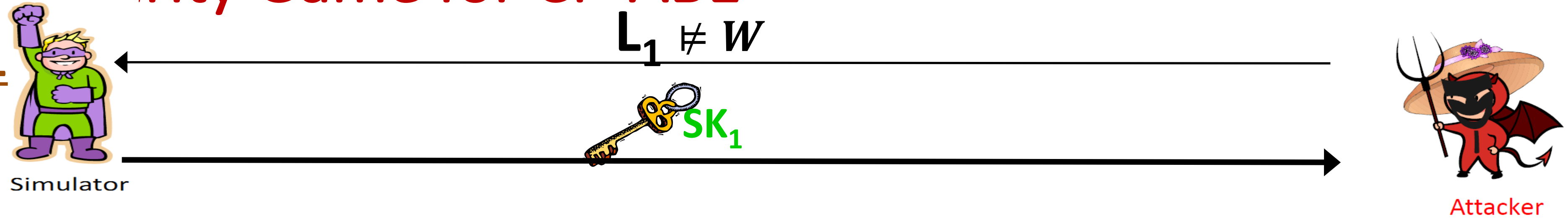
- $n_2' \leq N_2$ positive attributes which occur at positions $V' = \{v_1', \ldots, v_{n_2'}'\}$.
- $n_3' \leq N_3$ negative attributes which occur at positions $Z' = \{z_1', \ldots, z_{n_3'}'\}$.

By means of the Viète's formulas,

- for all the positive positions $\{v_k'\}\,(k = 0, 1,2, \cdots, n_2')$, calculate $\{\lambda_{v_k'}\}$ and set $t_v' = \sum_{k=0}^{n_2} \lambda_{v_k'}$;
- for all the negative positions $\{z_\tau'\}\,(\tau = 0, 1,2, \cdots, n_3')$, calculate $\{\lambda_{z_\tau'}\}$\$ and set $t_z' = \sum_{\tau=0}^{n_3'} \lambda_{z_\tau'}$.

CPA Security Game for CP-ABE

Phase 1



$$L_1 = (g^a)^{\frac{\sigma_2}{t'_v}}, L_2 = (g^a)^{\frac{\sigma_2}{t'_z}},$$

$$K_1 = \{K_{1,0}, K_{1,1}, \ldots, K_{1,N_1}\}$$

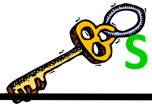
$$\{V_0^{\sigma_1} \prod_{att_i \in W^*, i \in V} g^{\sigma_2 a'_i} \prod_{att_i \notin W^*, i \in V} g^{\frac{\sigma_2 a'_i}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}, V_0^{\sigma_1} \prod_{att_i \in W^*, i \in V} g^{\sigma_2 a'_i i} \prod_{att_i \notin W^*, i \in V} g^{\frac{\sigma_2 a'_i i}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}$$

$$, \ldots, V_0^{\sigma_1} \prod_{att_i \in W^*, i \in V} g^{\sigma_2 a'_i i^{N_1}} \prod_{att_i \notin W^*, i \in V} g^{\frac{\sigma_2 a'_i i^{N_1}}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}\}$$

CPA Security Game for CP-ABE

Phase 1

$\mathbf{L_1} \nvDash W$



SK_1

$$K'_1 = \{K'_{1,0}, K'_{1,1}, \dots, K'_{1,N_1}\}$$

$$\{(g^b)^{\sigma_3\gamma_0} g^{-\sigma_3 \frac{\sum_{att_i\in W_i^*, i\in V} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i\in W^*, i\in V} (g^a)^{\sigma_2 a'_i} \cdot \prod_{att_i\notin W^*, i\in V} (g^a)^{\frac{\sigma_2 a'_i}{\sum_{att_m\in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}},$$

$$(g^b)^{\sigma_3\gamma_0} g^{-\sigma_3 \frac{\sum_{att_i\in W_i^*, i\in V} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i\in W^*, i\in V} (g^a)^{\sigma_2 a'_i i} \cdot \prod_{att_i\notin W^*, i\in V} (g^a)^{\frac{\sigma_2 a'_i i}{\sum_{att_m\in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}},$$

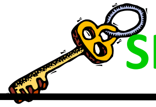
$$\dots,$$

$$(g^b)^{\sigma_3\gamma_0} g^{-\sigma_3 \frac{\sum_{att_i\in W_i^*, i\in V} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i\in W^*, i\in V} (g^a)^{\sigma_2 a'_i i^{N_1}} \cdot \prod_{att_i\notin W^*, i\in V} (g^a)^{\frac{\sigma_2 a'_i i^{N_1}}{\sum_{att_m\in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}\},$$

CPA Security Game for CP-ABE

Phase 1

$\mathbf{L_1} \nvDash W$



$$K_2 = \{K_{2,0}, K_{2,1}, \ldots, K_{2,N_1}\}$$

$$\{V_1^{\sigma_1} \prod_{att_i \in W^*, i \in Z} g^{\sigma_2 a'_i} \prod_{att_i \notin W^*, i \in Z} \frac{\sigma_2 a'_i}{g^{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}, V_1^{\sigma_1} \prod_{att_i \in W^*, i \in Z} g^{\sigma_2 a'_i i} \prod_{att_i \notin W^*, i \in Z} \frac{\sigma_2 a'_i i}{g^{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}$$

$$, \ldots, V_1^{\sigma_1} \prod_{att_i \in W^*, i \in Z} g^{\sigma_2 a'_i i^{N_1}} \prod_{att_i \notin W^*, i \in Z} \frac{\sigma_2 a'_i i^{N_1}}{g^{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}\}$$

CPA Security Game for CP-ABE

Phase 1

$$K'_2 = \{K'_{2,0}, K'_{2,1}, \ldots, K'_{2,N_1}\}$$

$$\{(g^b)^{\sigma_3\gamma_1} g^{-\sigma_3 \frac{\sum_{att_i \in W_i^*, i\in Z} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i \in W^*, i \in Z} (g^a)^{\sigma_2 a'_i} \cdot \prod_{att_i \notin W^*, i \in Z} (g^a)^{\frac{\sigma_2 a'_i}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}},$$

$$(g^b)^{\sigma_3\gamma_1} g^{-\sigma_3 \frac{\sum_{att_i \in W_i^*, i\in Z} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i \in W^*, i \in Z} (g^a)^{\sigma_2 a'_i i} \cdot \prod_{att_i \notin W^*, i \in Z} (g^a)^{\frac{\sigma_2 a'_i i}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}},$$

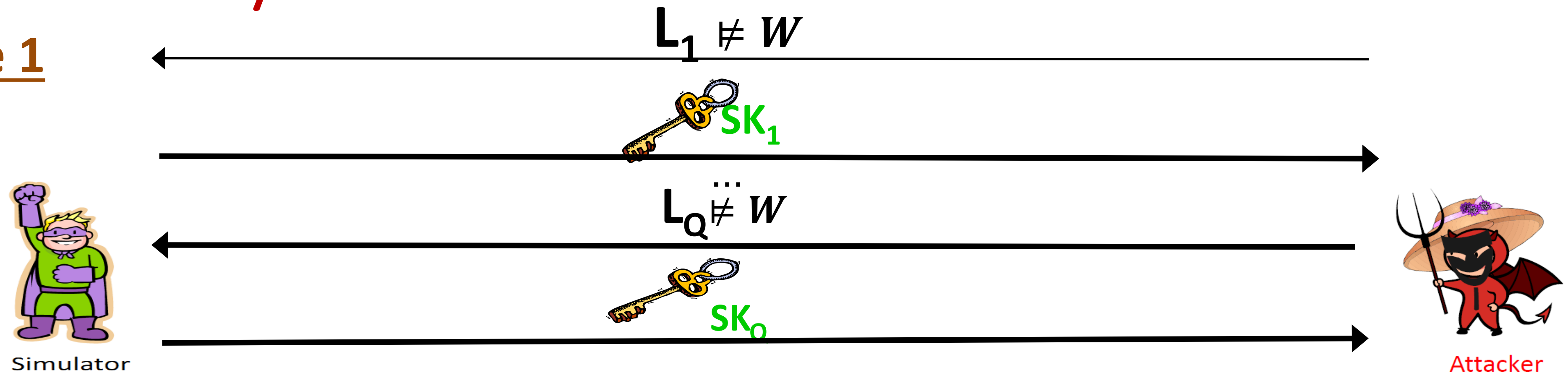
$$\ldots,$$

$$(g^b)^{\sigma_3\gamma_1} g^{-\sigma_3 \frac{\sum_{att_i \in W_i^*, i\in Z} a'_i \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \prod_{att_i \in W^*, i \in Z} (g^a)^{\sigma_2 a'_i i^{N_1}} \cdot \prod_{att_i \notin W^*, i \in Z} (g^a)^{\frac{\sigma_2 a'_i i^{N_1}}{\sum_{att_m \in W^*} a'_m \prod_{j=1}^{n_1}(m-w_j)}}\},$$

Implicitly sets $s = \sigma_2$

CPA Security Game for CP-ABE

Phase 1



CPA Security Game for CP-ABE

Challenge

Simulator

M_0, M_1, $|M_0| = |M_1|$

b Enc$(W, C_b, C_1, C_2, C_3, C_4)$

Attacker

$$
\begin{aligned}
C_0 = {} & M_\nu e(g^{ac}, g^b)^{\sigma_1\gamma_0} \cdot e(g^{ac}, g)^{(\sigma_1-\sigma_2)\sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, g^d)^{\sigma_2 \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^b, g^d)^{\sigma_3\gamma_0} \\
& \cdot e(g^{ac}, g^b)^{\sigma_1\gamma_1} \cdot e(g^{ac}, g)^{(\sigma_1-\sigma_2)\sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, g^d)^{\sigma_2 \sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^b, g^d)^{\sigma_3\gamma_1} \\
& \cdot e(g^d, g)^{\sigma_3 \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, T_\nu)^{\sigma_2\gamma_0} \cdot e(g^d, g)^{\sigma_3 \sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} \cdot e(g^a, T_\nu)^{\sigma_2\gamma_1},
\end{aligned}
$$

$$C_1 = (g^{ac})^{\frac{1}{t_w}}, C_2 = (g^d)^{\frac{1}{t_w}},$$

CPA Security Game for CP-ABE

Challenge

Simulator

M_0, M_1, $|M_0| = |M_1|$

Enc($\boldsymbol{W}, \boldsymbol{C_b}, \boldsymbol{C_1}, \boldsymbol{C_2}, \boldsymbol{C_3}, \boldsymbol{C_4}$)

Attacker

$$C_3 = (V_0 \prod_{i \in V} (A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1+r_2} = ((g^b)^{\gamma_0} g^{-\sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} g^{\sum_{att_i \in W_i^*, i \in V} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}})^{c+d} = T_\nu^{\gamma_0},$$

$$C_4 = (V_1 \prod_{i \in Z} (A_i^{\frac{\prod_{j=0}^{n_1}(i-w_j)}{t_w}})^{r_1+r_2} = ((g^b)^{\gamma_1} g^{-\sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}} g^{\sum_{att_i \in W_i^*, i \in Z} \frac{a_i' \prod_{j=1}^{n_1}(i-w_j)}{t_w}})^{c+d} = T_\nu^{\gamma_1},$$

Implicitly sets: $r_1 = c, r_2 = d$

CPA Security Game for CP-ABE

Guess

Simulator

Guess b of b’

Attacker

If $T = g^{b(c+d)}$, the simulator B gives a perfect simulation so we have:

$$\mathbf{Pr}\left[\mathcal{B}\left(g, g^{a}, g^{b}, g^{ac}, g^{d}, T = g^{b(c+d)}\right) = 1 \middle|\, T = g^{b(c+d)}\right] = \frac{1}{2} + Adv_{A}(k)$$

If T is a random group element the message M_b is completely hidden from the adversary and we have:

$$\mathbf{Pr}\left[\mathcal{B}\left(g, g^{a}, g^{b}, g^{ac}, g^{d}, T\right) = 1 \middle|\, T = g^{r}\right] = \frac{1}{2}$$

B can solve DLIN with non-negligible advantage if $Adv_A(k)$ is non-negligible

Comparison

Comparison among CP-ABE

Scheme	Ciphertext Length	Dec Cost	Wildcard	Assumption
CN[3]	$\lvert G_T\rvert + (t+1)\lvert G\rvert$	$(t+1)$p	√	DBDH
NYO[8]	$\lvert G_T\rvert + (2t+1)\lvert G\rvert$	$(2t+1)$p	√	DBDH + DLIN
Emura et al.[4]	$\lvert G_T\rvert + 2\lvert G\rvert$	2p	X	DBDH
ZH[12]	$\lvert G_T\rvert + 2\lvert G\rvert$	$2t$p + 1	√	n-BDHE
CZF[2]	$\lvert G_T\rvert + 2\lvert G\rvert$	2p	X	n-BDHE
DZCCZ12[5]	$\lvert G_T\rvert + 2\lvert G\rvert$	2p	X	n-BDHE
Our Scheme	$\lvert G_T\rvert + 4\lvert G\rvert$	6p	√	DLIN

UNIVERSITY OF WOLLONGONG

Conclusion

- In first proposal:
  - A constant-size ciphertext policy attribute based encryption scheme for the AND-Gates with wildcards access structure.
  - Proved the selective security of our scheme under the Decision Linear assumption.

Thank you
Q&A

References

[2] C. Chen, Z. Zhang, and D. Feng. Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost. In 5th ProvSec, pages 84–101, 2011.

[3] L. Cheung and C. Newport. Provably secure ciphertext policy abe. In 14th ACM CCS 2007, pages 456–465.

[4] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi. A ciphertext-policy attribute-based encryption scheme with constant ciphertext length. In 5th ISPEC, pages 13–23, 2009.

[5] A. Ge, R. Zhang, C. Chen, C. Ma, and Z. Zhang. In Information Security and Privacy, pages 336–349, 2012.

[8] T. Nishide, K. Yoneyama, and K. Ohta. Attribute-based encryption with partially hidden encryptor-specified access structures. In 6th ACNS 2008, pages 111–129.

[12] Z. Zhou and D. Huang. On efficient ciphertext-policy attribute based encryption and broadcast encryption extended abstract. In 17th ACM CCS 2010, pages 753–755.