Attribute based data sharing with attribute revocation

Shucheng Yu，Cong Wang，Kui Ren，Wenjing Lou

ASIA CCS ‘10: 5th ACM Symposium on Information, Computer and Communications Security 2010

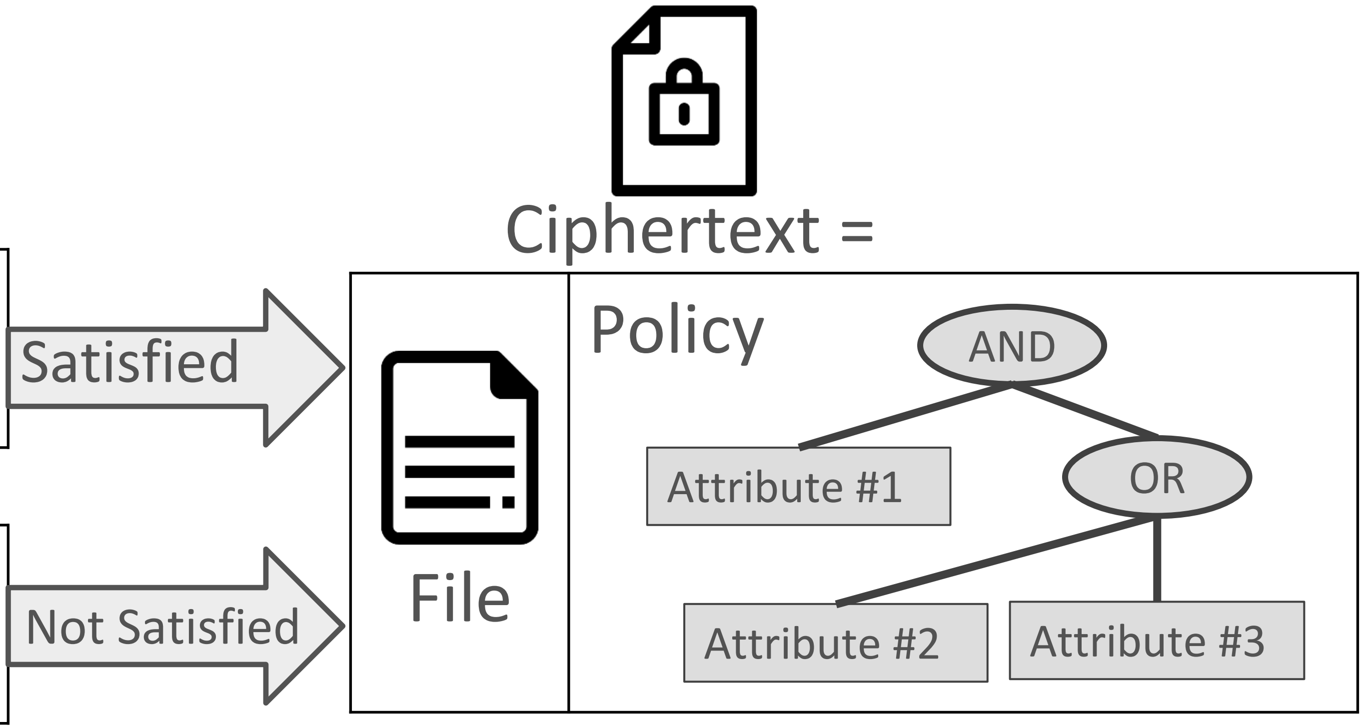
Outline

- Introduction
- System Model
- Proposed Scheme
- Security Analysis

Introduction

CP-ABE

User A	Attribute #1, Attribute #3
User B	Attribute #2, Attribute #3



CP-ABE with Attribute Revocation

2006

each attribute with expiration date

2007

secret key with expiration date

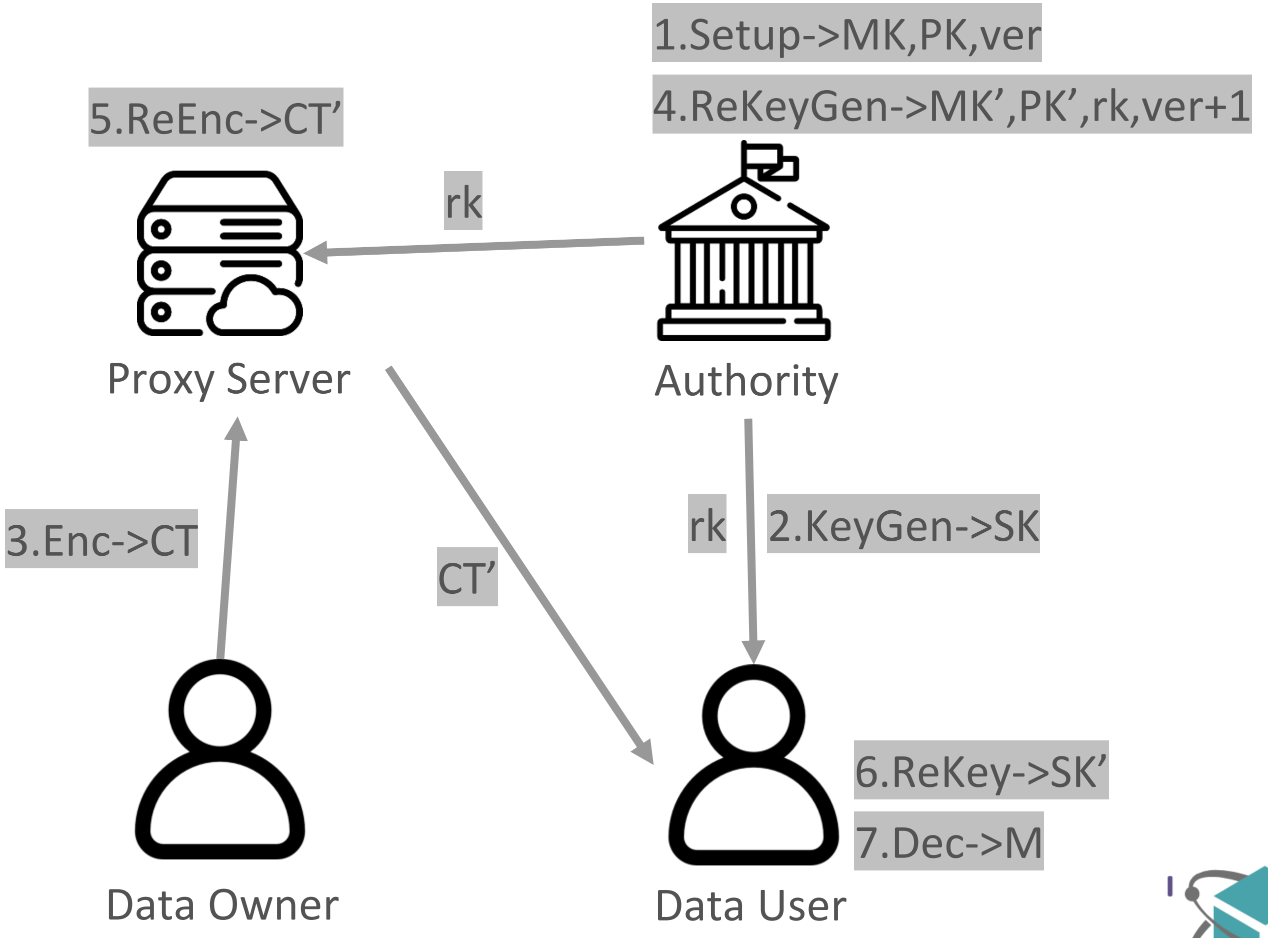
2010

re-encrypt ciphertext

System Model

System Model

- Authority
  - Setup
  - KeyGen
  - ReKeyGen
- Proxy server
  - ReEnc
- Data Owner
  - Enc
- Data User
  - Dec
  - Rekey



Proposed Scheme

Proposed Scheme

- Setup
- KeyGen
- Enc
- ReKeyGen
- ReEnc
- Rekey
- Dec

ICCSLab@NSYSU

Setup

(p, G_0, G_1, g, e) $\quad e: G_0 \times G_0 \rightarrow G_1$

Attribute universe $U = \{1,2,\ldots,n\}$

- Setup(1^{λ}) -> $\{MK, PK, ver$=1$\}$

  Random: $y, t_1, \ldots, t_{3n} \in Z_p$

  Public key: $PK = \{e, g, Y = e(g,g)^y,\ T_1 = g^{t_1}, \ldots, T_{3n} = g^{t_{3n}}\}$

  Master key: $MK = \{y, t_1, \ldots, t_{3n}\}$

$i \in U$	i=1	i=2	…	i=n	
positive part	t_1	t_2	…	t_n	
negative part	t_{n+1}	t_{n+2}	…	t_{2n}	
don't cared part	t_{2n+1}	t_{2n+2}	…	t_{3n}	

KeyGen

- KeyGen(MK, S) -> SK

Random: $r_i \in Z_p$, $i \in U$ $\qquad r = \Sigma_{i=1}^{n} r_i$

Secret key: $SK = \left\{ver, S, D = g^{y-r}, \bar{D} = \left\{D_i, F_i = g^{\frac{r_i}{t_{2n+1}}}\right\}_{i \in U}\right\}$

$$\begin{cases} D_i = g^{\frac{r_i}{t_i}} \text{ ,if } i \in S \\ D_i = g^{\frac{r_i}{t_{n+i}}} \text{ ,otherwise} \end{cases}$$

Encrypt

- Enc(M, AS, PK) -> CT

Single AND gate $AS = \wedge_{\tilde{i} \in I} \tilde{i}$
$M \in G_1$

Random: $s \in Z_p$

$$CT = \{ver, AS, \tilde{C} = MY^s, \hat{C} = g^s, \{C_i\}_{i \in U}\}$$

$$\begin{cases} C_i = T_i^s = g^{t_i s}, \text{ if } i \in I \text{ and } \tilde{i} = +i & \text{positive part} \\ C_i = T_{n+i}^s = g^{t_{n+i} s}, \text{ if } i \in I \text{ and } \tilde{i} = -i & \text{negative part} \\ C_i = T_{2n+i}^s = g^{t_{2n+i} s}, \text{ if } i \notin I & \text{don't cared part} \end{cases}$$

Update

- ReKeyGen(γ, MK) -> re-key,ver+1

Random: $t_i' \in Z_p$, $i \in U, \gamma \subseteq \{1, \dots, 2n\}$

$$\begin{cases} rk_i = \frac{t_i'}{t_i} \text{ ,if } i \in \gamma \\ rk_i = 1 \text{ ,if } i \in \{1, \dots, 2n\} \text{ and } i \notin \gamma \end{cases}$$

Proxy re-key $rk = \{ver, \{rk_i\}_{1 \le i \le 2n}\}$

Update

- ReEnc($CT_{ver}, rk_{ver}, \beta$) -> CT'
  - If $ver_{CT} \neq ver_{rk}$ ->not change
  - Else -> $i \in U, \beta \subseteq \{1, \dots, 2n\}$

$$\begin{cases} C_i' = C_i^{rk_i}, \text{ if } i \in \beta \text{ and } 1 \le i \le n & \text{positive part} \\ C_{i-n}' = (C_{i-n})^{rk_i}, \text{ if } i \in \beta \text{ and } n < i \le 2n & \text{negative part} \\ C_i' = C_i \text{ , if } (i \notin \beta \text{ and } i+n \notin \beta) \text{ or } (i \notin I) & \text{don't cared part} \end{cases}$$

$$CT' = \{ver + 1, AS, \tilde{C}, \hat{C}, \{C_i'\}_{i \in U}\}$$

Update

- ReKey(SK, rk_{ver}, θ) -> SK'

$i \in U, \theta \subseteq \{1, \dots, 2n\}$

$$\begin{cases} D_i' = D_i^{{rk_i}^{-1}}, \text{ if } i \in \theta \text{ and } 1 \leq i \leq n & \text{positive part} \\ D_{i-n}' = (D_{i-n})^{{rk_i}^{-1}}, \text{ if } i \in \theta \text{ and } n < i \leq 2n & \text{negative part} \\ D_i' = D_i \text{ , if } i \notin \theta \text{ and } i + n \notin \theta & \text{don't cared part} \end{cases}$$

$$SK' = \{ver + 1, S, D = g^{y-r}, \bar{D}' = \{D_i', F_i\}_{i \in U}\}$$

Decrypt

- Dec(CT,PK,Sk) -> M
  - If $ver_{CT} \neq ver_{PK}$ or $ver_{CT} \neq ver_{Sk} \rightarrow$ failed
  - Else $->$ $i \in U$ $\quad AS = \wedge_{\tilde{\imath} \in I}\ \tilde{\imath}$

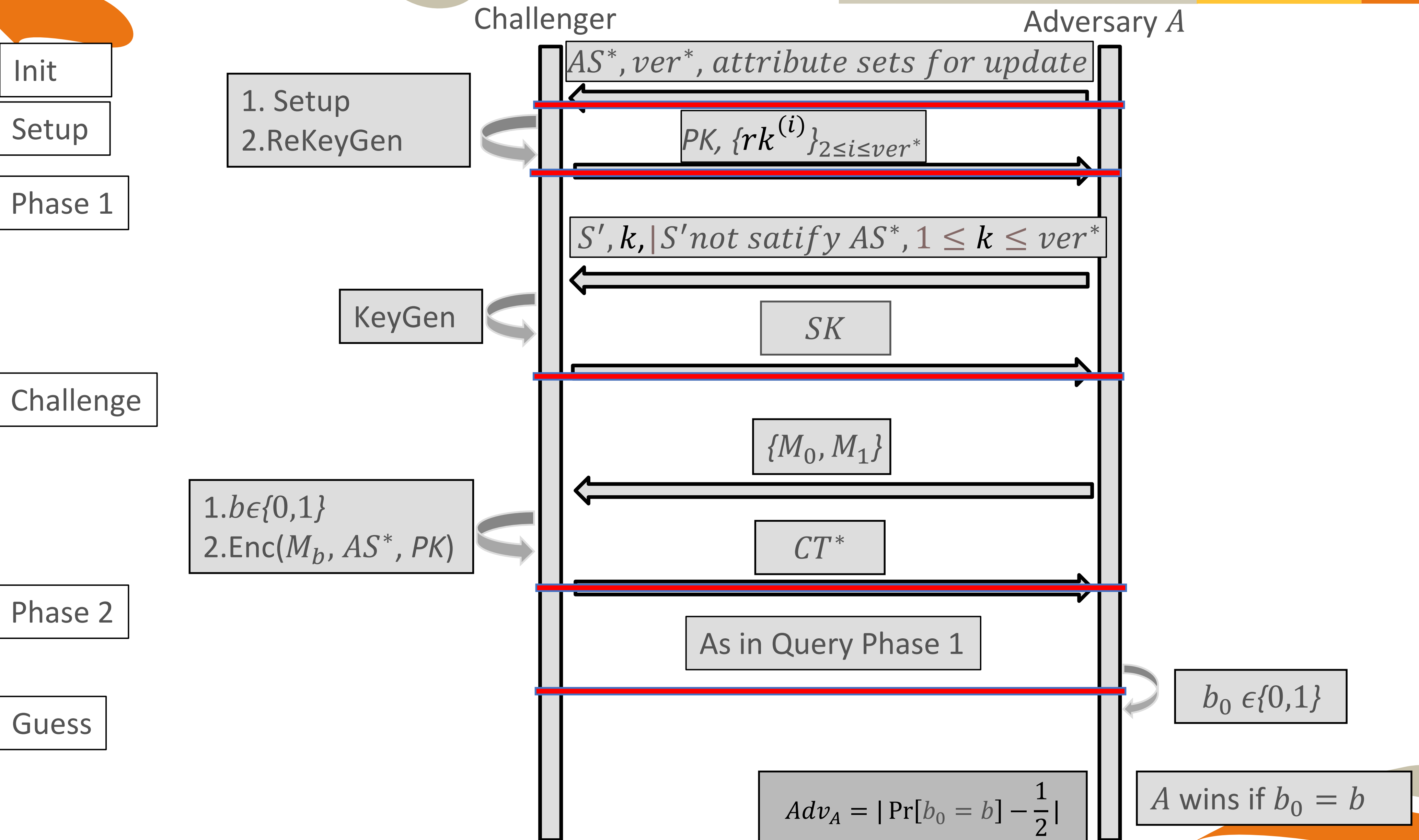
$$\begin{cases} e(C_i, D_i) = e\left(g^{t_i s}, g^{\frac{r_i}{t_i}}\right) = e(g,g)^{r_i s}, \text{ if } \tilde{\imath} \in I \,\&\, \tilde{\imath} = +i \,\&\, i \in S & \text{positive part} \\ e(C_i, D_i) = e\left(g^{t_{n+i} s}, g^{\frac{r_i}{t_{n+i}}}\right) = e(g,g)^{r_i s}, \text{ if } \tilde{\imath} \in I \,\&\, \tilde{\imath} = -i \,\&\, i \notin S & \text{negative part} \\ e(C_i, F_i) = e\left(g^{t_{2n+i} s}, g^{\frac{r_i}{t_{2n+i}}}\right) = e(g,g)^{r_i s}, \text{ if } \tilde{\imath} \notin I & \text{don't cared part} \end{cases}$$

$$\frac{\tilde{C}}{e(\hat{C},D)\prod_{i=1}^{n} e(C_i,D_i)} = \frac{Me(g,g)^{ys}}{e(g,g)^{s(y-r)}\prod_{i=1}^{n} e(g,g)^{r_i s}} =$$

$$\frac{Me(g,g)^{ys}}{e(g,g)^{(ys-rs)}\prod_{i=1}^{n} e(g,g)^{r_i s}} = \frac{Me(g,g)^{ys}}{e(g,g)^{(ys-rs)} e(g,g)^{rs}} = M$$

Security Analysis

Security Model



Security Analysis

- CPA Security Game
- Theorem 1.

  If a PPT algorithm (the adversary A) wins our CPA security game with non-negligible advantage ADV_{CPA}, we can use this algorithm to construct another PPT algorithm B to solve the DBDH problem with advantage $\frac{1}{2}ADV_{CPA}$.

- Proof: $a, b, c \in Z_p$ $\mu \in \{0,1\}$

$$\begin{cases} z = abc \; if \; \mu = 0 \\ z \in Z_p \; if \; \mu = 1 \end{cases}$$

The challenger $\xrightarrow{\{\mathrm{A, B, C, Z}\} = \{g^a, g^b, g^c, e(g,g)^z\}}$ algorithm B $\xleftrightarrow{\text{interact}}$ Adversary A

ICCSLab@NSYSU

Security Analysis

- Init by A

A selects $\{AS^* = \wedge_{\tilde{i} \in I}\ \tilde{i}, ver^*, attribute\ sets: \{\gamma^{(1)}, \gamma^{(2)}, \ldots, \gamma^{(ver^*-1)}\}\}$ -> B

- Setup by B

Random: $\delta_i, \zeta_i, \eta_i \in Z_p$, $i \in$U

$$\begin{cases} T_i = g^{\delta_i}, T_{n+i} = B^{\zeta_i}, T_{2n+i} = B^{\eta_i}, \text{ if } \tilde{i} \in I \text{ and } \tilde{i} = +i & \text{positive part} \\ T_i = B^{\delta_i}, T_{n+i} = g^{\zeta_i}, T_{2n+i} = B^{\eta_i}, \text{ if } \tilde{i} \in I \text{ and } \tilde{i} = -i & \text{negative part} \\ T_i = B^{\delta_i}, T_{n+i} = B^{\zeta_i}, T_{2n+i} = g^{\eta_i}, \text{ if } \tilde{i} \notin I & \text{don't cared part} \end{cases}$$

$1 \leq k \leq ver^*$-1 $\qquad 1 \leq j \leq 2n$

$$\begin{cases} rk_j^{(k)} \in Z_p \text{, if } j \in \gamma^{(k)} \\ rk_j^{(k)} = 1\text{, if } j \notin \gamma^{(k)} \end{cases} \qquad T_j^{(k+1)} = (T_j^{(k)})^{rk_j^{(k)}}$$

$rk^{(k)} = \{k, rk_1^{(k)}, rk_2^{(k)}, \ldots, rk_{2n}^{(k)}\}$ -> A

Security Analysis

$SK = \{ver, S, D, \overline{D} = \{D_i, F_i\}_{i\in U}\}$

- Phase 1

$\{S, k, | \ S \subseteq U, S \ not \ satify \ AS^*, 1 \leq k \leq ver^*\}$ ->B

Random: $r_j' \in Z_p$, $j \in U$

A witness attribute i $\in I$,i $\notin$S, $\tilde{i} = +i$

$$\begin{cases} r_j = r_j'.b \text{ ,if } j \neq i \\ r_j = ab + r_j'.b \text{ ,else} \end{cases}$$

$$r = \Sigma_{j\in U} r_j = ab + \Sigma_{j\in U} r_j'.b$$

$$D = \prod_{j=1}^{n} B^{-r_j'} = g^{-\Sigma_{j=1}^{n} r_j'.b} = g^{ab-r}$$

$$T_j^{(k)} = (T_j^{(1)})^{rk_j^{(2)}.rk_j^{(3)}.\dots.rk_j^{(k)}} = (T_j^{(1)})^{\prod_{i=2}^{k} rk_j^{(i)}}$$

$$T_{n+j}^{(k)} = (T_{n+j}^{(1)})^{rk_{n+j}^{(2)}.rk_{n+j}^{(3)}.\dots.rk_{n+j}^{(k)}} = (T_{n+j}^{(1)})^{\prod_{i=2}^{k} rk_{n+j}^{(i)}}$$

$$R_j^{(k)} = \prod_{i=2}^{k} rk_j^{(i)}$$

$$R_{n+j}^{(k)} = \prod_{i=2}^{k} rk_{n+j}^{(i)}$$

ICCSLab@NSYSU

Security Analysis

$SK = \{ver, S, D, \overline{D} = \{D_i, F_i\}_{i \in U}\}$

- Phase 1

For each $j \in U$ *and* j ≠ i

$$
\begin{cases}
D_j = B^{\frac{r_j'}{\delta_j . R_j^{(k)}}} = g^{\frac{r_j}{\delta_j . R_j^{(k)}}}, \text{If } j \in S,\ j \in I, \tilde{j} = +j \\
D_j = B^{\frac{r_j'}{\delta_j . R_j^{(k)}}} = g^{\frac{r_j}{\delta_j . R_j^{(k)} . b}}, \text{If } j \in S,\ (j \in I, \tilde{j} = -j) \text{ or } j \notin I \\
D_j = g^{\frac{r_j'}{\zeta_j . R_{n+j}^{(k)}}} = g^{\frac{r_j}{\zeta_j . R_{n+j}^{(k)} . b}}, \text{If } j \notin S,\ (j \in I, \tilde{j} = +j) \text{ or } j \notin I \\
D_j = B^{\frac{r_j'}{\zeta_j . R_{n+j}^{(k)}}} = g^{\frac{r_j}{\zeta_j . R_{n+j}^{(k)}}}, \text{If } j \notin S,\ j \in I, \tilde{j} = -j
\end{cases}
$$

$$D_i = A^{\frac{1}{\zeta_i . R_i^{(k)}}} . g^{\frac{r_i'}{\zeta_i . R_i^{(k)}}} = g^{\frac{ab + r_i' . b}{\zeta_i . R_i^{(k)} . b}} = g^{\frac{r_i}{\zeta_i . R_i^{(k)} . b}}$$

ICCSLab@NSYSU

Security Analysis

$SK = \{ver, S, D, \overline{D} = \{D_i, F_i\}_{i \in U}\}$

- Phase 1

For each $j \in U$ *and* j ≠ i

$$\begin{cases} F_j = g^{\frac{r_j{}'}{\eta_j}} = g^{\frac{r_j}{\eta_j . b}}, \text{if } j \in I \\ F_j = B^{\frac{r_j{}'}{\eta_j}} = g^{\frac{r_j}{\eta_j}}, \text{if } j \notin I \end{cases}$$

$$F_i = A^{\frac{1}{\eta_i}} . g^{\frac{r_i{}'}{\eta_i}} = g^{\frac{ab + r_i{}'.b}{\eta_i . b}} = g^{\frac{r_i}{\eta_i . b}}$$

SK -> A

Security Analysis

- Challenge

$\{M_0, M_1\}$ -> B

$b \epsilon \{0,1\}$

$\tilde{C} = M_b.Z$

$$\begin{cases} C_i = C^{\delta_i . R_i^{(ver^*)}}, \text{if } i \in I \ \& \ \tilde{i} = +i \\ C_i = C^{\zeta_i . R_{n+i}^{(ver^*)}}, \text{if } i \in I \ \& \ \tilde{i} = -i \\ C_i = C^{\eta_i}, \text{if } i \notin I \end{cases}$$

CT^* -> A

$CT^* = \{ver^*, AS^*, \tilde{C}, C, \{C_i\}_{i \in U}\}$

- Phase 2
  - phase 1 is repeated

Security Analysis

- Guess

b_0 ={0,1} -> B

$\mu' = 0$,if $b_0 = b$

$\mu' = 1$,if $b_0 \neq b$

$$\Pr[b_0 \neq b|\mu \quad = 1] = \frac{1}{2} \text{->} \Pr[\mu' = \mu \quad |\mu \quad = 1] = \frac{1}{2}$$

$$\Pr[b_0 = b|\mu \quad = 0] = \frac{1}{2} + ADV_{CPA} \text{->} \Pr[\mu' = \mu|\mu \quad = 0] = \frac{1}{2} + ADV_{CPA}$$

$The\ advantage\ of\ B\ in\ the\ DBDH\ game$:

$$\frac{1}{2}\Pr[\mu' = \mu \quad |\mu \quad = 1] + \frac{1}{2}\Pr[\mu' = \mu|\mu \quad = 0] - \frac{1}{2} = \frac{1}{2}ADV_{CPA}$$

ICCSLab@NSYSU

Thank You