Attribute-based Encryption and Its Application

王 晨

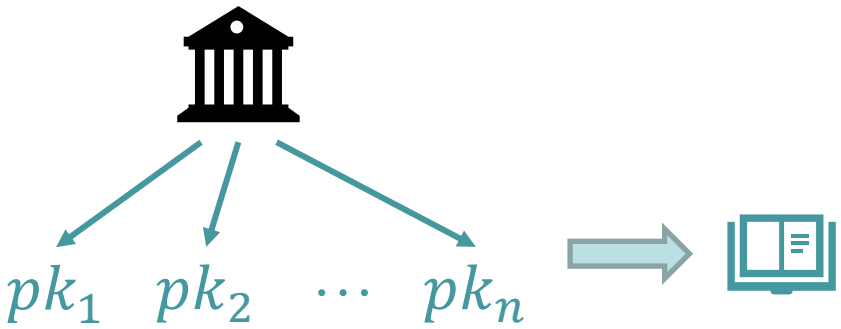
wangchen@zstu.edu.cn

中国密码学会2023年青年论坛

Contents

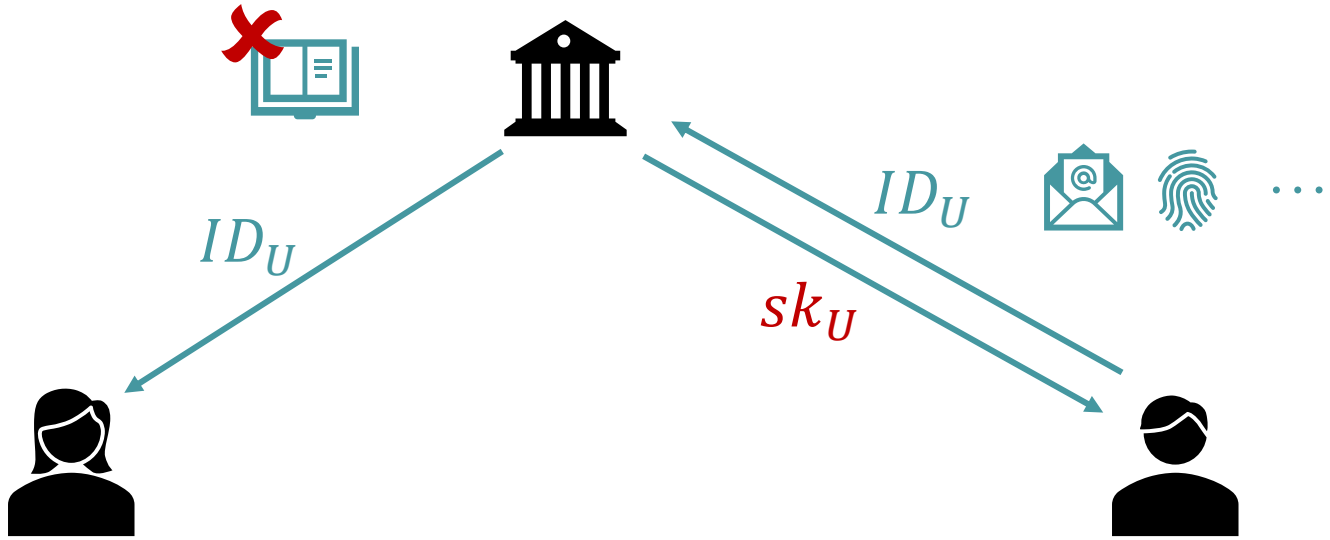
- Attribute based Encryption and CP-ABE
- Access Control with Multi-Authority
- IPFS assisted Access Control
- Future Work

Public Key Encryption



$$CT = Enc_{pk}(msg) \xrightarrow[\text{Public channel}]{CT} msg = Dec_{sk}(CT)$$

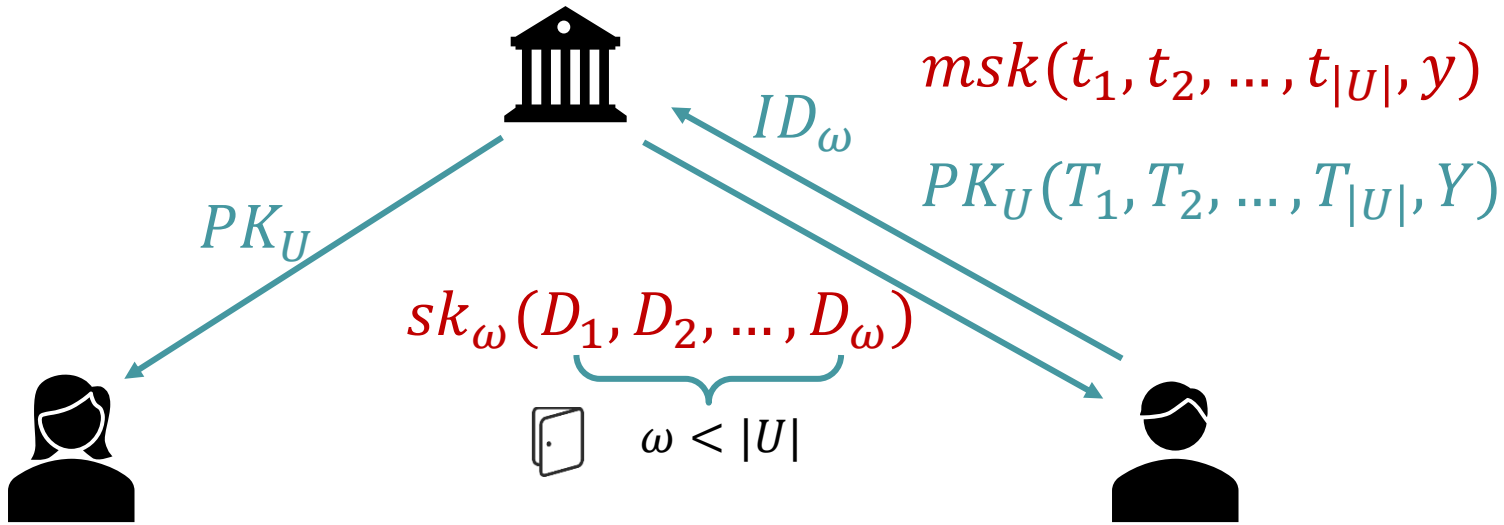
Identity-based Encryption (IBE)



$$CT = Enc_{ID_U}(msg) \xrightarrow[\text{Public channel}]{CT} msg = Dec_{sk_U}(CT)$$

Shamir A. Identity-based cryptosystems and signature schemes. CRYPTO 84

Fuzzy Identity-based Encryption (FIBE)



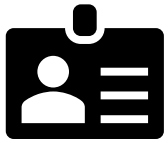
$$CT = Enc_{PK_U}(msg) \xrightarrow[\text{Public channel}]{CT} msg = Dec_{sk_\omega}(CT)$$

Sahai A, Waters B. Fuzzy identity-based encryption. EUROCRYPT 2005

Fuzzy Identity-based Encryption (FIBE)

$msk(t_1, t_2, \ldots, t_{|U|}, y)$

$att_1, att_2, \ldots, att_{|U|}$



attributes

Sahai A, Waters B. Fuzzy identity-based encryption. EUROCRYPT 2005

Fuzzy Identity-based Encryption (FIBE)

$$msk(t_1, t_2, \dots, t_{|U|}, y)$$

$$att_1, att_2, \dots, att_{|U|}$$

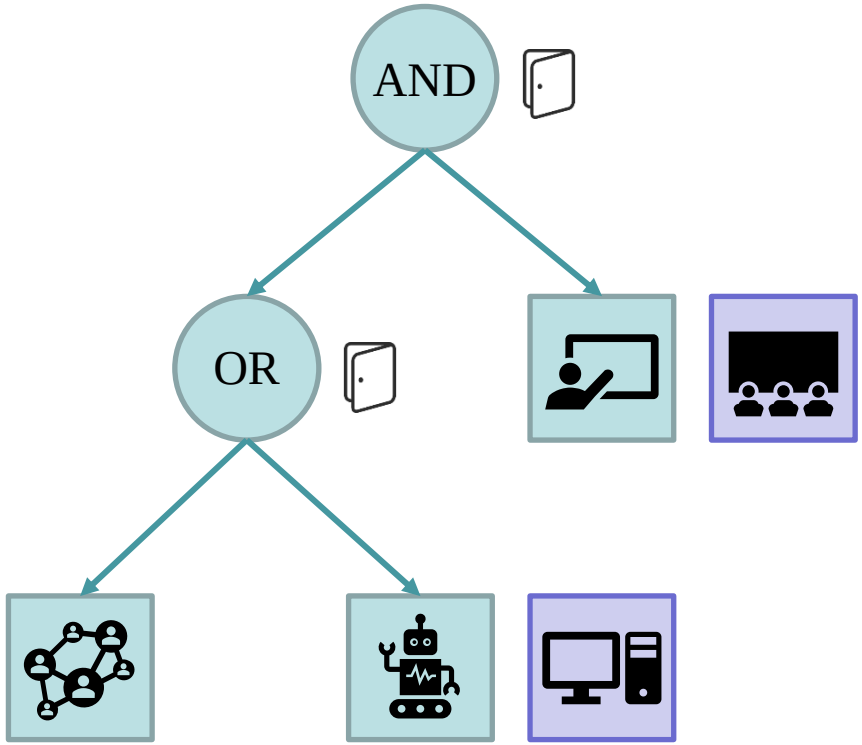
policy tree attributes

Attribute-based Encryption (ABE)

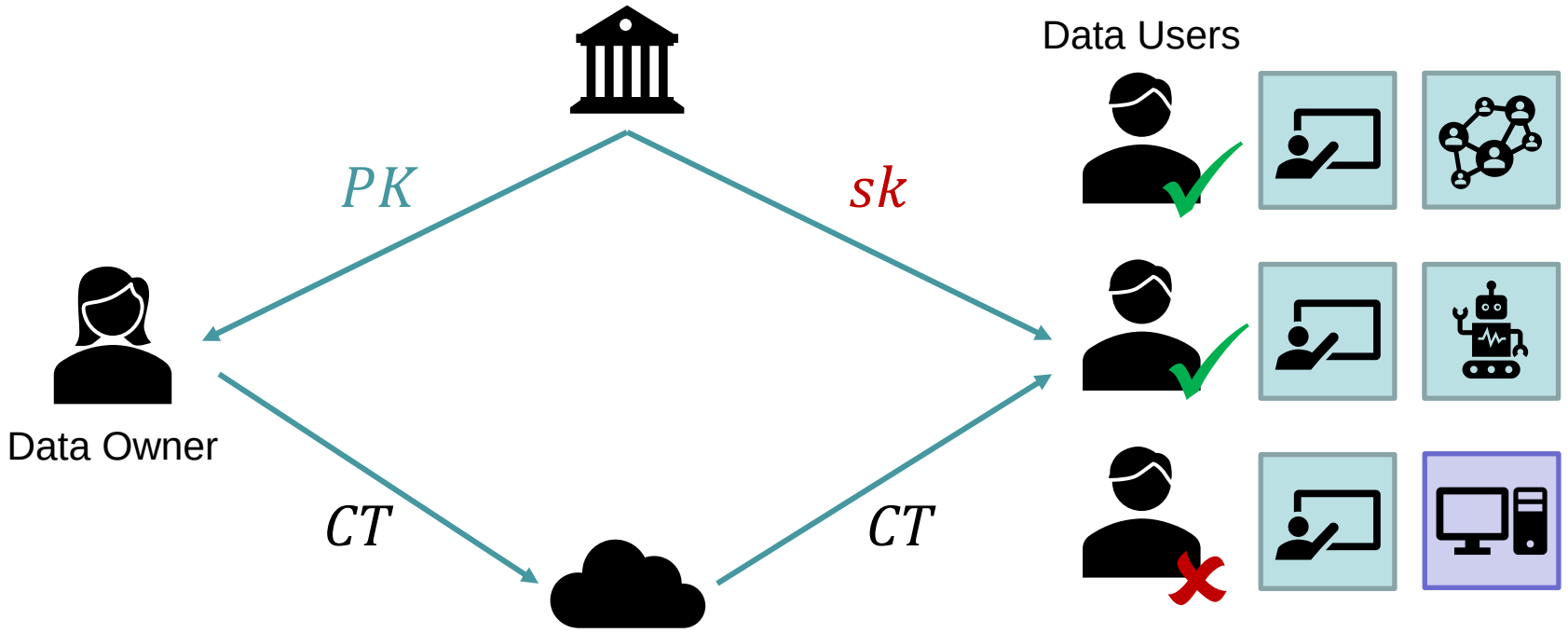
policy tree attributes

Attribute-based Encryption (ABE)

policy tree



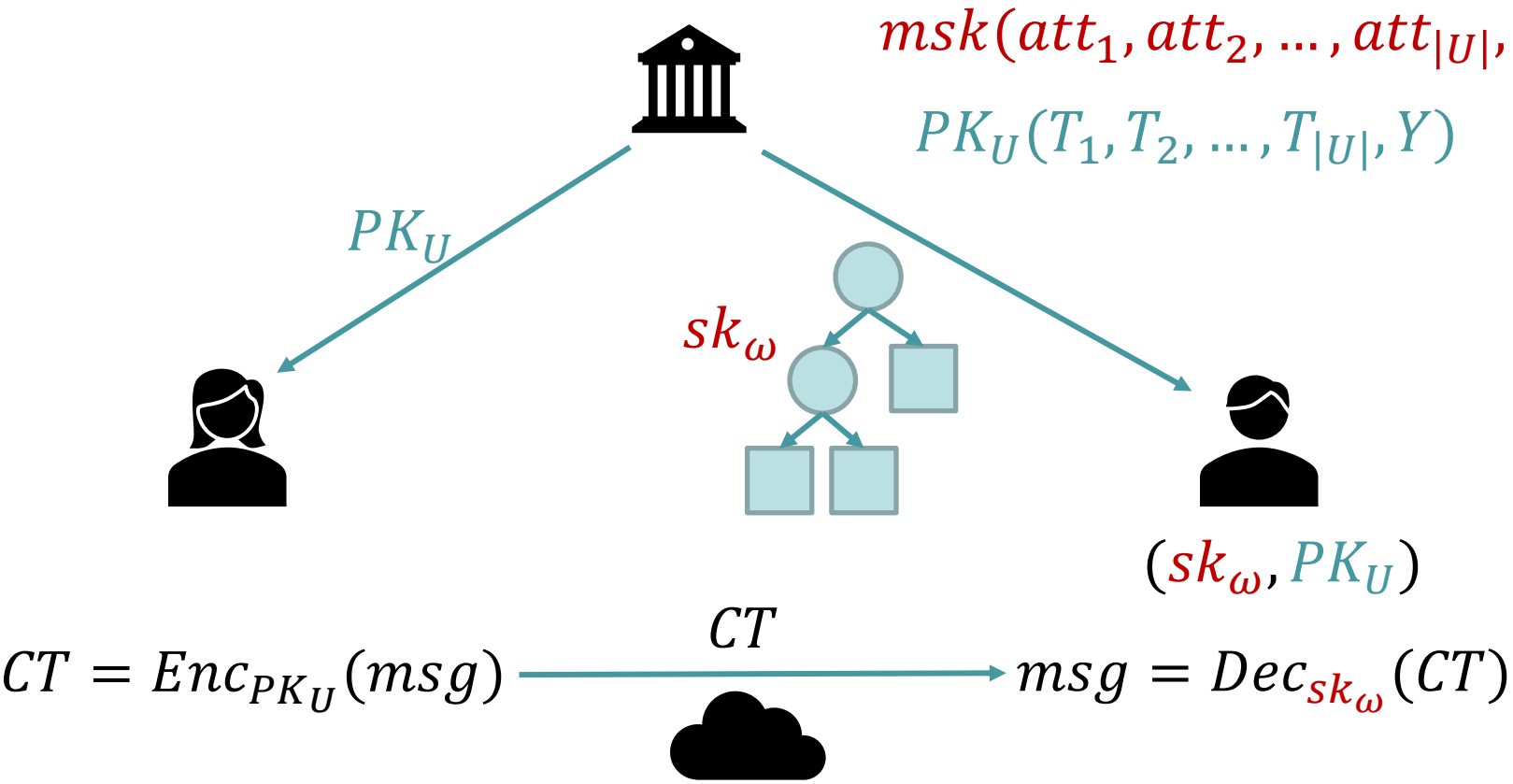
Attribute-based Encryption (ABE)



Attribute-based Encryption (ABE)

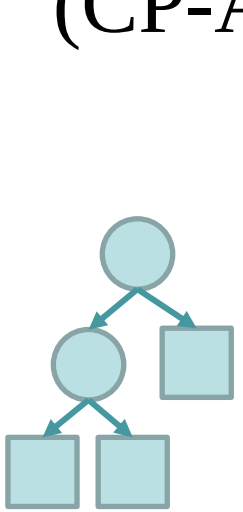
- Key Policy Attribute-based Encryption (KP-ABE)
- Ciphertext Policy Attribute-based Encryption (CP-ABE)

Key Policy Attribute-based Encryption (KP-ABE)



Goyal V, Pandey O, Sahai A, Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. CCS 2006

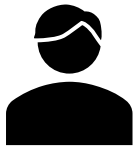
Ciphertext Policy Attribute-based Encryption (CP-ABE)



$msk: D, D_j = g^r \cdot H(att_j)^{r_j}, D'_j$

$\widetilde{sk}: \tilde{D}, \tilde{D}_k = g^r \cdot H(k)^{r_j}, \tilde{D}'_k$

PK



$CT = (\boldsymbol{Tree}, \tilde{C} = msg \cdot e(g,g)^{\alpha s}, C = h^s,$
$\forall y \in Y: C_y = g^{q_y(0)}, C'_y = H(att_y)^{q_y(0)})$

$(\widetilde{sk}, PK)$

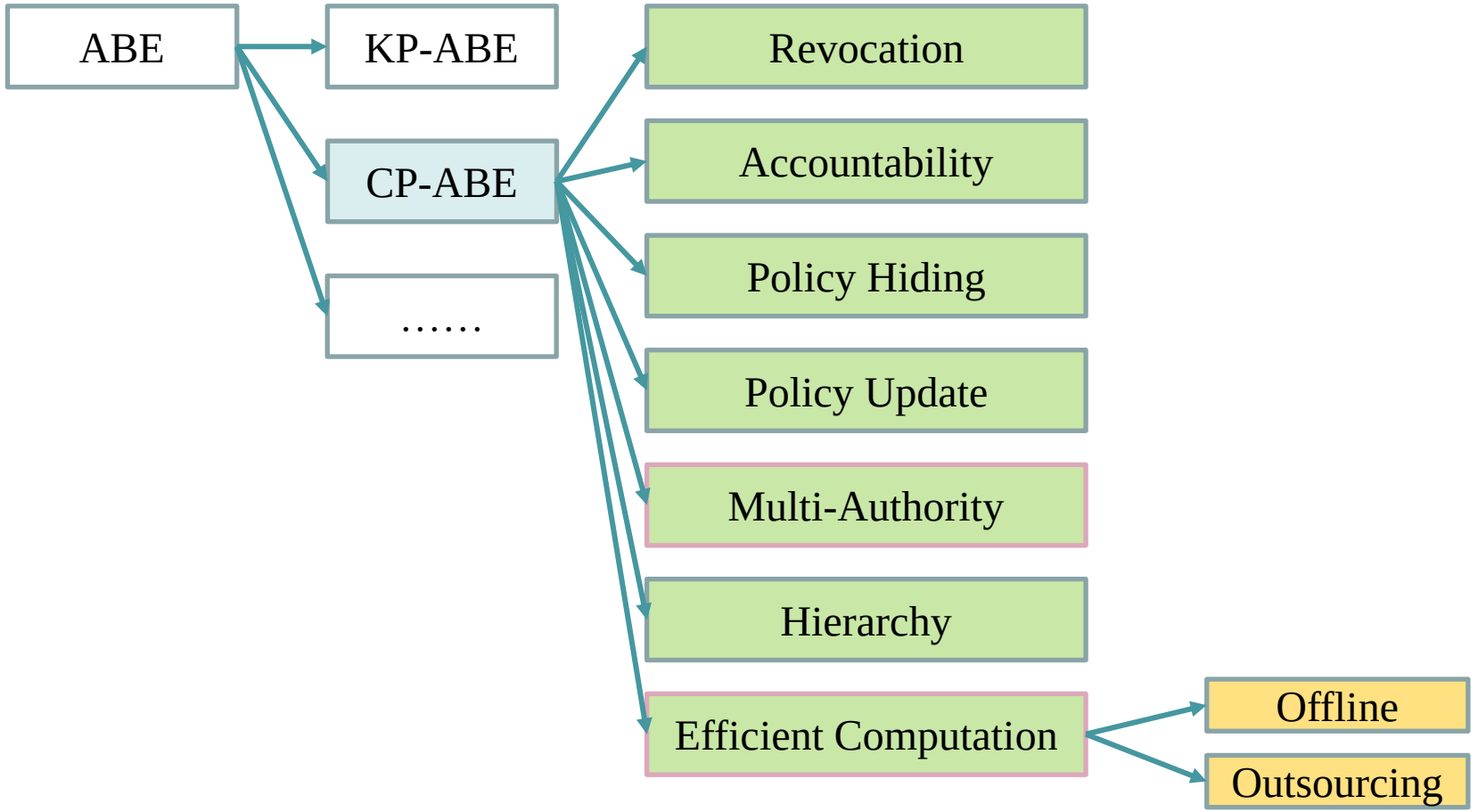
Data owner determines a policy for who can decrypt

CT

$msg = Dec_{\widetilde{sk}}(CT)$

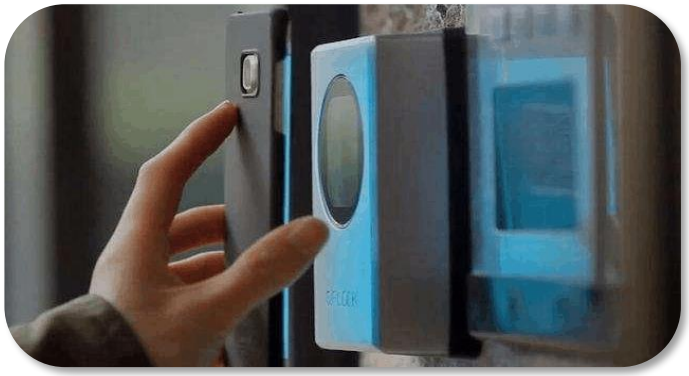
Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. S&P 2007

Taxonomy of ABE



Zhang Y, Deng R H, Xu S, et al. Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys

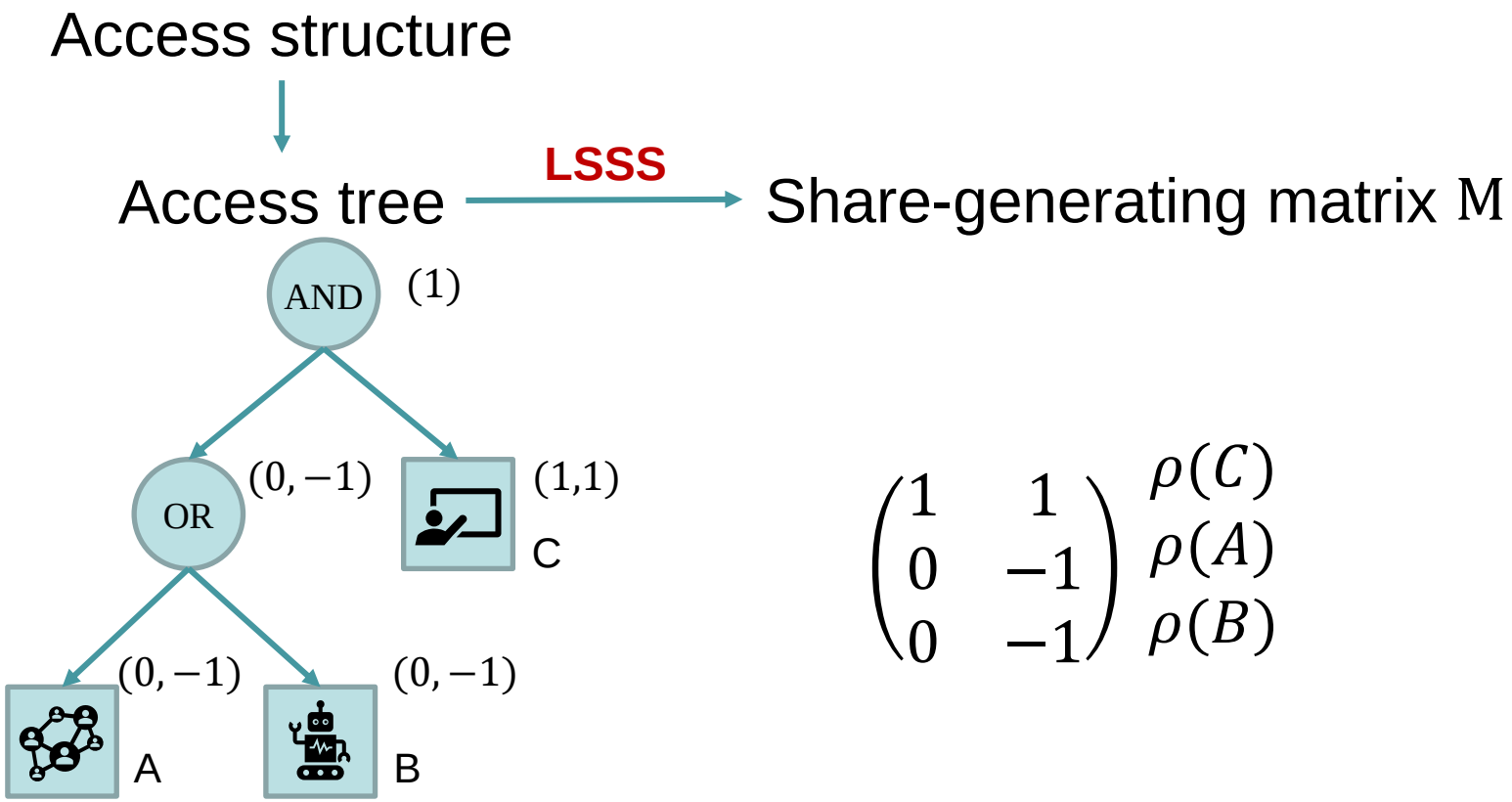
Application



Access Control with Multi-Authority

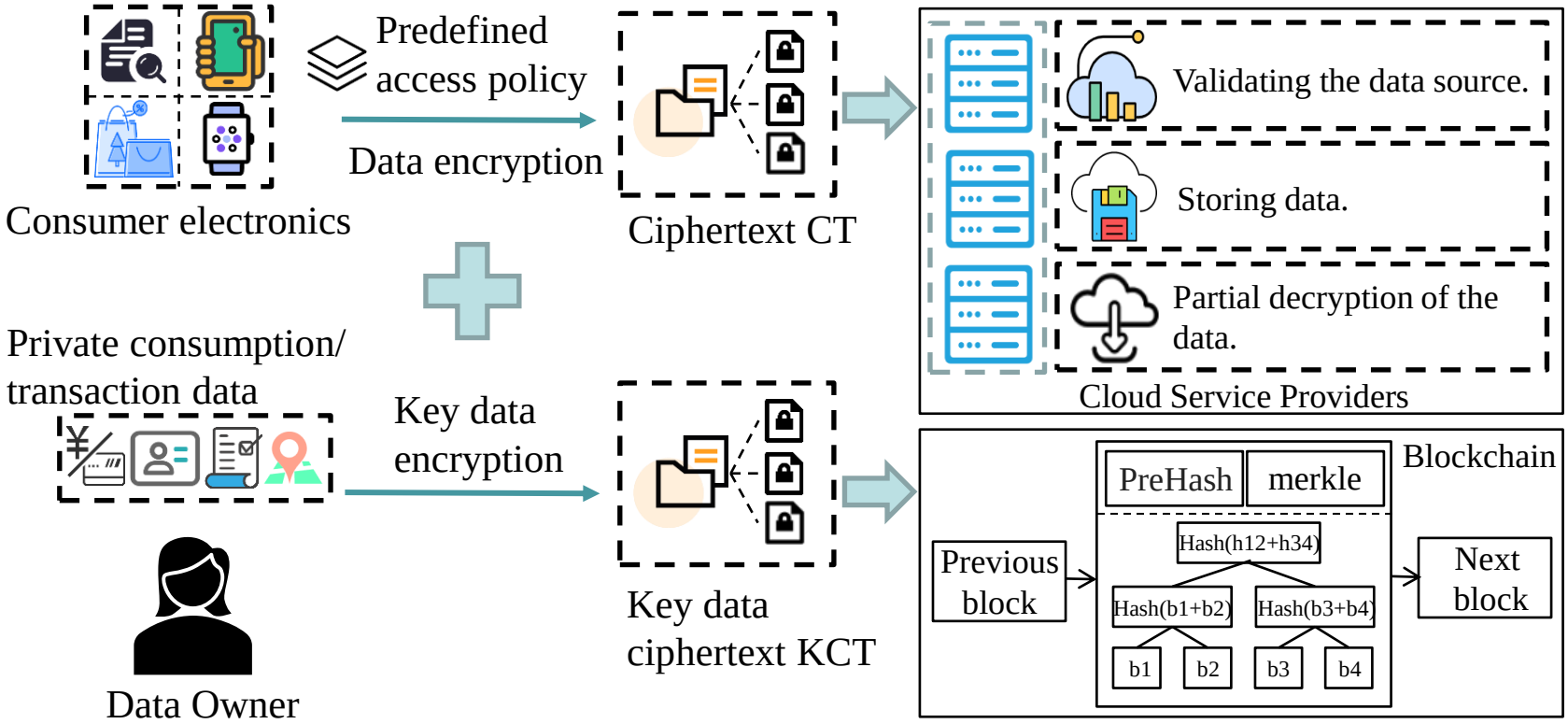
- Expressive and revocable access control
- Attribute ranking
- Negative constraints

Linear Secret Sharing Scheme (LSSS) matrix

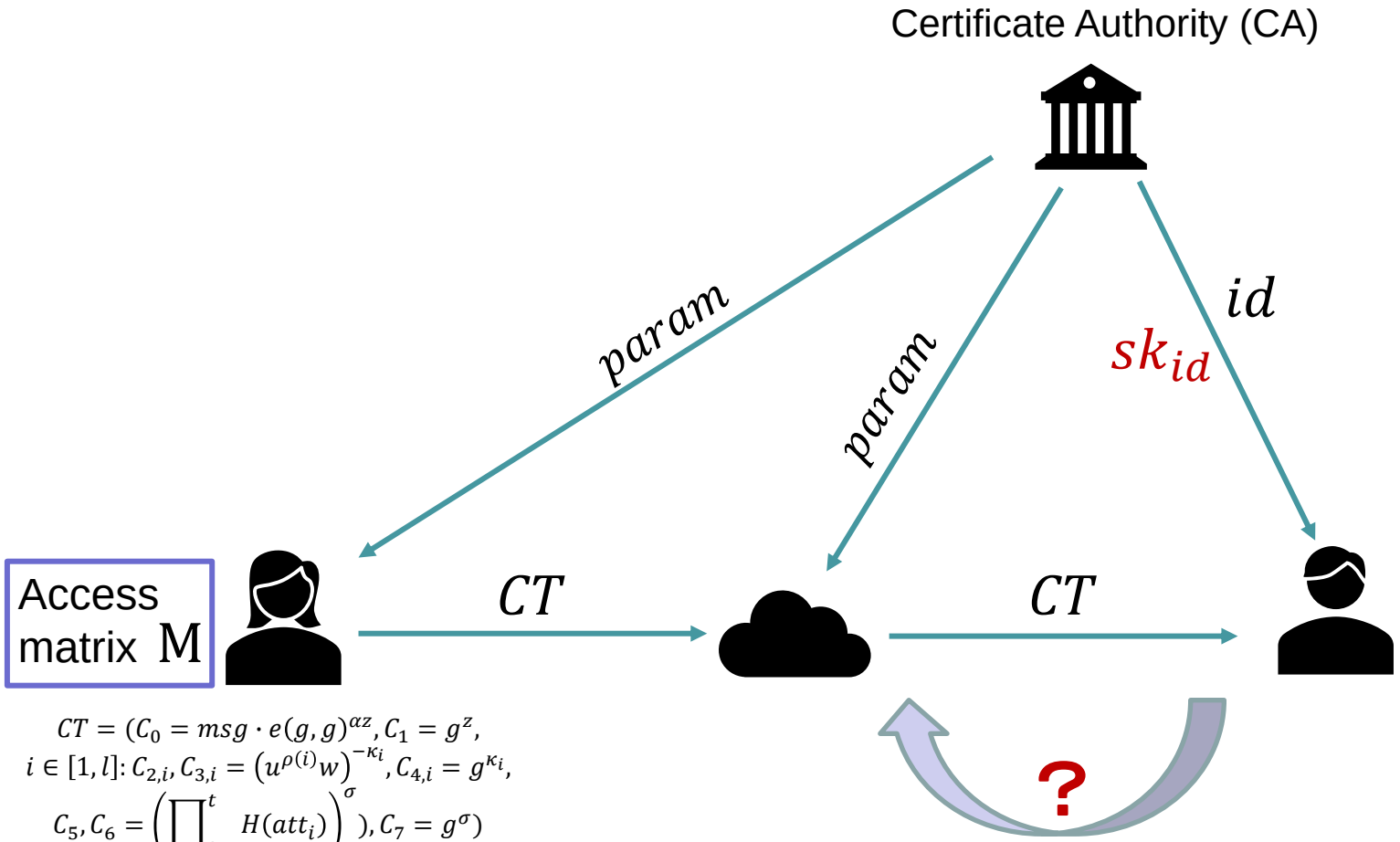


Waters B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. PKC 2011

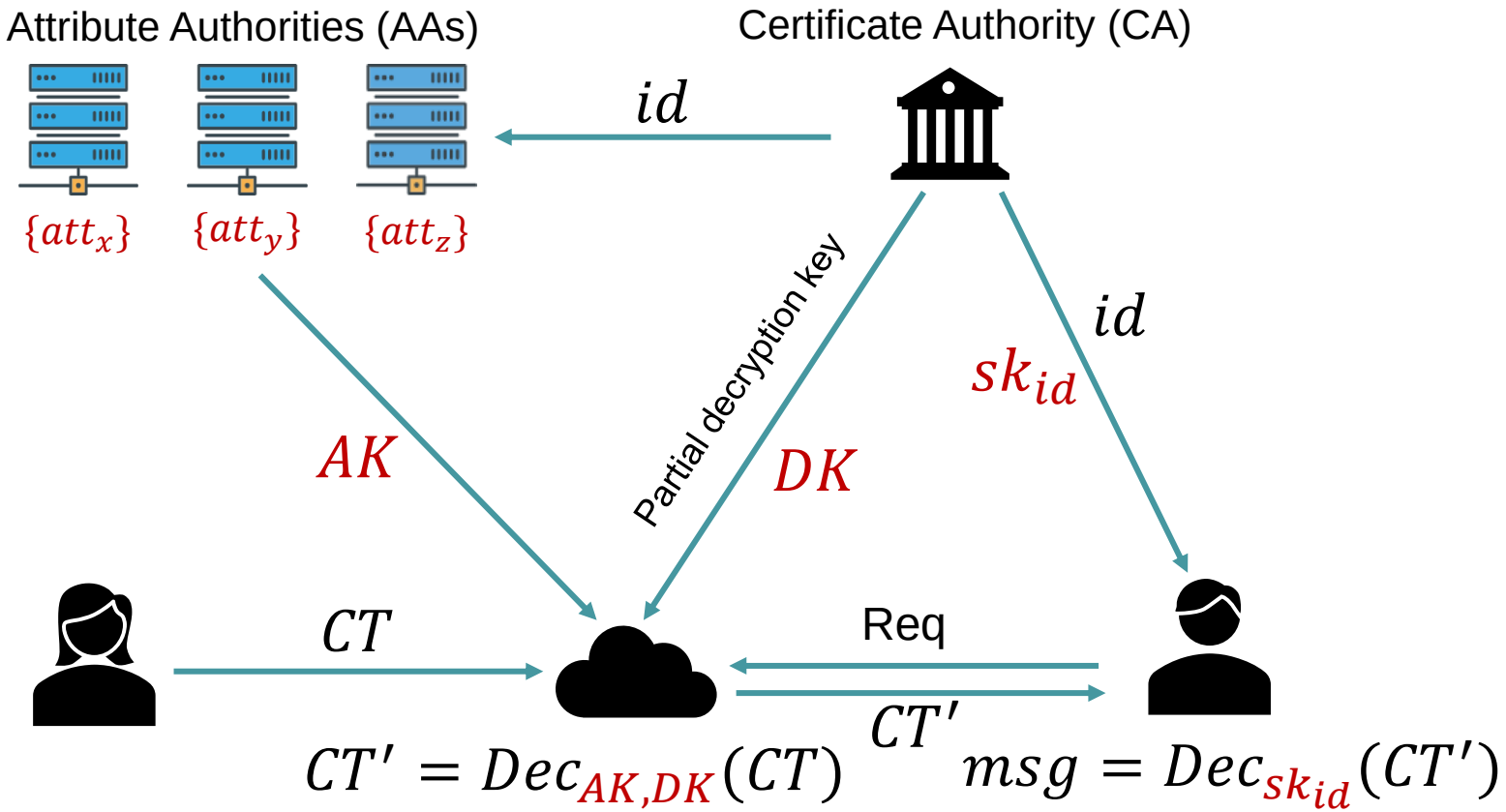
Human-centric consumer applications



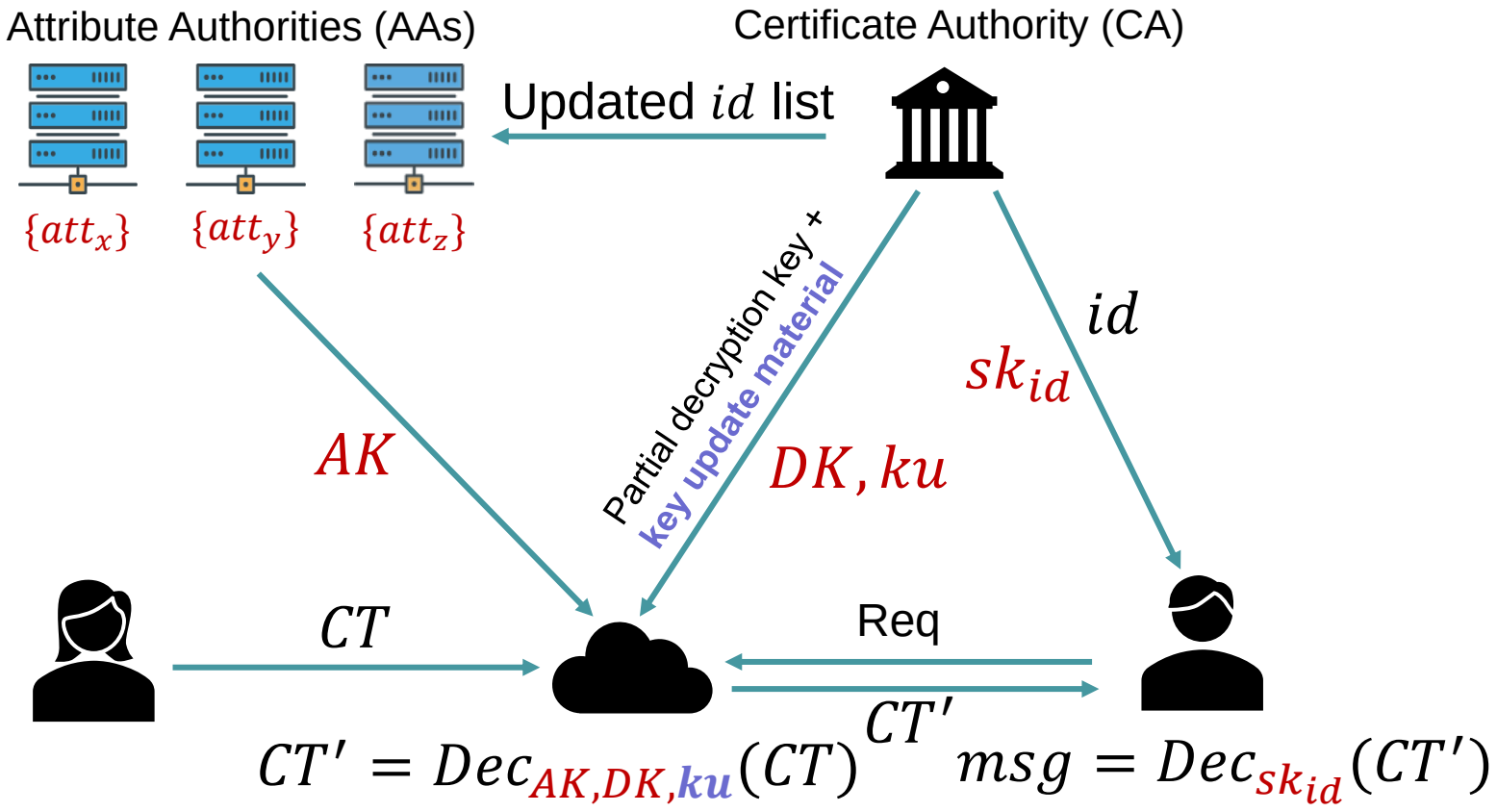
Access Control with Multi-Authority



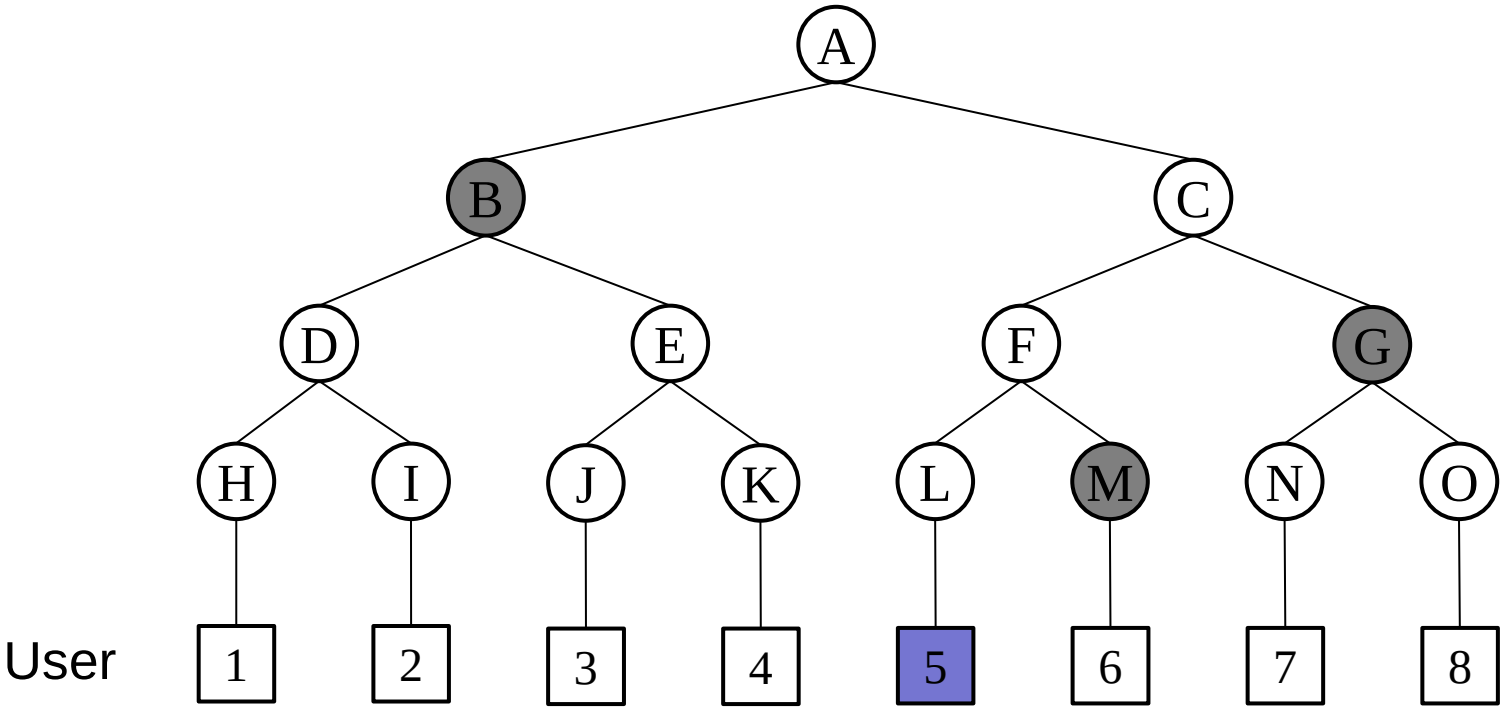
Access Control with Multi-Authority



Revocation


Attribute Authorities (AAs)
Certificate Authority (CA)
Updated id list
$\{att_x\}$
$\{att_y\}$
$\{att_z\}$
AK
Partial decryption key +
key update material
DK, ku
id
sk_{id}
CT
Req
CT'
$CT' = Dec_{AK,DK,ku}(CT)$
$msg = Dec_{sk_{id}}(CT')$

Revocation

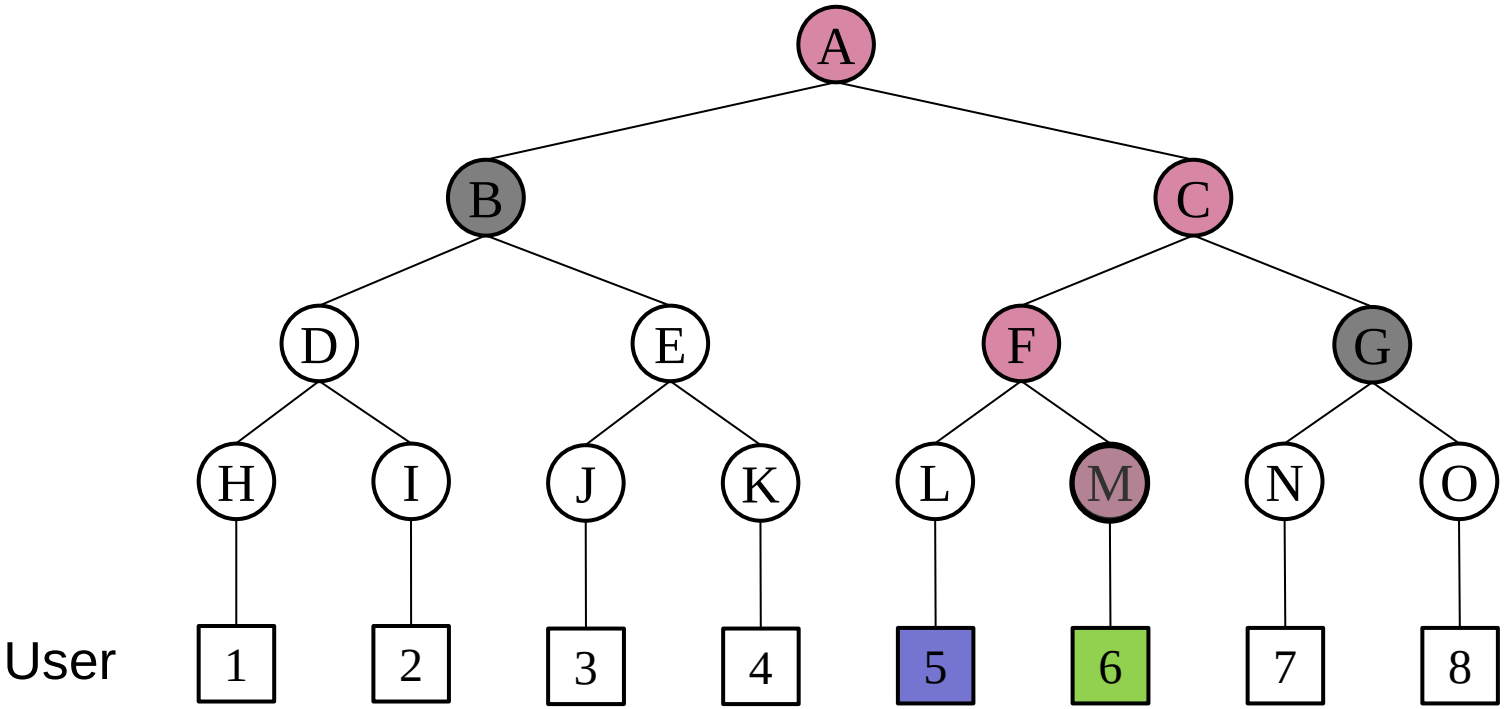


User 5 is revoked.

$$Path(5) = (A, C, F, L)$$

$$KUNodes \text{ return } \mathrm{Y} = (\mathrm{B}, \mathrm{G}, \mathrm{M})$$

Revocation



$KUNode\ return\ Y = (\mathrm{B}, \mathrm{G}, \mathrm{M})$

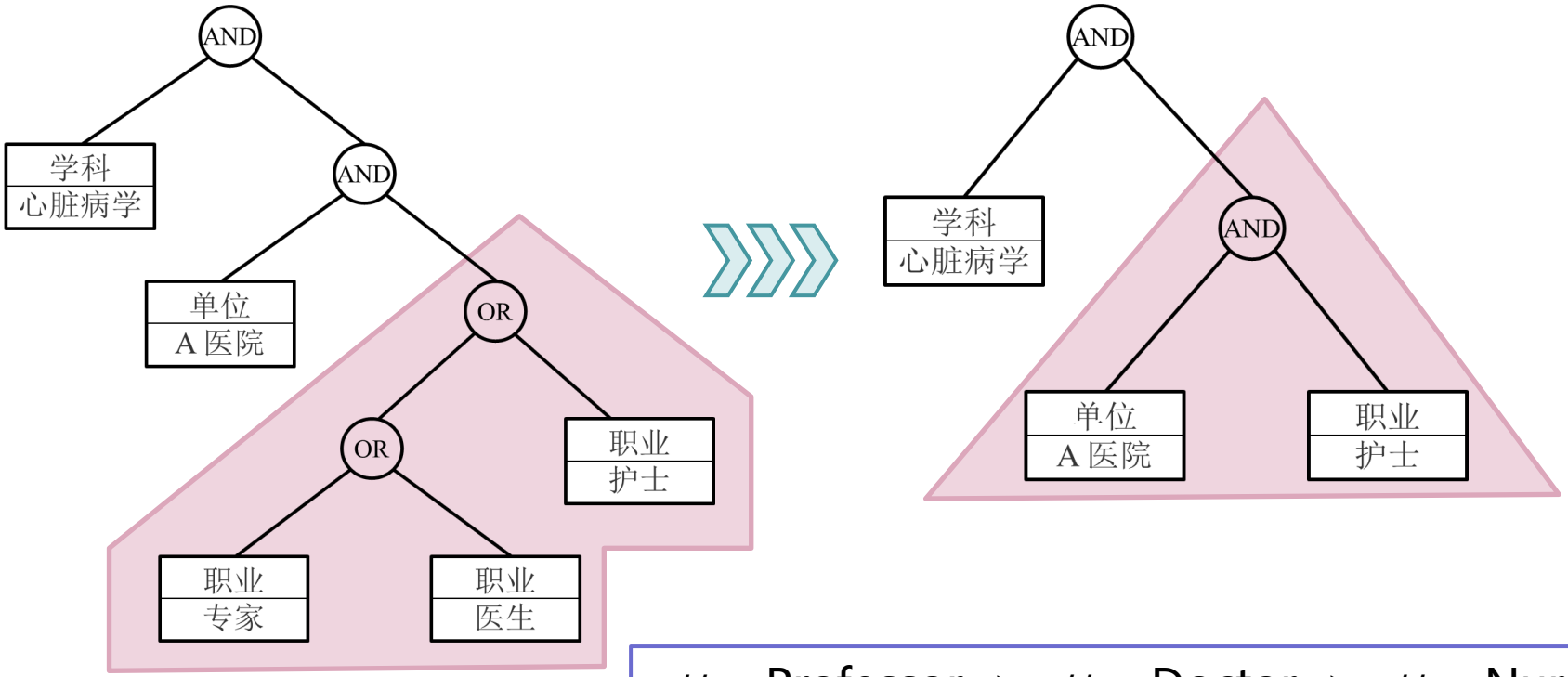
e.g. User 6 has not been revoked.

$Path(6) = (A, C, F, M)$

$Path(6) \cap Y = M$

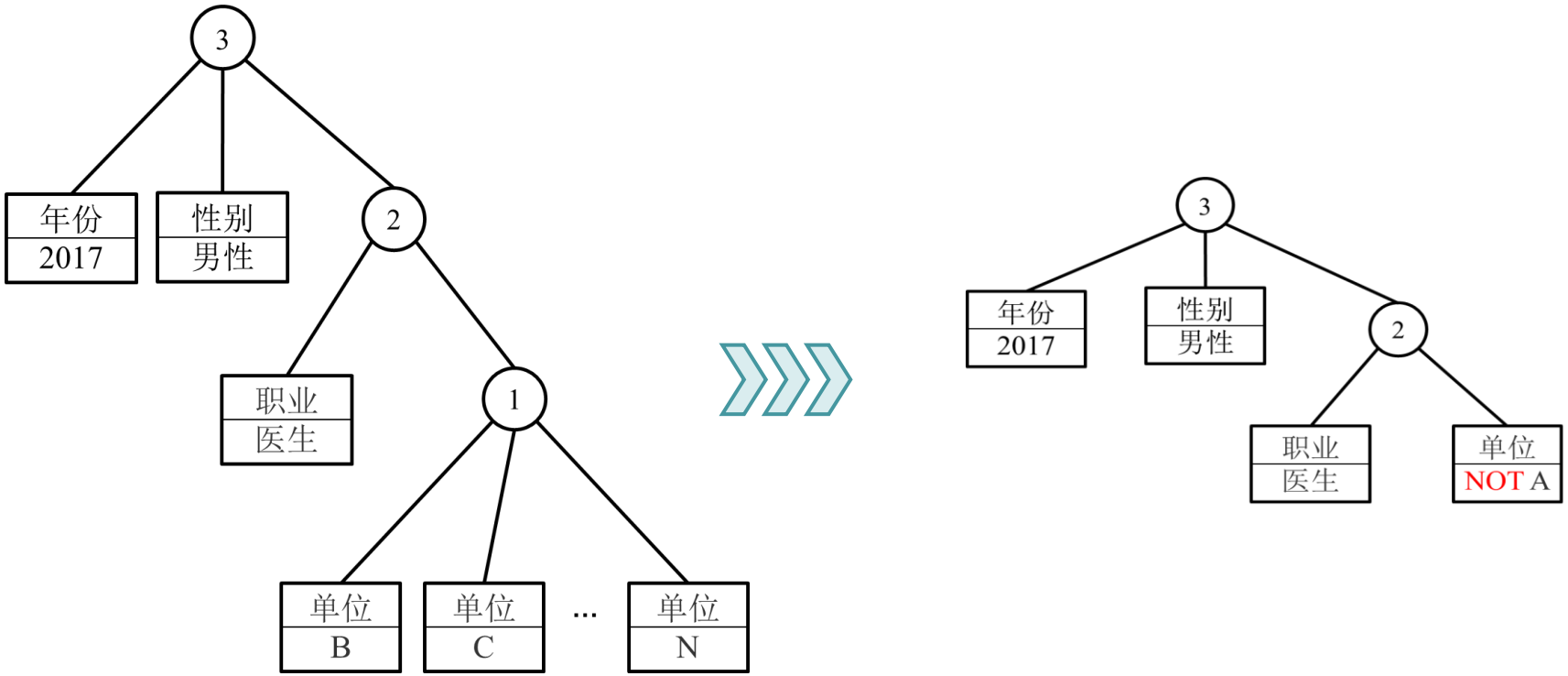
$\Rightarrow ku_6$

Attribute ranking



att_1=Professor > att_2=Doctor > att_3=Nurse

Negative constraints



Performance

Scheme	XLD+19 [30]	R-ABE [31]	Zhang et al [32]	Ours
AKeyGen	–	–	$(2+5S)E+$ $(1+3S)M$	$4SE+2SM$
DKeyGen	E	$[(3+4S)E+(1+2S)M]logN$	–	$(3E+2M)logN$
KeyUpdate	–	$[3E+(1+log_T)M]Rlog\frac{N}{R}$	–	$(3E+2M)Rlog\frac{N}{R}$
TKeyGen	$(8t+4S+1)E$	$(4+2S)E+$ $(5+logT+2S)M$	–	$2M$
Encrypt	$(5l+4t+2)E+$ $(2l+2t+1)M$	$(3+5l+logT)E+$ $(1+2l)M$	$(1+7l)E+$ $(1+2l)M+P$	$(6+5l)E+(2+2l+t)M$
Verify	–	–	–	$2E+tM+2P$
Transform	$(t+l)E+(2t+3l)M+$ $(3t+3l)P$	–	–	$lE+(3l+1)M+(2+4l)P$
Dec	$E+M$	$lE+(2l+2)M+(3l+2)P$	$(2l+1)E+$ $(4l+2)M+4lP$	$P+M$

S is defined as the number of attributes of the data user, N denotes the number of data users, P denotes a bilinear pairing operation, E denotes an exponential operation on the groups $\mathbb{G}$ and $\mathbb{G}_T$, M denotes the multiplication operation on the groups $\mathbb{G}$ and $\mathbb{G}_T$, l denotes the number of rows in the access policy, t denotes the number of attributes of the data owner, T denotes the lifetime of the ciphertext.

Performance

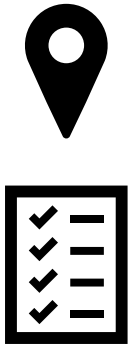
Scheme	Secret Key Size	Update Key Size	Ciphertext Size
XLD+19 [30]	$O(t+S)\|\mathbb{G}\|$	$-$	$O(l+t)\|\mathbb{G}\|+O(1)\|\mathbb{G}_T\|$
R-ABE [31]	$O(S\cdot logN)\|\mathbb{G}\|$	$O(logT\cdot Rlog\frac{N}{R})\|\mathbb{G}\|$	$O(l+logT)\|\mathbb{G}\|+O(1)\|\mathbb{G}_T\|$
Zhang et al. [32]	$O(S)$	$-$	$O(l)\|\mathbb{G}\|+O(1)\|\mathbb{G}_T\|$
Ours	$O(logN+S)\|\mathbb{G}\|$	$O(Rlog\frac{N}{R})\|\mathbb{G}\|$	$O(t+l)\|\mathbb{G}\|+O(1)\|\mathbb{G}_T\|$

$|\mathbb{G}|$ and $|\mathbb{G}_T|$ denote the size of a group element in $\mathbb{G}$ and $|\mathbb{G}_T|$ respectively.

IPFS assisted Access Control

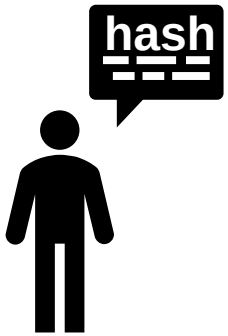
- Uploaded file deduplication
- Searched data verification
- Low communication overhead for user list update

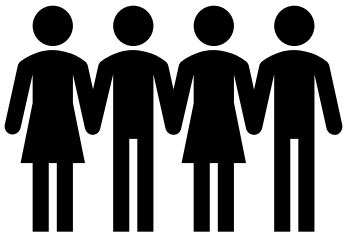
InterPlanetary File System (IPFS)



Location based addressing

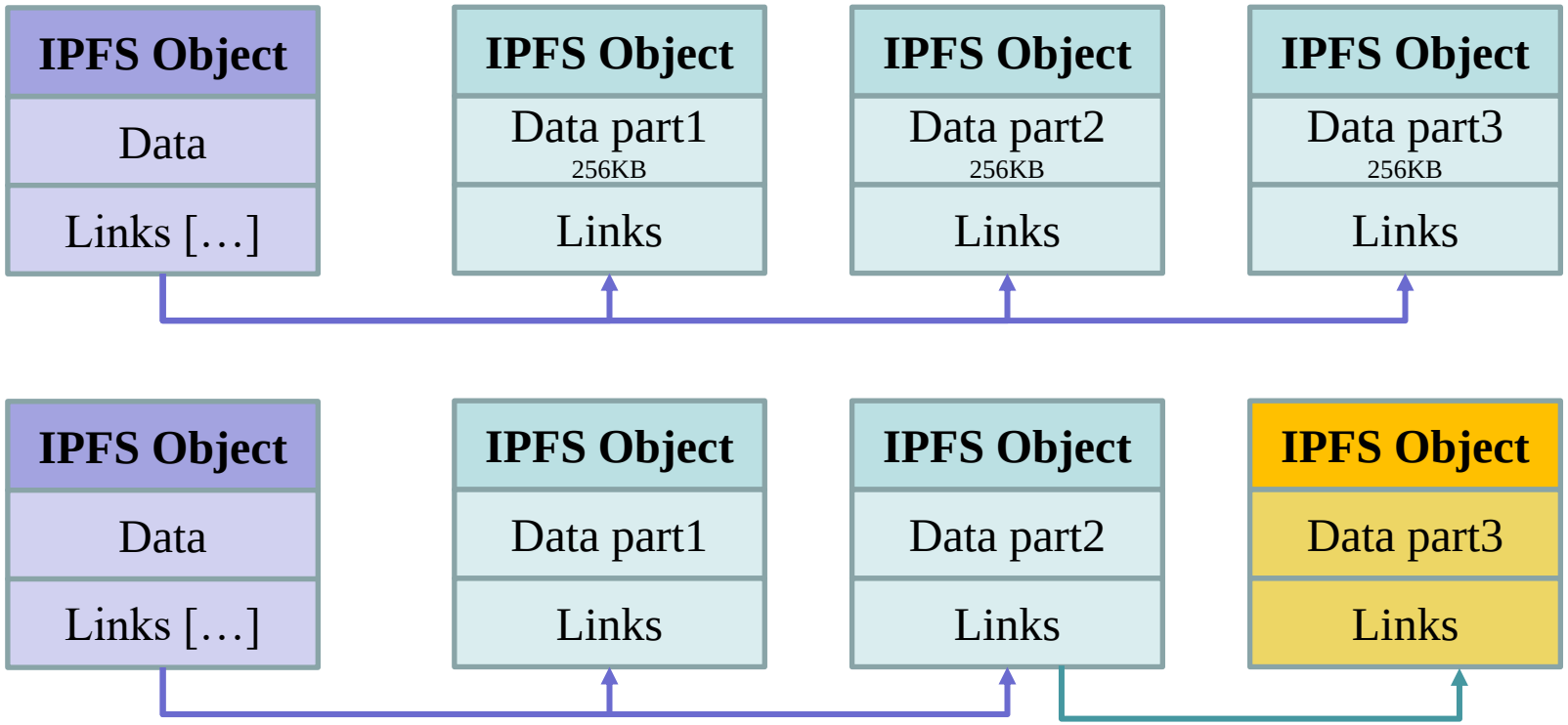
Content based addressing



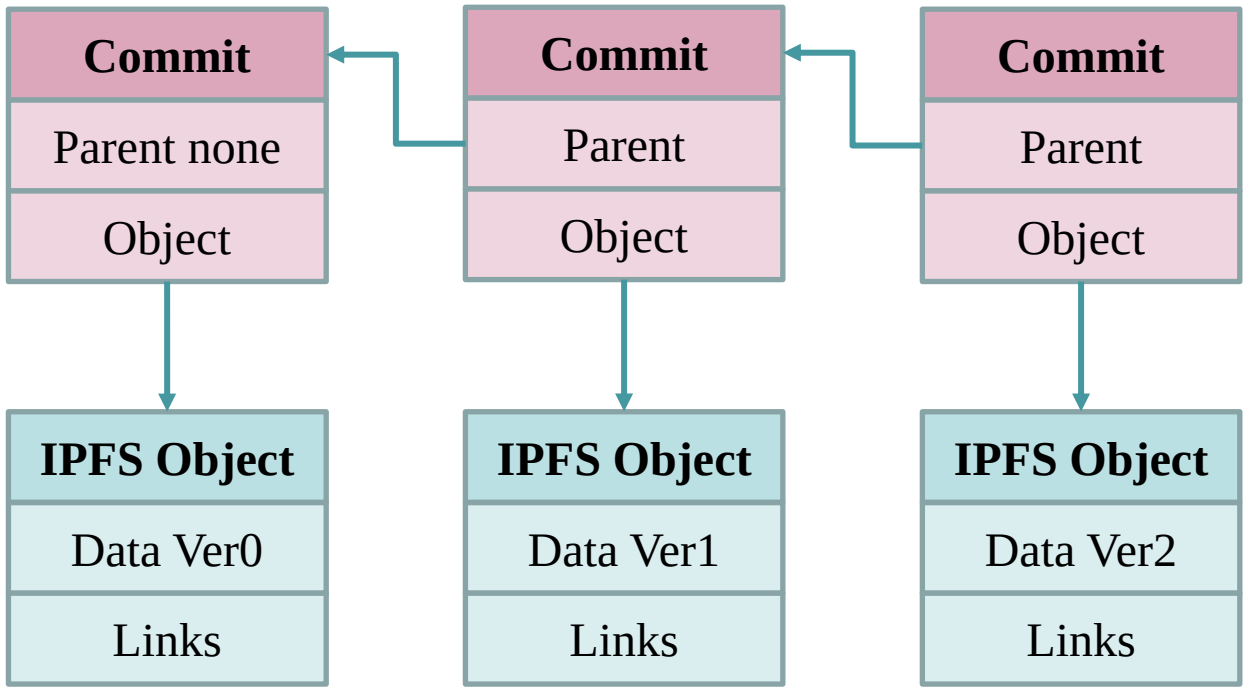


① File with this hash can be easily found
② Files with the same hash deleted

InterPlanetary File System (IPFS)



InterPlanetary File System (IPFS)



RSA based oblivious pseudo-random function (RSA-OPRF)

$h = H_1(msg)$ ← e, N — e, d, N

$x = hr^e \bmod N$ → x

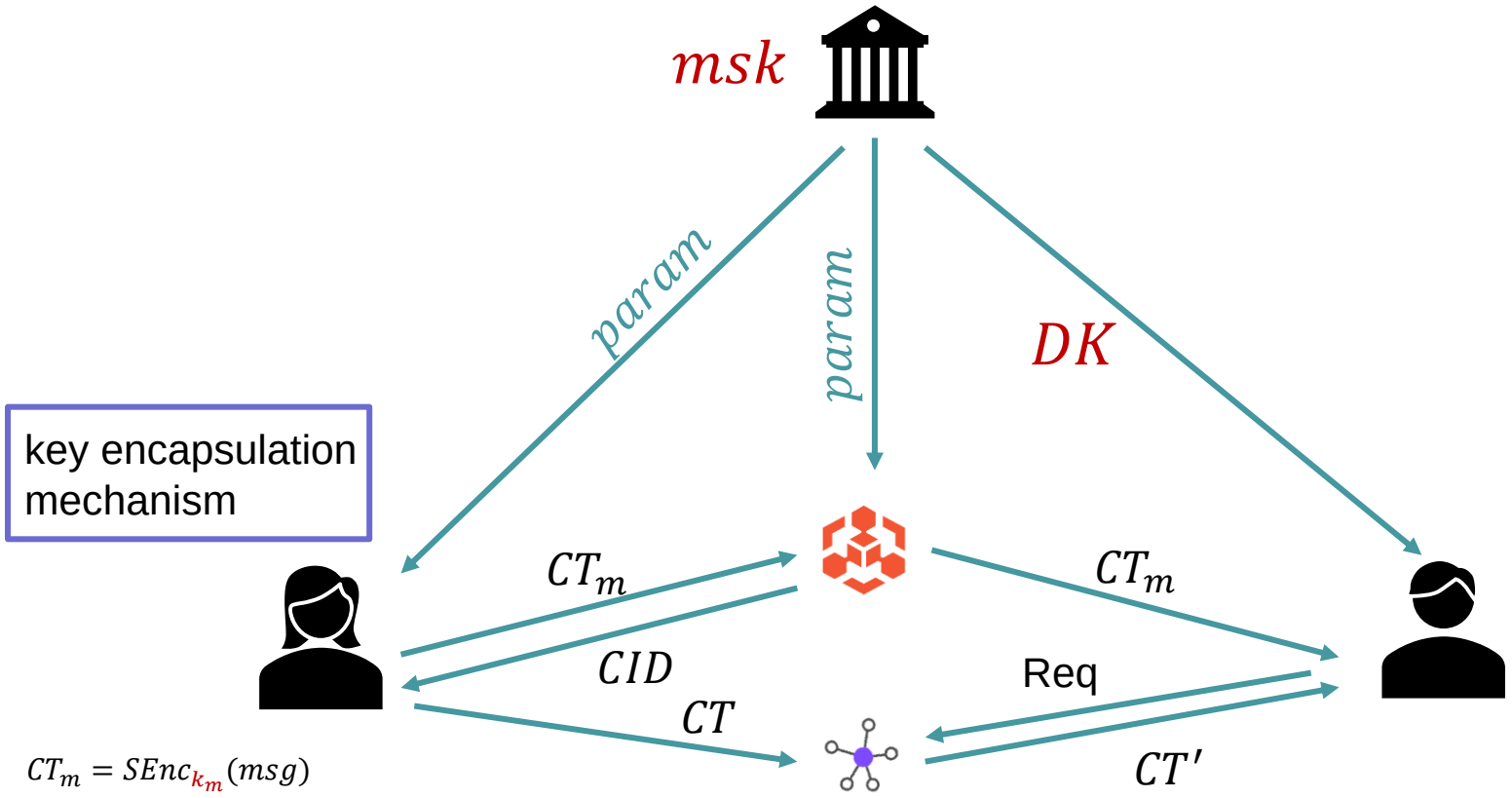
$y = x^d \bmod N$ ← y

$z = yr^{-1} \bmod N$

Verify $z^e = h \bmod N$

$k_m = H_2(z)$

IPFS assisted Access Control



$CT_m = SEnc_{k_m}(msg)$

$CT = (C = k_m \cdot e(g,g)^{\alpha s}, C_0 = g^s, C_1 = g^{\alpha s},$
$i \in [1,l]: C_{2,i}, C_{3,i} = g^{-t_i \cdot t_{\rho(i)} + \lambda_i}, C_{4,i} = g^{t_i}, T, R, \bar{A})$

IPFS assisted Access Control

Encryption Phase

1) Randomly selects secret value $s \in Z_p$ and $v_2, ..., v_n \in Z_p$, then computes $v = (s, v_2, ..., v_n)^{\mathrm{T}}$. For $i \in [1, l]$, $\lambda_i = M_i \cdot v$, where M_i represents the i-th row of M.

2) For $i \in [1, l]$, randomly selects $t_i \in Z_p$. The components of CT are calculated as follows.

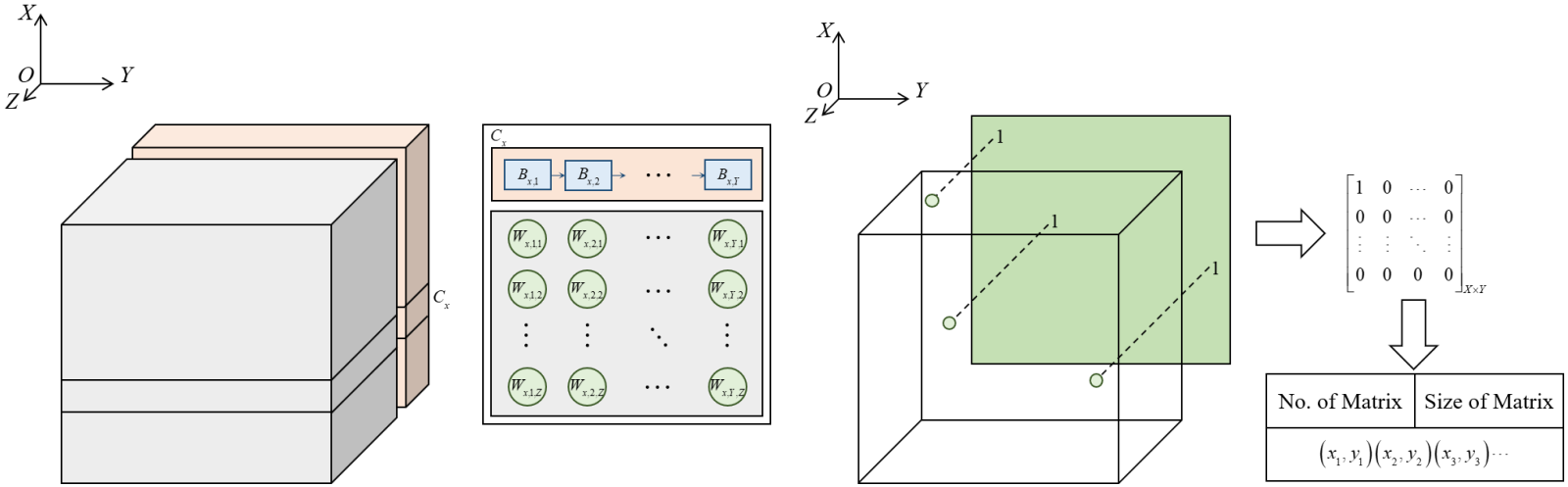
$$C = m \cdot e(g, g)^{\alpha s}, C_0 = g^s, C_1 = g^{as},$$
$$\{C_{i,1} = g^{\lambda_i} u^{t_i}, C_{i,2} = g^{-t_i \cdot t_{\rho(i)} + \lambda_i}, C_{i,3} = g^{t_i}\}_{i \in [1,l]}$$

3) Computes $cover(R)$ as a set which contains a minimum amount of tree nodes and the algorithm can reach all other unrevoked users through these nodes. For each $j \in cover(R)$, the algorithm computes $\{T_j = y_j^s\}_{j \in cover(R)}$

4) The algorithm output the final ciphertext

$$CT = \{C, C_0, C_1, \{C_{i,1}, C_{i,2}, C_{i,3}\}_{i \in [1,l]}, \{T_j = y_j^s\}_{j \in cover(R)}, R, M\}.$$

Cube data storage method

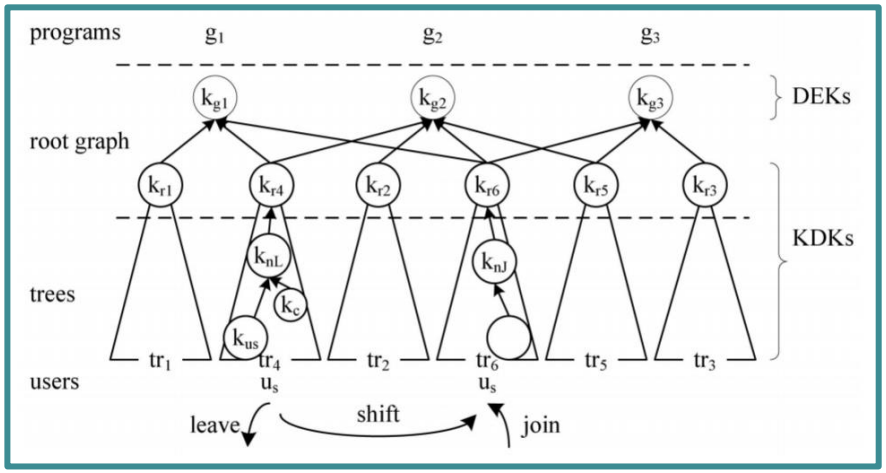


Data block tag generation $\sigma_i = \frac{m_i}{\lambda}\left(H_4\left(\sum_{n\in N}\omega_{i/n}\right)+s\right)$

Searched data set $K = \prod_{x\in X} K_x$

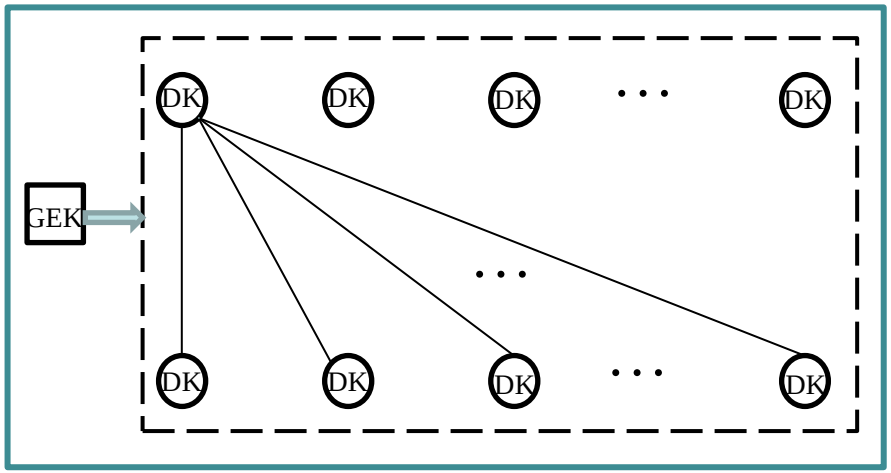
Challenge generation $chal = \left(\pi, K, X^*\right)$

Searched data verification $\varepsilon \overset{?}{=} H_5\left(\prod_{x\in X} e\left(v_x\sigma_x, \varphi\tau\right)\right)$



Tree based Update

- Easy to expand
- High computational overhead



Broadcast based Update

- Low computational overhead
- High communication overhead
- Weak scalability

BIBD based multi-broadcast update

BIBD

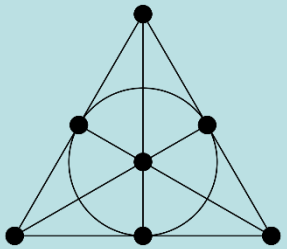
1. $bk = vr$
2. $\lambda(v-1) = r(k-1)$
3. $b = v$ **Symmetric**

(v, k, λ)

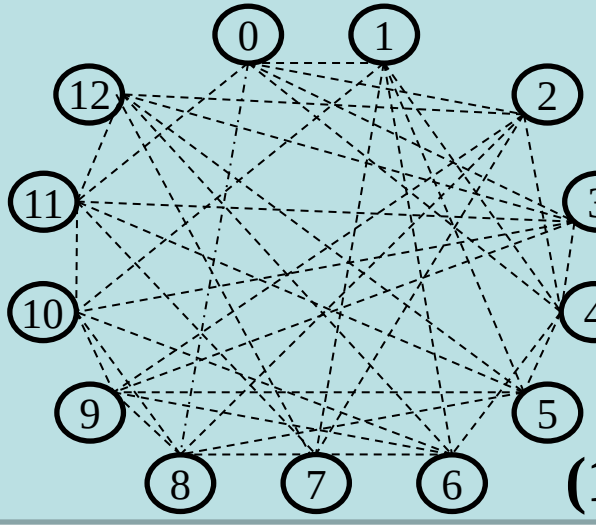
v	points, number of elements of X
b	number of blocks
r	number of blocks containing a given point
k	number of points in a block
λ	number of blocks containing any 2 (or more generally t) distinct points

(v, b, r, k, λ)

1	1	0	1	0	0	0
0	1	1	0	1	0	0
0	0	1	1	0	1	0
0	0	0	1	1	0	1
1	0	0	0	1	1	0
0	1	0	0	0	1	1
1	0	1	0	0	0	1

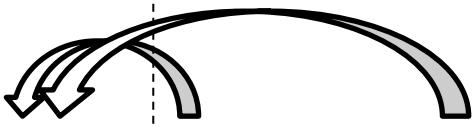


(7,3,1)



(13,4,1)

Round 1: Row-oriented



$r_{ij} = 1$	1	2	3	4	5	6	7
Party 1	**1**	**1**	**0**	**1**	**0**	**0**	**0**
Party 2	**0**	**1**	**1**	**0**	**1**	**0**	**0**
Party 3	**0**	**0**	**1**	**1**	**0**	**1**	**0**
Party 4	**0**	**0**	**0**	**1**	**1**	**0**	**1**
Party 5	**1**	**0**	**0**	**0**	**1**	**1**	**0**
Party 6	**0**	**1**	**0**	**0**	**0**	**1**	**1**
Party 7	**1**	**0**	**1**	**0**	**0**	**0**	**1**

Round 1: Row-oriented

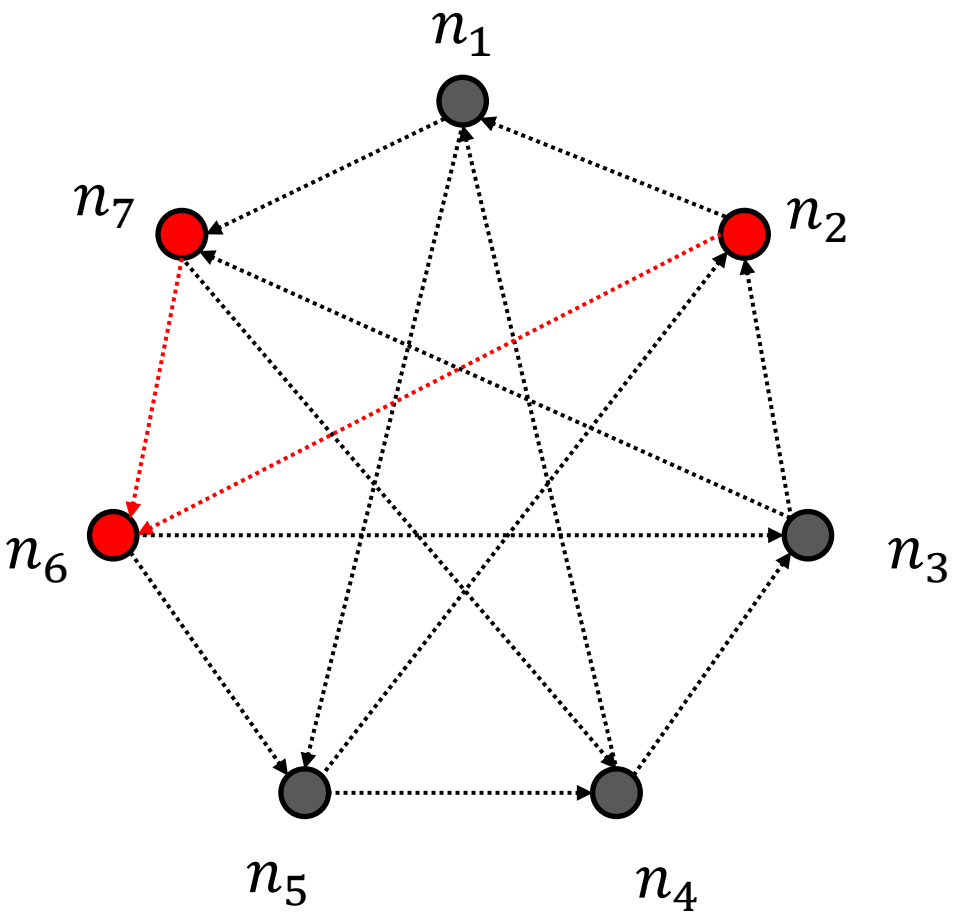
$r_{ij} = 1$

	1	2	3	4	5	6	7
Party 1	1	1	0	1	0	0	0
Party 2	0	1	1	0	1	0	0
Party 3	0	0	1	1	0	1	0
Party 4	0	0	0	1	1	0	1
Party 5	1	0	0	0	1	1	0
Party 6	0	1	0	0	0	1	1
Party 7	1	0	1	0	0	0	1

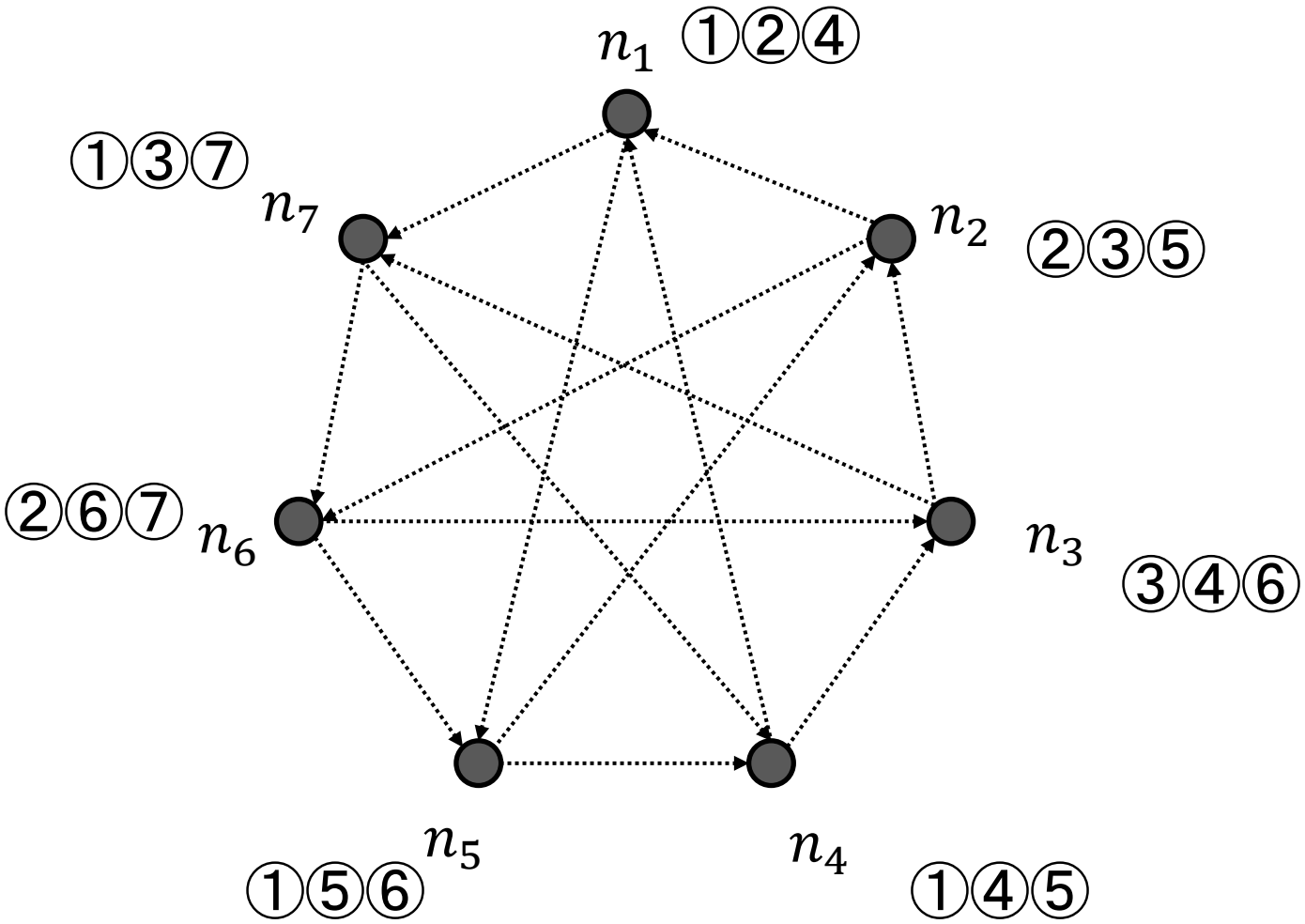
Round 2: Column-oriented

$c_{ij} = 1$	1	2	3	4	5	6	7
Party 1	1	1	0	1	0	0	0
Party 2	0	1	1	0	1	0	0
Party 3	0	0	1	1	0	1	0
Party 4	0	0	0	1	1	0	1
Party 5	1	0	0	0	1	1	0
Party 6	0	1	0	0	0	1	1
Party 7	1	0	1	0	0	0	1

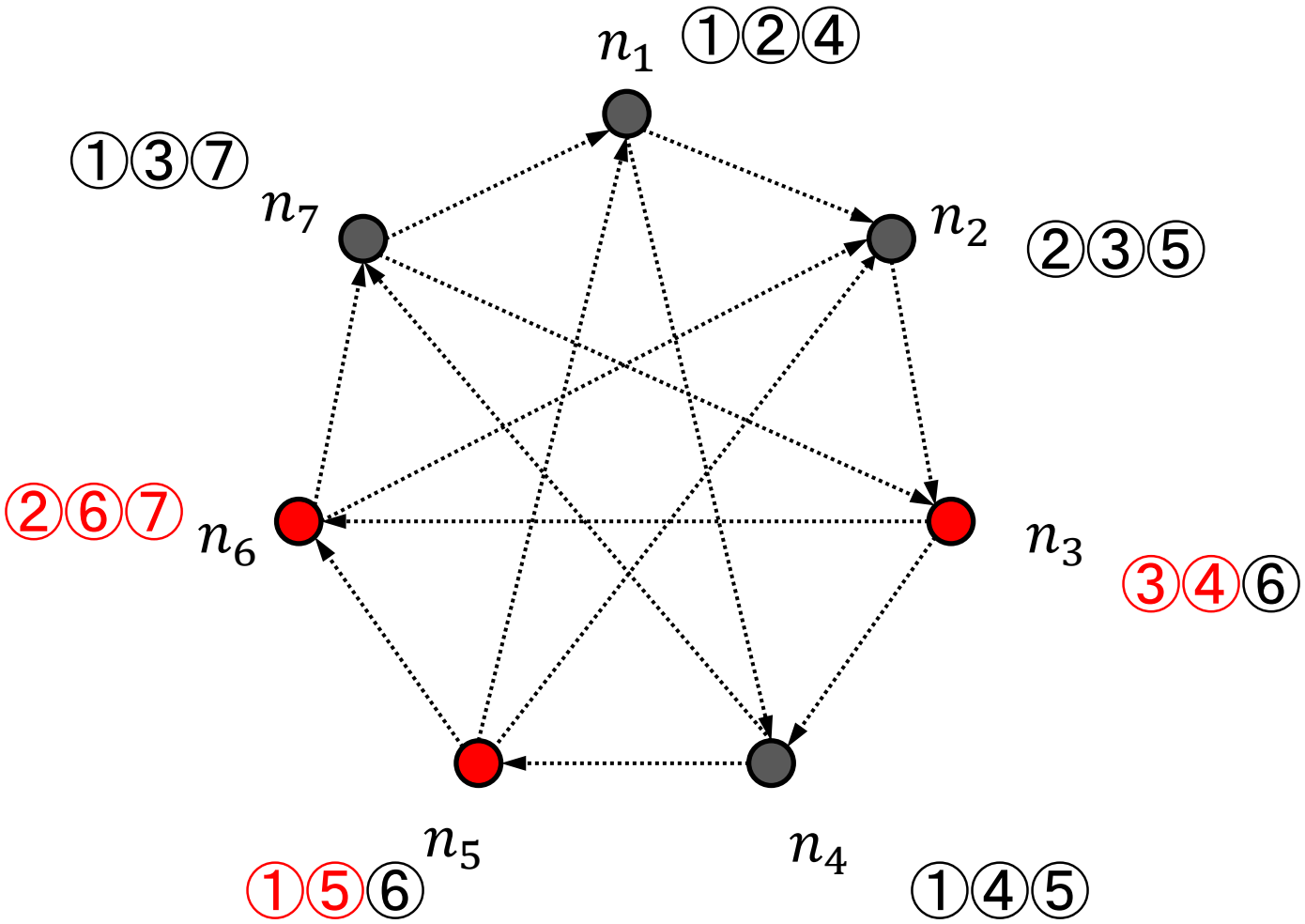
BIBD based multi-broadcast update



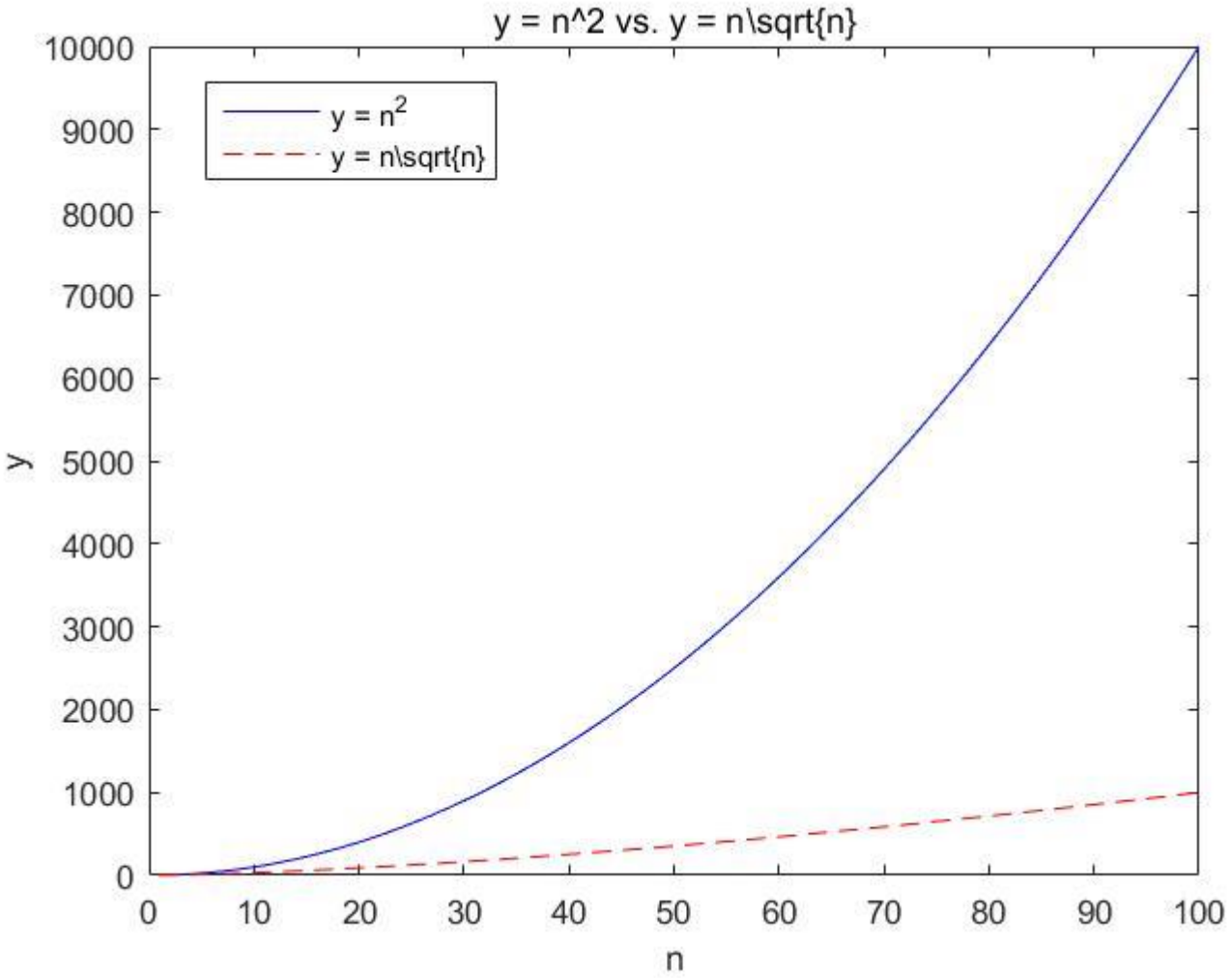
BIBD based multi-broadcast update



BIBD based multi-broadcast update



Performance



Future Work

- Improved BIBD structure
- MEC for Access Control
- Access Control for MEC

Q & A

王 晨

wangchen@zstu.edu.cn

中国密码学会2023年青年论坛