NSS-SocialSec 2023

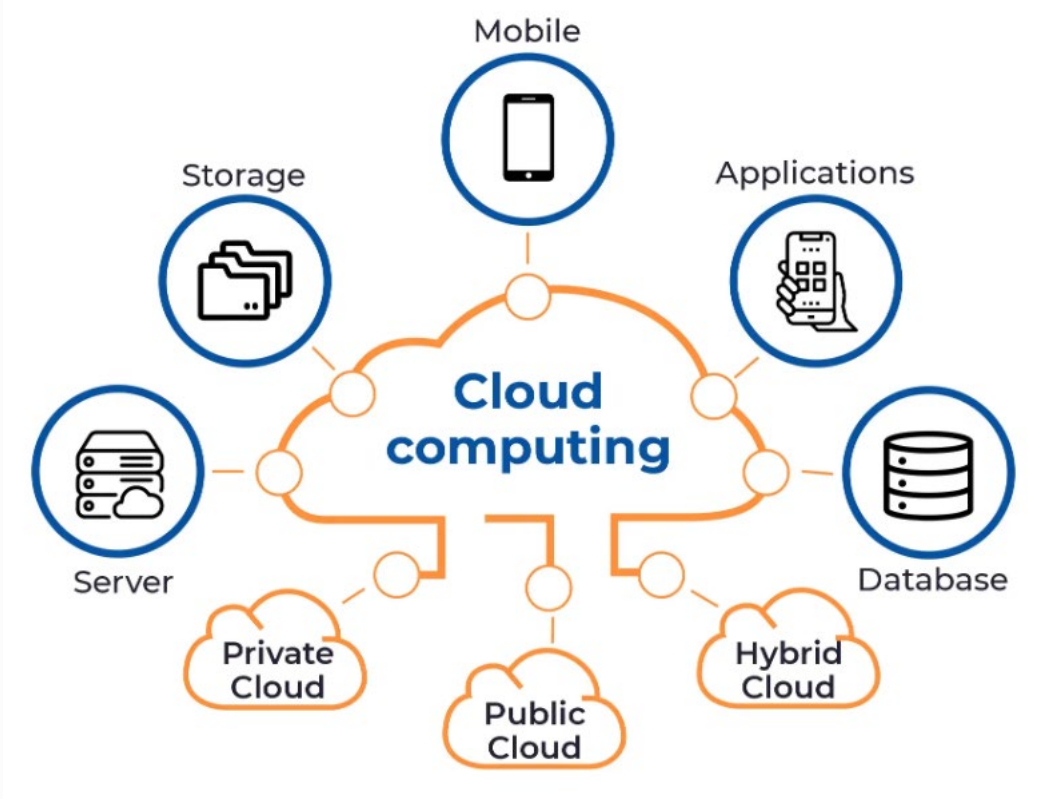
Secure and Efficient Data Processing for Cloud Computing with Fine-Grained Access Control

Jingjing Wang, Hao Feng, Zheng Yu, Rongtao Liao, Shi Chen,
and **Ting Liang**

Wuhan University of Technology
Wuhan, China

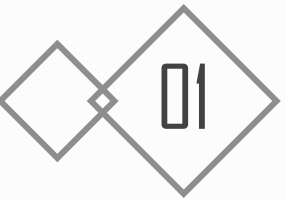
Background and Related Work

Cloud Computing



Cloud computing offers a flexible paradigm for data storage and processing.

Security is a crucial requirement!



Background

Desirable properties for data processing on the cloud platform.

- **Privacy preserving**

The cloud servers should be able to perform computations on the encrypted data without learning users' sensitive information.

- **Fine-grained access control**

Fine-grained access control should be enforced on the computed results.

- **Flexibility**

The identities who can access the computed results should be unknown when these results are generated.

- **Efficiency**

Low overheads on both computation and communication.

Related Works

Privacy preserving data processing

- **Multiparty computation**

Some applications: federated learning , computation of biomedical data, and collision avoidance for satellite.

Limitation: for general purpose MPC, it is impractical for large scale applications due to the heavy overheads in computation and communication.

- **Homomorphic encryption**

Fully homomorphic encryption: supports both addition and multiplication, but it needs large size of key and high storage overheads.

Partial homomorphic encryption: only supports either addition or multiplication, but it is more efficient. Many have been deployed in large scale applications.

Related Works

Fine-grained access control

- **Proxy re-encryption (PRE)**

Lack of flexibility: some schemes [1] require that the identities who can access the computed results are known in advance before these results being generated.

- **Attribute-based encryption (ABE)**

more flexible, but it suffers some limitations.

Lack of homomorphic property: most existing ABE schemes do not have the additive homomorphic property.

Low efficiency: computational overheads are relatively high when the access structure is complex, because the size of ciphertexts and the decryption time are proportional to the number of attributes.

[1] Zhang, W., Liu, S., Xia, Z.: A distributed privacy-preserving data aggregation scheme for smart grid with fine-grained access control. J. Inf. Secur. Appl. 103–118 (2022)

Our Contributions

- **Security:**

Privacy preserving. allows users' encrypted data to be processed without leaking their sensitive information

Fine-grained access control. achieves fine-grained access control for the computed results in a flexible way

Flexibility. the identities who can access the computed results can be configured after these results are generated.

- **Efficiency:**

More efficient than the state-of-the-art schemes that satisfy similar properties.

In particular, the size of ciphertexts and the decryption time for the computed results can be made constant in our scheme, regardless the access structure.

Preliminaries

Preliminaries

➢ A Homomorphic Encryption Scheme - BCP scheme [2]

Features: **1) double trapdoors: the master trapdoor can decrypt any ciphertext, a user's trapdoor can only decrypt the ciphertexts under her public key.**

2) It can be extended into a proxy re-encryption scheme.

Initialization. Given the security parameter κ, chooses two large safe primes p, q, such that $p = 2p' + 1, q = 2q' + 1$ $n = pq$ and $\lambda = p'q'$.

Let $\mathbb{G} = \mathsf{QR}_{n^2}$ be the cyclic group of quadratic residues modulo n^2, $\mathsf{ord}(\mathbb{G}) = n\lambda$

Then, one randomly chooses $\alpha \in \mathbb{Z}^*_{n^2}$ and compute $g = \alpha^2 \bmod n^2$. Publish (n, g)

Key generation. Chooses private key $a \in [1, \mathsf{ord}(\mathbb{G})]$ and sets public key $h = g^a \bmod n^2$

Encryption. randomly chooses $r \in [1, \mathsf{ord}(\mathbb{G})]$ and computes $C = (A, B)$ as:

$$A = g^r \bmod n^2 \qquad B = h^r(1+n)^m \bmod n^2$$

Decryption. The user can decrypt the ciphertext using her private key as: $m = \dfrac{B/A^a - 1 \bmod n^2}{n}$

[2] Bresson, E., Catalano, D., Pointcheval, D.: A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications. In: Laih, C.-S. (ed.) ASIACRYPT 2003. LNCS, vol. 2894, pp. 37–54. Springer, Heidelberg (2003).

Preliminaries

➢ A Homomorphic Re-encryption Scheme

Extend the BCP scheme into a proxy re-encryption scheme.

Initialization. Same as in the BCP scheme.

Key generation. Two proxies generate their key pairs.

One selects $a \in [1, \mathsf{ord}(\mathbb{G})]$ and sets $h_a = g^a$ .The other selects $b \in [1, \mathsf{ord}(\mathbb{G})]$, and sets $h_b = g^b$.

They negotiate a Diffie-Hellman key $h = {h_a}^b = {h_b}^a = g^{ab}$

Encryption. Same as in the BCP scheme, and the message is encrypted under the public key h.

Proxy re-encryption. re-encrypt $(A, B) = (g^r, h^r(1+n)^m)$ under h to a ciphertext under $\hat{h}$.

the first proxy computes $\sigma_1 = \mathsf{H}(\hat{h}^a)$ and $(A', B') = (A^a g^{\sigma_1}, B)$, and sends to the other proxy.

the second proxy computes $\sigma_2 = \mathsf{H}(\hat{h}^b)$ and $(A'', B'') = ({A'}^b g^{\sigma_2}, B')$, and sends the result to the designated recipient with public key $\hat{h}$.

Decryption. The recipient can decrypt the ciphertext (A'', B'') by computing

$$\sigma_1 = \mathsf{H}({h_a}^x),\ \sigma_2 = \mathsf{H}({h_b}^x) \text{ and } m = \frac{B'' \cdot {h_b}^{\sigma_1} \cdot g^{\sigma_2} / A'' - 1 \bmod n^2}{n}$$

➢ An Efficient ABE Scheme [3]

The size of ciphertext and the number of bilinear pairing operations remain constant in the decryption process.

Setup.

Choose: (e, g, p, G_1, G_2) Choose: $\alpha, a \in Z_P$, calculates :$Y = e(g,g)^{\alpha}$, g^a

$PK = (e, g, g^a, Y, h_1, h_2, \ldots, h_{3n})$, $MK = (g^{\alpha}, a)$.

KeyGen.

Choose:$r, c \in Z_P$, Set $L' = c$, calculate: $D = g^{-r}, L = g^{-ar}$

User attribute set S, system attribute set U:

For $i \in U, i \in S, \overline{i} = +i$, calculates :$D_i = {h_i}^r$

For $i \in U, i \notin S, \overline{i} = -i$, calculates :$D_i = {h_{n+i}}^r$

For $i \in U$:calculates :$F_i = {h_{2n+i}}^r$

chooses a random $j \in U$, computes: $D_j' = g^{\alpha/(a+c)} \cdot D_j$, $F_j' = g^{\alpha/(a+c)} \cdot F_j$

$SK = (D, L, L', \{D_i, F_i\}_{i \in U})$

[3] Li et al.: TRAC: traceable and revocable access control scheme for m-health in 5G-enabled IIoT. In IEEE Transactions on Industrial Informatics, 18(5):3437–3448, 2021.

➢ An Efficient ABE Scheme

The size of ciphertext and the number of bilinear pairing operations remain constant in the decryption process.

Encrypt.

access structure :$W = \wedge_{i \epsilon I}\ \bar{i}$

For $i \in I, \bar{i} = +i$, set $H_i = h_i$

For $i \in I, \bar{i} = -i$, set $H_i = h_{n+i}$

For $i \in U \backslash I$, set $H_i = h_{2n+i}$

Picks s $\epsilon\ Z_P$, computes $C = Me(g,g)^{\alpha s}$, $C_1 = g^s$, $C_2 = g^{as}$, $C_3 = (\prod_{i \in U} H_i)^s$

$CT = (W, C, C_1, C_2, C_3)$.

Decrypt.

For $i \in I, \bar{i} = +i, i \in S$: $A_1 = \prod D_i$

For $i \in I, \bar{i} = -i, i \notin S$: $A_2 = \prod D_i$

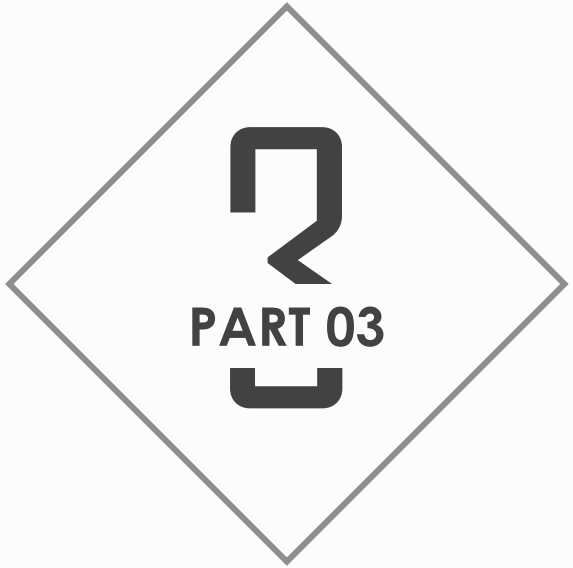
For $i \notin I$: $A_3 = \prod_{i \in U \backslash \mathrm{I}} F_i$

$M = C/K$

$$K = e\left(A_1 \cdot A_2 \cdot A_3, {C_1}^{L'} \cdot C_2\right) \cdot e\left(D^{L'} \cdot L, C_3\right)$$

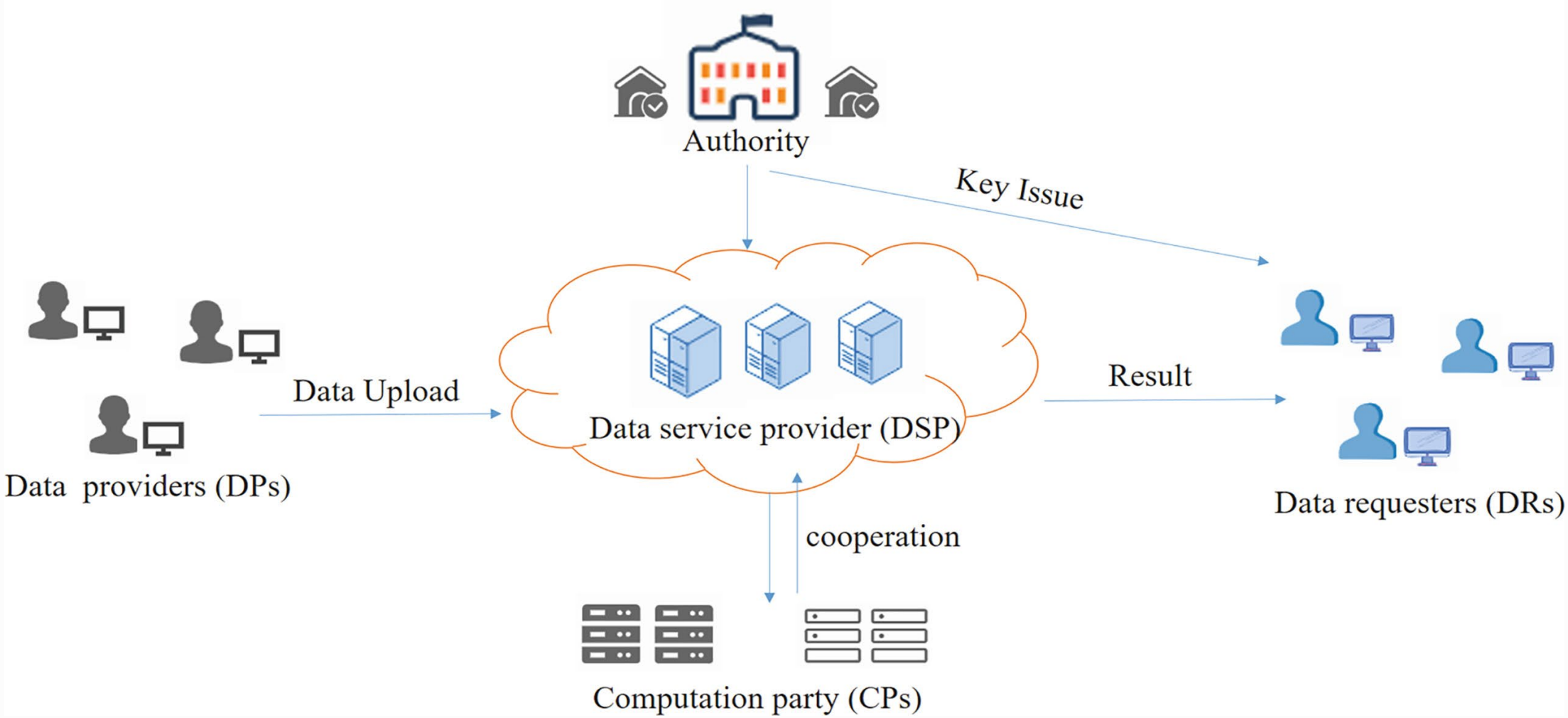
$$= e\left(g^{\frac{\alpha}{a+c}}, g^{s(a+c)}\right) \cdot \prod_{i \in I, \bar{i} = +i} e\left({h_i}^r, g^{s(a+c)}\right) \cdot \prod_{i \in I, \bar{i} = -i} e\left({h_{n+i}}^r, g^{s(a+c)}\right) \cdot \prod_{i \in U \backslash I} e\left({h_{2n+i}}^r, g^{s(a+c)}\right) \cdot e\left(g^{-r(a+c)}, (\prod_{i \in U} H_i)^s\right)$$

$$= e(g,g)^{\alpha s}$$



Models and Definitions

System Model



Communication Model & Adversary Model

➢ Communication Model

- Secure channels exist between the authority and the DRs
- Secure channels exist between the DSP and the CP.
- All other communications are exchanged through authenticated channels.

➢ Adversary Model

The authority is assumed to be fully trustworthy. All other entities are assumed to be semi-honest.

Adversary's capabilities

- $\mathcal{A}$ can eavesdrop the exchanged messages on the authenticated channels, but it cannot eavesdrop on the secure channels.
- $\mathcal{A}$ may compromise the DSP or the CP, but not both, with the purpose of learning DP's sensitive information or the computed results.
- $\mathcal{A}$ may compromise some DRs, trying to combine their attributes to form a larger set so that it can access the computed results that none of these DRs is authorized.

Security Requirements

Correctness. If all participants honestly follow the protocol, the uploaded encrypted data can be processed in the privacy preserving way and the computed results can only be decrypted by the designated recipient.

Privacy preserving. The adversary can neither learn the data stored in the cloud platform nor the computed results output by the CP.

Fine-grained access control. Only the designated recipient whose attributes satisfy the access structure can decrypt the computed results.

Flexibility. The identities who can access the computed results should be unknown when these results are generated, i.e. some parties can register after the computed results are generated and still be able to decrypt them.

Collusion resistance. The DRs cannot collude to gain more decryption privilege by combining their attributes..

PART 04

The Proposed Scheme

The Proposed Scheme -- overview

System setup.

Given the security parameter, the authority initializes both the PRE scheme and the ABE scheme.

Key generation. (1) The DSP and the CP each generates a key pair in the PRE scheme. (2) They also negotiate a Diffie-Hellman key as the system-wide public key. (3) Each DR registers with the authority, and receives her private key.

Encryption. Each DP can encrypt her data using the BCP scheme, and uploads it to the cloud platform..

Data processing. The DSP can perform data analysis and data mining using the stored data..

Proxy re-encryption I. The DSP performs partial decryption as well as re-encryption on the computed results.

Proxy re-encryption II. The CP continues to perform partial decryption and re-encryption on the computed results.

Decryption. Only the designated recipients whose attributes satisfy the access structure can decrypt the computed results.

The Proposed Scheme

System setup.

Publishes the public parameters $PK = (\bar{g}, n, \mathbb{G}, e, g, G_1, G_2, Y, g^a, h_1, h_2, \ldots, h_{3k}, \mathsf{H}, \mathsf{H}')$

Keeps the master secret key private $MK = (g^\alpha, a)$

Key generation.

(1) DSP chooses $x \in [1, \mathsf{ord}(\mathbb{G})]$, sets $pk_{DSP} = \bar{g}^x$.

(2) CP chooses $y \in [1, \mathsf{ord}(\mathbb{G})]$, sets $pk_{CP} = \bar{g}^y$.

(3) They negotiate a Diffie-Hellman key $\bar{h} = pk_{DSP}{}^{sk_{CP}} = pk_{CP}{}^{sk_{DSP}} = \bar{g}^{xy}$

(4) Each DR obtain her private key $SK = (D = g^{-r}, L = g^{-ar}, L' = c, \langle D_i, F_i \rangle \mid i \in U)$

Encryption. Each DP encrypts its data $m_i \in \mathbb{Z}_n$, uploads the ciphertext $(A, B) = (\bar{g}^r, h^r(1+n)^m)$

Data processing. The DSP processes the encrypted data. Suppose result is $(\bar{g}^r, \bar{h}^r(1+n)^{m_i})$

The Proposed Scheme -- continue

Proxy re-encryption I.

(1) DSP selects $w_1 \in G_2$, encrypts it with ABE as $CT_1 = (W, C, C_1, C_2, C_3)$

(2) Transform the ciphertext (A,B) into $(A', B') = (\bar{g}^{xr}, h^r(1+n)^{m+\sigma_1})$

Proxy re-encryption II.

(1) CP selects $w_2 \in G_2$, encrypts it with ABE as $CT_2 = (W, C', C_1', C_2', C_3')$

(2) Transform the ciphertext (A', B') into $(A'', B'') = (\bar{g}^{x\bar{y}r}, \bar{h}^r(1+n)^{m+\sigma_1+\sigma_2})$

Decryption. Only

(1) DR first computes $m' = m + \sigma_1 + \sigma_2$ $m' = \dfrac{B''/A'' - 1 \bmod n^2}{n}$

(2) It decrypts CT_1 and CT_2, obtaining w_1 and w_2.

$$w_1 = \frac{C}{e(A_1 \cdot A_2 \cdot A_3, C_1^{L'} \cdot C_2) \cdot e(D^{L'} \cdot L, C_3)}$$

(3) plaintext m can be derived, $m = m' - \mathsf{H}'(w_1) - \mathsf{H}'(w_2) \bmod n$

Security Analyses

Security Analyses

➢ Privacy.

Adversary A cannot learn any information in our proposed scheme.

(1) A can not learn information from DP's uploaded encrypted data.

DP's uploaded data is encrypted using the BCP scheme, and this scheme is semantic secure under the DDH assumption over $\mathbb{Z}_{n^2}^*$

(2) A can not learn information from the transformed ciphertext.

The transformed ciphertexts are encrypted using an ABE scheme that is semantic secure under the *l*-BDHE assumption.

Security Analyses

- **Fine-grained access control**

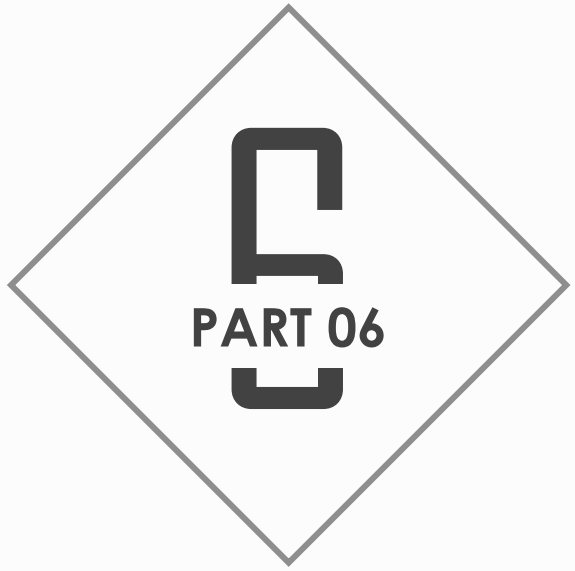
  After the proxy re-encryption, the computed result is blinded by two random values σ_1, σ_2, and these two values are encrypted by an ABE scheme. Hence, only the parties whose attribute satisfy the access structure can decrypt them and derive the computed result.

- **Flexibility**

  Proxy re-encryption is used to transform a ciphertext into an ABE ciphertext. In this way, the identities do not need to be known by the time these results are generated, and users can join afterwards.

- **Collusion resistance**

  When generating private keys for the DRs, the authority will assign a unique value r for each DR. Therefore, the private keys for different DRs will be associated with different values. Hence, they cannot put their attributes together to form a larger attribute sets.



Efficiency Analyses

Communication Costs

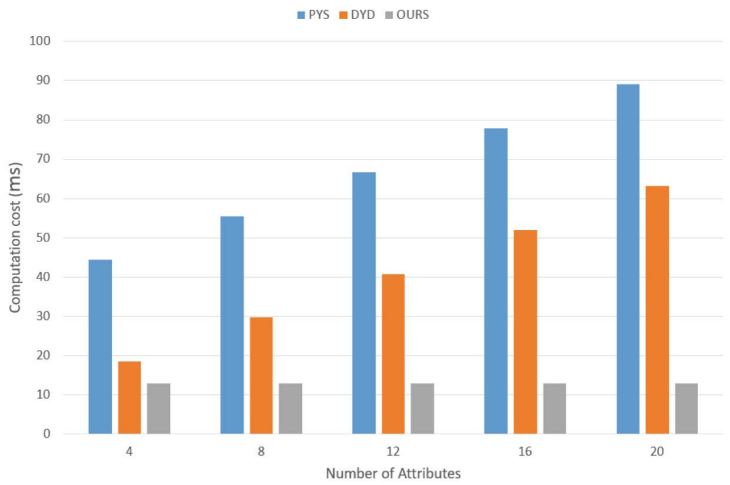
Table 1. Comparison of communication costs

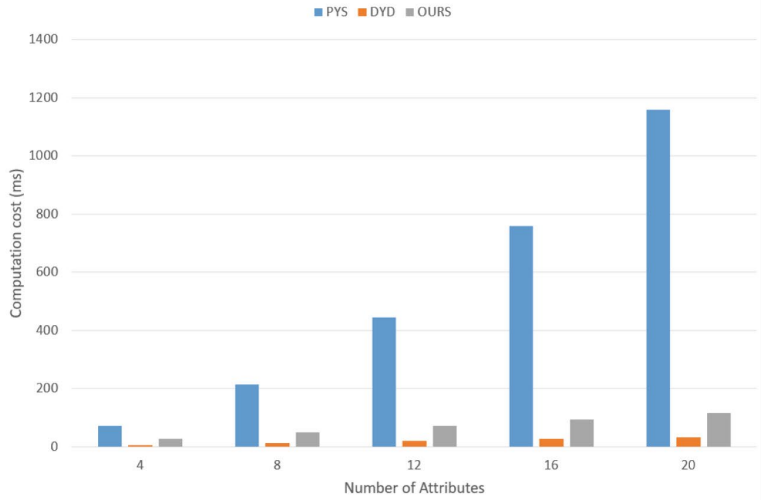
	Public parameters	Ciphertext	Secret Key
PYS Scheme	$(n+4)\|G_1\| + 2\|G_2\|$	$3\|G_1\| + \|G_2\| + \|W\|$	$(n+6)\|G_1\|$
DYD Scheme	$(n+1)\|G_1\| + \|G_2\|$	$\lambda\|G_1\| + \|G_2\| + \|W\|$	$\lambda\|G_1\|$
Our scheme	$(3n+2)\|G_1\| + \|G_2\|$	$3\|G_1\| + \|G_2\| + \|W\|$	$(2n+2)\|G_1\| + \|G_2\|$

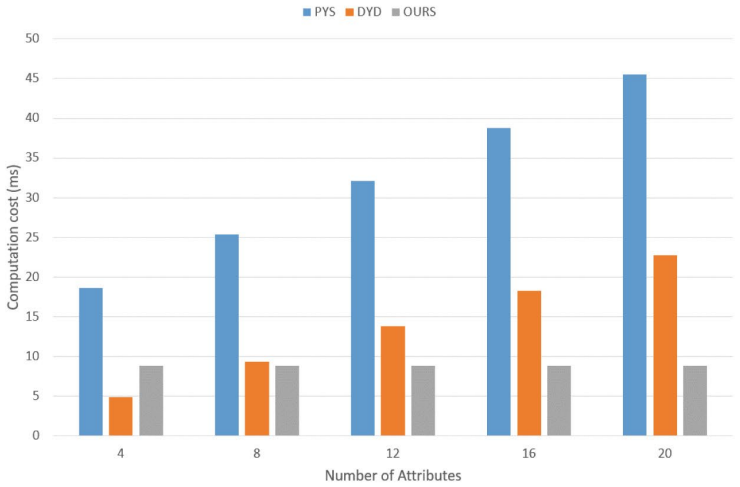
[PYS] Phuong et al.: Hidden ciphertext policy attribute-based encryption under standard assumptions. In IEEE transactions on information forensics and security, 11(1):35–45, 2015.

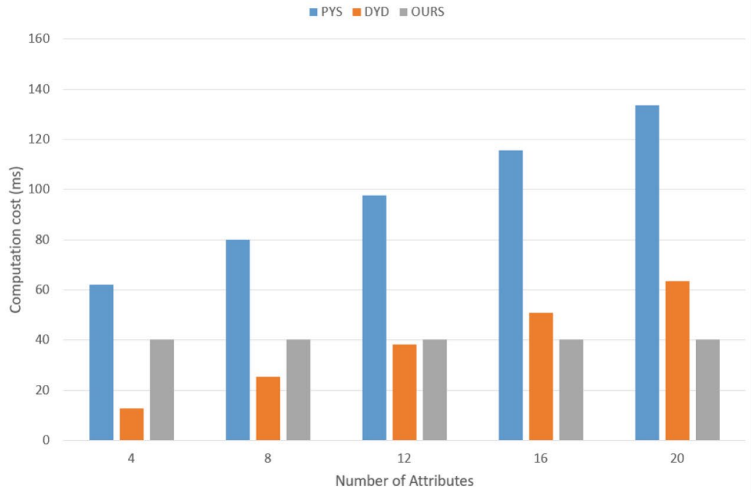
[DYD] Ding et al.: Privacy-preserving data processing with flexible access control. In IEEE Transactions on Dependable and Secure Computing, 17(2):363–376, 2020.

Computation Costs









Thanks!