Project on Secure Data Sharing and Distribution Platform for Integrated Big Data Utilization

Oct.2015-Mar.2021

Secure Data Sharing and Distribution Platform for Integrated Big Data Utilization

- Handling all data with encryption -

July 10th, 2018

Group Members

Waseda University Hayato YAMANA

Institute of Information Security Atsuhiro GOTO

Ochanomizu University Masato OGUCHI

Kogakuin University Saneyasu YAMAGUCHI

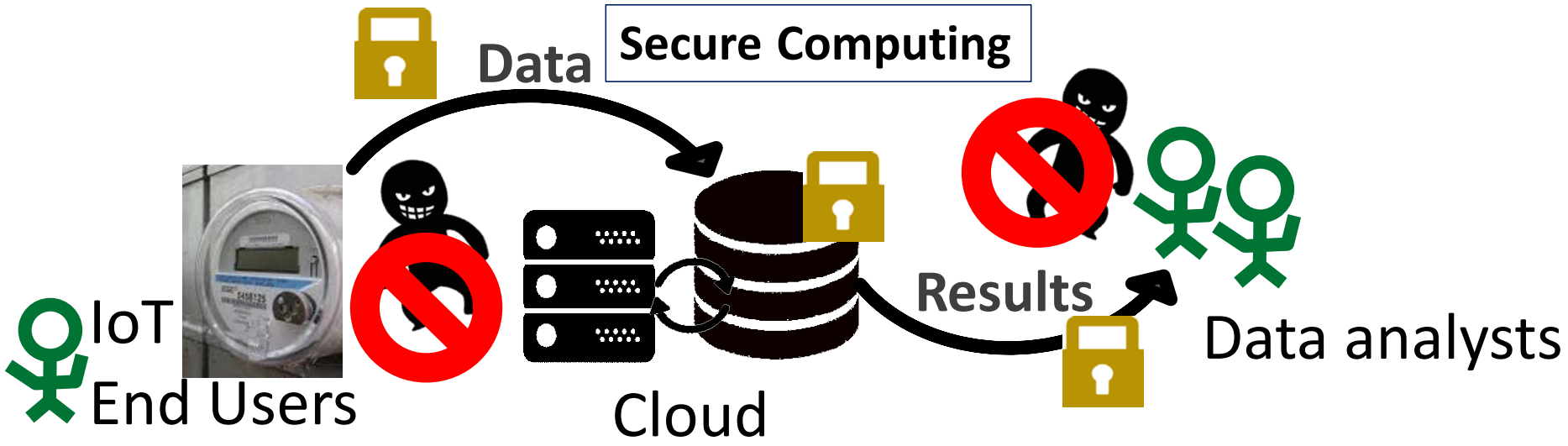
The University of Electro-Communications Takahiko SHINTANI

Meiji Pharmaceutical University Tamotsu NOGUCHI

Research Goals

SD² Platform for Integrated Big Data Utilization

HANDLING ALL DATA WITH ENCRYPTION
THROUGHOUT DATA LIFE CYCLE



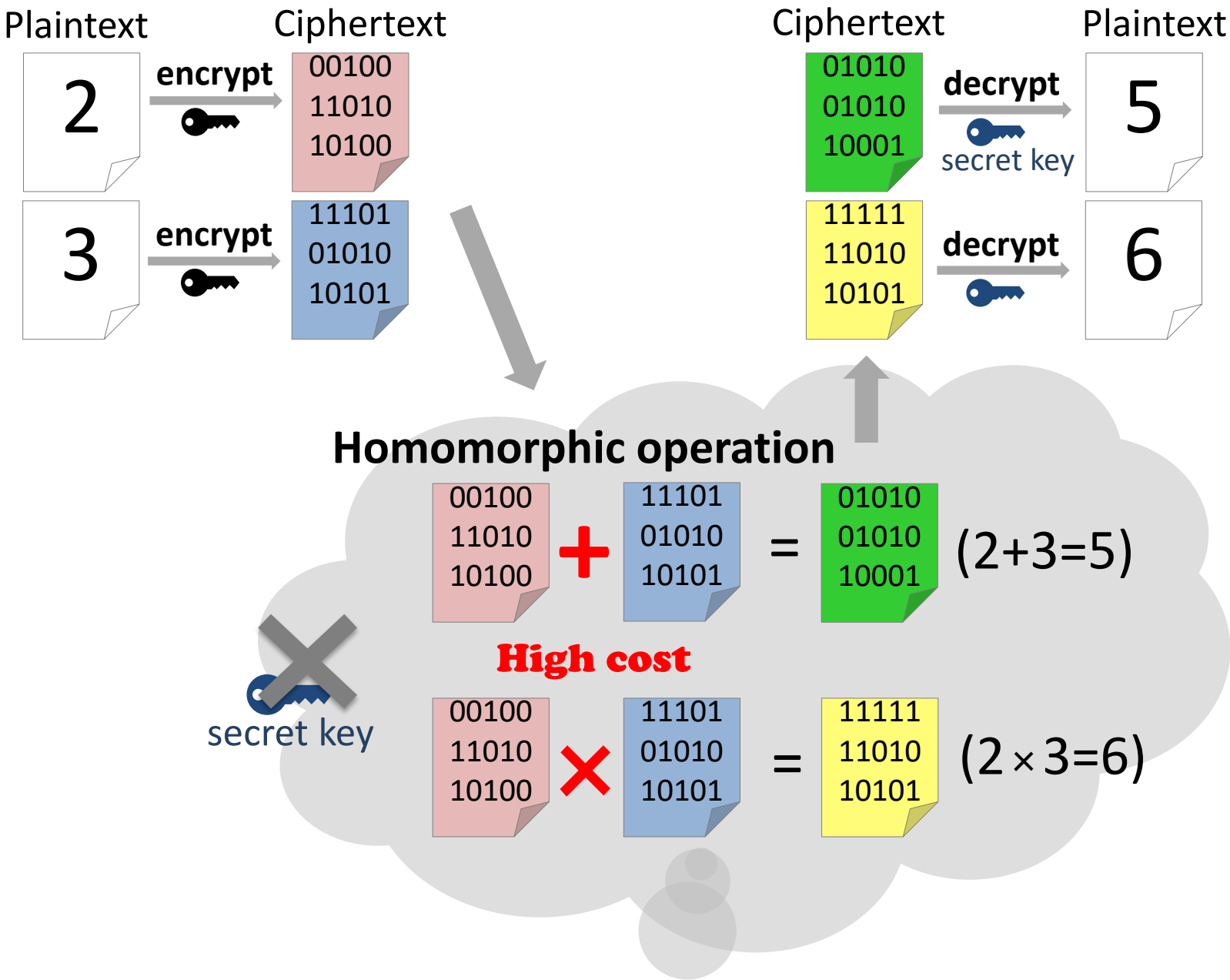
Solution: Crypto-system → preserving whole process
Fully Homomorphic Encryption (FHE)
Outsourcing and calc. over encrypted data
→ Currently too slow ($O(10^{10})$) to adopt

Subring Homomorphic Encryption

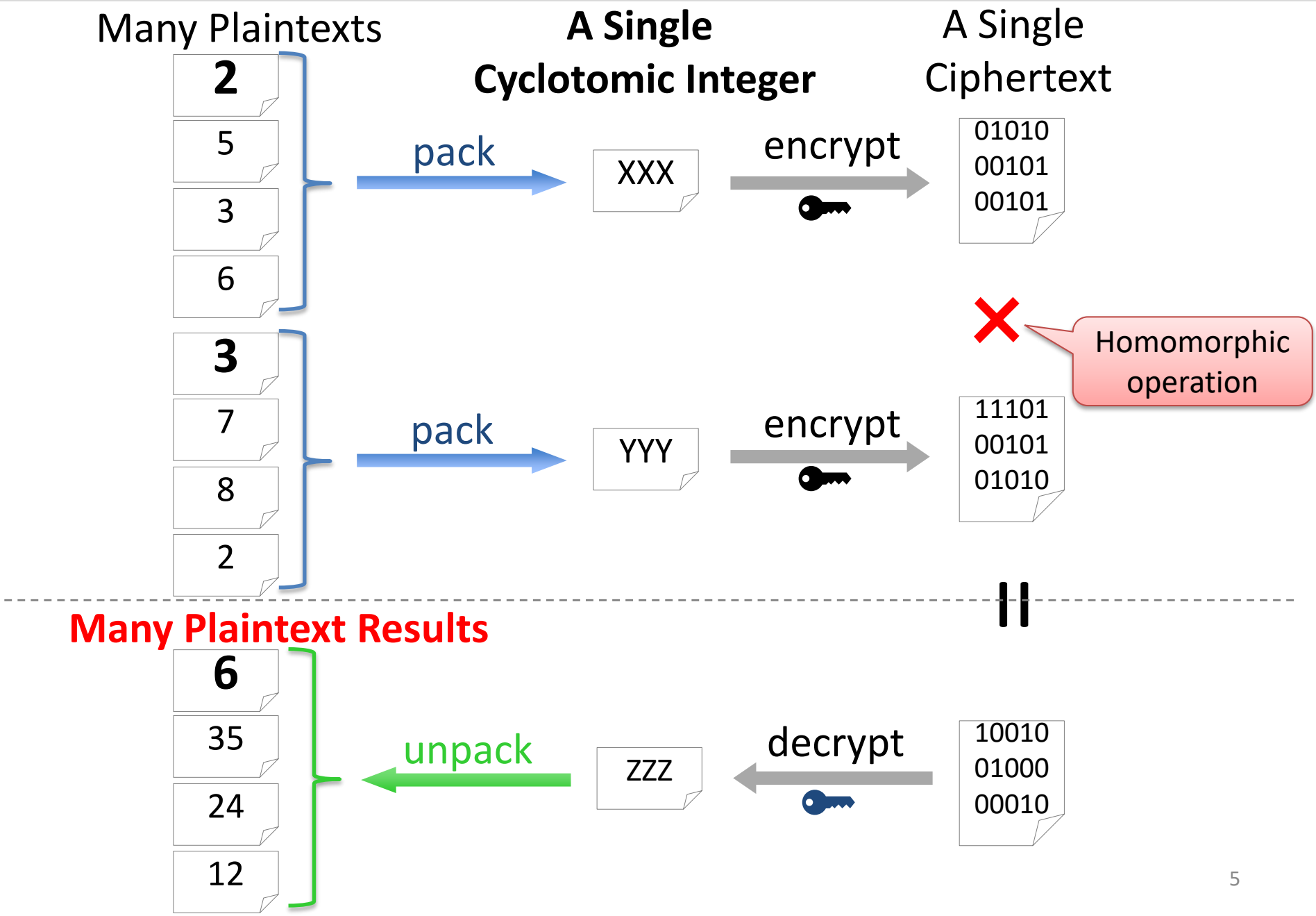
Seiko Arita[1] Sari Handa[1]

[1] Institute of Information Security, Yokohama, JAPAN

Homomorphic Encryption

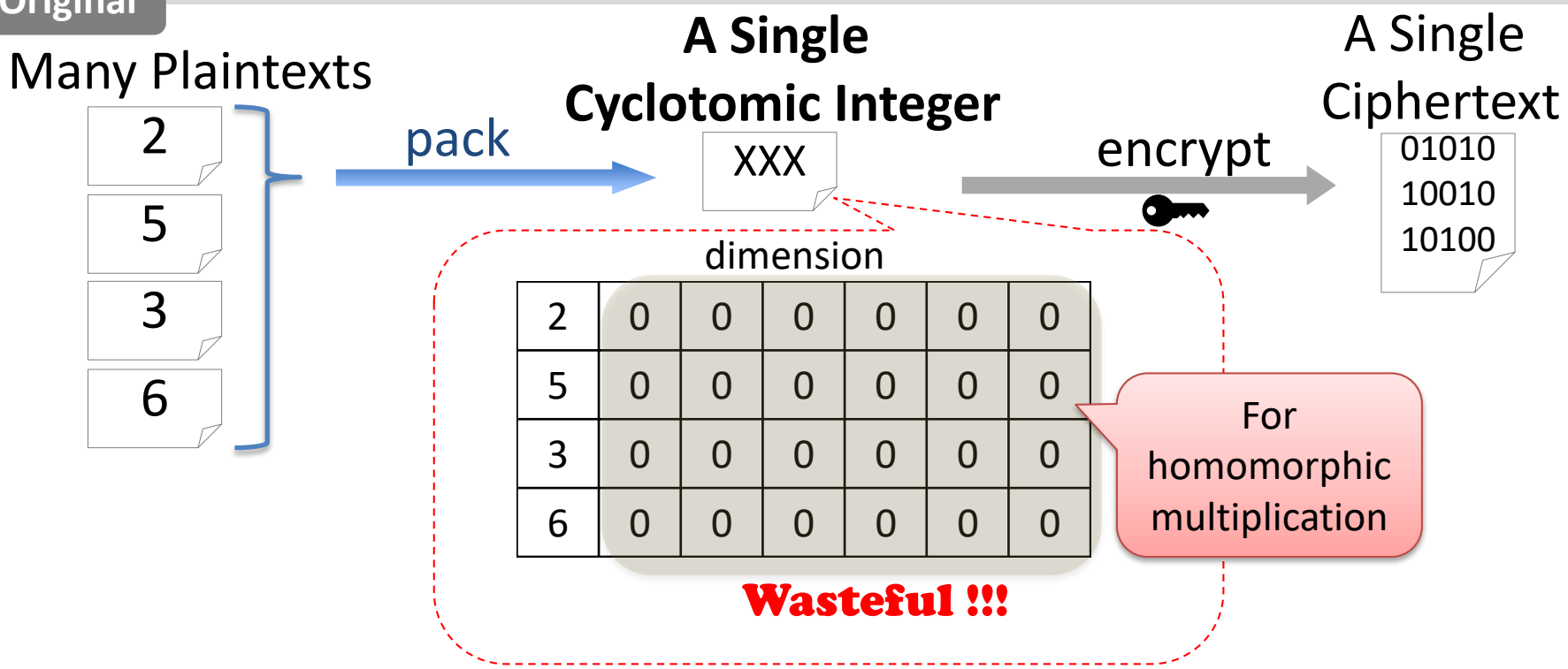


Parallel Computation



Original Structure

Original



Shrink Structure

Original

Many Plaintexts

2
5
3
6

pack

A Single Cyclotomic Integer

xxx

encrypt

A Single Ciphertext

01010
10010
10100

dimension

2	0	0	0	0	0	0
5	0	0	0	0	0	0
3	0	0	0	0	0	0
6	0	0	0	0	0	0

Shrink

Our approach

2
5
3
6

pack

x

encrypt

01010

More compact Ciphertext

An Integer of Subring

$\mathbb{Z}_p$ slots by Decomposition Ring

Original Many Plaintexts

$$\frac{R}{\mathfrak{P}_0} \oplus \cdots \oplus \frac{R}{\mathfrak{P}_{g-1}} \simeq \frac{R}{pR}$$

Cyclotomic Ring
$R=\mathbb{Z}[\zeta]$

$GF(p^d)$

Ours

Hensel Lift $\mathbb{Z}_{p^d}$

Integer

$$\mathbb{Z}_p \oplus \cdots \oplus \mathbb{Z}_p \simeq \frac{R_z}{pR_z}$$

subring

Decomposition Ring
$R_z \stackrel{\text{def}}{=} R^{G_z}$

G_z :Decomposition Group

$(\alpha_0, \cdots, \alpha_{g-1})$
$(\beta_0, \cdots, \beta_{g-1})$
Pack & Encrypt
a
b

Decrypt & Unpack
$(\alpha_0\beta_0, \cdots, \alpha_{g-1}\beta_{g-1})$
$a \times b$

Not Wasteful

Efficient homomorphic parallel computation!

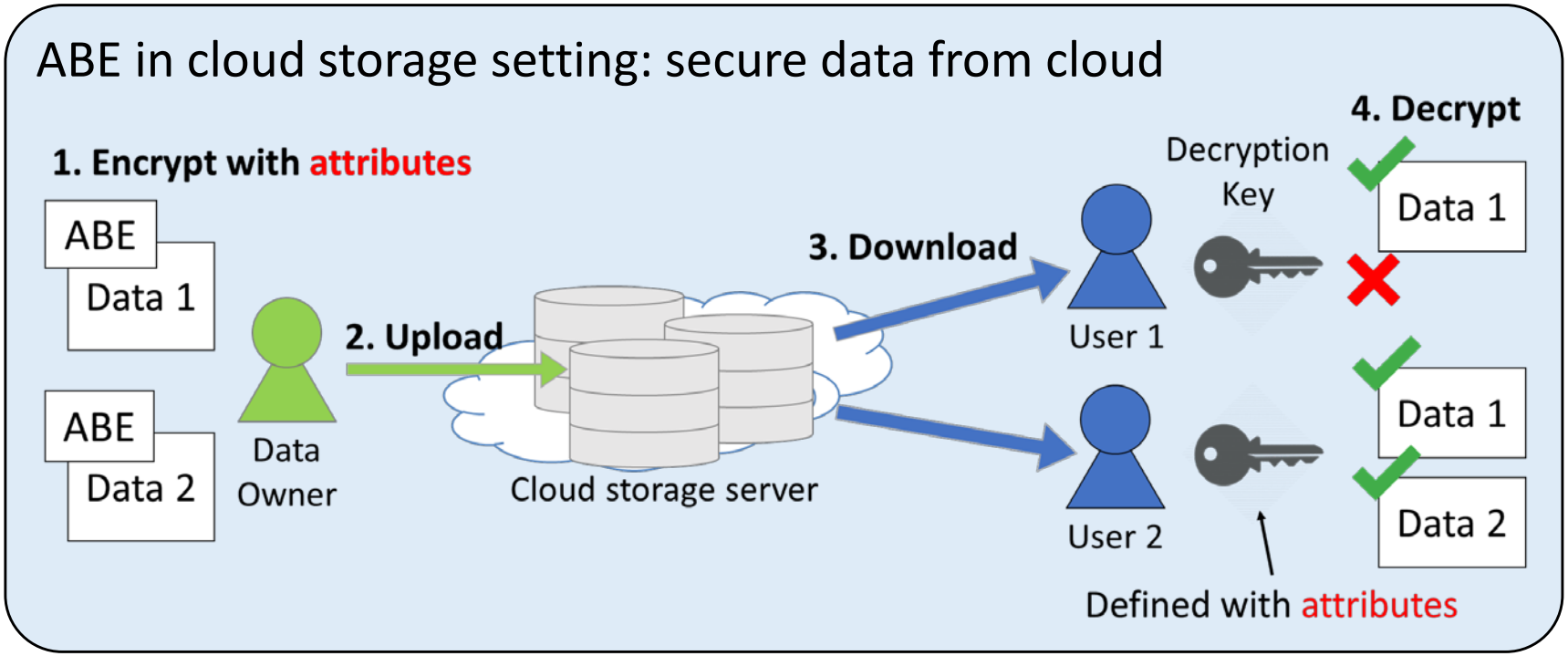
Attribute-based Proxy Re-encryption Method for Revocation in Cloud Data Storage

DATAIA-JST International Symposium on Data Science and AI @Paris
July 10th, 2018

Yoshiko Yasumura
Team Yamana, Waseda University, Japan
http://www.yama.info.waseda.ac.jp/crest/

Introduction

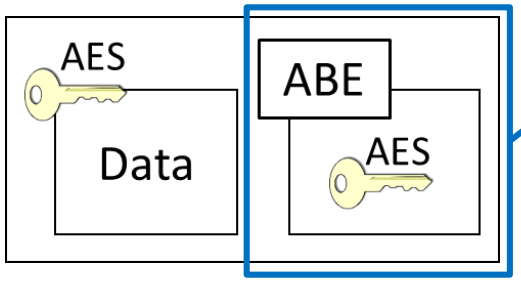
- **Attribute-based encryption (ABE)**
  - Secure and controlled data sharing



- Revocation: Remove users or their attributes
  - Necessary for real-world application

Problem

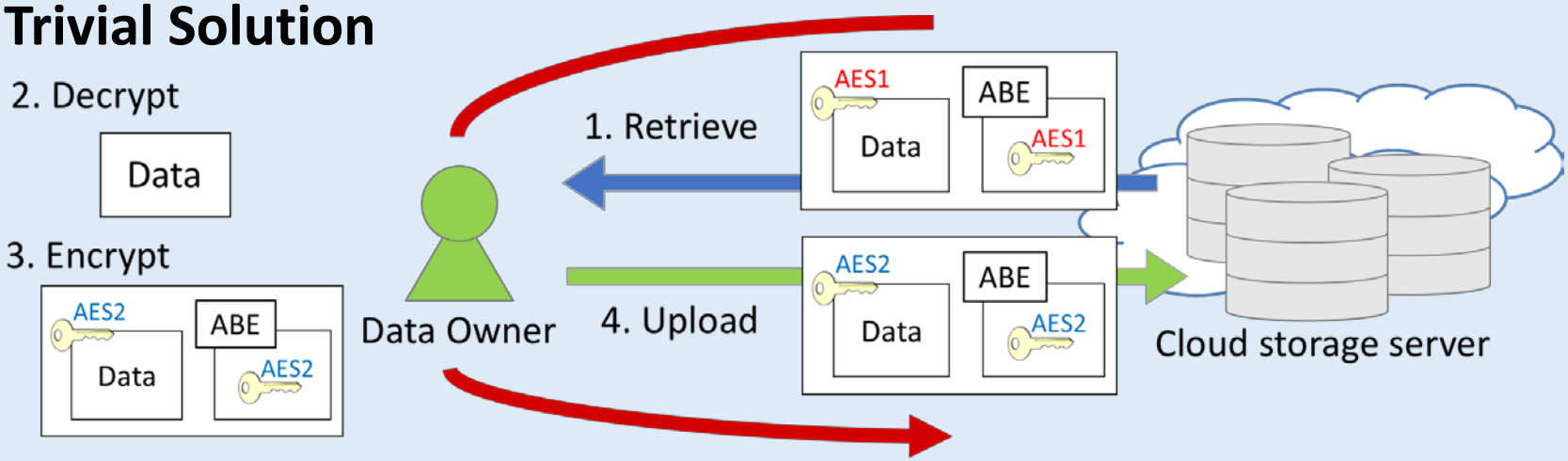
- Real world application uses ABE in hybrid with AES



Where revocation takes place

Data needs to be re-encrypted with a new AES key at revocation

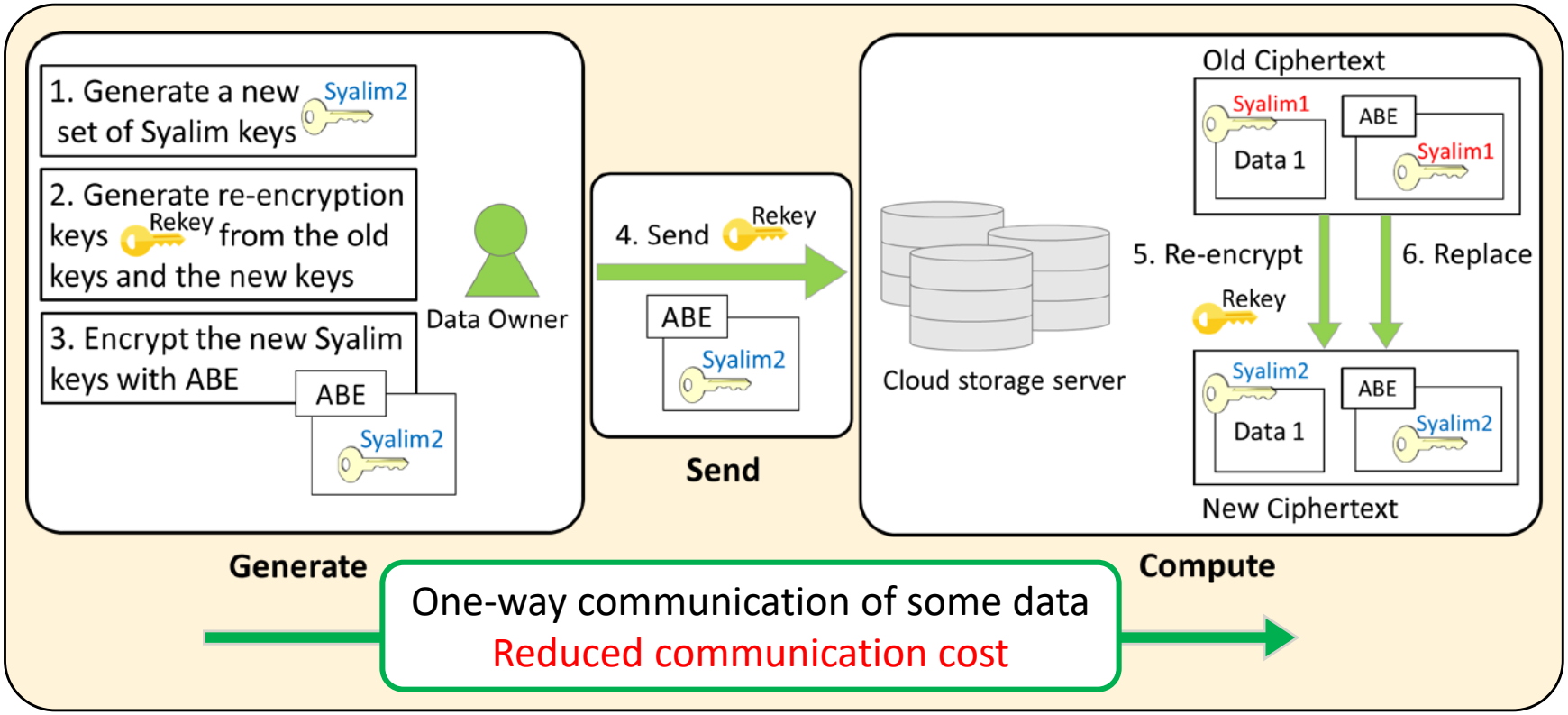
Trivial Solution



Huge communication cost and burden on data owner

Proposed Method

- Attribute-based proxy re-encryption method
  - Symmetric encryption scheme by Syalim et al. [SNS11] with ABE

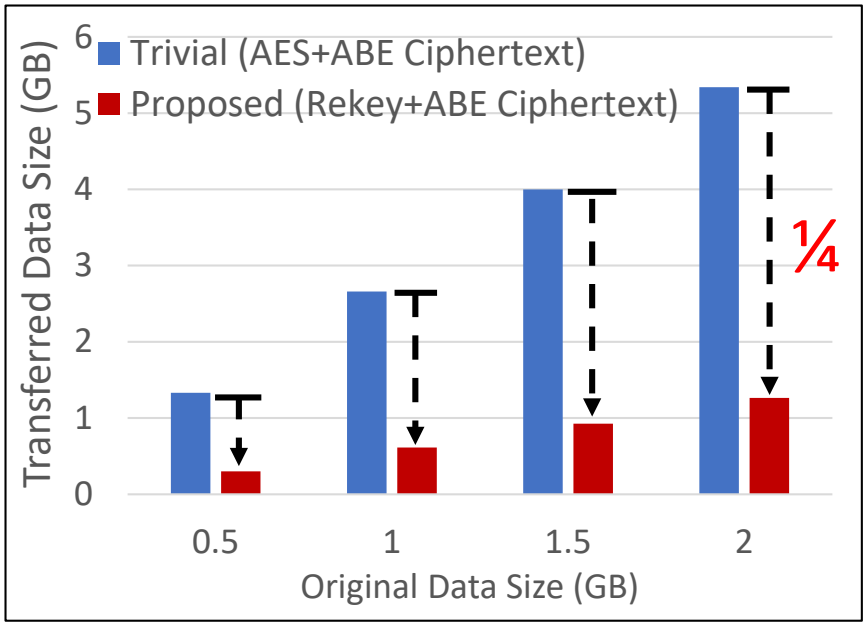


Yasumura, Yoshiko, Hiroki Imabayashi, and Hayato Yamana. "Attribute-based proxy re-encryption method for revocation in cloud storage: Reduction of communication cost at re-encryption." *2018 IEEE 3rd International Conference on Big Data Analysis (ICBDA),* pp. 312-318, 2018.

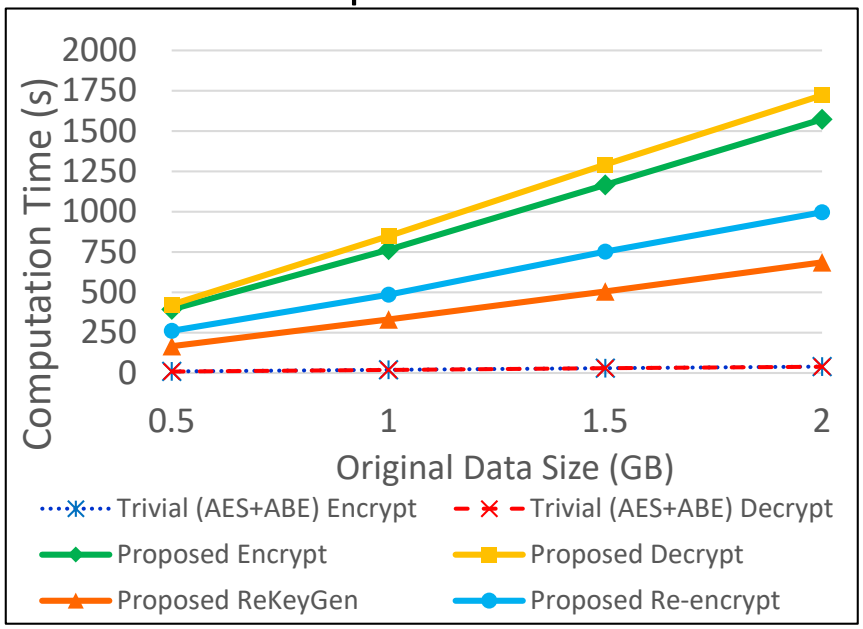
Experimental Results

- Lower communication cost but longer computation time
  - Suitable in some scenarios where large data must be re-encrypted

Communication Cost



Computation Cost

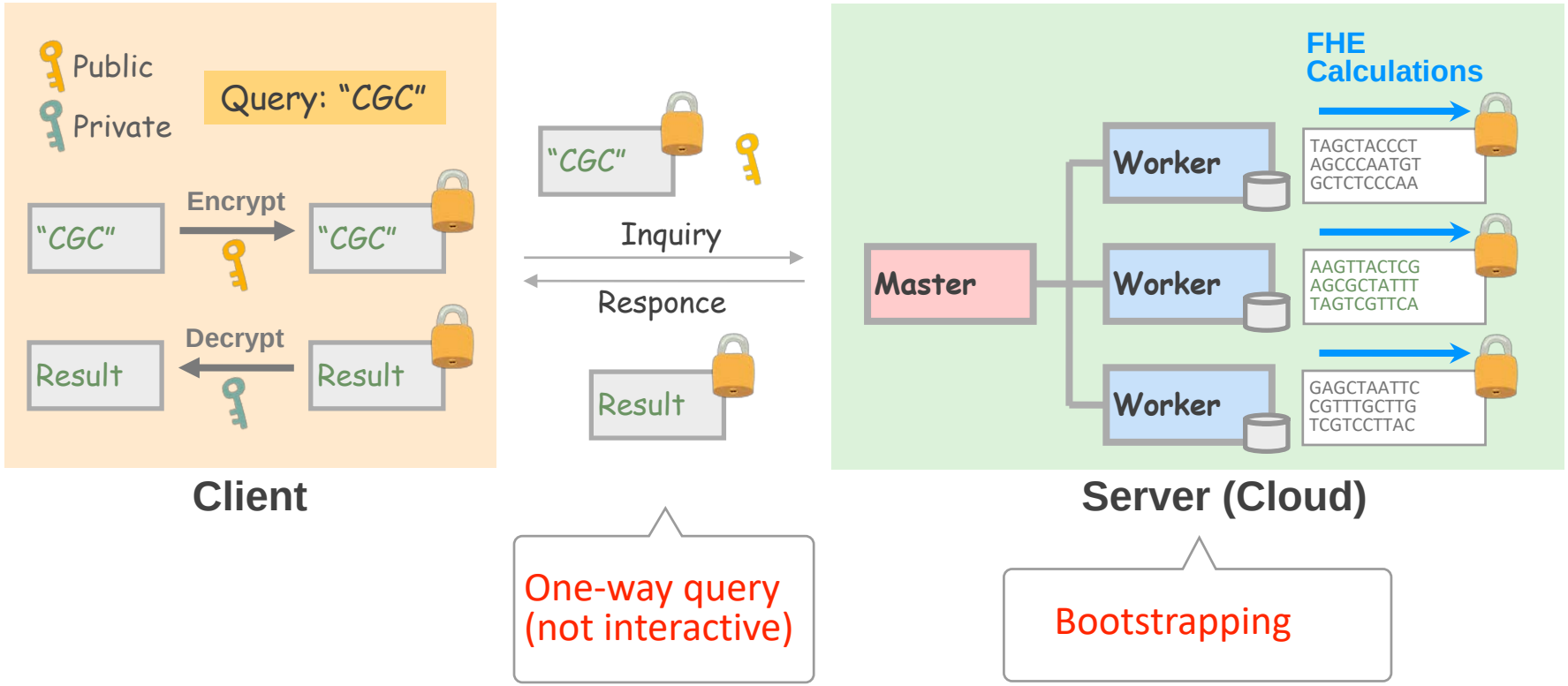


Distributed Platform of Privacy-Preserving Genome Search and Secure Data Mining

Masato Oguchi

Ochanomizu University, Japan

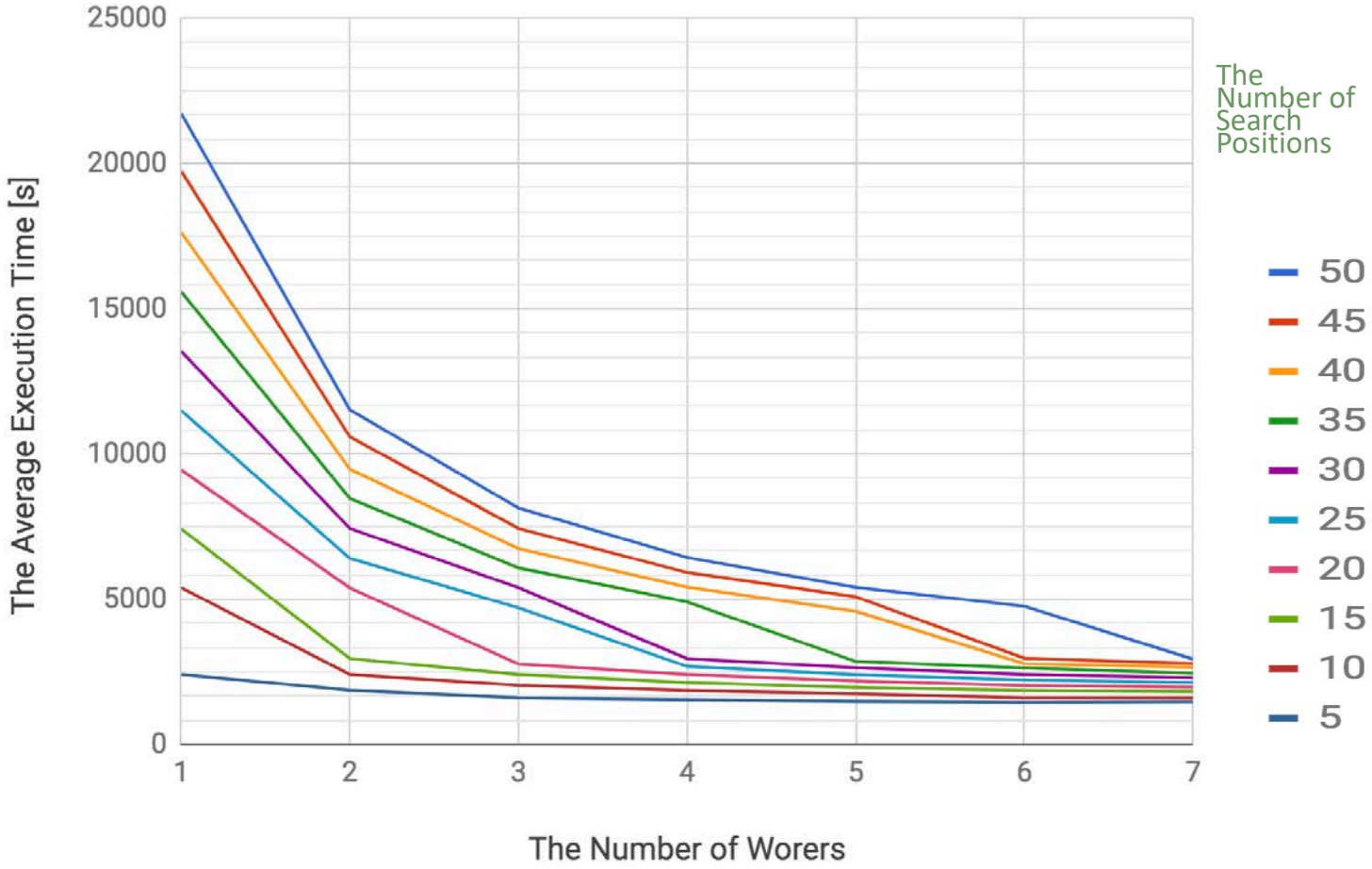
Proposed Method of Privacy-Preserving Genome Search on Distributed Platform



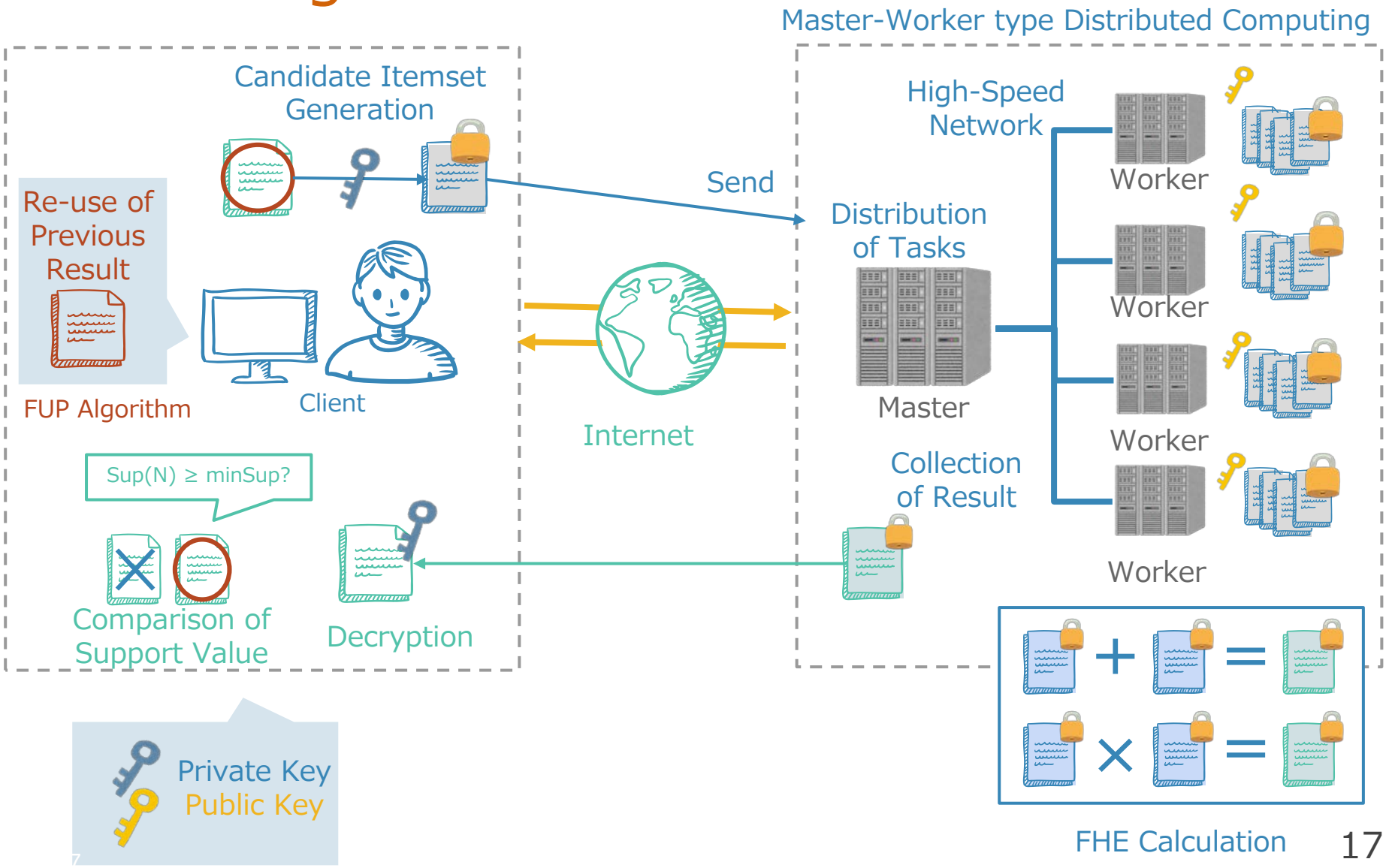
Evaluation Result

Execution Time in Each Number of Search Positions

Length of Query = 5, Number of Samples = 512



Proposed Method of Secure Data Mining on Distributed Platform



Evaluation Result of Secure FUP Algorithm

- Comparison of Re-Calculation of Secure Apriori and Secure FUP algorithm