차세대 암호기술: 함수암호

Functional Encryption

2021.05.26.

덕성여자대학교
서 민 혜
mhseo@duksung.ac.kr

Contents

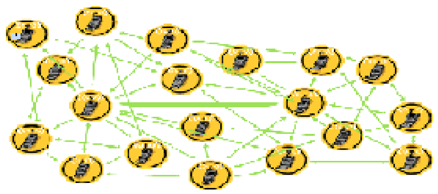
- **History of Cryptography**
- **Functional Encryption**
  - Definition
  - Related Work
  - Simple Scheme
- **Applications**

History of Cryptography

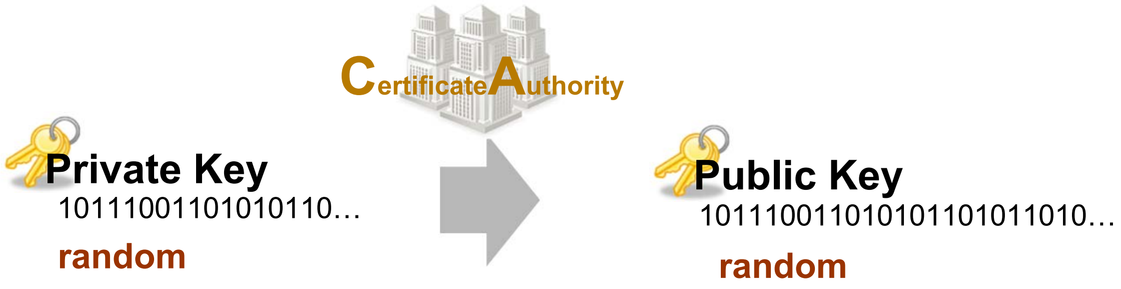
1940	● Symmetric-Key Encryption
1970	● Public-Key Encryption
2000	● Identity-Based Encryption (IBE)
2005	● Attribute-Based Encryption (ABE)
2011	● Functional Encryption (FE)

History of Cryptography

- 1940 Symmetric-Key Encryption



- 1970 Public-Key Encryption

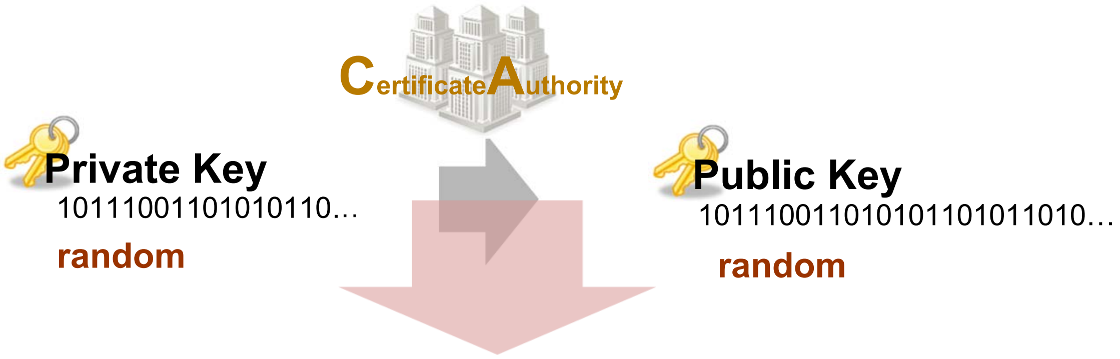


- 2000 Identity-Based Encryption (IBE)
- 2005 Attribute-Based Encryption (ABE)
- 2011 Functional Encryption (FE)

History of Cryptography

1940 ● Symmetric-Key Encryption

1970 ● Public-Key Encryption

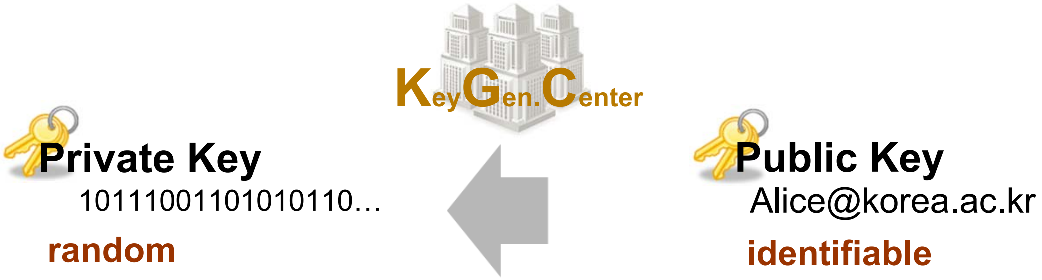


CertificateAuthority

Private Key
101110011010101110…
random

Public Key
1011100110101011010110 10…
random

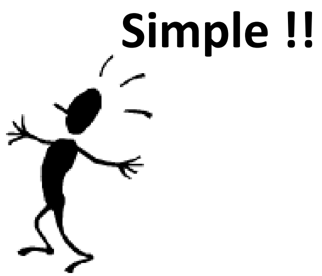
2000 ● Identity-Based Encryption (IBE)



KeyGen.Center

Private Key
101110011010101110…
random

Public Key
Alice@korea.ac.kr
identifiable



2005 ● Attribute-Based Encryption (ABE)

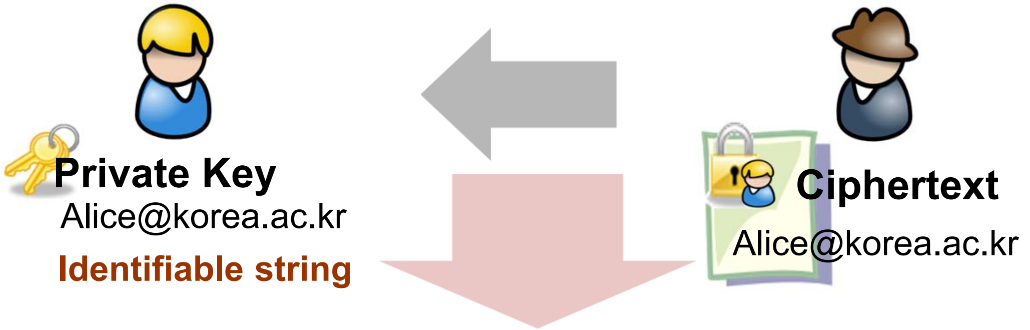
2011 ● Functional Encryption (FE)

History of Cryptography

1940 ● Symmetric-Key Encryption

1970 ● Public-Key Encryption

2000 ● Identity-Based Encryption (IBE)

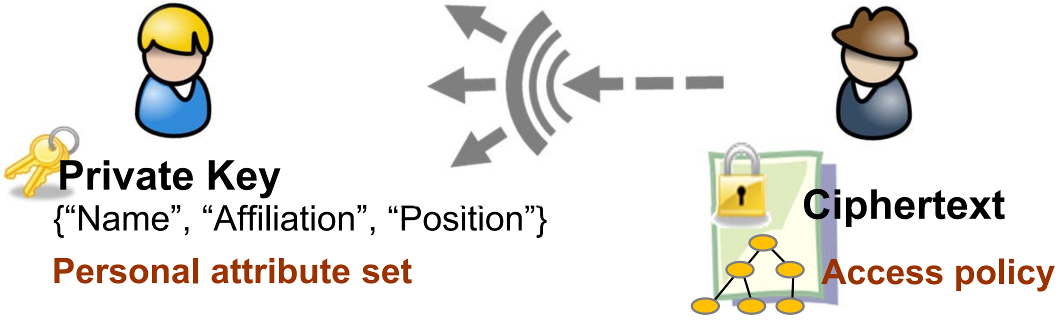


Private Key
Alice@korea.ac.kr
Identifiable string

Ciphertext
Alice@korea.ac.kr

Who should have access to the message?

2005 ● Attribute-Based Encryption (ABE)



Private Key
{"Name", "Affiliation", "Position"}
Personal attribute set

Ciphertext
Access policy

2011 ● Functional Encryption (FE)

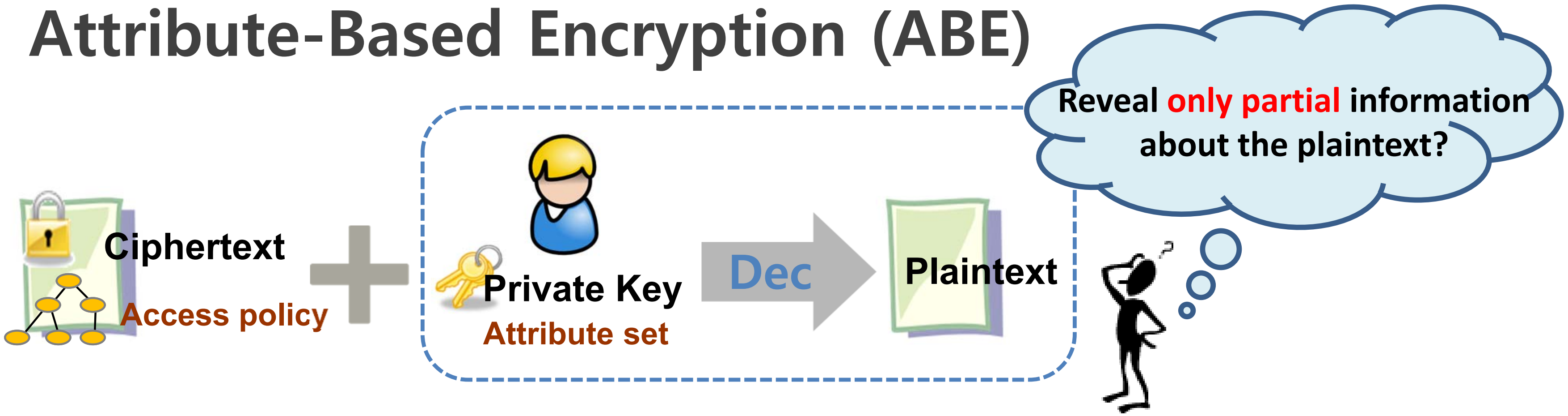
History of Cryptography

1940 ● Symmetric-Key Encryption

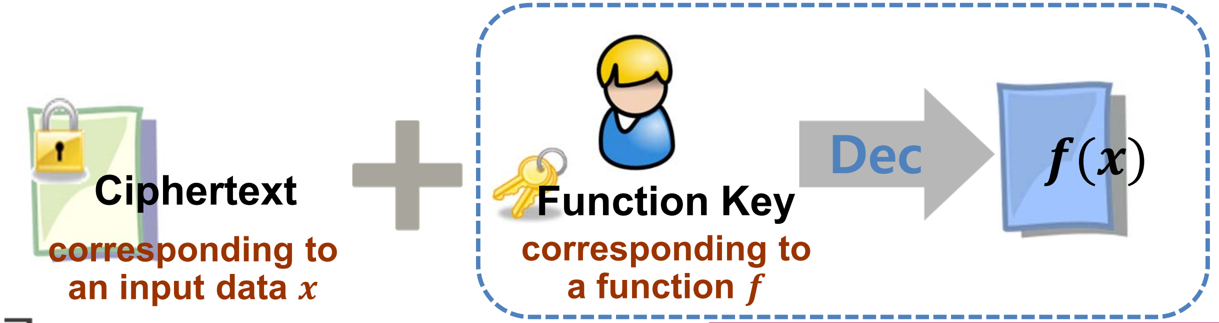
1970 ● Public-Key Encryption

2000 ● Identity-Based Encryption (IBE)

2005 ● Attribute-Based Encryption (ABE)



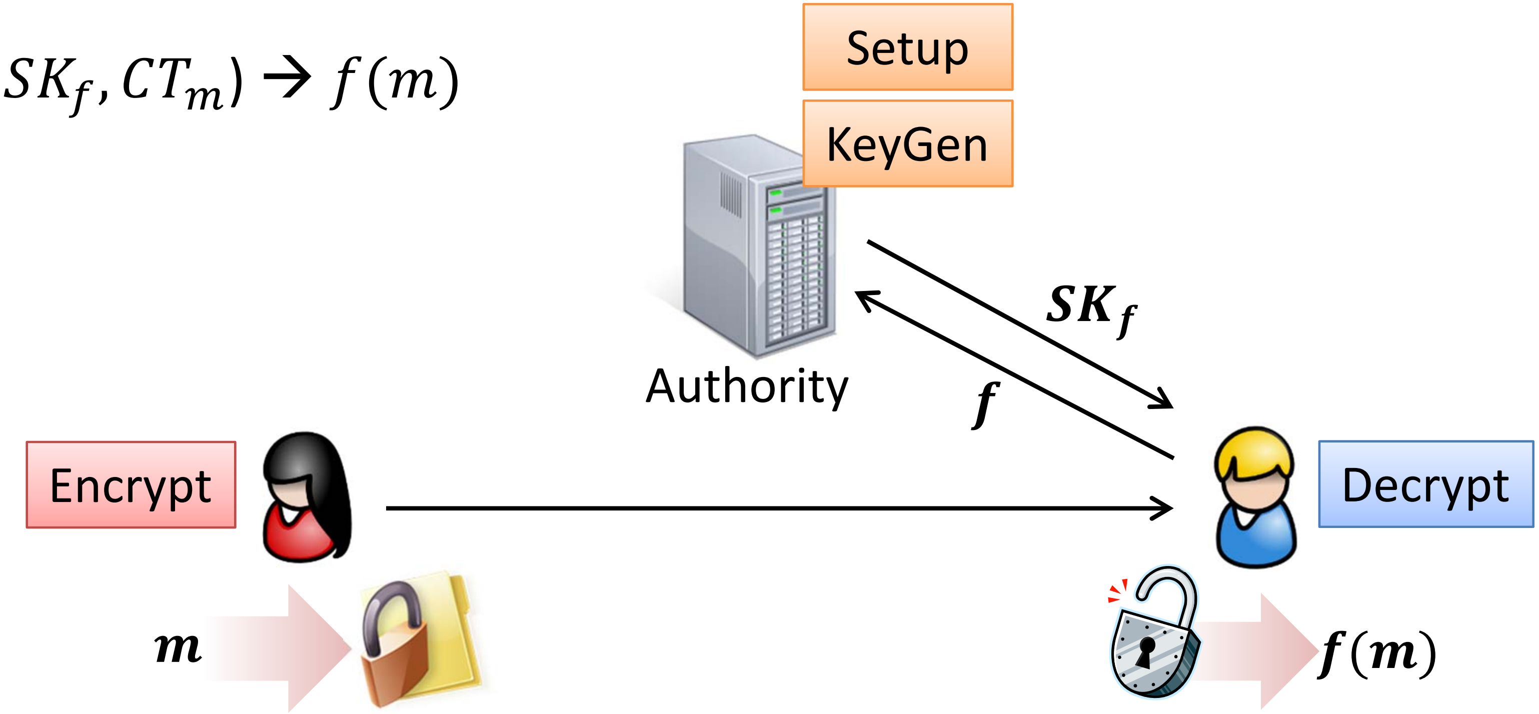
2011 ● Functional Encryption (FE)


Ciphertext
corresponding to an input data x
Function Key
corresponding to a function f
Dec
$f(x)$

Functional Encryption

Definition [BSW11]

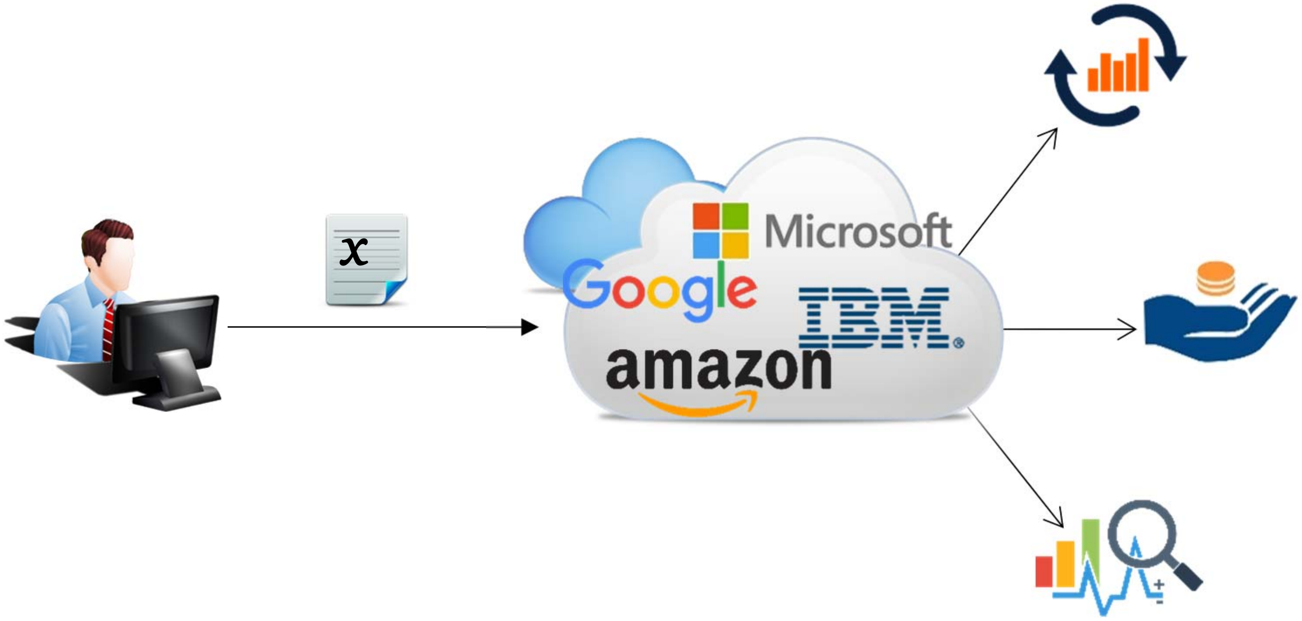
- Setup (1^{λ}) → (PK, MSK)
- KeyGen (MSK, f) → SK_f
- Encrypt (PK, m) → CT_m
- Decrypt (SK_f, CT_m) → $f(m)$



Functional Encryption

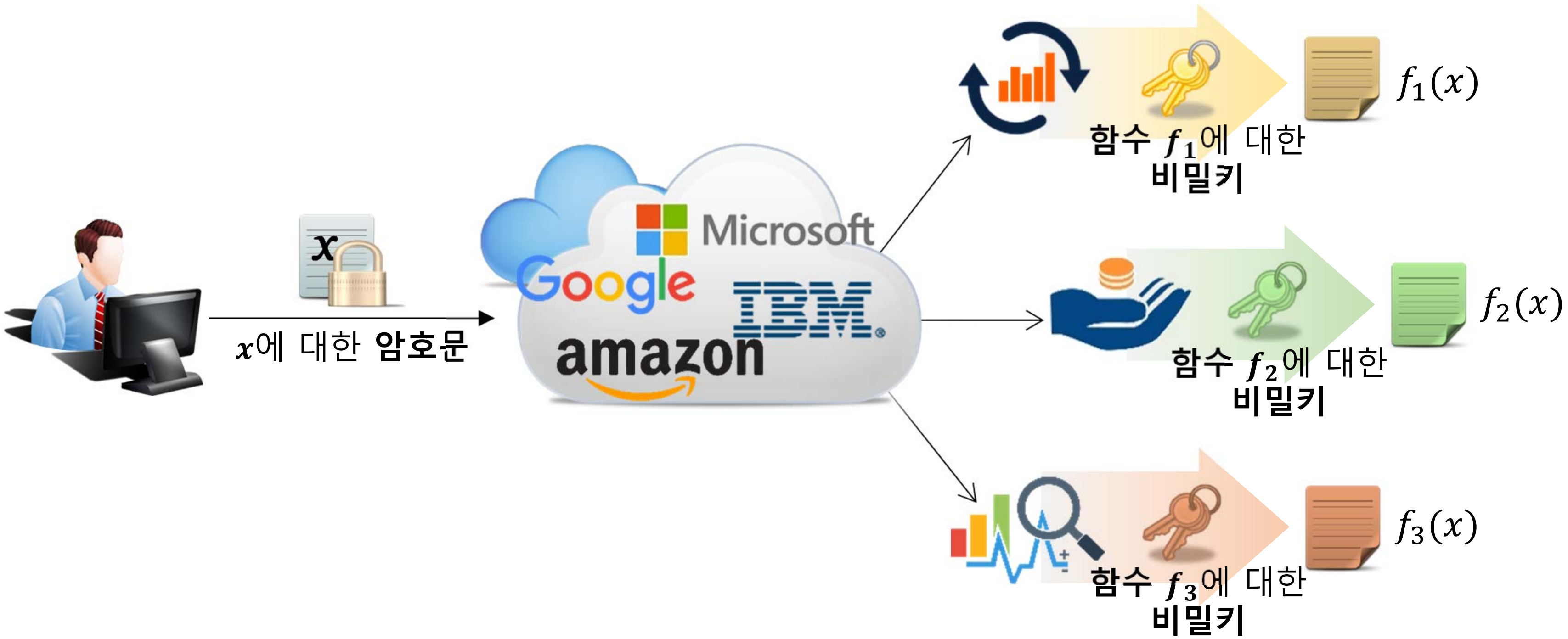
❖ ***"Computation on Encryption Data"***

- 클라우드 컴퓨팅 시대 (Cloud computing)
- 프라이버시 문제 (User privacy)



Functional Encryption

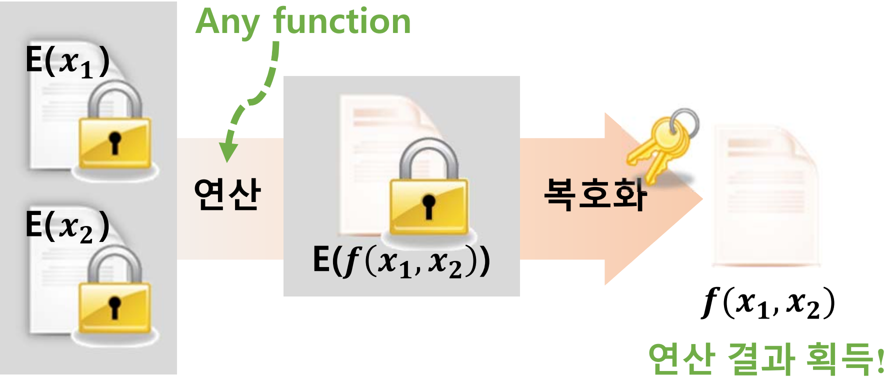
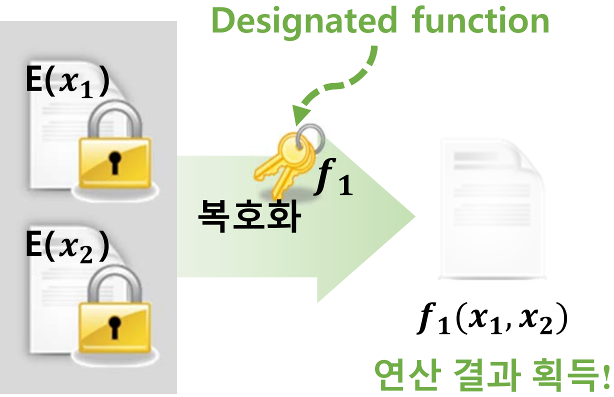
- ***"Computation on Encryption Data"***
  - 클라우드 컴퓨팅 시대 (Cloud computing)
  - 프라이버시 문제 (User privacy)



x
x에 대한 **암호문**
Microsoft
Google
IBM
amazon
함수 f_1에 대한 **비밀키**
$f_1(x)$
함수 f_2에 대한 **비밀키**
$f_2(x)$
함수 f_3에 대한 **비밀키**
$f_3(x)$

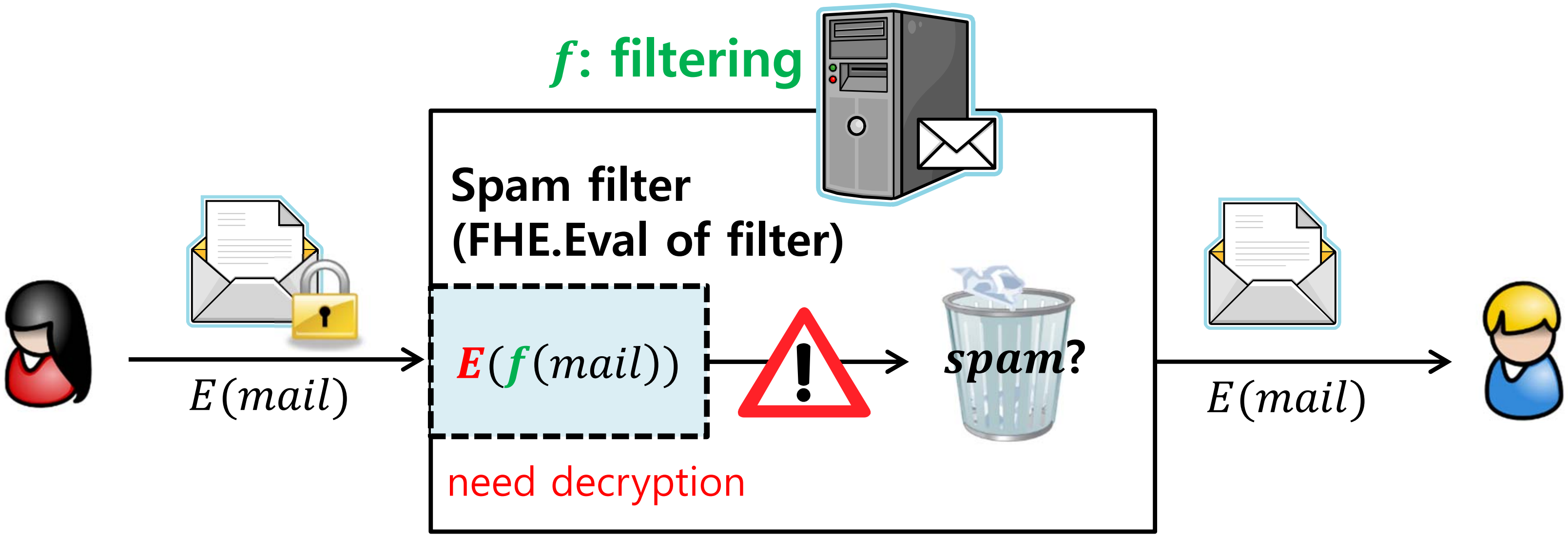
Functional Encryption

❖ vs. Homomorphic Encryption

Homomorphic Encryption	
Functional Encryption	

Functional Encryption

vs. Homomorphic Encryption



f: filtering

Spam filter
(FHE.Eval of filter)

$E(f(mail))$

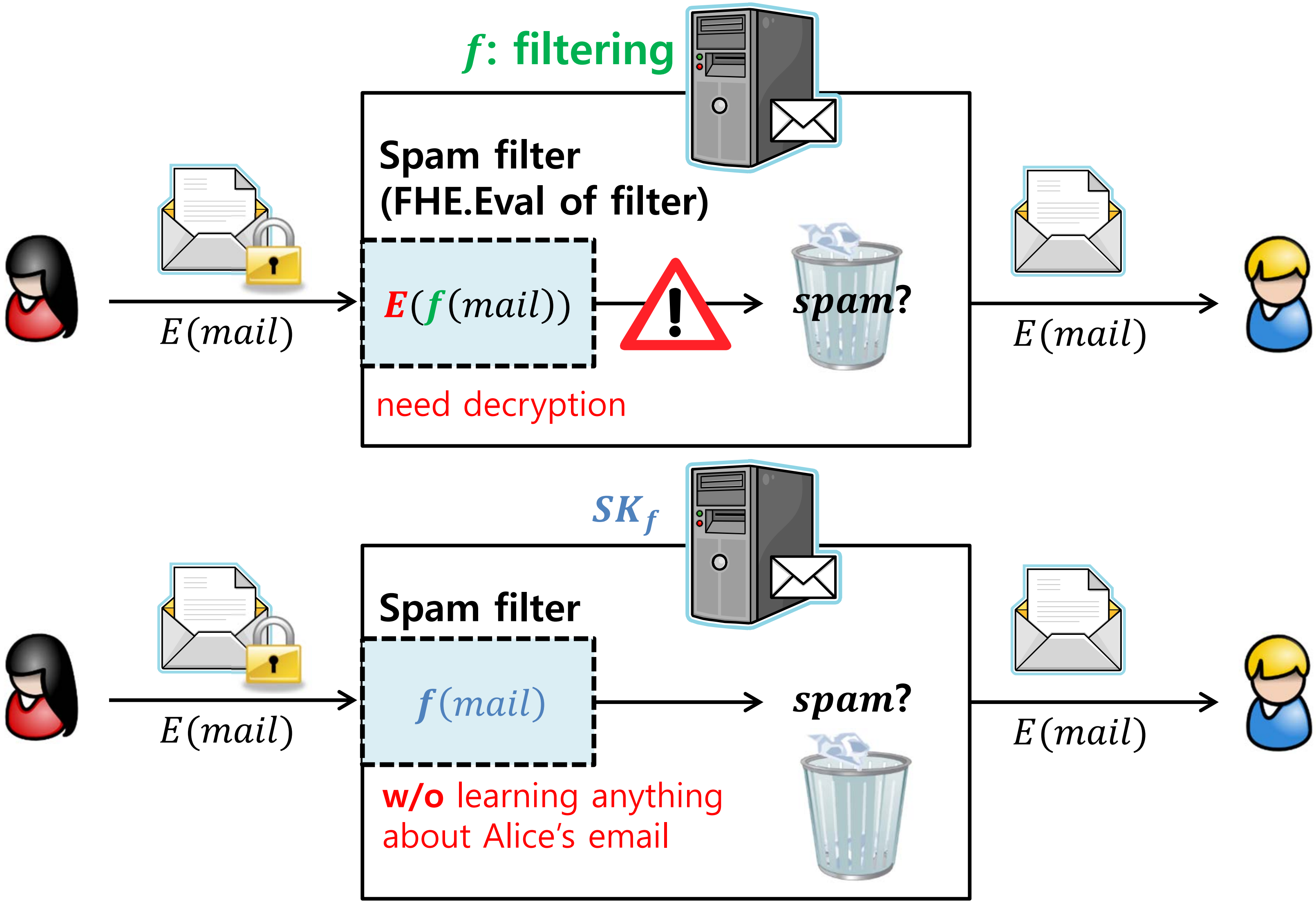
need decryption

$E(mail)$

$E(mail)$

Functional Encryption

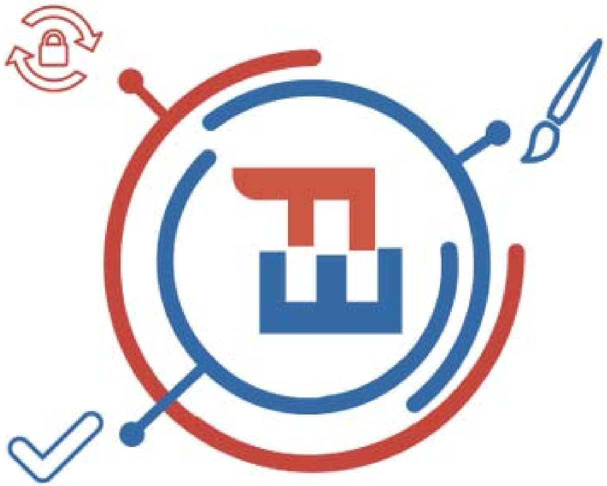
vs. Homomorphic Encryption



Functional Encryption

FENTEC project

- Increasing trustworthiness of ICT solutions by developing **F**unctional **EN**cryption **TEC**hnologies



Implement a unified **cryptographic API** of Functional Encryption systems

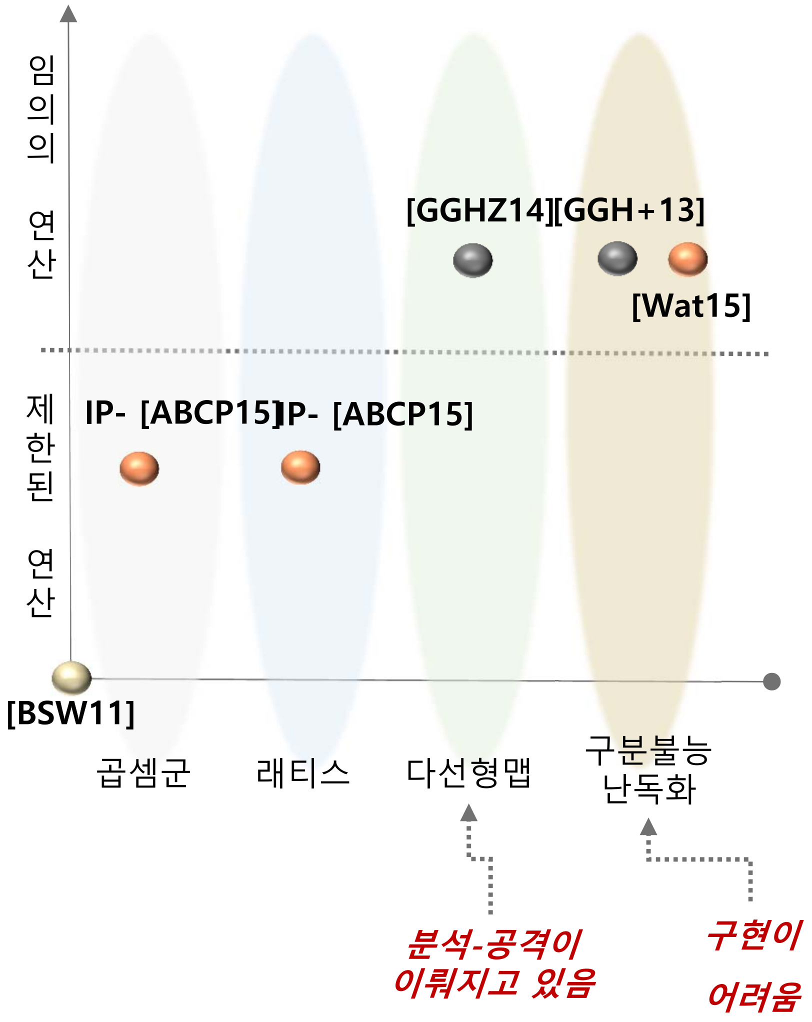
Design **functional encryption systems** with varying functional, security, **hardware** and **software** requirements

Validate and **demonstrate** FENTEC technologies and **solutions**

(http://fentec.eu/)

Functional Encryption

❖ Related Work



2011 함수암호 개념 최초 정립[BSW11] (TCC 2011)

2013 구분불능 난독화를 이용하여 임의의 연산을 지원하는 함수암호가 최초로 설계됨[GGH+13] (FOCS 2013)

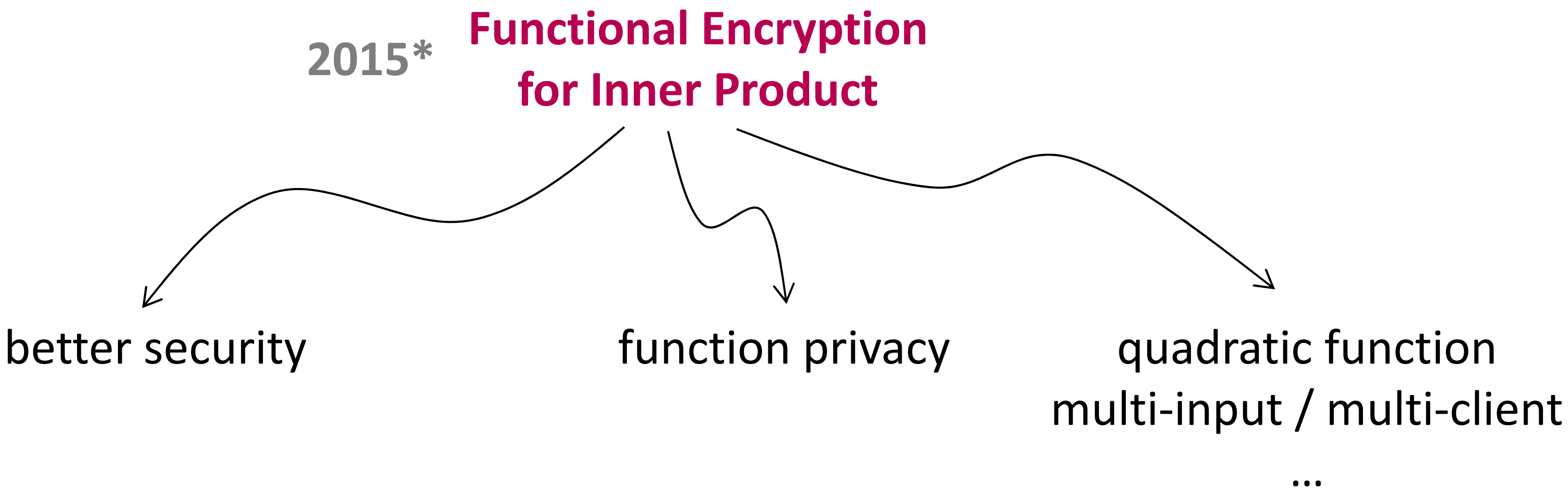
2014 다선형맵을 이용하여 임의의 연산을 지원하는 함수암호가 설계됨[GGHZ14]

2015 곱셈군 및 래티스 기반으로 내적 연산을 지원하는 효율적인 함수암호가 설계됨[ABCP15] (PKC 2015)

구분불능 난독화를 이용하여 임의의 연산을 지원하는 함수암호가 설계됨[Wat15] (Crypto 2015)

Functional Encryption

❖ Related Work (Inner Product)



2015* **Functional Encryption for Inner Product**

better security

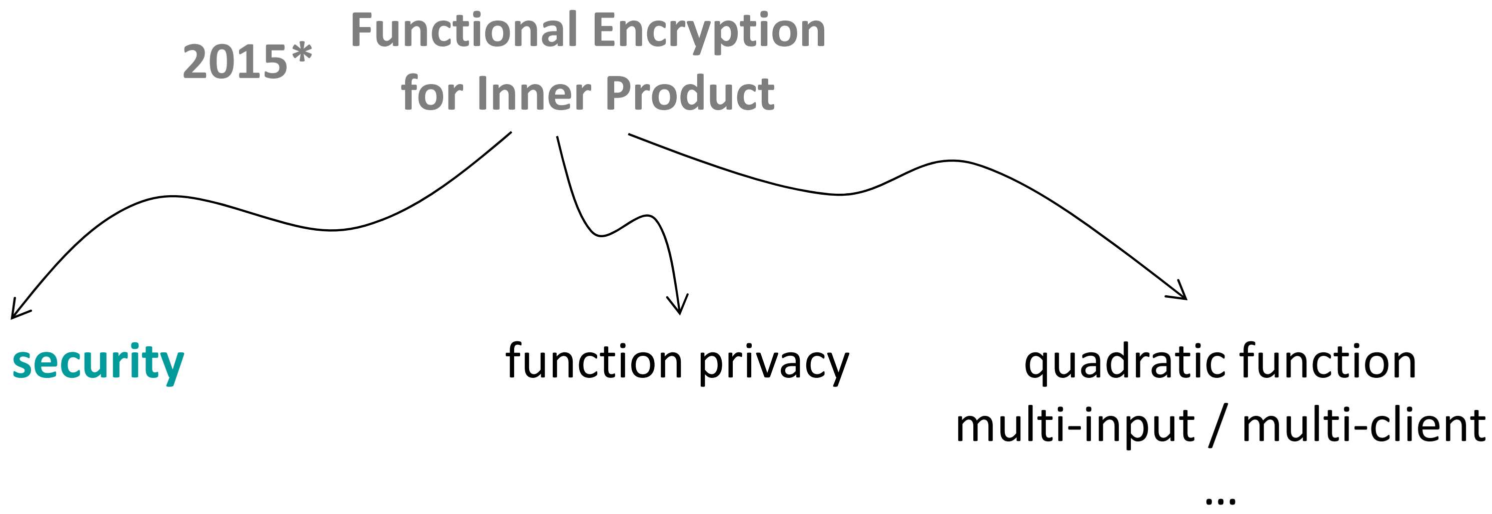
function privacy

quadratic function
multi-input / multi-client
…

* Simple Functional Encryption Schemes for Inner Products (PKC'15)
- M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval

Functional Encryption

❖ Related Work (Inner Product)



2015* Functional Encryption for Inner Product

better security

function privacy

quadratic function
multi-input / multi-client
…

2016

Fully Secure Functional Encryption for Linear Functions from Standard Assumption (CRYPTO’16)
- S. Agrawal, B. Libert, and D. Stehle

Better Security for Functional Encryption for Inner Product Evaluations (ePrint 2016/011)
- M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval

2019

Unbounded Inner-Product Functional Encryption with Succinct Keys (ACNS’19)
- E. Dufour-Sans and D. Pointcheval

Tightly Secure Inner Product Functional Encryption: Multi-input and Function-Hiding Constructions (ASIACRYPT’19)
- J. Tomida

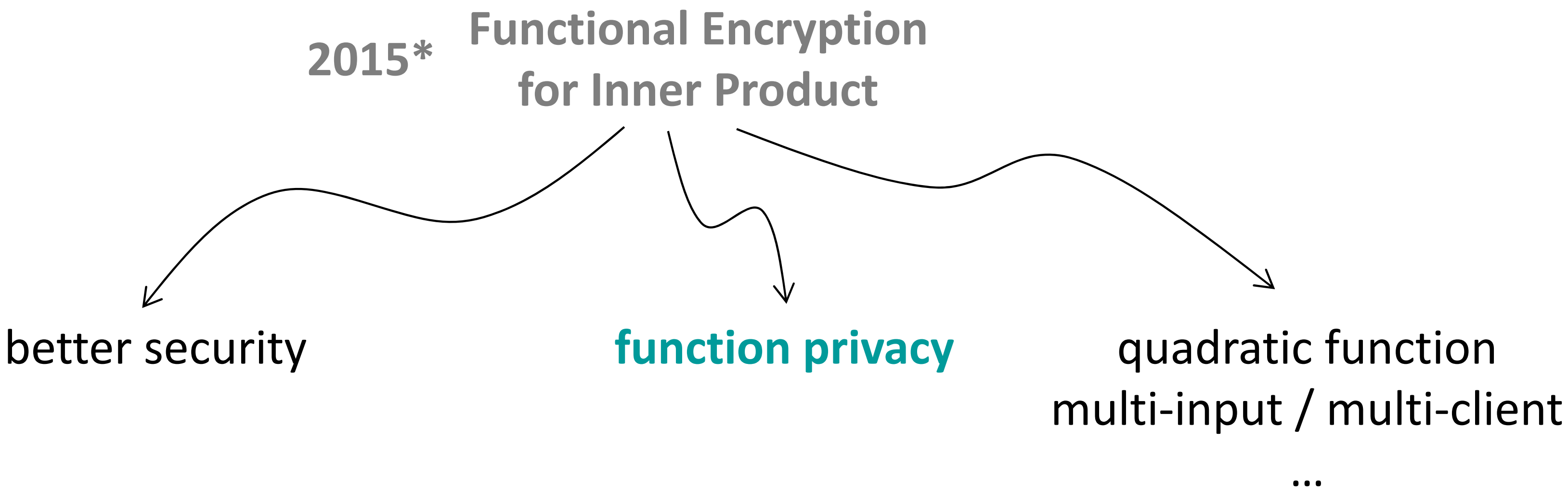
2020

Adaptive Simulation Security for Inner Product Functional Encryption (PKC’20)
- S. Agrawal, B. Libert, M. Maitra, and R. Titiu

Functional Encryption

ct_m sk_f

❖ Related Work (Inner Product)



2015* Functional Encryption for Inner Product

better security

function privacy

quadratic function
multi-input / multi-client
…

2015 Function-Hiding Inner Product Encryption (ASIACRYPT'15)
- A. Bishop, A. Jain, and L. Kowalczyk

2016 Functional Encryption for Inner Product with Full Function Privacy (PKC'16)
- P. Datta, R. Dutta, and S. Mukhopadhyay

Efficient Functional Encryption for Inner-Product Values with Full Hiding Security (ISC'16)
- J. Tomida, M. Abe, and T. Okamoto

2018 Function-Hiding Inner Product Encryption is Practical (SCN'18)
- S. Kim, K. Lewi, A. Mandal, H. Montgomery, A. Roy, and D.J. Wu

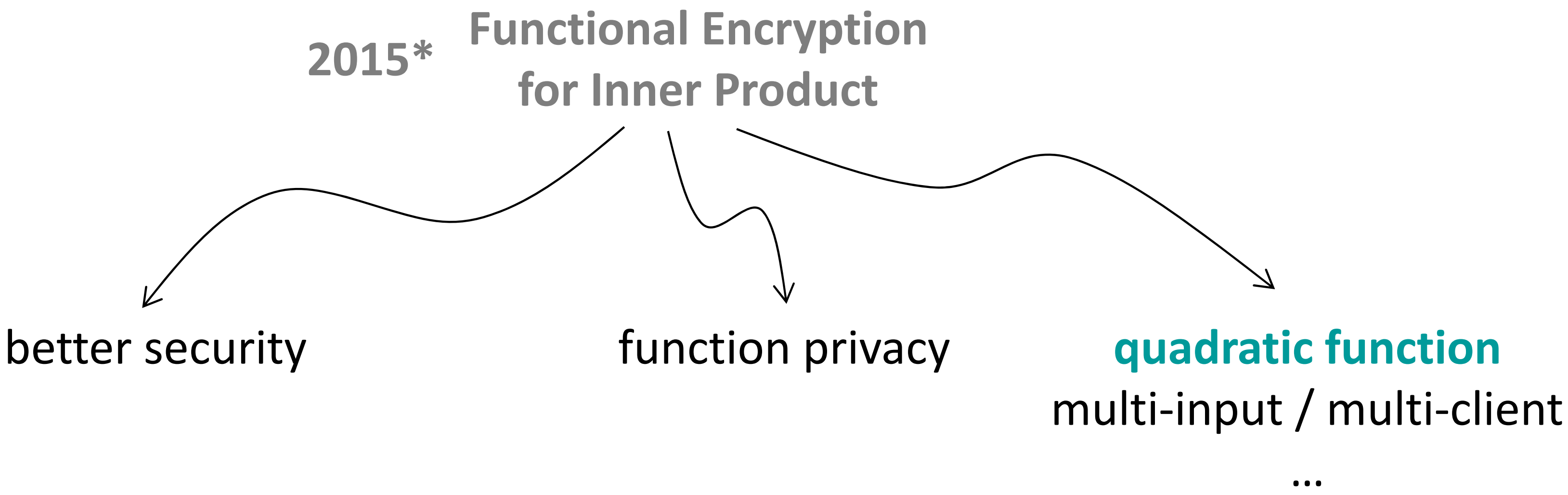
2019 Efficient Function-Hiding Functional Encryption: From Inner-Product to Orthogonality (CT-RSA'19)
- M. Barbosa, D. Catalano, A. Soleimanian, and B. Warinschi

Functional Encryption

$$x^T F y = \begin{bmatrix} x_1 & x_2 & x_3 \end{bmatrix} \begin{bmatrix} f_{1,1} & f_{1,2} & f_{1,3} \\ f_{2,1} & f_{2,2} & f_{2,3} \\ f_{3,1} & f_{3,2} & f_{3,3} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

data Model data

❖ Related Work (Inner Product)



2015* Functional Encryption for Inner Product

better security

function privacy

quadratic function

multi-input / multi-client

…

2017 Practical Functional Encryption for Quadratic Functions with Applications to Predicate Encryption (CRYPTO’17)
- C.E.Z. Baltico, D. Catalano, D. Fiore, and R. Gay

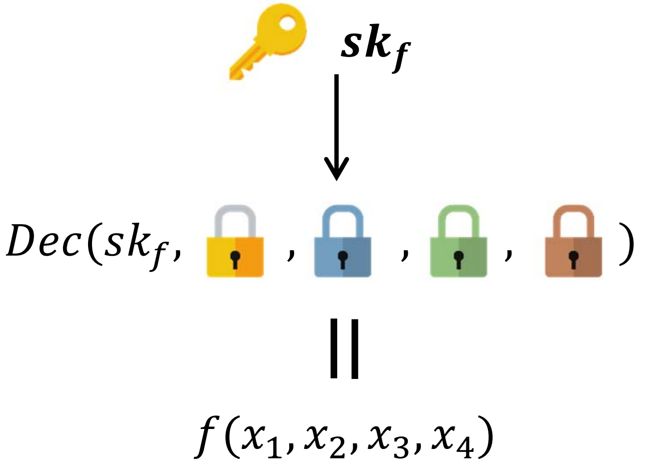
2019 Partially Encrypted Machine Learning using Functional Encryption (NeurIPS’19)
- T. Ryffel, E. Dufour-Sans, R. Gay, F. Bach, and D. Pointcheval

2020 A New Paradigm for Public-Key Functional Encryption for Degree-2 Polynomials (PKC’20)
- R. Gay

Functional Encryption for Quadratic Functions from k-Lin, Revisited (TCC’20)
- H. Wee

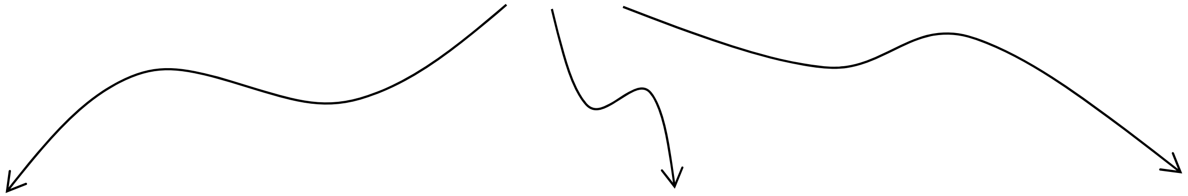
2021 2-Step Multi-Client Quadratic Functional Encryption from Decentralized Function-Hiding Inner-Product (ePrint 2021/1)
- M. Abdalla, D. Pointcheval, and A. Soleimanian

Functional Encryption



❖ Related Work (Inner Product)

2015* Functional Encryption for Inner Product



better security

function privacy

quadratic function

multi-input / multi-client

…

2017 Multi-input Inner-Product Functional Encryption from Pairings (EUROCRYPT’17)
- M. Abdalla, R. Gay, M. Raykova, and H. Wee

Functional Encryption with Oblivious Helper (AsiaCCS’17)
- P.-A. Dupont and D. Pointcheval

2018 Multi-input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions Without Pairings (CRYPTO’18)
- M. Abdalla, D. Catalano, D. Fiore, R. Gay, and B. Ursu

2019 Decentralizing Inner-Product Functional Encryption (PKC’19)
- M. Abdalla, F. Benhamouda, M. Kohlweiss, and H. Waldner

From Single-Input to Multi-client Inner-Product Functional Encryption (ASIACRYPT’19)
- M. Abdalla, F. Benhamouda, and R. Gay

2020 Traceable Inner Product Functional Encryption (CT-RSA’20)
- X.T. Do, D.H. Phan, and D. Pointcheval

Functional Encryption for Attribute-Weighted Sums from k-Lin (CRYPTO’20)
- M. Abdalla, J. Gong, and H. Wee

Dynamic Decentralized Functional Encryption (CRYPTO’20)
- J. Chotard, E. Dufour-Sans, R. Gay, D.H. Phan, and D. Pointcheval

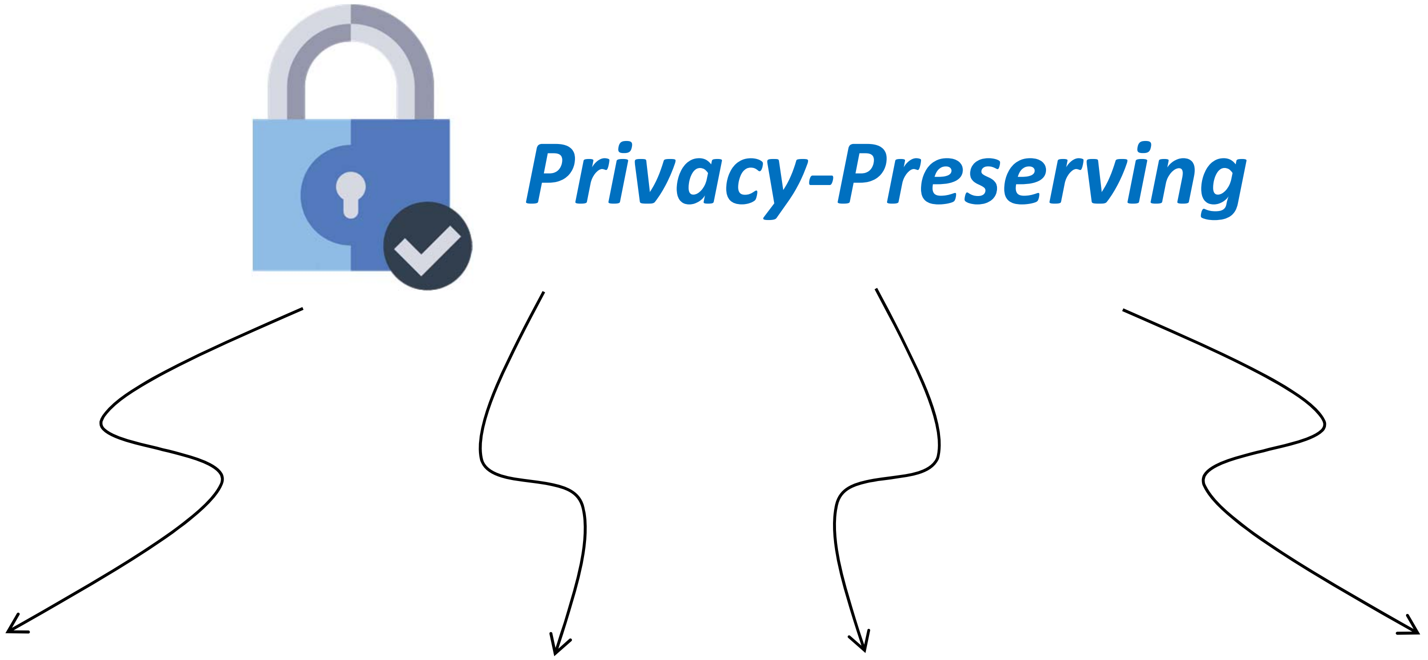
Functional Encryption

Simple Scheme*

- **Setup**$(1^\lambda, n)$ → (mpk, msk)
  - » $\boldsymbol{s} = (s_1, \dots, s_n) \leftarrow \mathbb{Z}_p^n$
  - » $msk = (\boldsymbol{s}), mpk = \{h_i = g^{s_i}\}_{i\in[n]}$
- **KeyGen**$(msk, \boldsymbol{x})$ → $sk_{\boldsymbol{x}}$
  - » $\boldsymbol{x} \in \mathbb{Z}_p^n$
  - » $sk_{\boldsymbol{x}} =< \boldsymbol{x}, \boldsymbol{s} >$
- **Encrypt**$(mpk, \boldsymbol{y})$ → $ct_{\boldsymbol{y}}$
  - » $\boldsymbol{y} \in \mathbb{Z}_p^n$
  - » $\gamma \leftarrow \mathbb{Z}_p$
  - » $ct_{\boldsymbol{y}} = (ct_0, \{ct_i\}_{i\in[n]}) = \left(g^\gamma, \{h_i^\gamma \cdot g^{y_i}\}_{i\in[n]}\right)$
- **Decrypt**$(sk_{\boldsymbol{x}}, ct_{\boldsymbol{y}})$ → $< \boldsymbol{x}, \boldsymbol{y} >$
  - » $V = \prod_{i\in[n]} ct_i^{x_i} \,/\, ct_0^{sk_x}$
  - » Output $\log(V)$

* Simple Functional Encryption Schemes for Inner Products (PKC'15)
- M. Abdalla, F. Bourse, A. De Caro, and D. Pointcheval

Applications



Privacy-Preserving

Data mining
- Big Data Analysis
- Log Auditing

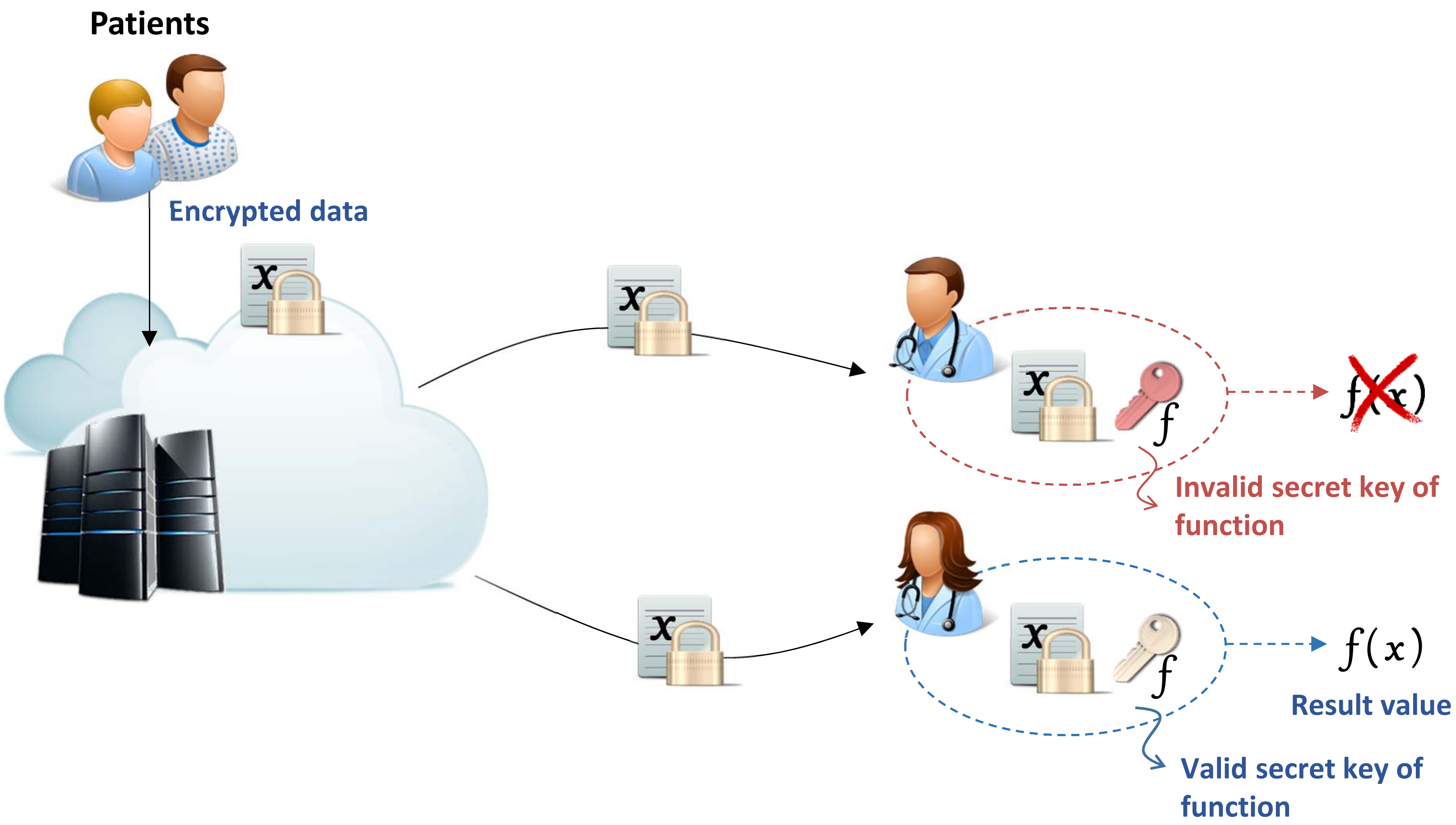
Authentication
- Biometric
- Location

Machine Learning

COVID-19
Contact Tracing

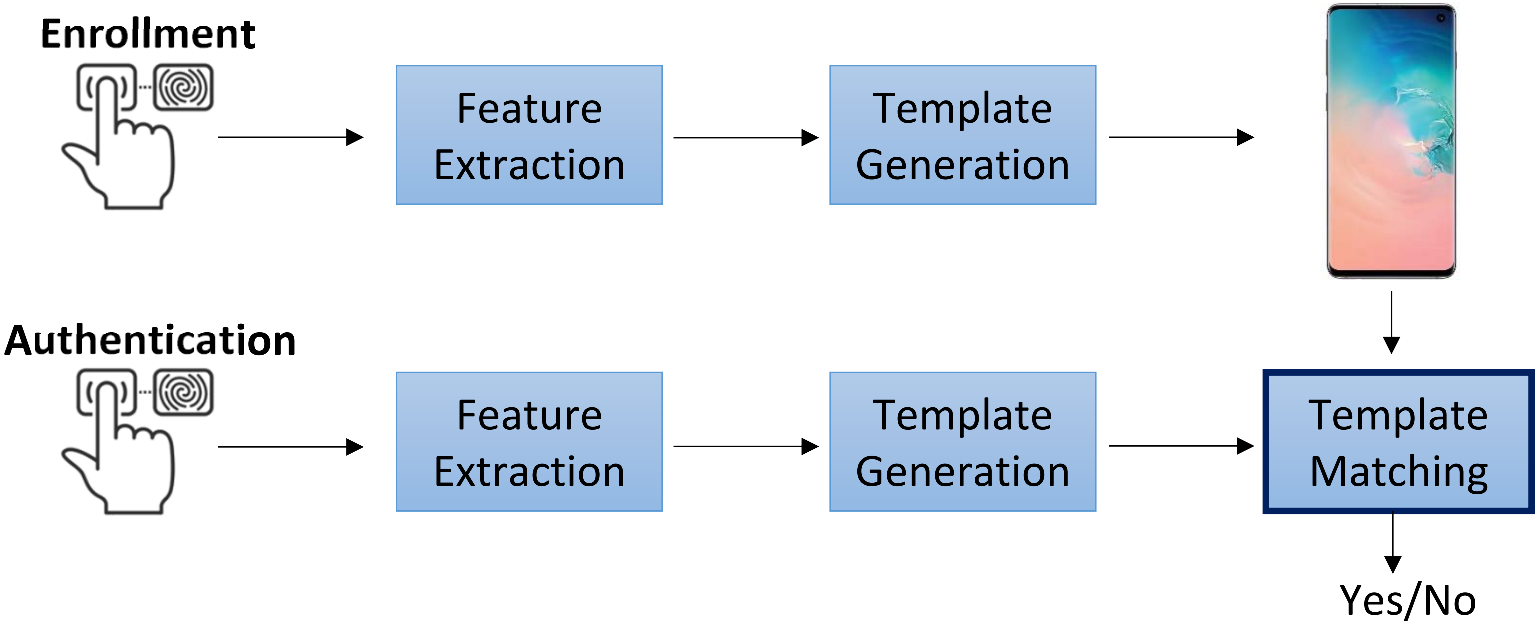
Applications [1]

❖ Big Data Analysis



Applications [2]

Biometric Authentication



Enrollment

Feature Extraction

Template Generation

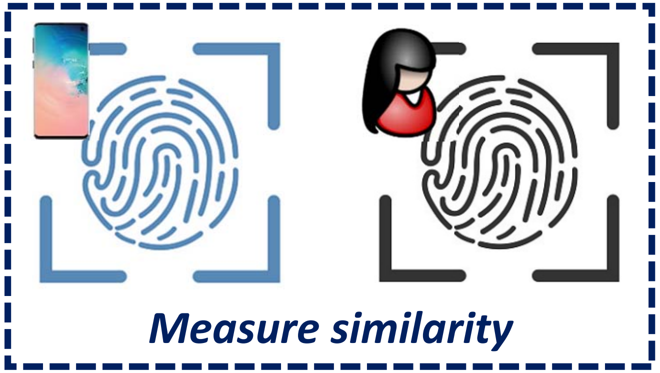
Authentication

Feature Extraction

Template Generation

Template Matching

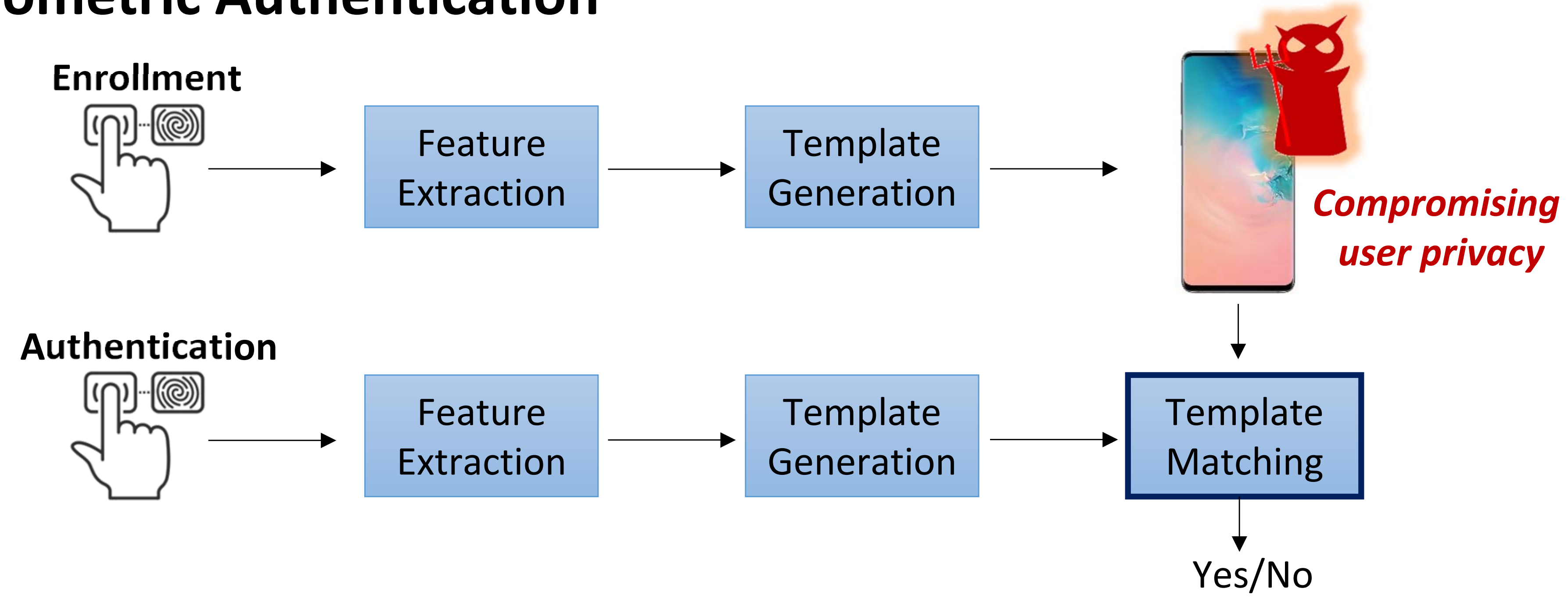
Yes/No



Measure similarity

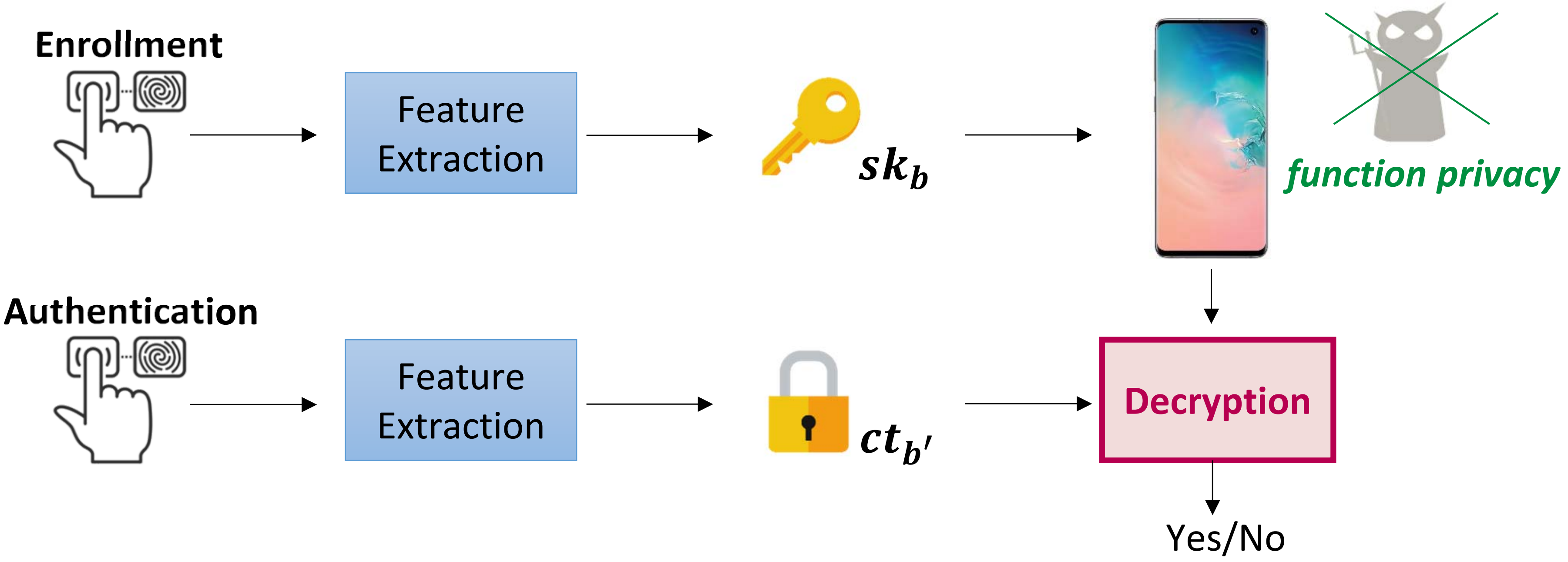
Applications [2]

Biometric Authentication



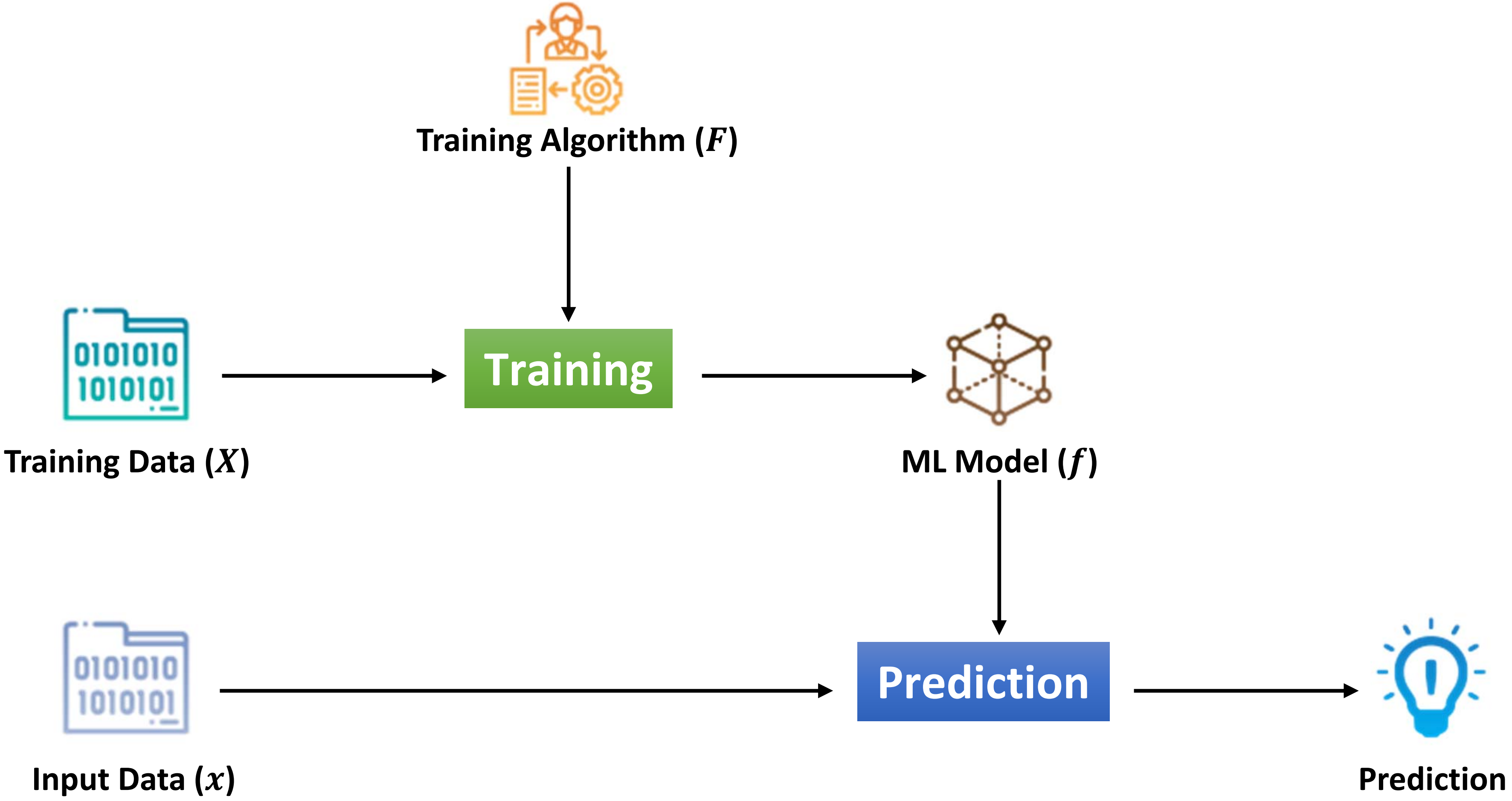
Applications [2]

❖ Biometric Authentication



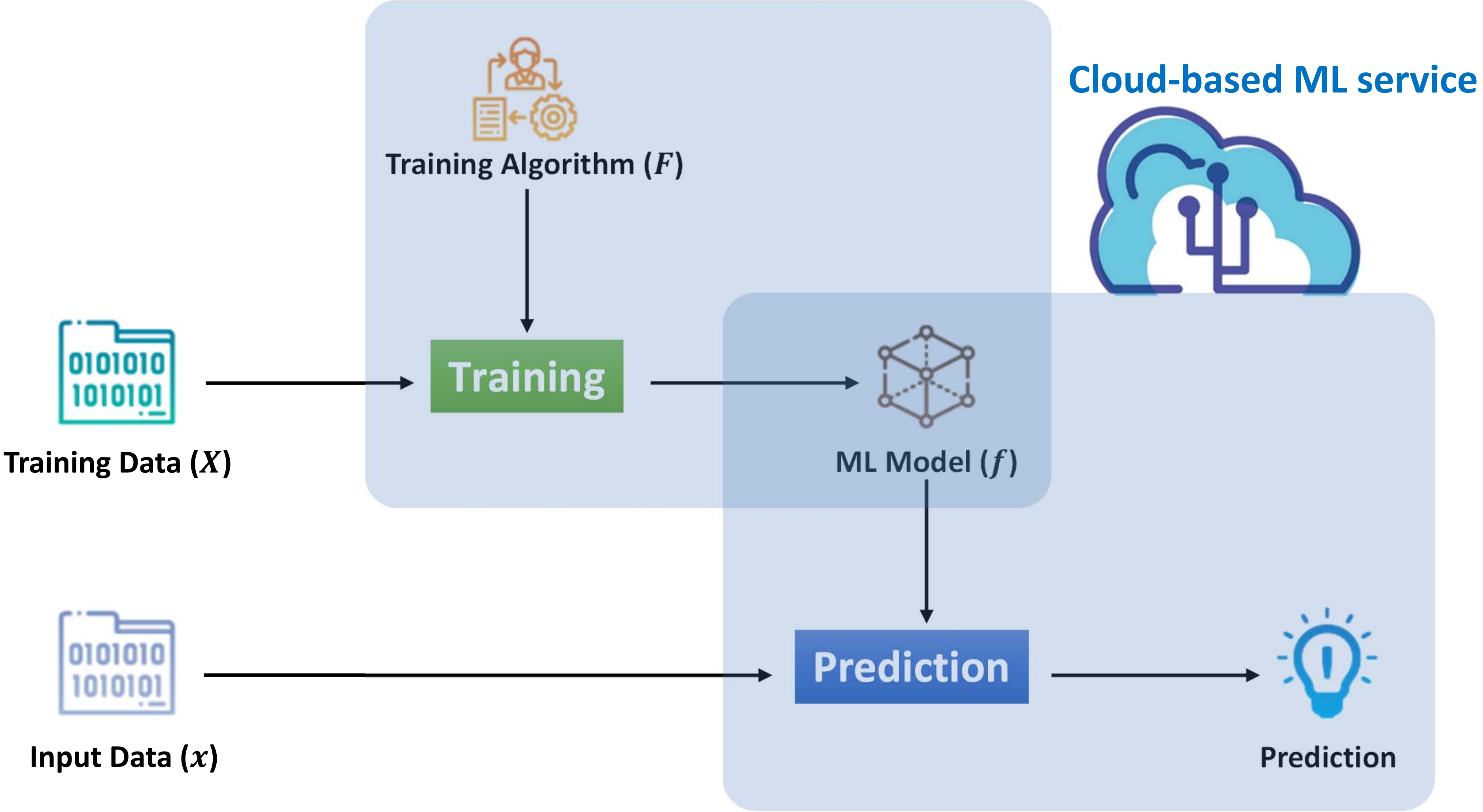
Applications [3]

Machine Learning



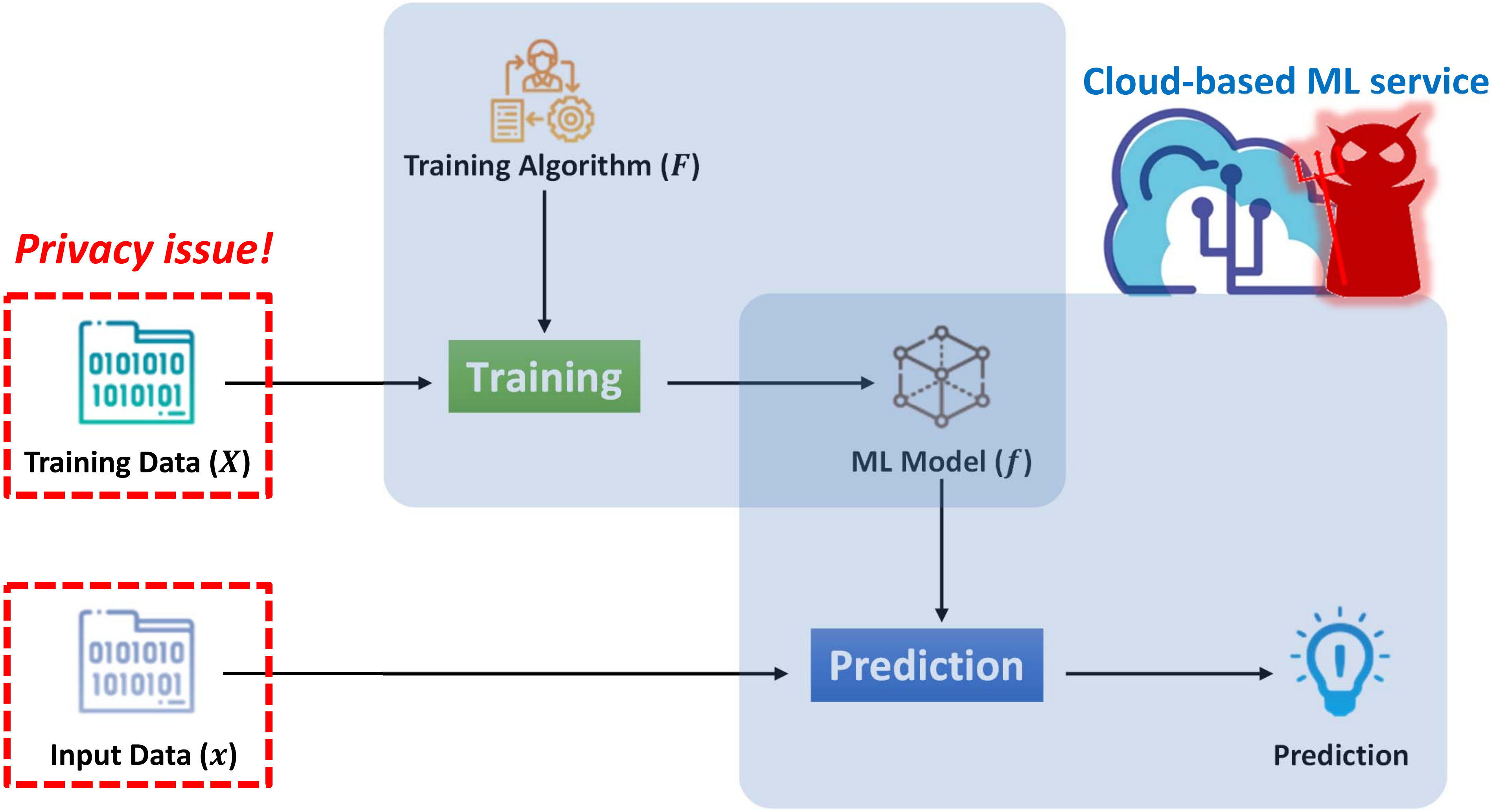
Applications [3]

❖ Machine Learning



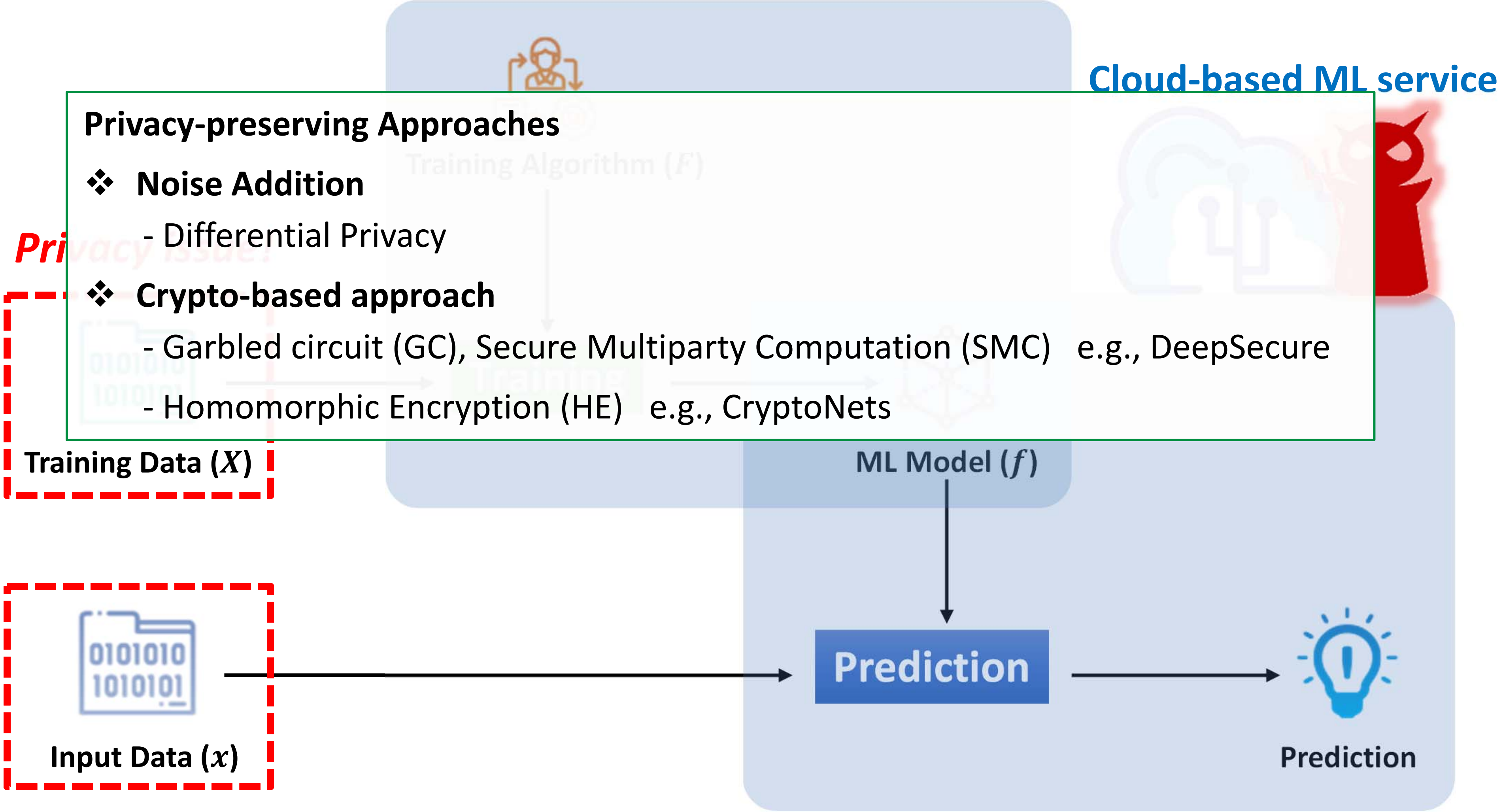
Applications [3]

Machine Learning



Applications [3]

❖ Machine Learning



Privacy-preserving Approaches

❖ **Noise Addition**

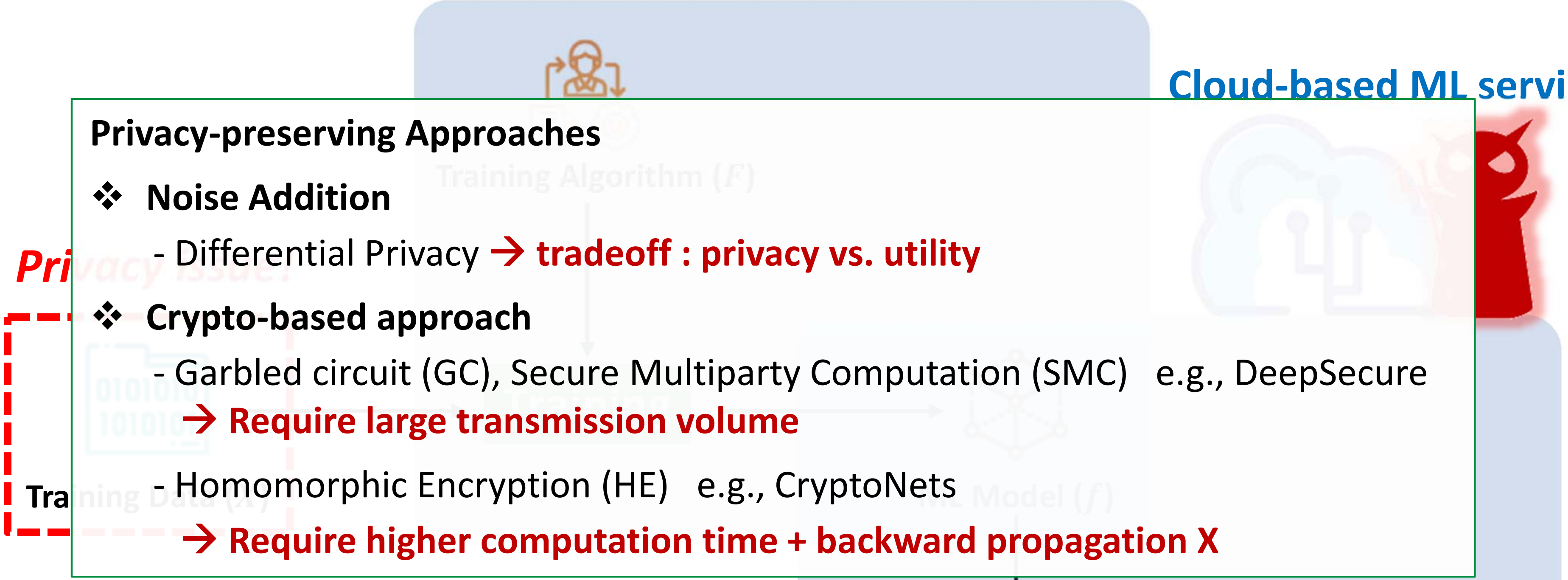
- Differential Privacy

❖ **Crypto-based approach**

- Garbled circuit (GC), Secure Multiparty Computation (SMC) e.g., DeepSecure
- Homomorphic Encryption (HE) e.g., CryptoNets

Applications [3]

❖ Machine Learning



Privacy-preserving Approaches

❖ **Noise Addition**

- Differential Privacy → **tradeoff : privacy vs. utility**

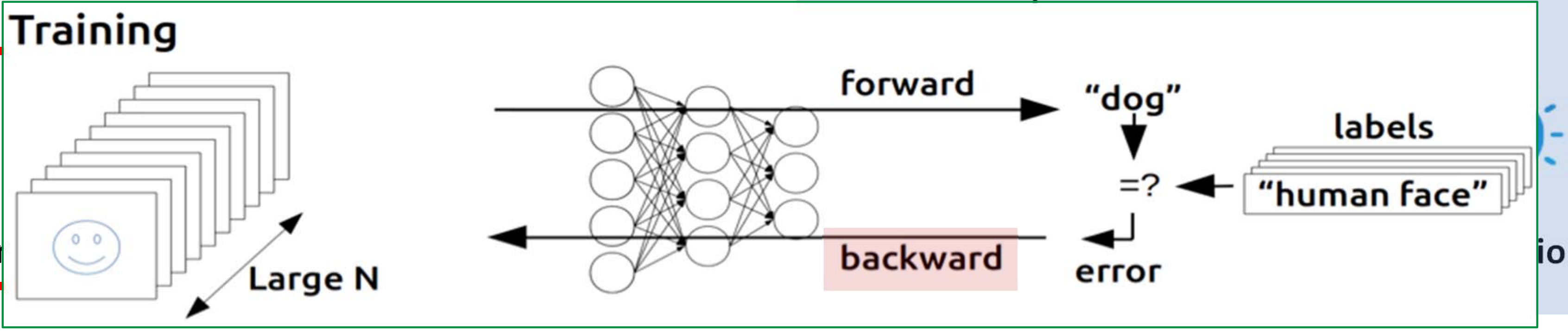
❖ **Crypto-based approach**

- Garbled circuit (GC), Secure Multiparty Computation (SMC)   e.g., DeepSecure

→ **Require large transmission volume**

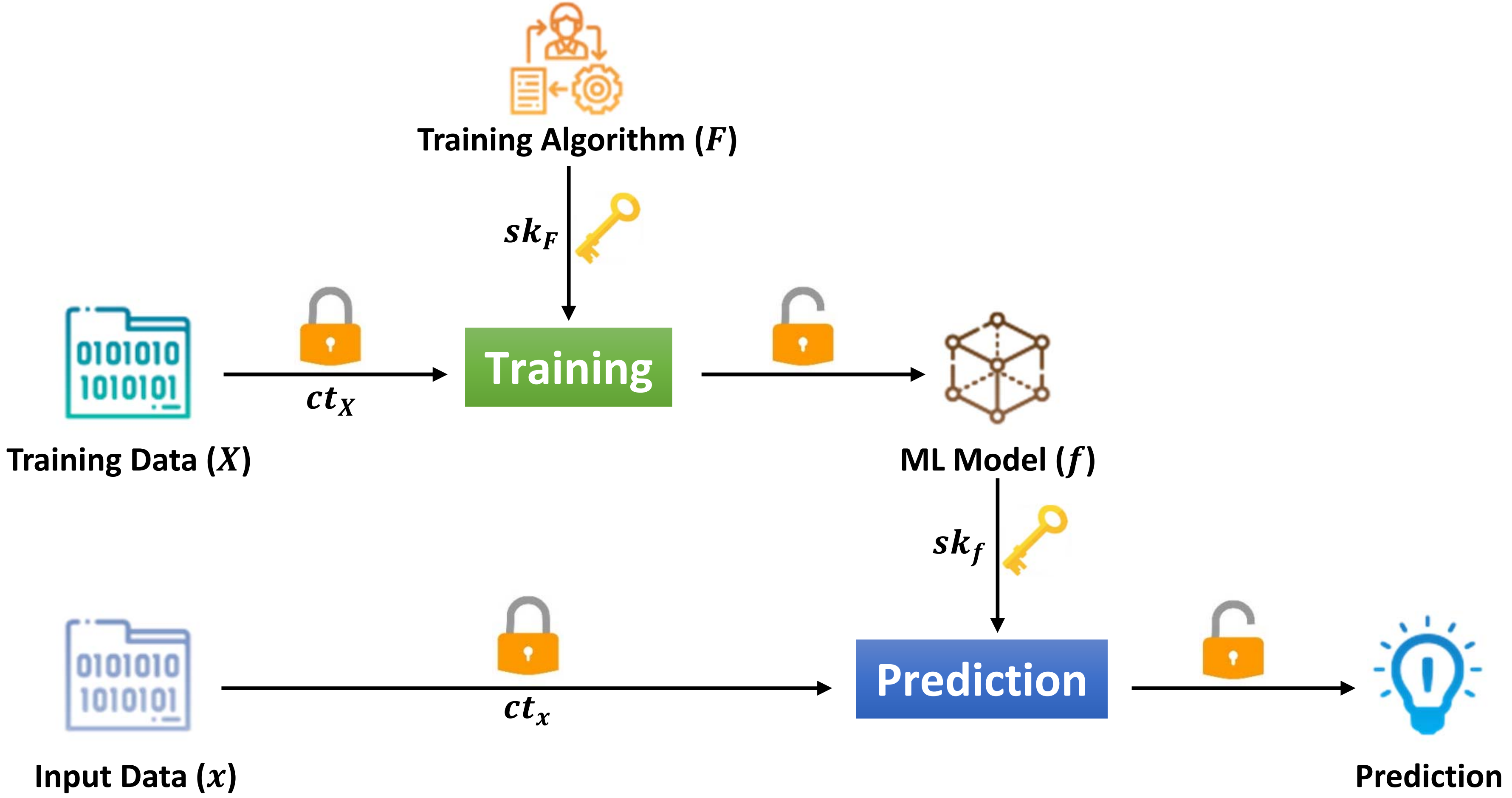
- Homomorphic Encryption (HE)   e.g., CryptoNets

→ **Require higher computation time + backward propagation X**



Applications [3]

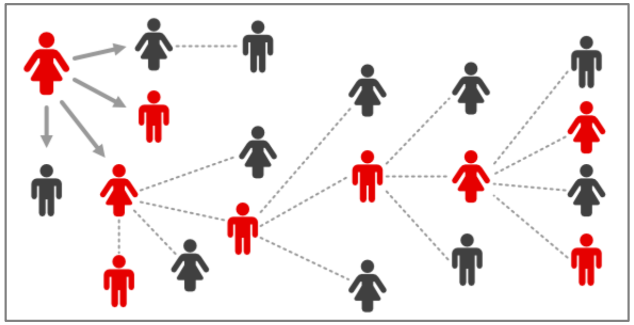
Machine Learning (w/ functional encryption)

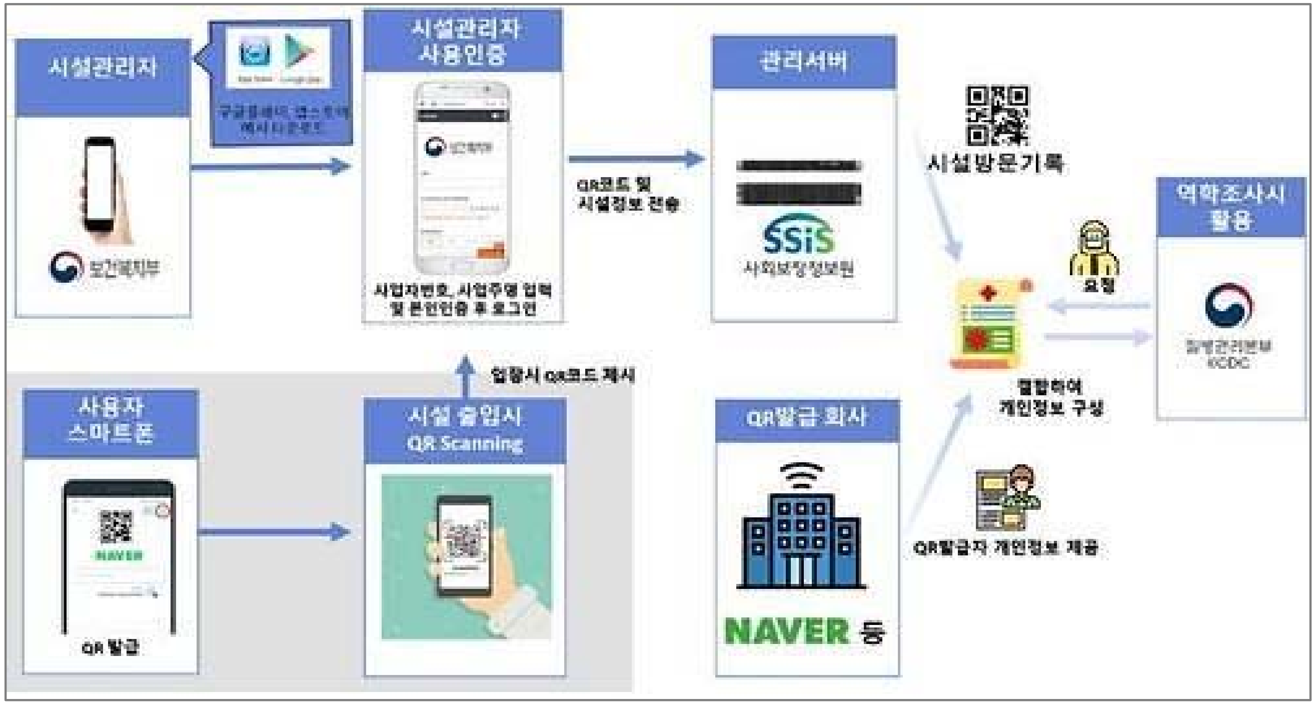


Applications [4]

COVID-19 Contact Tracing

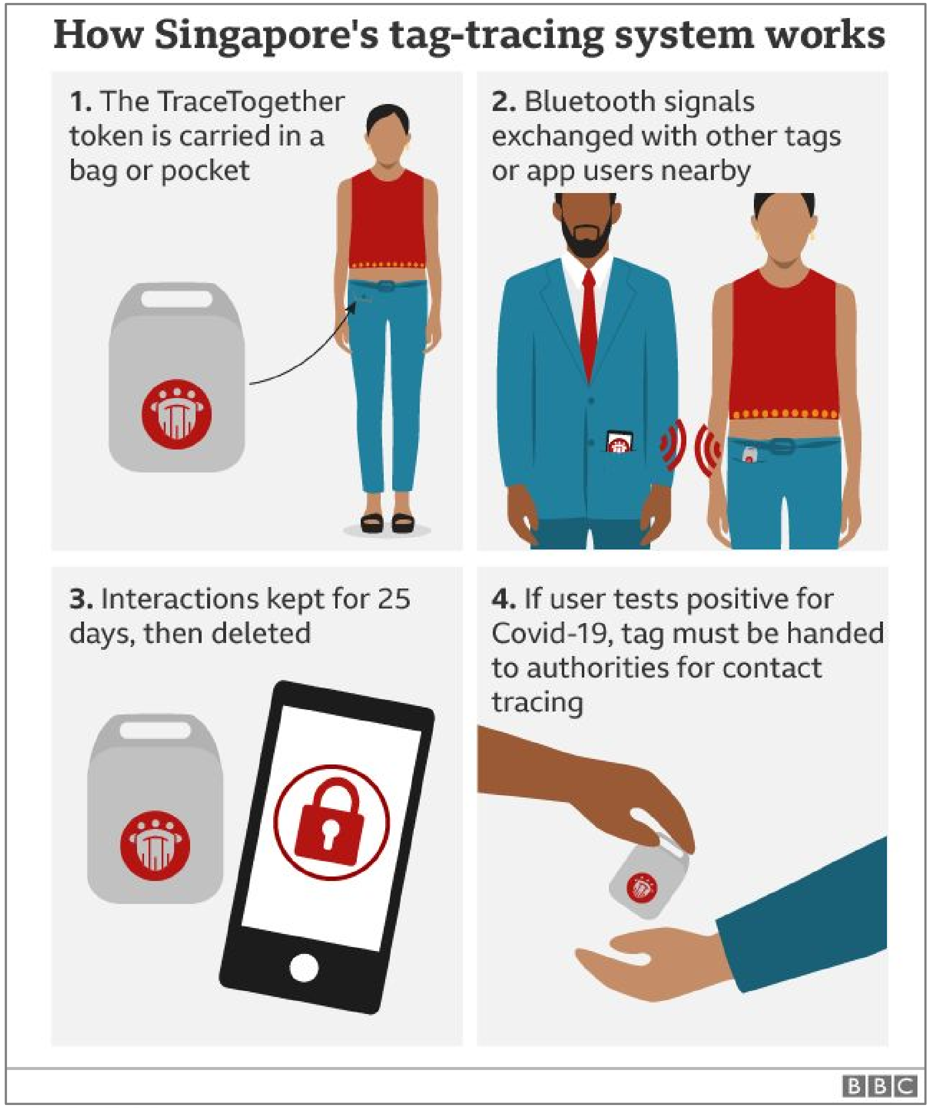
- Contact tracing aims to identify and alert people who have come into contact with a person infected with coronavirus





Applications [4]

COVID-19 Contact Tracing



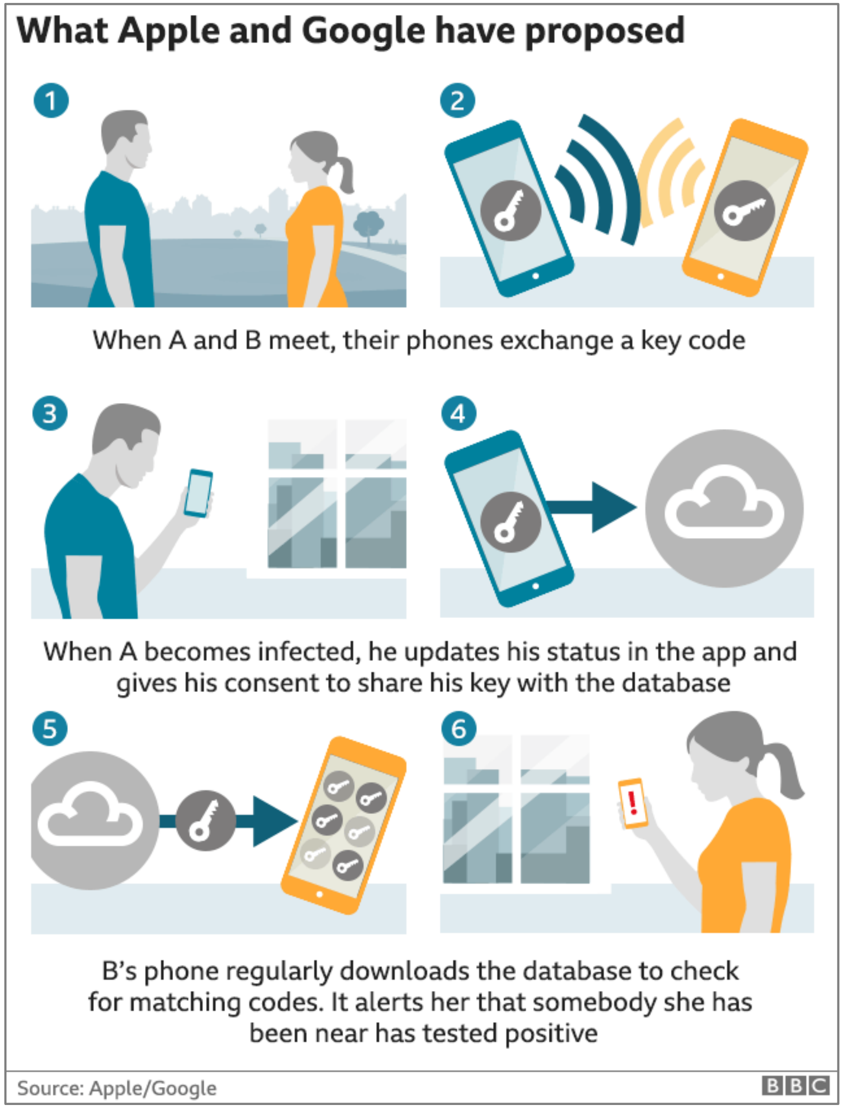
How Singapore's tag-tracing system works

1. The TraceTogether token is carried in a bag or pocket

2. Bluetooth signals exchanged with other tags or app users nearby

3. Interactions kept for 25 days, then deleted

4. If user tests positive for Covid-19, tag must be handed to authorities for contact tracing



What Apple and Google have proposed

When A and B meet, their phones exchange a key code

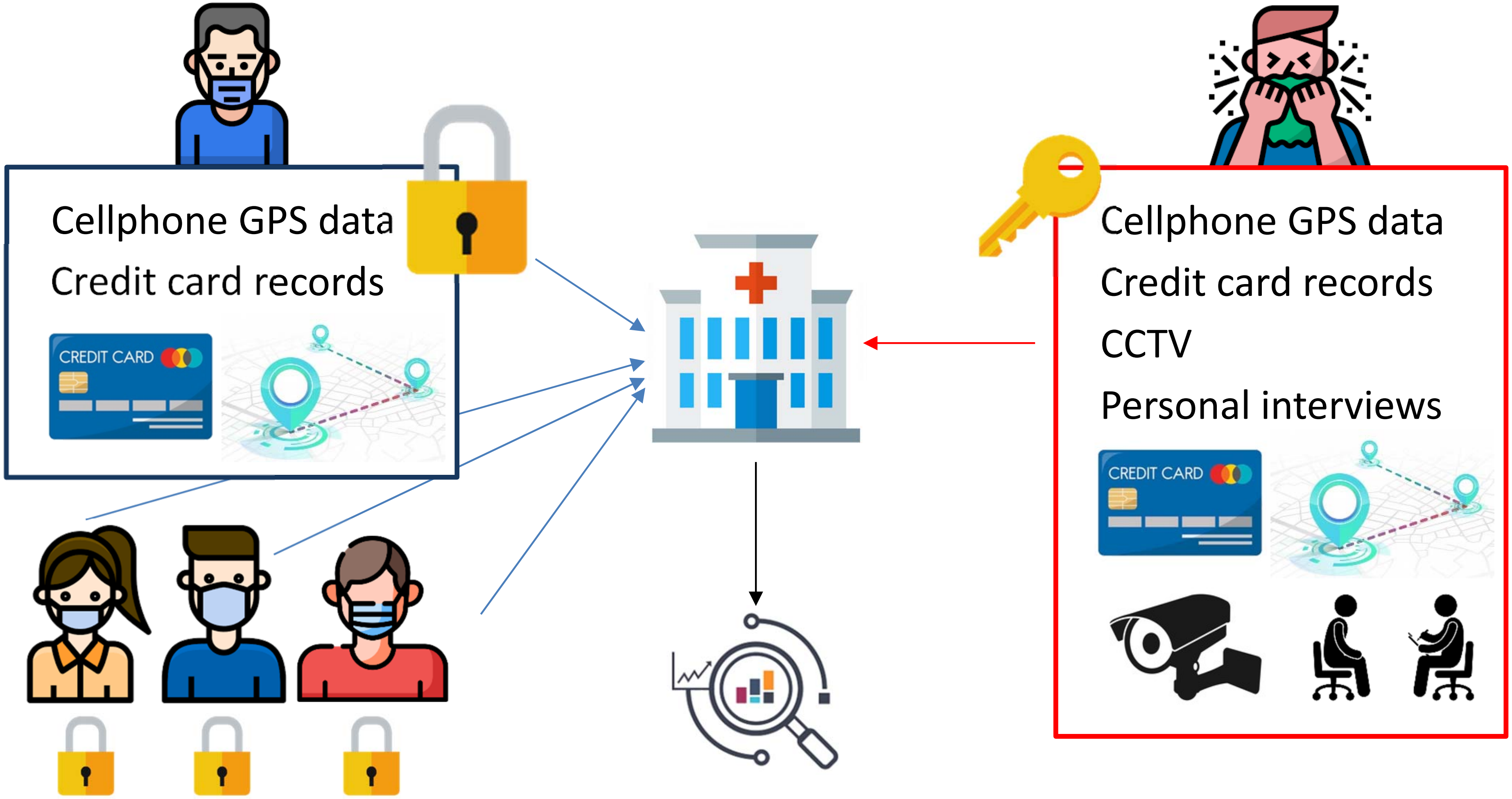
When A becomes infected, he updates his status in the app and gives his consent to share his key with the database

B's phone regularly downloads the database to check for matching codes. It alerts her that somebody she has been near has tested positive

Source: Apple/Google

Applications [4]

❖ COVID-19 Contact Tracing



Cellphone GPS data
Credit card records

Cellphone GPS data
Credit card records
CCTV
Personal interviews

Summary

- **History of Cryptography**
- **Functional Encryption**
  - Definition
    - Vs. Homomorphic Encryption
  - Related Work (FE for IP)
  - Simple Scheme
- **Applications**
  - (Privacy-preserving) Big Data Analysis
  - (Privacy-preserving) Biometric Authentication
  - (Privacy-preserving) Machine Learning
  - (Privacy-preserving) COVID-19 Contact Tracing

Q&A

Thank you ☺

덕성여자대학교
DUKSUNG WOMEN'S UNIVERSITY