暗号プラットフォーム研究の展望

Nuttapong (Nuts) Attrapadung

CPSEC symposium 2018.12.17

AIST

CPSEC
Cyber Physical Security Research Center

On Cryptography Platform:
Attribute-based Encryption and More

Nuttapong (Nuts) Attrapadung

CPSEC symposium 2018.12.17

AIST

CPSEC
Cyber Physical Security Research Center

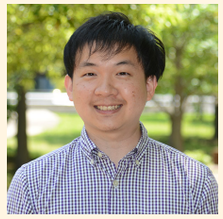
About Myself

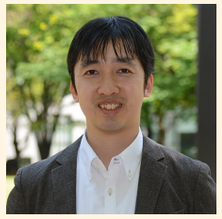
Nuttapong Attrapadung (Nut/Nuts/Nattsu/ナッツ)

1997-2001 Thailand	Chulalongkorn University Bachelor Engineering
2001-2007 Japan	University of Tokyo Master, Ph.D. (Info.Science&Tech)
2007-now Japan	AIST researcher

1997 Argentina	International Math Olympiad
2012-2013 France	École normale supérieure, Paris visiting researcher

暗号プラットフォーム研究チームの紹介


ナッツ


村上


照屋


須崎


塚本

他チーム@ CPSEC Cyber Physical Security Research Center

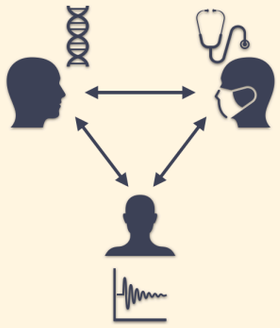
共同研究先：三菱電機、パナソニック、NTT、日立、KDDI研究所

外部企業・機関

設計した汎用的フレームワークの中で、ニーズに沿った応用機能を提供

Q. Utility + Privacy?

A. Advance encryption, Differential privacy

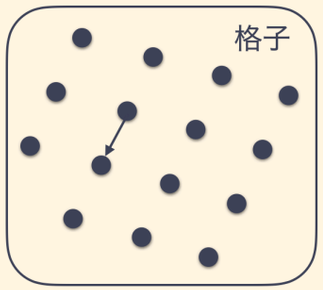


Q. Computation +Privacy ?

A. secure multi-party protocols framework

本研究チーム：暗号技術を応用し、システムの様々なレイヤでセキュアプラットフォーム・フレームワークを設計・開発

研究プロジェクト
- JST CREST
- Kakenhi
- JST ACT-i
- 他 (調整中)



Shortest Vector Problem

Q. 格子暗号は 本当に安全？

A. 解読実験による安全性評価

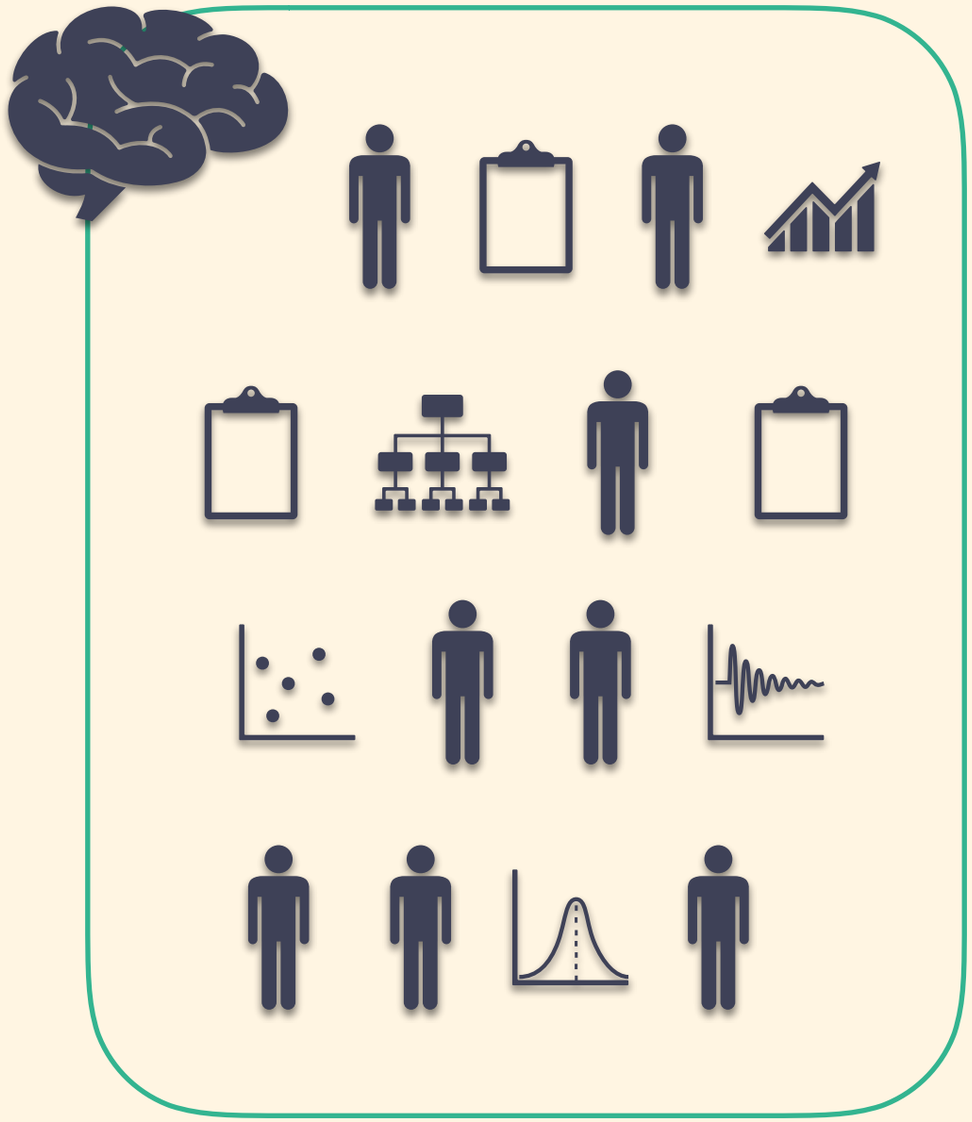
これまでの成果：SVP challengeの世界記録を達成

Q. Boot process +Security?

A. secure boot via ARM TrustZone™

権威ある国際学会・ジャーナルへの論文採録による安全性保証

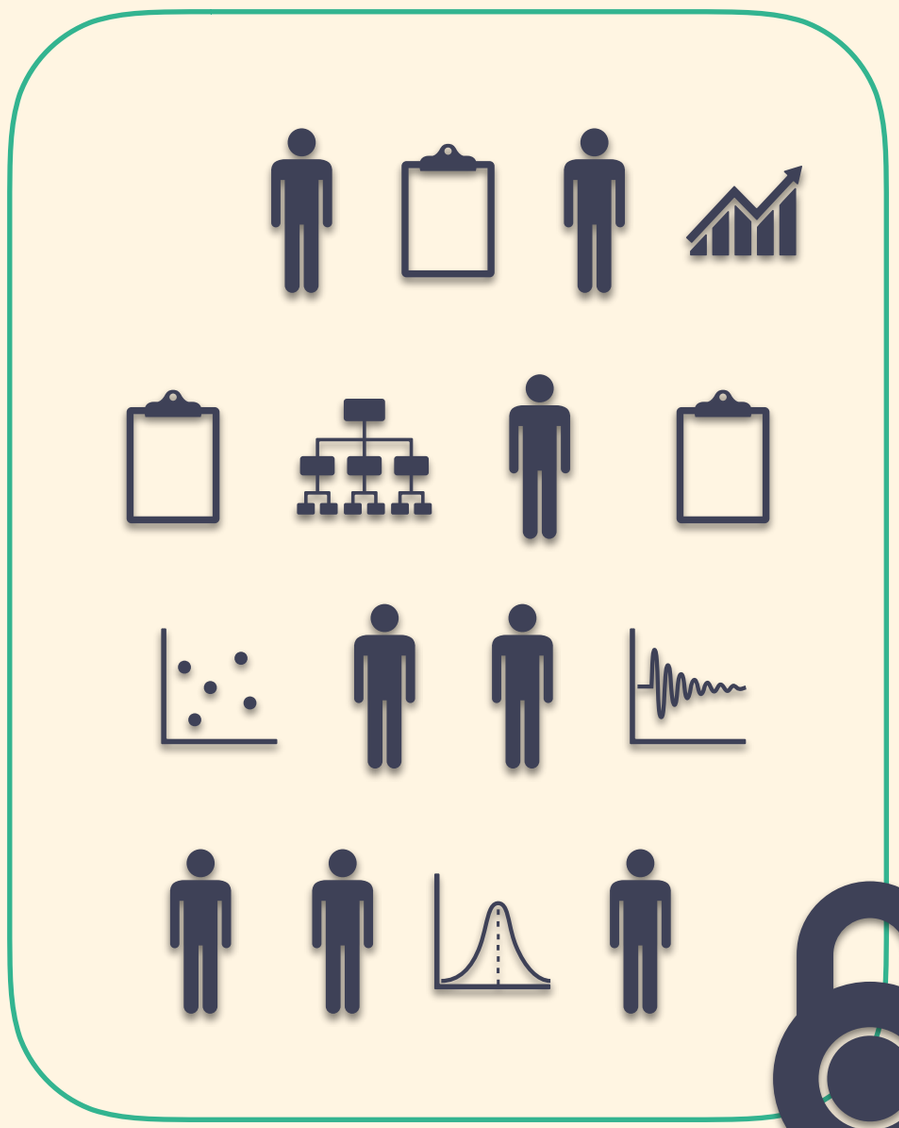
Big Data



Utility

health care, marketing,
financial, machine learning ...

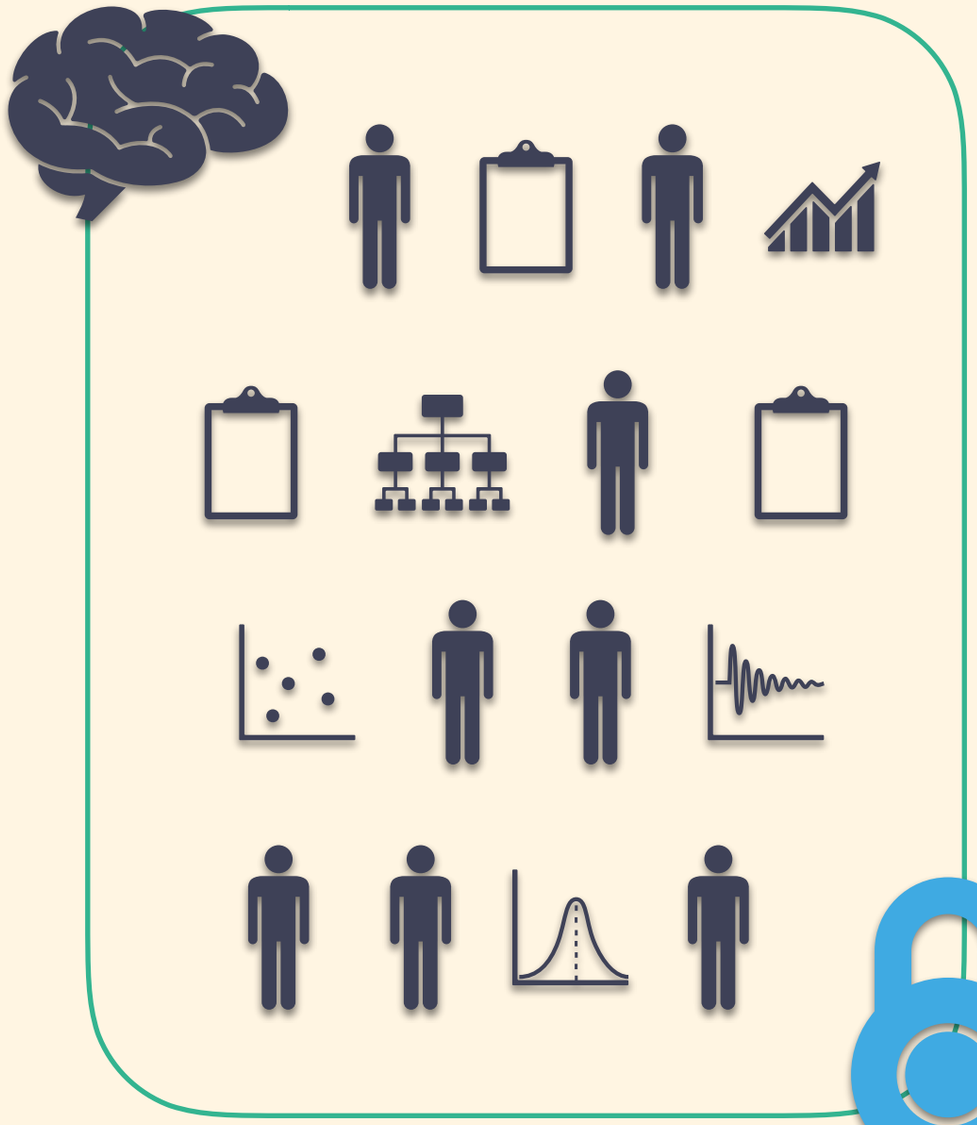
Big Data



Privacy

Problem:
traditional encryption
is **all-or-nothing**

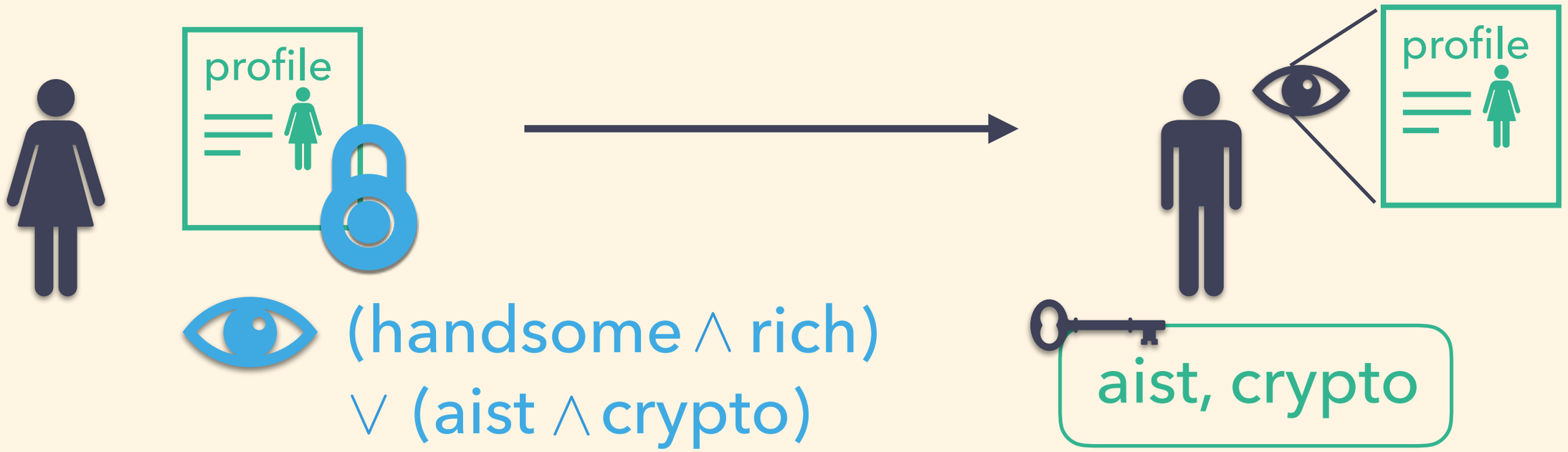
Big Data



Utility + Privacy?

encryption
with access control

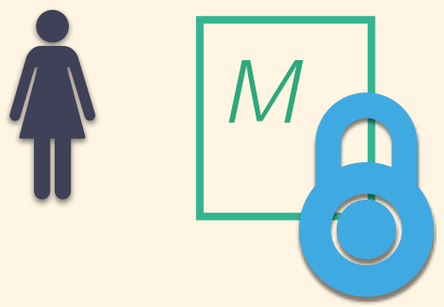
Example: Matchmaker Application



- 2015: infamous leak incident on a matchmaker service Ashley Madison http://www.businessinsider.com/cheating-affair-website-ashley-madison-hacked-user-data-leaked-2015-7

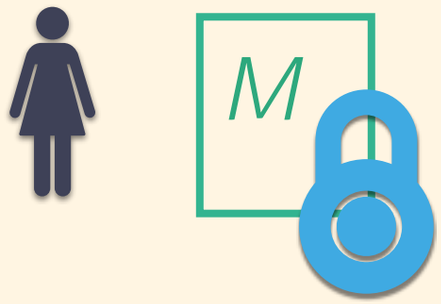
This application example is inspired by Hoeteck Wee's Asiacrypt 2016 talk.

Attribute Based Encryption



(aist ∧ crypto)

Attribute Based Encryption (naively)



(aist ∧ crypto)

$C = M \oplus R_{\text{aist}} \oplus R_{\text{crypto}}$

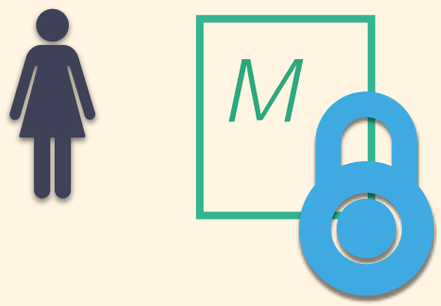
R_{aist} R_{crypto}

$C \oplus R_{\text{aist}} \oplus R_{\text{crypto}} \Rightarrow M$

R_{aist} R_{AI}

R_{phd} R_{crypto}

Attribute Based Encryption (naively)



(aist ∧ crypto)

$C = M \oplus R_{\text{aist}} \oplus R_{\text{crypto}}$

R_{aist} R_{crypto}

$C \oplus R_{\text{aist}} \oplus R_{\text{crypto}} \Rightarrow M$

R_{aist} R_{AI}

R_{phd} R_{crypto}

mix&match

Not secure if users **collude** ☹️

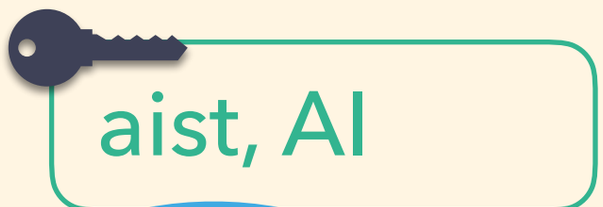
Attribute Based Encryption: Key Idea

Key Idea [SW05]

string $\mapsto$ **function**

$R_{\mathsf{aist}} \mapsto R_{\mathsf{aist}}(s)$

$R_{\mathsf{aist}}(s)$ $R_{\mathsf{crypto}}(s)$

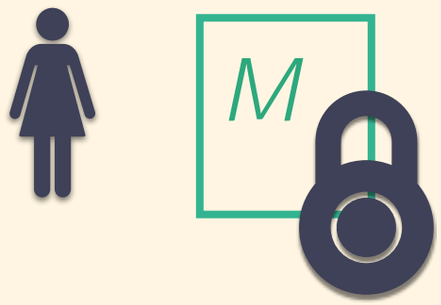


$R_{\mathsf{aist}}(t)$ $R_{\mathsf{AI}}(t)$

$R_{\mathsf{phd}}(u)$ $R_{\mathsf{crypto}}(u)$

mix&match **failed!**

Attribute Based Encryption: Toy Scheme



(aist $\wedge$ crypto)

$$C = \begin{cases} M + A \\ B_{\text{aist}} \quad B_{\text{crypto}} \end{cases}$$

$A - s + B_{\text{aist}}$ $\quad$ $s + B_{\text{crypto}}$

$A - t + B_{\text{aist}}$ $\quad$ $t + B_{\text{AI}}$

$A - u + B_{\text{phd}}$ $\quad$ $u + B_{\text{crypto}}$

still **one-time, private-key** scheme ☹️

Attribute Based Encryption

The Toy scheme	ABE	Key idea
one-time enc	multiple-time enc	$A \mapsto A(r)$
private-key enc	public-key enc	$B \mapsto g^B \bmod N$

- Public-key scheme: **Anyone** can encrypt.
- $g^B \bmod N$ hides B, and hence can be public.

(crypto basic: discrete log is hard.)

2-input AND

Inner product

Subspace membership

Bounded boolean formulae

Unbounded boolean formulae

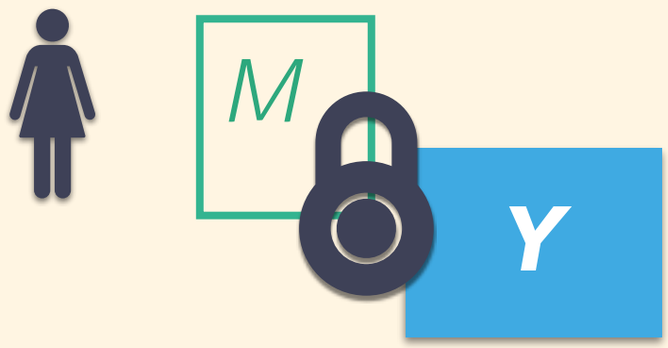
Boolean circuits

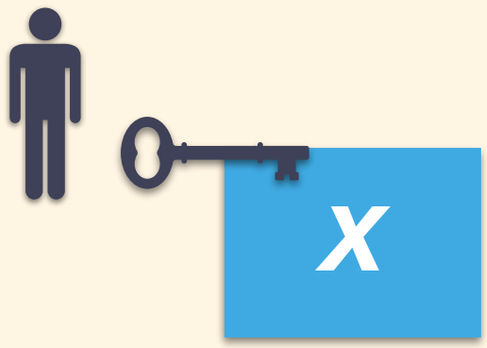
Arithmetic circuits

Turing machines

ABE for any policies?

General Design Framework for ABE





if $R(Y, X)=1$

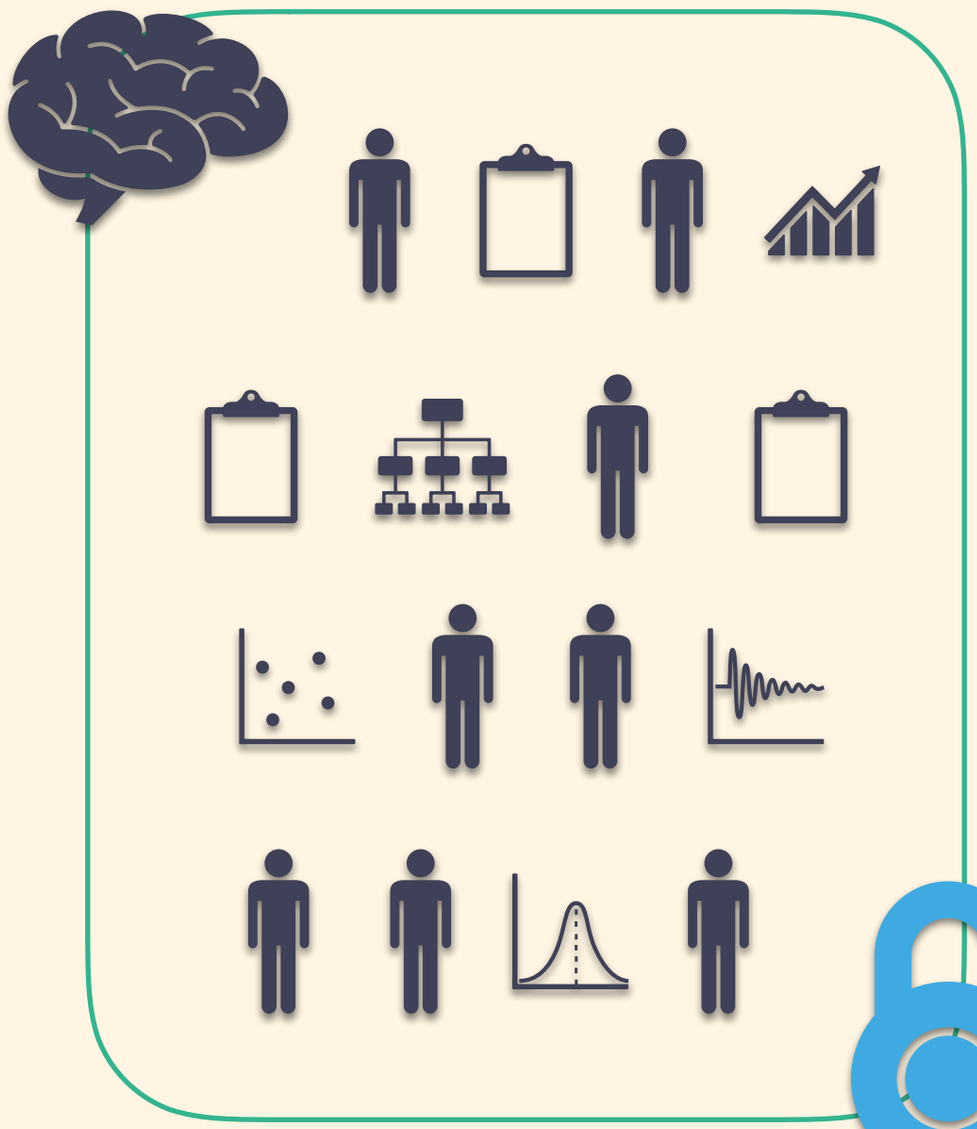
if $R(Y, X)=0$

Main results:

- [Attrapadung EUROCRYPT14]
- [Attrapadung ASIACRYPT16]
- [Attrapadung PKC17]
- Independently by [Wee TCC14], [Chen et. al. EUROCRYPT15]

Introduce "**Pair encoding**" functions *f(Y)* and *g(X)*

Big Data



Utility + Privacy?

Attribute Based Encryption

Utility+ Privacy/Security/Authenticity

Cryptography Platform

functional encryption

attribute-based encryption

homomorphic signature

homomorphic encryption

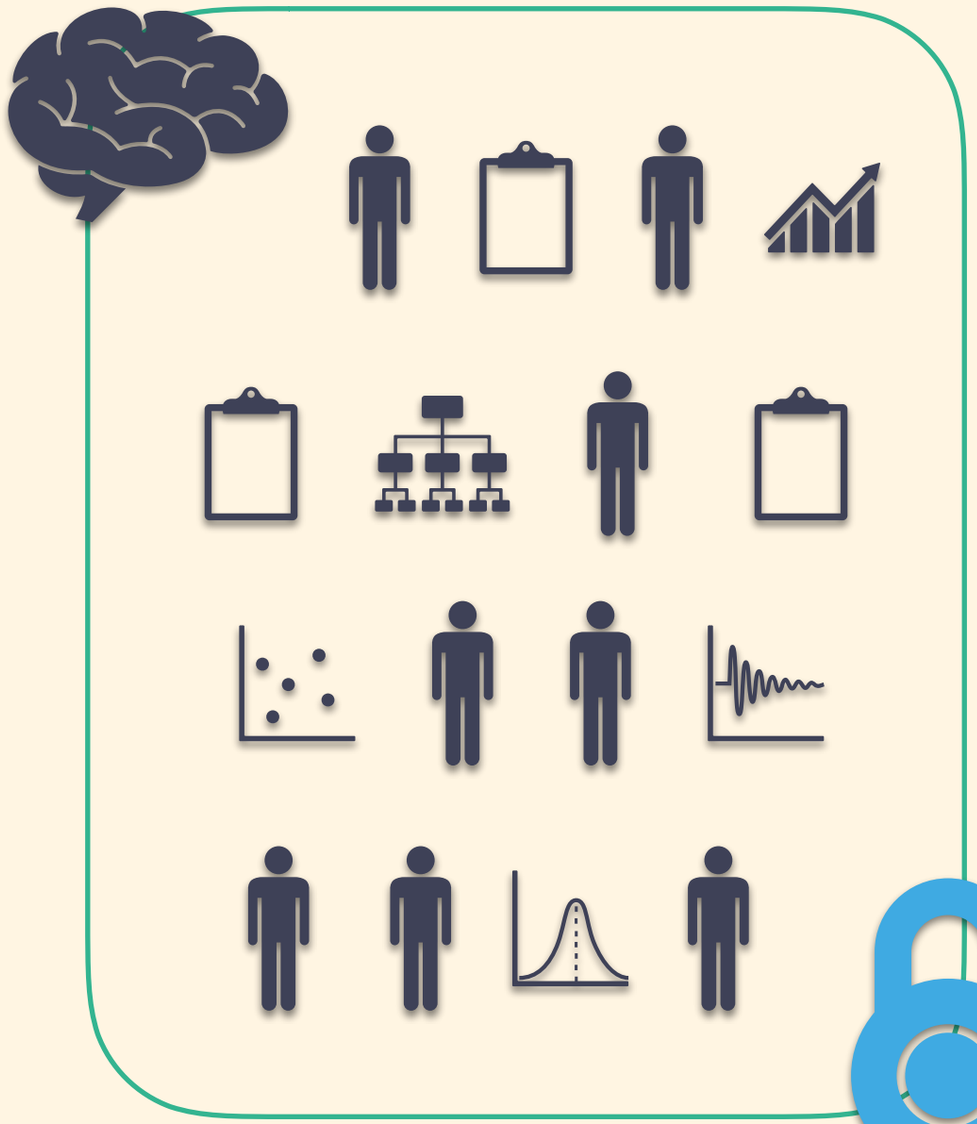
attribute-based signature

secure multi-party computation

pseudo-random functions

secure boot in trusted execution environment

Big Data

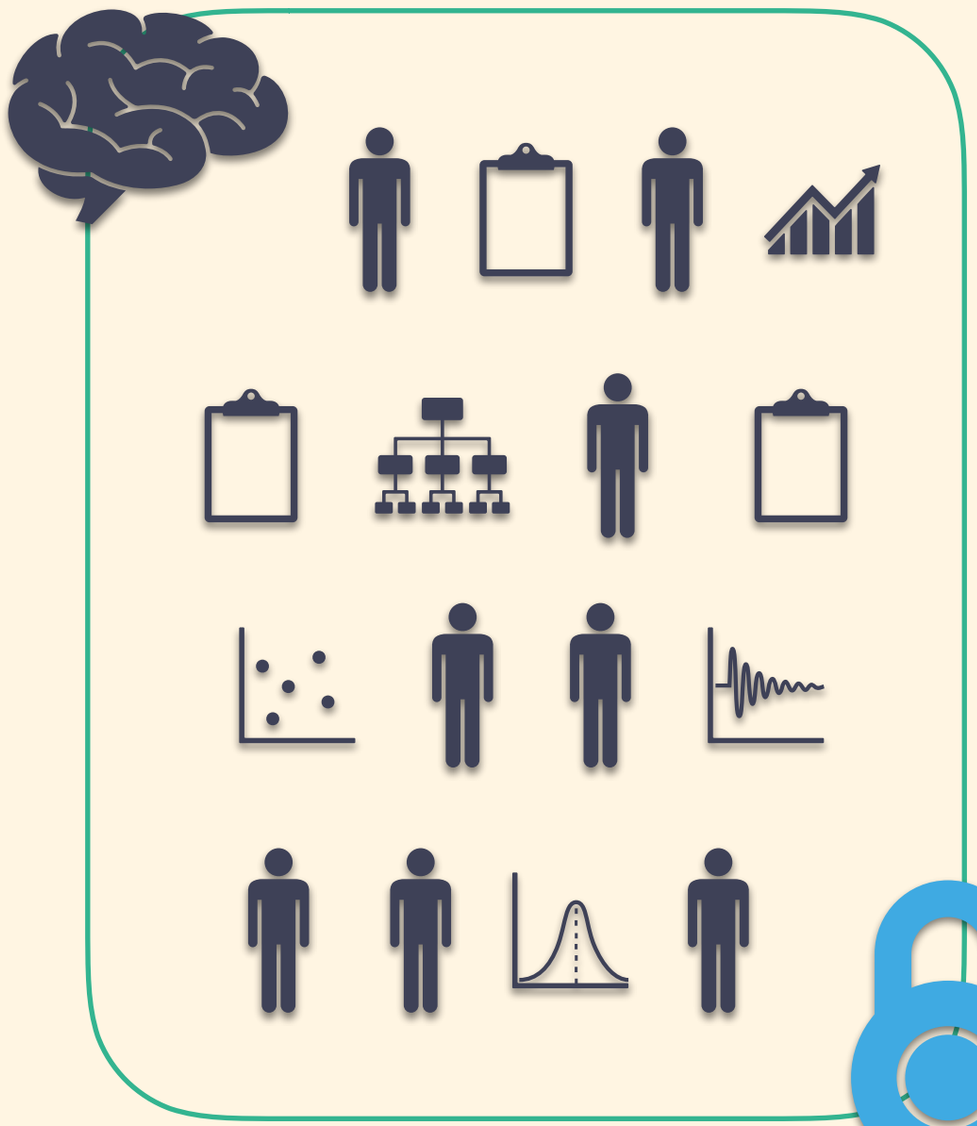


Utility + Privacy?

when accessing

Attribute Based Encryption

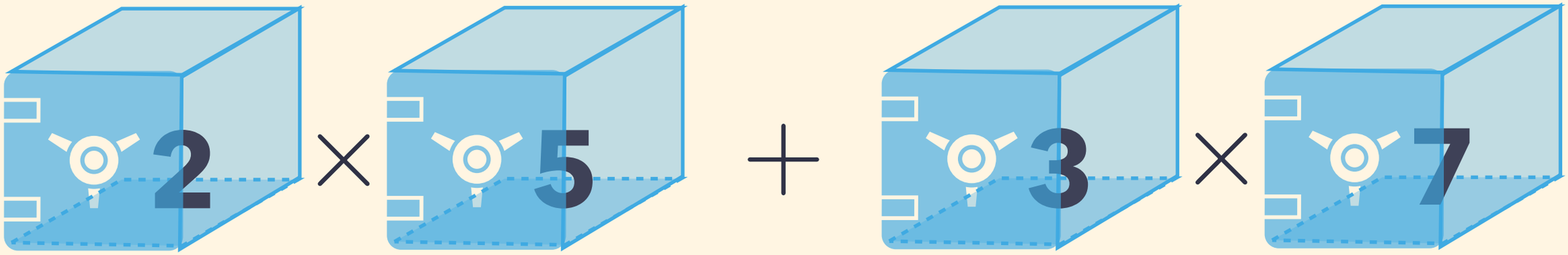
Big Data



Utility + Privacy?
when computing

Computing over encrypted data

Homomorphic Encryption



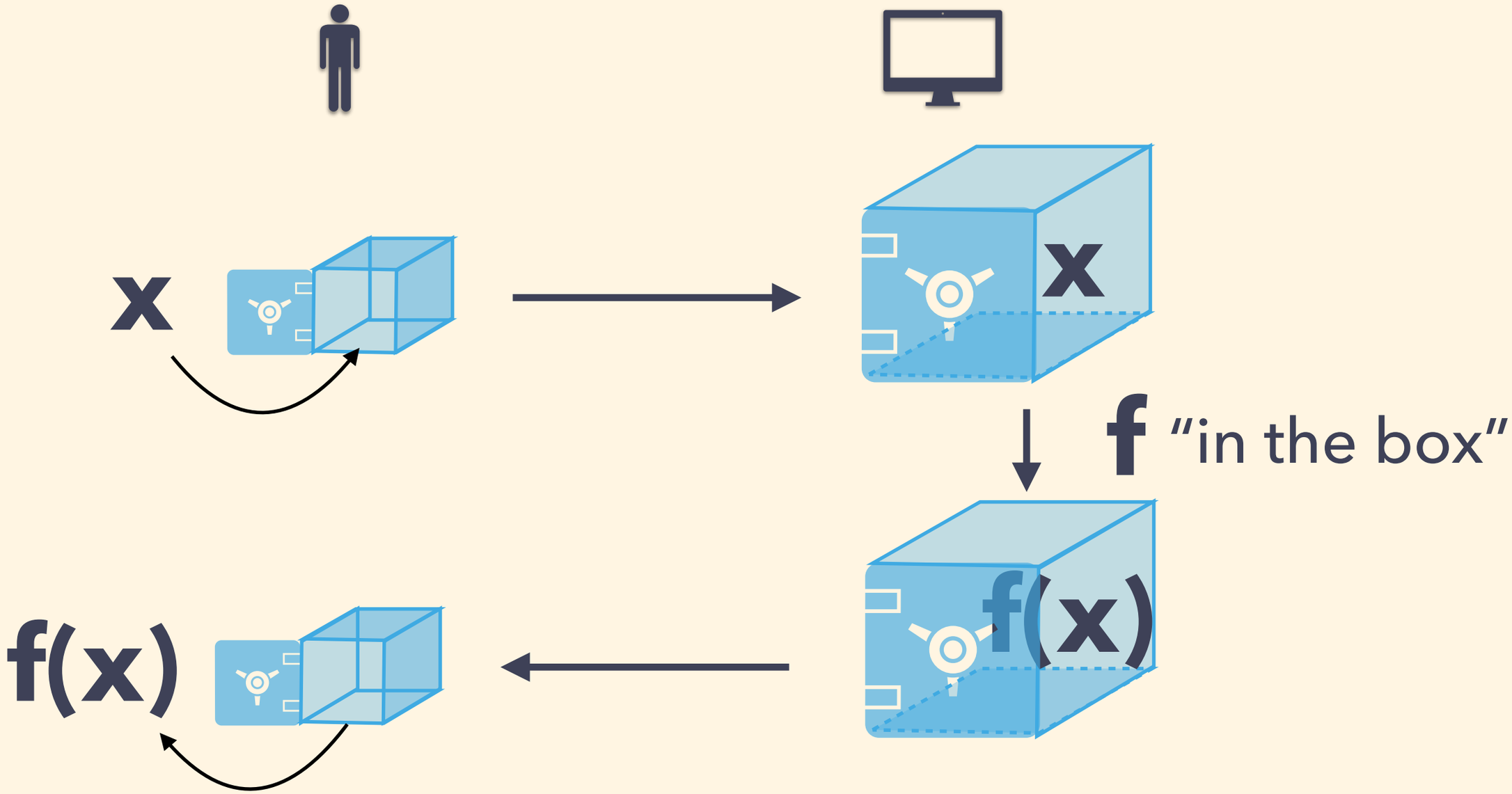
Our WebAssembly implementation

Encrypt	0.96 msec
Multiply	24.3 msec
Decrypt	12.6 msec

@Safari iPhone 7

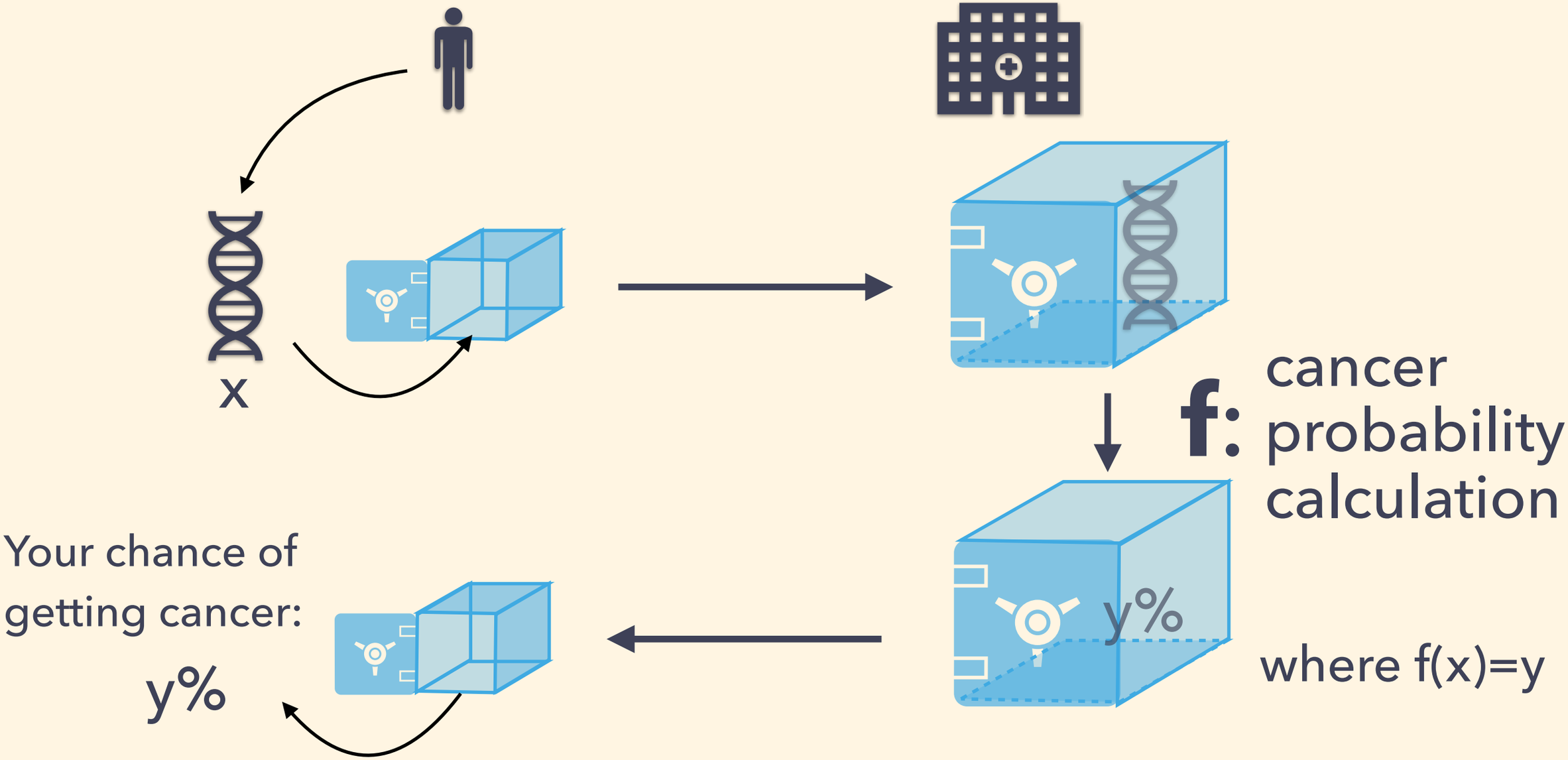
- Application: Secure outsourcing
- **Fully** homomorphic: can do any $+, \times$
- **Leveled** homomorphic: limited number of $\times$
  - Ours: fastest 2-level scheme [Attrapadung et al. AsiaCCS18]

Secure Outsourced Computation



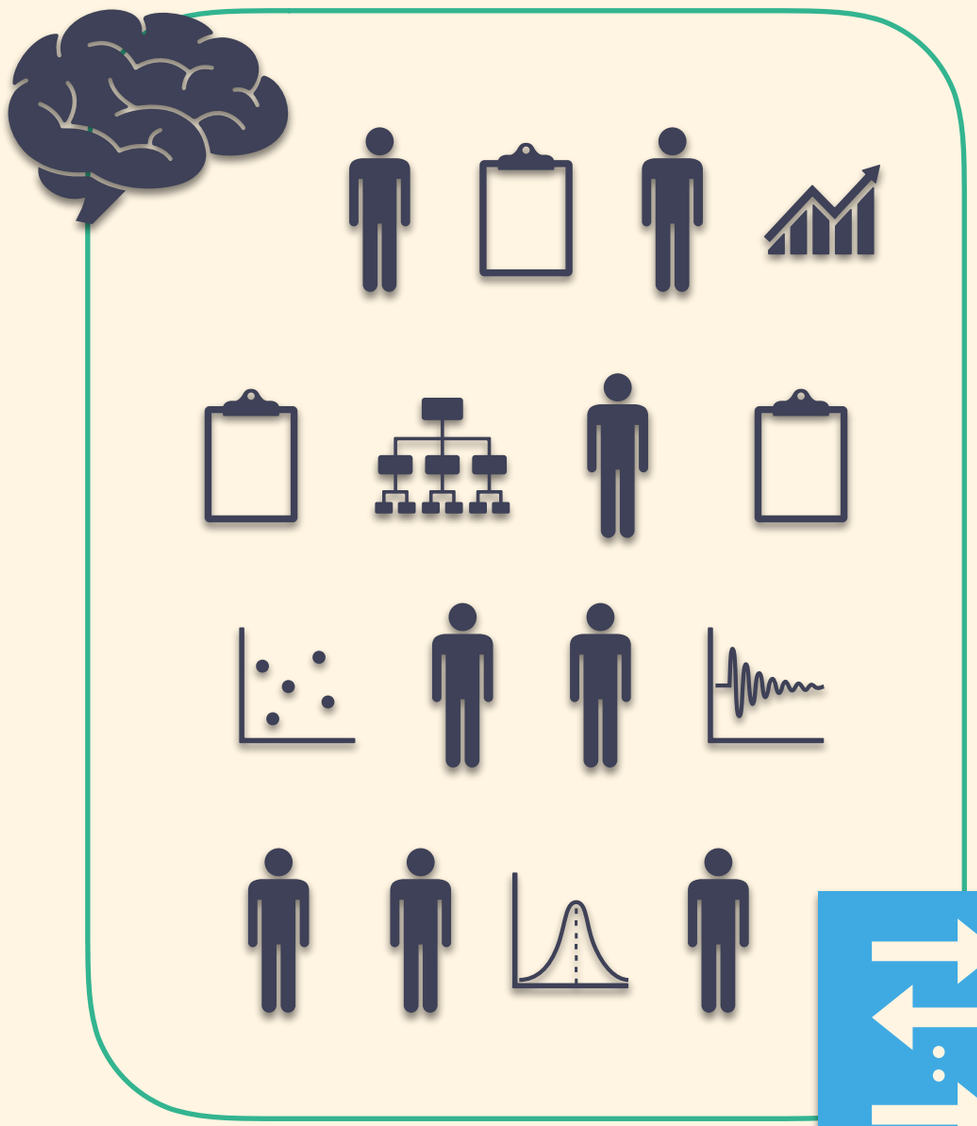
- **Hot topic:** f for **machine learning** (training/classification)
  - example: Microsoft Cryptonet [Dowlin et al. ICML16], …

Example: Private Personal Genome Test



- Not practical yet when f is heavy ☹️

Big Data

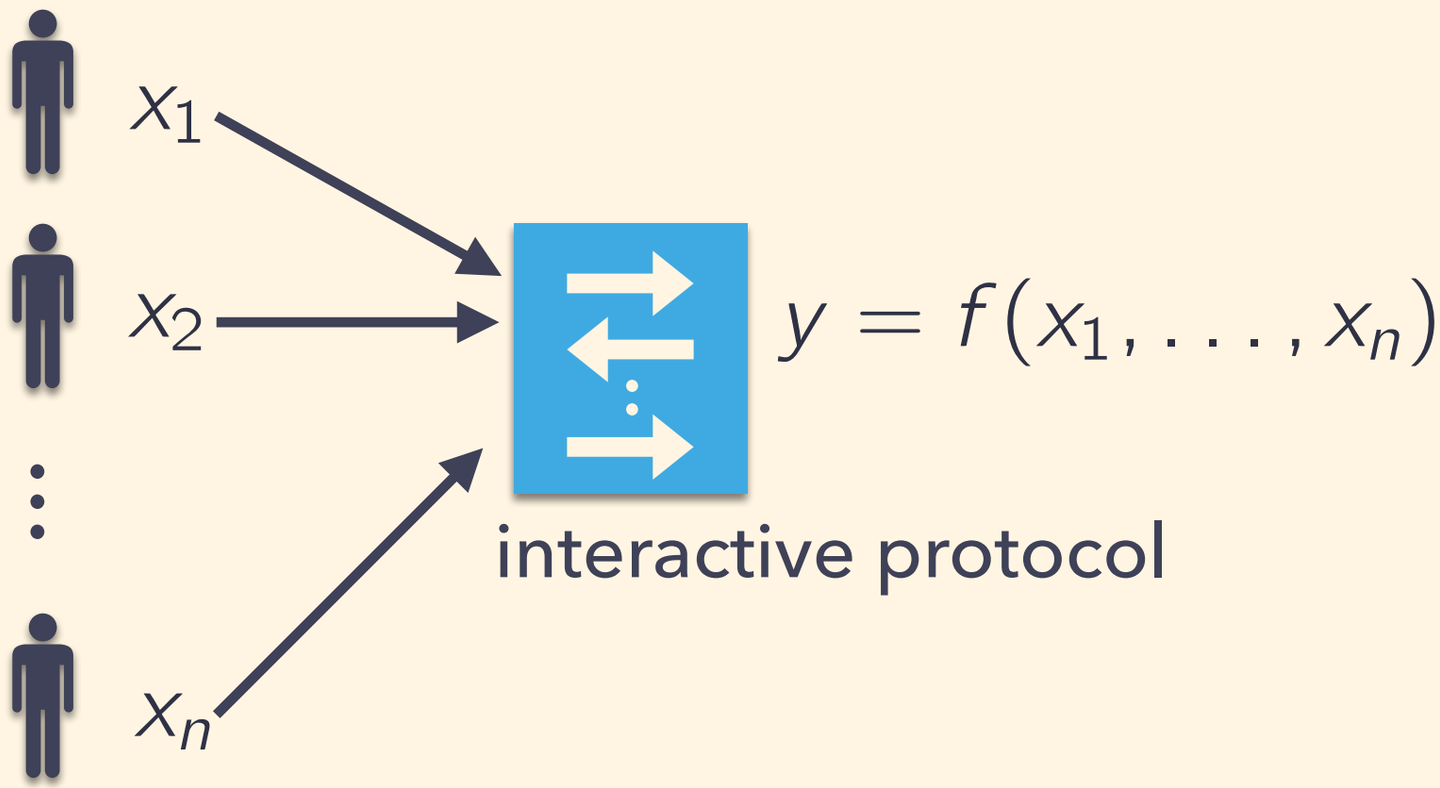


Utility + Privacy?
in joint computing

Secure Multi-Party Computation Protocol

Secure Multi-Party Computation (MPC)

Each holds private input

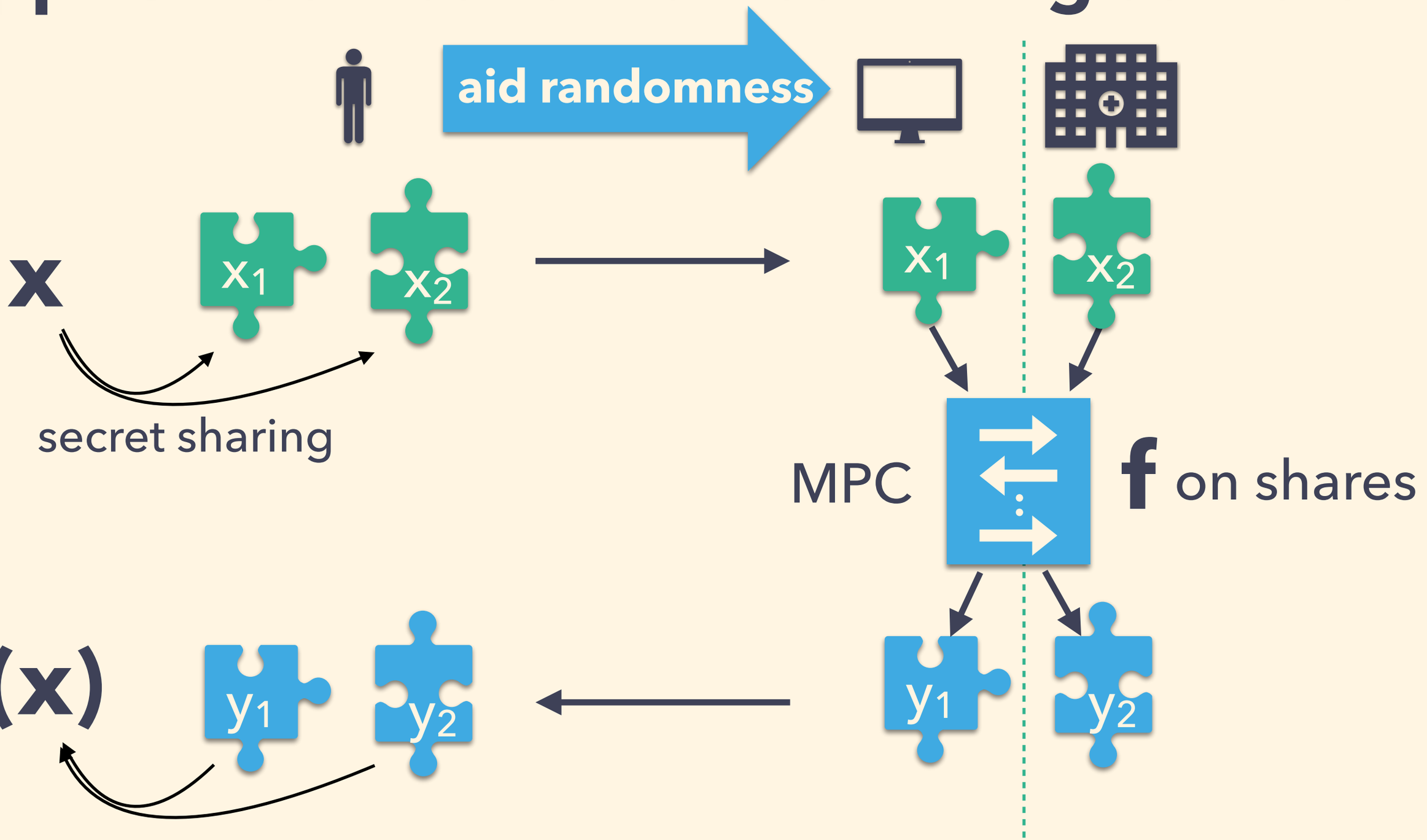


At the end

(i) knows only x_i, y

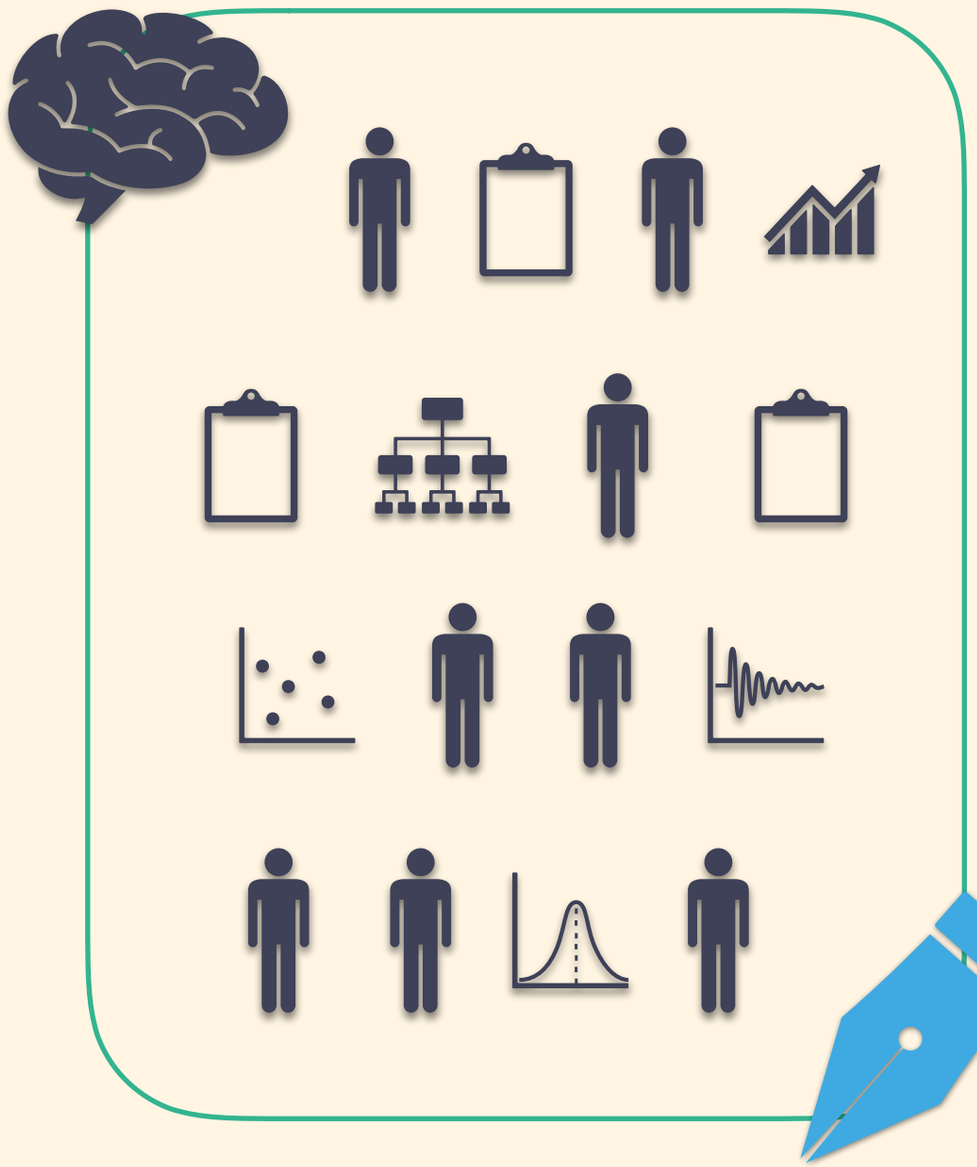
- **Hot topic:** f for **machine learning**
  - SecureML [CCS17], MiniONN [CCS17], Gazelle [USENIX18], Tapas [ICML18], …, Mobius [Our paper, arXiv18]

App: Outsource to Non-colluding servers



- Our result: Practical protocols via **client-aid** techniques
  [Morita, Attrapadung, Teruya, Ohata, Nuida, Hanaoka ESORICS18]

Big Data

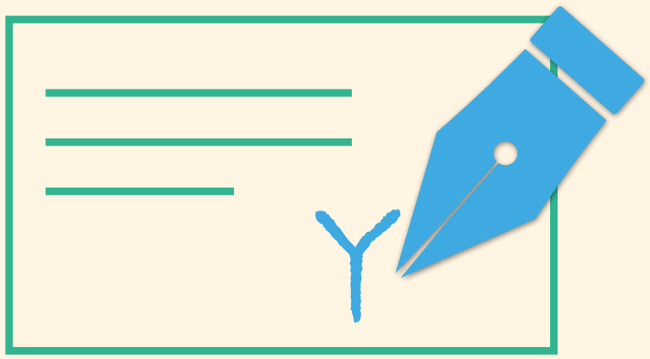


Utility + Privacy?
while authenticating

Attribute Based Signature

Attribute Based Signature

can sign



if $R(X, Y)=1$

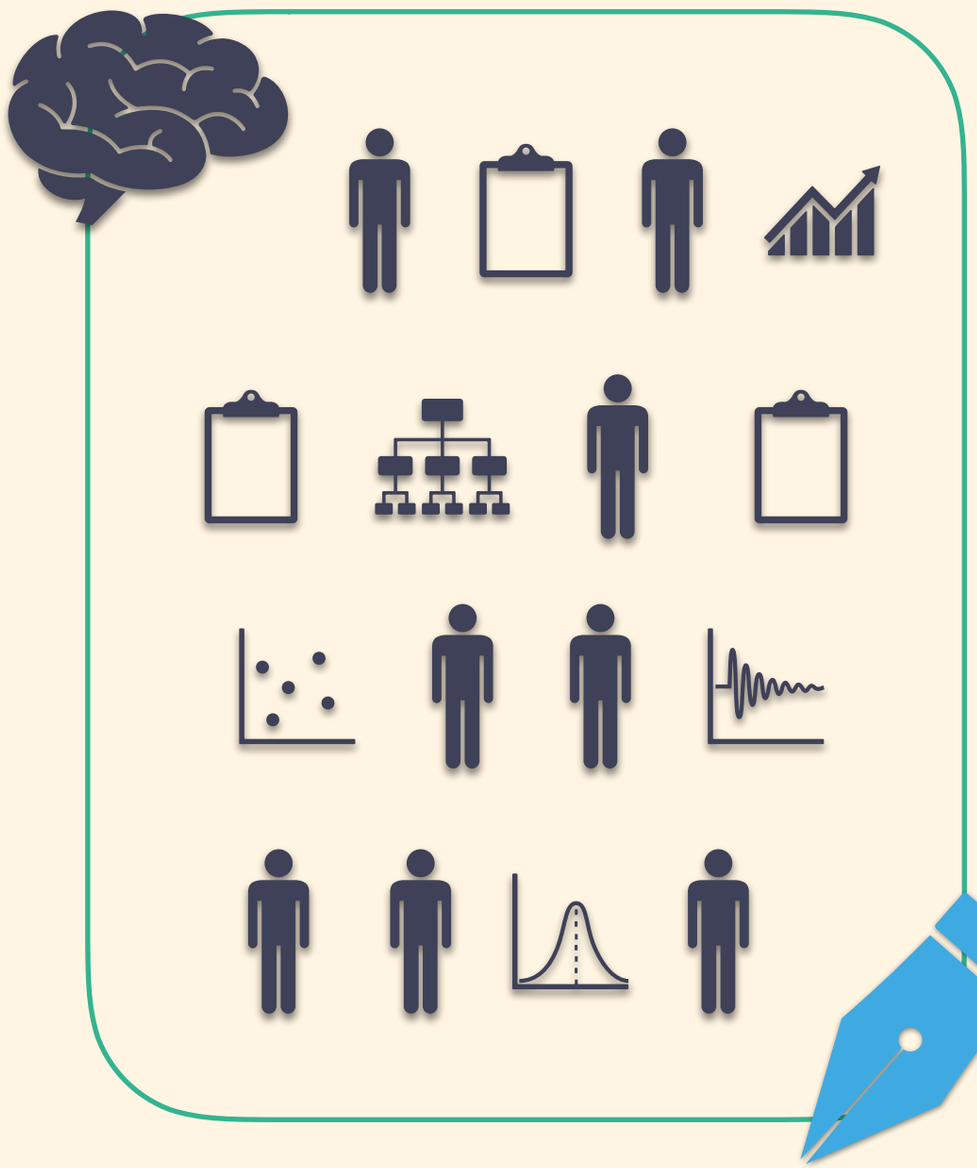
X: aist, crypto

Y: $(\text{aist} \vee \text{phd}) \wedge (\text{crypto} \vee \text{AI})$

Privacy: X is private

- Applications: anonymous credentials
- Our result: Schemes for **any circuits/ Turing machines**
  - [Sakai, Attrapadung, Hanaoka PKC16]
  - [Sakai, Katsumata, Attrapadung, Hanaoka Asiacrypt18]

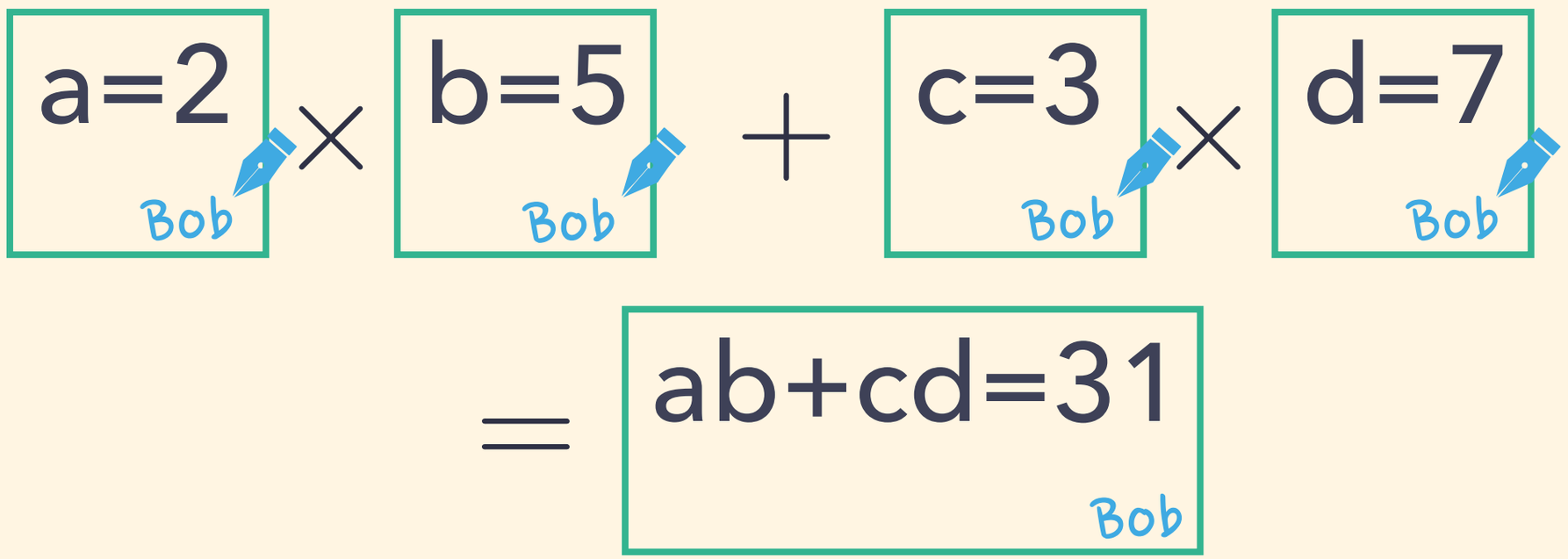
Big Data



Util.+ Authenticity?

Homomorphic Signature

Homomorphic Signature



- Application: **Verifiable** computation
- **Fully** homomorphic: can do any $+, \times$
- **Linear** homomorphic: can do $+$
  - Ours: efficient schemes [Attrapadung et al. PKC11, PKC13 ASIACRYPT12]

What We Do from Now

Utility + Privacy/Security/Authenticity

Cryptography Platform

functional encryption

attribute-based encryption

homomorphic signature

homomorphic encryption

attribute-based signature

secure multi-party computation

pseudo-random functions

secure boot in trusted execution environment

What We Do from Now

Utility + Privacy/Security/Authenticity

- **New applications** — Society 5.0

Cryptography Platform

functional encryption

attribute-base

homomorphi

secure multi-p

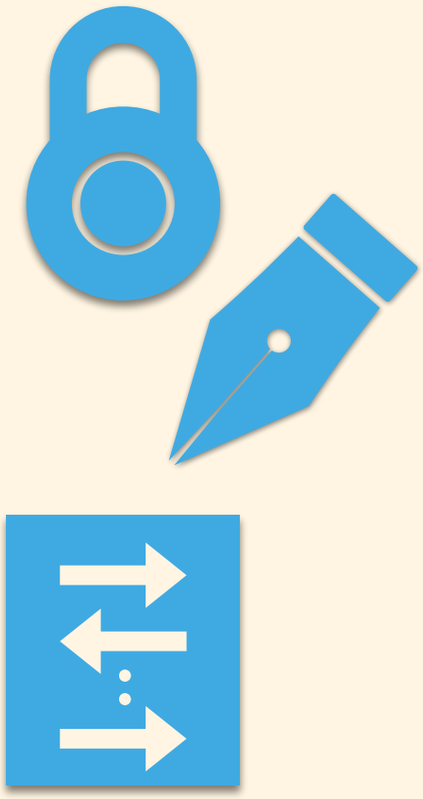
ons

- **New primitives/improved schemes**
- **"Cryptographic Agility"**
  ability to switch/combine tools

secure boot in trusted execution environment

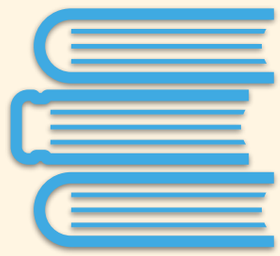
Summary: I introduced

- **Cryptography Platform Research Team @** CPSEC Cyber Physical Security Research Center



- **attribute based** / **homomorphic** encryption
- **attribute based** / **homomorphic** signature
- **secure multi-party computation** protocols

- Ongoing work
  - **Cryptographic Agility**
  - Secure and fast **implementations**



Thank you !

AIST

CPSEC
Cyber Physical Security Research Center