# Toward Practical Threshold FHE: Low Communication, Computation and Interaction

Hyeongmin Choe

Seoul National University

Oct 14, 2024
Salt Lake City, USA

ACM CCS'24 Doctoral Symposium

# Table of Contents

- Brief Introduction
  - Homomorphic Encryption (HE)
  - Threshold HE
  - Challenges

- This Work

0. Another new challenge in efficient Threshold HE [CCS:CCP+24].

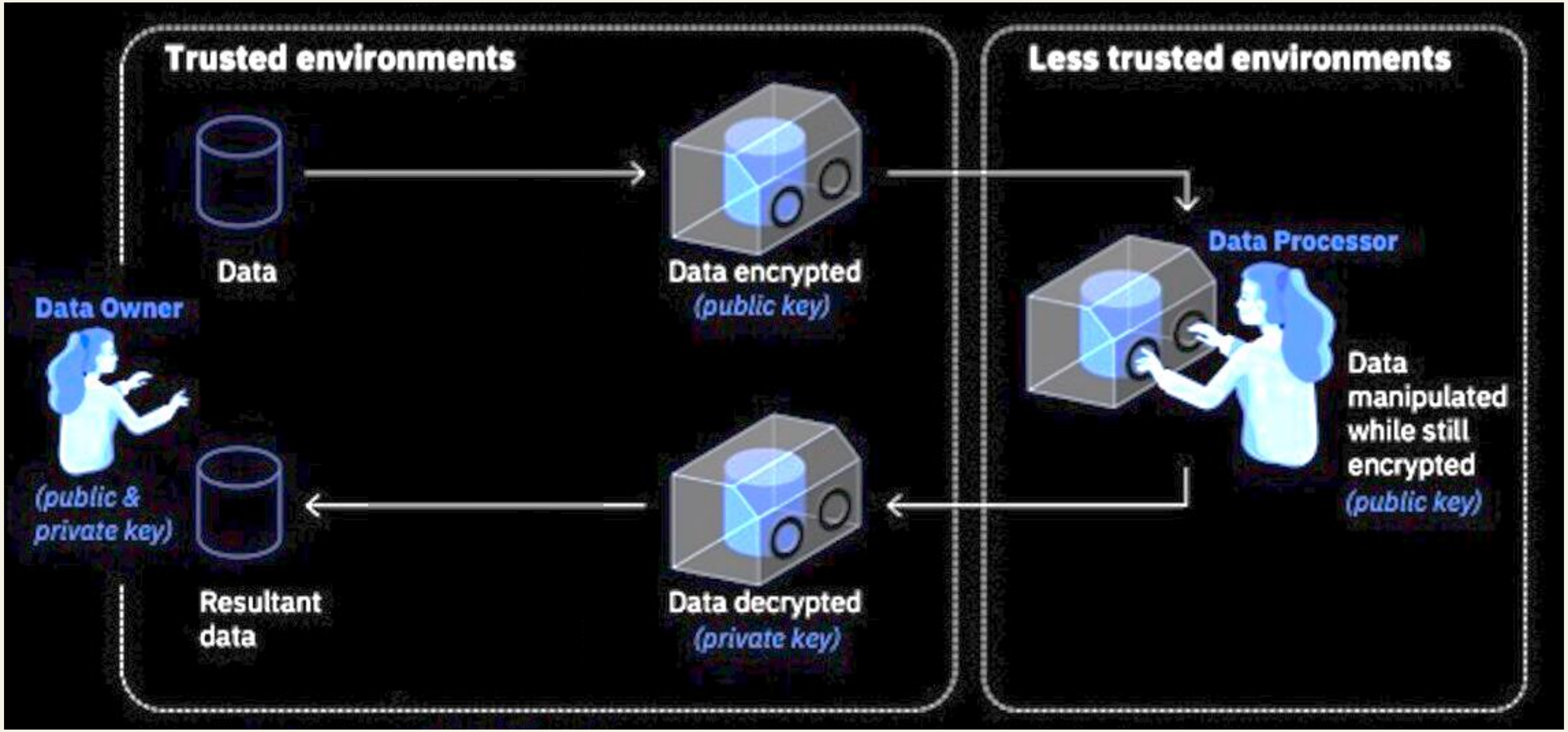
1. Simpler, more efficient, and more secure construction based on [AC:BS23].

2. Infeasibility of the assumption used in both [AC:BS23] and 1.

3. New definition for Threshold HE achieving Sim-security, efficiency in practical scenarios, whose performance close to HE.

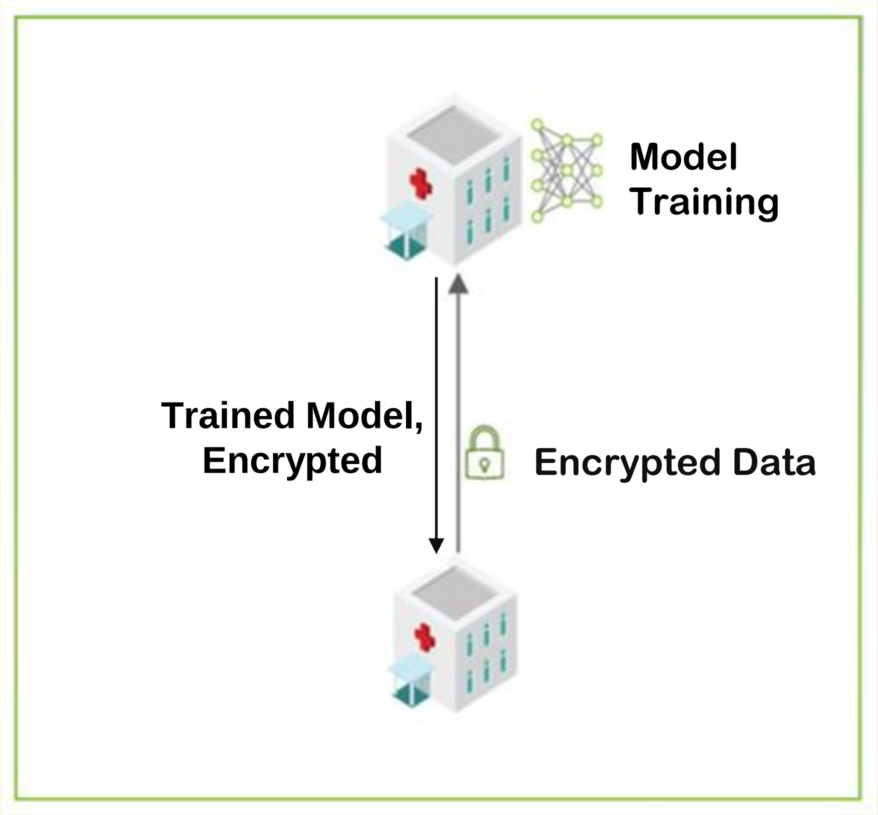
# Homomorphic Encryption (HE)

- Encryption scheme for computing without decryption.

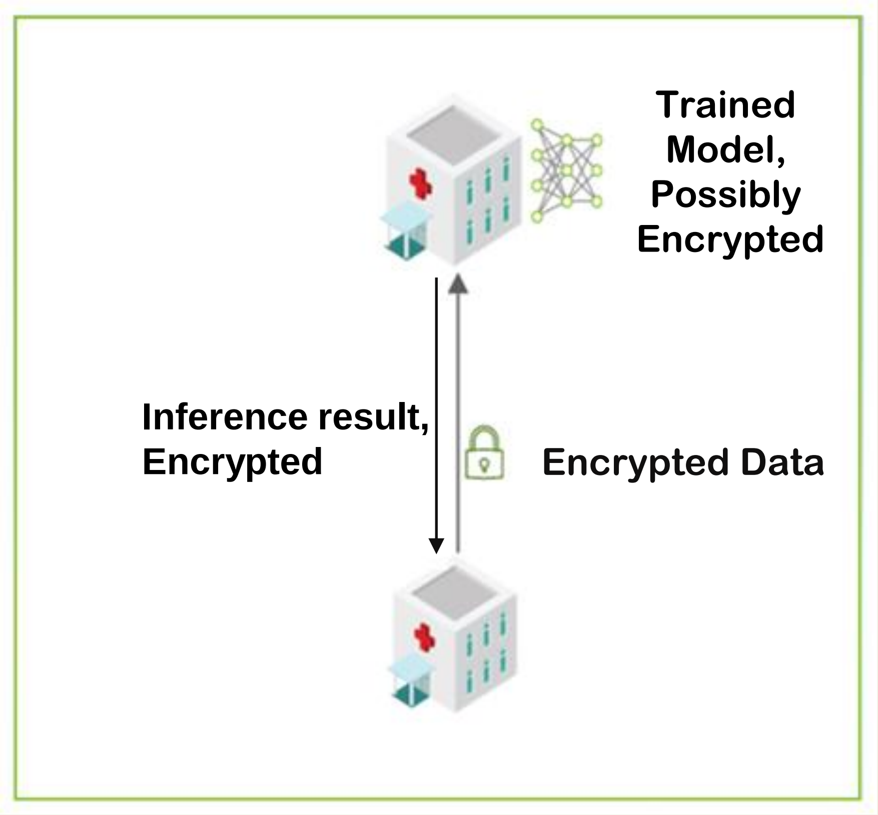


# Homomorphic Encryption (HE)

- Privacy Enhancing Technology (PET)
  - Private AI or Privacy-preserving ML (PPML)




Training

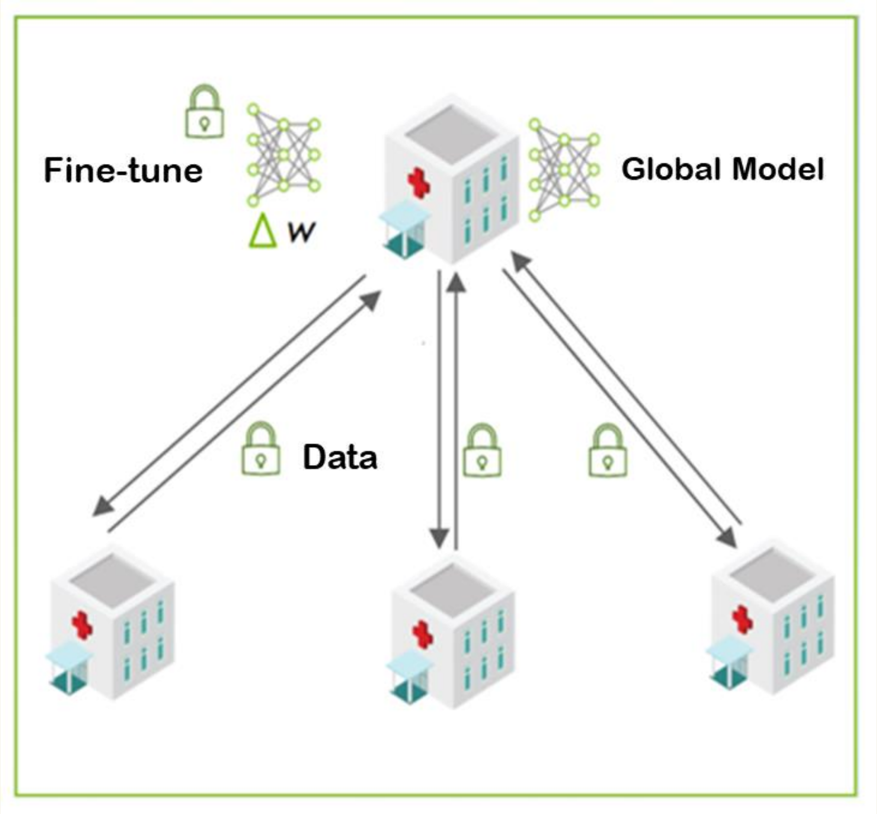



Inference

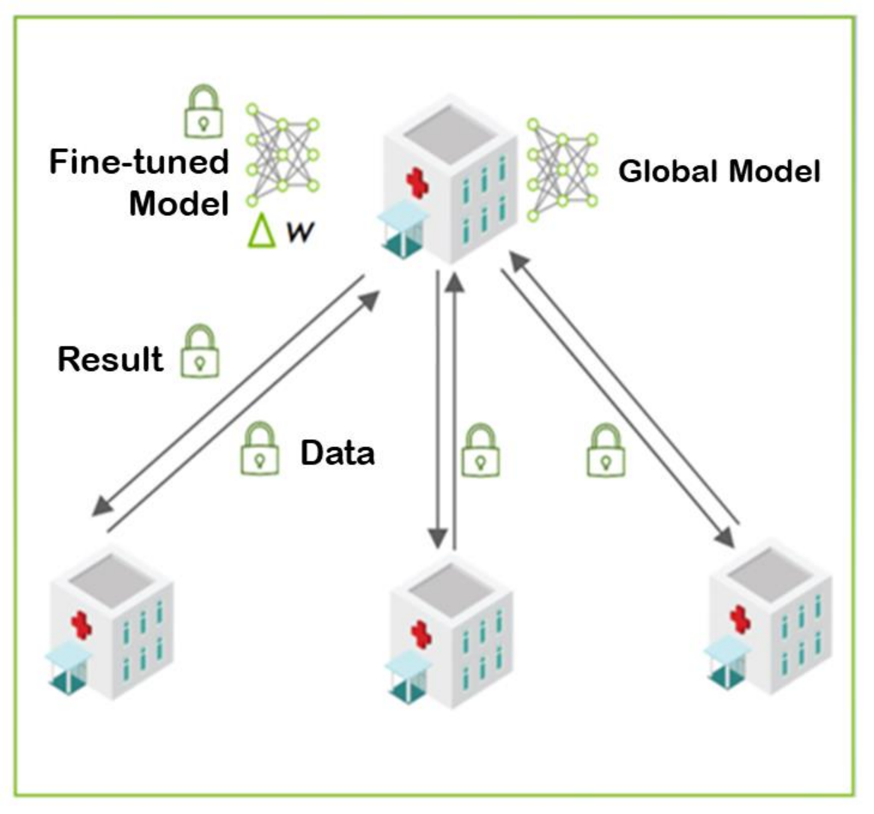
Image from https://files.speakerdeck.com/presentations/bbb6d1c6c1084af9b033a99910900ecd/slide_32.jpg, modified.

# Homomorphic Encryption (HE)

- Privacy Enhancing Technology (PET)
  - Private AI or Privacy-preserving ML (PPML) with multiple parties



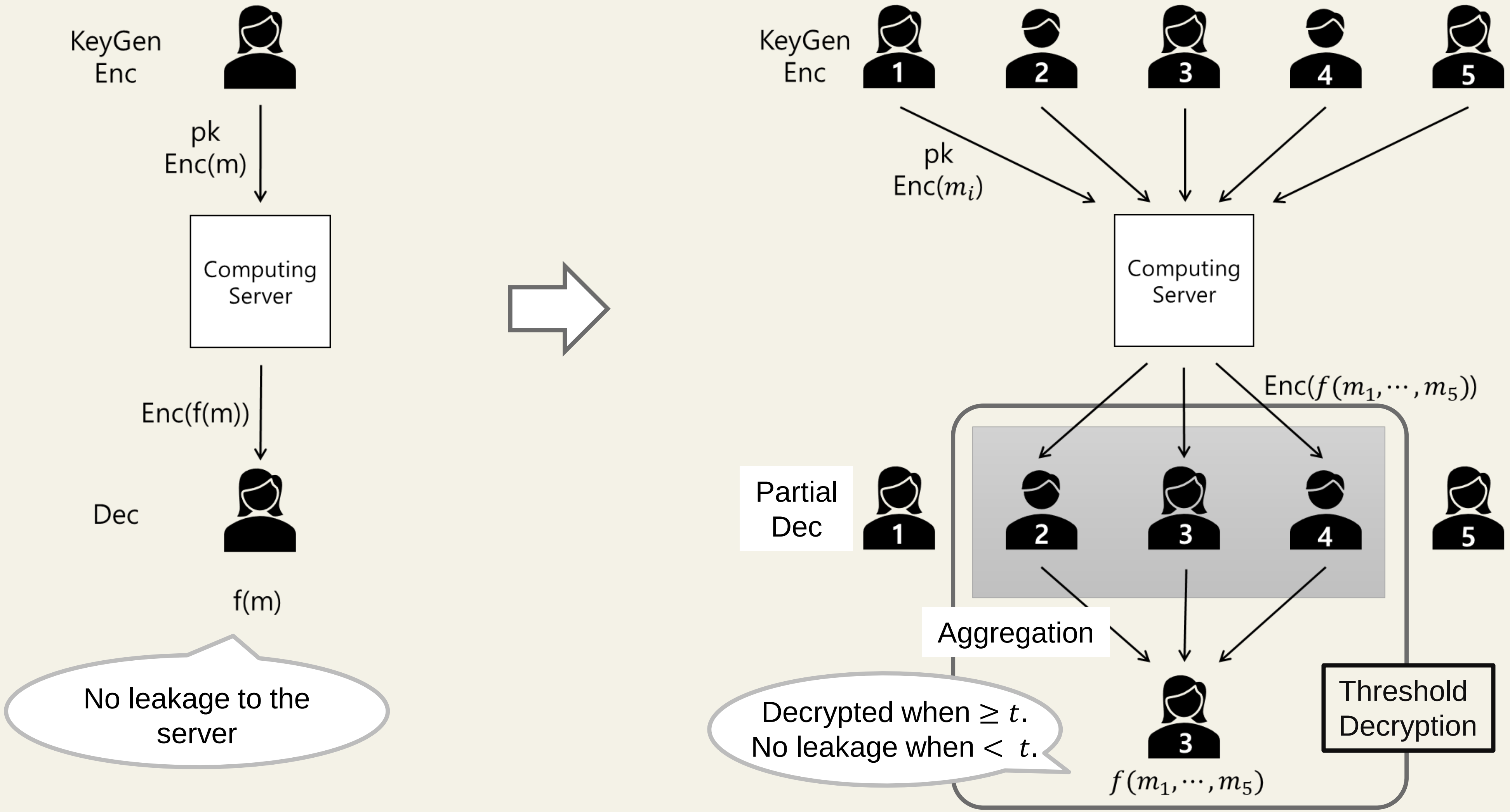

Fine-tuning with global model




Inference

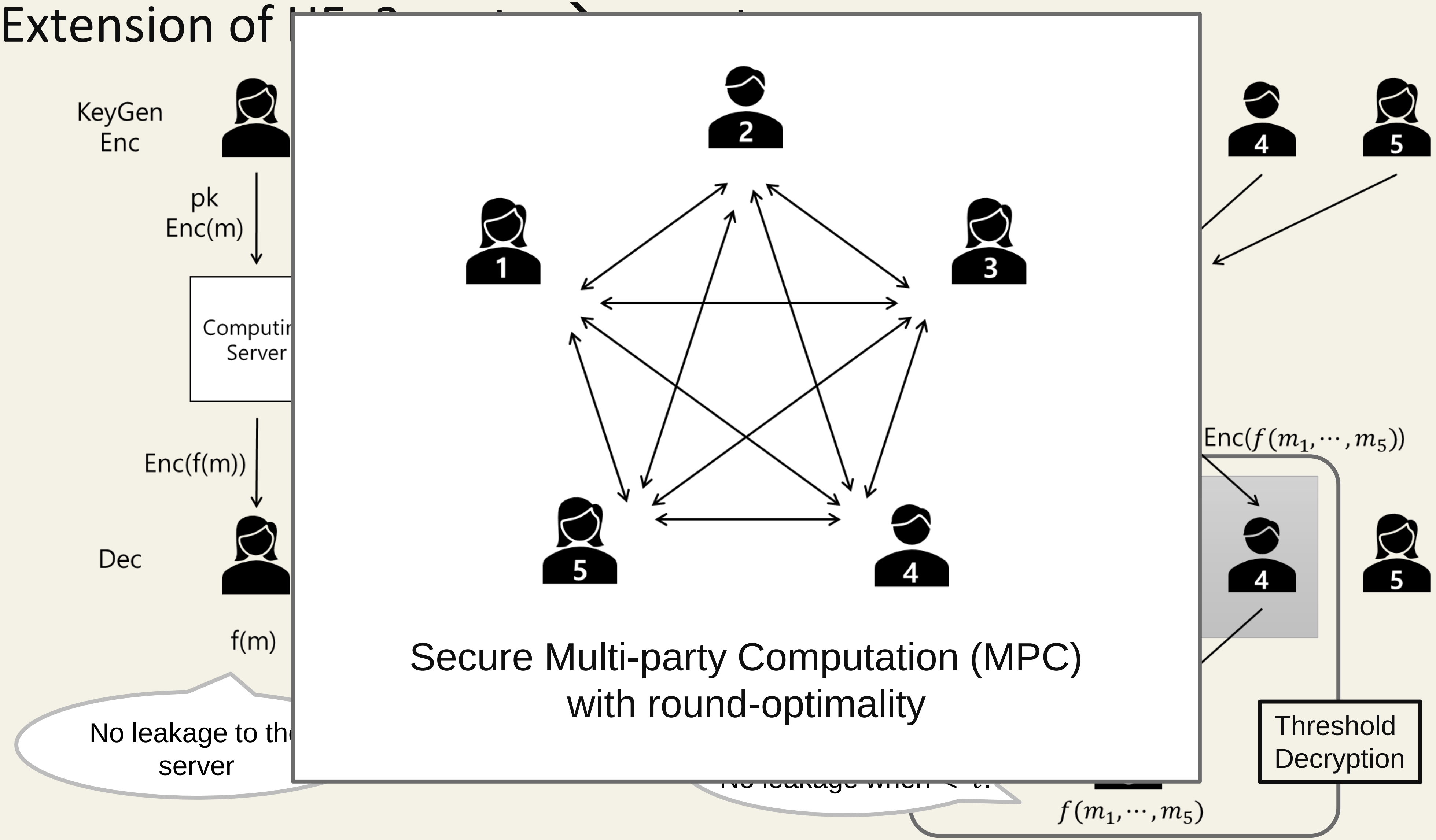
# Threshold HE

- Extension of HE: 2-party → n-party



# Threshold HE

- Extension of



# Threshold HE

- Encryption/Decryption in 2-party HE
  - based on Ring LWE (Learning-With-Errors)

over a polynomial ring $R_Q = \mathbb{Z}_Q[x]/(x^N + 1)$

  - $\mathrm{Enc}(m) = (a, b = -a \cdot s + \Delta \cdot m + e\ )$
  - $\mathrm{Dec}(a, b) = \left\lfloor \frac{b+as}{\Delta} \right\rceil = m$

# Threshold HE

- Threshold Decryption in Threshold HE
  - The secret is additively shared: $s = s_1 + \cdots + s_n$
  - Partial Dec by $i$-th party:

Smudging error

$$(a, b) \in R_Q^2 \mapsto p_i := as_i + e_i \in R_Q$$

  - Aggregation by receiver party:

Correct if $\Delta > e + \sum e_i$

$$\left\lfloor \frac{b + p_1 + \cdots + p_n}{\Delta} \right\rceil = \left\lfloor \frac{b + as + e_1 + \cdots + e_n}{\Delta} \right\rceil = m$$

- Exponentially large smudging error
  - Exponentially large $\Delta = O(\sqrt{n} \cdot 2^\lambda)$ & $Q = O(\sqrt{n} \cdot 2^\lambda)$
  - Introducing comp & comm inefficiency

# Threshold HE

- Threshold Decryption in Threshold HE
  - The secre
  - Partial De

One of the main challenges for efficient Threshold HE compared to 2-party HE!

$e + \sum e_i$

  - Aggregat

[ $\Delta$ ] [ $\Delta$ ]

- Exponentially large smudging error
  - Exponentially large $\Delta = O\left(\sqrt{n} \cdot 2^{\lambda}\right)$ & $Q = O\left(\sqrt{n} \cdot 2^{\lambda}\right)$
  - Introducing comp & comm inefficiency

# Threshold HE

- Prior works reducing smudging errors
  - Weaker security definition
    - Bounded queries, ROM [DWF22]
    - IND-security, non-adaptive [CSS+22]
    - IND-security, ROM, Circuit Privacy [AC:BS23] which is claimed wrong [AC:PS24]
  - New assumption
    - Known-norm RLWE [MS23]
    - RLWE + error sharing [OT24]
  - Mitigating/generalizing Threshold HE definition
    - Sanitizing algorithm [AC:PS24]

Weak for MPC

Threshold PKE
not HE

Need
“non-corrupting”
party


[DWF22] Dai, Wu, and Feng. Key lifting: Multi-key fully homomorphic encryption in plain model without noise flooding.
[CSS+22] Chowdhury et al. Efficient threshold FHE with application to real-time systems.
[AC:BS23] Boudgoust and Scholl. Simple Threshold (Fully Homomorphic) Encryption From LWE With Polynomial Modulus, *Asiacrypt 2023.*
[AC:PS24] Passelegue and Stehle. Low Communication Threshold Fully Homomorphic Encryption, *Asiacrypt 2024.*
[MS23] Micciancio and Suhl. Simulation-Secure Threshold PKE from LWE with Polynomial Modulus.
[OT24] Okada and Takagi. Simulation-Secure Threshold PKE from Standard (Ring-)LWE.

# This Work

- Prior works reducing smudging errors

0. Another challenge in efficient Threshold HE: Requiring "IND-CPA^D" security and overwhelming correctness [CCS:CCP+24].

  - IND-security, non-adaptive [CSS+22]
  - IND-security, ROM, Circuit Privacy [AC:BS23] which is claimed wrong [AC:PS24]

1. Simpler and efficient variant with Sim-security under weaker assumptions.

2. Infeasibility of the "Circuit Privacy" assumption in both [AC:BS23] and 1.

⇨ 0, 1, 2: Hardness of achieving both "efficiency" close to HE & the strongest "Sim-security."

- Mitigating/generalizing Threshold HE definition

Need

⇨ 3. New definition, which is efficient in practical scenarios, achieving Sim-security, and performance close to HE.

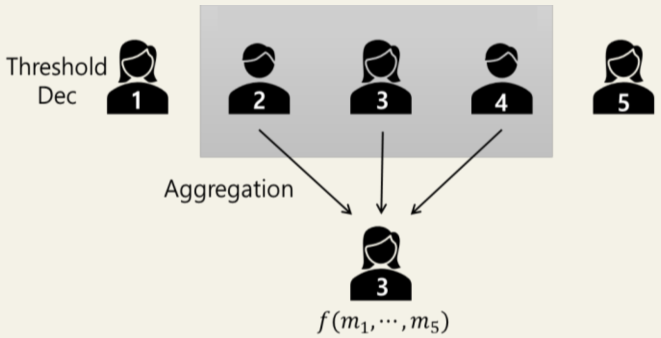

[DWF22] Dai, Wu, ...
[CSS+22] Chowdhury et al. Efficient threshold FHE with application to real-time systems.
[AC:BS23] Boudgoust and Scholl. Simple Threshold (Fully Homomorphic) Encryption From LWE With Polynomial Modulus, *Asiacrypt 2023.*
[AC:PS24] Passelegue and Stehle. Low Communication Threshold Fully Homomorphic Encryption, *Asiacrypt 2024.*
[MS23] Micciancio and Suhl. Simulation-Secure Threshold PKE from LWE with Polynomial Modulus.
[OT24] Okada and Takagi. Simulation-Secure Threshold PKE from Standard (Ring-)LWE.

# This Work

- Mitigate the “Threshold Decryption”
  - Trade-off: comp. + comm. cost vs. rounds:

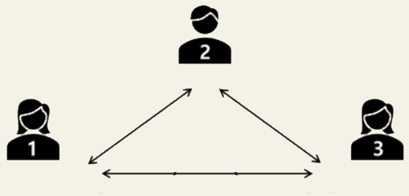
---

- 1-round threshold dec.
- Exponentially large $\Delta$ & $Q$




$p_i \coloneqq as_i + e_i \in$

- Constant-round threshold dec.
- Small $\Delta$ & $Q$




$$a, b, [s] \mapsto [\Delta m + e] \mapsto \left[ \left\lfloor \frac{\Delta m + e}{\Delta} \right\rceil = m \right]$$

Given $ctxt = (a, b)$, each party makes secret share of $b + as = \Delta m + e \bmod Q$:

$$[b + as]_i = \begin{cases} b + as_1 & (i = 1) \\ as_i & (i \neq 1) \end{cases}$$

Exact division (truncation)

Cf. $[X]$: secret share of $X = \sum X_i$, where each party holds a random $X_i$

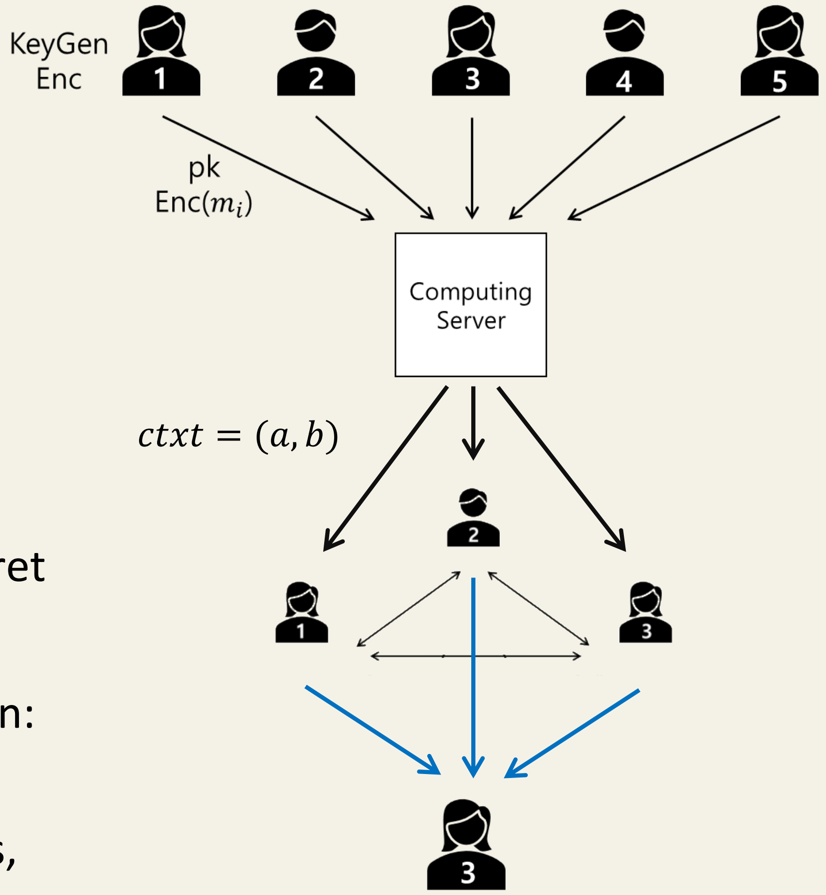
# This Work

- More practical approach: mitigate the definition
  - Trade-off between communication cost and rounds:

As same as in Threshold HE

Multi-round Threshold Dec

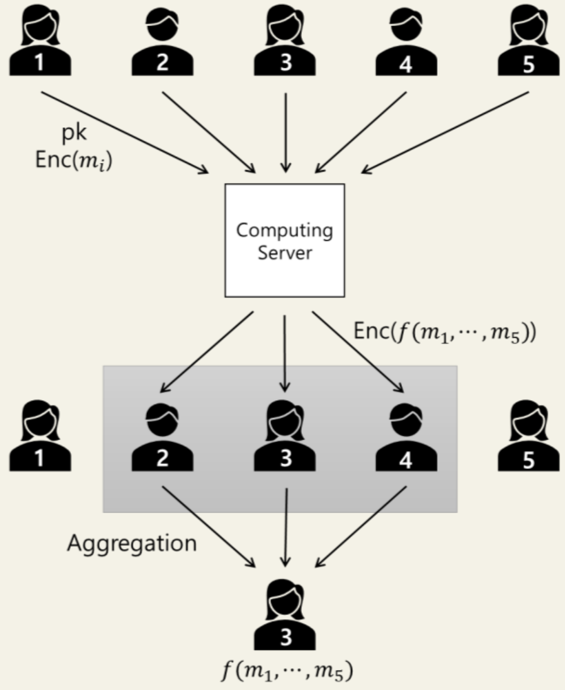
1. Given $ctxt = (a, b)$, each party makes a secret share of $\Delta m + e \bmod Q$
2. MPC-based truncation: $[\Delta m + e] \mapsto [m]$
3. A receiver aggregates, $\sum m_i = m$



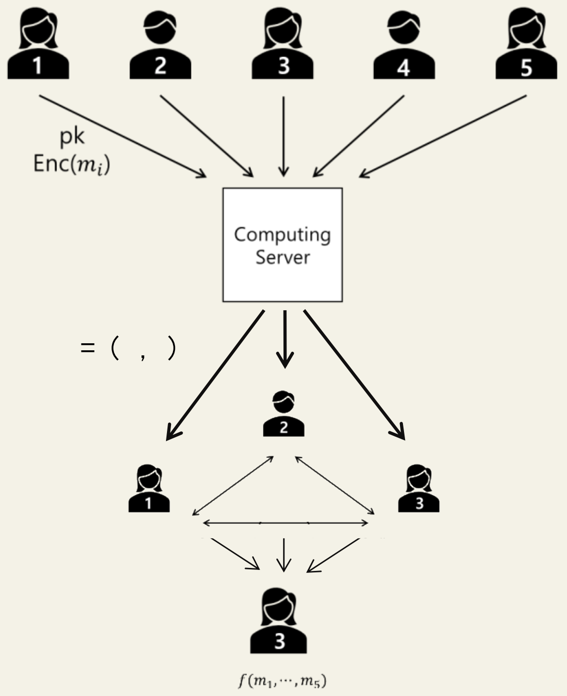

Decrypting parties require to be on-line

# This Work

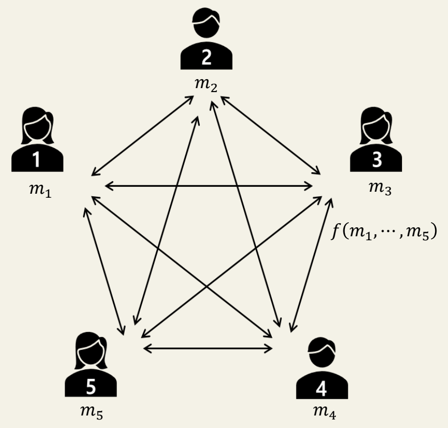
## Threshold HE




## This Work




## General MPC




A trade-off between Threshold HE & MPC

# This Work

- We instantiate exact truncation from [SCN:CT10]
  - 3-round Threshold Dec
  - Comp cost: $O(\log \Delta)$ $\mathbb{Z}_q$-inverse per party
  - Comm cost: each transcript size of $O(\log \Delta)$

- Advantages
  - Parameter sizes ⇩, Performance ⇧ (close to HE)
  - Especially benefit from large & deep circuits

- Disadvantages
  - #Rounds ⇧ (for threshold decryption)
    - But… for online parties who want to decrypt

[SCN:CT10] Catrina and de Hoogh, Improved Primitives for Secure Multiparty Integer Computation, *SCN 2010.*

# This Work

- Advantages
  - Parameter sizes ⇩, Performance ⇧ (close to HE)
  - Especially benefit from large & deep circuits

- Disadvantages
  - #Rounds ⇧ (for threshold decryption)
    - But… for online parties who want to decrypt

$f$: evaluating function, $n$: number of parties,
$\Delta \approx Q \ll Q_{comp}$, where $\Delta$ is the smallest possible one.

| | # Rounds | Comp. cost | Comm. Cost (per party, per round) |
|---|---|---|---|
| Threshold HE | 2=1+1 | $O\left(\lvert f\rvert \cdot \log Q_{comp} + n \cdot \log\left(\Delta \cdot 2^{\lambda} \cdot \sqrt{n}\right)\right)$ | $O\left(\log\left(\Delta \cdot 2^{\lambda} \cdot \sqrt{n}\right)\right)$ |
| MPC | $O(\lvert f\rvert)$ | $O(n \cdot \lvert f\rvert \cdot \log \Delta)$ | $O(\log \Delta)$ |
| This work | 4=1+3 | $O\left(\lvert f\rvert \cdot \log Q_{comp} + n \cdot \log \Delta\right)$ | $O(\log \Delta)$ |

# Further (On-going) Directions

- Implementations and Applications
- Mitigation on Security Definition
  - with practical scenarios
- Threshold-CKKS
  - HE over real numbers
  - More complicated due to some related attacks [EC:LM21], [USENIX:GNSJ24], [CCS:CCP+24].
- MPC Triple Generation
  - Threshold HE-based (Top/Low Gear) with smaller modulus

# Thank You!

From Feb. 2025, I am on the job market!
Please take a look:

# Appendix: Applications in Threshold HE vs. MPC

- Naïve examples for comparison in [MTBH20]
  - Secure input selection
    - Compute $f(r, x_1, \ldots, x_n) = x_r$ where all the inputs and outputs are encrypted state (or owned by each party)

| | | Time (sec) | | | Comm. / party (MB) | | |
|---|---|---|---|---|---|---|---|
| | #parties | 2 | 4 | 8 | 2 | 4 | 8 |
| MP-SPDZ | off | 0.35 | 1.04 | 3.56 | 6.58 | 25.74 | 101.82 |
| | on | 0.02 | 0.04 | 0.07 | 1.31 | 4.72 | 17.83 |
| | total | 0.37 | 1.08 | 3.66 | 7.89 | 30.46 | 119.65 |
| MTBH20 | Setup | 0.59 | 0.58 | 0.69 | 42.93 | 42.93 | 42.93 |
| | Eval | 0.27 | 0.28 | 0.31 | 1.31 | 1.31 | 1.31 |

[MTBH20] Christian Mouchet, Juan Troncoso-Pastoriza, Jean-Philippe Bossuat and Jean-Pierre Hubaux. Multiparty Homomorphic Encryption from Ring-Learning-with-Errors

# Appendix: Key Components of Threshold FHE

- From FHE to Threshold FHE: What is needed?
  - Threshold KeyGen/Enc/Eval/Dec
    - pk-Enc: (R)LWE-based.
    - pk-Eval: usually same, but maybe larger params.
    - KeyGen/Dec: in a distributed manner.
  - Threshold SIM/IND-Security
    - Trusted vs. Untrusted Setup
    - Honest vs Dishonest Majority
    - IND-CPA^D security

⋮

# Appendix: Key Components of Threshold FHE

- Distributed Key Generation
  - Top-down with trusted dealer [C:BGG+18]:
    - (pk, sk) ← FHE.KeyGen
    - $(\mathrm{sk}_1, \cdots, \mathrm{sk}_N) \leftarrow \mathrm{Share}(\mathrm{sk})$ so that any set $|I| \geq t$ can reveal sk.

$\{0,1\}$-LSSS:
$q$=$O(N)$, but $O(N^{5.3})$ shares

Shamir Secret Sharing:
N shares, but $q$=$O(N!)$

TreeSSS [CCK23]:
trade-off

  - Bottom-up without trusted dealer:

[EC:AJL+12] Only for t=N, use CRS.

Each party generates $s_i$ and $b_i = a \cdot s_i + e_i$
$\Rightarrow pk = (a, \sum b_i = a \cdot \sum s_i + e')$

[Access:KJY+20] Generalize [EC:AJW12] for t<N.

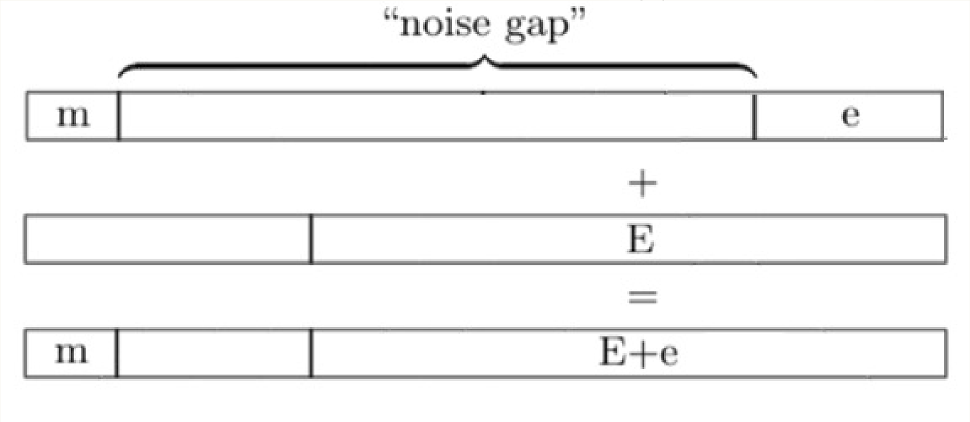
Having $s_i$ and pk for $\sum s_i$, distribute $(s_{i1}, \cdots, s_{iN}) \leftarrow \mathrm{Share}(s_i)$. Then, $(s_1', \cdots, s_N') := \sum (s_{i1}, \cdots, s_{iN}) \sim \mathrm{Share}(\sum s_i)$,


[C:BGG+18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, Amit Sahai. Threshold Cryptosystems From Threshold Fully Homomorphic Encryption, Crypto 2018.
[CCK23] Jung Hee Cheon, Wonhee Cho and Jiseung Kim. Improved Universal Thresholdizer from Iterative Shamir Secret Sharing. Eprint 2023.
[EC:AJL+12] Gilad Asharov, Abhishek Jain, Adriana L´opez-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. EUROCRYPT 2012.
[Access:KJY+20] Eunkyung Kim, Jinhyuck Jeong, Hyojin Yoon, Younghyun Kim, Jihoon Cho, and Jung Hee Cheon. How to securely collaborate on data: Decentralized threshold he and secure key update. IEEE Access, 2020.

# Appendix: Exponentially large $\Delta$ & $Q$

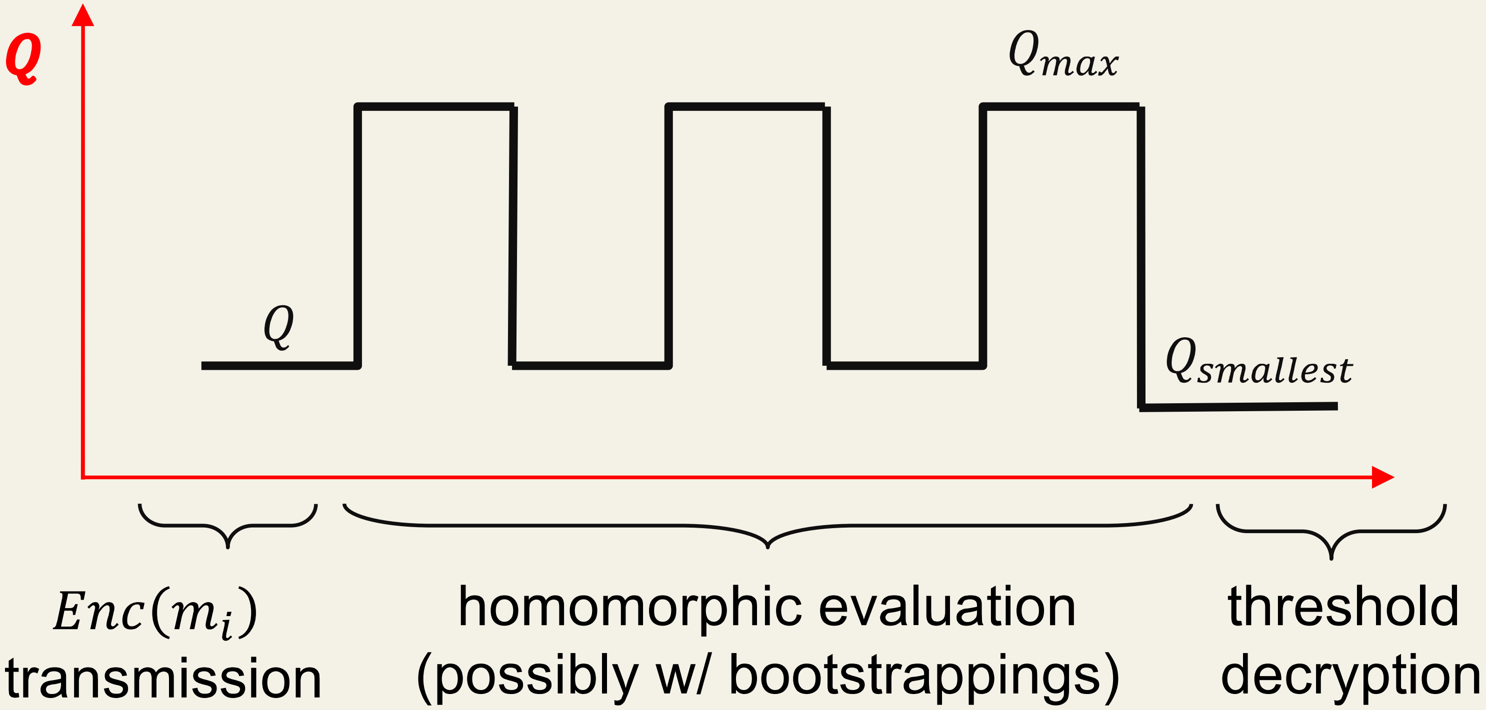
- In RLWE-based FHEs, $Q \gg |e|$ already.
- $\Delta$ is usually set smaller, $\approx$ 32-60 bits
  - $\Delta$ may become 96-124 bits

- Indeed, the gap between $m$ & $e$ is implertant!
  - BGV: $b = a \cdot s + m + \Delta e$ in $R_q$
  - CKKS/BFV: $b = a \cdot s + \Delta m + e$ in $R_q$
  - CGGI: $\vec{b} = \vec{a} \cdot \vec{s} + \Delta \vec{m} + \vec{e}$ in $\mathbb{Z}_q$



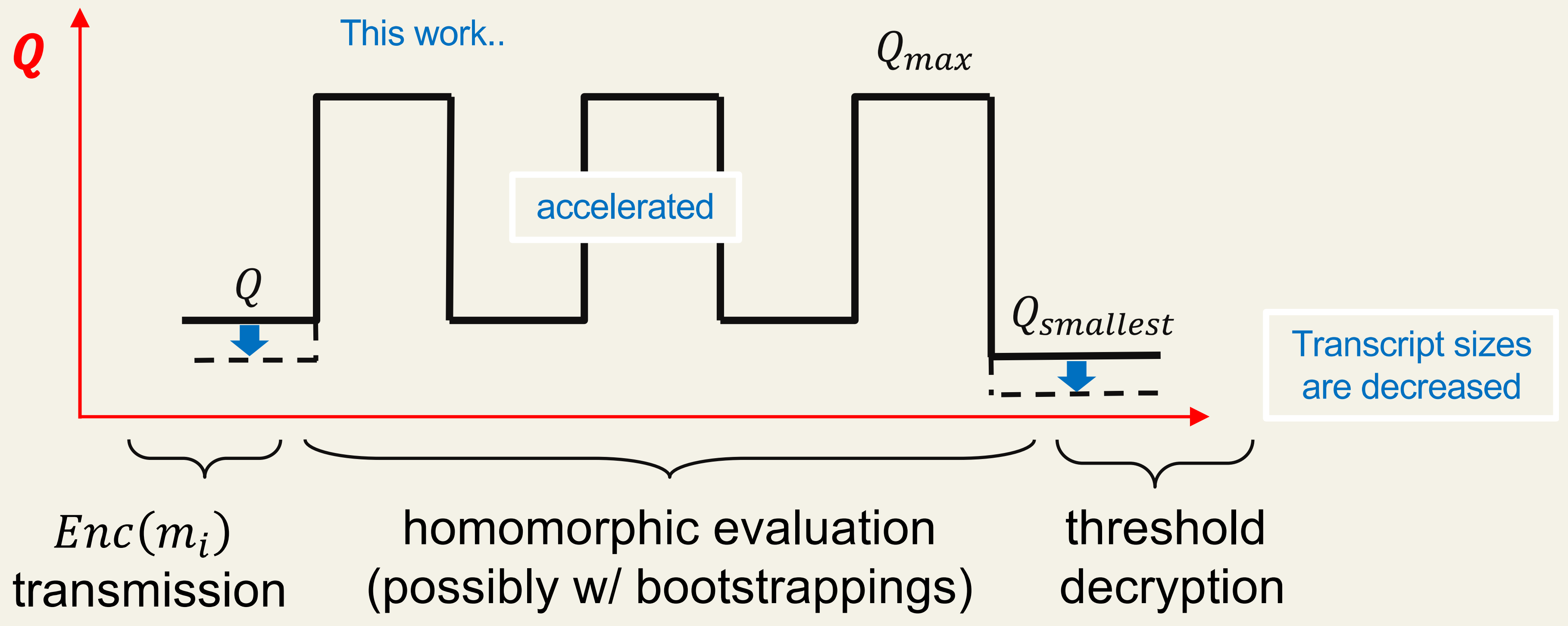
# Appendix: Exponentially large $\Delta$ & $Q$

- The modulus during the protocols:



# Appendix: Exponentially large $\Delta$ & $Q$

- The modulus during the protocols:



# Appendix: A bit more details on 1 & 2

1. Simpler than [AC:BS23] under the same assumption

   - Assuming "Circuit Privacy (CP)" in the multi-party setting.

   - More efficient than [AC:BS23].

2. HOWEVER, the assumption cannot be achieved.

   - [AC:BS23] uses tools for circuit-private "HE"

     → Do not work in the multi-party setting.

# Appendix: Asymptotic Comparison

- We instantiate exact truncation from [SCN:CT10]
  - Rounds: 3 rounds (assuming precomputations, e.g., triples)
  - Computation cost: $O(\log \Delta)$ $\mathbb{Z}_q$-inverse per party
  - Communication cost: each component of $O(\log \Delta)$ size

- Asymptotic comparison

| | **# Rounds** | **Comp. cost** | **Comm. Cost (per party, per round)** |
|---|---|---|---|
| Threshold HE | 2=1+1 | $O\left(\lvert f\rvert \cdot \log Q_{comp} + n \cdot \log\left(\Delta \cdot 2^{\lambda} \cdot \sqrt{n}\right)\right)$ | $O\left(\log\left(\Delta \cdot 2^{\lambda} \cdot \sqrt{n}\right)\right)$ |
| MPC | $O(\lvert f\rvert)$ | $O(n \cdot \lvert f\rvert \cdot \log \Delta)$ | $O(\log \Delta)$ |
| This work | 4=1+3 | $O\left(\lvert f\rvert \cdot \log Q_{comp} + n \cdot \log \Delta\right)$ | $O(\log \Delta)$ |

$f$: evaluating function, $n$: number of parties,
$\Delta \approx Q \ll Q_{comp}$,
where $\Delta$ is the smallest possible one.

# Appendix: Homomorphic Encryption (HE)

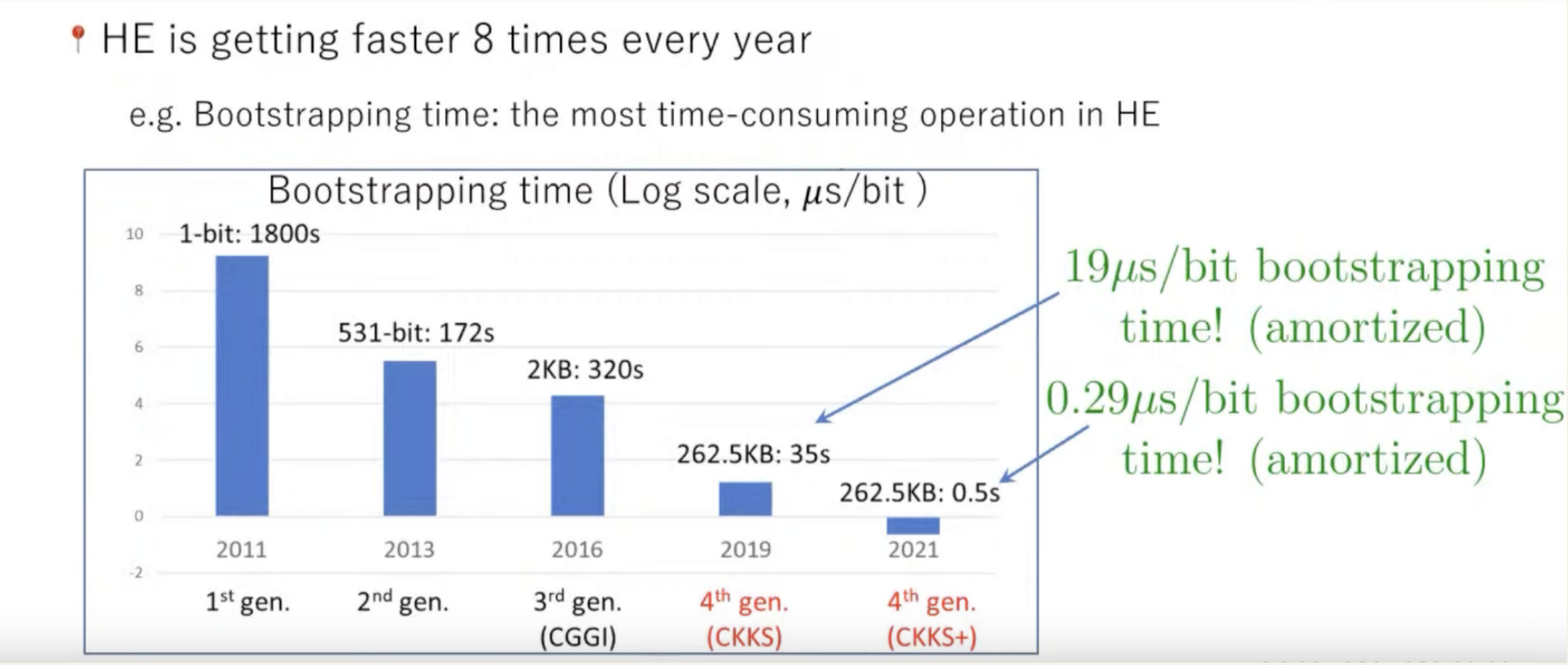



Image from https://medium.com/asecuritysite-when-bob-met-alice/the-rise-and-rise-of-homomorphic-encryption-735c77d18958, originally from an invited talk by Craig Gentry, presented at Eurocrypt 2021