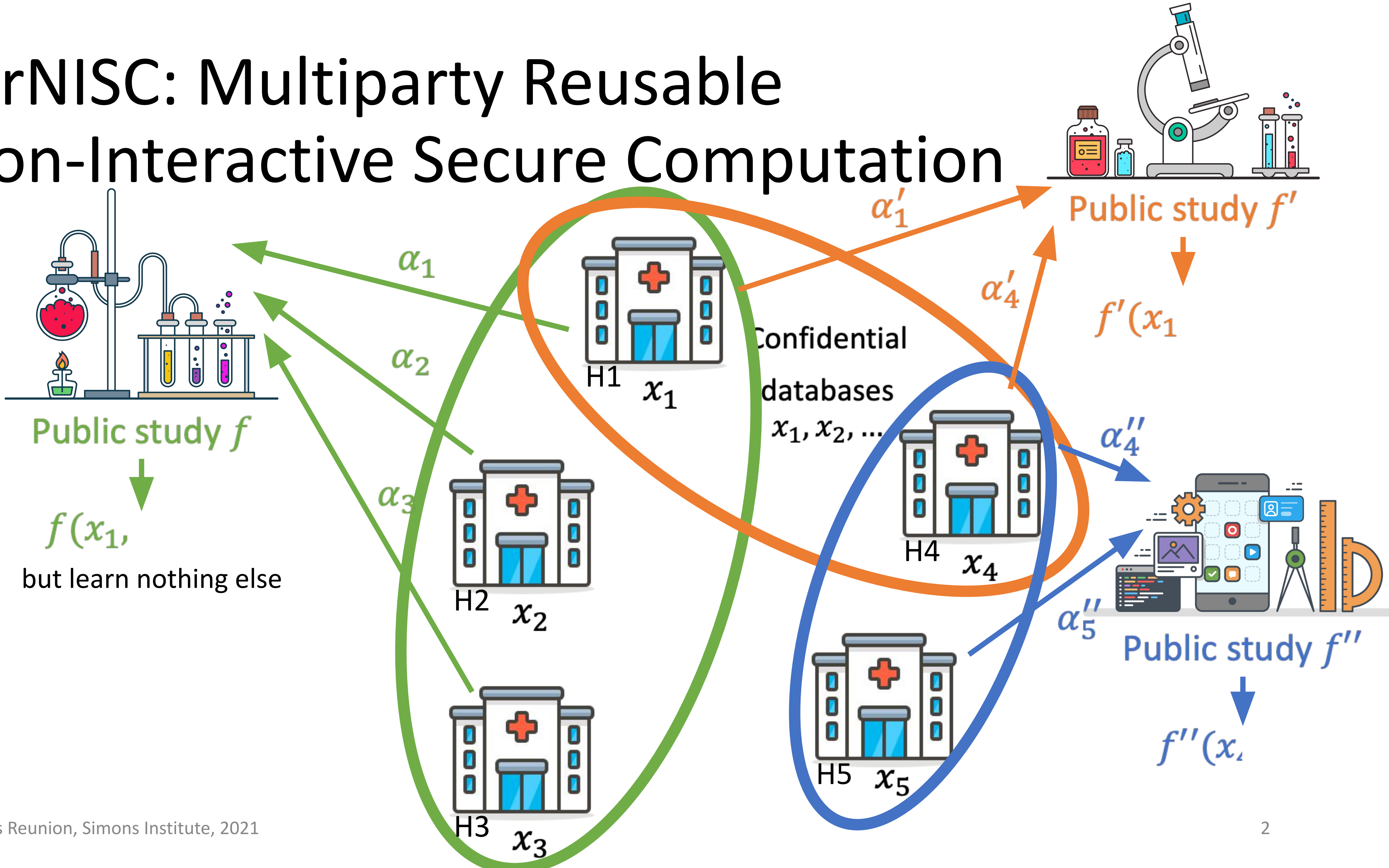
Mr NISC from LWE: Multiparty Reusable Non-Interactive Secure Computation

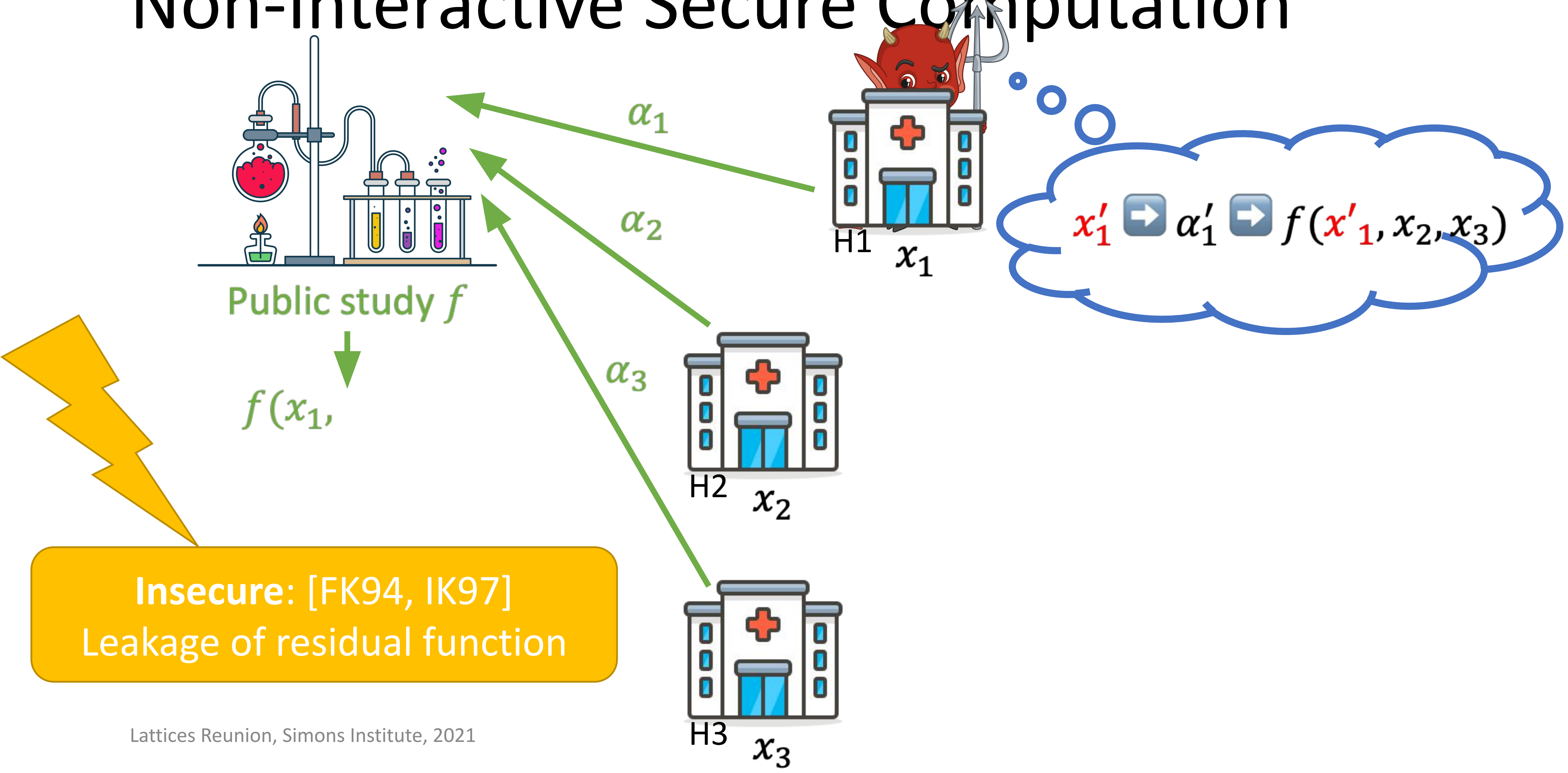
Fabrice Benhamouda
(Algorand Foundation)

Joint work with
Aayush Jain (UCLA, NTT),
Ilan Komargodski (Hebrew University, NTT),
Rachel Lin (University of Washington)

mrNISC: Multiparty Reusable Non-Interactive Secure Computation

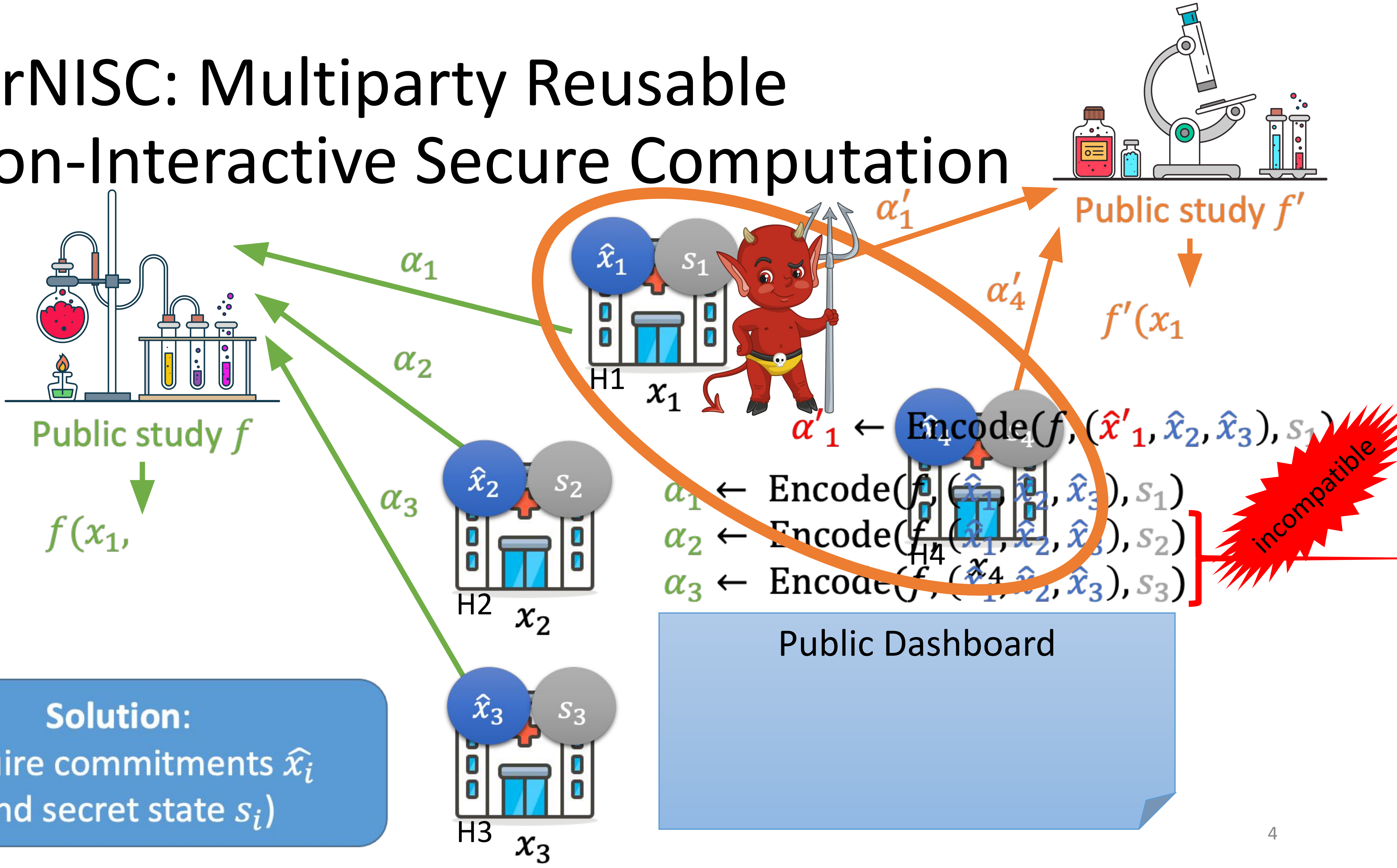


mrNISC: Multiparty Reusable Non-Interactive Secure Computation



Insecure: [FK94, IK97]
Leakage of residual function

mrNISC: Multiparty Reusable Non-Interactive Secure Computation



Solution:
Require commitments $\hat{x}_i$
(and secret state s_i)

mrNISC: Multiparty Reusable Non-Interactive Secure Computation

- Input encoding / commitment: $(\hat{x}_i, s_i) \leftarrow \mathrm{Com}(x_i)$

Public commitment

Secret state

- Computation: $\alpha_i \leftarrow \mathrm{Encode}(f, \{\hat{x}_j\}, s_i)$

Public computation encoding

($j \in S$, chosen set of inputs/parties)

- Output: $y \leftarrow \mathrm{Eval}(f, \{\hat{x}_j\}, \{\alpha_j\})$

- Correctness with dynamic parties joining
- Simulation security:
  - Semi-honest adversary, static corruptions, dishonest majority

Another View of mrNISC

mrNISC

=

2-round MPC with

reusable first round & dynamic set of parties

<u>Round 1</u> = broadcast commitments $\hat{x}_i$

<u>Round 2</u> = broadcast computation encodings α_i

Comparison with Previous Reusable 2-round MPC

		Setup	Assumptions	Reusable?	Dynamic set of parties?
Obfuscation	[GGHR14, GP15, CGP15, DKR15]	No setup	iO	✅	✅
Witness Encryption	[GLS15]	No setup	Witness Encryption	✅	✅
Multi-key FHE	Ananth, Jain, Jin, Malavolta (TCC 2020)	No setup	LWE	✅	❌
Homomorphic Secret Sharing	Bartusek, Garg, Masny, Mukherjee (TCC 2020)	No setup	DDH	✅	❌
Pairing	Benhamouda, Lin (TCC 2020)	No setup	SXDH	✅	✅
This work	(Eurocrypt 2021)	No setup	LWE	✅	✅

😀 > 🙂 > 🙁

Our Contributions

- Definition of Reusable Functional OT
  - mrNISC with 2 parties for specific functionality
- LWE $\Rightarrow$ Reusable Functional OT $\Rightarrow$ mrNISC
- Applications
  - Multi-Key FHE $\Rightarrow$ Threshold Multi-Key FHE
    - For NC1, first polynomial-modulus threshold multi-key FHE

Construction Overview

[GGHR14] Obfuscation → mrNISC

[GLS15] Garbled Circuits + Witness Encryption → mrNISC

[This work] LWE → Garbled Circuits + Reusable Functional OT → mrNISC

Overview

- [GGHR14] Compress L-round MPC to 2 rounds using iO
  - Round 1: commitment of input
  - Round 2: obfuscation of

Input: previous messages in L-round MPC
+ …
Output: next message + …

- [GLS15] Replace iO by witness encryption + garbled circuit

Allow to compute the garbled circuit labels

Input: previous messages in L-round MPC

Output: message + …

Overview of Construction from iO [GGHR14…] L-round MPC

For each party P_i:

Input of Party P_i

Randomness of Party P_i

Round 1: broadcast $m_i^1 = \text{Next}(x_i, r_i)$

Round 2: broadcast $m_i^2 = \text{Next}(x_i, r_i, \vec{m}^{<2})$

…

Round L: broadcast $m_i^L = \text{Next}(x_i, r_i, \vec{m}^{<L})$

Output: $y = \text{Output}(\vec{m})$

Overview of Construction from iO [GGHR14…] Round Compression

For each party P_i:

Round 1: broadcast $c_i = \text{Commit}(x_i, r_i)$

Round $\cancel{1}$ 2: broadcast $m_i^1 = \text{Next}(x_i, r_i)$

+ obfuscation of

Input: $\vec{m}^{<2}$, $\{\pi_j^1\}$
Abort if any proof π_j^1 invalid
Output: $m_i^2 = \text{Next}(x_i, r_i, \vec{m}^{<2})$ + proof π_i^2

⋮

+ obfuscation of

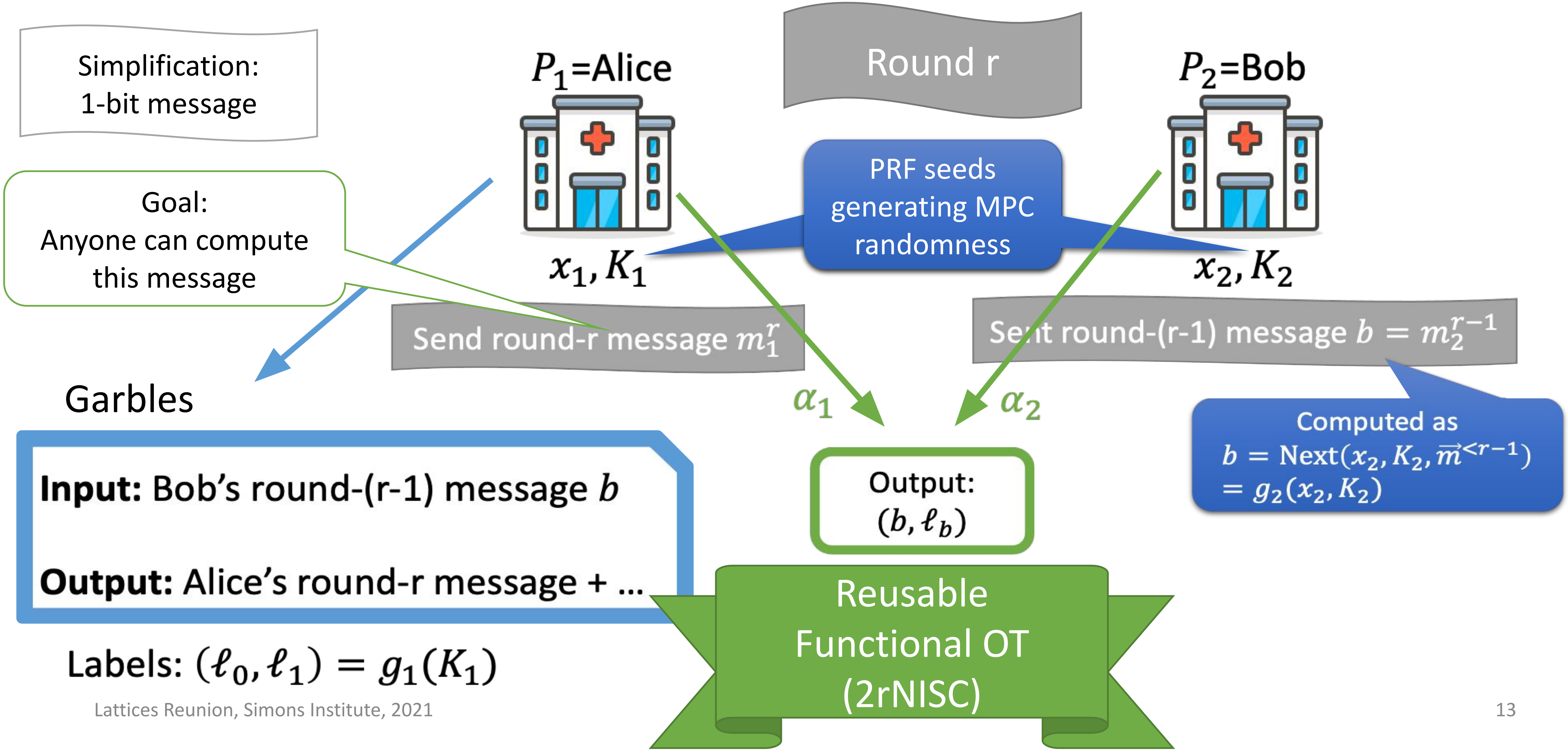
Input: $\vec{m}^{<L}$, $\{\pi_j^{L-1}\}$
Abort if any proof π_j^{L-1} invalid
Output: $m_i^L = \text{Next}(x_i, r_i, \vec{m}^{<L})$

Make it reusable:
Replace r_i
by PRF seed K_i

Correct: local evaluation of MPC

Insecure: leakage of residual function

Construction from Reusable Functional OT



Reusable Functional OT from LWE

Can use GSW commitments!

Ideas from [GVW15] and [BD18]

- Goal: 2rNISC for
  - Alice's input = x_1, Bob's input = x_2
  - Output: $y = (b, \ell_b)$ with $(\ell_0, \ell_1) = g_1(x_1)$ and $b = g_2(x_2)$
- Bob commits to x_2 using fully homomorphic commitment:

$$\widehat{x_2} = \mathrm{Com}(x_2) \longrightarrow C_{g_2} = \mathrm{Com}(g_2(x_2))$$

$\widehat{x_2} = (A, A\,R + x_2\,G)$

$C_{g_2} = A\,R_{g_2} + (1-b)\,G$

R_{g_2} known by Bob only

- α_1 : Alice encrypts ℓ_β for $\beta = 0,1$
  - can be decrypted with ZK proof "$C_{g_2} = \mathrm{Com}(\beta)$"

$\widehat{\ell_\beta} = Ext(s_\beta) \oplus \ell_\beta$
$w_\beta = s_\beta \cdot [A\,|C_{g_2}] + noise$

- α_2 : Bob provides ZK proof that $C_{g_2} = \mathrm{Com}(b)$

Can recover s_β

Short basis of lattice $\{z \mid [A|C_{g_2}] \cdot z = 0\}$

Conclusion

- Definition of Reusable Functional OT
  - mrNISC with 2 parties for specific functionality
- LWE ⇒ Reusable Functional OT ⇒ mrNISC
- Applications
  - Multi-Key FHE ⇒ Threshold Multi-Key FHE
    - For NC1, first polynomial-modulus threshold multi-key FHE


THANK
YOU