Secret Sharing with Statistical Privacy and Computational Non-Malleability

Tasuku Narita* Fuyuki Kitagawa † Yusuke Yoshida * Keisuke Tanaka *

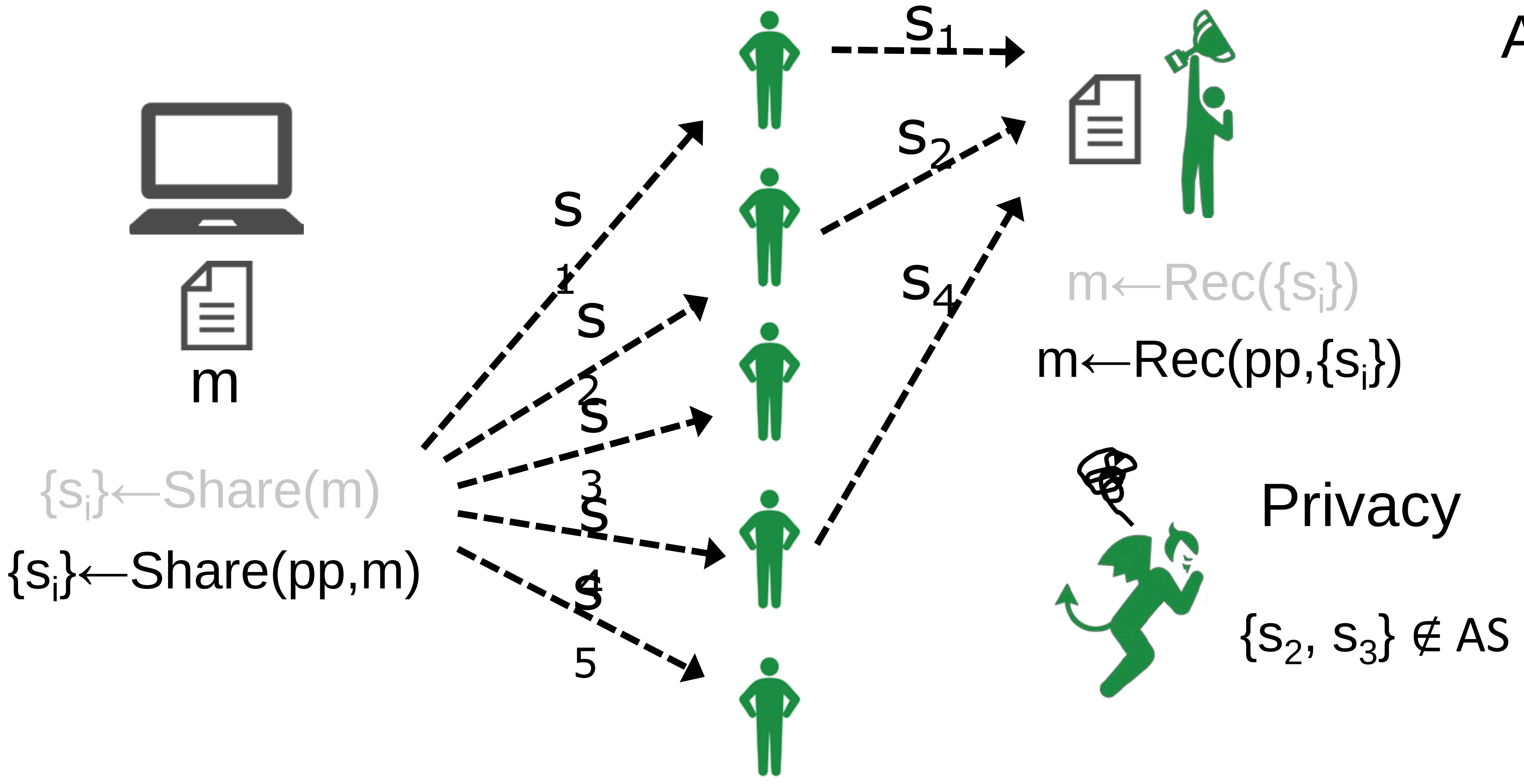
* Tokyo Institute of Technology † NTT Secure Platform Laboratories

Our Result

- Define the relaxed notion of computational non-malleability for secret sharing
- Construct non-malleable secret sharing in public parameter model

Secret Sharing [Bla79, Sha79]

$pp \leftarrow Setup(1^\lambda)$



Access Structure

$\{ s_1, s_2 \}$

$\{ s_1, s_2, s_4 \}$

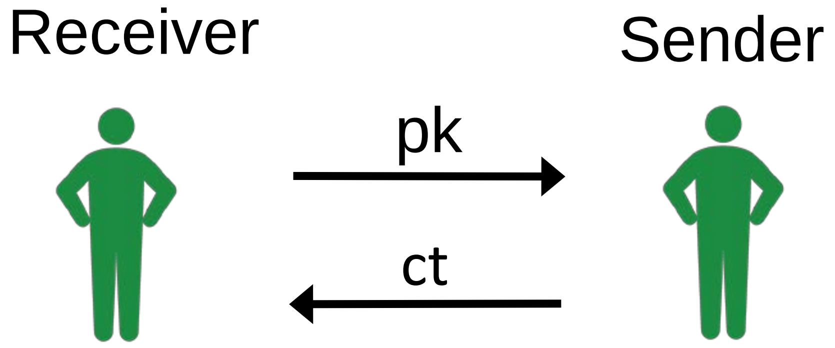
Privacy

$\{s_2, s_3\} \notin AS$

- Computational
- Statistical

Tampering in the Case of PKE

Privacy does not imply non-malleability



$(pk, sk) \leftarrow KG(1^{\lambda})$

$ct \leftarrow Enc(pk, m)$

IND-CCA security can prevent tampering.

ct →  → $\widetilde{ct}$ → Dec → $\widetilde{m}$

Another meaningful message

Tampering in the Case of Secret Sharing

2-out-of-2 secret sharing

r : randomness

$s_1 = r$

m

~~$s_2 = -r + m$~~

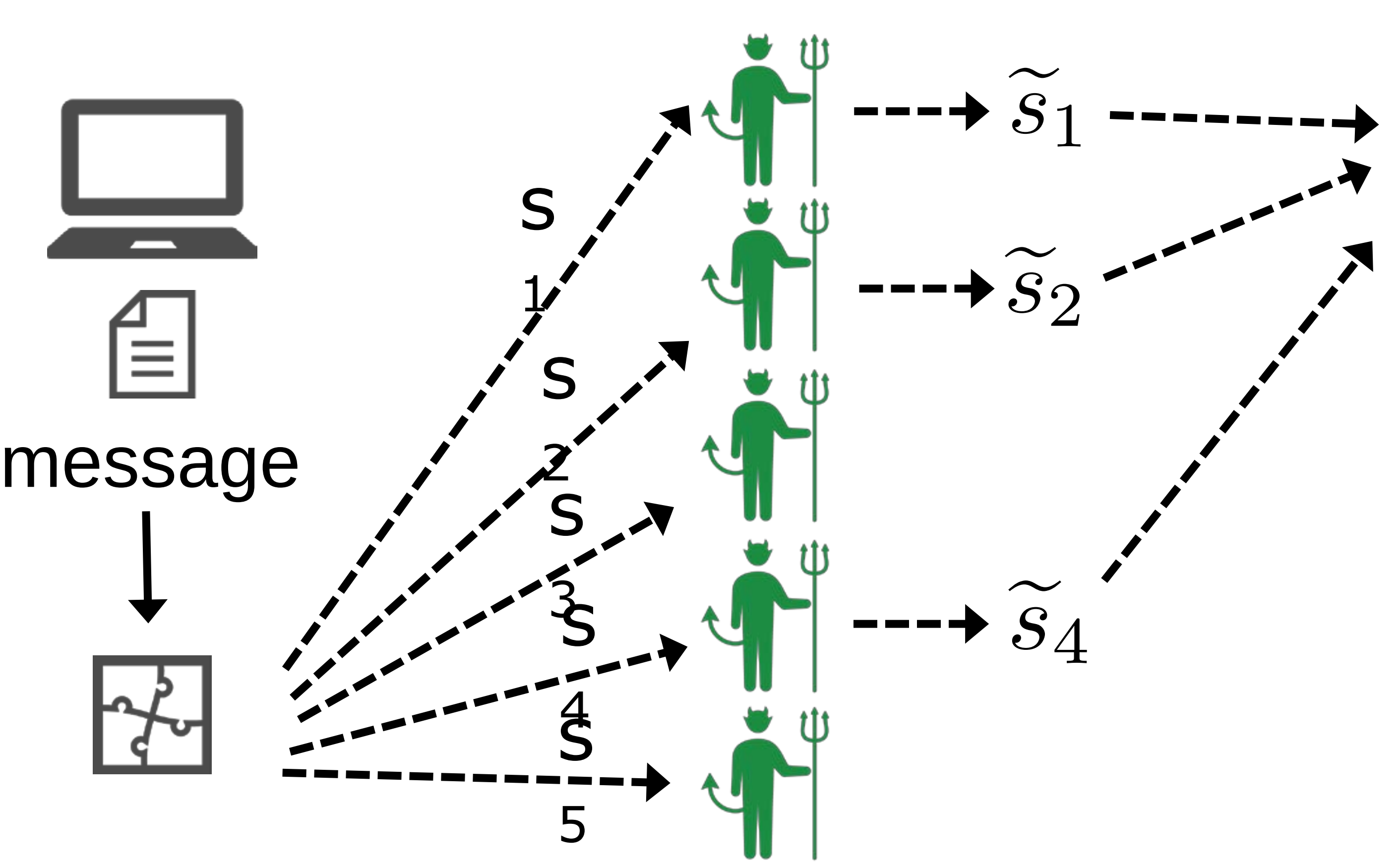
↳ $\widetilde{s}_2 = s_2 + 1$

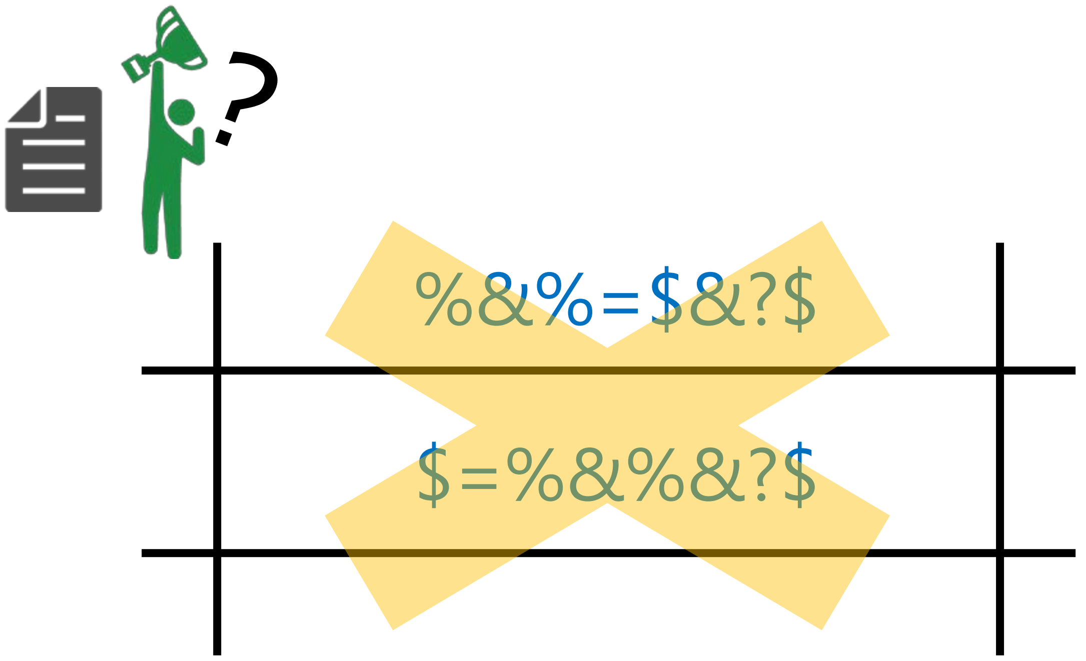
~~$s_1 + s_2 = m$~~

↳ $s_1 + \widetilde{s}_2 = m + 1$

Tampering attack is easy

Non-Malleability for Secret Sharing

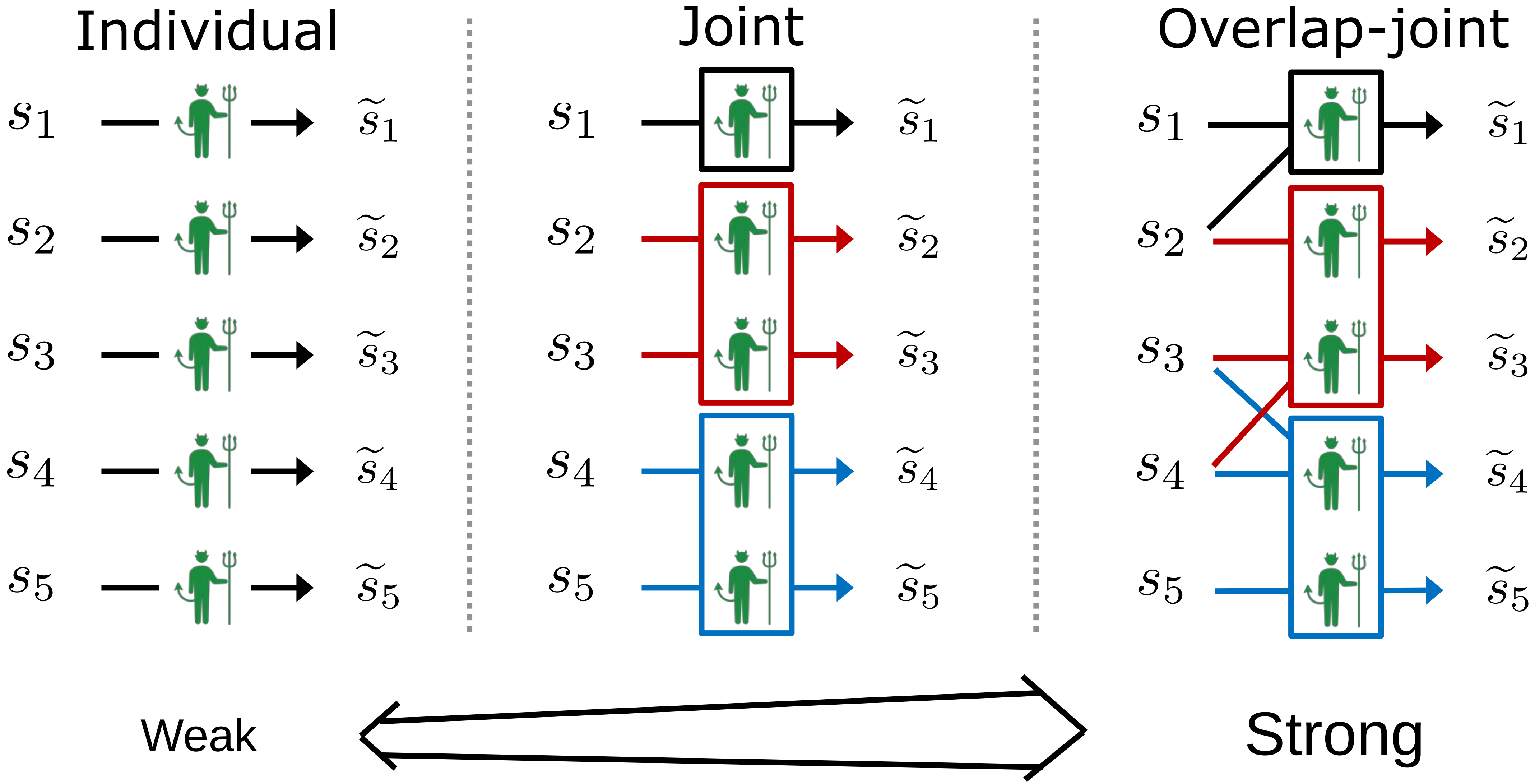




Can not change
the reconstruction result at will

There are computational / statistical non-malleability

Tampering Model [GK18a, GK18b]



Previous Works

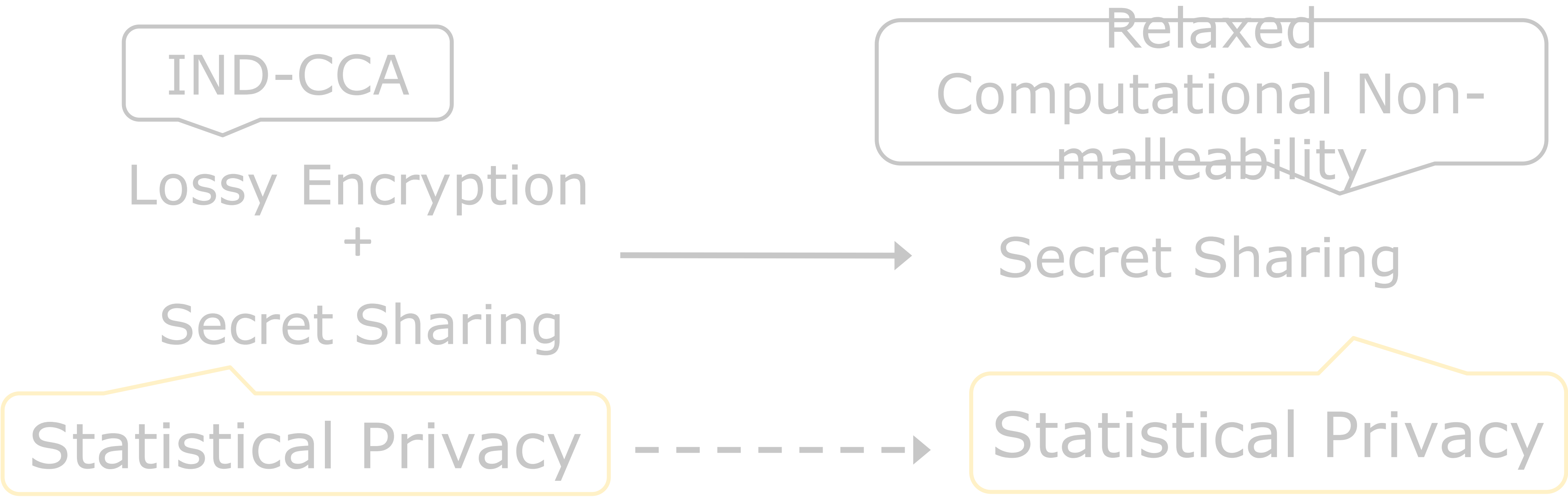
These are the result which has non-malleability against (over-lap) joint tampering

	Access Structure	Tampering Model	Non-Malleability	Privacy
GK18a	Thredhold	Joint	Statistical	Statistical
GK18b	n-out-of-n	Overlap-Joint	Statistical	Statistical

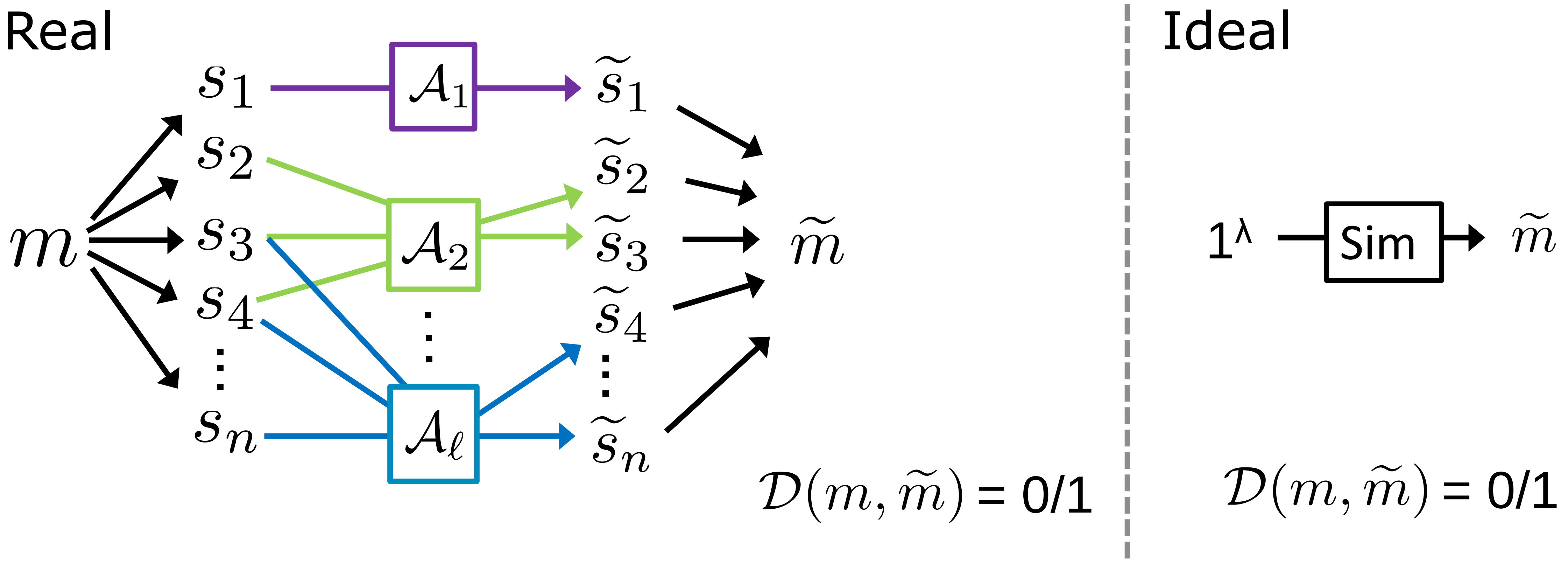
Our Result

- Define the notion of relaxed computational non-malleability

- Construct non-malleable secret sharing in the public parameter model



(Not Relaxed) Computational Non-Malleability



For any adversary, exist a simulator s.t. for any distinguisher $\mathcal{D}$

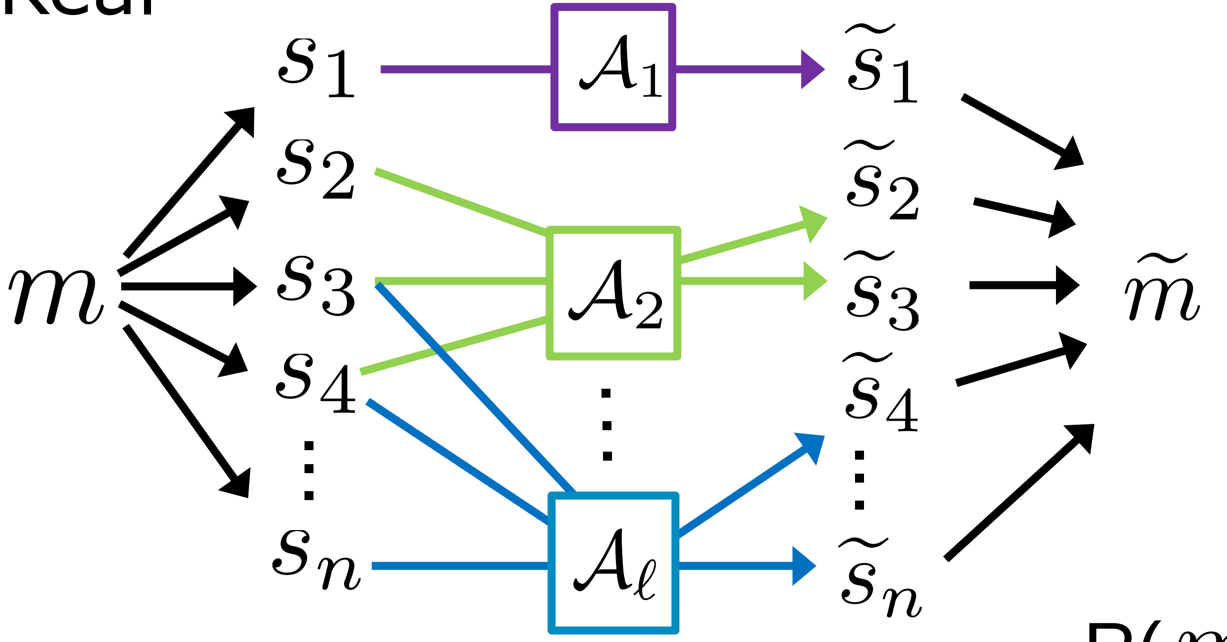
| Pr[Real =1] – Pr[Ideal = 1] | = negl(λ)

➡ Satisfy the comp. non-malleability

Require strict simulation

Relaxed Computational Non-Malleability

Real



R(m, $\tilde{m}$)=0/1

Ideal

Restriction:

R(m , m) = R(m , $\perp$) = 0

R(m, $\tilde{m}$)=0/1

Some information is lost

For any adversary, exist a simulator s.t. for any relation R

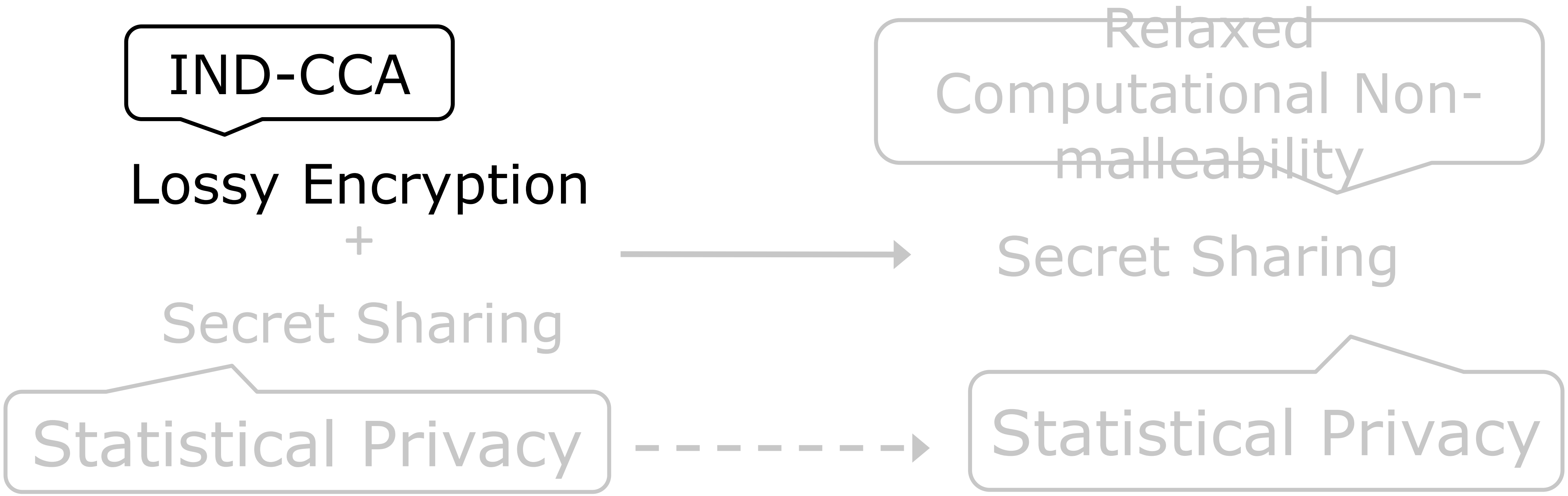
Pr[Real = 1] – Pr[Ideal = 1] $\leq$ negl(λ)

➡ Satisfy the relaxed comp. non-malleability

Refer to non-malleability for commitment by Crescenzo et al.

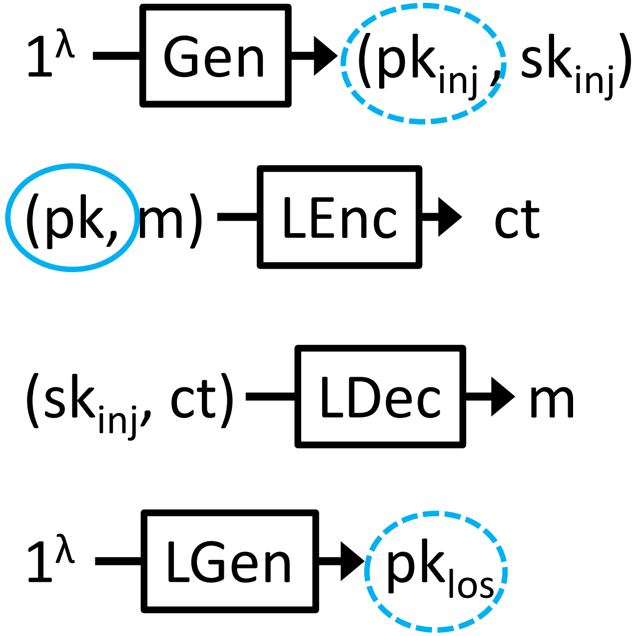
Our Result (Repost)

- Define the notion of relaxed computational non-malleability
- Construct non-malleable secret sharing in the public parameter model



Lossy Encryption

Lossy Encryption Scheme: Λ = (Gen, LGen, LEnc, LDec)



Injective Mode（When using pk_{inj} ）

➡ INDCCA PKE

Lossy Mode （When using pk_{los} ）

➡ Information of m disappears

- Key Indistinguishability $pk_{inj} \approx_c pk_{los}$
- Statistical Privacy in the Lossy Mode $LEnc(pk_{los}, m_0) \approx_s LEnc(pk_{los}, m_1)$

Lossy Encryption in the Injective Mode

Construction(Repost)

IND-CCA

Lossy Encryption
+
Secret Sharing

→

Relaxed Computational Non-Malleability

Secret Sharing

Non-Malleable Secret Sharing

IND-CCA Lossy Encryption Scheme

LPKE = (Gen, LGen, LEnc, LDec)

+

Secret Sharing Scheme

Σ = (Setup, Share, Rec)

$\longrightarrow$

Secret Sharing Scheme

$\Sigma_{\mathtt{NM}}$ = (NMSetup, NMShare, NMRec)

NMSetup(1^λ):

Run Setup and LGen

Output $pp_{nm} := (pk_{los}, pp)$

NMShare(pp_{nm}, m):

$pp_{nm} = (pk_{los}, pp)$

lossy mode

$(pk_{los}, m) \rightarrow$ LEnc $\rightarrow$ ct

r

concatenate

(pp, m||r) $\rightarrow$ Share $\rightarrow$ $\{s_i\}$

$share_i := (ct, s_i)$

NMRec(pp_{nm}, $\{share_i\}_{i \in T}$):

$share_i = (ct_i, s_i)$

$(pp, \{s_i\}) \rightarrow$ Rec $\rightarrow$ m'||r'

For all ct_i,

LEnc(pk_{los}, m' ;r') = ct_i ?

Yes $\rightarrow$ m'   No $\rightarrow$ $\perp$

Intuition of Statistical Privacy

Ciphertext by LPKE in the lossy mode

Share by Σ

$$\text{share}_i = (\, ct_i \,,\ s_i \,)$$

Information of m

Information of m||r

Statistical Privacy of LPKE in the Lossy Mode

Statistical Privacy of Σ

Intuition of Computational Non-Malleability

Output of NMRec is not $\perp$ $\rightarrow$ "contents" of ct_i

➡ Must tamper with ct_i

➡ Can not tamper with ct_i IND-CCA of LPKE

NMRec(pp_{nm}, $\{share_i\}_{i\in T}$):

Compute $m'||r'$ from $\{s_i\}$

For all ct_i,

$LEnc(pk_{los}, m';r') = ct_i$?

Yes $\rightarrow$ m' No $\rightarrow$ $\perp$

⊖ IND-CCA security can not apply in the lossy mode

➡ Switch to the injective mode from lossy mode **Key Indistinguishability**

⊜Information of m and r is not leaked from s_i?

➡ Information on m and r is not leaked **Privacy of Σ**

➡ Can apply IND-CCA security

Can not tamper with shares

Summary

We can give relaxed computational non-malleability for over-lap joint tampering to any secret sharing.

public parameter model

IND-CCA
Lossy Encryption
+
Secret Sharing

→

Secret Sharing with Relaxed Computational Non-Malleability

Conversion while preserving statistical privacy