Non-Committing Encryption with Constant Ciphertext Expansion from Standard Assumptions

(Amplify Weak NCE)

Yusuke Yoshida[1], Fuyuki Kitagawa[2], Keita Xagawa[2], Keisuke Tanaka[1]

[1]Tokyo Institute of Technology, [2]NTT Secure Platform Laboratories

ASIACRYPT2020

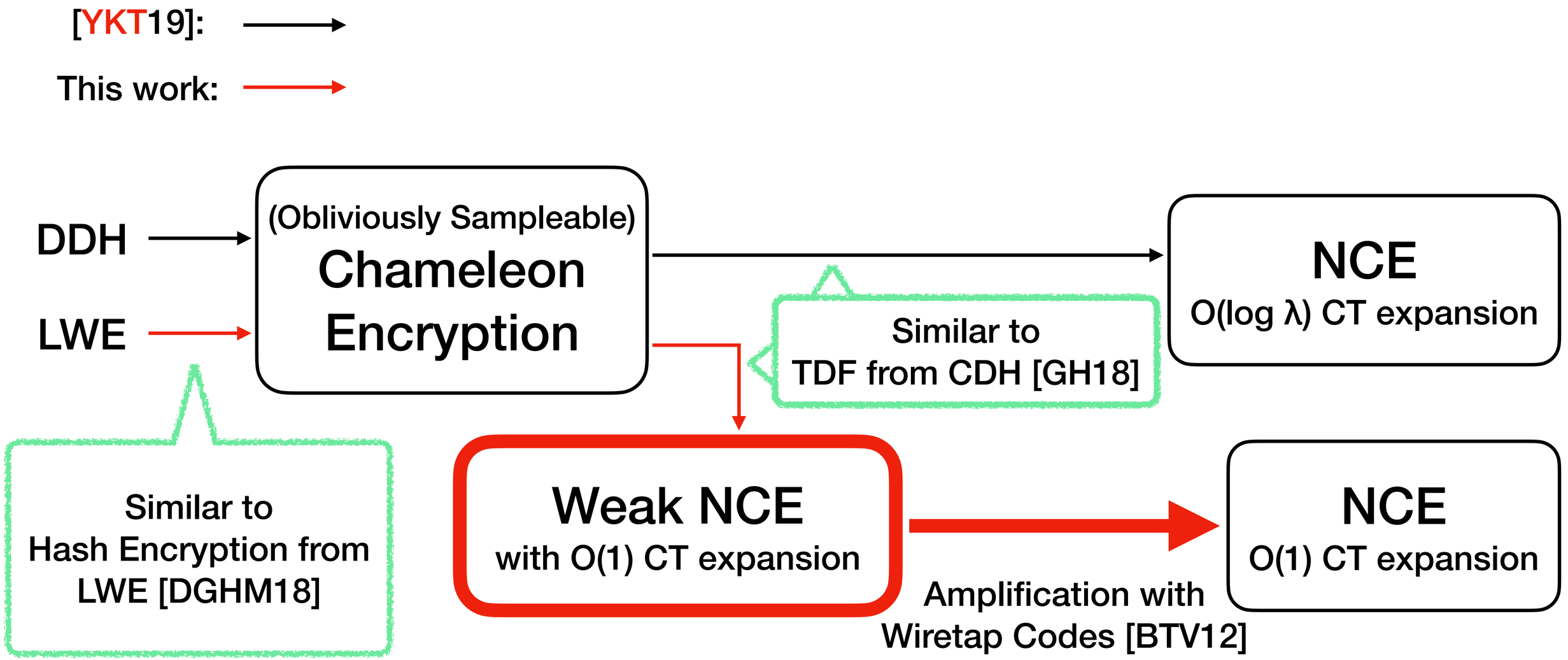
Outline

1. Backgrounds & Overview
2. Weak NCE
3. Wiretap Codes
4. Amplify Weak NCE

Non-Committing Encryption（NCE）

- NCE is public-key encryption with non-committing property.
- NCE establishes secure channels in adaptively secure MPC [CHGN96].
- Security considers when **sk, r** are revealed to the adversary.
- Drawbacks: $|sk| \geq |m|$, Pr[Dec Error]>0, Large Ciphertext
- CT expansion := |ct| / |m|, PK expansion := |pk| / |m| .

Overview


[YKT19]:
This work:
DDH
LWE
(Obliviously Sampleable)
Chameleon
Encryption
NCE
O(log λ) CT expansion
Similar to
TDF from CDH [GH18]
Similar to
Hash Encryption from
LWE [DGHM18]
Weak NCE
with O(1) CT expansion
Amplification with
Wiretap Codes [BTV12]
NCE
O(1) CT expansion

Previous Works

Reference	CT expansion	PK expansion	Assumption
[CFGN96]	$O(\lambda^2)$	$O(\lambda^2)$	CDH, RSA
[CDMW09]	$O(\lambda)$	$O(\lambda)$	DDH etc.
[HOR15]	$O(\log \lambda)$	$\lambda \mathrm{poly}(\log \lambda)$	ϕ-hiding
[HORR16]	$\mathrm{poly}(\log \lambda)$	$\lambda \mathrm{poly}(\log \lambda)$ $\mathrm{poly}(\log \lambda)$	LWE Ring-LWE
[YKT19]	$O(\log \lambda)$	$O(\lambda^2)$	DDH
[BBD+20] (concurrent)	$O(1)$	$O(\lambda^2)$ $\lambda \mathrm{poly}(\log \lambda)$	DDH,QR LWE
This work	$O(1)$	$O(\lambda^2)$ $\lambda \mathrm{poly}(\log \lambda)$	DDH LWE

Table: NCE from standard assumptions.

Our Contribution

- The first NCE schemes with CT expansion O(1) from DDH, LWE.
- PK is smaller than [YKT19] if constructed from LWE.

This Work vs［BBD+20］

- Identical result, but technique is different.

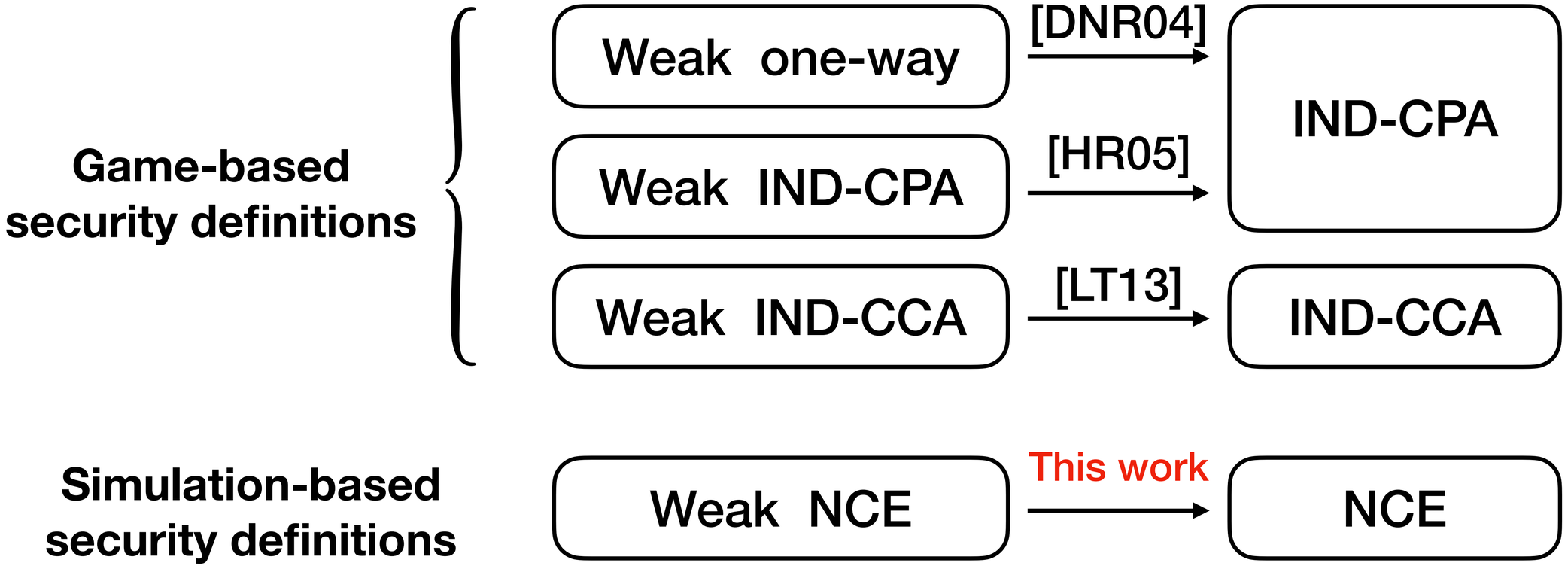
	This work	[BBD+20]
Construction is inspired by	[YKT19], [Beaver97]	[HORR16], [CDMW09]
Introduced intermediate primitive	Weak NCE	PEPE
Required error-correcting codes	Rate >1/2	Error Rate>1/2-δ

Other Related Works

- 3-round NCE [Beaver97, DN00] .
- NCE with CT&PK expansion 1+o(1) from iO in the CRS model [CPR17] .
- Relaxed notions of NCE.
  - Receiver NCE / Sender NCE.
    Only {receiver /sender} is corrupted and {**sk** / **r**} is revealed to the adversary.
  - Somewhat NCE.
    ct can be explained as encryption of limited messages m’.

Amplify PKE

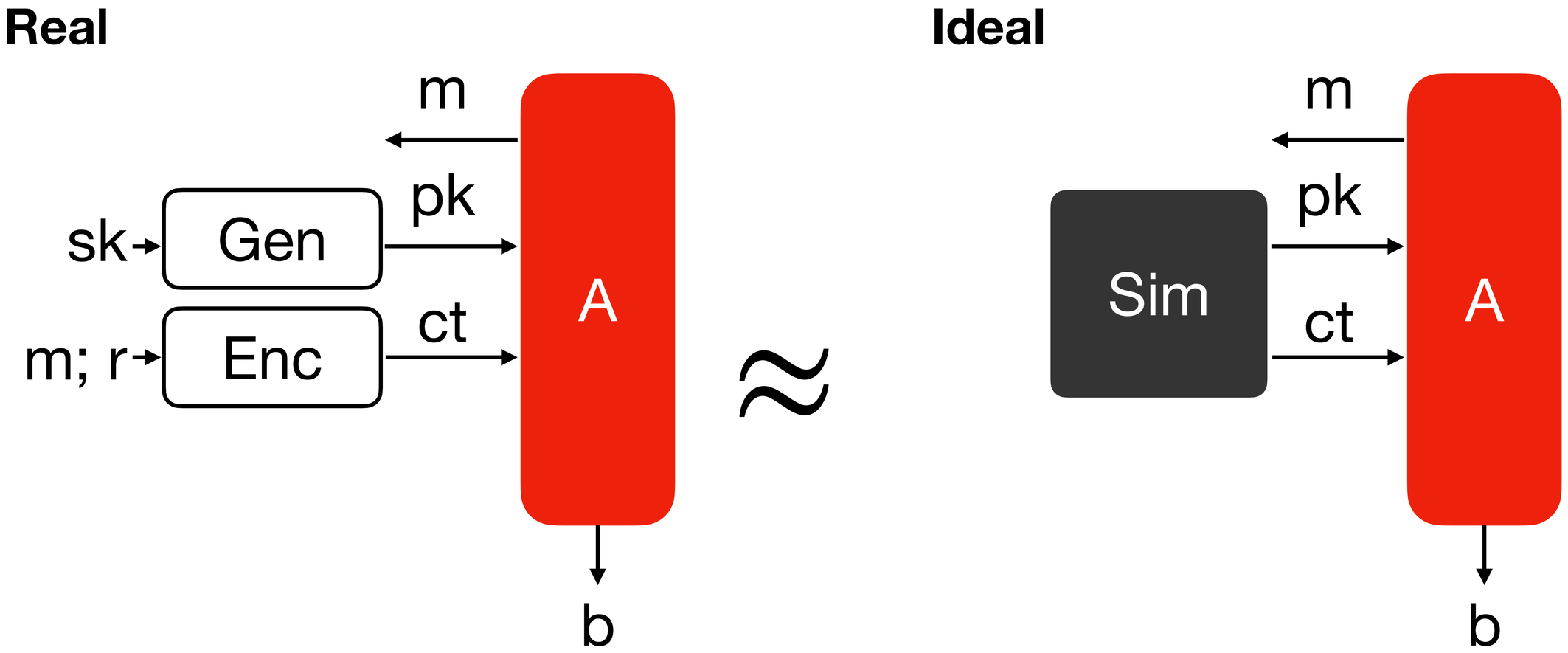
"How far can we weaken a security definition
so that it still can be transformed into full-fledged one?"



Outline

1. Backgrounds & Overview
2. **Weak NCE**
3. Wiretap Codes
4. Amplify Weak NCE

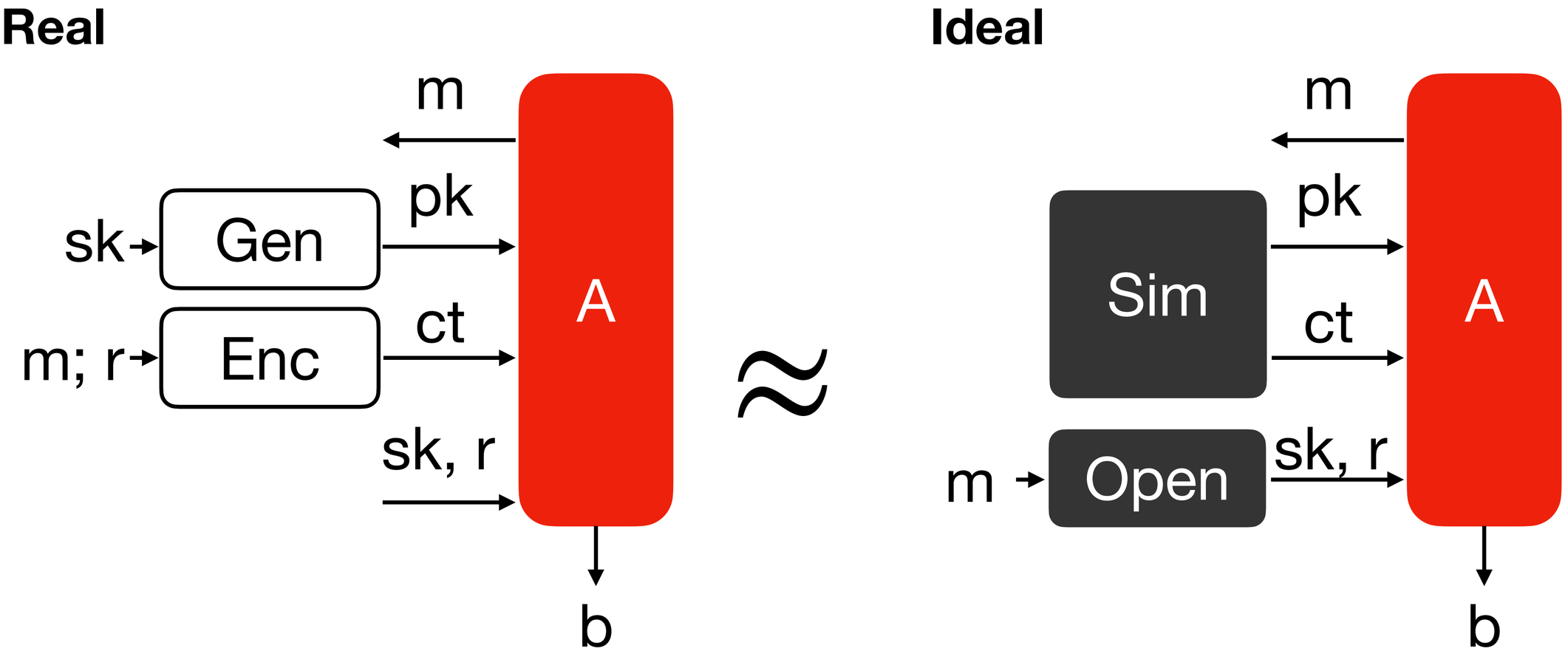
Semantic Security*



* Adversary chooses m before pk.

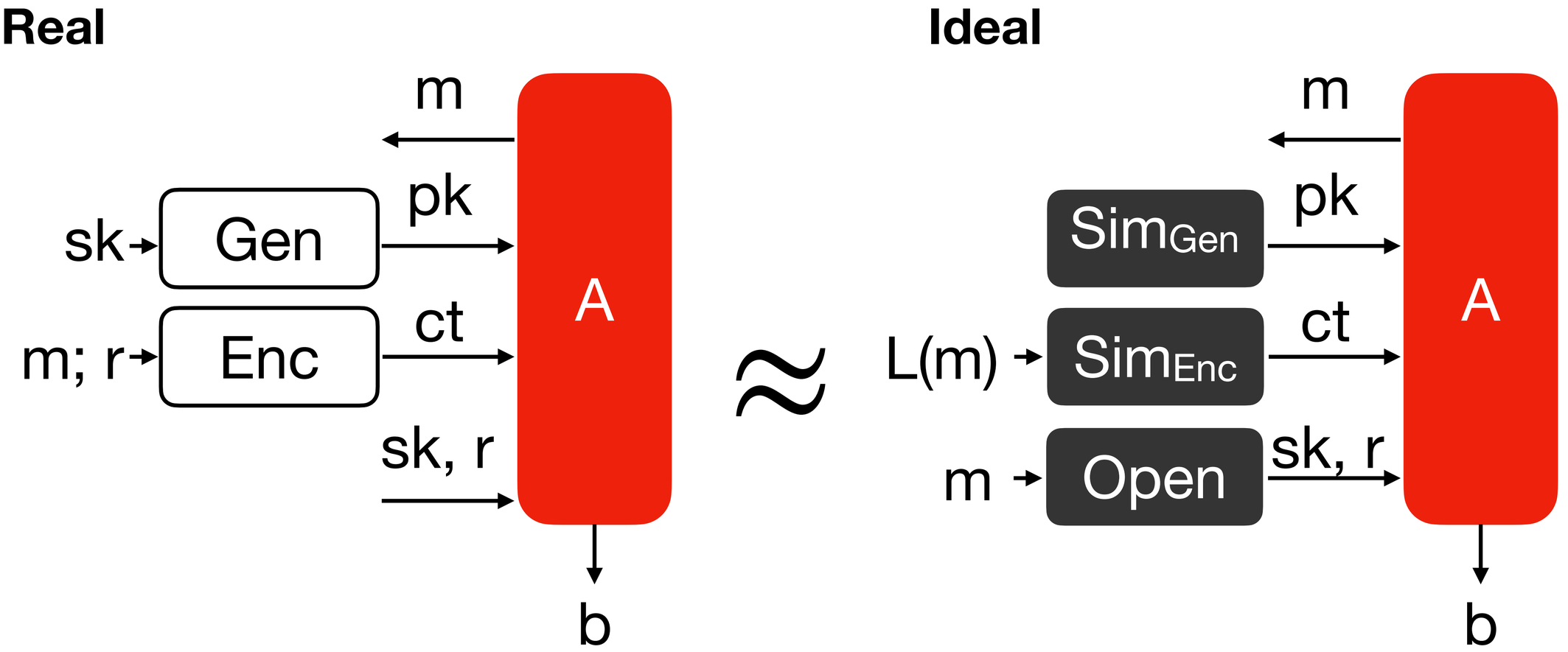
Easily fixed using hybrid encryption with OTP. i.e. ct = (Enc(R), m⊕R)

NCE Security*



- After adaptively corrupting parties in MPC, the adversary obtains **sk**, **r**.
- **Open** must output **sk**, **r** consistent to **m.**

NCE Weak Security



- Sim can take **L(m)** to generate **ct**.
  - Adversary may obtain **L(m)** from **ct.**

Why Our NCE is Weak

Dec(sk_z, ct)
Recompute k'_z from **y**, sk_z.

Output **z** if $k'_z = k_z$, otherwise **1-z** .

Decryption fails when $k'_z = \$$ which happens w.p. $\varepsilon = 1/2^{\ell+1}$.

$y \leftarrow \text{ChameleonHash}(x)$

$\text{Enc}(0) = (y, k_0, \$)$

$\text{Enc}(1) = (y, \$, k_1)$

$k_0, k_1 \in \{0,1\}^{\ell}$

Security

$\text{Enc}(x) \approx ct_{Sim} = (y, k_0, k_1)$ holds only if **z = x** .

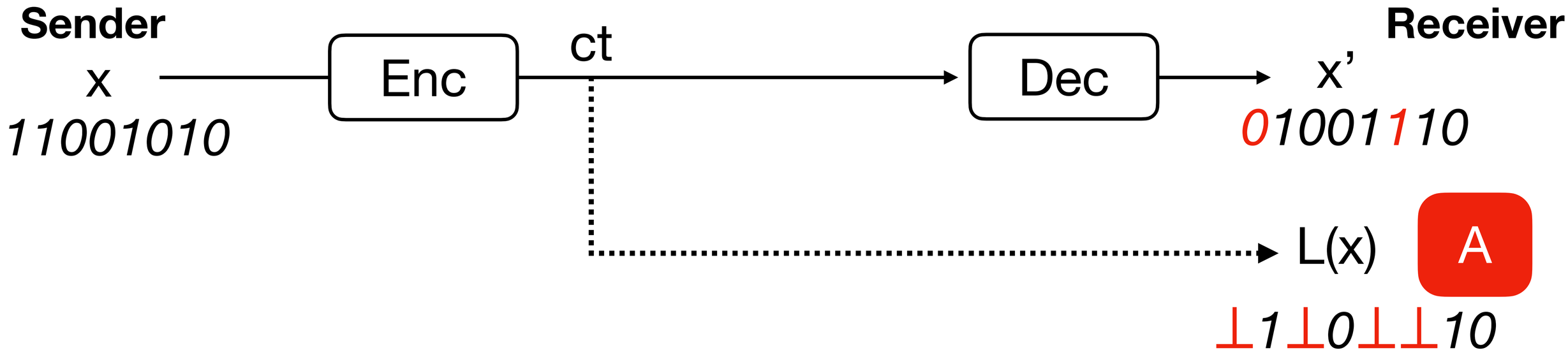
Because sk_z, k_z are revealed.

Adversary can obtain message bit w.p. 1/2.

ct for n-bit message $(y, \{k_{i,0}, k_{i,1}\}_{i=1,\ldots,n})$

CT expansion $(2\ell + o(1))$.

Summary of Weak NCE



We construct NCE with constant $(2\ell + o(1))$ CT expansion.

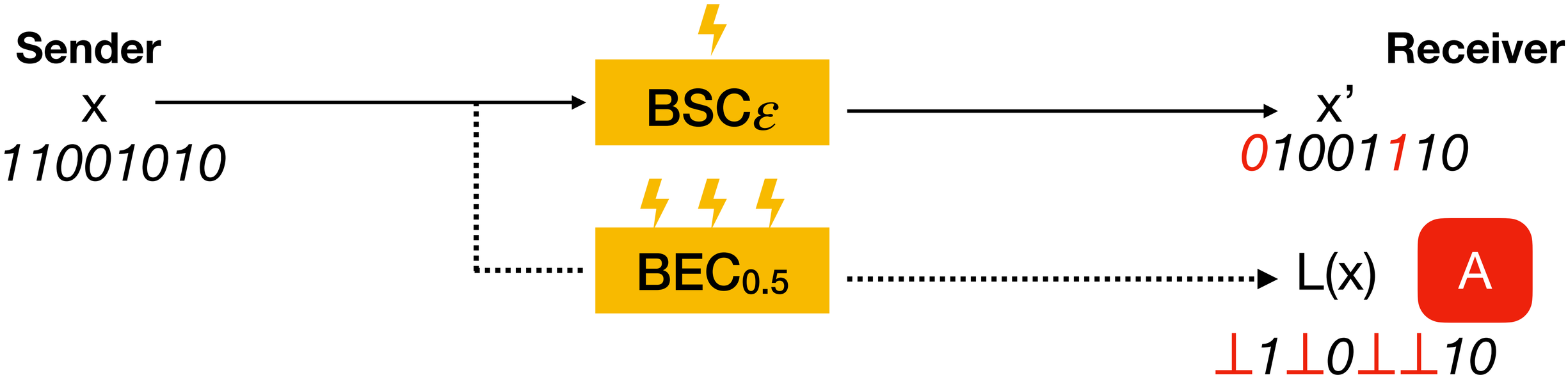
However, it only satisfies weak correctness and weak security.

- Weak Correctness: Decryption result flips w.p. $\varepsilon = 1/2^{\ell+1}$.
- Weak Security: Adversary can obtain half of message bits L(x) from ct.

Outline

1. Backgrounds & Overview
2. Weak NCE
3. **Wiretap Codes**
4. Amplify Weak NCE

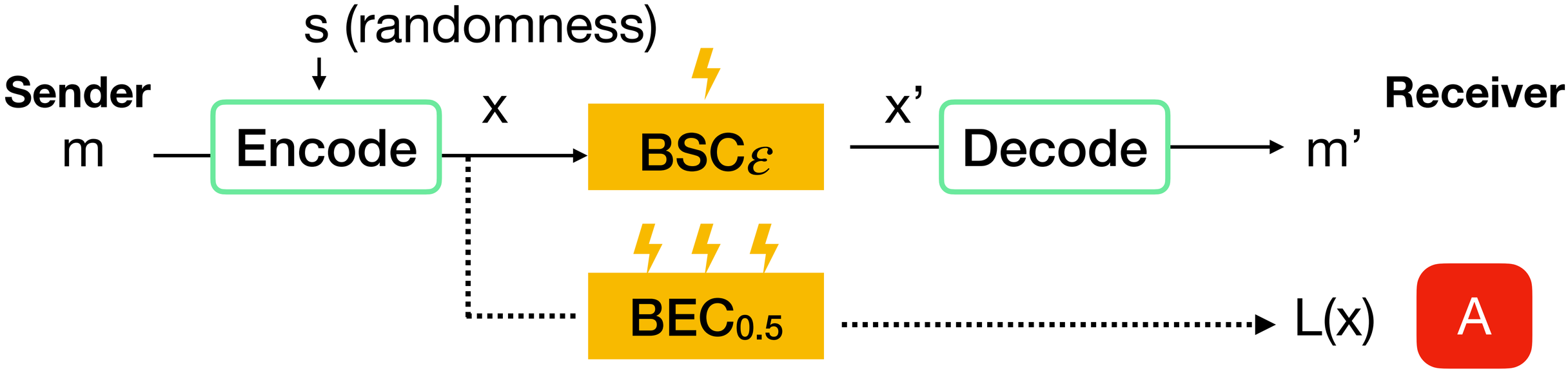
Wiretap Channel Model [Wyner75]



BSC: Binary Symmetric Channel, BEC: Binary Erasure Channel

- Adversary is affected by more noise than Receiver.
- Natural situations in wireless communication.

Wiretap Codes

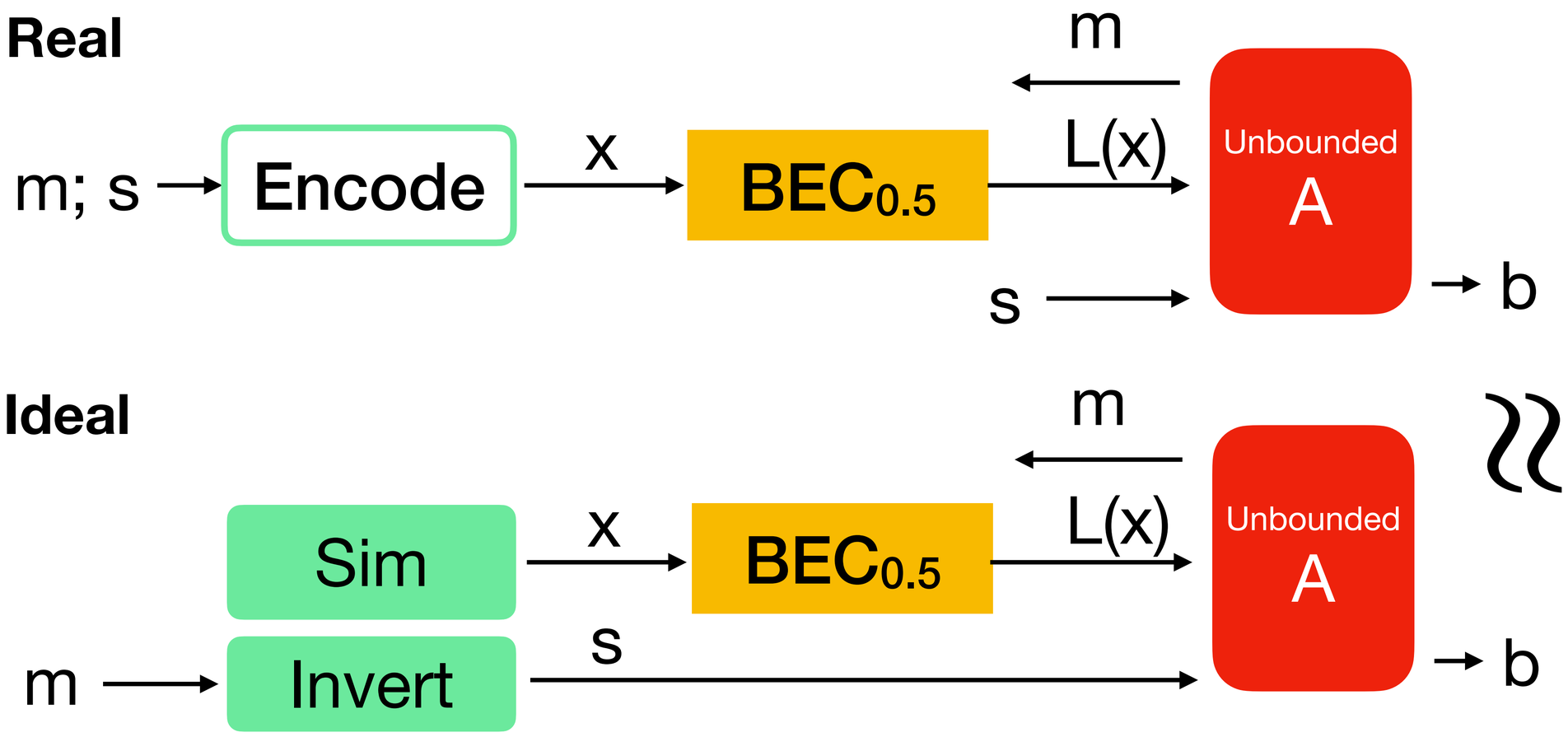


- Correctness : m = m'
- Security [BTV12] : L(Encode(m_0; s)) $\overset{s}{\approx}$ L(Encode(m_1; s))
- Rate : |m|/|x| $\leq$ Capacity of the Channel : H(U|ChA(U))-H(U|ChR(U))

  $= 1/2 - h_2(\varepsilon)$ (when ChR = BSCε, ChA = BEC$_{0.5}$) $h_2(\cdot)$: binary entropy function

Conditional Invertibility

- NCE (deniable) -style security for wiretap codes.
- Wiretap codes by [BTV12] already satisfy it.



Outline

1. Backgrounds & Overview
2. Weak NCE
3. Wiretap Codes
4. Amplify Weak NCE

Overview of Amplification

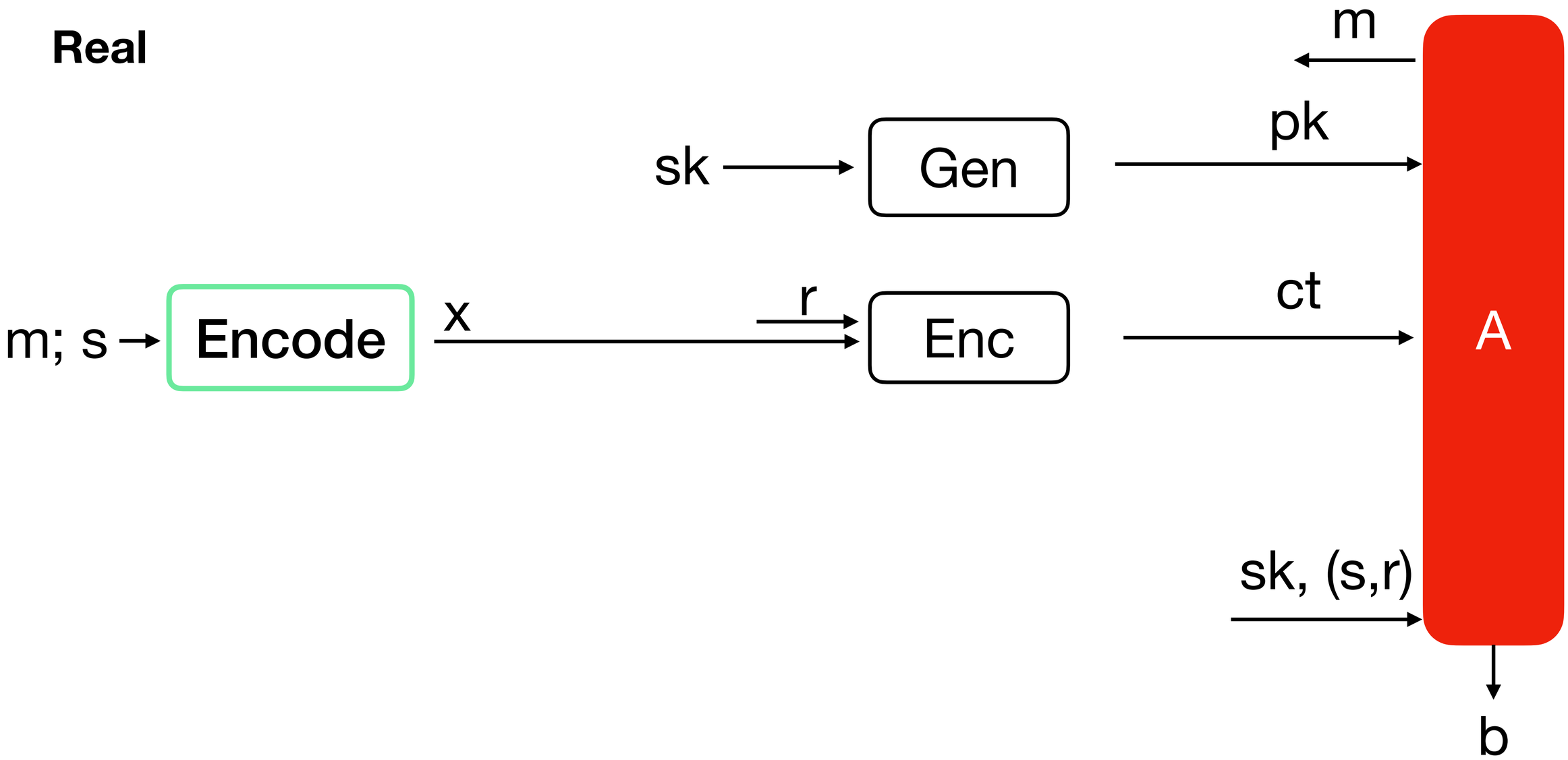
$$ct \leftarrow \mathbf{Enc}(pk, \mathbf{Encode}(m; s); r)$$

Weak Security + Conditional Invertibility → NCE is secure

$$m' \leftarrow \mathbf{Decode}(\mathbf{Dec}(sk, ct))$$

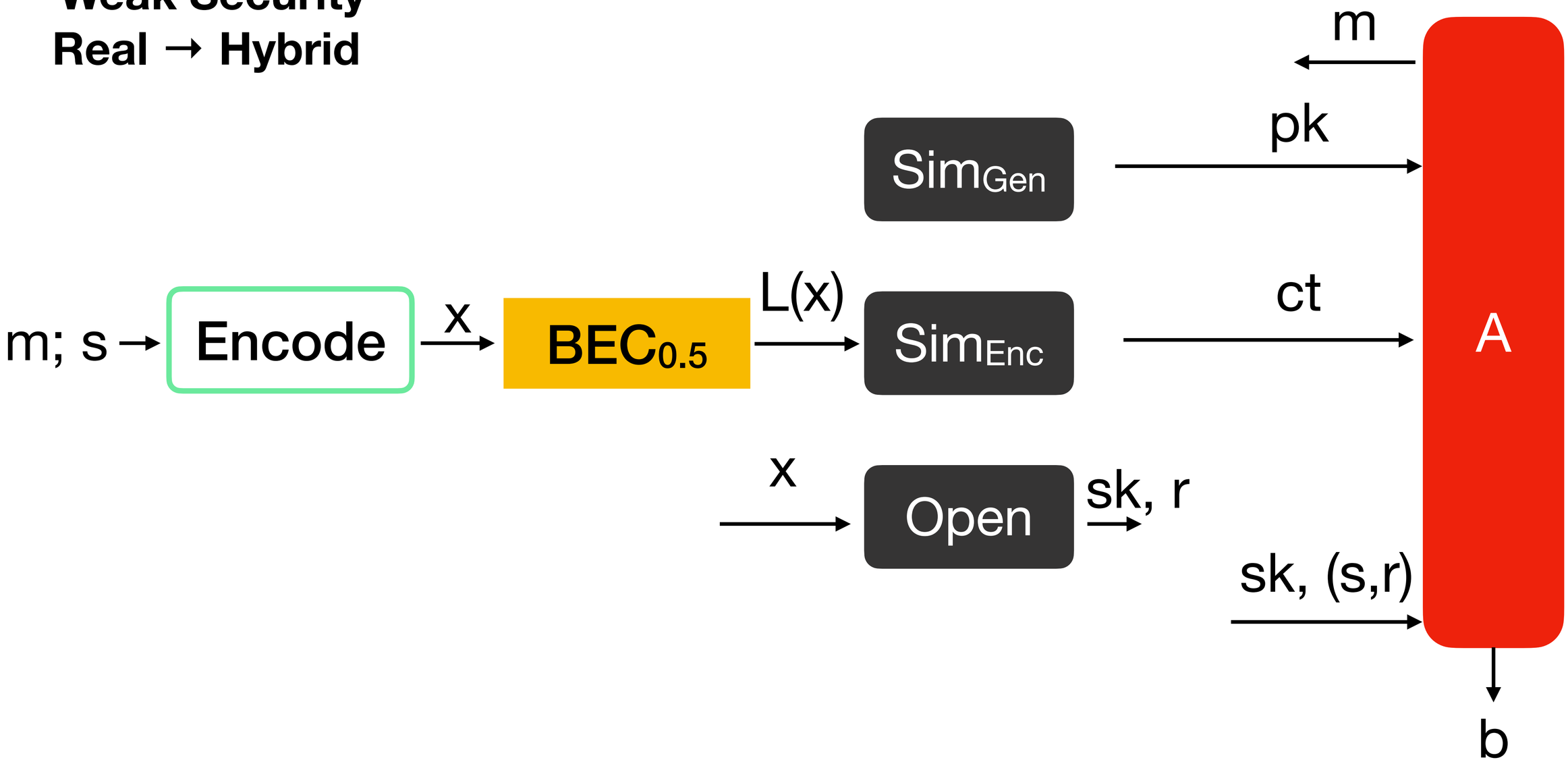
Correctness + Weak Correctness → NCE is correct

Security Proof

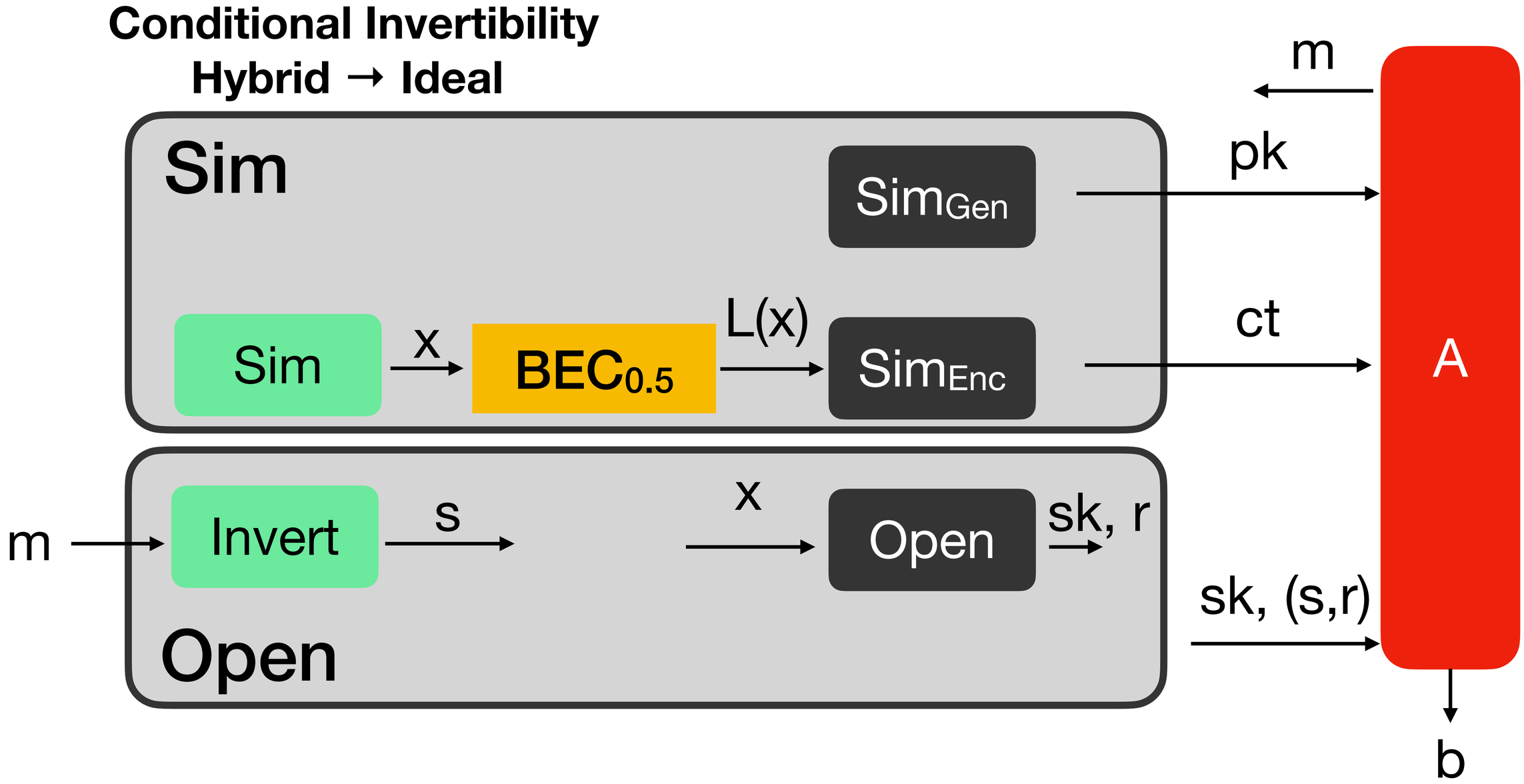


Security Proof

Weak Security
Real → Hybrid



Security Proof



Optimize the CT Expansion

- The weak NCE scheme has
  - CT expansion $R_{wNCE} = 2\ell + o(1)$.
  - Correctness error for each bit $\varepsilon = 1/2^{\ell+1}$.

Min. of $R_{NCE} \approx 27$ when $\ell = 5$.

- Wiretap codes for $\mathrm{BEC}_{0.5}$ (to adversary) and $\mathrm{BSC}_{\varepsilon}$ (to receiver) have
  - Rate $R_{WC} \leq 1/2 - h_2(\varepsilon)$.
- CT expansion of the amplified NCE $R_{NCE} = R_{wNCE}/R_{WC} + 1$.

(+1 come from the hybrid encryption with OTP)

Summary

- **NCE** is a key tool to establish secure channel in adaptively secure MPC.
- We define **weak NCE** and construct it from chameleon encryption.
- We amplified the weak NCE scheme using **wiretap codes** with conditional invertibility.
- The resulting NCE schemes achieved the first **O(1) CT expansion**.
- The **LWE** based scheme **improves PK expansion** over [YKT19].

Thank you for watching!