Broadcast, Trace and Revoke with Optimal Parameters from Polynomial Hardness

Shweta Agrawal
IIT Madras, India

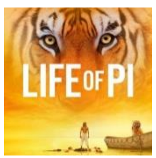
Simran Kumari
IIT Madras, India

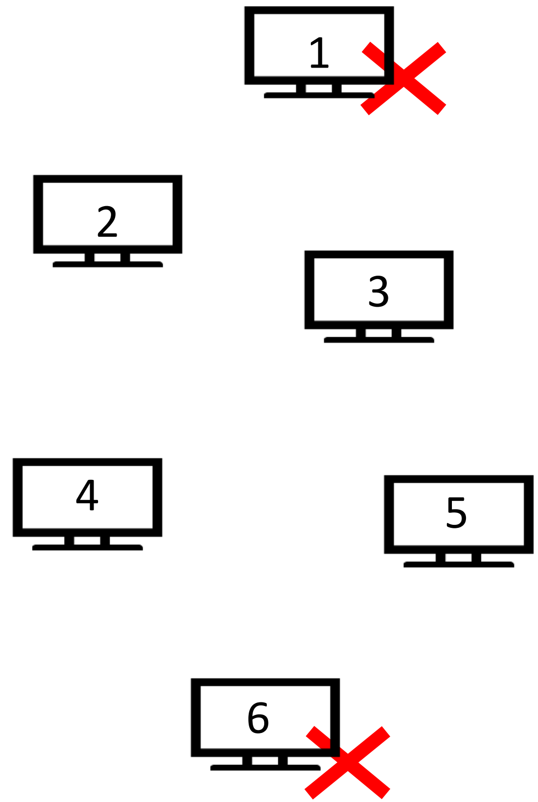
Anshu Yadav
IIT Madras, India

Shota Yamada
AIST, Japan

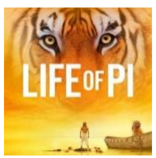
EUROCRYPT 2023

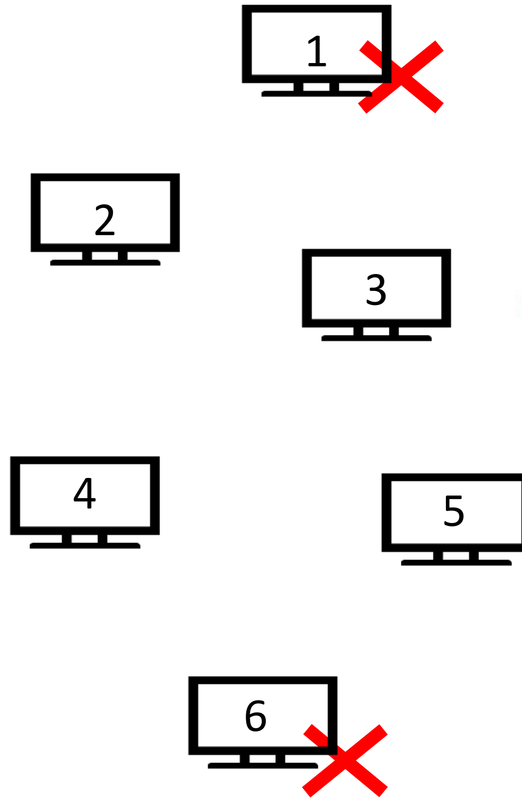
Motivation





Motivation

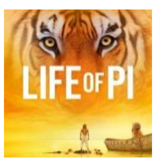


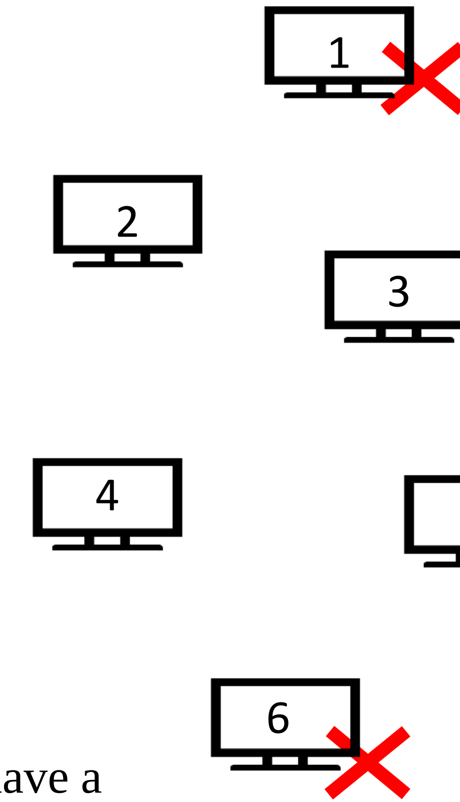


Trivial Approach : Using Public Key Encryption

|**ct**| grows linearly with the no. of users

Motivation



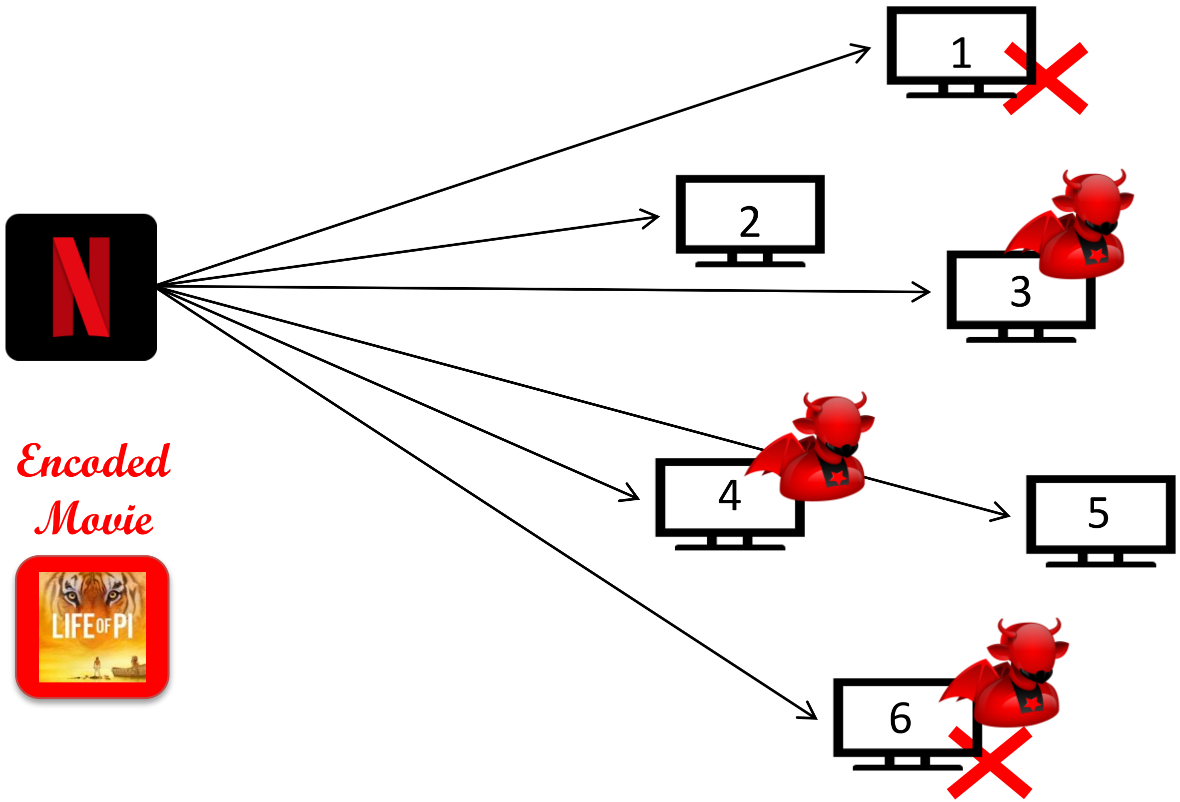


Trivial Approach : Using Public Key Encryption

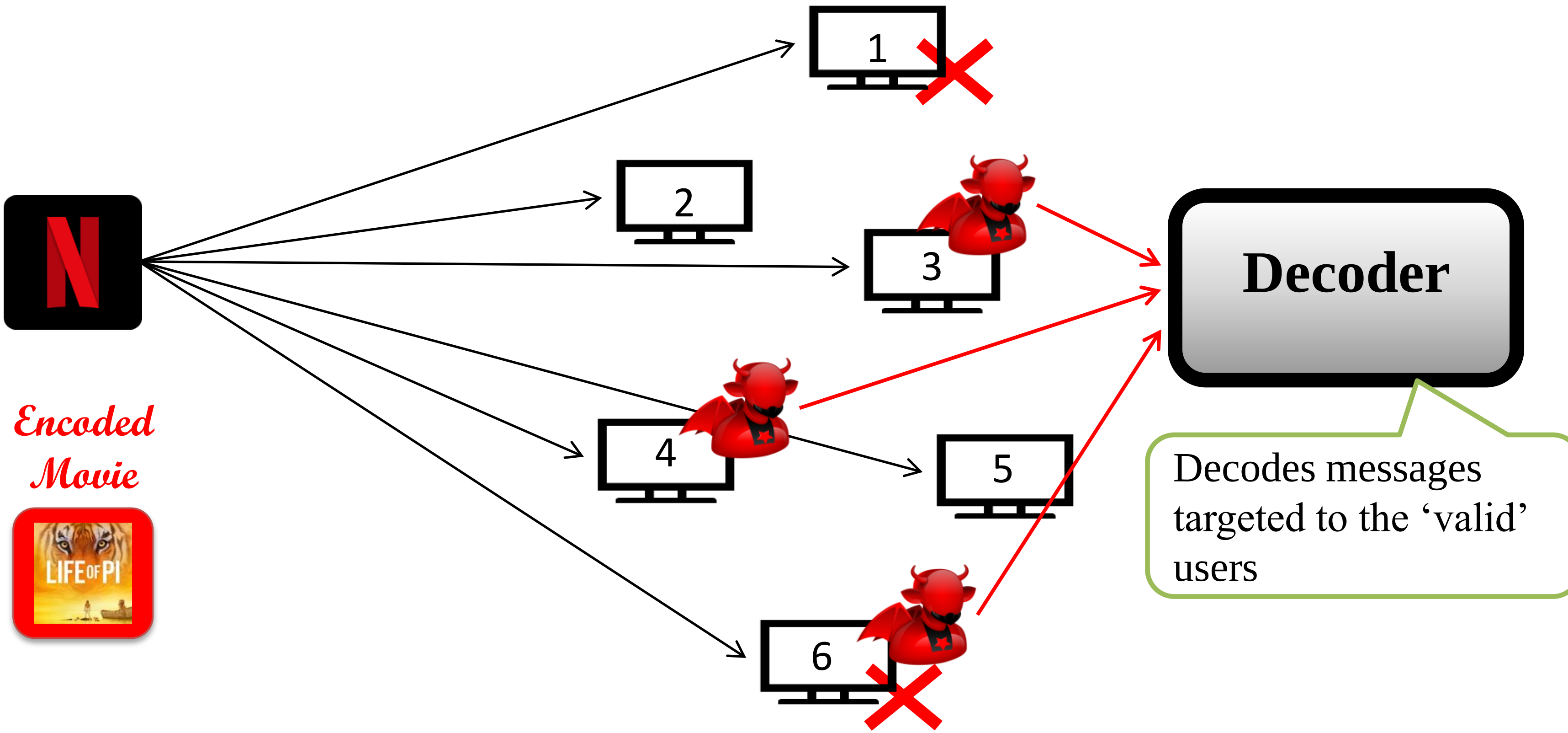
|ct| grows linearly with the no. of users

A better approach? Can we have a **short** common ct for all the users?

Motivation

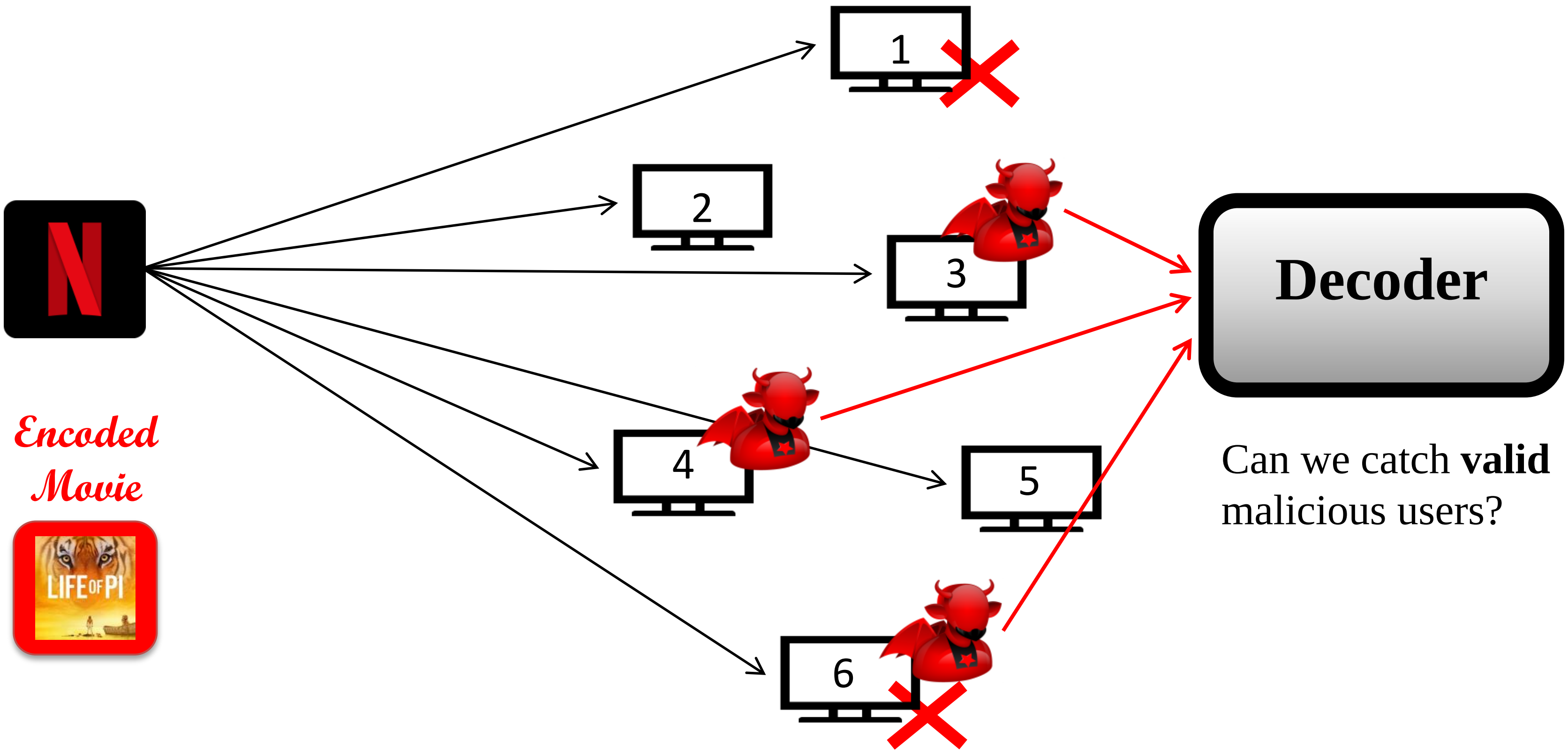


Motivation



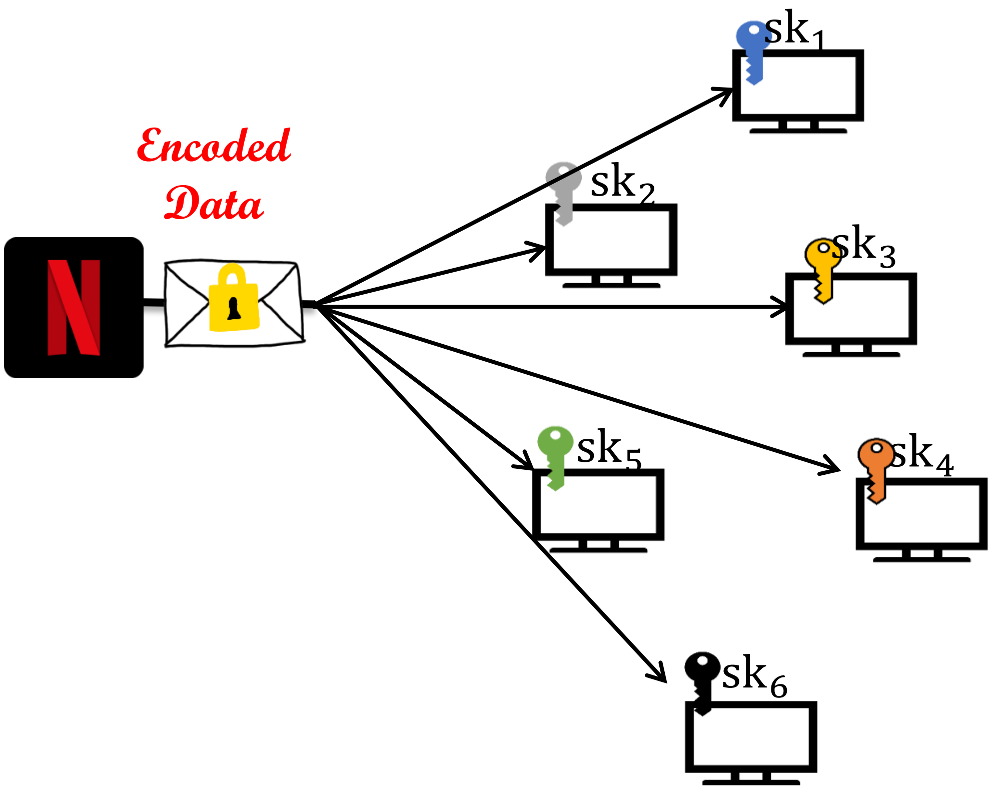
Encoded Movie
LIFE OF PI
1
2
3
4
5
6
Decoder
Decodes messages targeted to the 'valid' users

Motivation

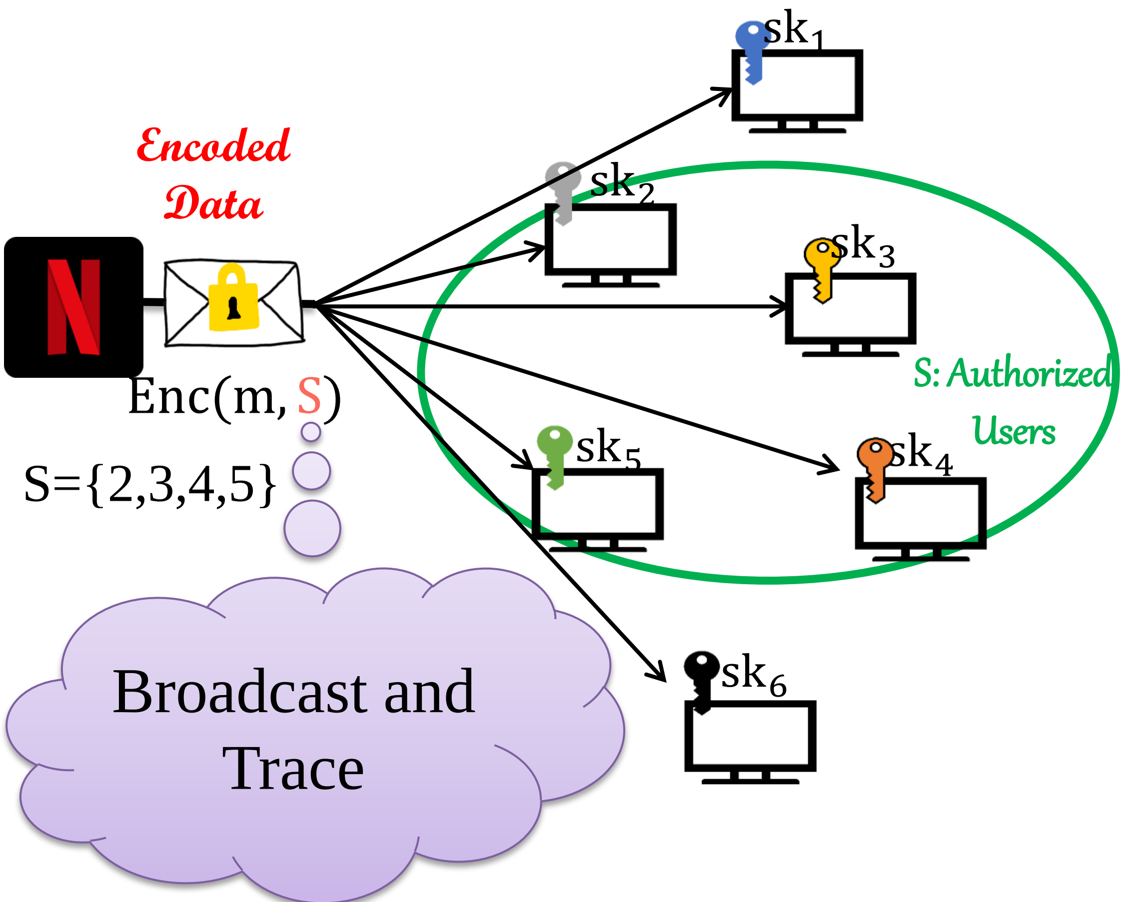


Can we catch **valid** malicious users?

Broadcast, Trace and Revoke[NP00]

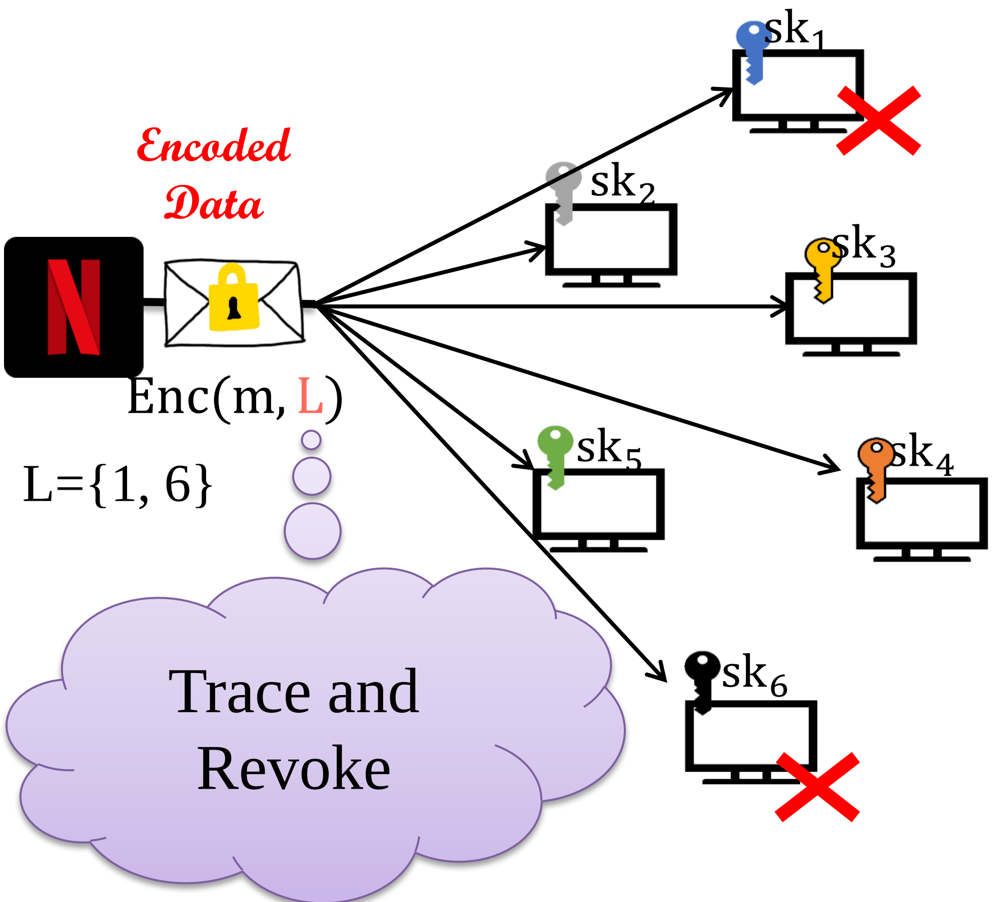


Broadcast, Trace and Revoke[NP00]



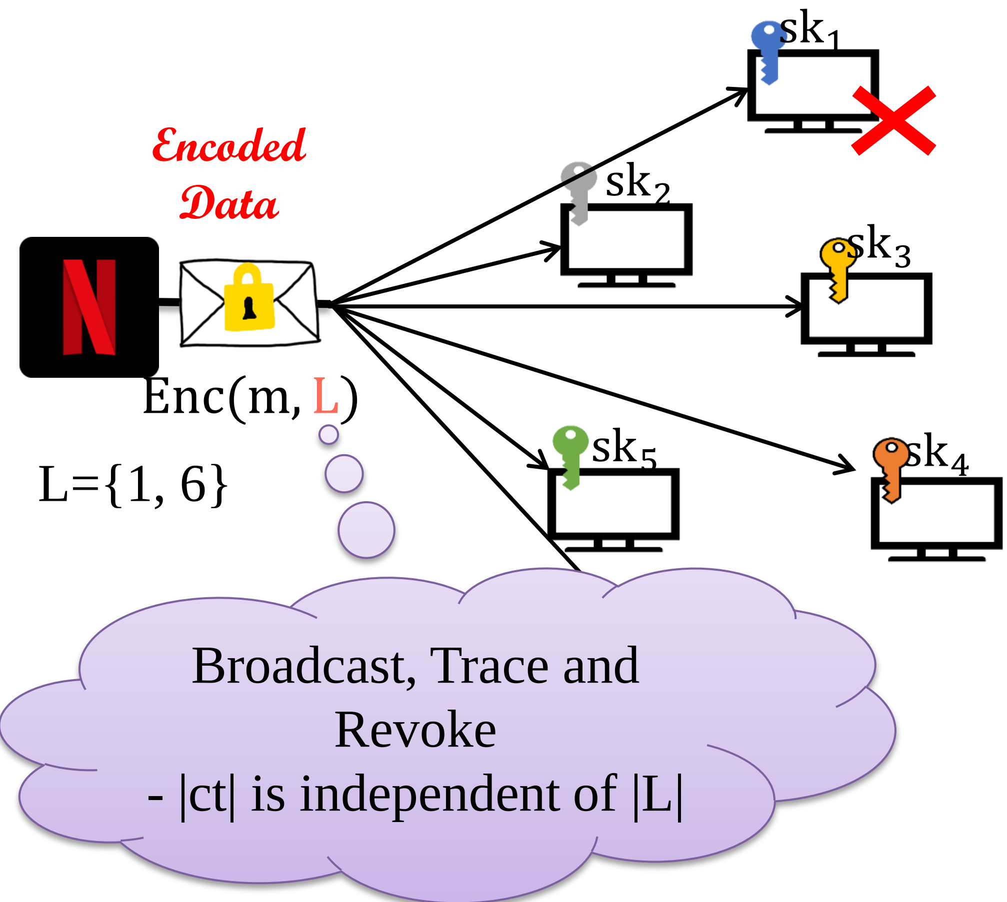
❖ Correctness: Any user in S can decrypt

Broadcast, Trace and Revoke[NP00]



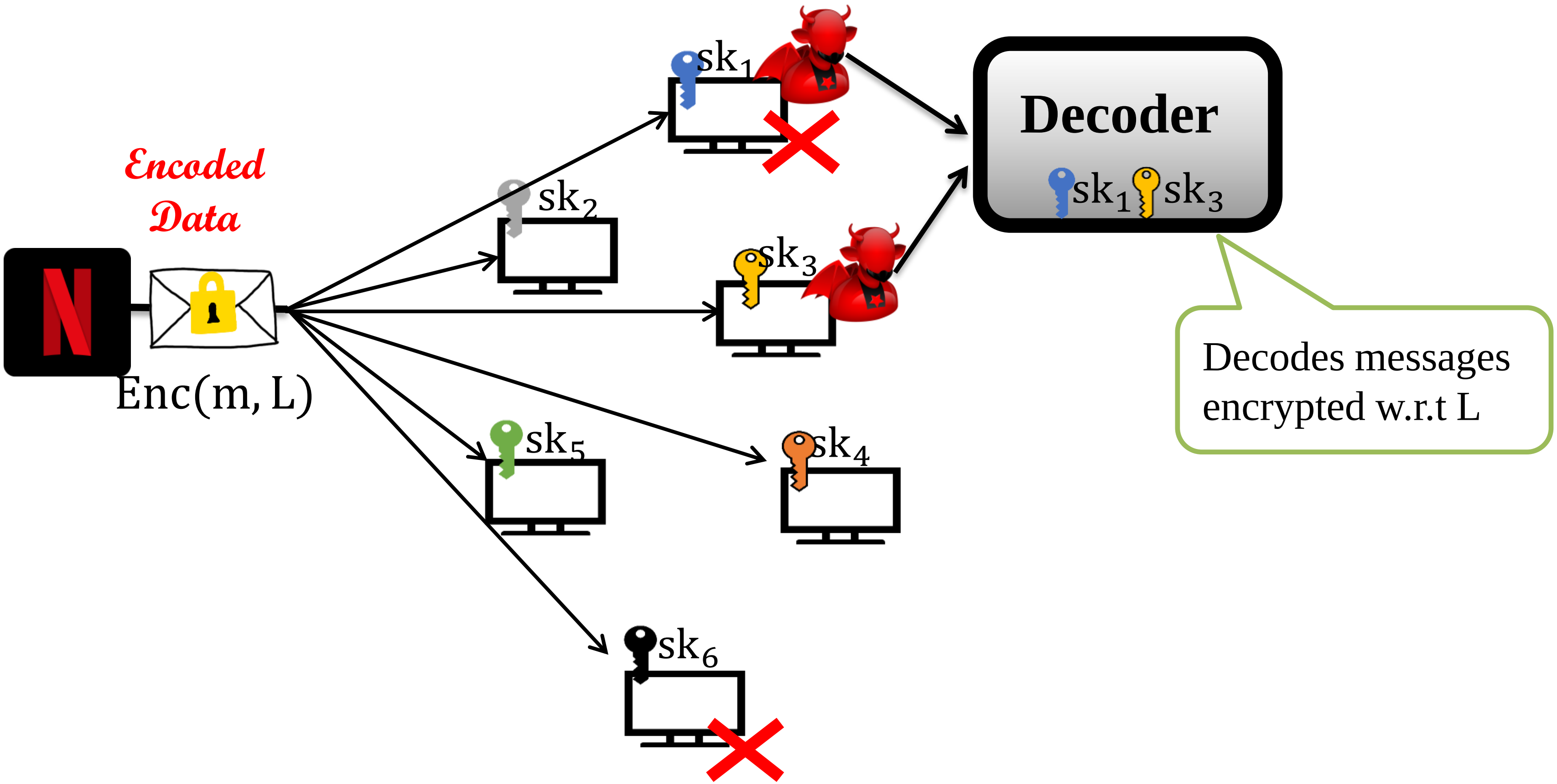
- Correctness: Any user outside L can decrypt

Broadcast, Trace and Revoke[NP00]

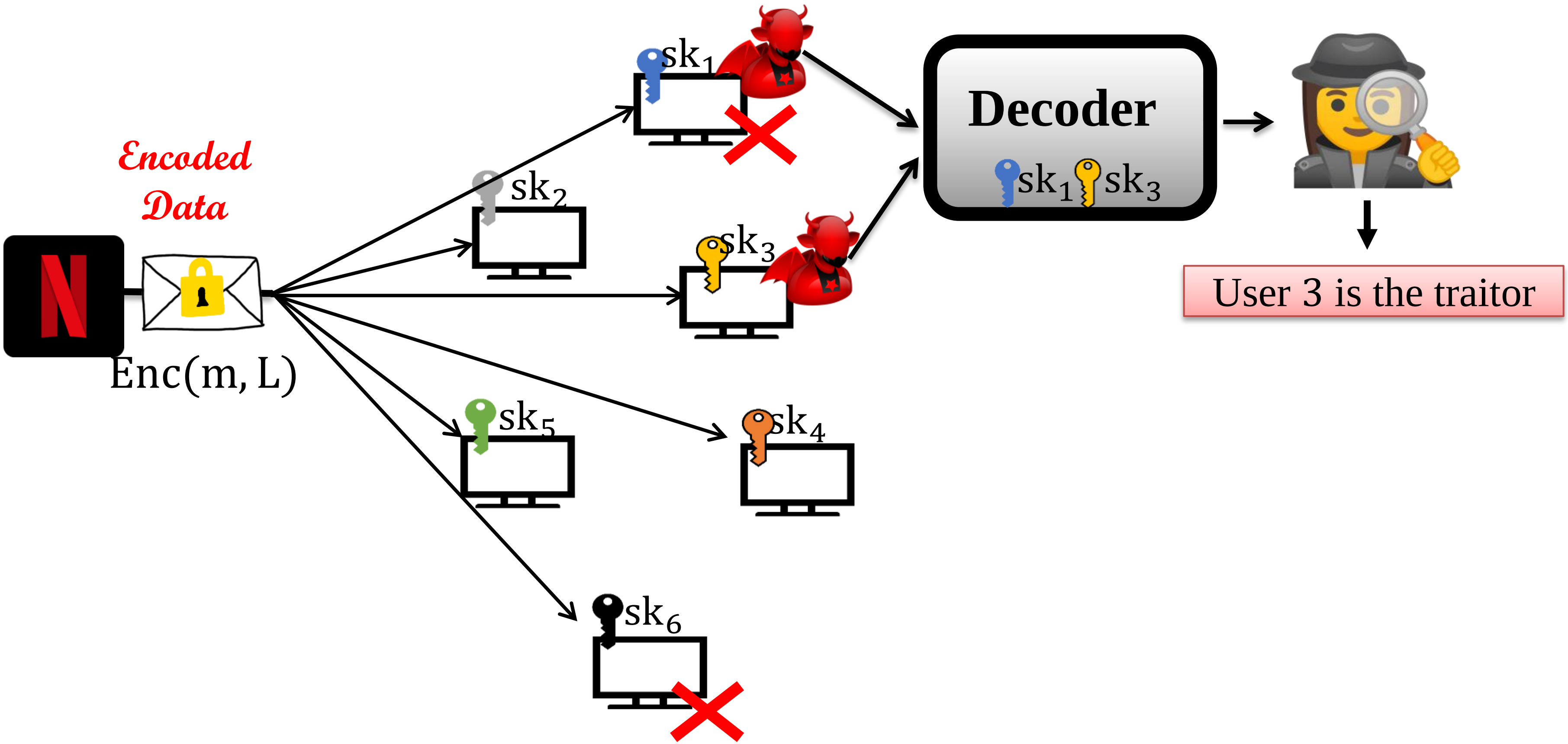


- Correctness: Any user outside L can decrypt

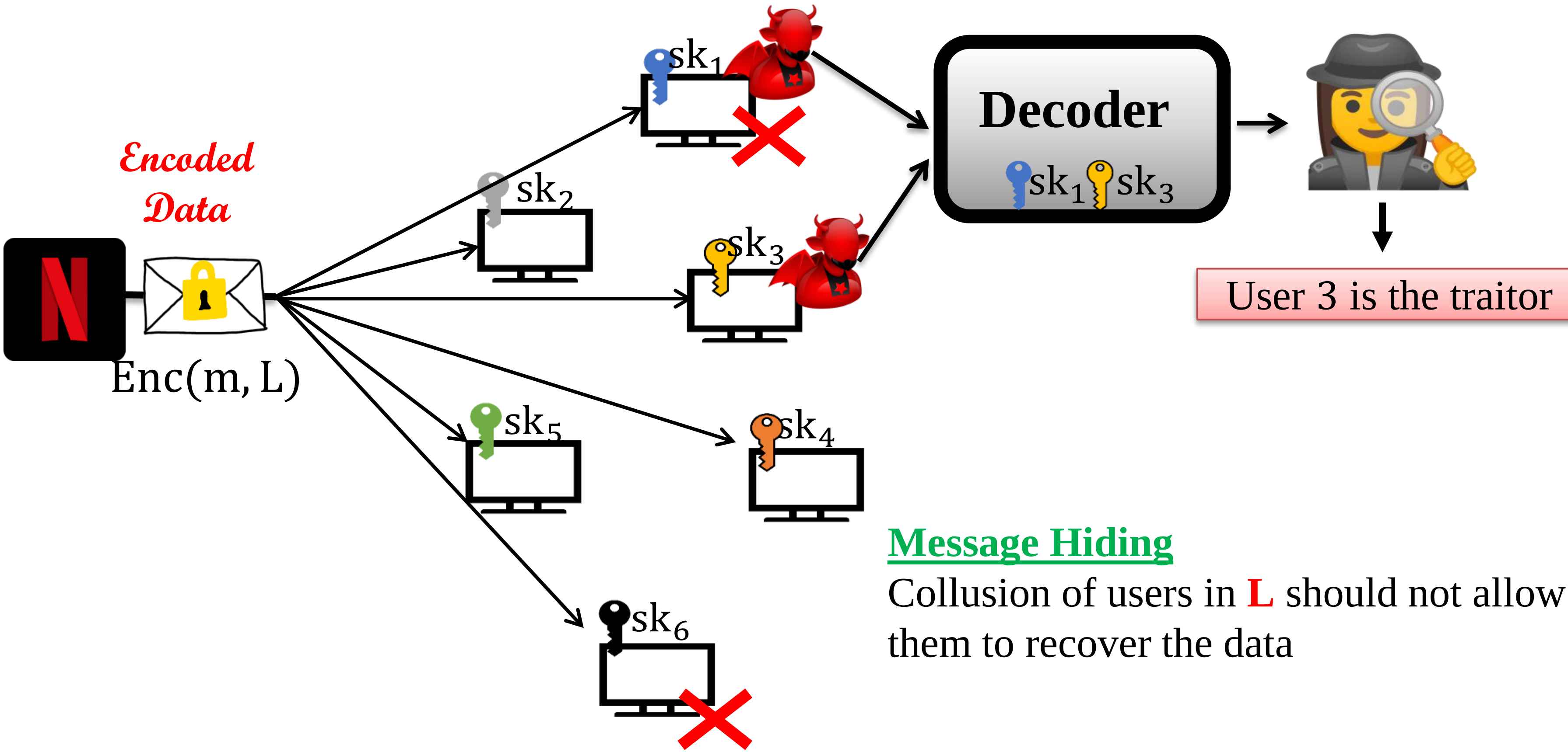
Broadcast, Trace and Revoke [NP00]



Broadcast, Trace and Revoke[NP00]



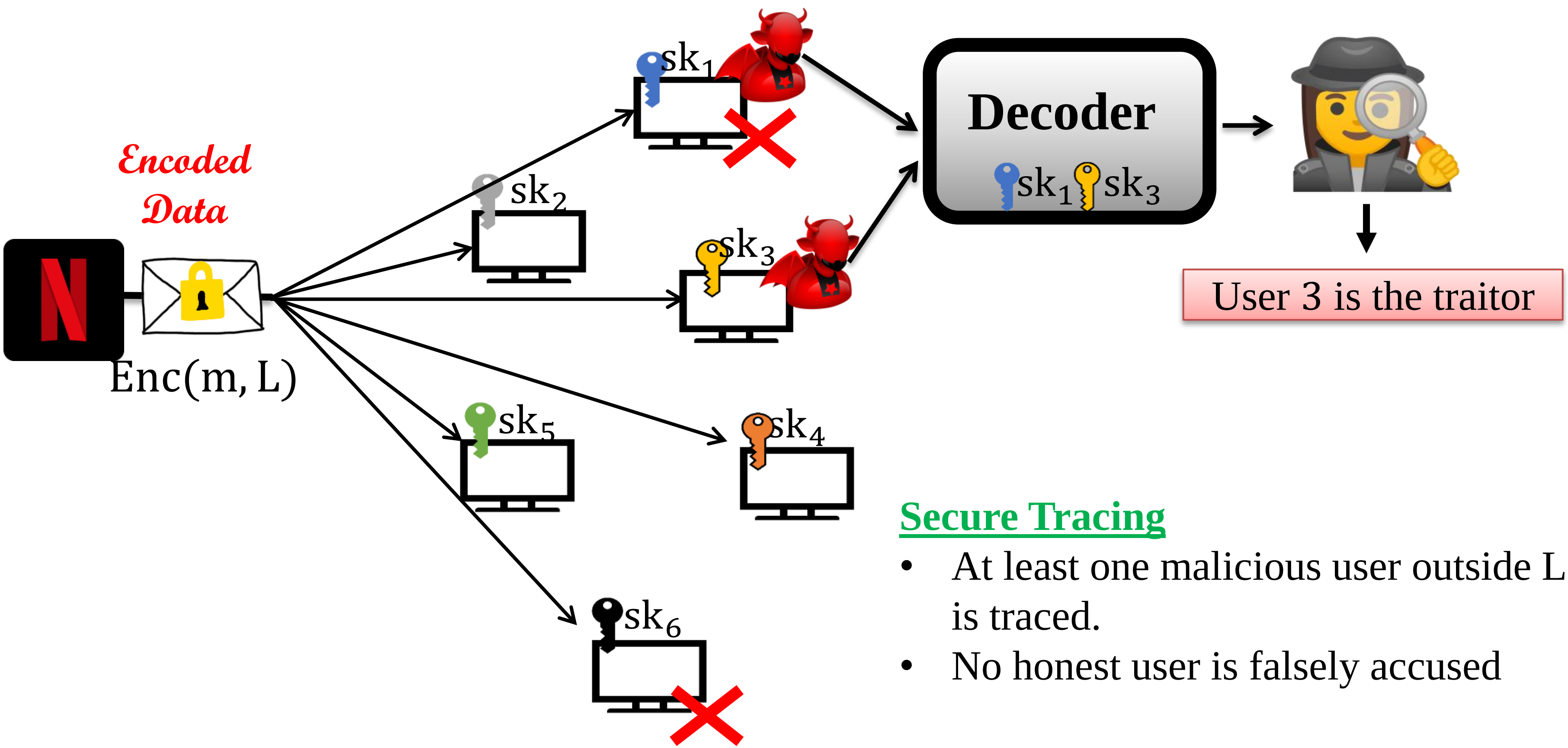
Broadcast, Trace and Revoke[NP00]



Message Hiding

Collusion of users in **L** should not allow them to recover the data

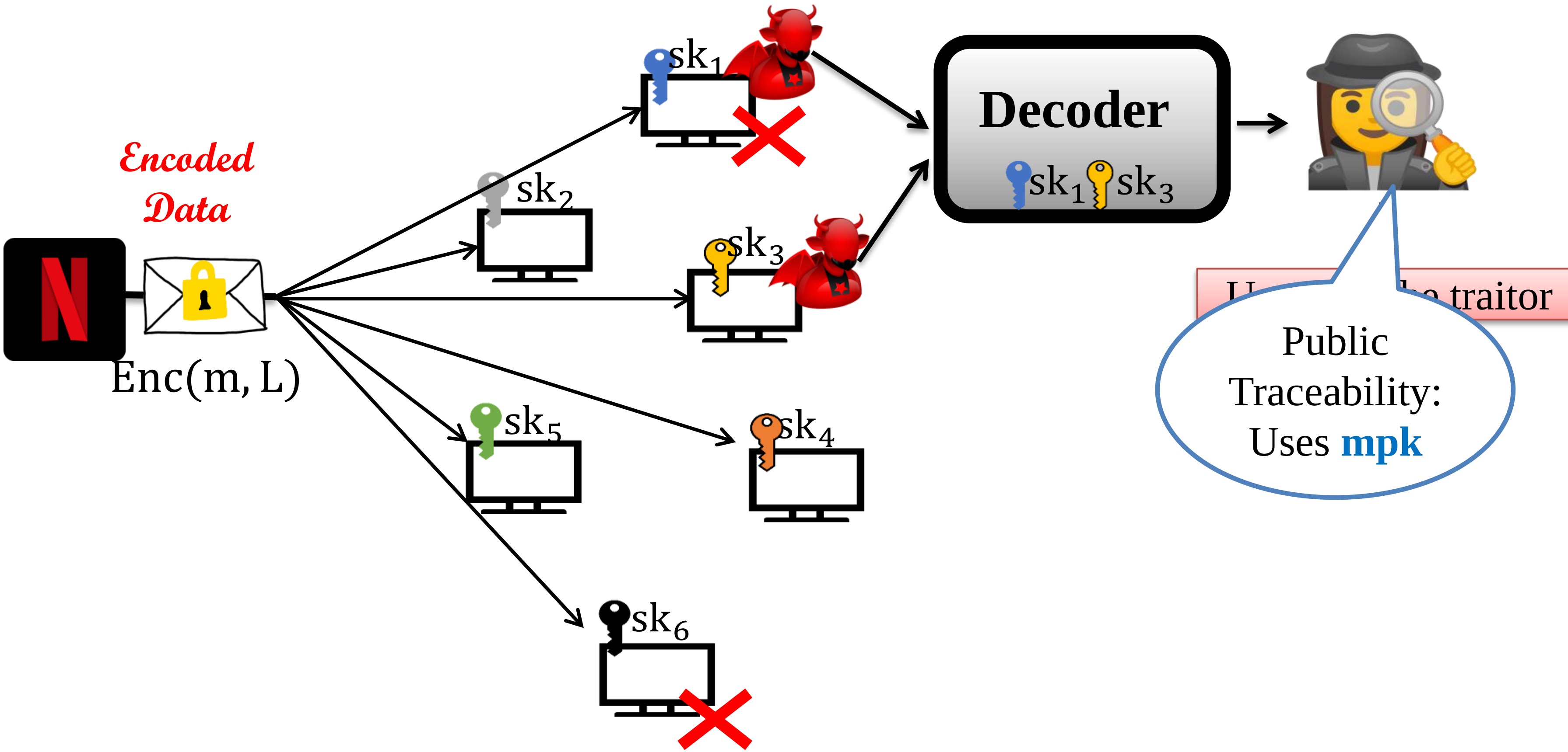
Broadcast, Trace and Revoke[NP00]



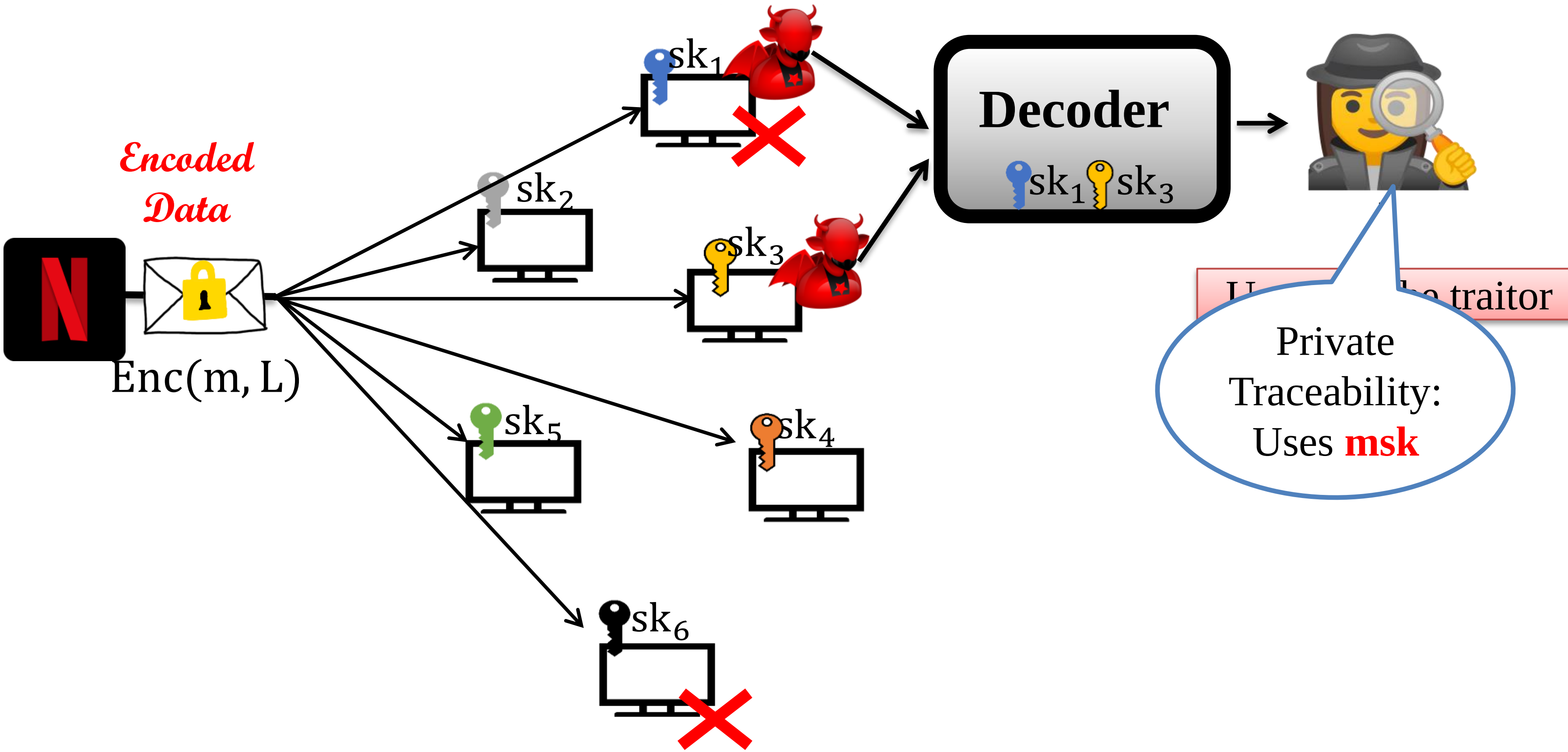
Secure Tracing

- At least one malicious user outside L is traced.
- No honest user is falsely accused

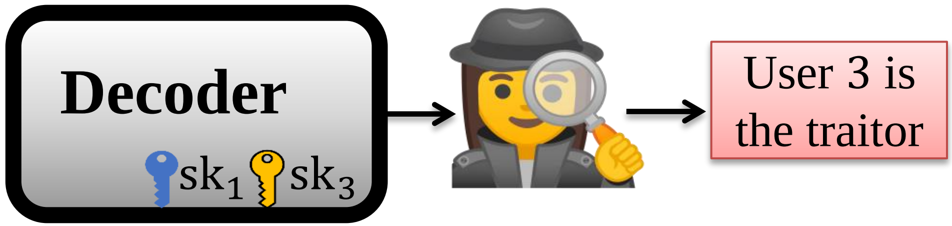
Broadcast, Trace and Revoke[NP00]



Broadcast, Trace and Revoke [NP00]



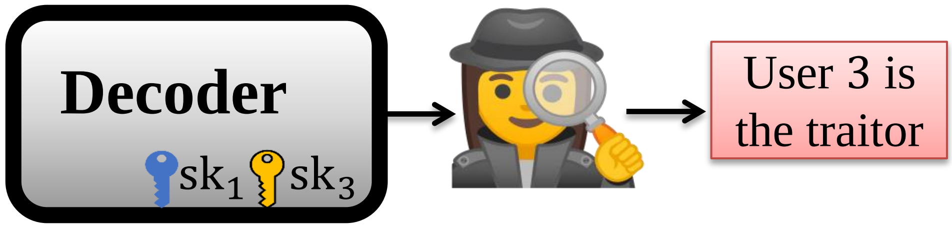
Embedded Identities [NWZ16]



User Index	User Identity
1	Nisha
2	Sampan
3	Rohin
4	Anuja
5	Anshu

'Rohin' is the traitor.
Revoke 'Rohin'

Embedded Identities[NWZ16]

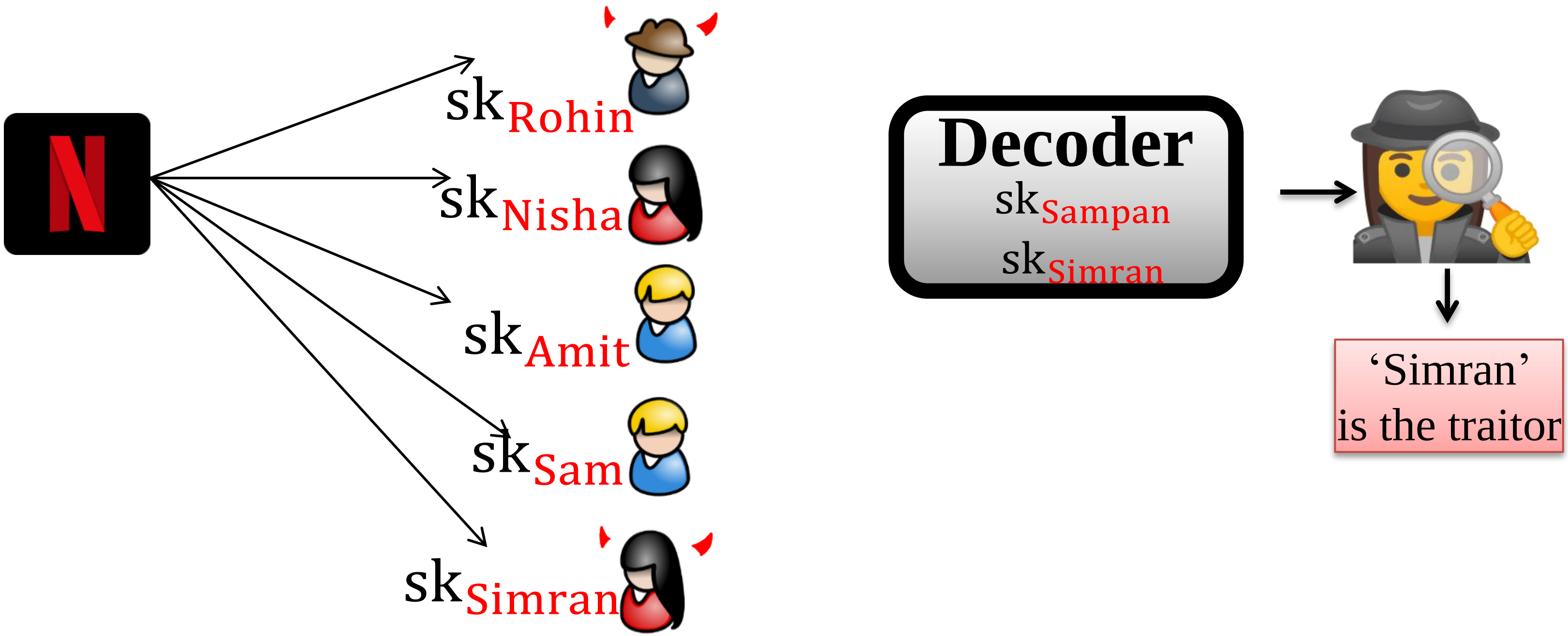


User Index	User Identity
1	Nisha
2	Sampan
3	Rohin
4	Anuja
5	Anshu

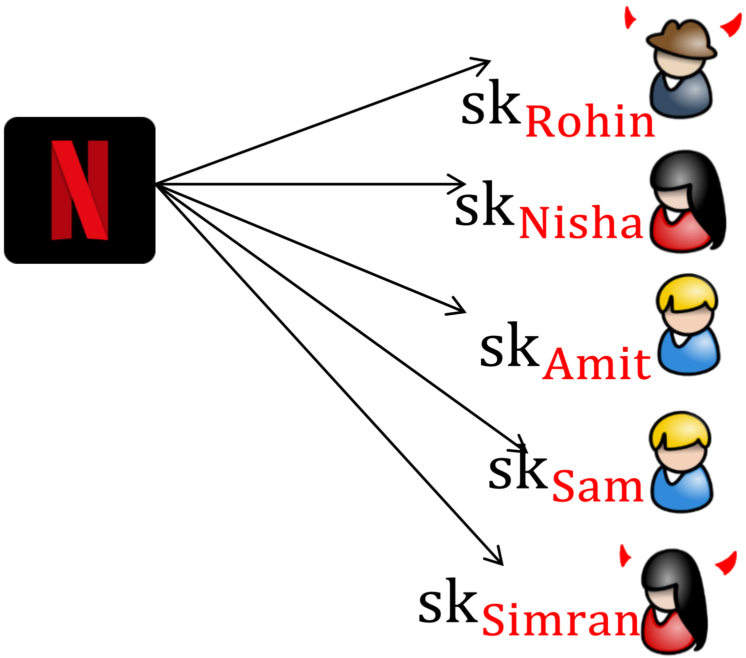
Limitations

- The authority needs to maintain user index-identity mapping
- Violates user's identity privacy.

Embedded Identities[NWZ16]



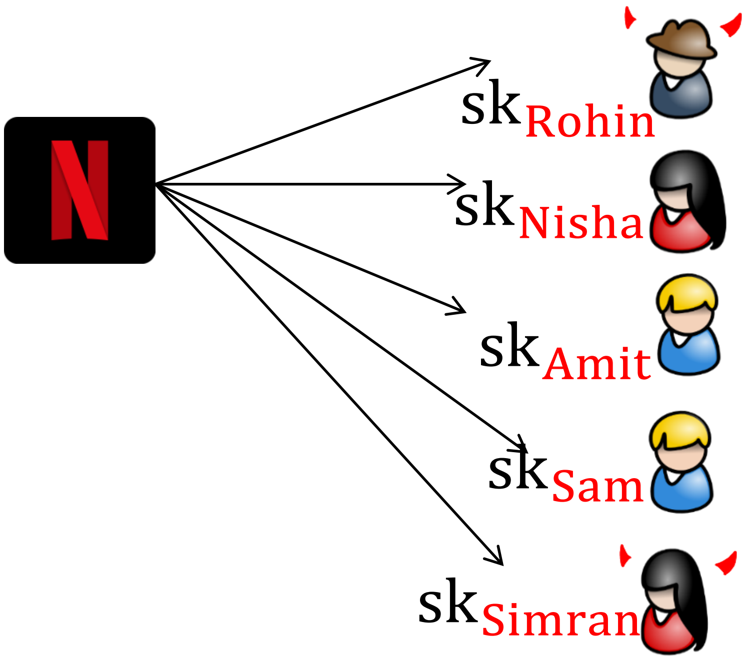
Embedded Identities[NWZ16]



Challenges:

- Traditional tracing method - ***linear search*** on the user space.
- Identity space can be exponential -- *exponential time* to output traitors

Embedded Identities[NWZ16]



Solutions:

- [Nishimaki-Wichs-Zhandry16] - Traitor Tracing & Trace and Revoke schemes with embedded identities.
- [Goyal-Koppula-Waters19] - Traitor tracing scheme with embedded identities

Broadcast, Trace and Revoke : Goals

Optimal Parameters

|ct|, |pk| and |sk| independent of no. of users

Broadcast, Trace and Revoke : Goals

Optimal Parameters

Adaptive Security w.r.t Revocation List L

$ct \leftarrow Enc(m, L)$

Adaptive: L can be chosen after the adversary gets the public parameters and user secret keys.

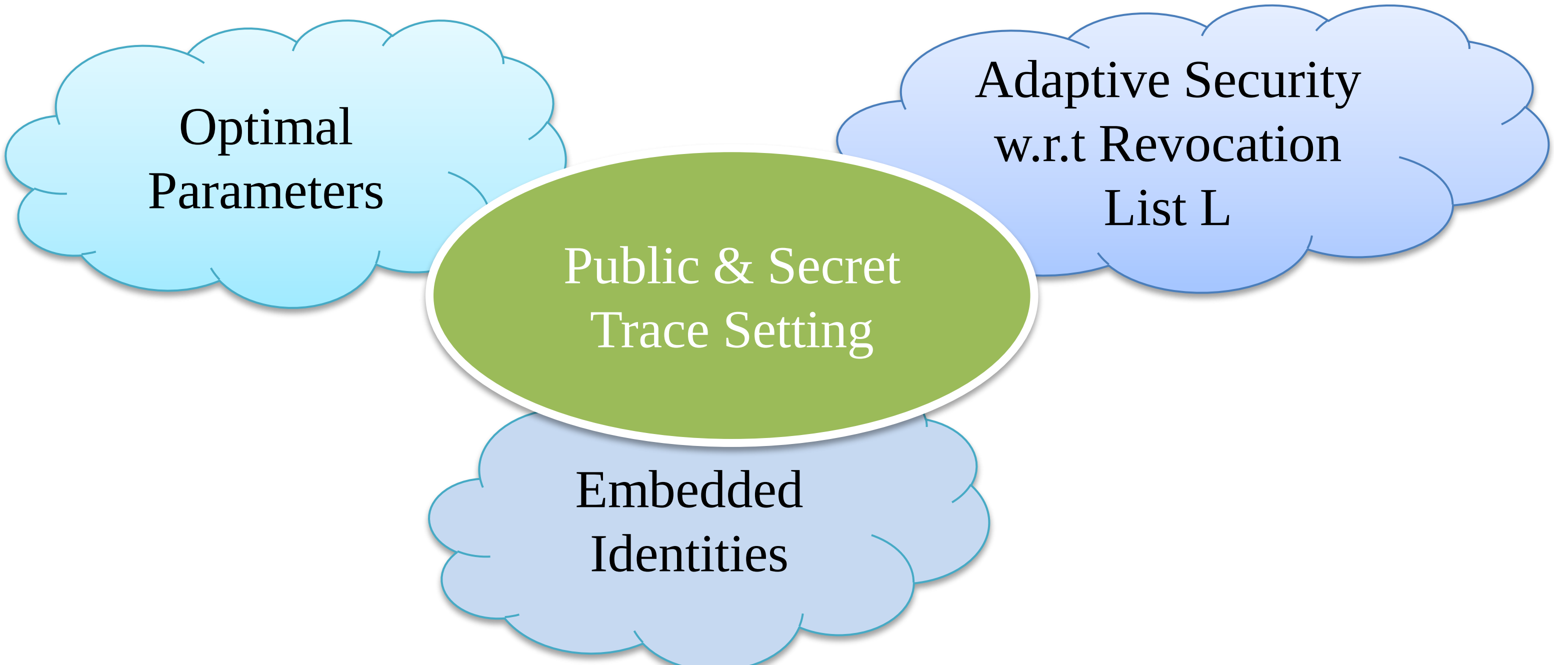
Broadcast, Trace and Revoke : Goals

Optimal Parameters

Adaptive Security w.r.t Revocation List L

Embedded Identities

Broadcast, Trace and Revoke : Goals



Prior Work : Public Traceability

	|CT|	|SK|	|PK|	Trace Space	Selective/ Adaptive	Asspn	Identities
[NWZ16]	1	1	1	Exp	Selective	Subexp (iO)	Yes

polylog(N, L) and poly(sec param) shown as 1.

Prior Work : Public Traceability

	|CT|	|SK|	|PK|	Trace Space	Selective/ Adaptive	Asspn	Identities
[NWZ16]	1	1	1	Exp	Selective	Subexp (iO)	Yes
[GVW19]	1	1	1	Poly	Adaptive	Subexp (subexp Positional Witness Enc)	No

polylog(N, L) and poly(sec param) shown as 1.

Prior Work : Public Traceability

	|CT|	|SK|	|PK|	Trace Space	Selective/ Adaptive	Asspn	Identities
[NWZ16]	1	1	1	Exp	Selective	Subexp (iO)	Yes
[GVW19]	1	1	1	Poly	Adaptive	Subexp (subexp PWE)	No
This Work	**1**	**1**	**1**	**Exp**	**Adaptive**	**Poly (FE and Spcl ABE)**	**Yes**

polylog(N, L) and poly(sec param) shown as 1.

Public Traceability : Assumptions

[NWZ16] **iO** Inherently sub-exponential assumption

[GVW19] **Sub-exp PWE** No construction from poly hardness known

Public Traceability : Assumptions

[NWZ16]	**iO**	Inherently sub-exponential assumption
[GVW19]	**Sub-exp PWE**	No construction from poly hardness known
This Work	**Spcl FE**	**Spcl ABE**

Building Blocks

Functional Encryption (FE)

$$sk_C + Enc(m) \xrightarrow{\text{Decrypt}} C(m)$$

The decryptor learns **only** $C(m)$ and nothing else.

Building Blocks

Functional Encryption (FE)

$$sk_C + Enc(m) \xrightarrow{\text{Decrypt}} C(m)$$

The decryptor learns **only** $C(m)$ and nothing else.

Key Policy Attribute Based Encryption (KP-ABE)

$$sk_C + Enc(m, x) \xrightarrow{\text{Decrypt}} m \text{ iff } C(x) = 1$$

Restricted access using the secret key

Building Blocks

Functional Encryption (FE)

$$sk_C + Enc(m) \xrightarrow{\text{Decrypt}} C(m)$$

The decryptor learns **only** $C(m)$ and nothing else.

CT Policy Attribute Based Encryption (CP-ABE)

$$sk_x + Enc(m, C) \xrightarrow{\text{Decrypt}} m \text{ iff } C(x) = 1$$

Restricted access using the secret key

Public Traceability : Assumptions

[NWZ16]	**iO**	Inherently sub-exponential assumption
[GVW19]	**Sub-exp PWE**	No construction from poly hardness known
This Work	**Spcl FE [JLS21,JLS22]** **Spcl KP-ABE [BGG+14]**	

Known from polynomially hard assumptions

Prior Work: Secret Traceability

	|CT|	|SK|	|PK|	Trace Space	Asspn	Identities
[GQWW19]	N^a	N^c	N	Poly	LWE and Pairings	No

$0 < a < 1$, c large constant.

Prior Work: Secret Traceability

	|CT|	|SK|	|PK|	Trace Space	Asspn	Identities
[GQWW19]	N^a	N^c	N	Poly	LWE and Pairings	No
[Zha20]	N^a	N^{1-a}	N^{1-a}	Poly	GGM Pairings	No

$0 < a < 1$, c large constant.

Prior Work: Secret Traceability

	|CT|	|SK|	|PK|	Trace Space	Asspn	Identities
[GQWW19]	N^a	N^c	N	Poly	LWE and Pairings	No
[Zha20]	N^a	N^{1-a}	N^{1-a}	Poly	GGM Pairings	No
This Work: Modified [GQWW19]	**1**	$\boldsymbol{N^c}$	$\boldsymbol{N}$	**Poly**	**LWE and Pairings**	**No**

polylog(N, L) and poly(sec param) shown as 1.
$0 < a < 1$, c large constant.

Prior Work: Secret Traceability

	|CT|	|SK|	|PK|	Trace Space	Asspn	Identities
[GQWW19]	N^{ϵ}	N^{c}	N	Poly	LWE and Pairings	No
[Zha20]	N^{a}	N^{1-a}	N^{1-a}	Poly	GGM Pairings	No
This Work: Modified [GQWW19]	**1**	$\boldsymbol{N^{c}}$	$\boldsymbol{N}$	**Poly**	**LWE and Pairings**	**No**
[KW20]	L	1	1	Exp	Subexp LWE	Yes

polylog(N, L) and poly(sec param) shown as 1.
$0 < a < 1$, c large constant.

Prior Work: Secret Traceability

	|CT|	|SK|	|PK|	Trace Space	Asspn	Identities
[GQWW19]	N^{ϵ}	N^{c}	N	Poly	LWE and Pairings	No
[Zha20]	N^{a}	N^{1-a}	N^{1-a}	Poly	GGM Pairings	No
This Work: Modified [GQWW19]	**1**	$\boldsymbol{N^{c}}$	$\boldsymbol{N}$	**Poly**	**LWE and Pairings**	**No**
[KW20]	L	1	1	Exp	Subexp LWE	Yes
This Work	**1**	**1**	**1**	**Exp**	**Poly (spcl CP-ABE & KP-ABE)**	**Yes**

polylog(N, L) and poly(sec param) shown as 1.

Secret Traceability : Assumptions

[GQWW19]

[Zha20]

Pairings Post-Quantum insecure

Secret Traceability : Assumptions

[GQWW19] [Zha20]	**Pairings**	Post-Quantum insecure
[KW19]	**Sub-exp LWE**	|ct| linear in size of revocation list

Secret Traceability : Assumptions

[GQWW19] [Zha20]	**Pairings**	Post-Quantum insecure
[KW19]	**Sub-exp LWE**	|ct| linear in size of revocation list
This Work	**Spcl CP-ABE** **Spcl KP-ABE**	

Secret Traceability : Assumptions

[GQWW19] [Zha20]	**Pairings**	Post-Quantum insecure
[KW19]	**Sub-exp LWE**	|ct| linear in size of revocation list
This Work	**Spcl CP-ABE** Evasive & Tensor LWE [Wee22] **Spcl KP-ABE** Std. LWE [BGG+14]	• Polynomially hard • Lattice based – conjectured post quantum safe

Public-Key vs Secret-Key BTR

Public Traceability

- Succinct KP-ABE
- Compact FE

Secret Traceability

- Succinct KP-ABE
- Compact CP-ABE

Public-Key vs Secret-Key BTR

Public Traceability

- Succinct KP-ABE
- Compact FE

Secret Traceability

- Succinct KP-ABE
- Compact CP-ABE

ABE is weaker than FE since ABE is an all or nothing primitive in contrast to FE.

Outline

Public-Key
Revocable Predicate Encryption (RPE)

→

Public-Key
Broadcast, Trace and Revoke with Embedded Identity (EI-BTR)

Secret-Key
Revocable Predicate Encryption (RPE)

→

Secret-Key
Broadcast, Trace and Revoke with Embedded Identity (EI-BTR)

Revocable Predicate Encryption[KW19]

Revoked labels
L=$\{lb_2, lb_5\}$

sk_{lb_1,x_1}

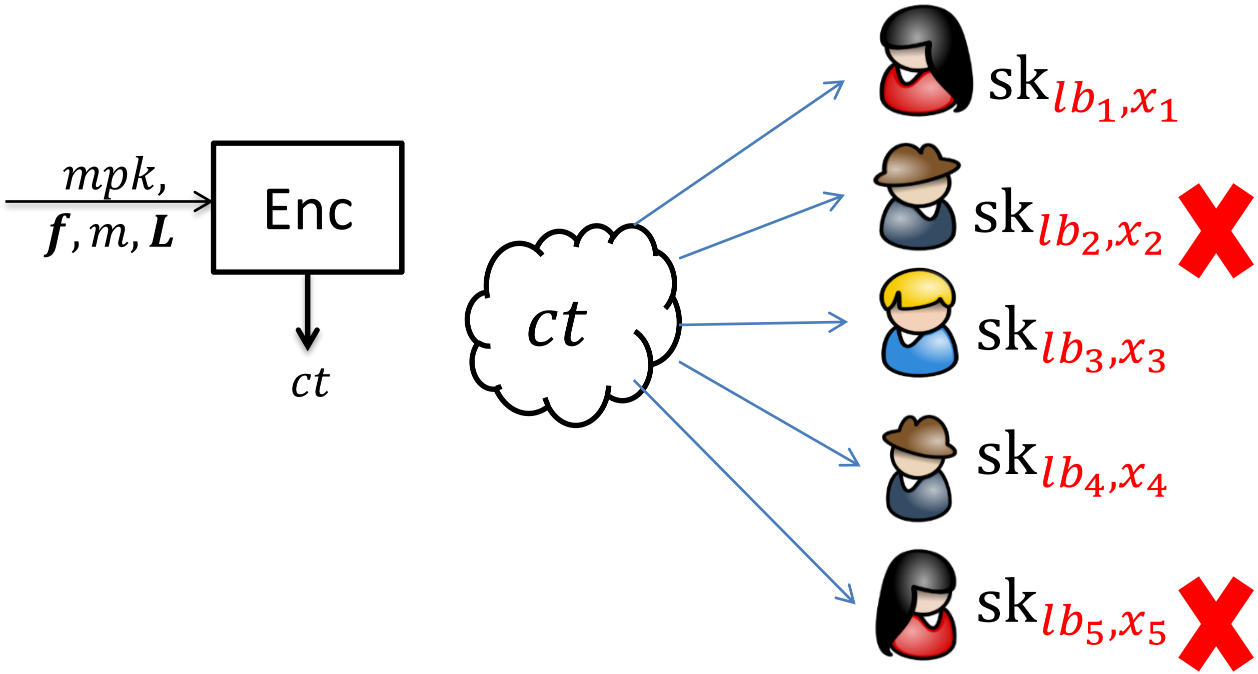
sk_{lb_2,x_2}

sk_{lb_3,x_3}

sk_{lb_4,x_4}

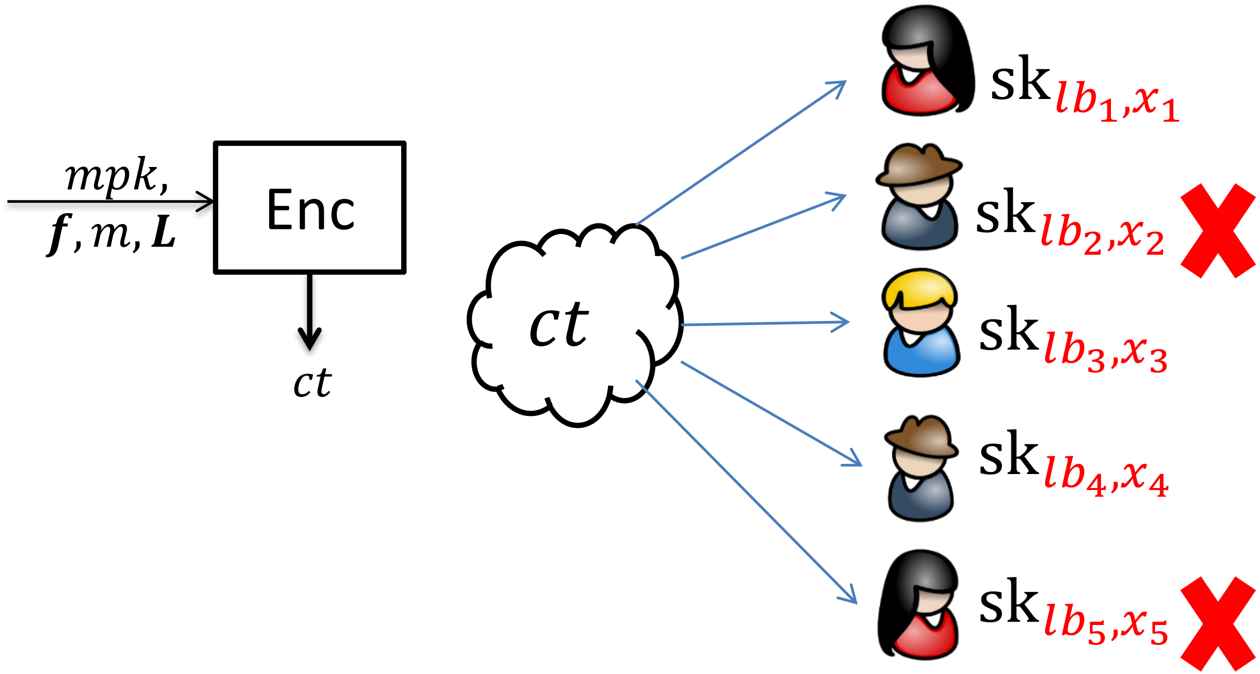
sk_{lb_5,x_5}

Revocable Predicate Encryption[KW19]



Revoked labels
L=$\{lb_2, lb_5\}$

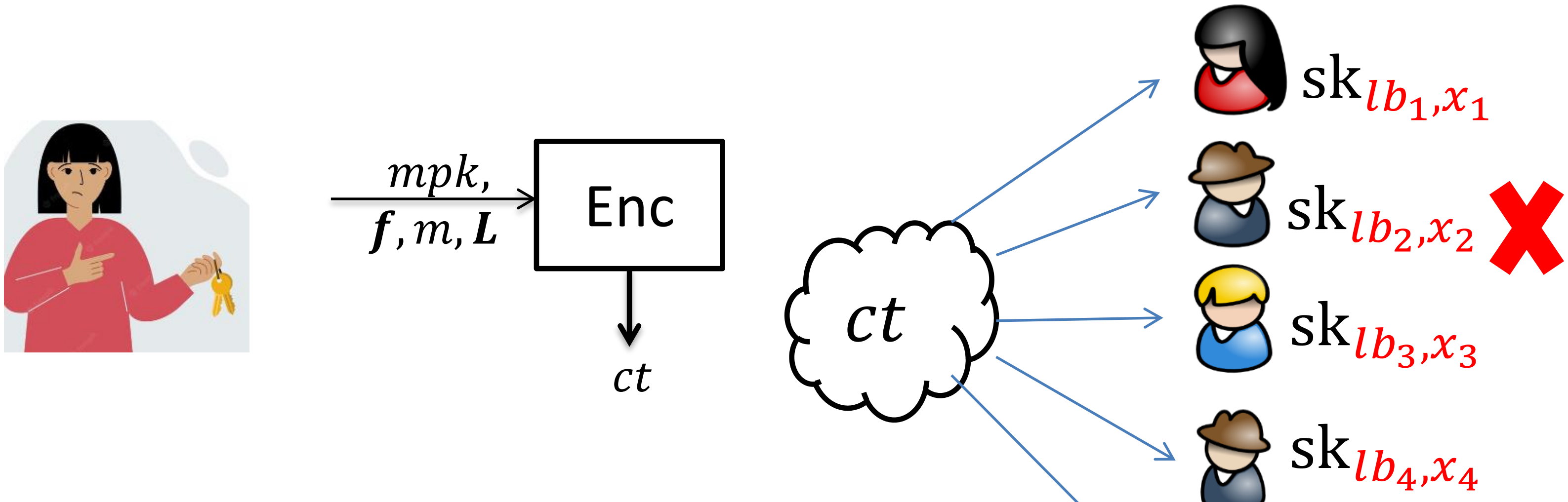
Revocable Predicate Encryption[KW19]



Revoked labels
L={lb_2, lb_5}

Correctness : A user with associated (lb_i, x_i) can recover message m if $\boldsymbol{f(x_i) = 1}$ **and** $\boldsymbol{lb_i \notin L}$

Revocable Predicate Encryption[KW19]



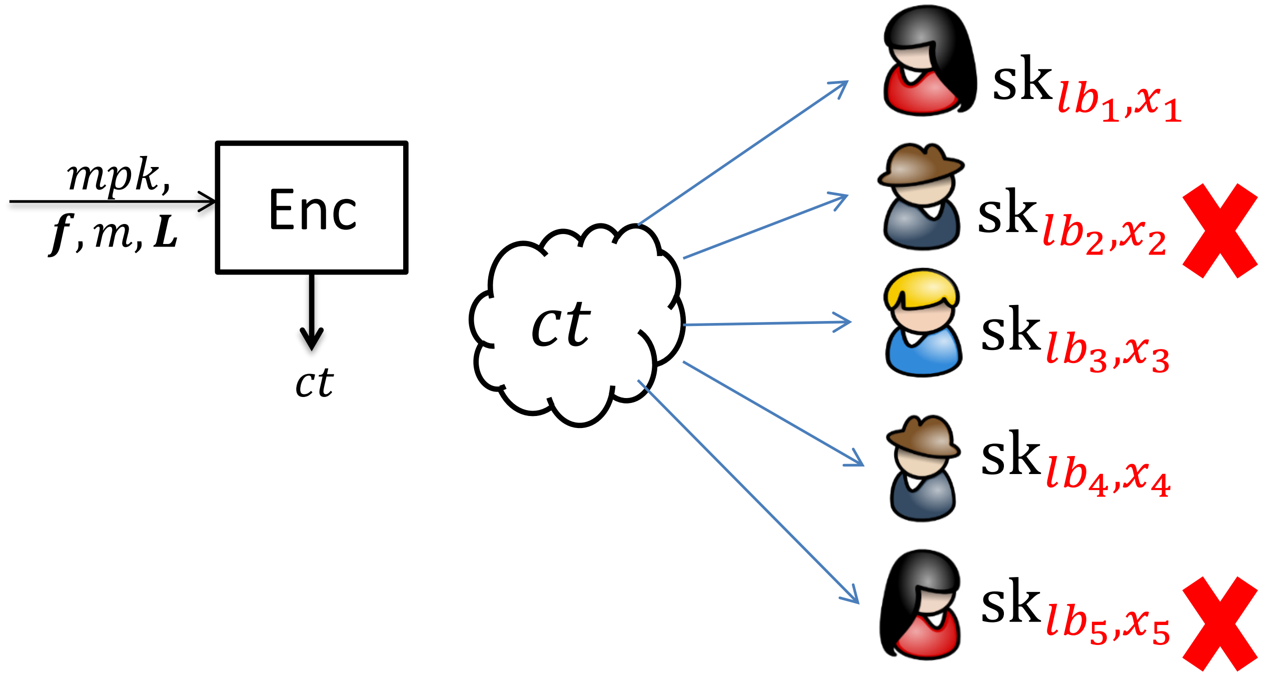
Revoked labels
L=$\{lb_2, lb_5\}$

Message Hiding Security

$\mathrm{Enc}(mpk, f, m_0, L) \approx \mathrm{Enc}(mpk, f, m_1, L)$; if for all key queries (lb, x)

$\boldsymbol{f(x) = 0}$ or $\boldsymbol{lb \in L}$

Revocable Predicate Encryption[KW19]



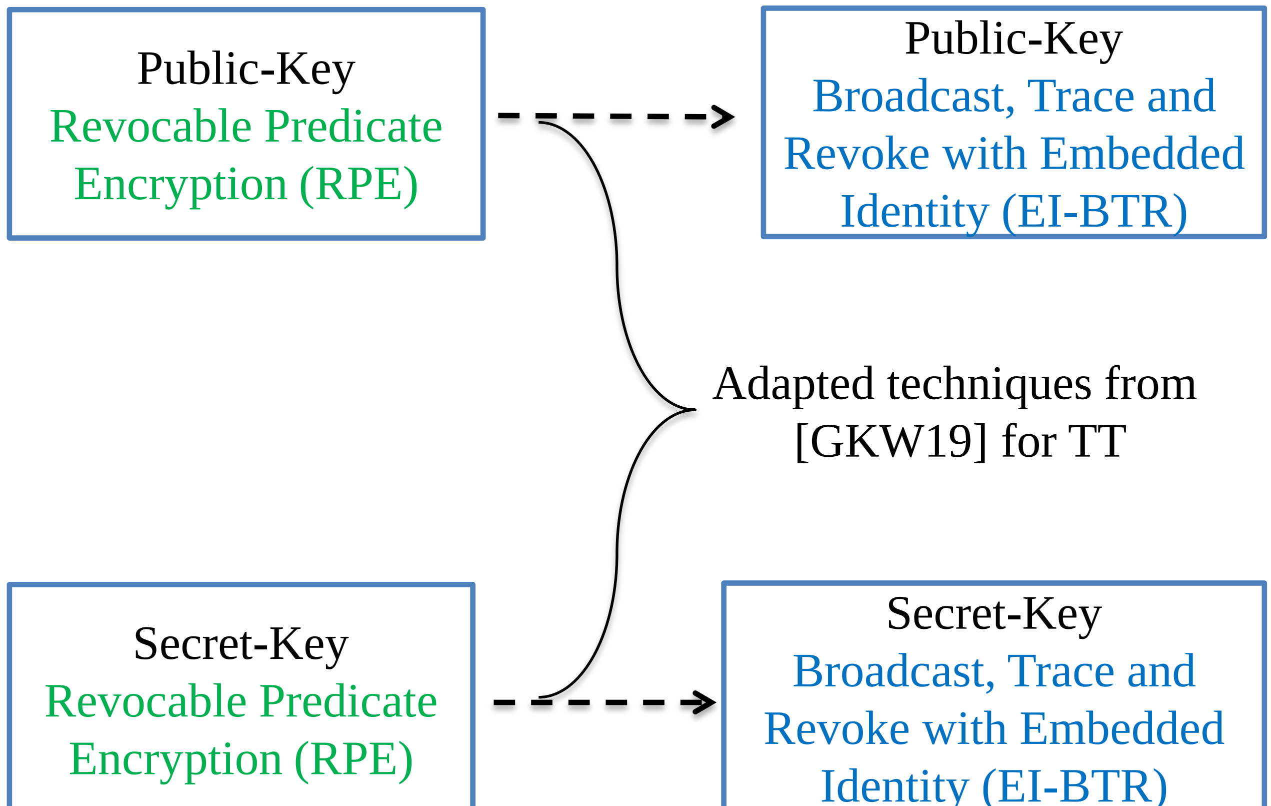
Revoked labels
L=$\{lb_2, lb_5\}$

Function Hiding Security

$$\mathrm{Enc}(mpk, f_0, m, L) \approx \mathrm{Enc}(mpk, f_1, m, L) \text{ ; if for all key queries } (lb, x)$$

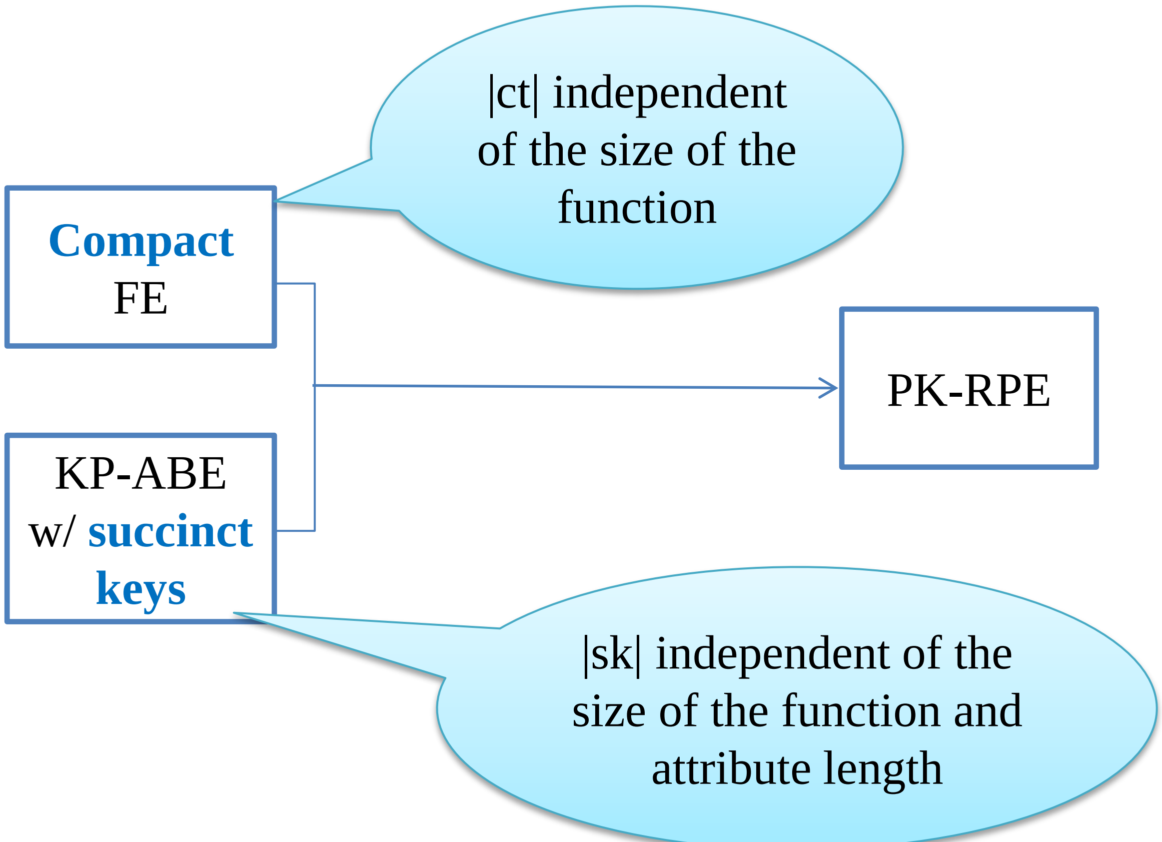
$$\boldsymbol{f_0(x) = f_1(x)} \text{ or } \boldsymbol{lb \in L}$$

Outline

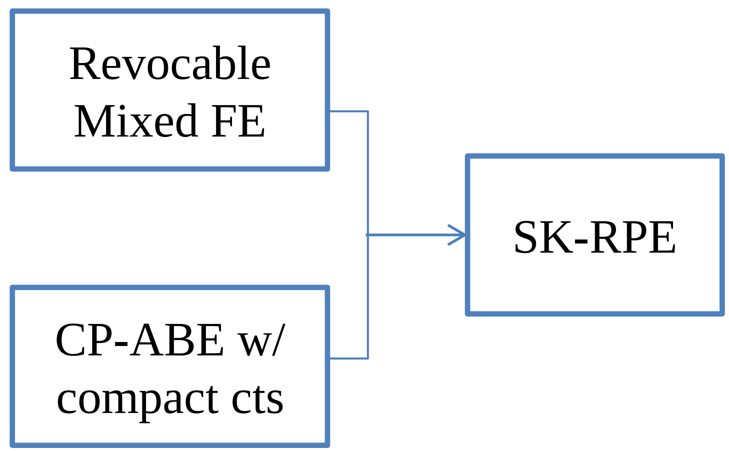

Public-Key
Revocable Predicate Encryption (RPE)
Public-Key
Broadcast, Trace and Revoke with Embedded Identity (EI-BTR)
Adapted techniques from [GKW19] for TT
Secret-Key
Revocable Predicate Encryption (RPE)
Secret-Key
Broadcast, Trace and Revoke with Embedded Identity (EI-BTR)

Public Key RPE : Outline

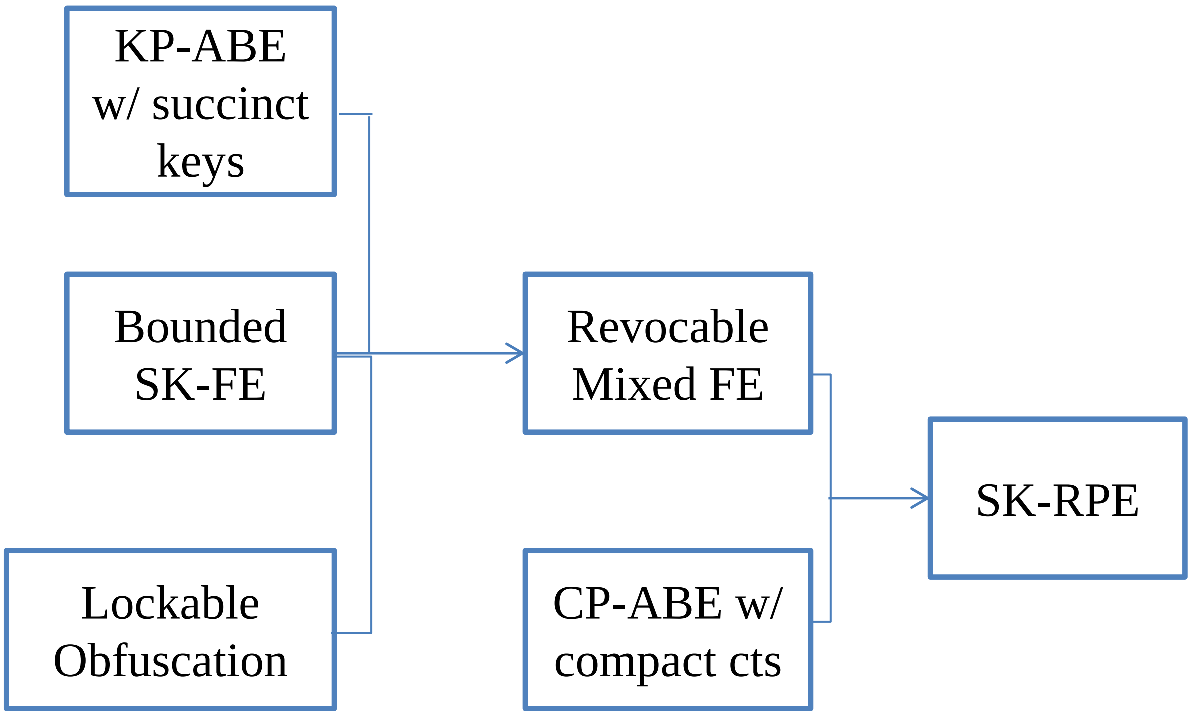
Public Key RPE : Optimal Parameters



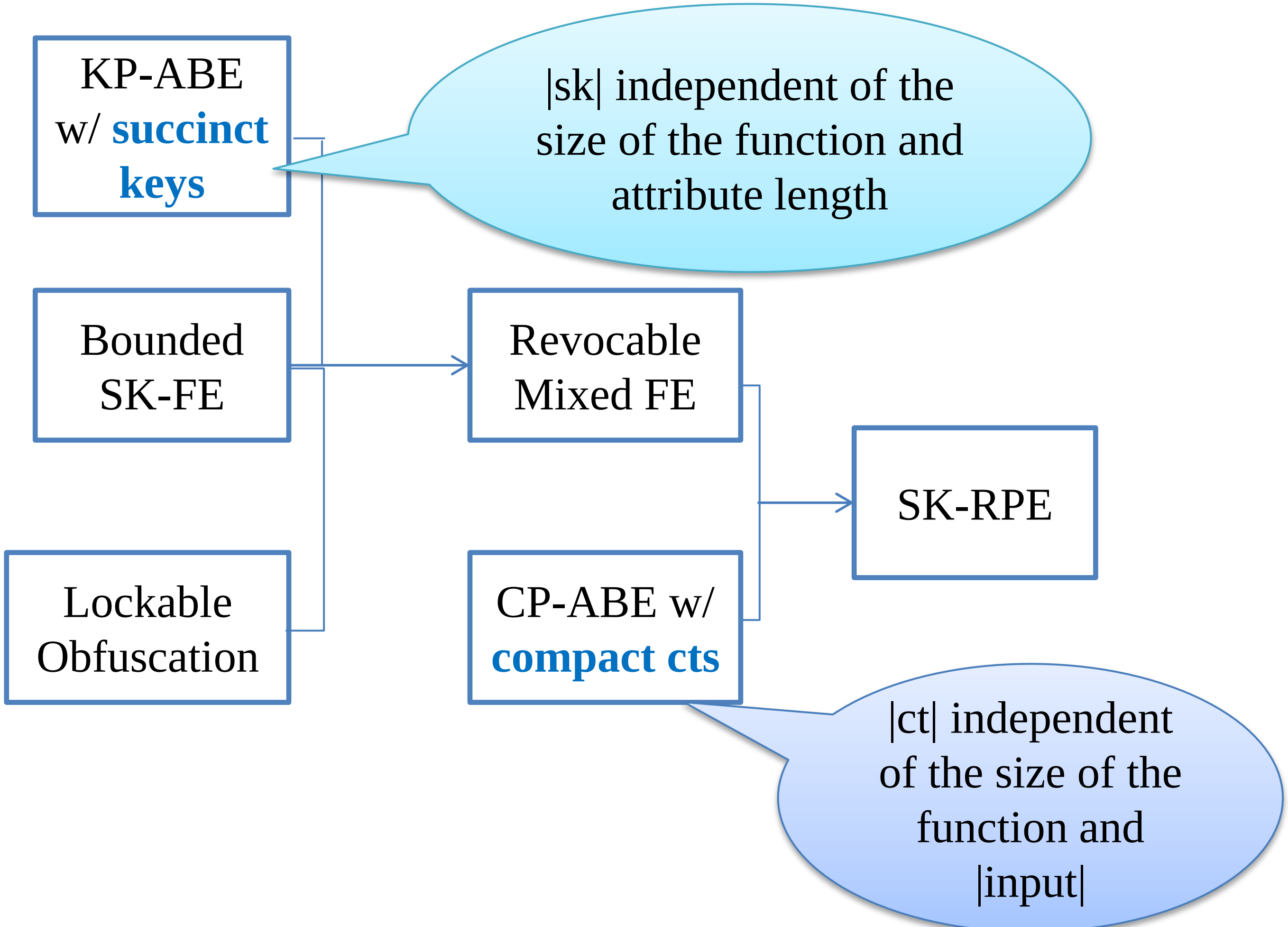
Secret Key RPE : Outline



Secret Key RPE : Outline



Secret Key RPE: Optimal Parameters



Summary

Unified framework for secret and public EI-BTR via RPE

Summary

Unified framework for secret and public EI-BTR via RPE

Public Traceability

- Optimal size of CT, PK, SK
- Embedded Identities
- Adaptive security
- Poly hard assumptions: FE, ABE

Open: Weaker version of FE to allow post quantum scheme?

Summary

Unified framework for secret and public EI-BTR via RPE

Public Traceability

- Optimal size of CT, PK, SK
- Embedded Identities
- Adaptive security
- Poly hard assumptions: FE, ABE

Open: Weaker version of FE to allow post quantum scheme?

Secret Traceability

- Optimal size of CT, PK, SK
- Embedded Identities
- Poly hard assumptions
  - ABEs instead of FE

Open: Adaptive Security? Remove reliance on evasive/tensor LWE?

Summary

Unified framework for secret and public EI-BTR via RPE

Public Traceability

- Optimal size of CT, PK, SK
- Embedded Identities
- Adaptive security
- Poly hard assumptions: FE, ABE

Open: Weaker version of FE to allow post quantum scheme?

Secret Traceability

- Optimal size of CT, PK, SK
- Embedded Identities
- Poly hard assumptions
  - ABEs instead of FE

Open: Adaptive Security? Remove reliance on evasive/tensor LWE?

First work to support superpoly revocation list size!
(with efficient representation & membership testing)

Thank you!