Compact Selective Opening Security From LWE

Dennis Hofheinz, Kristina Hostáková, Julia Kastner, Karen Klein

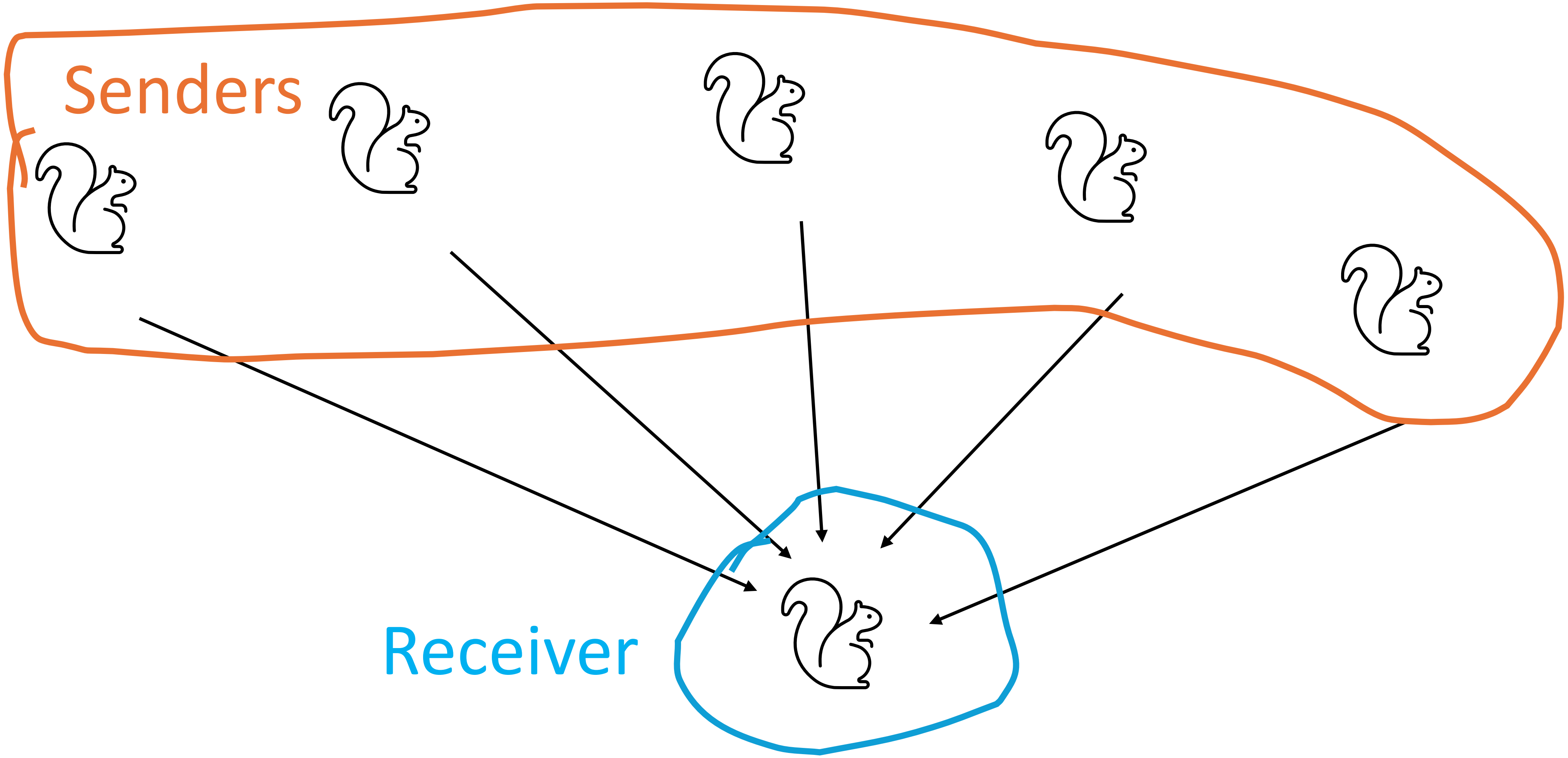
Department of Computer Science, ETH Zurich, Zurich, Switzerland

{hofheinz,kristina.hostakova,julia.kastner,karen.klein}@inf.ethz.ch

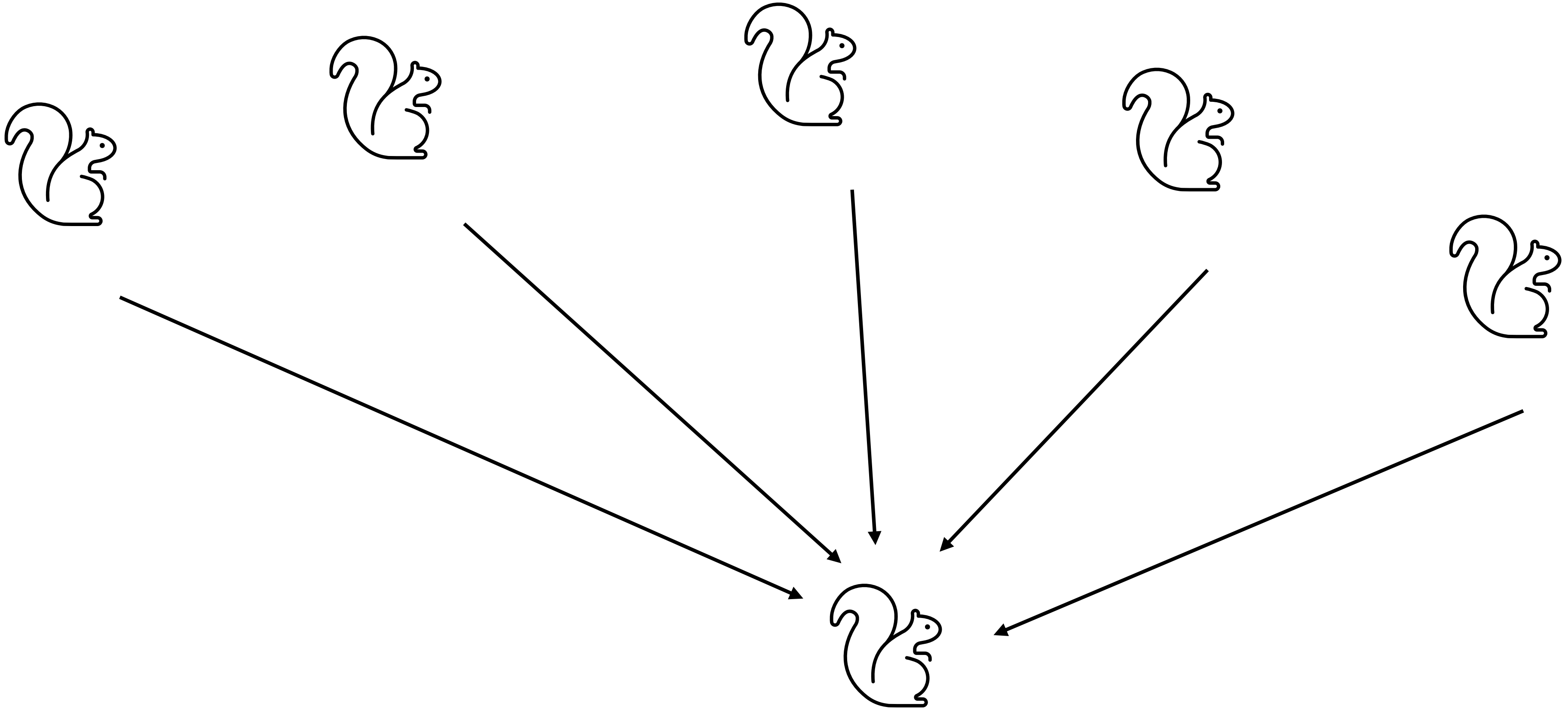
Akin Ünal, ISTA, Klosterneuburg, Austria

akin.uenal@ist.ac.at

IND-Selective Opening-CPA Security [BHY09]

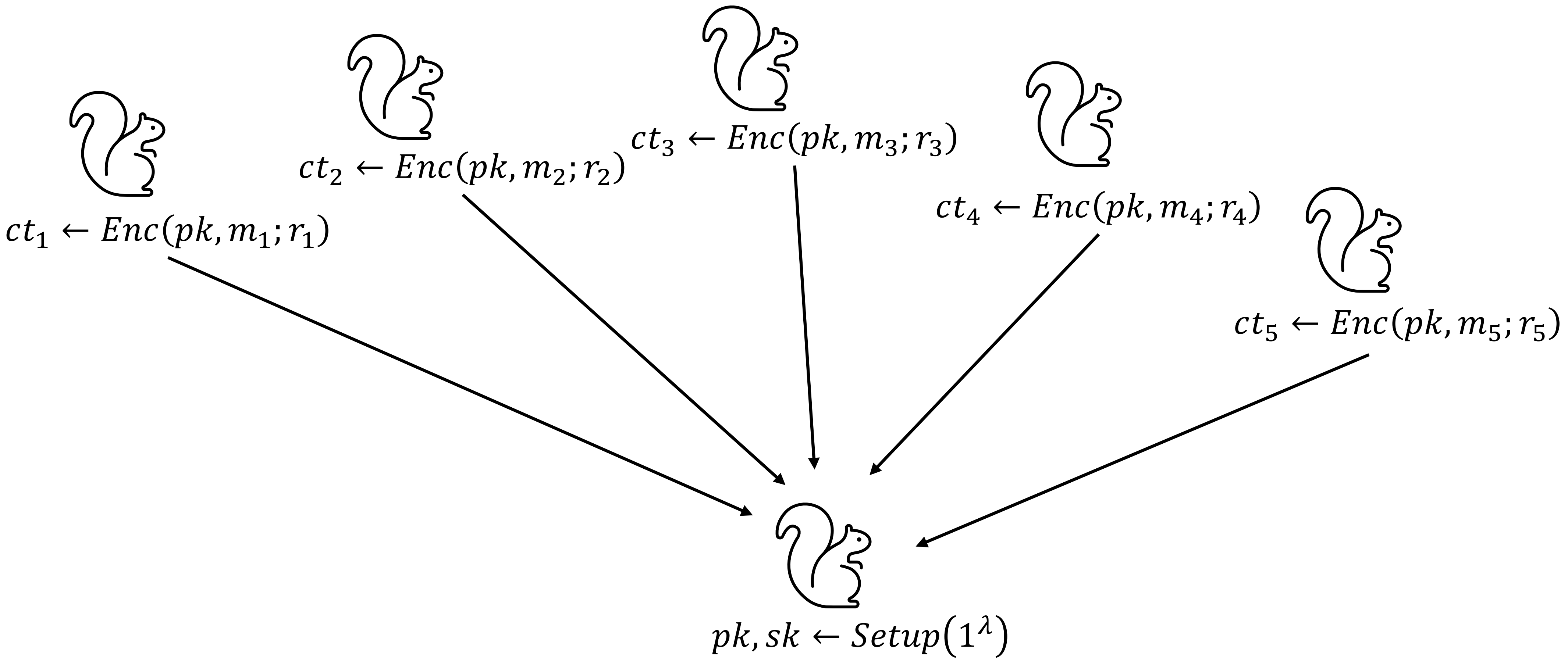


IND-Selective Opening-CPA Security [BHY09]

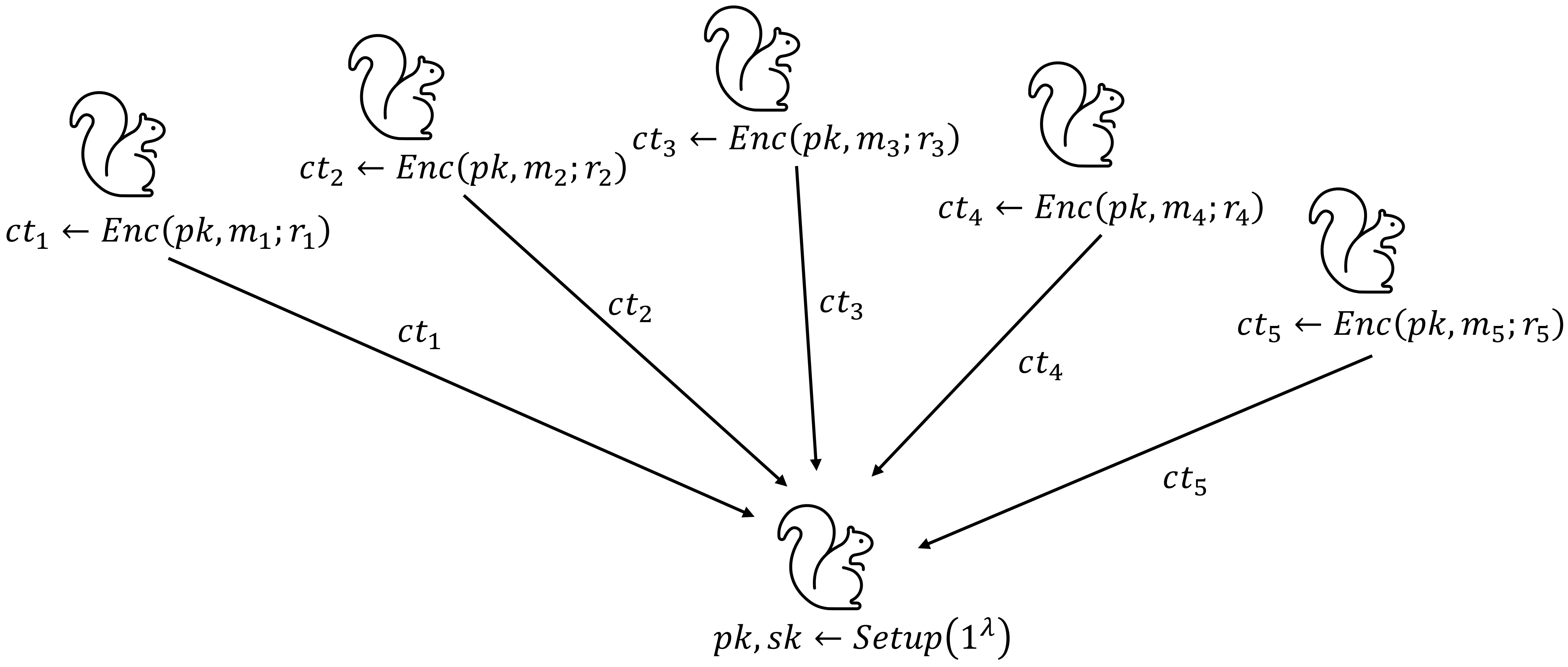


$pk, sk \leftarrow Setup(1^\lambda)$

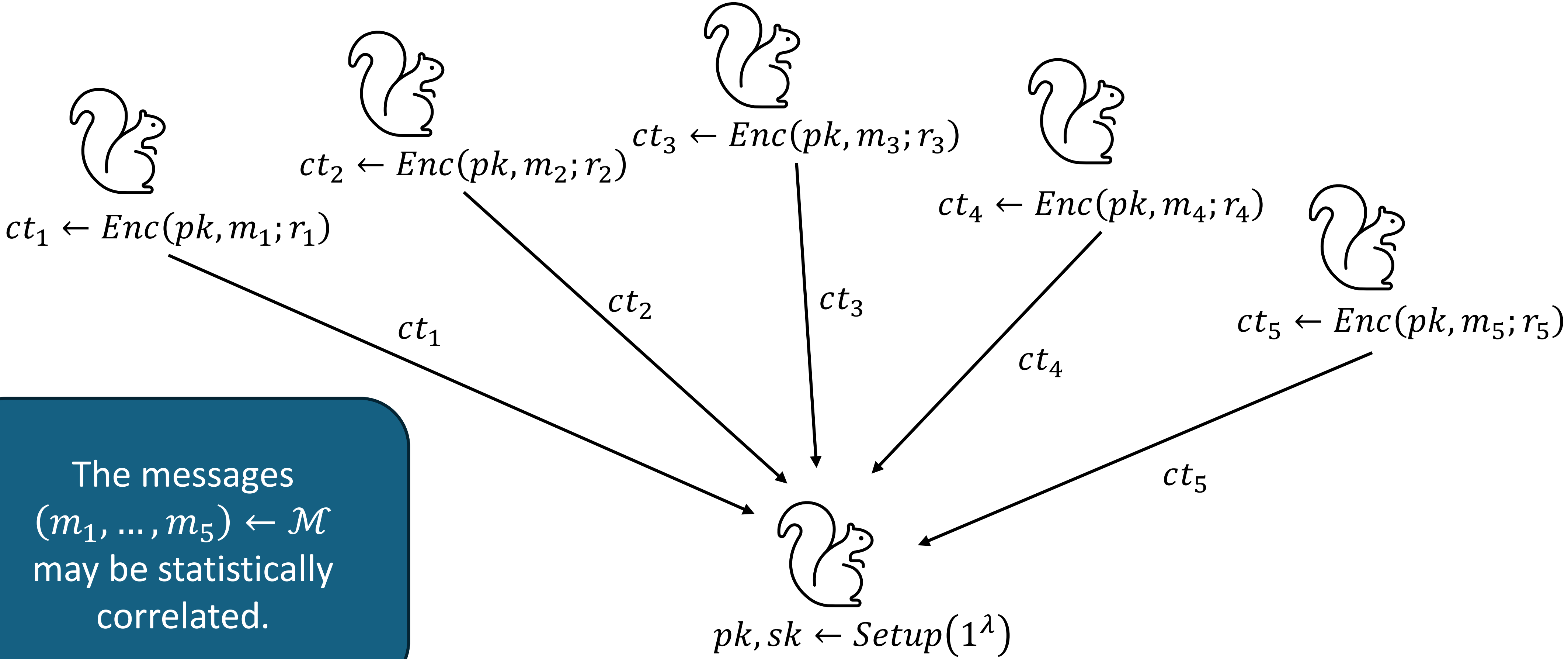
IND-Selective Opening-CPA Security [BHY09]



IND-Selective Opening-CPA Security [BHY09]

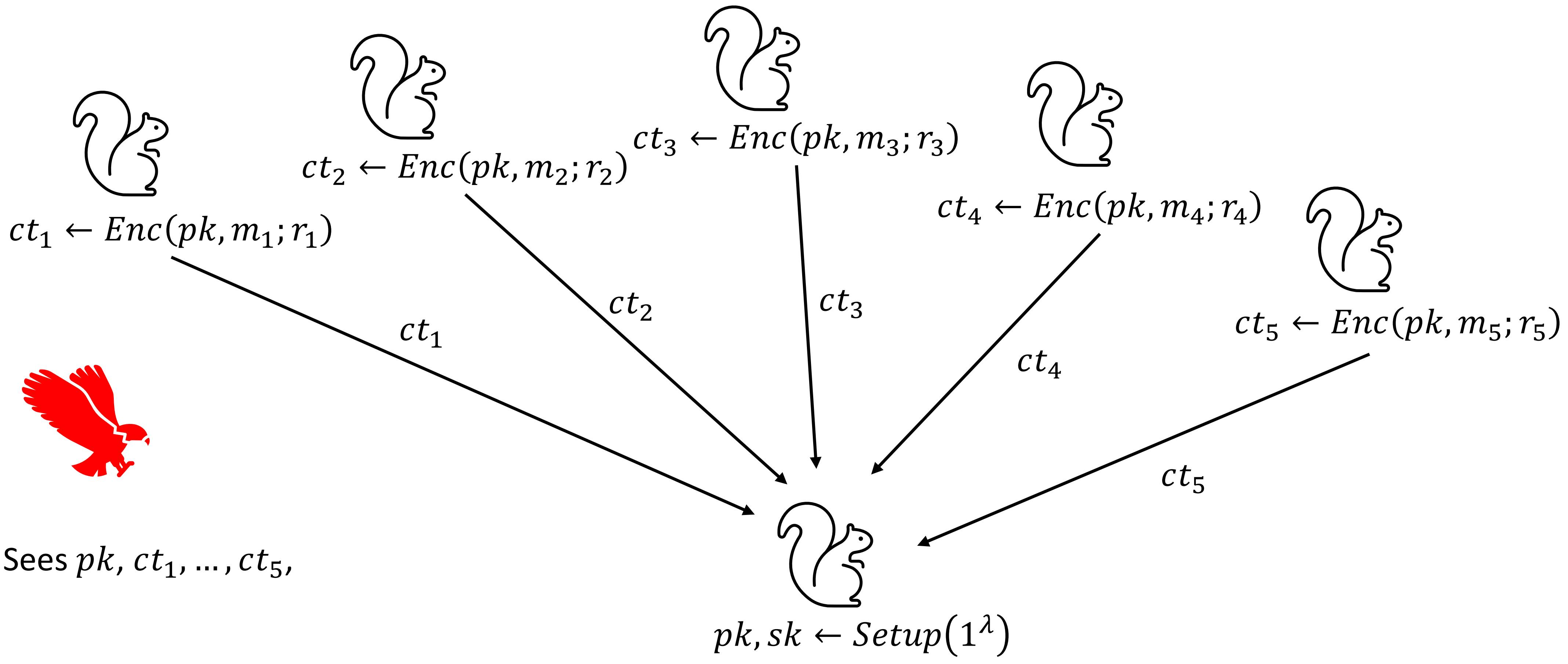


IND-Selective Opening-CPA Security [BHY09]

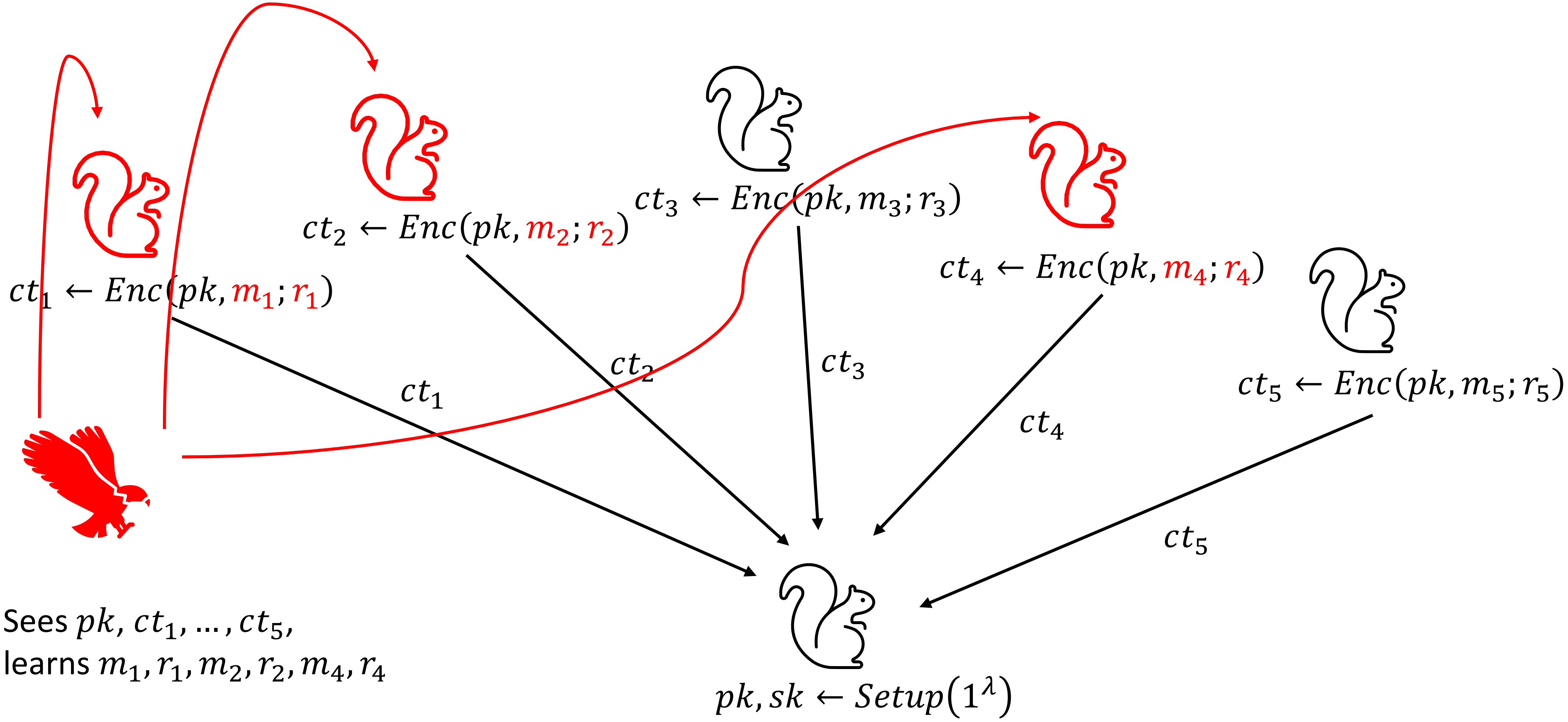


The messages $(m_1, \ldots, m_5) \leftarrow \mathcal{M}$ may be statistically correlated.

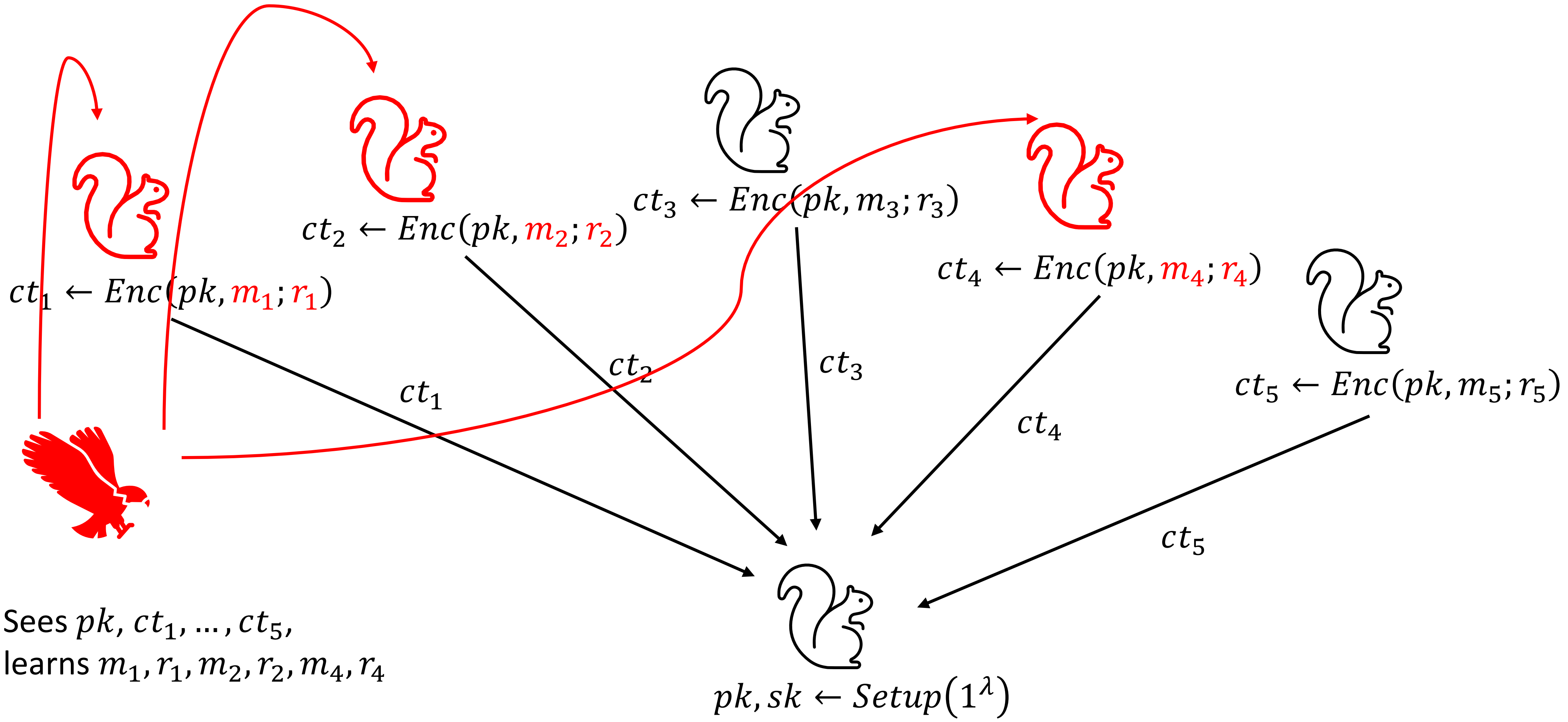
IND-Selective Opening-CPA Security [BHY09]



IND-Selective Opening-CPA Security [BHY09]

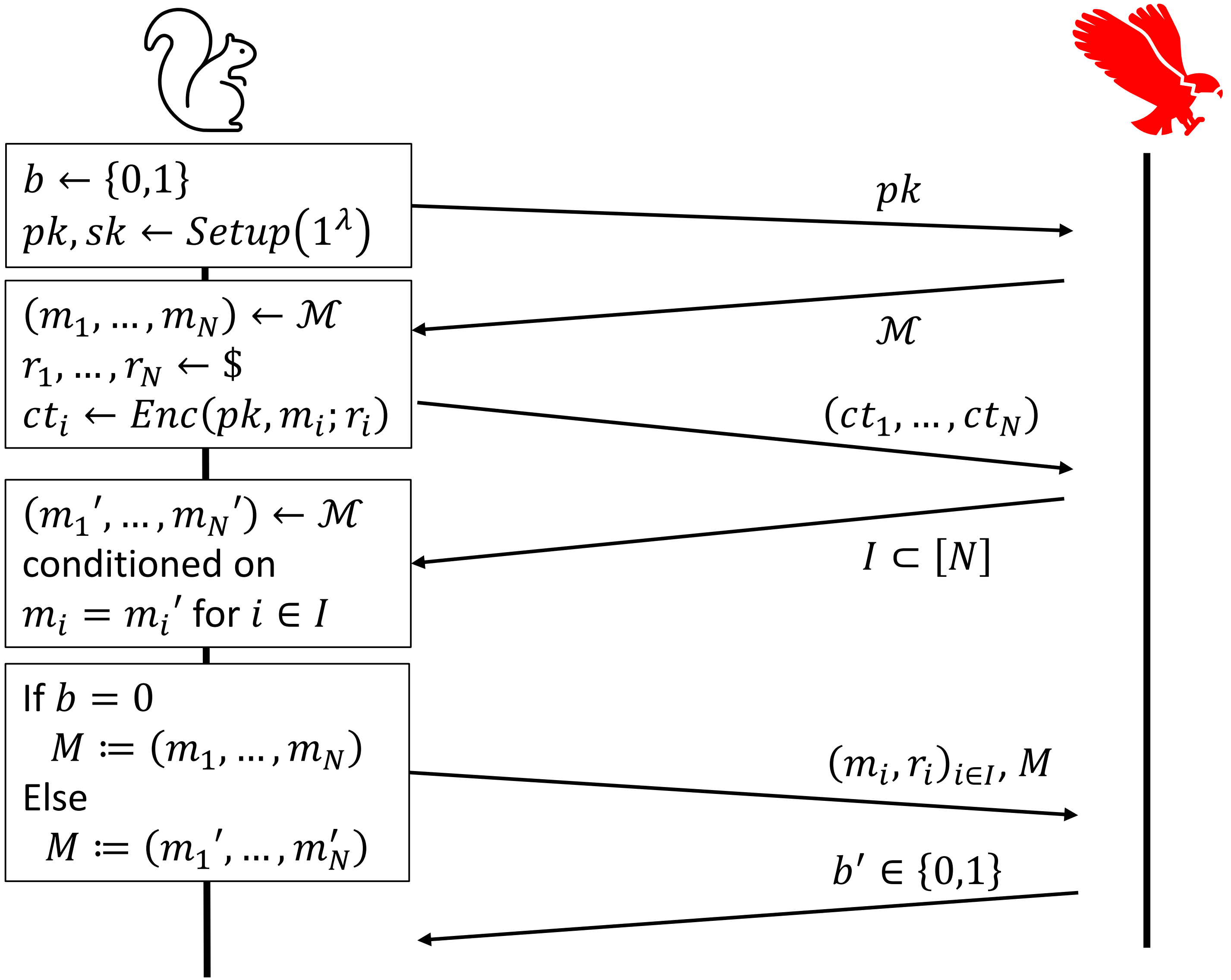


IND-Selective Opening-CPA Security [BHY09]

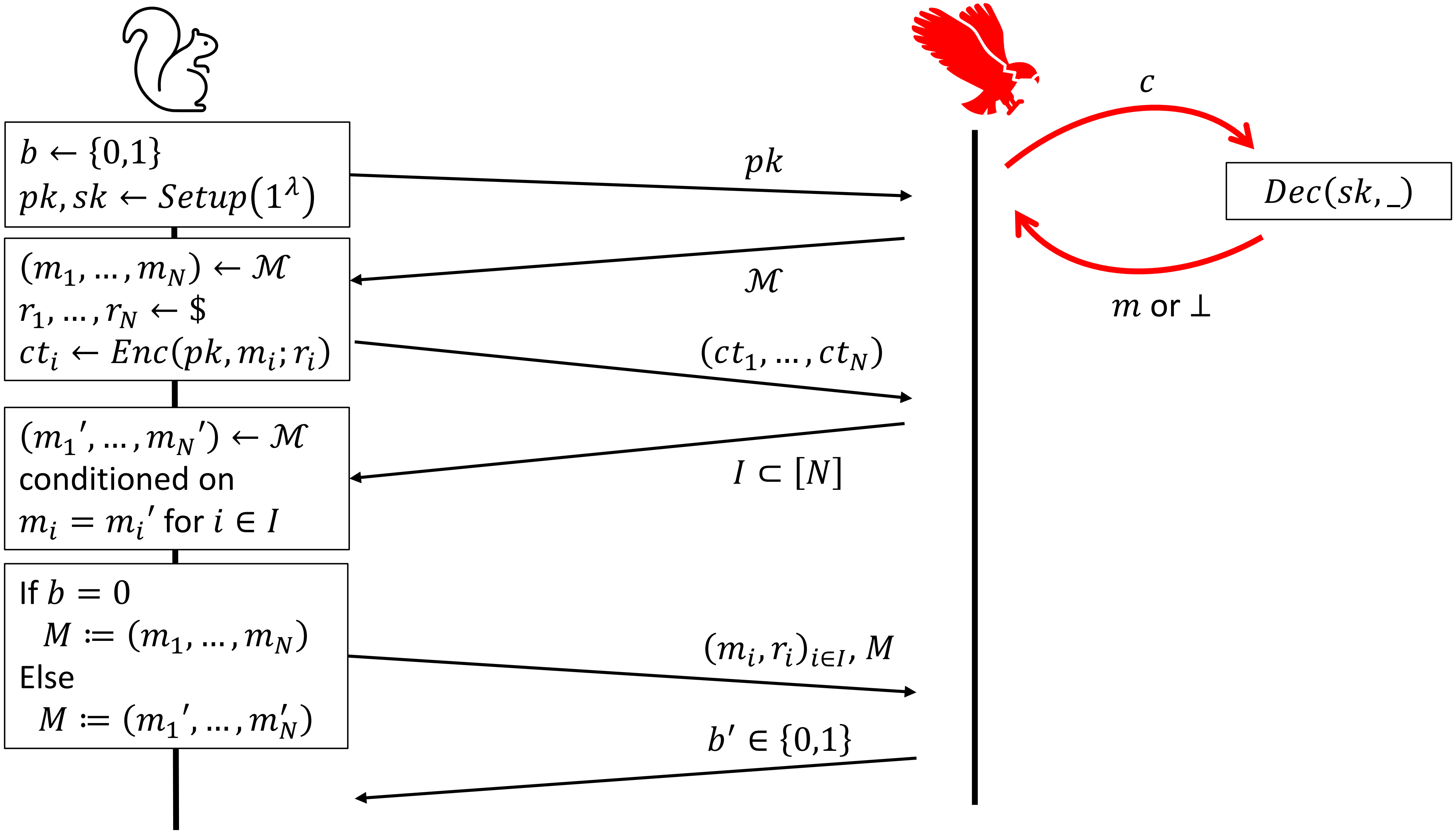


Security guarantee: Adversary does not learn any more about m_3, m_5 than what m_1, m_2, m_4 do trivially tell it.

IND-Selective Opening-CPA Security



IND-Selective Opening-CCA Security



IND-Selective Opening-CCA Security

- Not implied by IND-CCA security (counterexamples [BDWY12, HR14, HRW16])

.

IND-Selective Opening-CCA Security

- Not implied by IND-CCA security (counterexamples [BDWY12, HR14, HRW16])
- „Post-Quantum“ IND-so-CCA PKE does already exist from LWE [LSSS17,BL17]
  - But these constructions are not *compact* ☹

.

IND-Selective Opening-CCA Security

- Not implied by IND-CCA security (counterexamples [BDWY12, HR14, HRW16])
- „Post-Quantum“ IND-so-CCA PKE does already exist from LWE [LSSS17,BL17]
  - But these constructions are not *compact* ☹
- C*ompact* IND-so-CCA PKE do exist [Hof12]
  - But from non-quantum-resistant assumptions (Paillier-like)

.

IND-Selective Opening-CCA Security

- Not implied by IND-CCA security (counterexamples [BDWY12, HR14, HRW16])
- „Post-Quantum“ IND-so-CCA PKE does already exist from LWE [LSSS17,BL17]
  - But these constructions are not *compact* ☹
- C*ompact* IND-so-CCA PKE do exist [Hof12]
  - But from non-quantum-resistant assumptions (Paillier-like)

Our Result:

The first *compact* IND-so-CCA secure PKE scheme from LWE (and PRFs in **NC**1).

IND-Selective Opening-CCA Security

- Not implied by IND-CCA security (counterexamples [BDWY12, HR14, HRW16])
- „Post-Quantum“ IND-so-CCA PKE does already exist from LWE [LSSS17,BL17]
  - But these constructions are not *compact* ☹
- C*ompact* IND-so-CCA PKE do exist [Hof12]
  - But from non-quantum-resistant assumptions (Paillier-like)

Our Result:

The first *compact* IND-so-CCA secure PKE scheme from LWE (and PRFs in **NC**1).

Our Technique:

Use dual GSW FHE [GSW13] and a compression trick for messages.

Construction of IND-so-CCA PKE [Hof12]

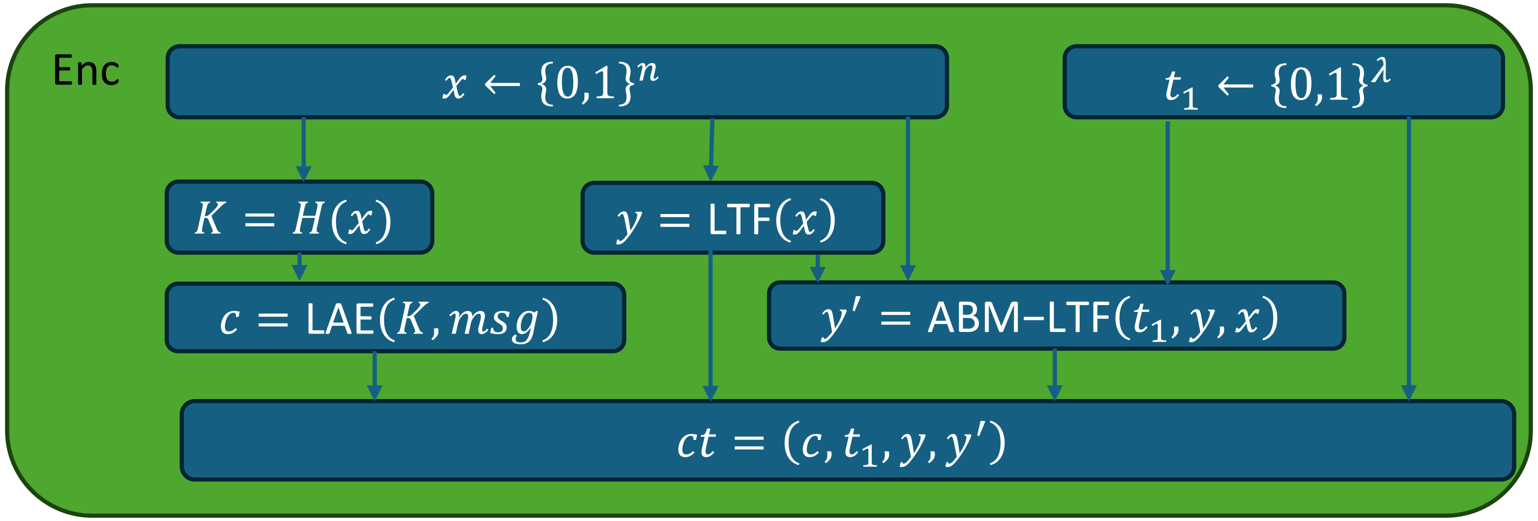
In the standard model:

- A lossy trapdoor function LTF
- An all-but-many lossy trapdoor function ABM-LTF
- A universal family of hash functions H
- A (one-time) statistically secure lossy authenticated encryption scheme LAE

Construction of IND-so-CCA PKE [Hof12]

In the standard model:

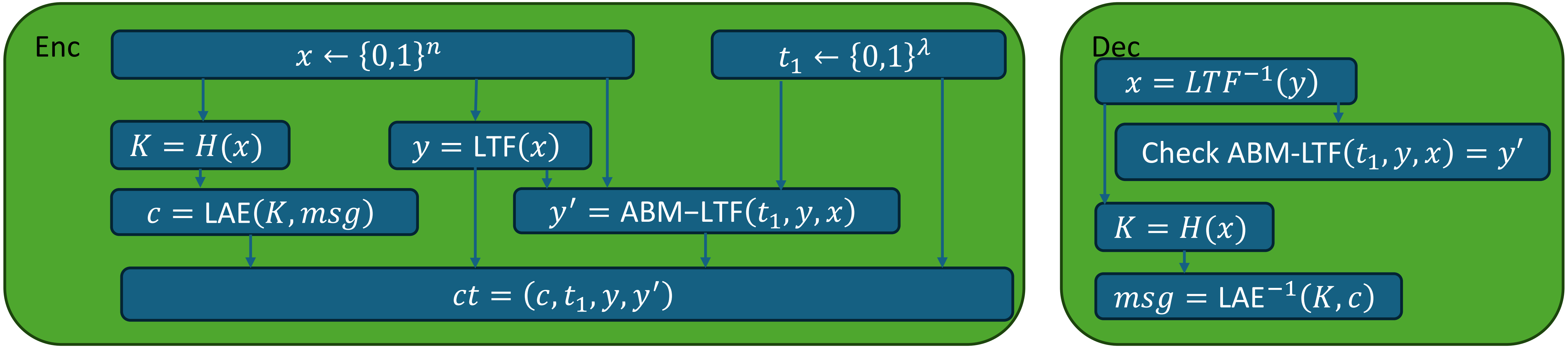
- A lossy trapdoor function LTF
- An all-but-many lossy trapdoor function ABM-LTF
- A universal family of hash functions H
- A (one-time) statistically secure lossy authenticated encryption scheme LAE



Construction of IND-so-CCA PKE [Hof12]

In the standard model:

- A lossy trapdoor function LTF
- An all-but-many lossy trapdoor function ABM-LTF
- A universal family of hash functions H
- A (one-time) statistically secure lossy authenticated encryption scheme LAE

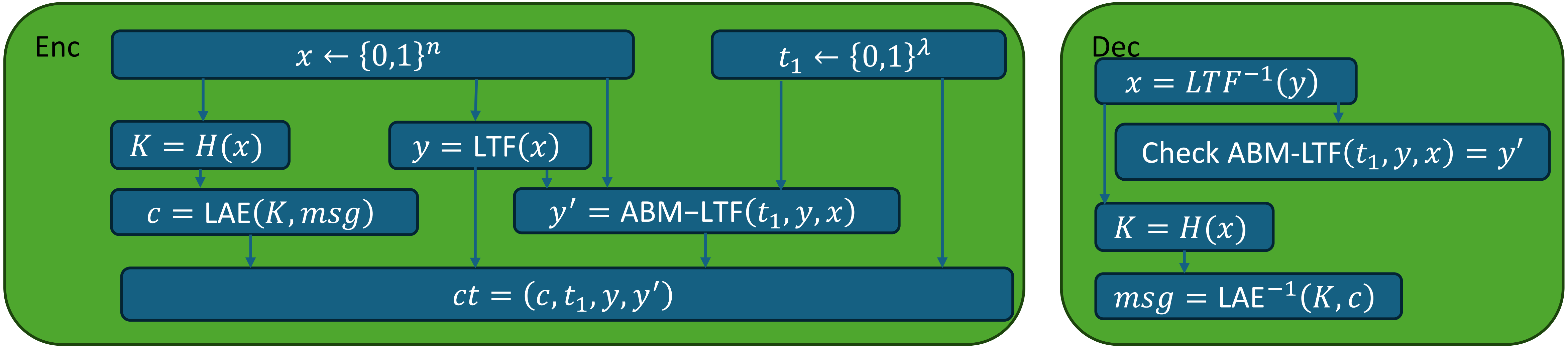


Construction of IND-so-CCA PKE [Hof12]

In the standard model:

- A lossy trapdoor function LTF
- An all-but-many lossy trapdoor function ABM-LTF
- A universal family of hash functions H
- A (one-time) statistically secure lossy authenticated encryption scheme LAE

Exist unconditionally. Even compact.



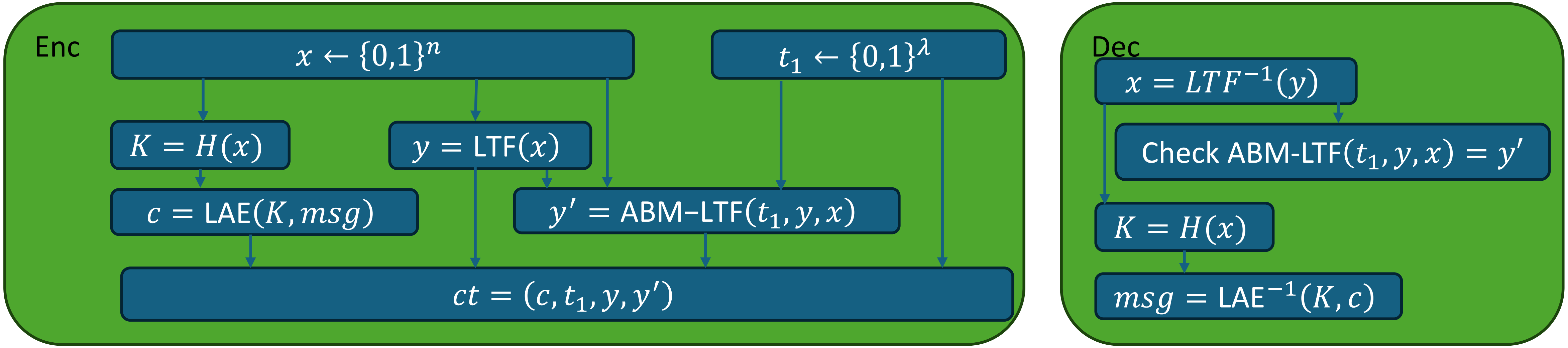
Construction of IND-so-CCA PKE [Hof12]

Build compactly from LWE (+PRFs).

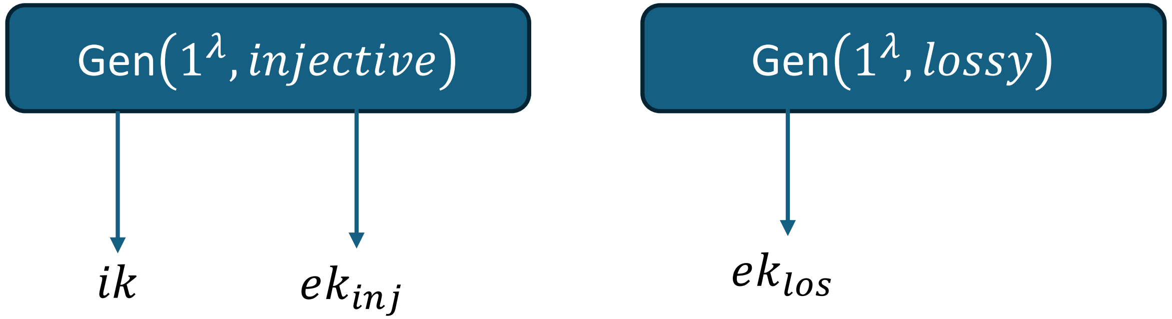
In the standard model:

- A lossy trapdoor function LTF
- An all-but-many lossy trapdoor function ABM-LTF
- A universal family of hash functions H
- A (one-time) statistically secure lossy authenticated encryption scheme LAE

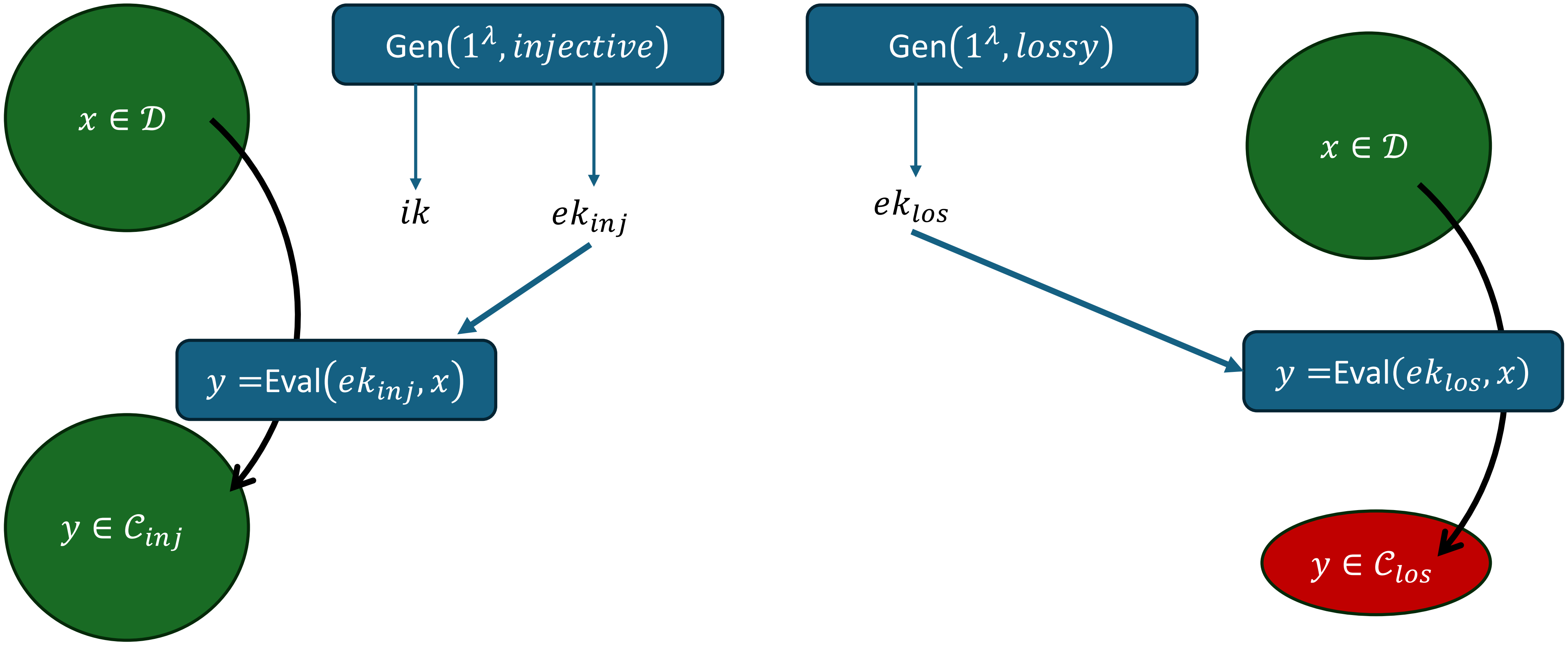
Exist unconditionally. Even compact.



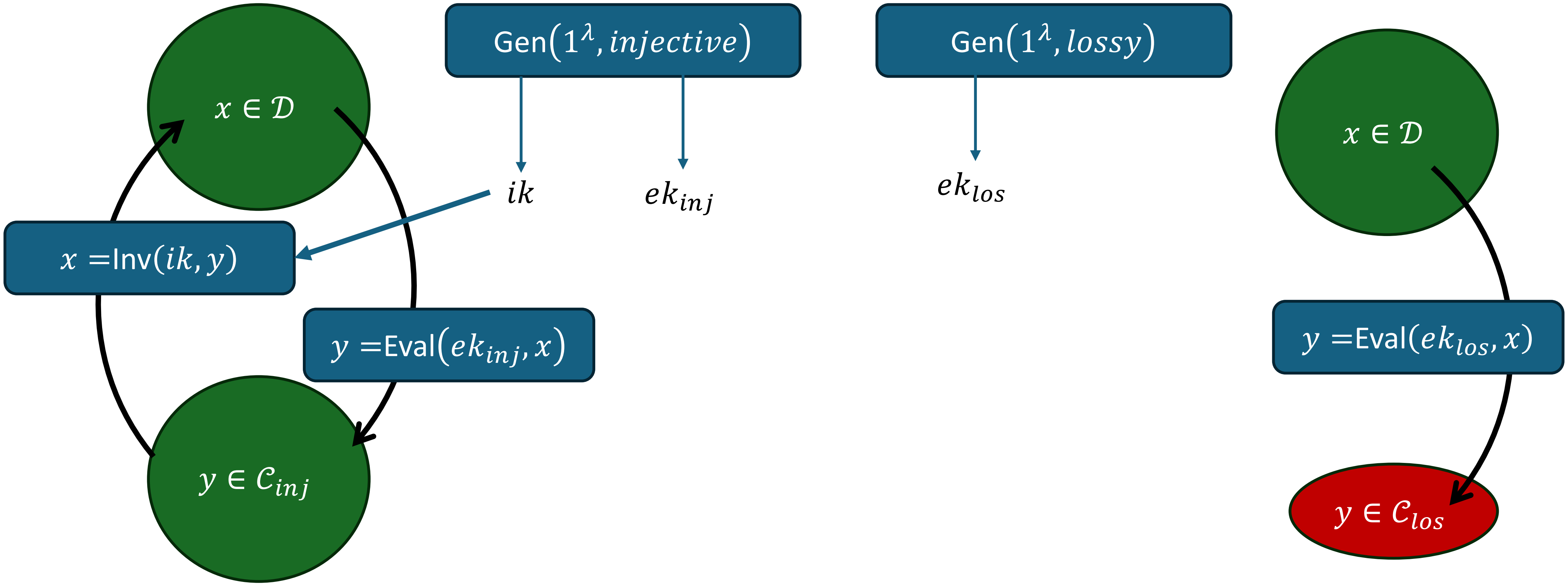
Compact Lossy Trapdoor Functions



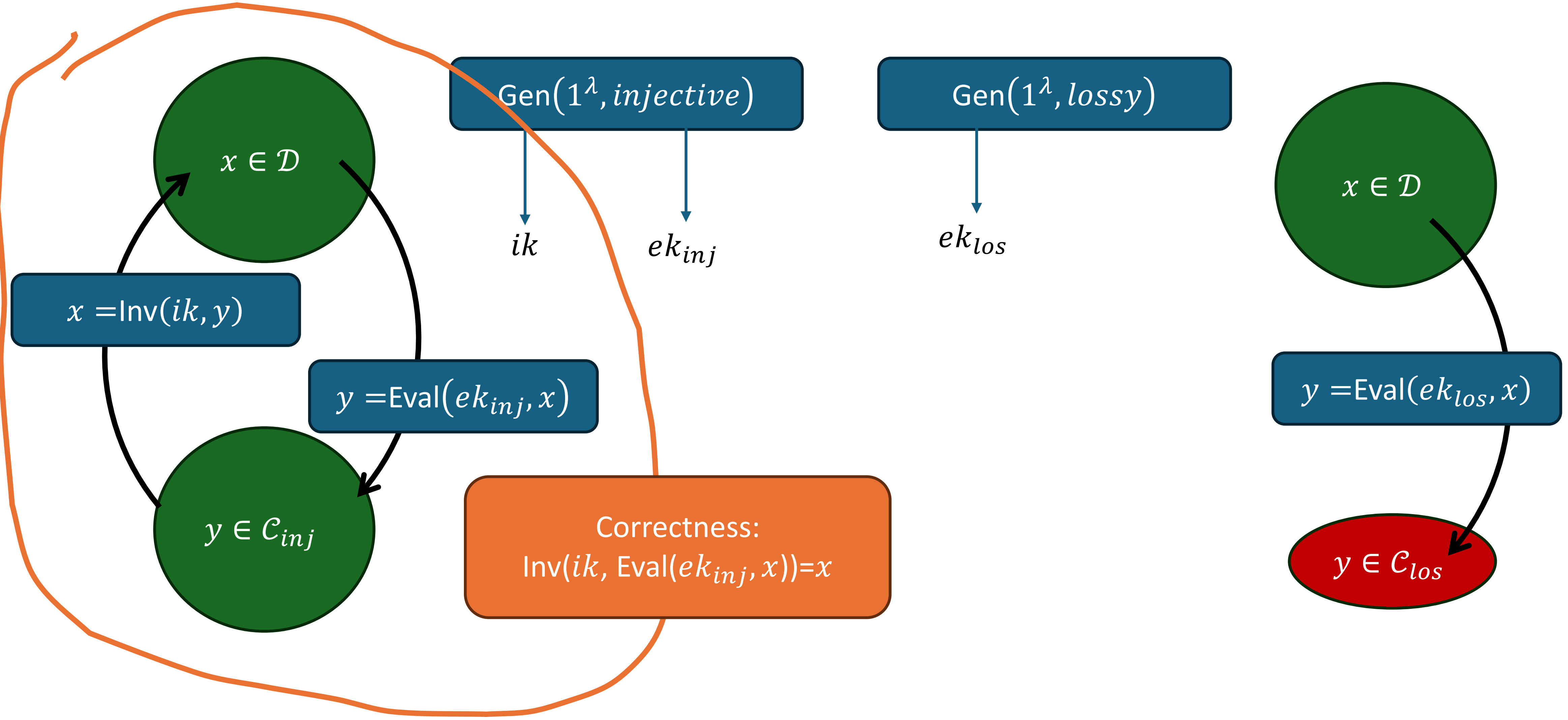
Compact Lossy Trapdoor Functions



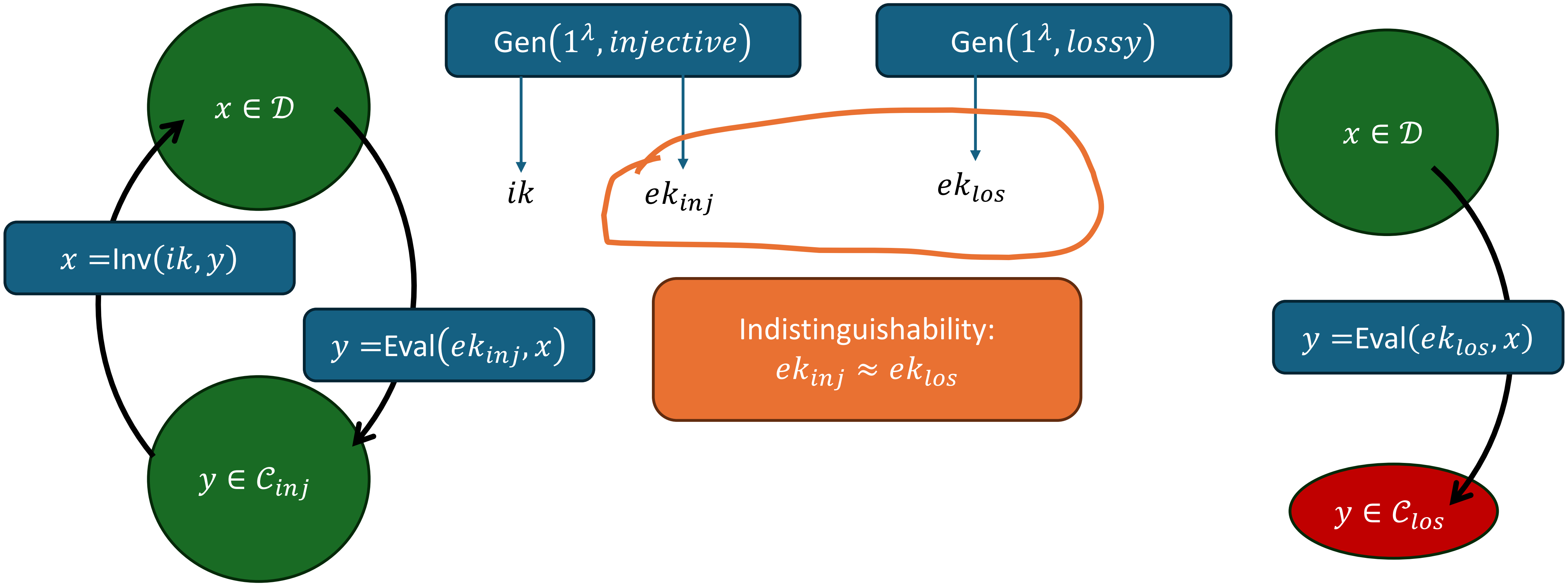
Compact Lossy Trapdoor Functions



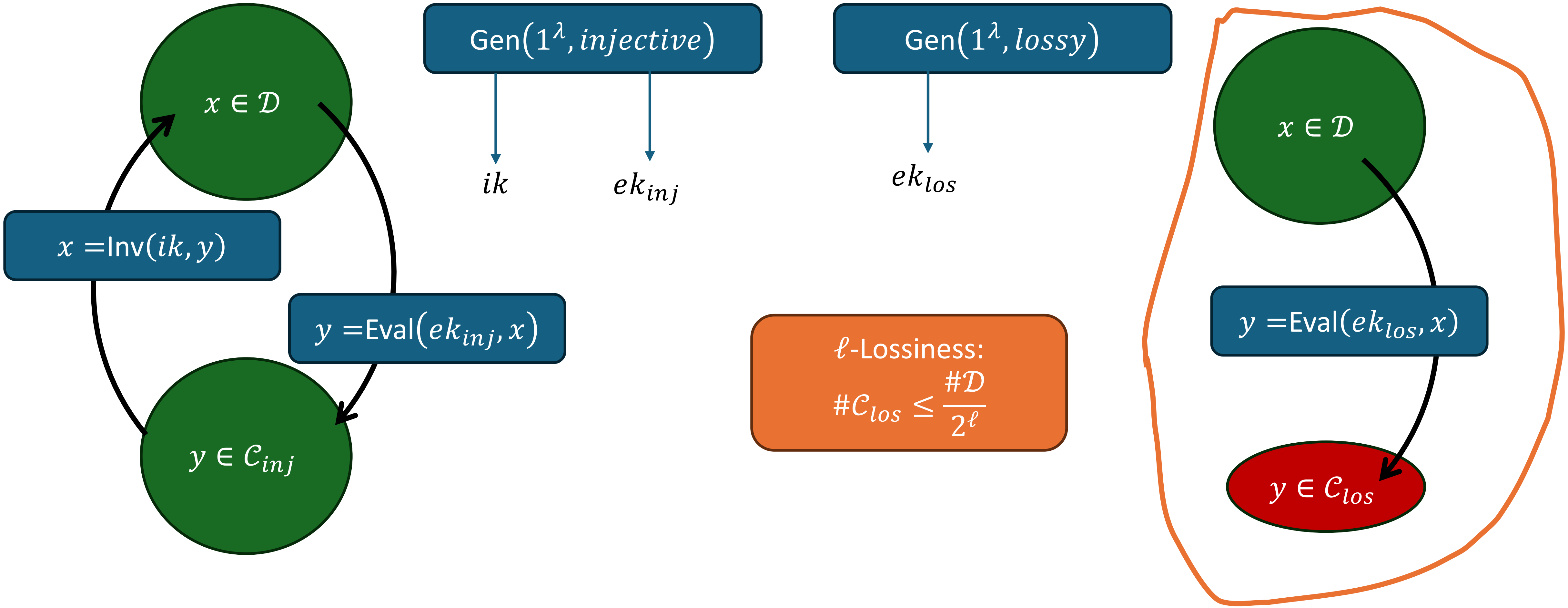
Compact Lossy Trapdoor Functions



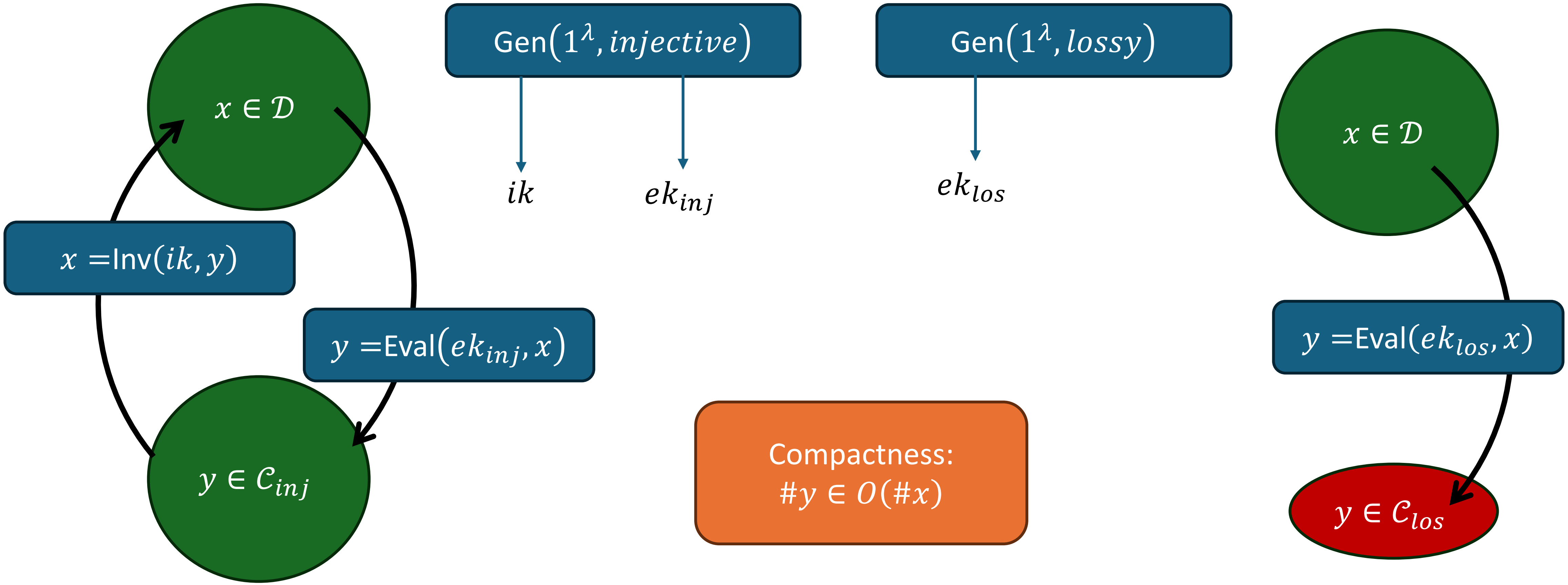
Compact Lossy Trapdoor Functions



Compact Lossy Trapdoor Functions



Compact Lossy Trapdoor Functions



A Compact LTF from LWE

Generating Keys:

Draw an MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S} \leftarrow \mathbb{Z}_q^{n \times N}, \mathbf{E} \leftarrow \chi^{(m+u) \times N}$.

Output $ek \coloneqq \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$
and $ik \coloneqq (A, B, td)$ (if injective mode).

A Compact LTF from LWE

Generating Keys:

Draw an MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S} \leftarrow \mathbb{Z}_q^{n \times N}, \mathbf{E} \leftarrow \chi^{(m+u) \times N}$.

Output $ek \coloneqq \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$
and $ik \coloneqq (A, B, td)$ (if injective mode).

$$\mathbf{G} = \begin{pmatrix} 1\ 2\ 4\ \ldots\ 2^{\log q} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & 1\ 2\ 4\ \ldots\ 2^{\log q} \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

Draw an MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S} \leftarrow \mathbb{Z}_q^{n \times N}, \mathbf{E} \leftarrow \chi^{(m+u) \times N}$.

Output $ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$
and $ik := (A, B, td)$ (if injective mode).

Injective Mode: $b = 1$
Lossy Mode: $b = 0$

$$\mathbf{G} = \begin{pmatrix} 1\ 2\ 4\ \ldots\ 2^{\log q} & \cdots & \\ \vdots & \ddots & \vdots \\ & \cdots & 1\ 2\ 4\ \ldots\ 2^{\log q} \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

$$ek \coloneqq \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y \coloneqq ek \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Inverting y:

A Compact LTF from LWE

$$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}$$

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Inverting y:

$$y = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S} \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix} \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Let's call this g.

Inverting y:

$$y = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Let‘s call this g.

Inverting y:

$$y = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{AS}g + \mathbf{E}_1 g \\ \mathbf{BS}g + \mathbf{E}_2 g + \frac{q}{p} \cdot x \end{pmatrix}$$

A Compact LTF from LWE

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Let's call this g.

Inverting y:

$$y = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S} \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix} \cdot \mathbf{G}^{-1} \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{AS}g + \mathbf{E}_1 g \\ \mathbf{BS}g + \mathbf{E}_2 g + \frac{q}{p} \cdot x \end{pmatrix}$$

Use MP12 trapdoor td to extract Sg.

A Compact LTF from LWE

Generating Keys:

$$ek := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$$

$\mathbf{E} = \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix}$

Evaluating $x \in \mathbb{Z}_p^{m'}$:

$$y := ek \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

Let's call this g.

Inverting y:

$$y = \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} \mathbf{E}_1 \\ \mathbf{E}_2 \end{pmatrix} \cdot \mathbf{G}^{-1}\begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix} + \begin{pmatrix} 0 \\ \frac{q}{p} \cdot x \end{pmatrix}$$

$$= \begin{pmatrix} \mathbf{AS}g + \mathbf{E}_1 g \\ \mathbf{BS}g + \mathbf{E}_2 g + \frac{q}{p} \cdot x \end{pmatrix}$$

Use MP12 trapdoor td to extract Sg.

Use Sg to extract $\frac{q}{p} \cdot x$.

A Compact LTF from LWE

- Correctness: ✓

A Compact LTF from LWE

- Correctness: ✓
- Indistinguishability: $\binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + \mathbf{G} \approx \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E}$.

A Compact LTF from LWE

- Correctness: ✓
- Indistinguishability: $\begin{pmatrix}\mathbf{A}\\\mathbf{B}\end{pmatrix} \cdot \mathbf{S} + \mathbf{E} + \mathbf{G} \approx \begin{pmatrix}\mathbf{A}\\\mathbf{B}\end{pmatrix} \cdot \mathbf{S} + \mathbf{E}$.
- ℓ-Lossiness: Counting argument.

A Compact LTF from LWE

- Correctness: ✓
- Indistinguishability: $\begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix} \cdot \mathbf{S} + \mathbf{E} + \mathbf{G} \approx \begin{pmatrix}\mathbf{A}\\ \mathbf{B}\end{pmatrix} \cdot \mathbf{S} + \mathbf{E}.$
- ℓ-Lossiness: Counting argument.

Low Rank

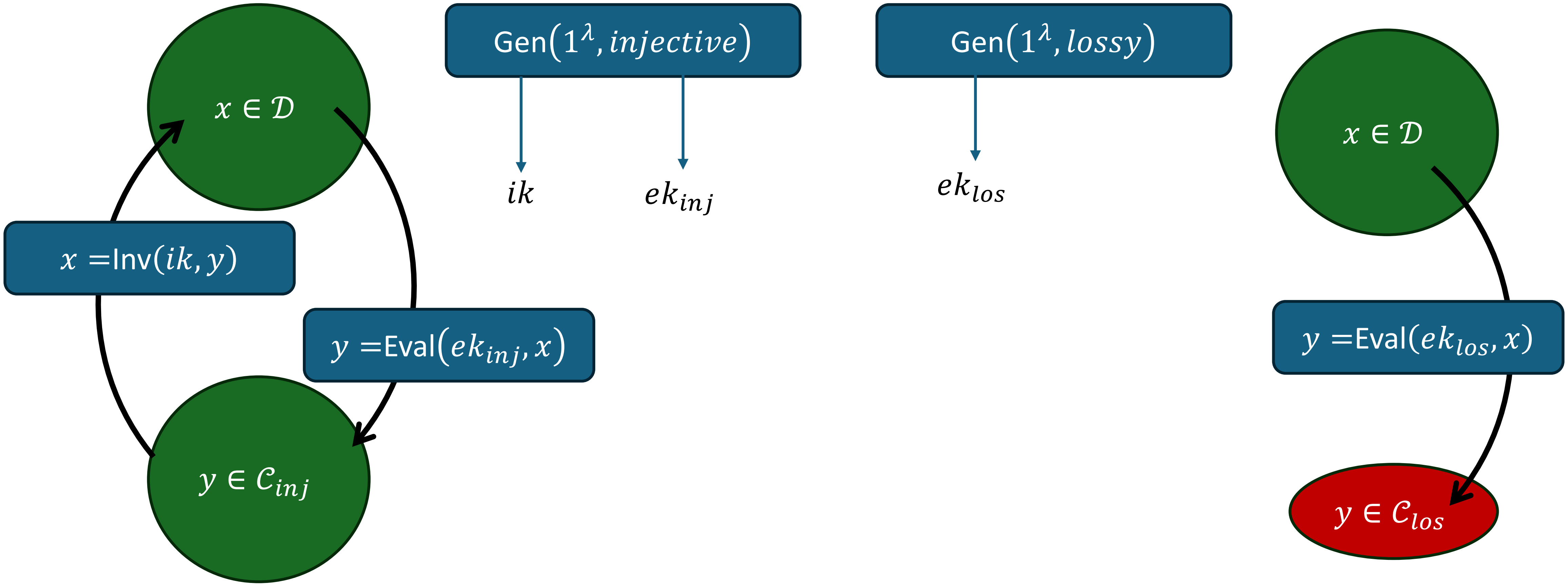
Short Entries

A Compact LTF from LWE

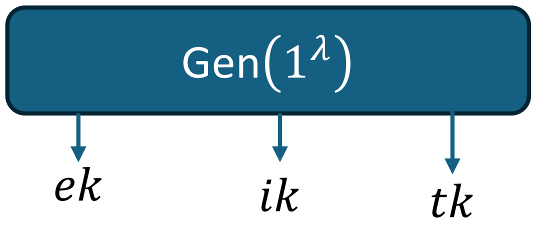
- Correctness: ✓
- Indistinguishability: $\binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + \mathbf{G} \approx \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E}$.
- ℓ-Lossiness: Counting argument.
- Compactness:

  Messages lie in $\mathbb{Z}_p^{m'}$.
  Ciphertexts lie in $\mathbb{Z}_q^{m+u}$.
  Choose $\log p \in \Omega(\log q)$ and $m' \in \Omega(m+u)$.

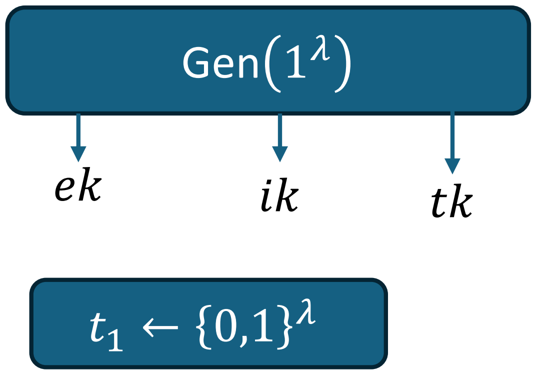
Lossy Trapdoor Function



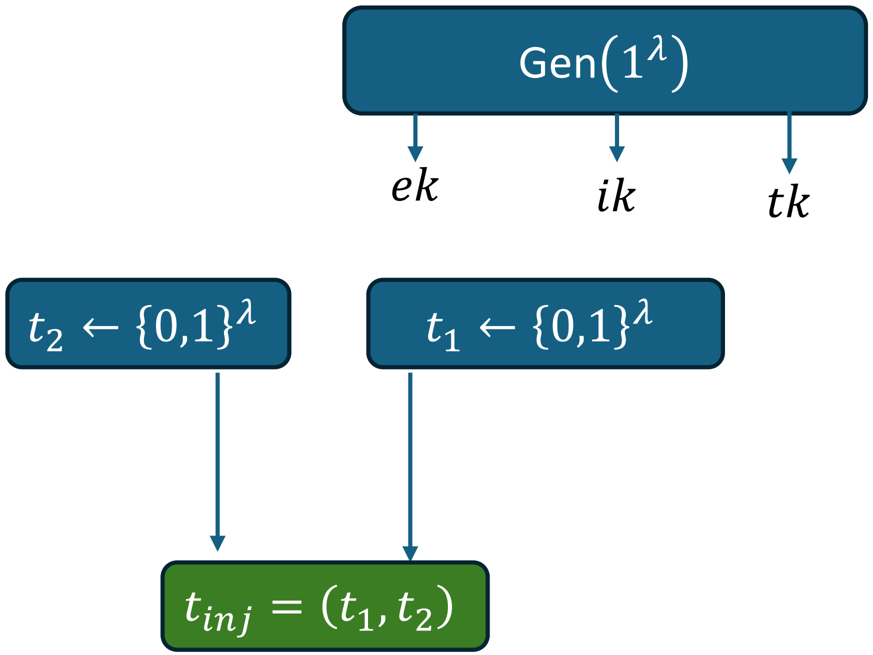
All-But-Many Lossy Trapdoor Functions



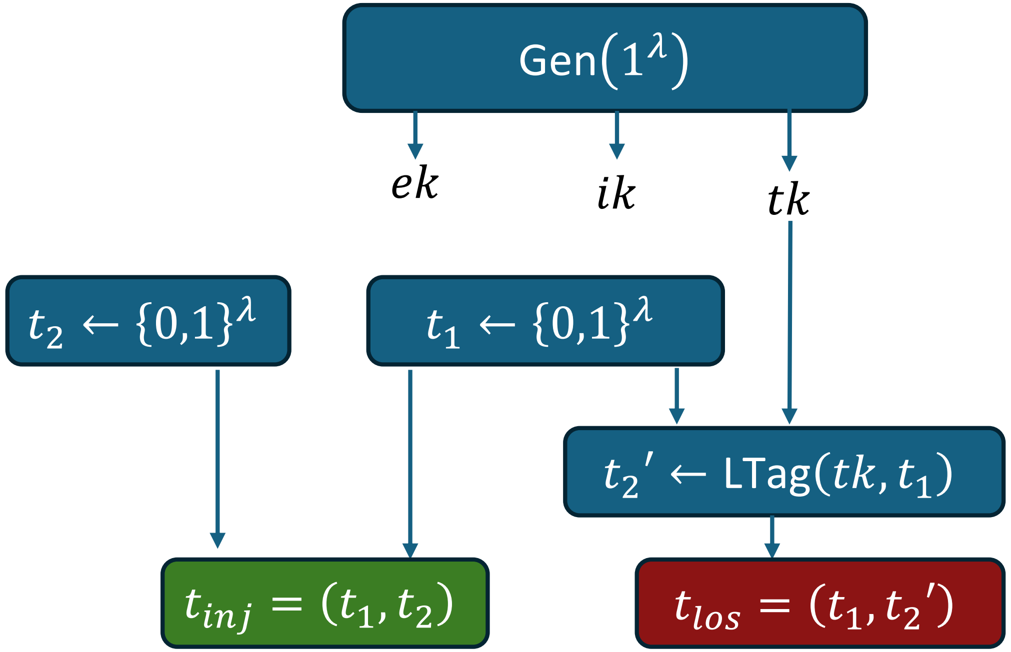
All-But-Many Lossy Trapdoor Functions



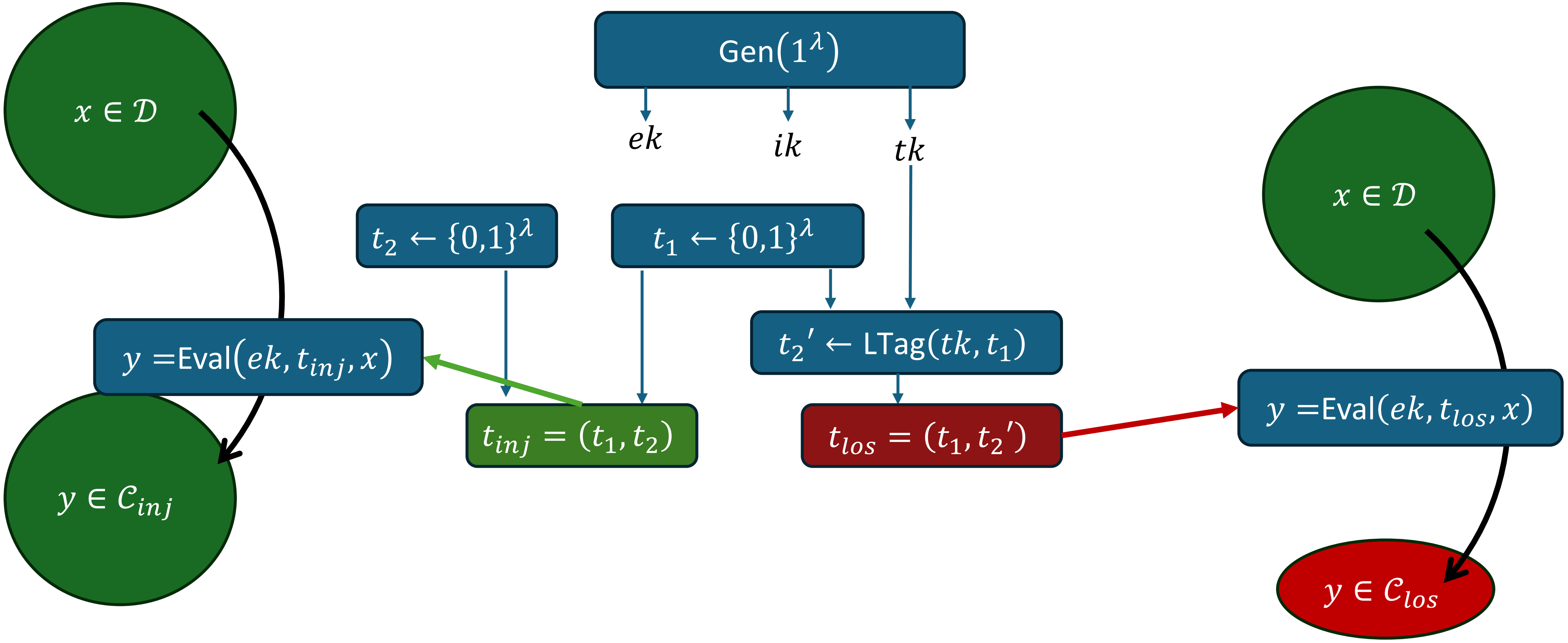
All-But-Many Lossy Trapdoor Functions



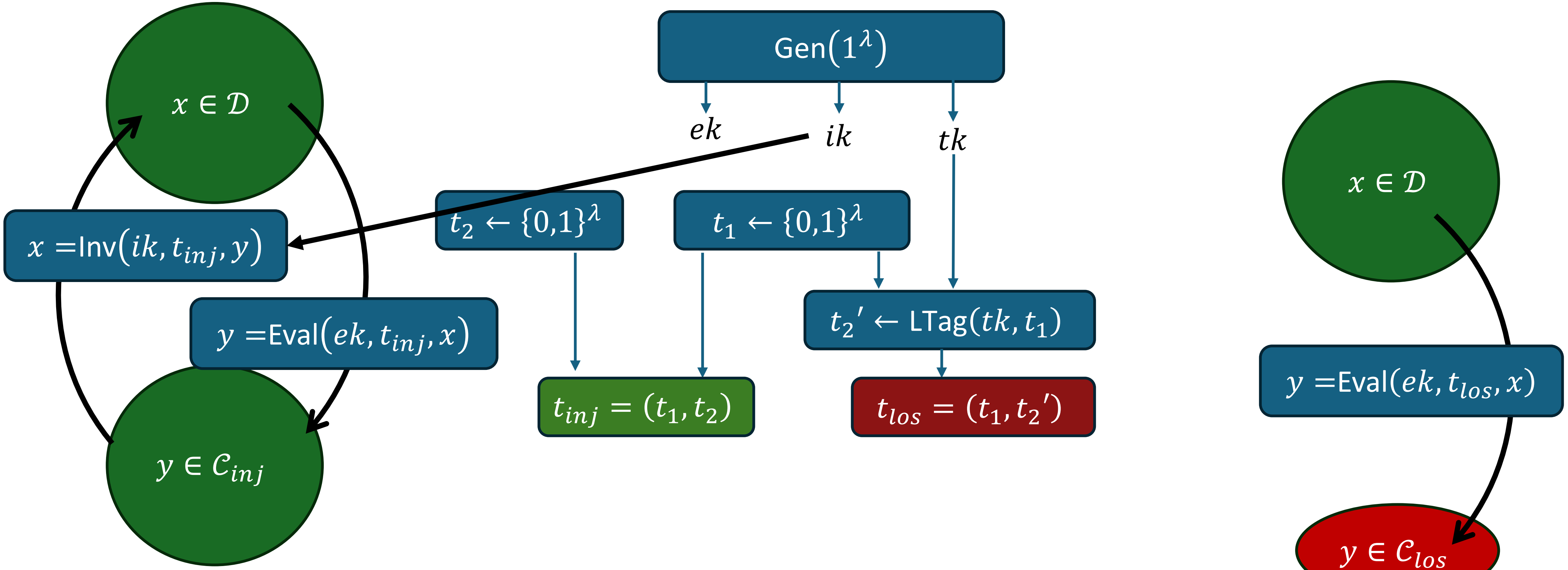
All-But-Many Lossy Trapdoor Functions



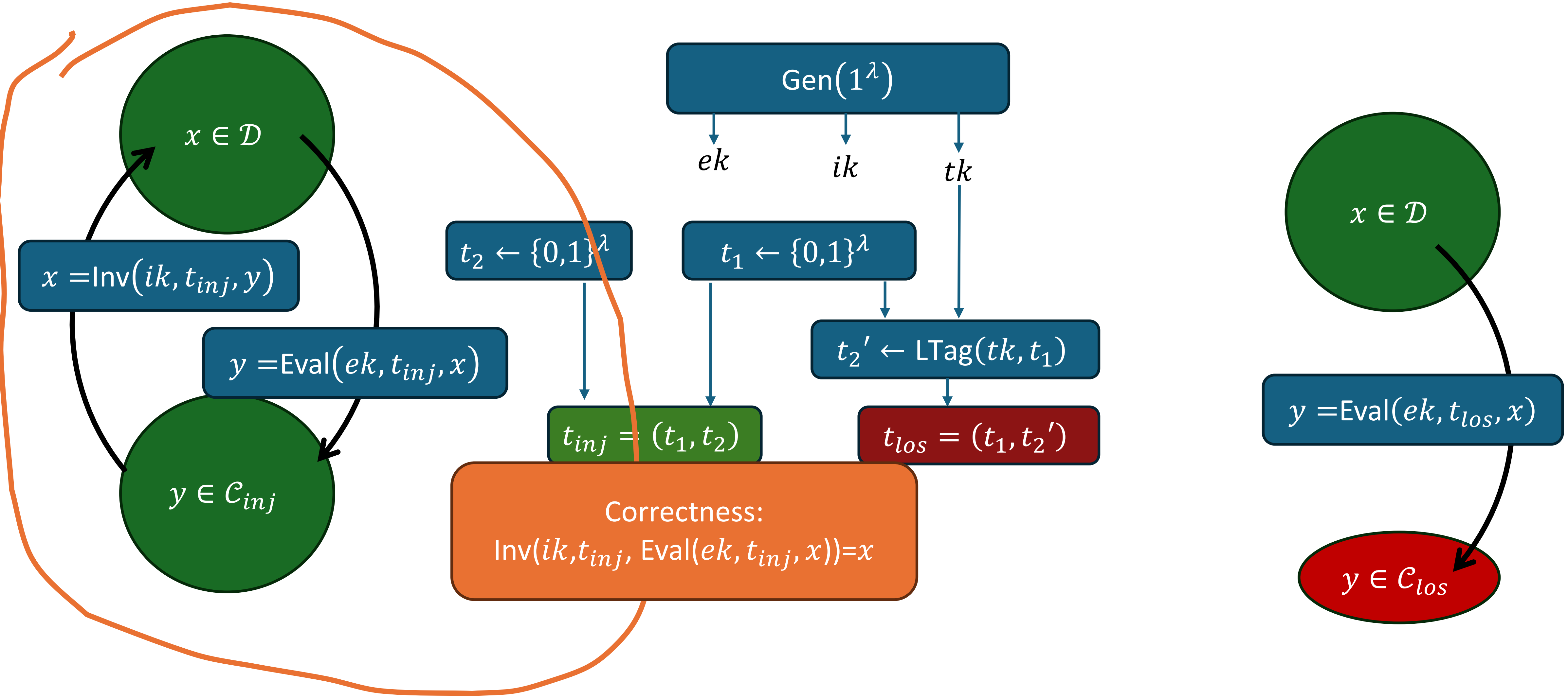
All-But-Many Lossy Trapdoor Functions



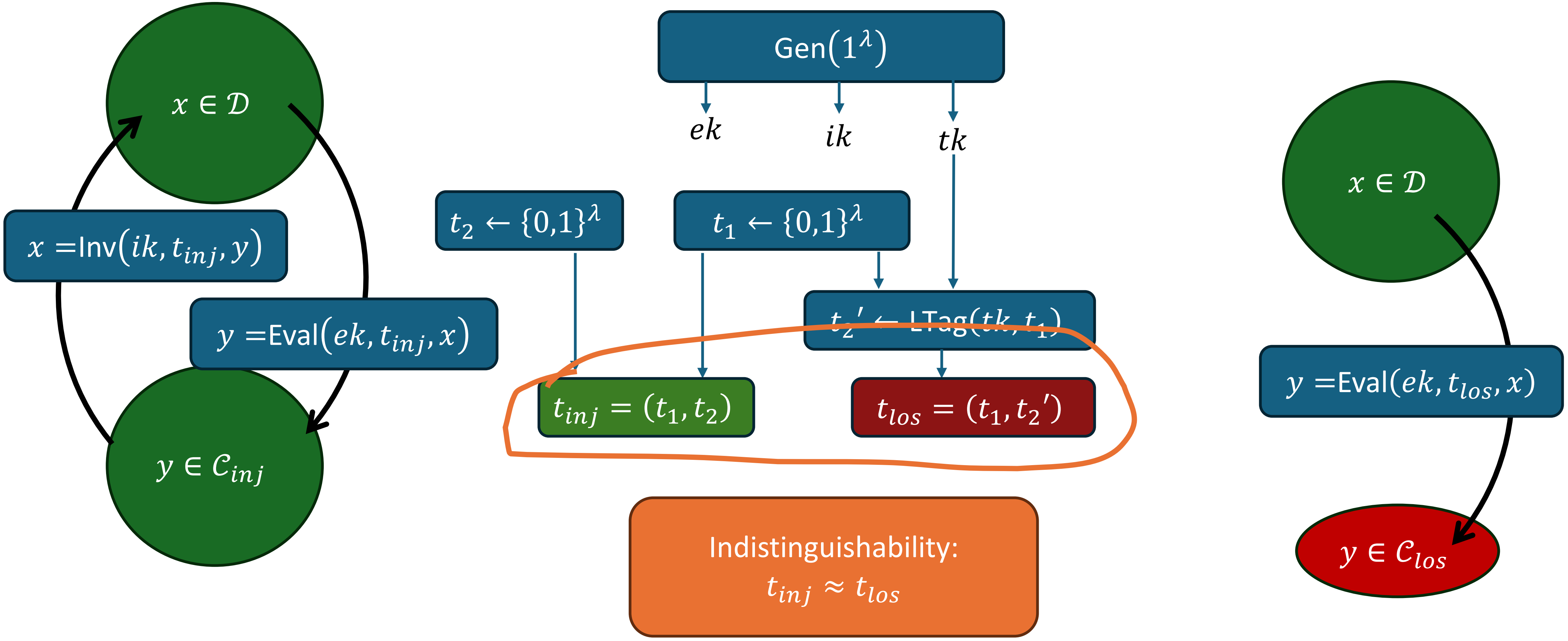
All-But-Many Lossy Trapdoor Functions



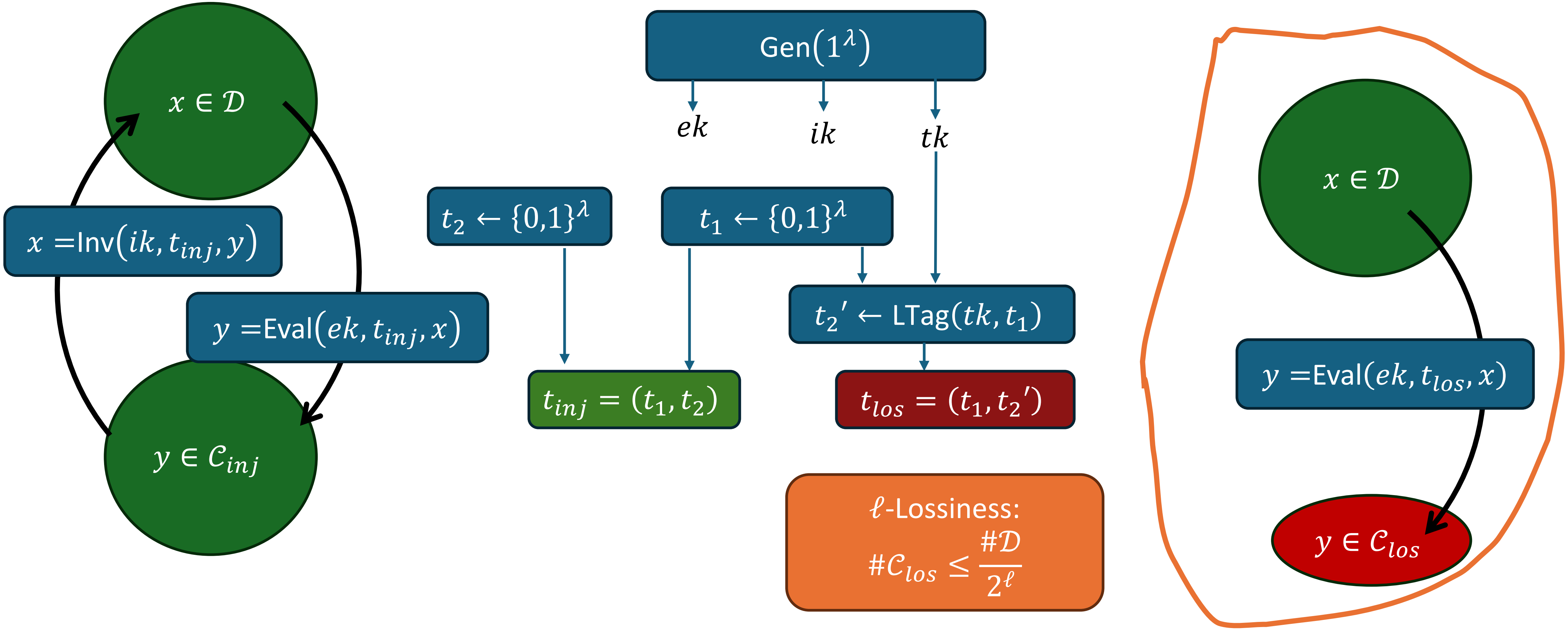
All-But-Many Lossy Trapdoor Functions



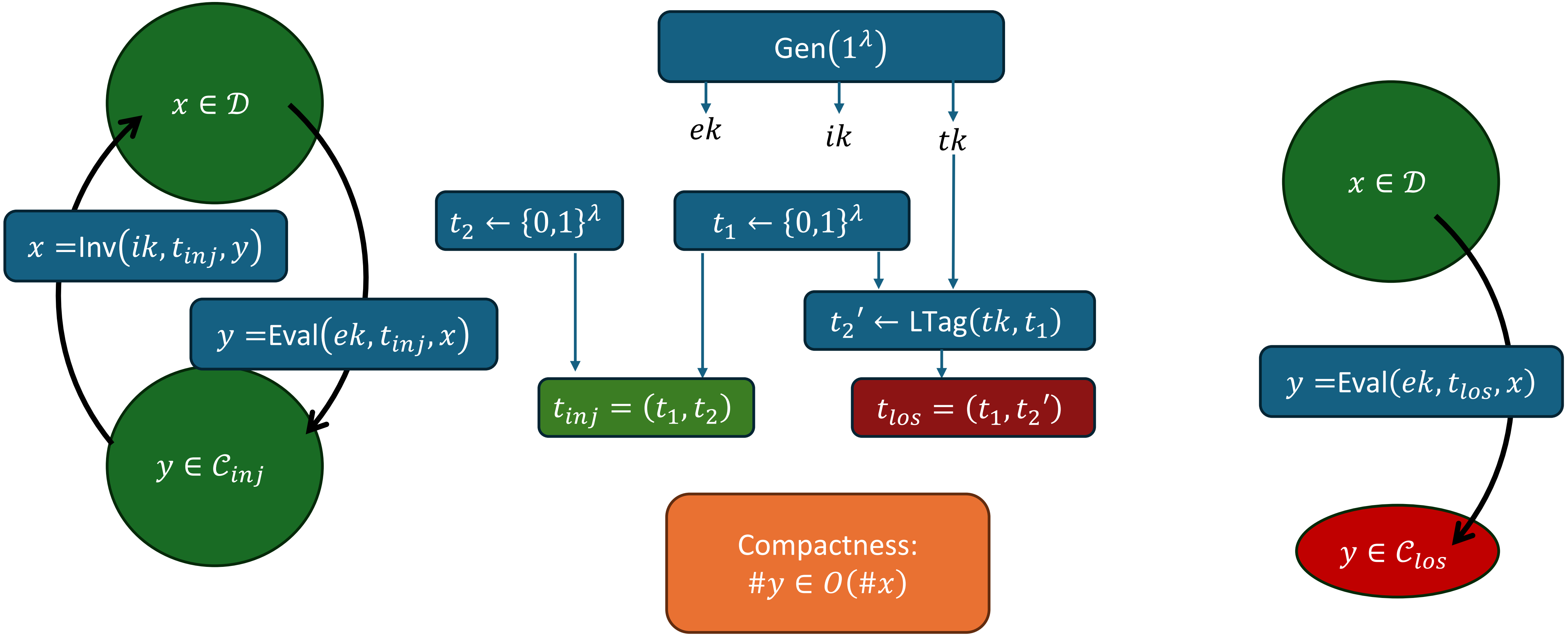
All-But-Many Lossy Trapdoor Functions



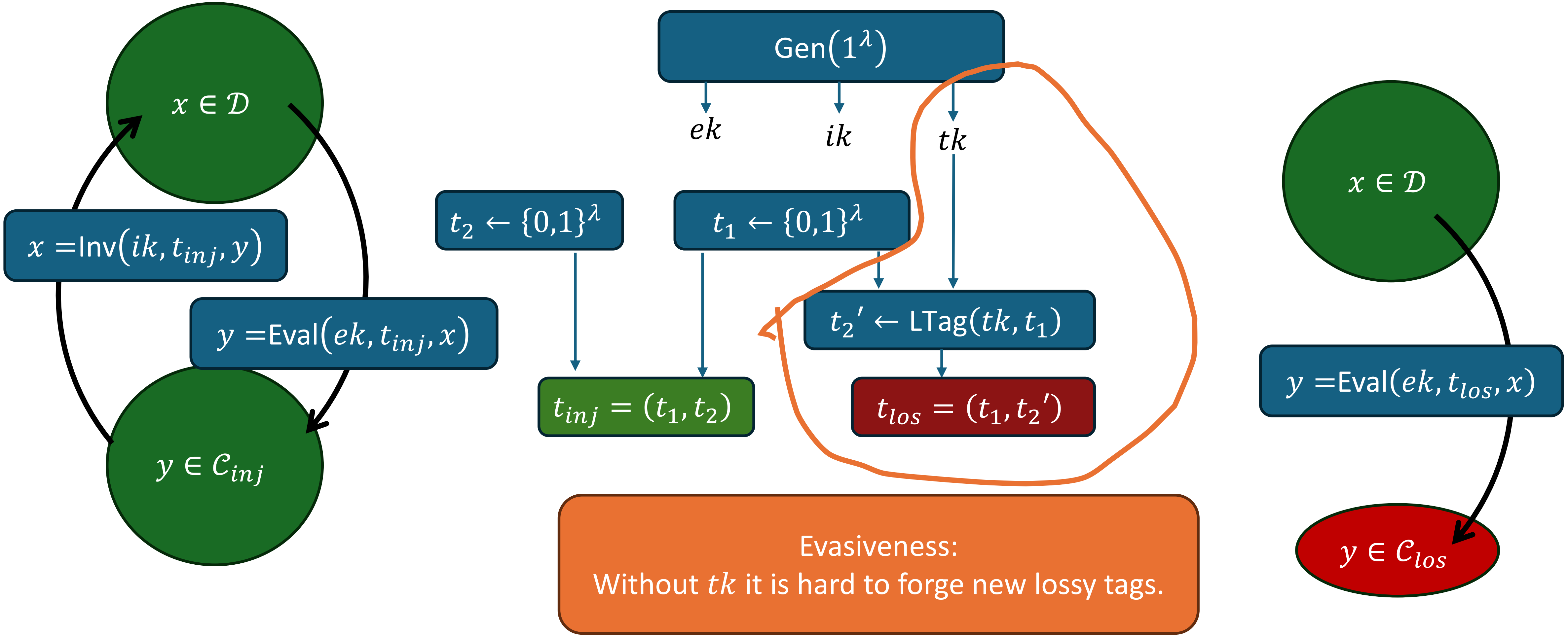
All-But-Many Lossy Trapdoor Functions



All-But-Many Lossy Trapdoor Functions



All-But-Many Lossy Trapdoor Functions



Compact ABM Lossy Trapdoor Functions

ABM-LTF = (Gen, Eval, Inv, LTag)

- Gen(1^λ) outputs ek and ik and tag key tk.
- LTag(tk, t_1) outputs t_2 s.t. (t_1, t_2) is lossy.
- Eval(ek, t_1, t_2, x) evaluates x to y.
- Inv(ik, t_1, t_2, y) extracts x if (t_1, t_2) is injective.

A Compact LTF from LWE

Generating Keys:

Draw a MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S} \leftarrow \mathbb{Z}_q^{n \times N}, \mathbf{E} \leftarrow \chi^{(m+u) \times N}$.

Output $ek \coloneqq \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S} + \mathbf{E} + b \cdot \mathbf{G}$
and $ik \coloneqq (A, B, td)$ (if injective mode).

A Compact ABM-LTF from LWE

Fix $\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$.
Generating Keys:

Draw a PRF key $k = (k_1, \dots, k_\lambda) \leftarrow \{0,1\}^\lambda$.

Draw an MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S}_1, \dots, \mathbf{S}_\lambda \leftarrow \mathbb{Z}_q^{n \times N}$, $\mathbf{E}_1, \dots, \mathbf{E}_\lambda \leftarrow \chi^{(m+u) \times N}$.

Output $\mathbf{C}_1 := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_1 + \mathbf{E}_1 + k_1 \cdot \mathbf{G}, \dots,$

$\mathbf{C}_\lambda := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_\lambda + \mathbf{E}_\lambda + k_\lambda \cdot \mathbf{G}$ as ek.

and $ik := (A, B, td)$ and $tk := k$.

A Compact ABM-LTF from LWE

Fix PRF : $\{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$.
Generating Keys:

Draw a PRF key $k = (k_1, \dots, k_\lambda) \leftarrow \{0,1\}^\lambda$.

Draw an MP12-Trapdoor $(\mathbf{A}, td) \leftarrow GenTrap(u \times n)$,

$\mathbf{B} \leftarrow \mathbb{Z}_q^{m \times n}$,

$\mathbf{S}_1, \dots, \mathbf{S}_\lambda \leftarrow \mathbb{Z}_q^{n \times N}$, $\mathbf{E}_1, \dots, \mathbf{E}_\lambda \leftarrow \chi^{(m+u) \times N}$.

Output $\mathbf{C}_1 := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_1 + \mathbf{E}_1 + k_1 \cdot \mathbf{G}, \dots,$

$\mathbf{C}_\lambda := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_\lambda + \mathbf{E}_\lambda + k_\lambda \cdot \mathbf{G}$ as ek.

and $ik := (A, B, td)$ and $tk := k$.

$\mathbf{C}_1, \dots, \mathbf{C}_\lambda$ are dual GSW encryptions of $k_1 \dots, k_\lambda$.

A Compact ABM-LTF from LWE

Fix PRF : $\{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$.
Generating Keys:

$$\mathbf{C}_i := \begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix} \cdot \mathbf{S}_i + \mathbf{E}_i + k_i \cdot \mathbf{G} \qquad \text{for } i = 1, \ldots, \lambda$$

A Compact ABM-LTF from LWE

Fix $\mathsf{PRF}: \{0,1\}^{\lambda} \times \{0,1\}^{\lambda} \to \{0,1\}^{\lambda}$.
Generating Keys:

$$\mathbf{C}_i := \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_i + \mathbf{E}_i + k_i \cdot \mathbf{G} \qquad \text{for } i = 1, \ldots, \lambda$$

Generating Lossy Tags:

$$\mathrm{Ltag}(tk = k, t_1) \text{ outputs } t_2 := \mathrm{PRF}(k, t_1).$$

A Compact ABM-LTF from LWE

Fix $\mathsf{PRF} : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda$.

Generating Keys:

$$\mathbf{C}_i \coloneqq \binom{\mathbf{A}}{\mathbf{B}} \cdot \mathbf{S}_i + \mathbf{E}_i + k_i \cdot \mathbf{G} \qquad \text{for } i = 1, .., \lambda$$

Generating Lossy Tags:

Ltag$(tk = k, t_1)$ outputs $t_2 \coloneqq \mathsf{PRF}(k, t_1)$.

Evaluating x:

Eval(ek, t_1, t_2, x) uses FHE to evaluate the function

$$f(k) \coloneqq \begin{cases} x, & \text{if } \mathrm{PRF}(k, t_1) \neq t_2 \\ 0, & \text{if } \mathrm{PRF}(k, t_1) = t_2 \end{cases}$$

on $ek = (\mathbf{C}_1, \dots, \mathbf{C}_\lambda)$.

A Compact ABM-LTF from LWE

- Correctness
- Indistinguishability of injective and lossy tags
- Evasiveness of lossy Tags
- Compactness
- ℓ-Lossiness

A Compact ABM-LTF from LWE

- Correctness ✓
- Indistinguishability of injective and lossy tags ✓
- Evasiveness of lossy Tags ✓ (follows from pseudorandomness of PRF)
- Compactness ✓
- ℓ-Lossiness ✓

On Parameters

In theory, we get high lossiness and small ciphertext expansion.

On Parameters

In theory, we get high lossiness and small ciphertext expansion.

But in praxis, parameters turn out to be huge ☹

Problem: using FHE/PRF makes modulus large.

On Parameters

In theory, we get high lossiness and small ciphertext expansion.

But in praxis, parameters turn out to be huge ☹

Problem: using FHE/PRF makes modulus large.

Possible solution:

Switch to (Q)ROM and use Fujisaki-Okamoto transformation [next talk, Pan&Zeng].

Summary

Our results:

- Compact ABM-LTFs from LWE (and PRFs in **NC**1).
- Compact IND-so-CCA PKE from LWE (and PRFs in **NC**1).
- Along the way: fix mistake in proof of [Hof12].

Our techniques:

- Use dual GSW FHE [GSW13].
- Compression technique for elements of $\mathbb{Z}_p$.

Summary

Our results:

- Compact ABM-LTFs from LWE (and PRFs in **NC**1).
- Compact IND-so-CCA PKE from LWE (and PRFs in **NC**1).
- Along the way: fix mistake in proof of [Hof12].

Our techniques:

- Use dual GSW FHE [GSW13].
- Compression technique for elements of $\mathbb{Z}_p$.

Thank you for your Attention!