Security of Symmetric Primitives under Incorrect Usage of Keys

Pooya Farshim[1] Claudio Orlandi[2] Răzvan Roşie[1]

[1]ENS, CNRS, INRIA & PSL Research University, Paris, France

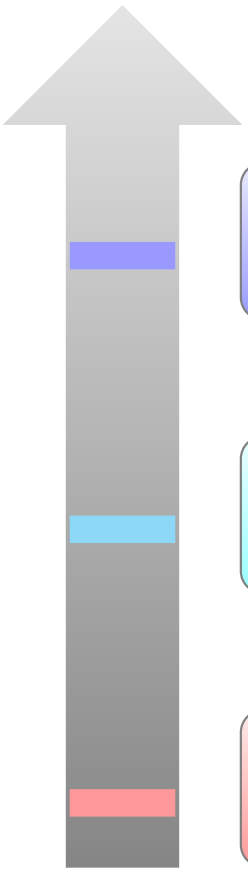
[2]Aarhus University, Aarhus, Denmark

FSE 2017, Tokyo, Japan

8^{th} March 2017

Key-Robustness in a Nutshell

Robustness: ciphertext can't be decrypted under two different keys.



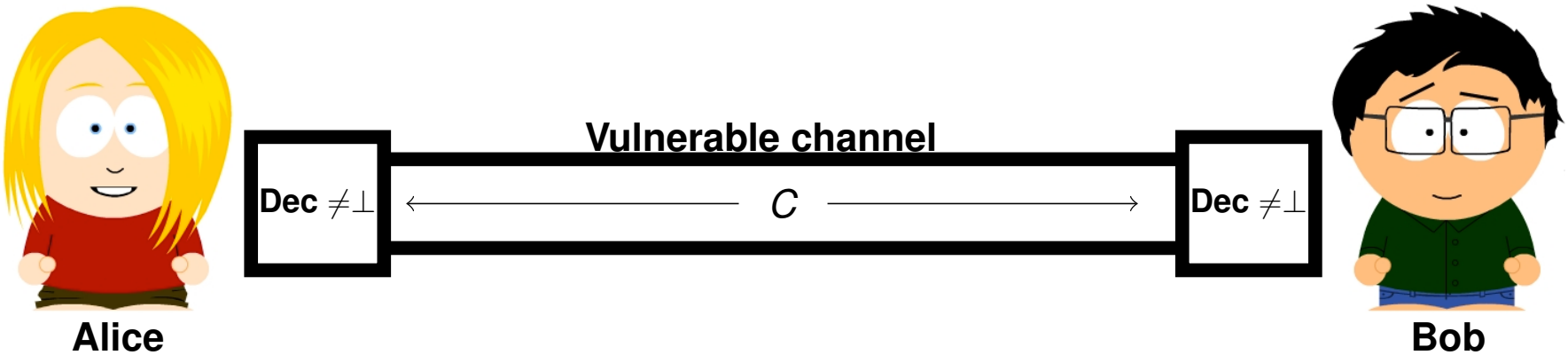
PKC13: robustness for PKE & IBE revisited by Farshim et al.

AC10: Mohassel extends robustness to Hybrid Encryption.

TCC10: robustness introduced for PKE & IBE by Abdalla et al.

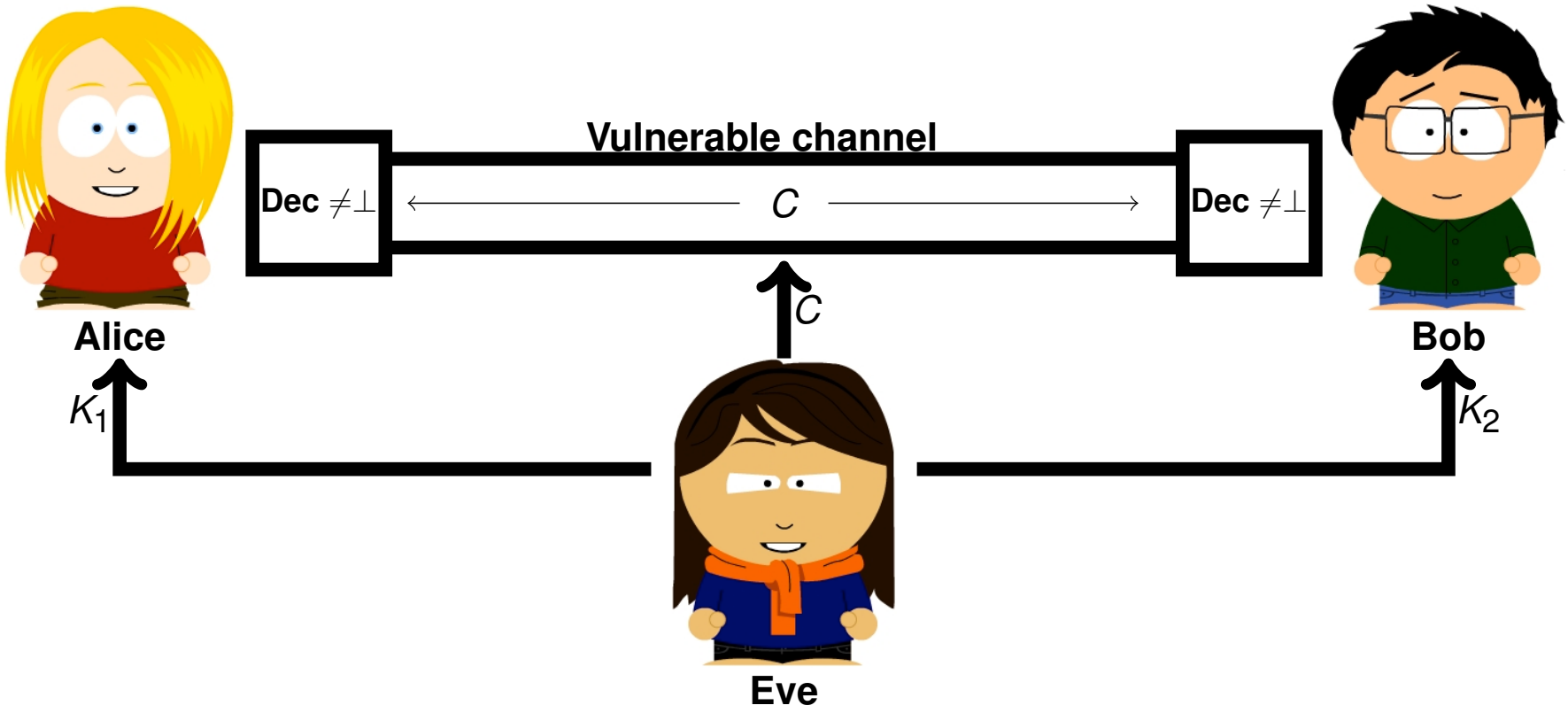
Key-Robustness in a Nutshell

Robustness: ciphertext can't be decrypted under two different keys.



Key-Robustness in a Nutshell

Robustness: ciphertext can't be decrypted under two different keys.



Motivating Key-Robustness - Example 1

Digital Signatures from Symmetric Encryption:

- $sk \leftarrow (K, s)$
- $pk \leftarrow \mathbf{Enc}(K, s)$ — contains the Symm. Enc. of s.
- $\sigma \leftarrow (\mathbf{PRF}(s, M), \pi)$ — PRF evaluation + ZK proof for correctness.

Is the scheme unforgeable?

Motivating Key-Robustness - Example 1

Digital Signatures from Symmetric Encryption:

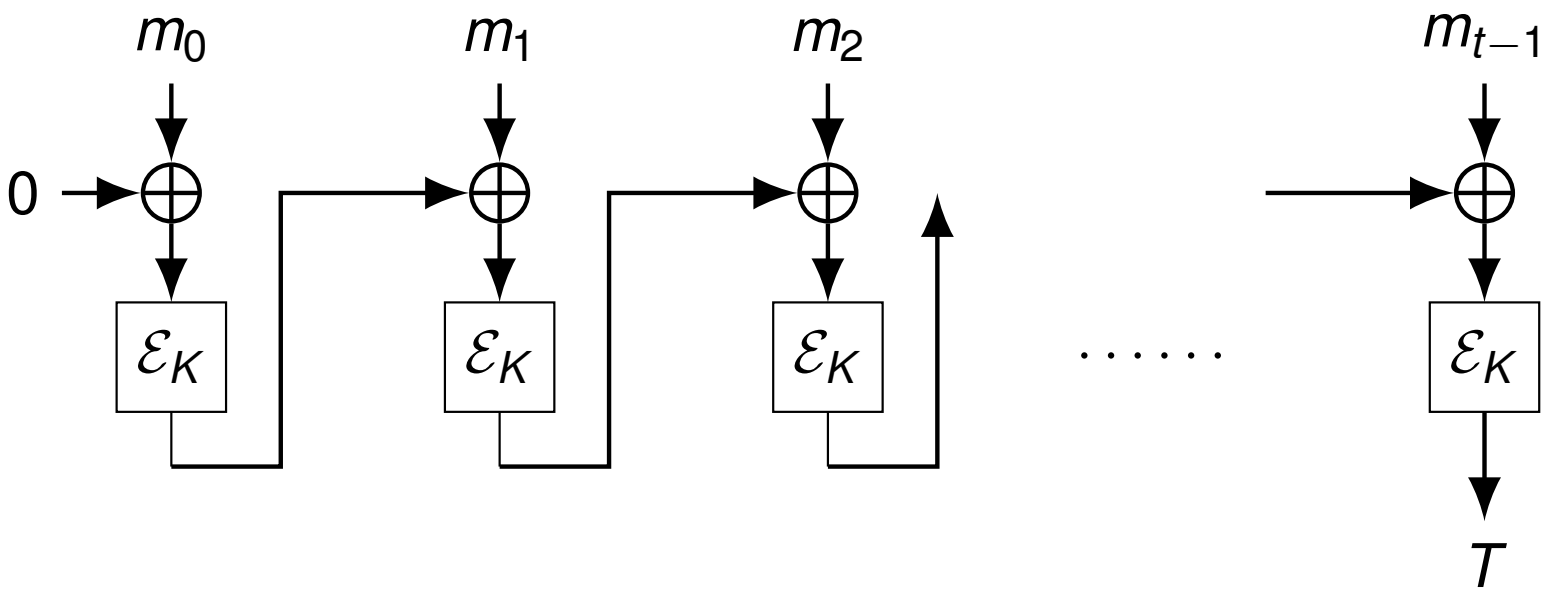
- $sk \leftarrow (K, s)$
- $pk \leftarrow \mathbf{Enc}(K, s)$ — contains the Symm. Enc. of s.
- $\sigma \leftarrow (\mathbf{PRF}(s, M), \pi)$ — PRF evaluation + ZK proof for correctness.

Is the scheme unforgeable?

$\mathbf{Enc}(K, s) = \mathbf{Enc}(K', s') \implies$ **FORGE**

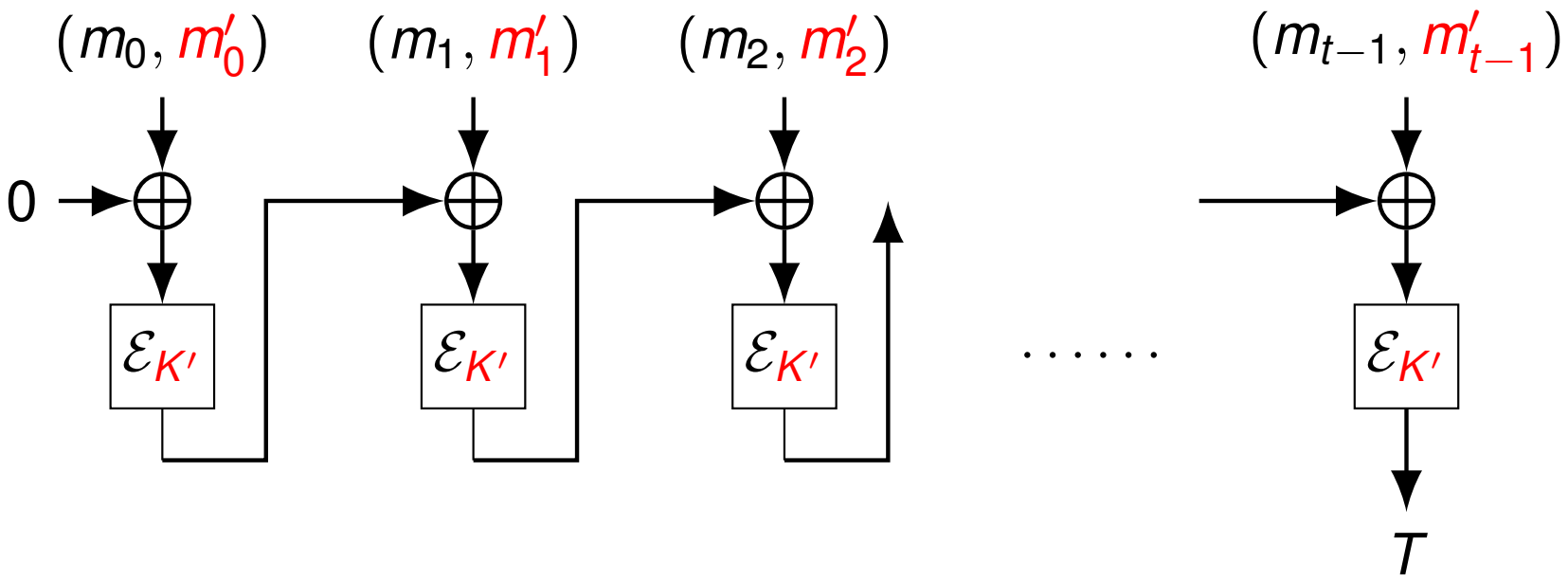
Motivating Key Robustness - Example 2

CBC-MAC:



Motivating Key Robustness - Example 2

CBC-MAC:



$$\mathbf{MAC}(K, M) = \mathbf{MAC}(K', M') = T$$

Definitional Landscape

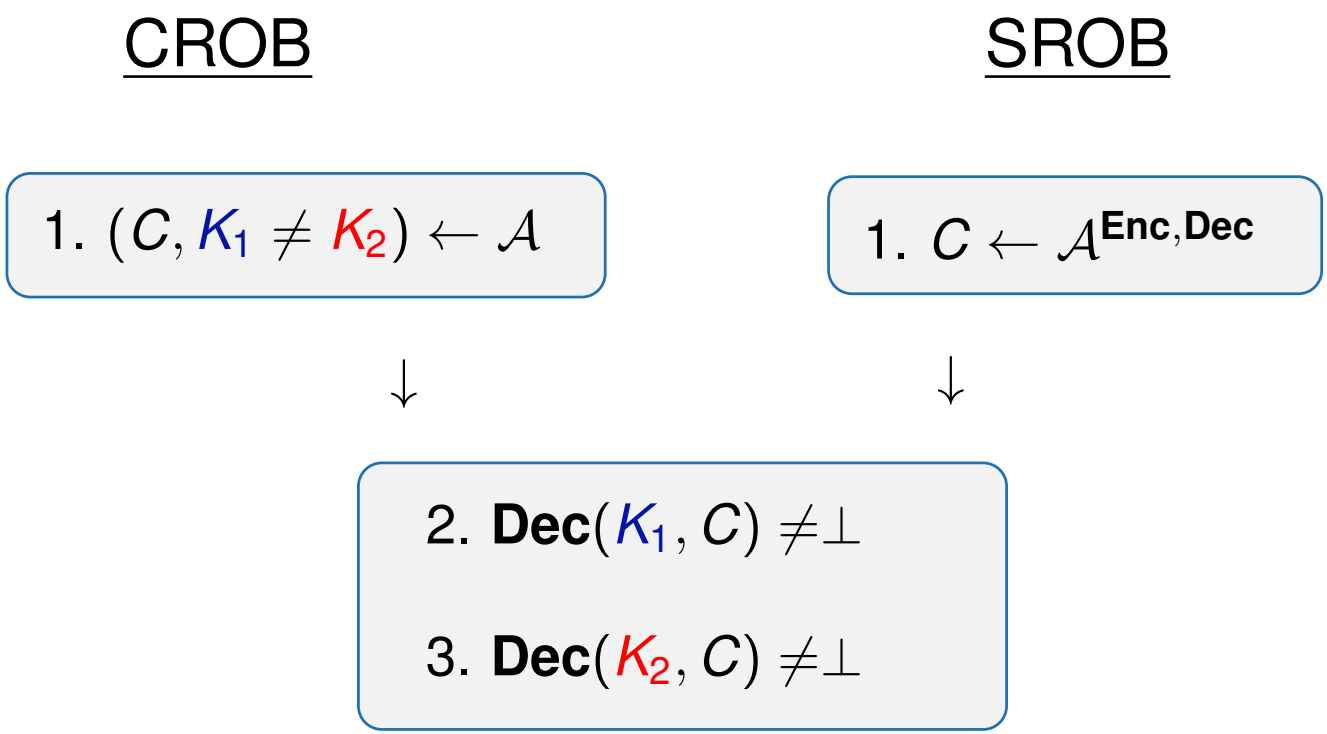
- Complete Robustness (CROB): adversarially generated K_1, K_2.
- Goal: find C decryptable under K_1, K_2.

- CROB security:

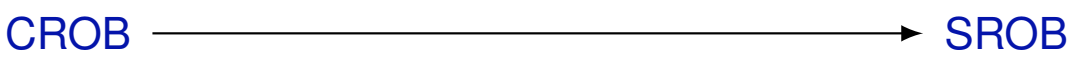
1. $(C, K_1 \neq K_2) \leftarrow \mathcal{A}$
2. $\mathbf{Dec}(K_1, C) \neq \perp$
3. $\mathbf{Dec}(K_2, C) \neq \perp$

Definitional Landscape

- Strong Robustness (SROB): honestly generated K_1, K_2.
- Goal: find C decryptable under K_1, K_2.



Definitional Landscape

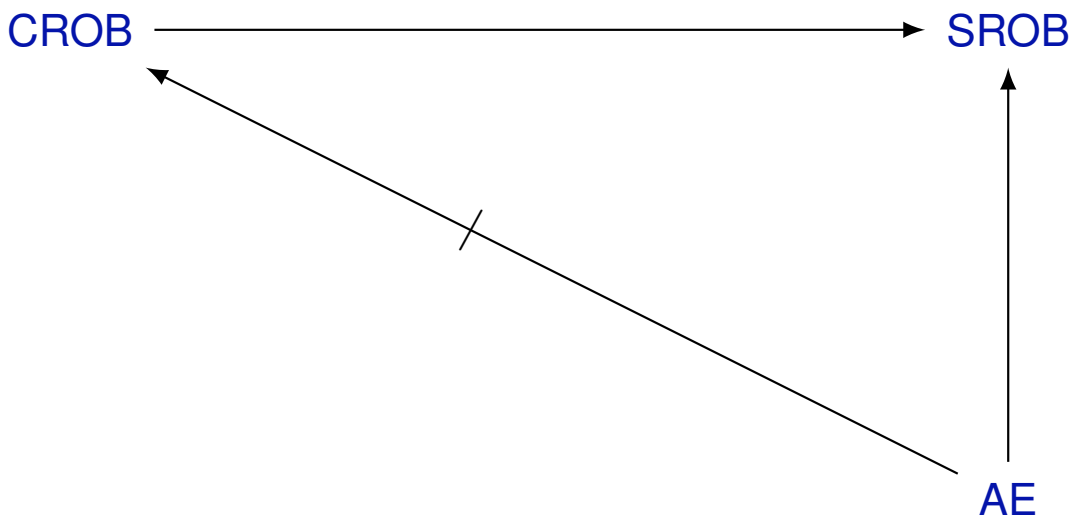


Definitional Landscape

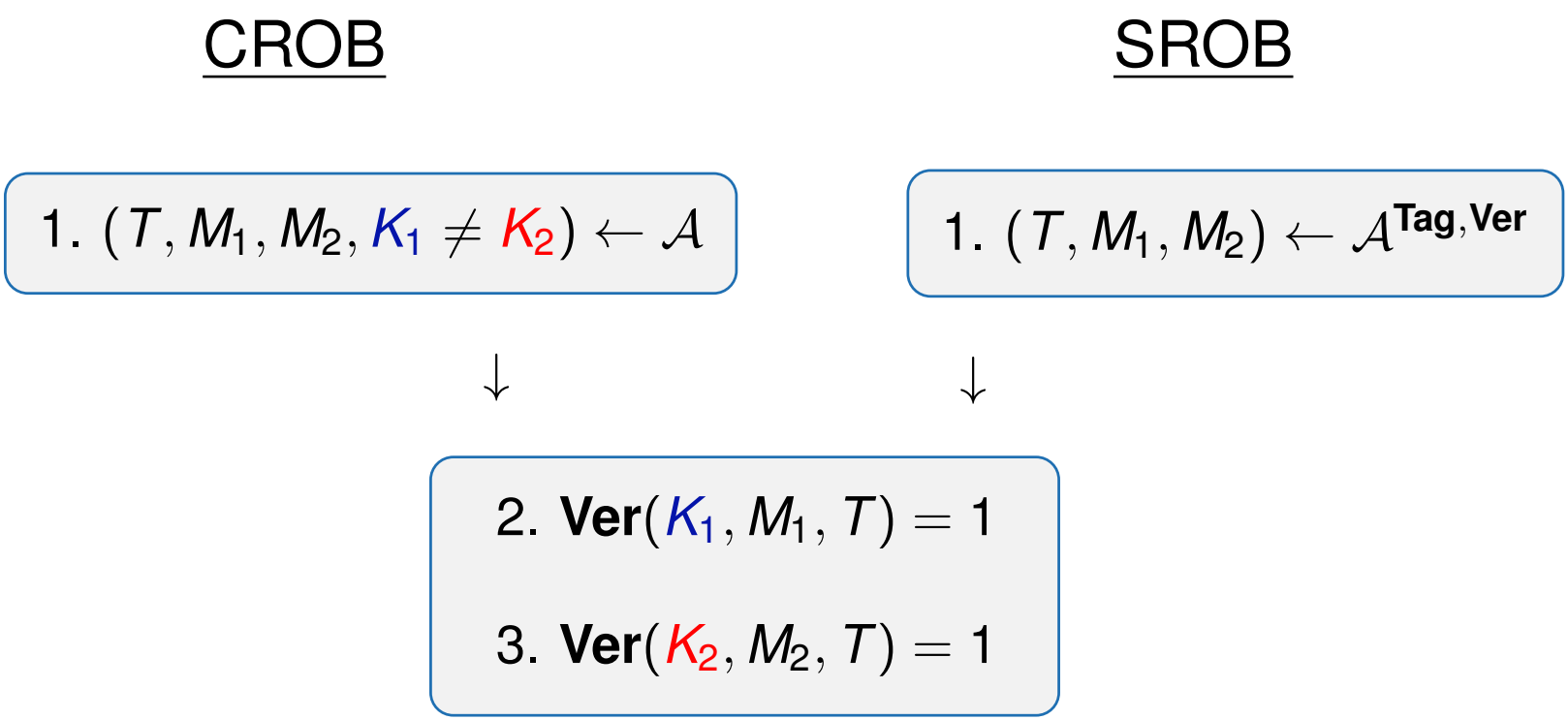
- AE-secure scheme $\Longrightarrow$ SROB-secure.

Definitional Landscape

- AE-secure scheme $\not\Rightarrow$ CROB-secure.

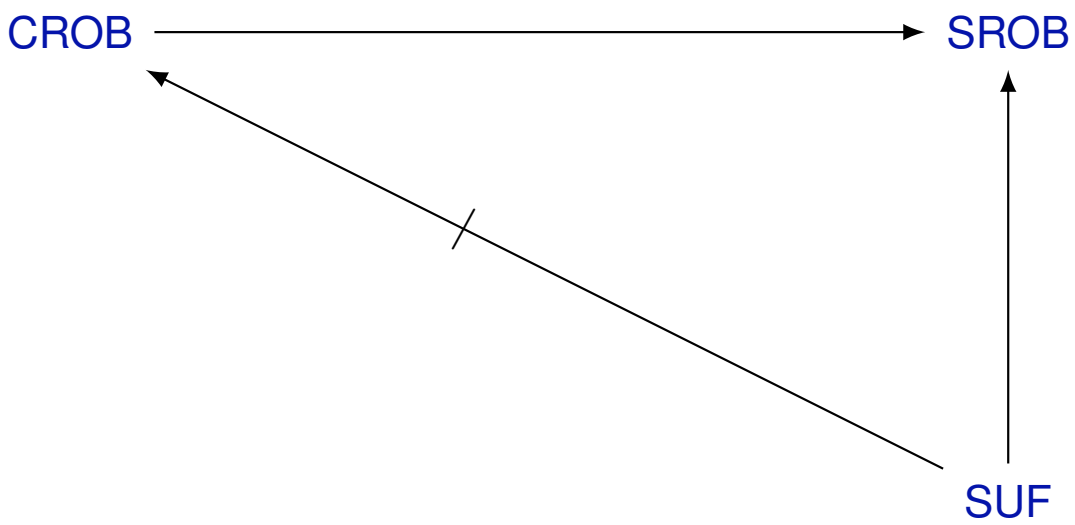


Definitional Landscape - MACs

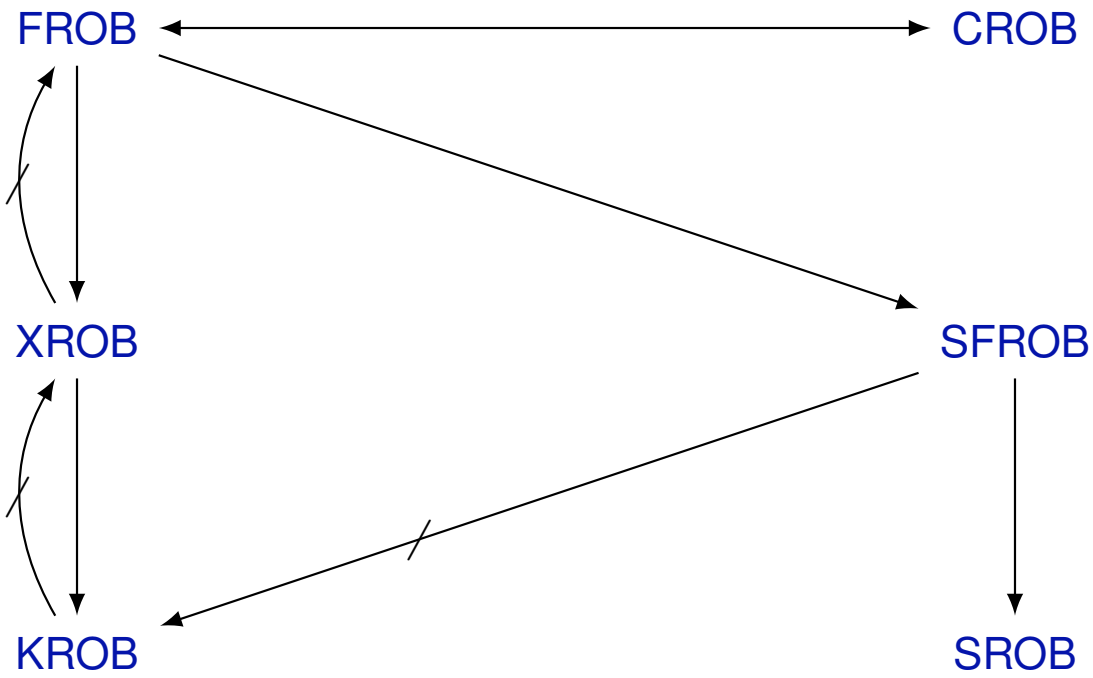


Definitional Landscape - MACs

- SUF-secure MAC scheme $\Longrightarrow$ SROB-secure.



The Big Picture



Generic Composition

Same Keys:

$$\textbf{Enc} \text{ is CROB} \quad \text{OR} \quad \textbf{MAC} \text{ is CROB} \Rightarrow \begin{cases} \textbf{Enc}\text{-Then-}\textbf{MAC} \text{ is CROB} \\ \textbf{Enc}\text{-And-}\textbf{MAC} \text{ is CROB} \\ \textbf{MAC}\text{-Then-}\textbf{Enc} \text{ is CROB} \end{cases}$$

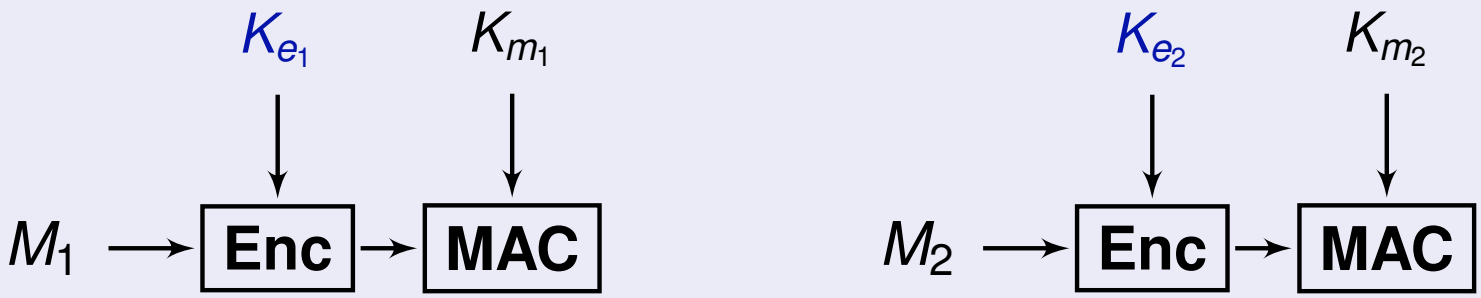
Different Keys:

$$\textbf{Enc} \text{ is CROB} \quad \text{AND} \quad \textbf{MAC} \text{ is CROB} \Rightarrow \begin{cases} \textbf{Enc}\text{-Then-}\textbf{MAC} \text{ is CROB} \\ \textbf{Enc}\text{-And-}\textbf{MAC} \text{ is CROB} \\ \textbf{MAC}\text{-Then-}\textbf{Enc} \text{ is CROB} \end{cases}$$

Generic Composition

Proof intuition (Enc-Then-Mac):

$\mathcal{A}$ outputs a CROB winning tuple $(C||T, K_{e_1}||K_{m_1}, K_{e_2}||K_{m_2})$.

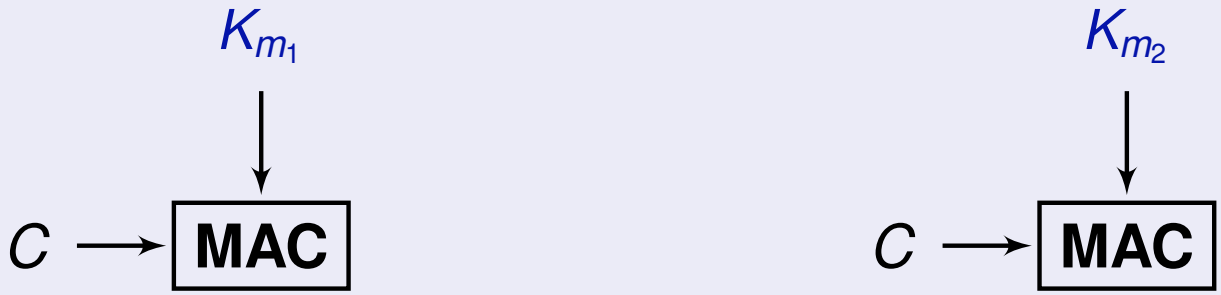


- Case $K_{e_1} \neq K_{e_2}$: (C, K_{e_1}, K_{e_2}) wins CROB against **Enc**.
- Case $K_{m_1} \neq K_{m_2}$: $(T, K_{m_1}, C, K_{m_2}, C)$ wins CROB against **MAC**.

Generic Composition

Proof intuition.

$\mathcal{A}$ outputs a CROB winning tuple $(C||T, K_{e_1}||K_{m_1}, K_{e_2}||K_{m_2})$.



- Case $K_{e_1} \neq K_{e_2}$: (C, K_{e_1}, K_{e_2}) wins CROB against **Enc**.
- Case $K_{m_1} \neq K_{m_2}$: $(T, K_{m_1}, C, K_{m_2}, C)$ wins CROB against **MAC**.

CROB AE in the RO Model

Instantiate a CROB MAC: $\mathbf{MAC}(K, M) := \mathbf{RO}(K, M)$.

- Same-Key: Enc-Then-Mac via a CROB **MAC**.

CROB AE in the RO Model

Instantiate a CROB MAC: $\mathbf{MAC}(K, M) := \mathbf{RO}(K, M)$.

- Same-Key: Enc-Then-Mac via a CROB **MAC**.
- Different-Keys: authenticate the encryption key.

$\overline{\mathbf{Enc}}((K_e||K_m), M)$:
$C \twoheadleftarrow \mathbf{Enc}(K_e, M)$
$T \leftarrow \mathbf{RO}(K_m, (C||K_e))$
return (C, T)

✓ AE-security

✓ CROB

CROB AE in the Standard Model

Idea: construct a CROB secure MAC in the Standard Model.

- First attempt:

$\overline{\mathbf{Enc}}((K_e||K_m), M)$:
$C \twoheadleftarrow \mathbf{Enc}(K_e, M)$
$T \leftarrow \mathbf{MAC}(K_m, (C||K_e))$
return (C, T)

- Issue: pseudorandomness for **MAC**.

CROB AE in the Standard Model

Idea: construct a CR-PRF in the Standard Model.

- Second attempt:

$\overline{\textbf{Enc}}((K_e||K_m), M)$:
$C \twoheadleftarrow \textbf{Enc}(K_e, M)$
$T \leftarrow \textbf{PRF}(K_m, (C||K_e))$
return (C, T)

- Issue: ensure the **PRF** is Collision-Resistant.

Collision-Resistant PRFs in the Standard Model

- Collision-Resistant PRF:

$$\mathbf{PRF}(K_1, M_1) = \mathbf{PRF}(K_2, M_2) \implies (K_1, M_1) = (K_2, M_2)$$

- Key-Injective PRF:

$$\mathbf{PRF}(K_1, M) = \mathbf{PRF}(K_2, M) \Rightarrow K_1 = K_2$$

- Right-Injective PRG:

$$\mathbf{PRG}_{RHS}(K_1) = \mathbf{PRG}_{RHS}(K_2) \Rightarrow K_1 = K_2$$

Collision-Resistant PRFs in the Standard Model

Construction for Collision-Resistant PRF:

$\underline{\overline{\mathbf{PRF}}(K, M):}$
$(K_1 || K_2) \leftarrow \mathbf{PRG}(K)$
$C_1 \leftarrow \mathbf{PRP}(K_1, M)$
$C_2 \leftarrow \mathbf{PRF}(K_2, C_1)$
return $(C_1 || C_2)$

Collision-Resistant PRF:

$$\mathbf{PRF}(K, M) = \mathbf{PRF}(K', M') \implies (K, M) = (K', M')$$

Collision-Resistant PRFs in the Standard Model

Construction for Collision-Resistant PRF:

$\overline{\mathbf{PRF}}(K, M)$:
$(K_1 || K_2) \leftarrow \mathbf{PRG}(K)$
$C_1 \leftarrow \mathbf{PRP}(K_1, M)$
$C_2 \leftarrow \mathbf{PRF}(K_2, C_1)$
return $(C_1 || C_2)$

Proof intuition:

Step 1 - Key-Injective PRF:

$$\mathbf{PRF}(K_2, C_1) = \mathbf{PRF}(K_2', C_1) \Rightarrow K_2 = K_2'$$ □

Collision-Resistant PRFs in the Standard Model

Construction for Collision-Resistant PRF:

$\overline{\mathbf{PRF}}(K, M)$:
$(K_1 || K_2) \leftarrow \mathbf{PRG}(K)$
$C_1 \leftarrow \mathbf{PRP}(K_1, M)$
$C_2 \leftarrow \mathbf{PRF}(K_2, C_1)$
return $(C_1 || C_2)$

Proof intuition:

Step 2 - Right-Injective PRG:

$$\mathbf{PRG}_{RHS}(K) = \mathbf{PRG}_{RHS}(K') \Rightarrow K = K'$$ □

Collision-Resistant PRFs in the Standard Model

Construction for Collision-Resistant PRF:

$\overline{\mathbf{PRF}}(K, M)$:
$(K_1 || K_2) \leftarrow \mathbf{PRG}(K)$
$C_1 \leftarrow \mathbf{PRP}(K_1, M)$
$C_2 \leftarrow \mathbf{PRF}(K_2, C_1)$
return $(C_1 || C_2)$

Proof intuition:

Step 3 - Permutation:

$$\mathbf{PRP}(K_1, M) = \mathbf{PRP}(K_1, M') \Rightarrow M = M'$$

Right-Injective PRGs

Building-block 1: a right injective PRG.

- Use the construction by Yao:

$$\mathbf{PRG}(x) := \underbrace{\mathbf{HC}(x)||\mathbf{HC}(\pi(x))||\ldots||\mathbf{HC}(\pi^{|x|-1}(x))}_{\text{Left Part}} || \underbrace{\pi^{|x|}(x)}_{\text{Right Part}}$$

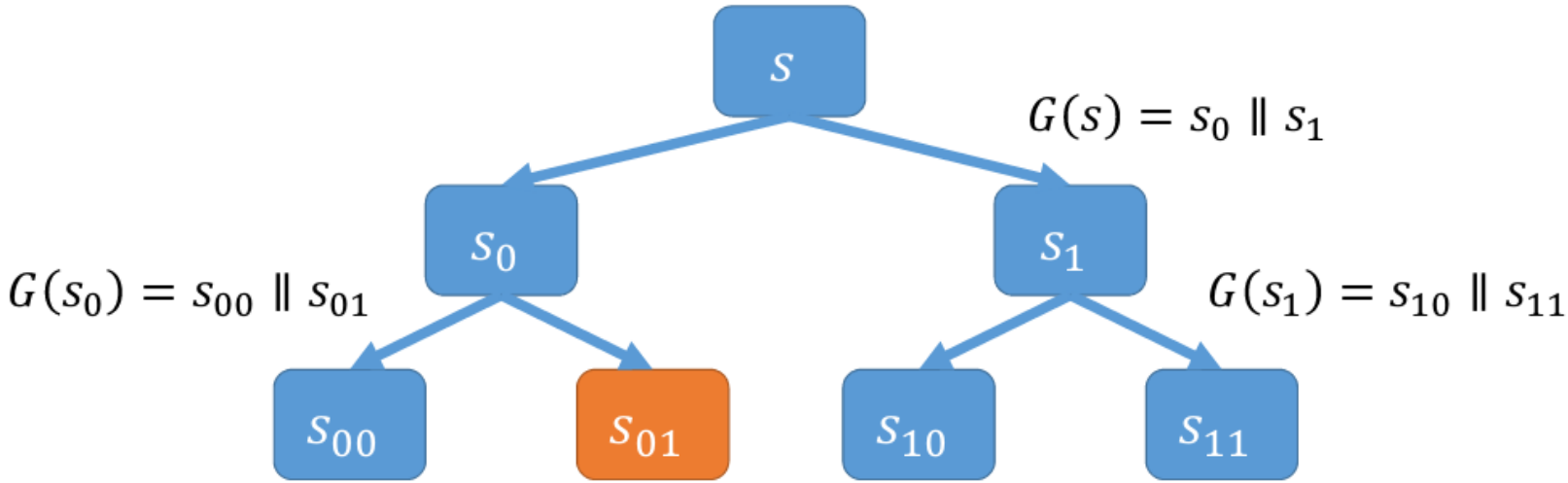
- π is a pseudorandom permutation.

- **HC** is a hardcore predicate.

Key-Injective PRFs

Building-block 2:

- a Key-Injective PRF via the GGM construction.



- Open problems: more efficient constructions from weaker assumptions.

Left/Right Collision-Resistant PRGs

Building-block 3:

- length doubling Left/Right Collision-Resistant PRGs.

$$\mathbf{PRG}_{\mathsf{LHalf}}(K) = \mathbf{PRG}_{\mathsf{LHalf}}(K') \Rightarrow K = K'$$

AND

$$\mathbf{PRG}_{\mathsf{RHalf}}(K) = \mathbf{PRG}_{\mathsf{RHalf}}(K') \Rightarrow K = K'$$

- Example:
  $G(x_1, x_2, x_3) := \left((g^{x_1}, g^{x_1 x_2}, g^{x_2 x_3}), (g^{x_2}, g^{x_1 x_3}, g^{x_3})\right)$

CROB transforms in the Standard Model

- Analogue of the ABN transform in the symmetric setting:
- **MAC** key is generated “on the fly”.
- **MAC** is collision-resistant.

Definition

$\overline{\mathbf{Enc}}(K_e, M)$:
$K_m \twoheadleftarrow \mathbf{Gen}_m(1^\lambda)$
$(K_e^1 || K_e^2) \leftarrow \mathbf{PRG}(K_e)$
$C \twoheadleftarrow \mathbf{Enc}(K_e^1, (M || K_m))$
$T \twoheadleftarrow \mathbf{Tag}(K_m, (C || K_e^2))$
return $(C || T)$

Summary

Robustness: { **AE**: ciphertext can't be decrypted wrt. different keys.
MAC: tag can't be validated under two different keys.

1. What goes wrong if the keys are adversarially generated.
2. Level of robustness achieved by AE/MAC schemes.
3. Generic transforms of AE schemes into CROB AE schemes.
4. How to construct collision-resistant PRFs

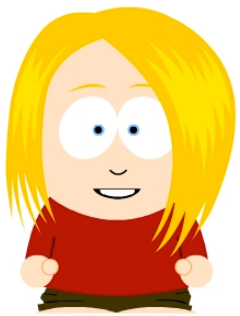
Summary

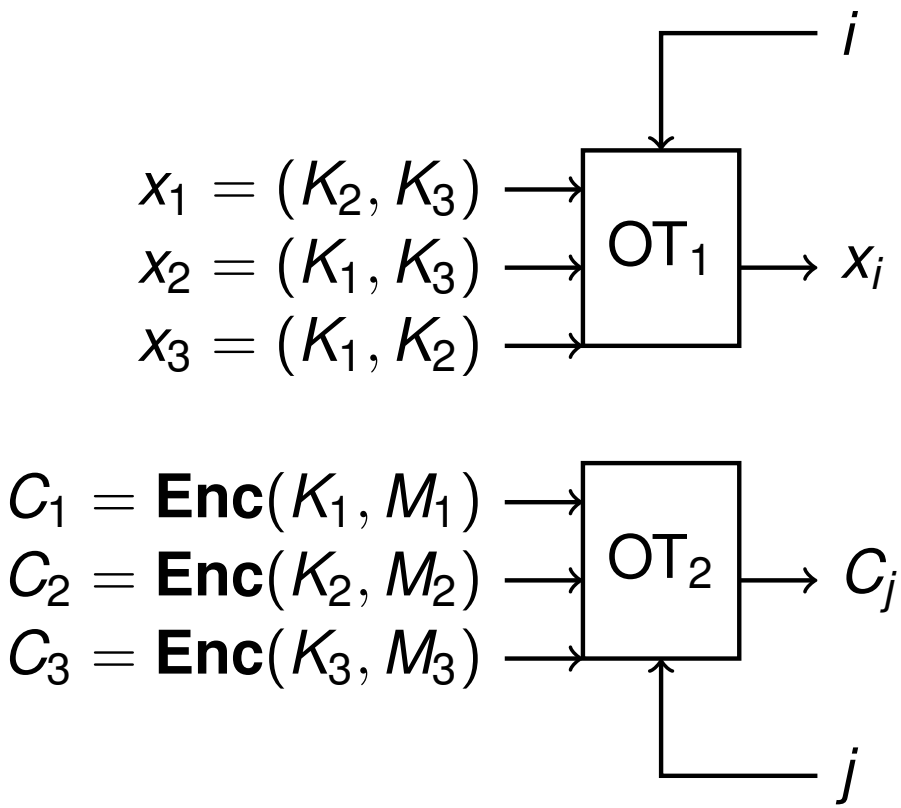
Robustness: { **AE**: ciphertext can't be decrypted wrt. different keys.
MAC: tag can't be validated under two different keys.

1. What goes wrong if the keys are adversarially generated.
2. Level of robustness achieved by AE/MAC schemes.
3. Generic transforms of AE schemes into CROB AE schemes.
4. How to construct collision-resistant PRFs

Motivating Key-Robustness - Example 3

Oblivious-Transfer protocol:

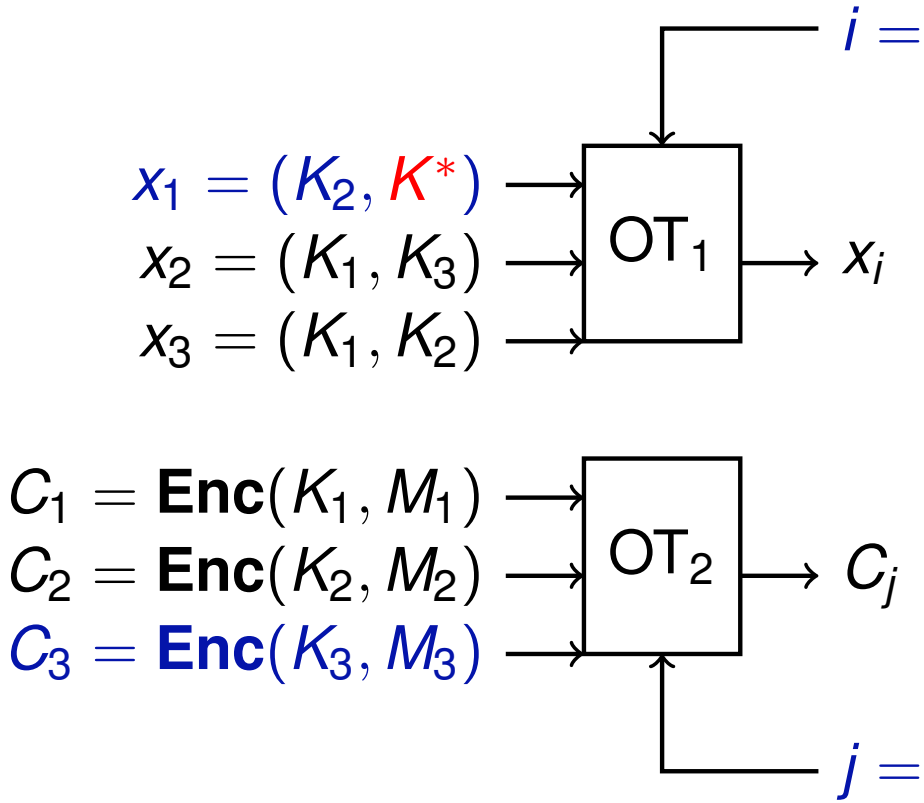




Motivating Key-Robustness - Example 3

Oblivious-Transfer protocol:

Malicious sender



$\mathbf{Dec}(K^*, C_3) = M^*$

Motivating Key-Robustness - Example 3

Oblivious-Transfer protocol:

Malicious sender

$i = 2$

$x_1 = (K_2, K^*)$

$x_2 = (K_1, K_3)$

$x_3 = (K_1, K_2)$

$\mathsf{OT}_1 \rightarrow x_i$

$C_1 = \mathbf{Enc}(K_1, M_1)$

$C_2 = \mathbf{Enc}(K_2, M_2)$

$C_3 = \mathbf{Enc}(K_3, M_3)$

$\mathsf{OT}_2 \rightarrow C_j$

$j = 3$

$\mathbf{Dec}(K_3, C_3) = M_3$