Multi-Instance Secure Public-Key Encryption

Hans Heum

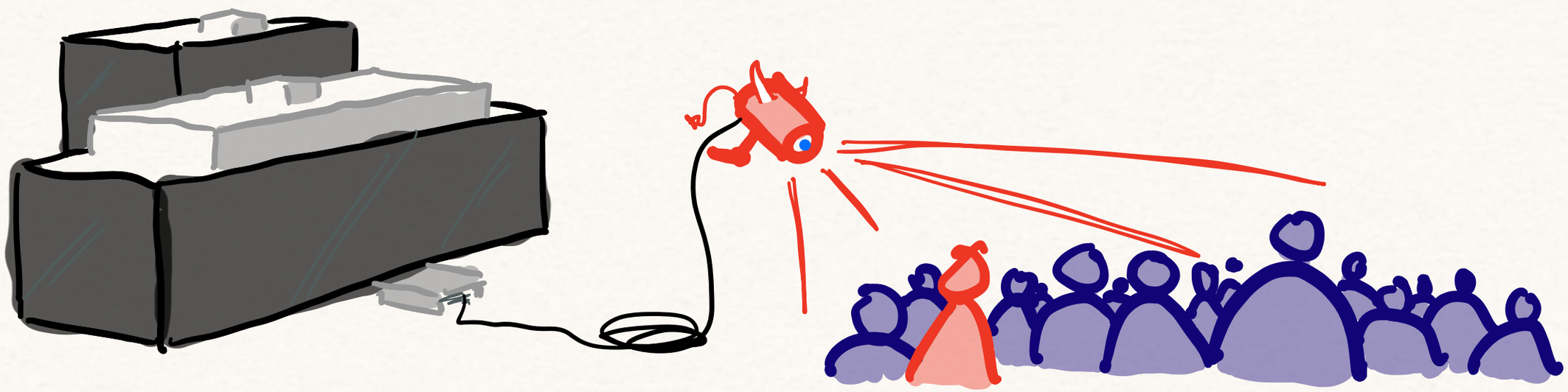
NTNU

with Carlo Brunetta and Martijn Stam

Simula UiB

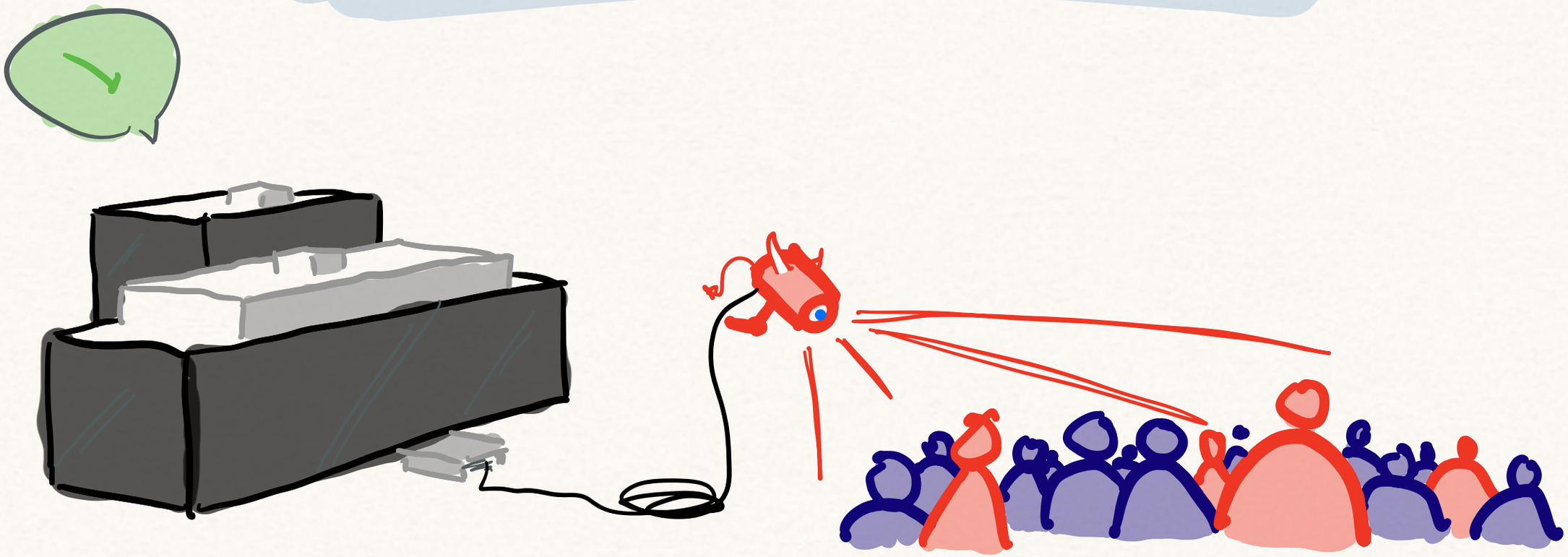
The Multi-Instance Setting

Bellare, Ristenpart, Tessaro (Crypto'12)



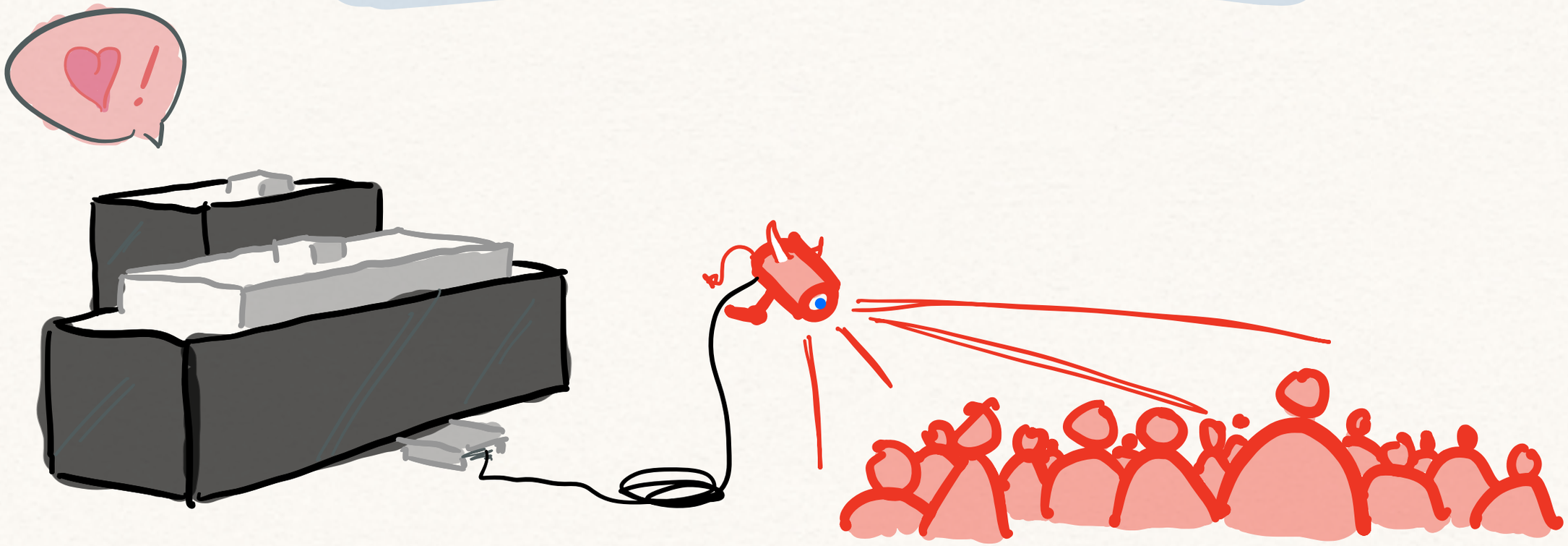
The Multi-Instance Setting

Bellare, Ristenpart, Tessaro (Crypto'12)



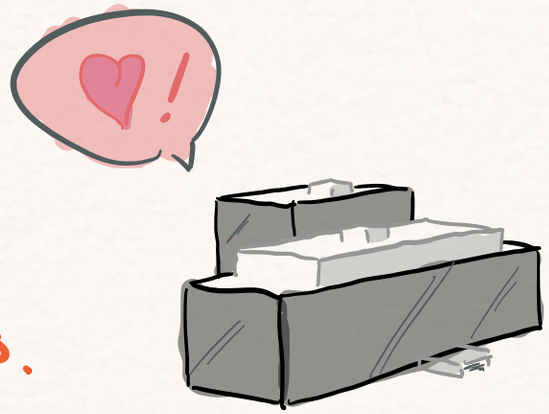
The Multi-Instance Setting

Bellare, Ristenpart, Tessaro (Crypto'12)



AUERBACH, GIACON, KILZ (EC'20):

EXIST KEM SCHEMES SUCH THAT:

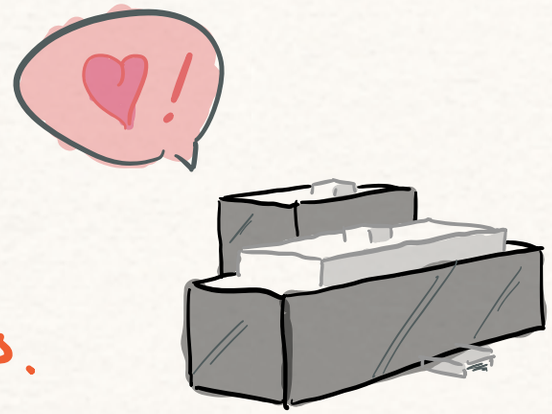


PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING 1 USER $\Rightarrow$ SUFFICIENT TO BREAK <u>ALL</u> USERS.

AUERBACH, GIACON, KILZ (EC'20):

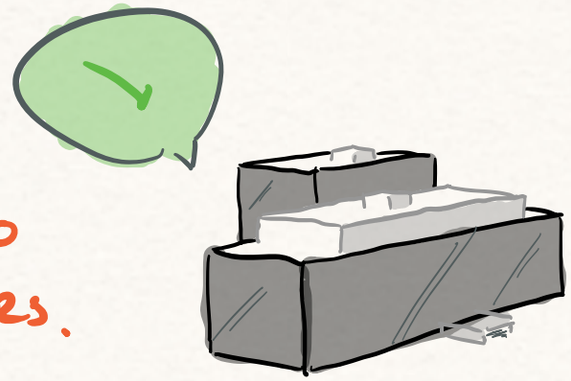
EXIST KEM SCHEMES SUCH THAT:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING 1 USER $\Rightarrow$ SUFFICIENT TO BREAK **ALL** USERS.



MANY KEM SCHEMES:

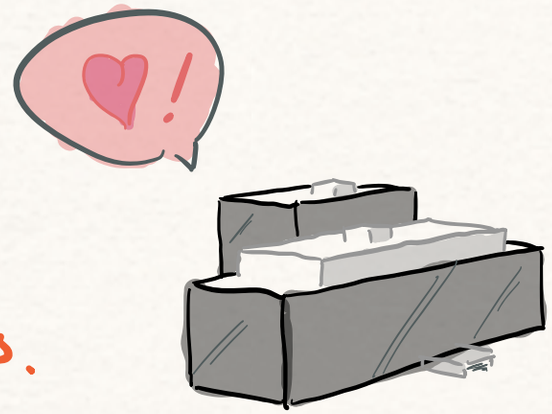
PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS $\Rightarrow$ SUFFICIENT TO BREAK n^2 USERS.



AUERBACH, GIACON, KILZ (EC'20):

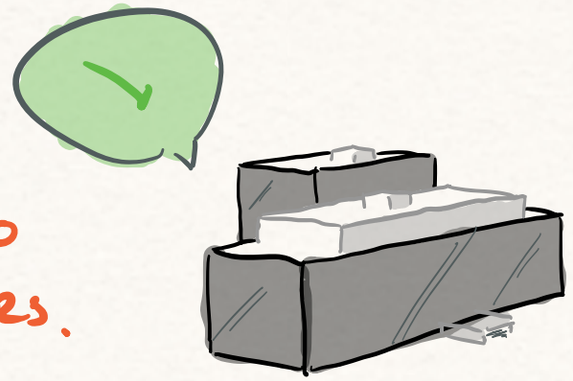
EXIST KEM SCHEMES SUCH THAT:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING 1 USER $\Rightarrow$ SUFFICIENT TO BREAK **ALL** USERS.



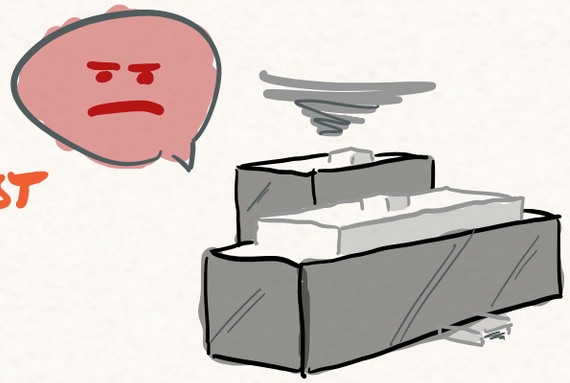
MANY KEM SCHEMES:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS $\Rightarrow$ SUFFICIENT TO BREAK n^2 USERS.



WANT PKE SCHEME S.TH.:

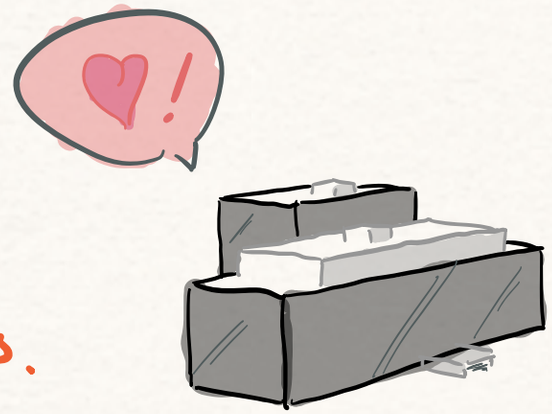
PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS $\Rightarrow$ BREAKS AT MOST n USERS.



AUERBACH, GIACON, KILZ (EC'20):

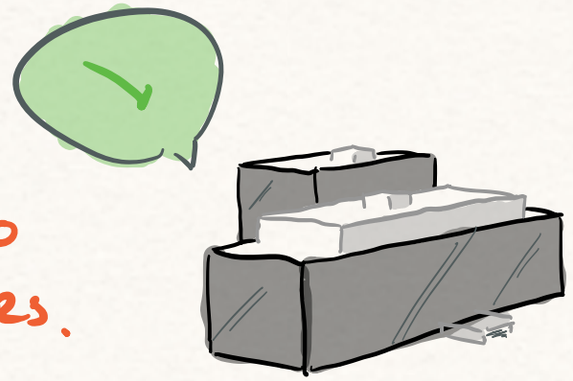
EXIST KEM SCHEMES SUCH THAT:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING 1 USER $\Rightarrow$ SUFFICIENT TO BREAK **ALL** USERS.



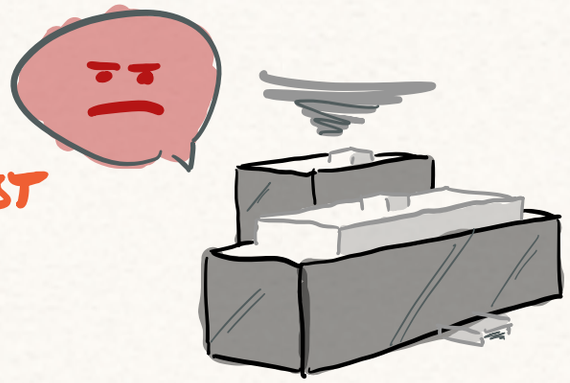
MANY KEM SCHEMES:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS $\Rightarrow$ SUFFICIENT TO BREAK n^2 USERS.



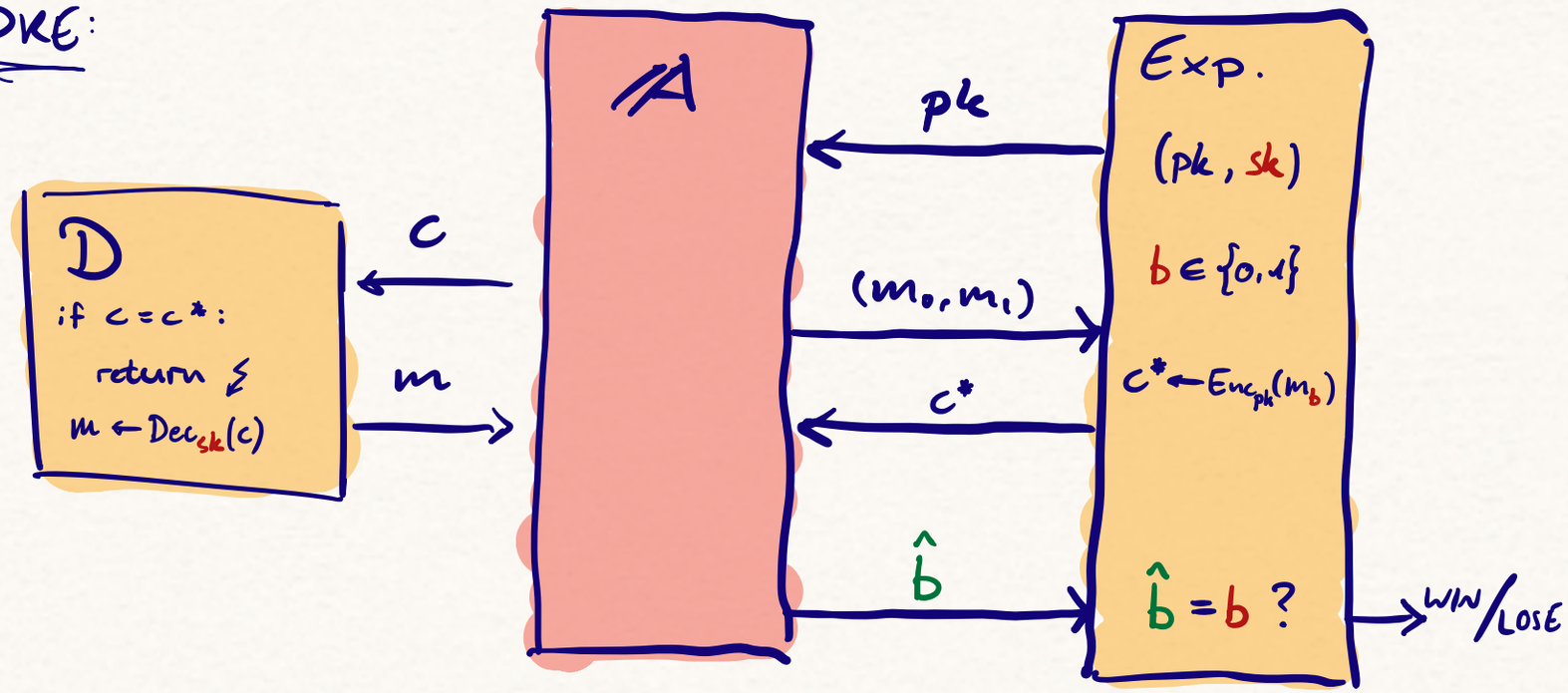
WANT PKE SCHEME S.TH.:

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS $\Rightarrow$ BREAKS AT MOST n USERS.

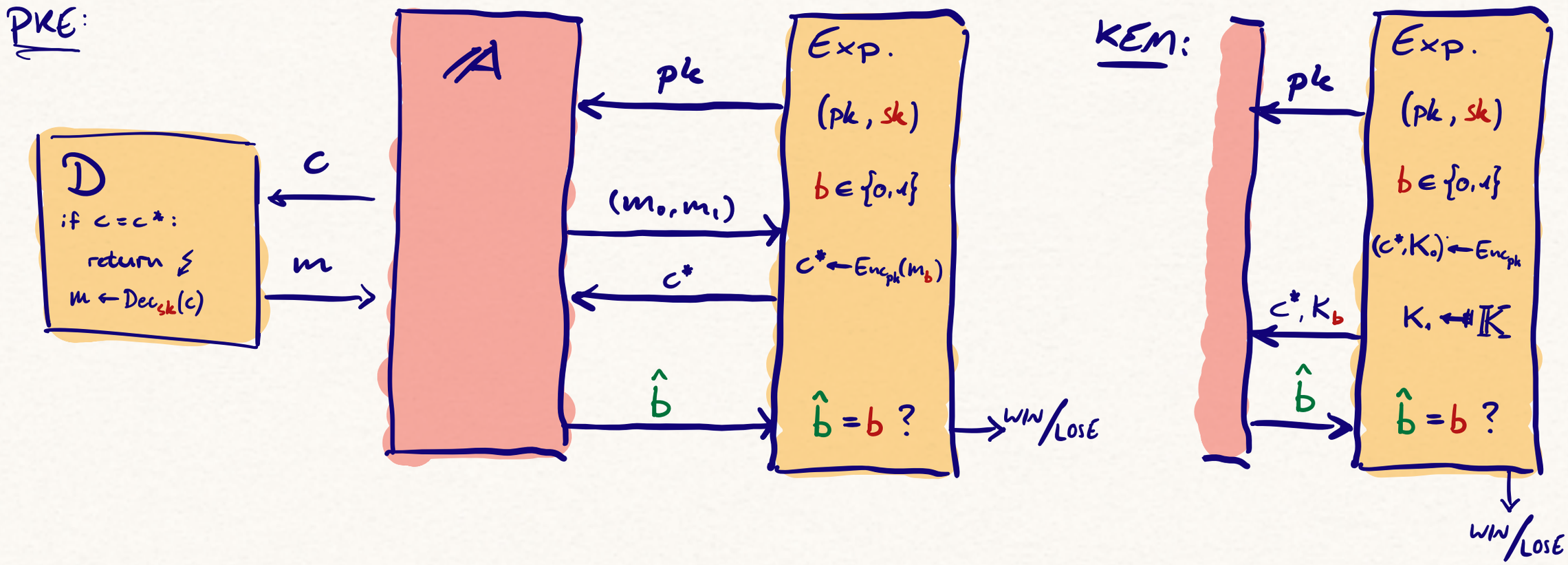


THE SINGLE-INSTANCE IND-CCA EXPERIMENTS:

PKE:

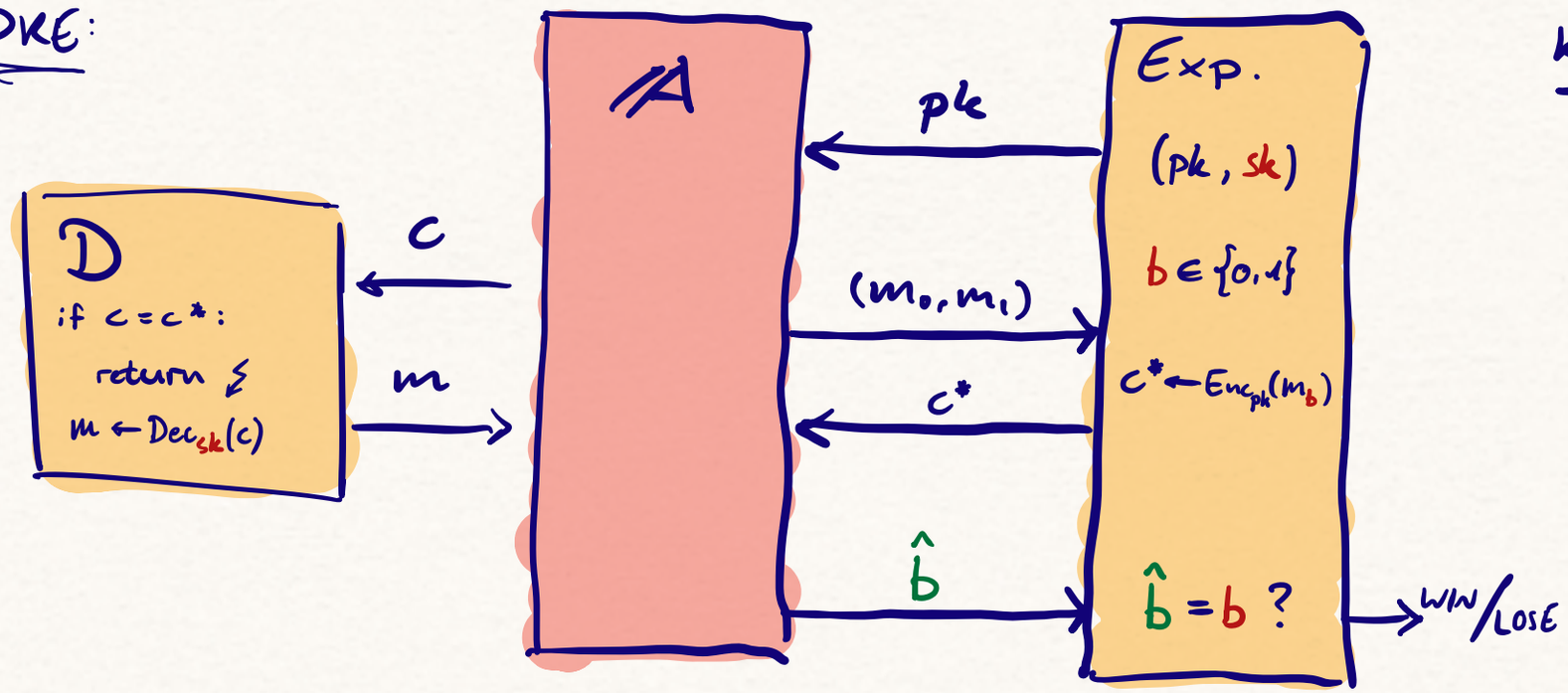


THE SINGLE-INSTANCE IND-CCA EXPERIMENTS:

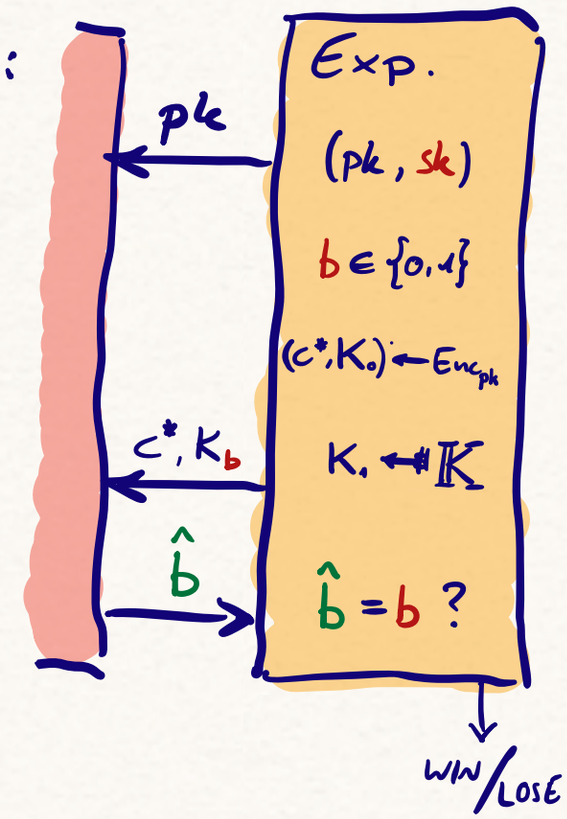


THE SINGLE-INSTANCE IND-CCA EXPERIMENTS:

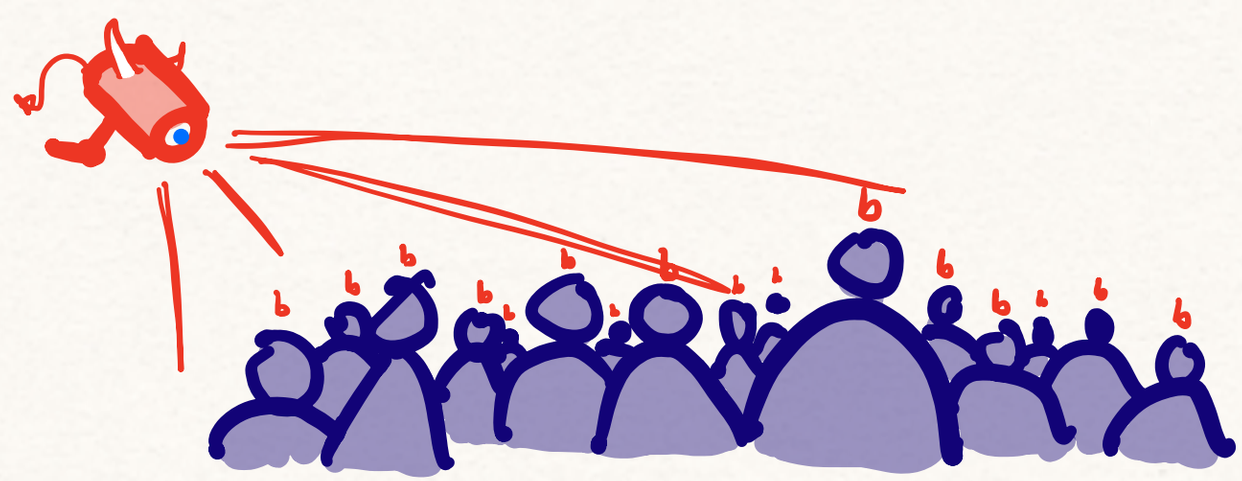
PKE:



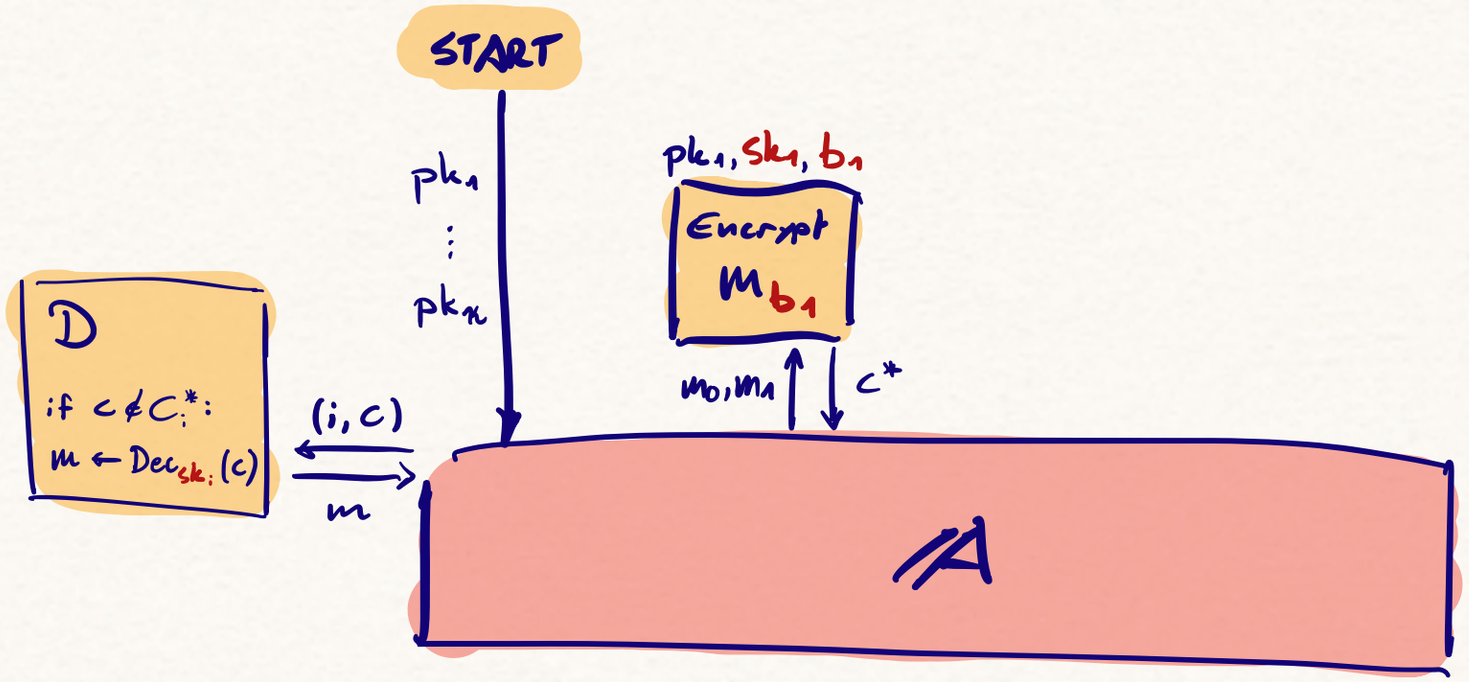
KEM:



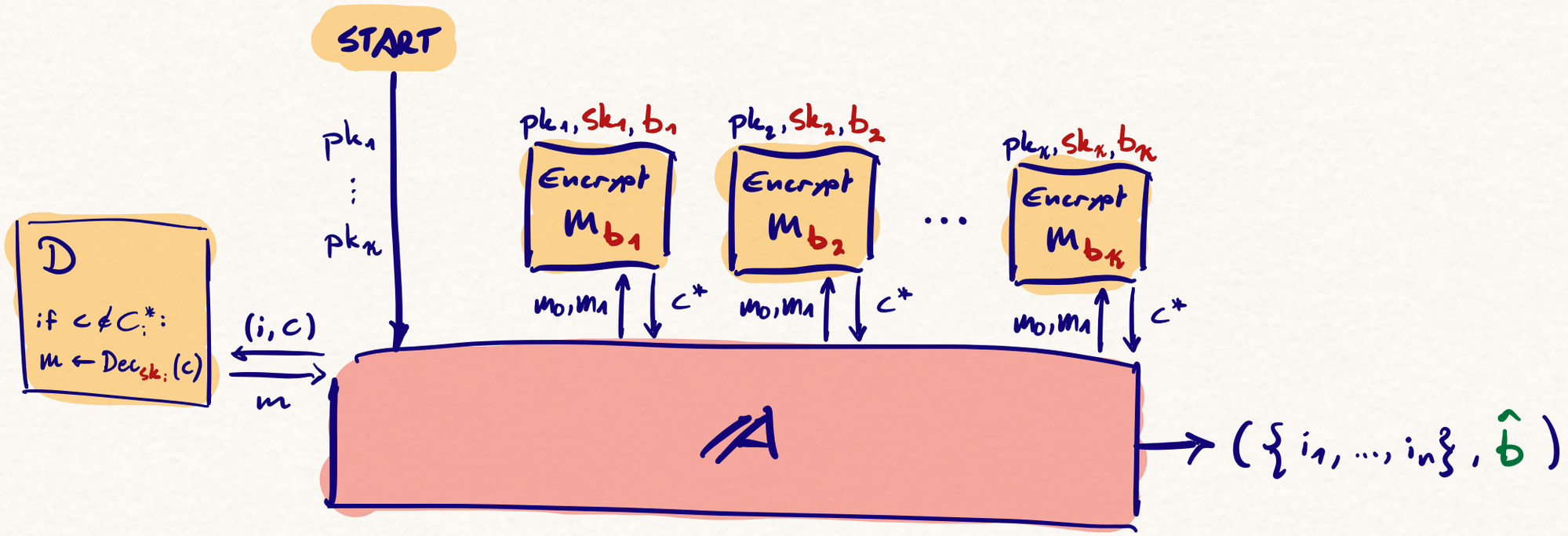
MULTI-USER SECURITY:

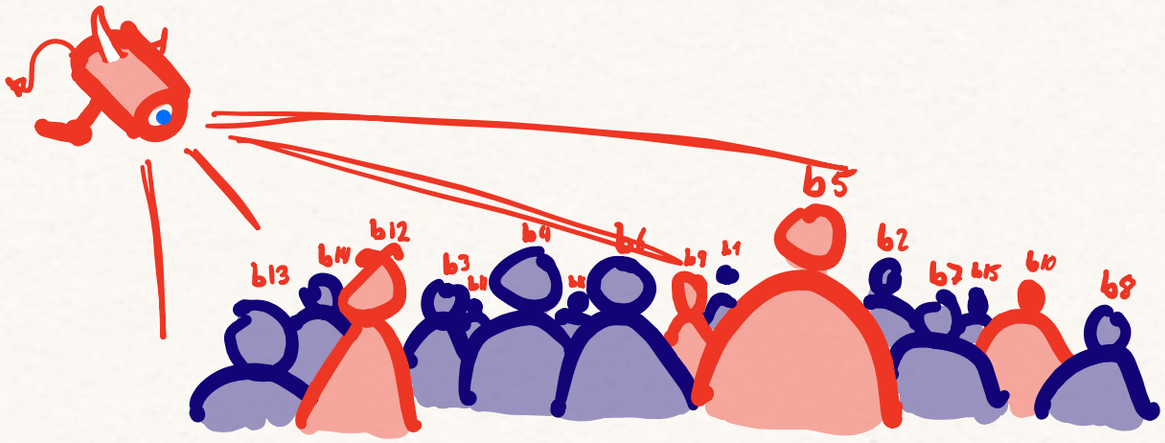


(n-OUT-OF-n) MI-IND-CCA FOR PKE

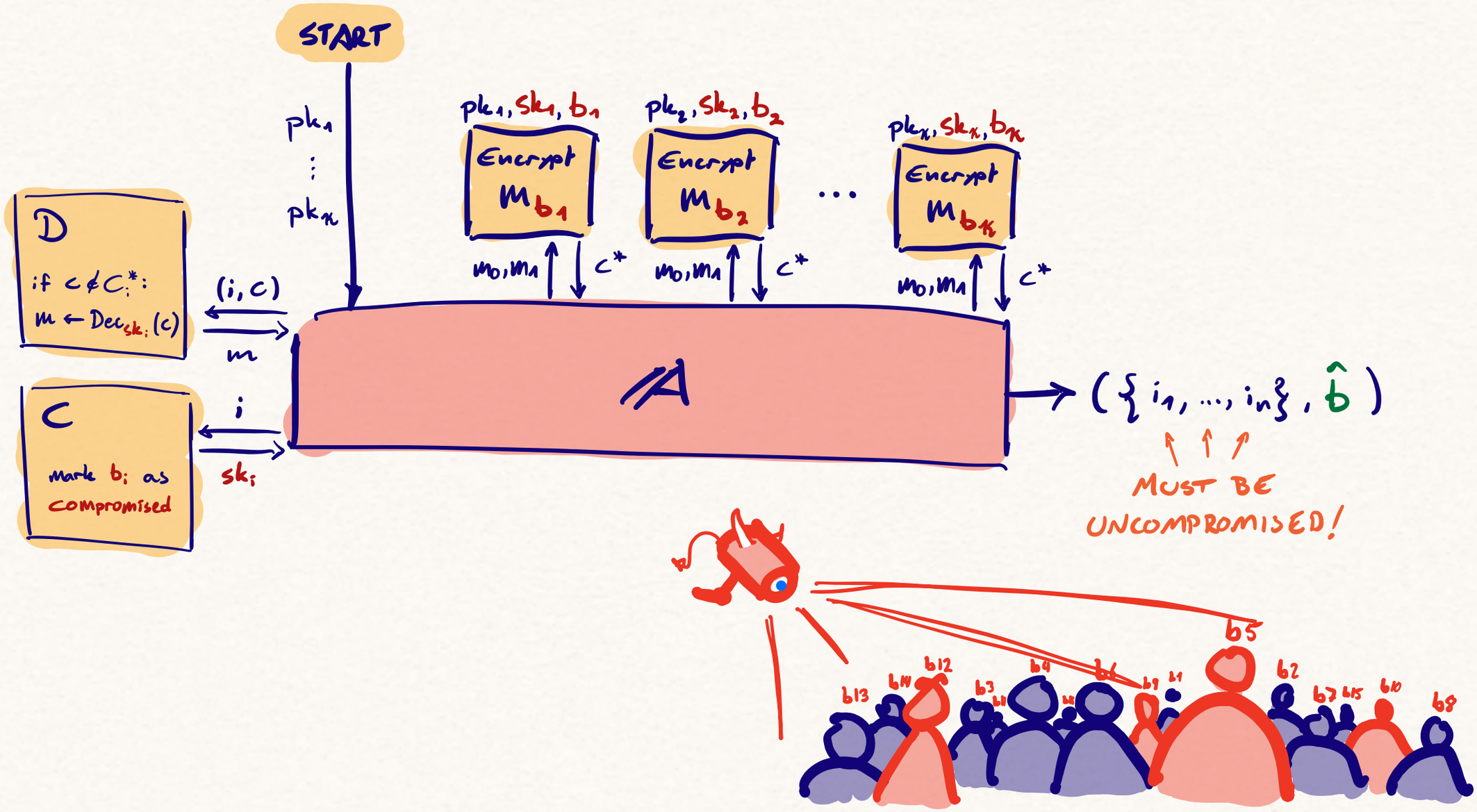


(n-OUT-OF-κ) MI-IND-CCA FOR PKE

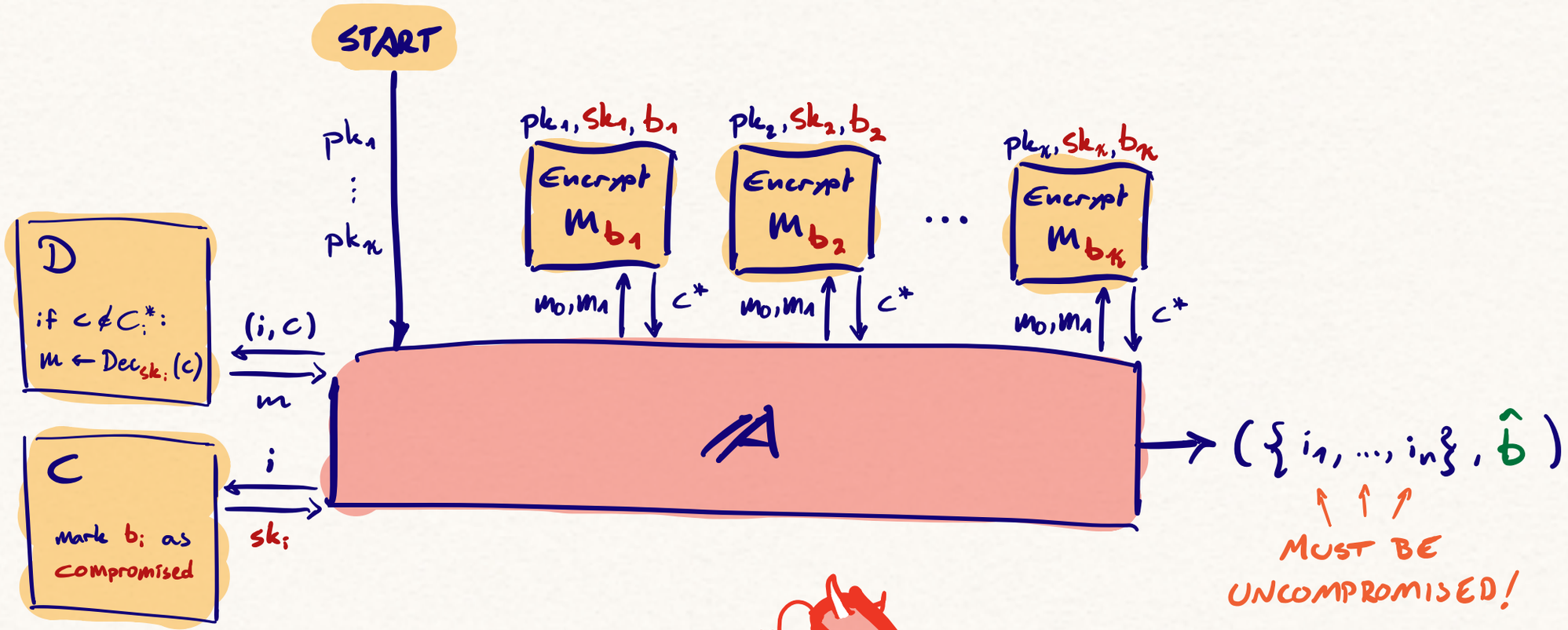




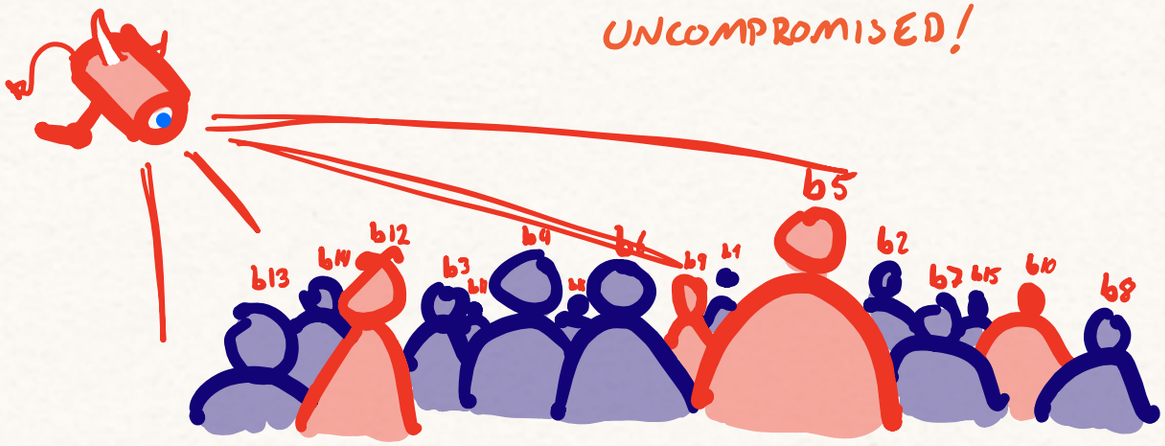
(n-OUT-OF-k) MI-IND-CCA FOR PKE



(n-OUT-OF-k) MI-IND-CCA FOR PKE



WW IF: $\hat{b} = b_{i_1} \oplus b_{i_2} \oplus \dots \oplus b_{i_n}$



Hybrid Encryption

e.g. AES

Cramer-Shoup (2003): KEM + DEM $\Rightarrow$ PKE

IND-CCA OT-IND-CCA IND-CCA

(almost) tightly!

Hybrid Encryption

e.g. AES

Cramer-Shoup (2003): KEM + DEM $\Rightarrow$ PKE

IND-CCA OT-IND-CCA IND-CCA

(almost) tightly!

AGK (EC'20): KEM with good MI-security

pre-computation equivalent to brute-forcing n users $\Rightarrow$ breaks at most n users.

Hybrid Encryption

Cramer-Shoup (2003): KEM + DEM ⇒ PKE

IND-CCA OT-IND-CCA IND-CCA

e.g. AES

(almost) tightly!

AGK (EC'20): KEM with good MI-security

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS ⇒ BREAKS AT MOST n USERS.

PKE with good MI-security?

Hybrid Encryption

Cramer-Shoup (2003): KEM + DEM ⇒ PKE

IND-CCA OT-IND-CCA IND-CCA

e.g. AES

(almost) tightly!

AGK (EC'20): KEM with good MI-security

PRE-COMPUTATION EQUIVALENT TO BRUTE-FORCING n USERS ⇒ BREAKS AT MOST n USERS.

PKE with good MI-security?

Nope!

Initial Attempts

1. KEM + DEM $\Rightarrow$ PKE ?

MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE ?

   MI-IND-CCA OT-INF.TH.-CPA MI-IND-CCA

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CPA MI-IND-CCA ✗

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CPA

   $\hookrightarrow$ MI-IND-CCA ✗

   $\hookrightarrow$ MI-ROR-CCA ✓

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE

MI-IND-CCA OT-INF.TH.-CPA

↳ MI-IND-CCA ✗

↳ MI-ROR-CCA ✓

Single-instance: $\text{ROR-CCA}_{\text{PKE}} \xrightarrow{\cdot 2} \text{IND-CCA}_{\text{PKE}}$

Multi-instance:

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE

   MI-IND-CCA OT-INF.TH.-CPA

   $\hookrightarrow$ MI-IND-CCA ✗

   $\hookrightarrow$ MI-ROR-CCA ✓

Single-instance: $\text{ROR-CCA}_{\text{PKE}} \xrightarrow{\cdot 2} \text{IND-CCA}_{\text{PKE}}$

Multi-instance: $\text{ROR-CCA}_{\text{PKE}} \xrightarrow{\cdot \binom{\kappa}{n} \cdot 2^n} \text{IND-CCA}_{\text{PKE}}$

Initial Attempts

1. KEM + DEM $\not\Rightarrow$ PKE

MI-IND-CCA OT-INF.TH.-CCA MI-IND-CCA

2. TagKEM + OTP $\Rightarrow$ PKE

MI-IND-CCA OT-INF.TH.-CPA

↳ MI-IND-CCA ✗

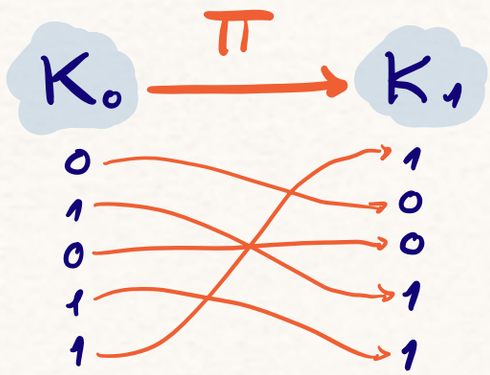
↳ MI-ROR-CCA ✓

SINGLE-INSTANCE: $\text{ROR-CCA}_{\text{PKE}} \xrightarrow{\cdot 2} \text{IND-CCA}_{\text{PKE}}$

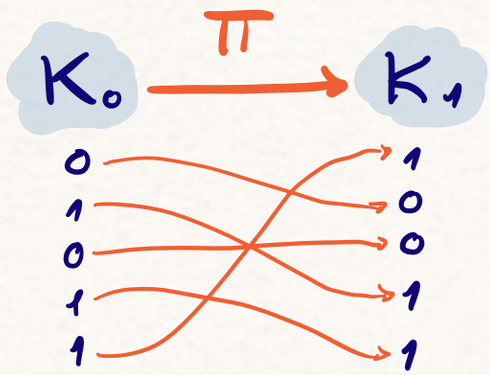
MULTI-INSTANCE: $\text{ROR-CCA}_{\text{PKE}} \xrightarrow{\cdot \binom{\kappa}{n} \cdot 2^n} \text{IND-CCA}_{\text{PKE}}$

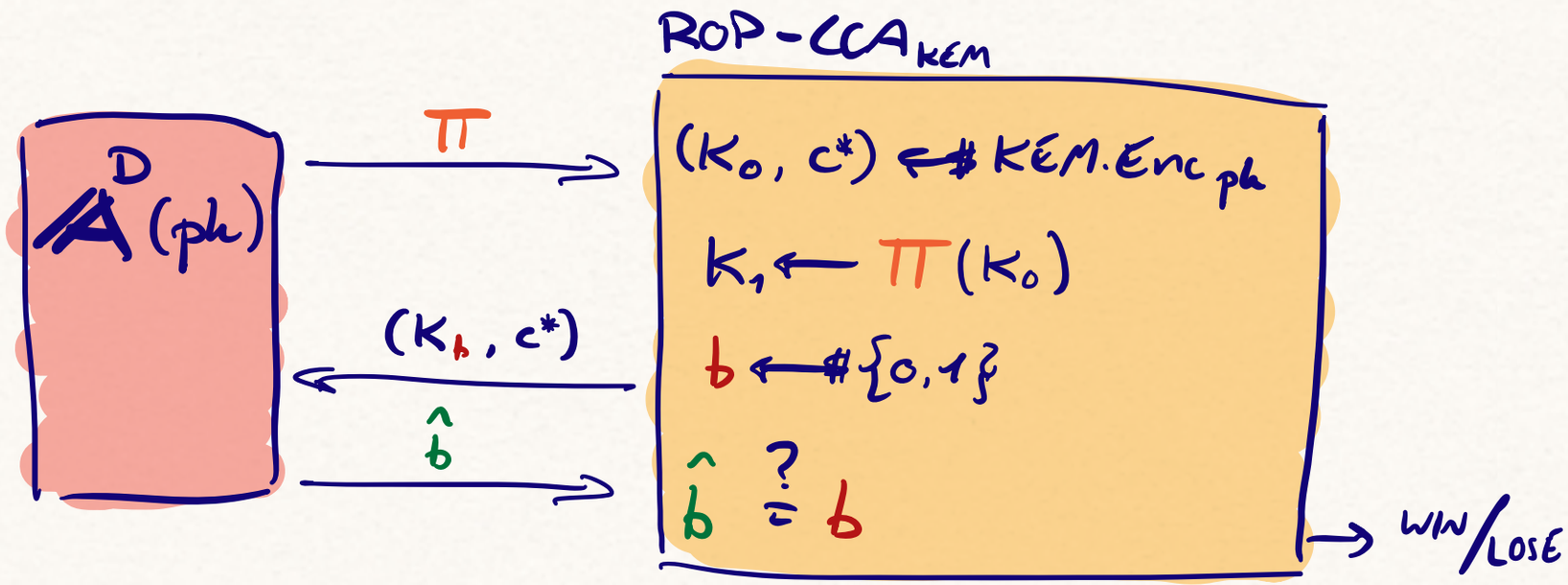
NEED A MORE DIRECT ROUTE ...

NEW KEM NOTION: REAL-OR-PERMUTED

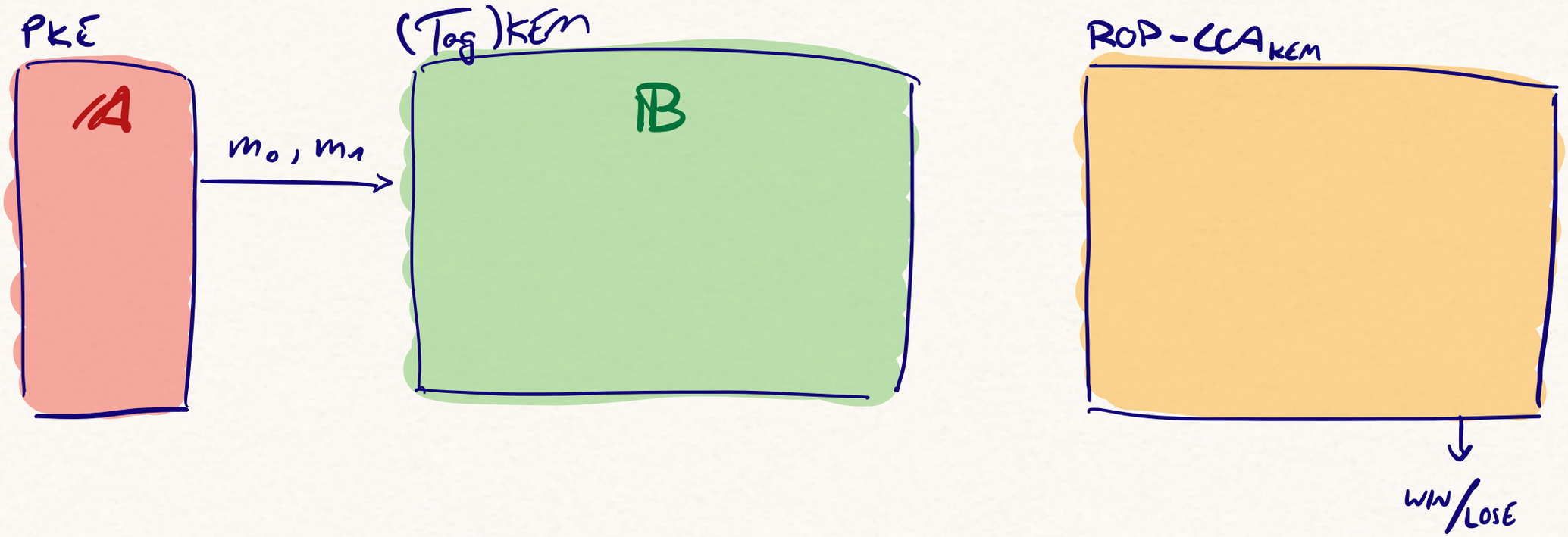


NEW KEM NOTION: REAL-OR-PERMUTED

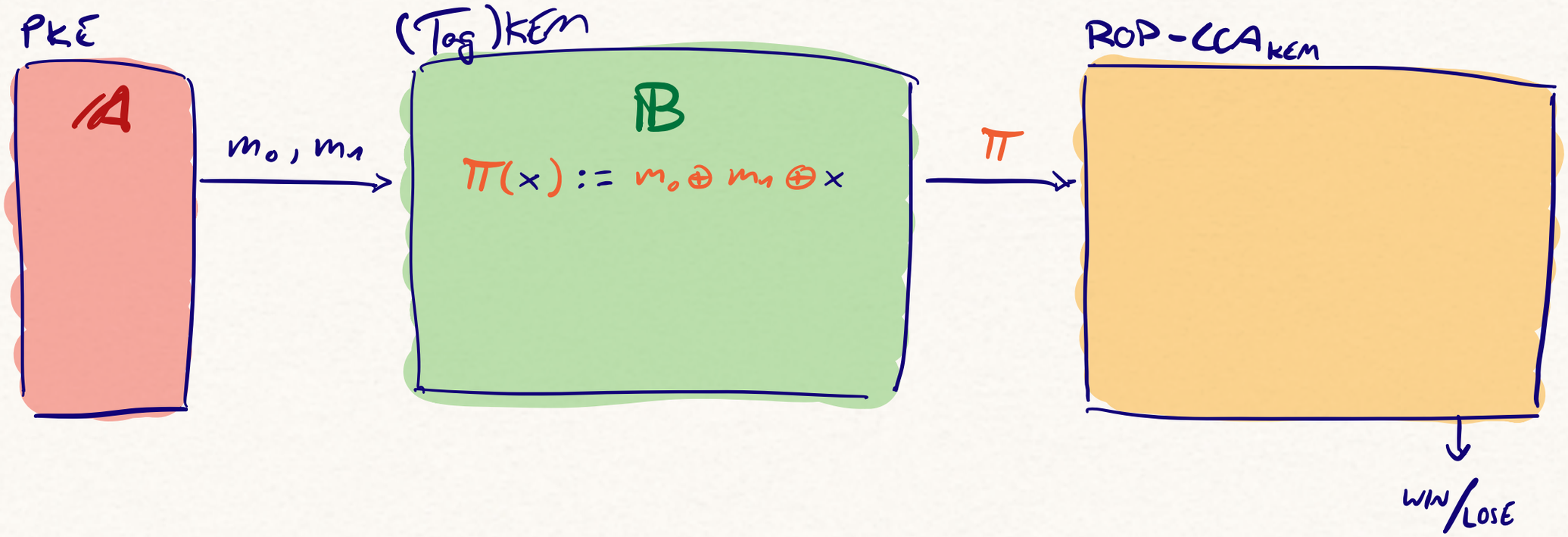




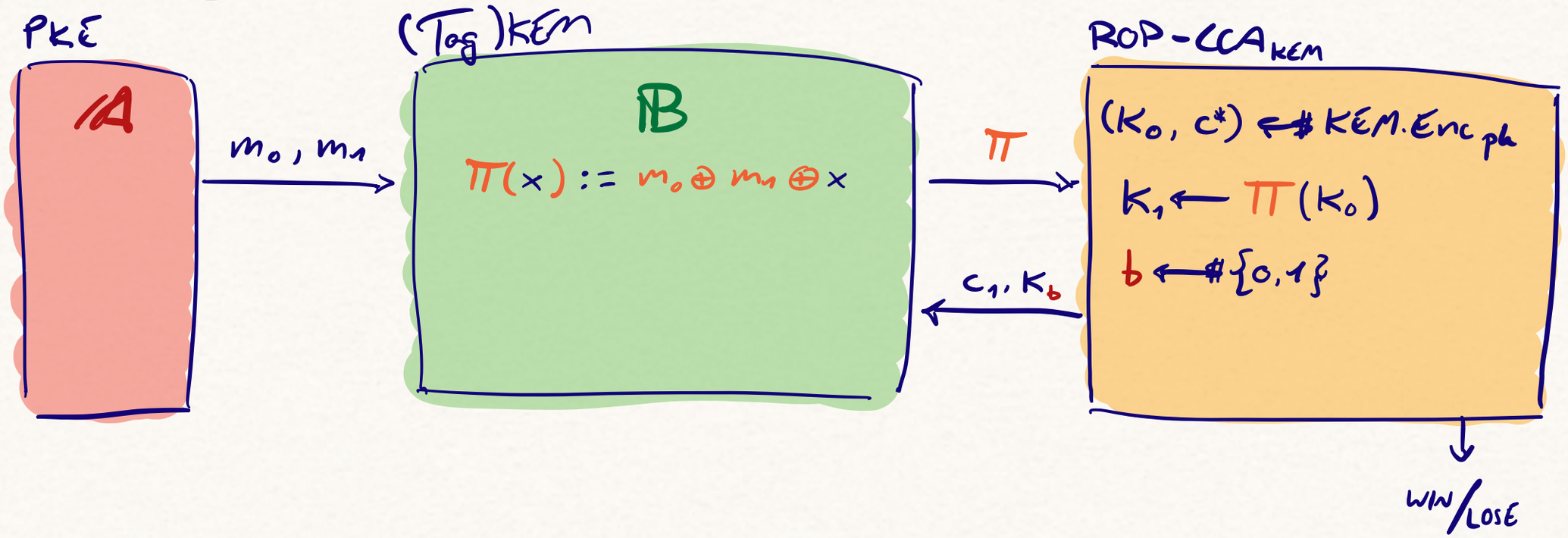
Simulating Left-or-Right IND-CCA



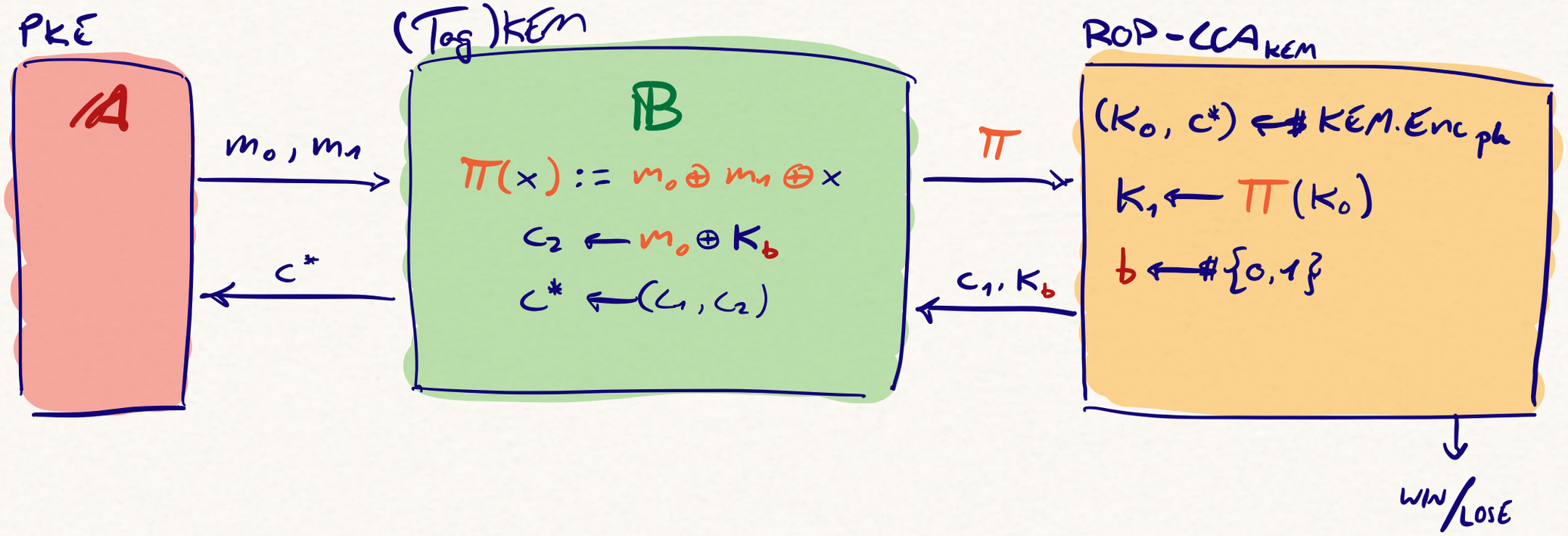
Simulating Left-or-Right IND-CCA



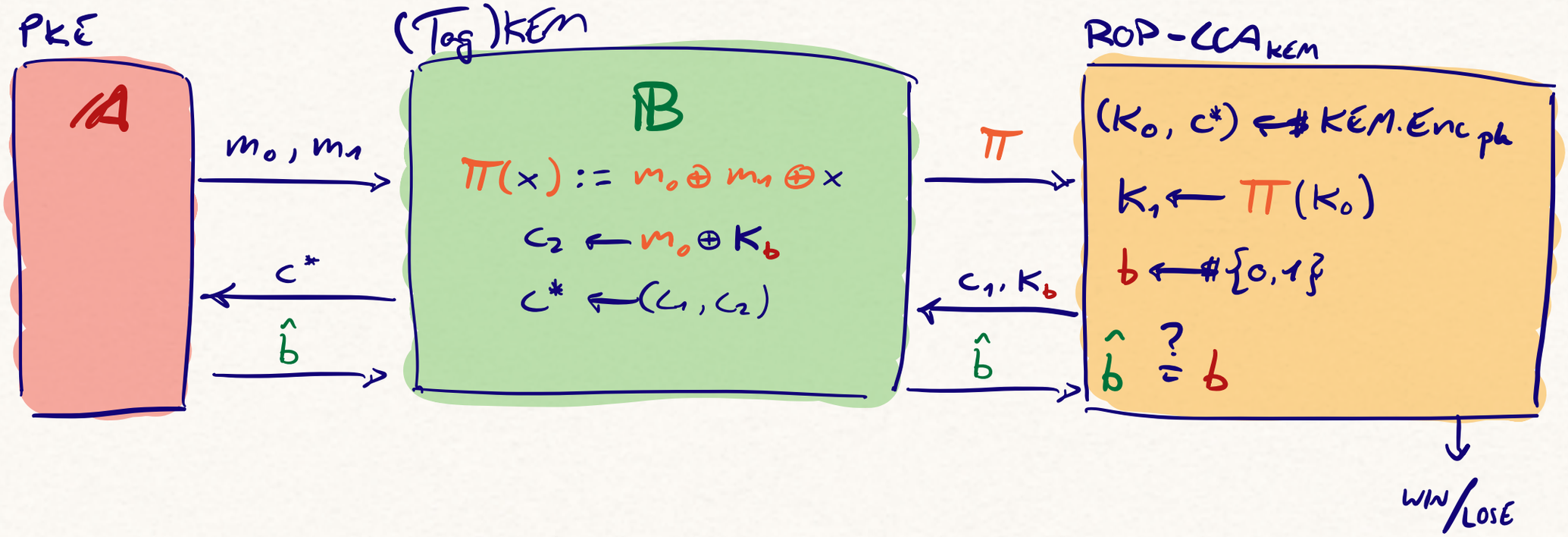
Simulating Left-or-Right IND-CCA



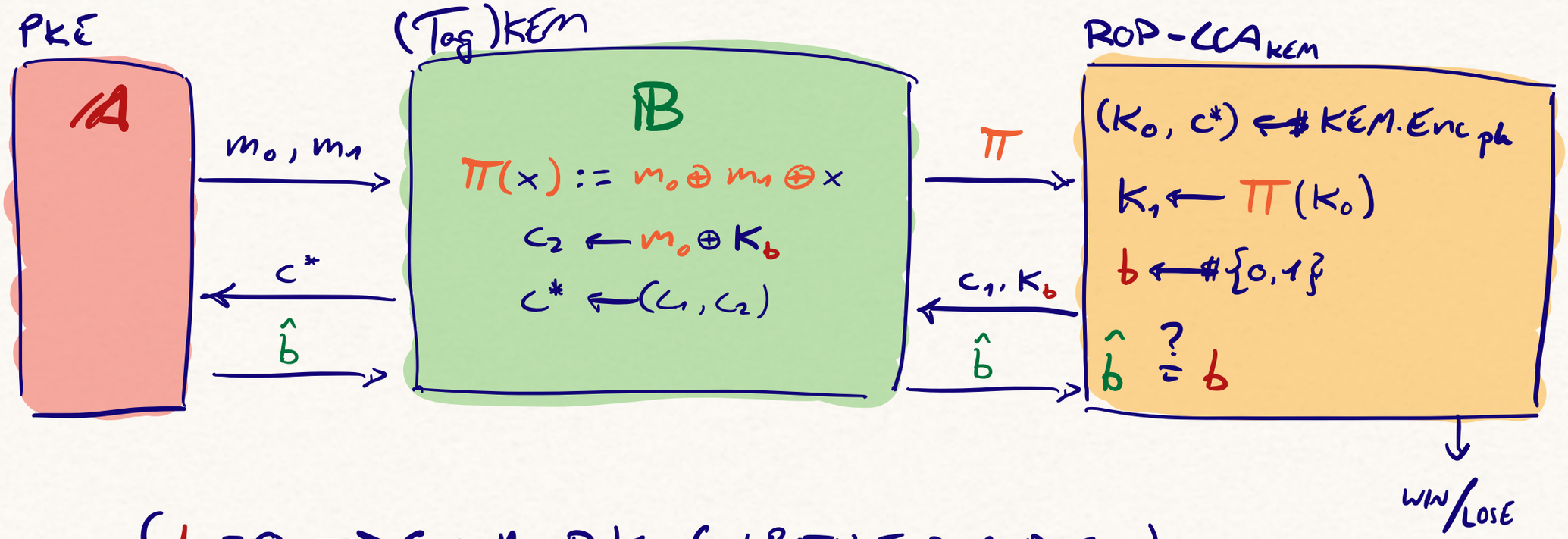
Simulating Left-or-Right IND-CCA



Simulating Left-or-Right IND-CCA

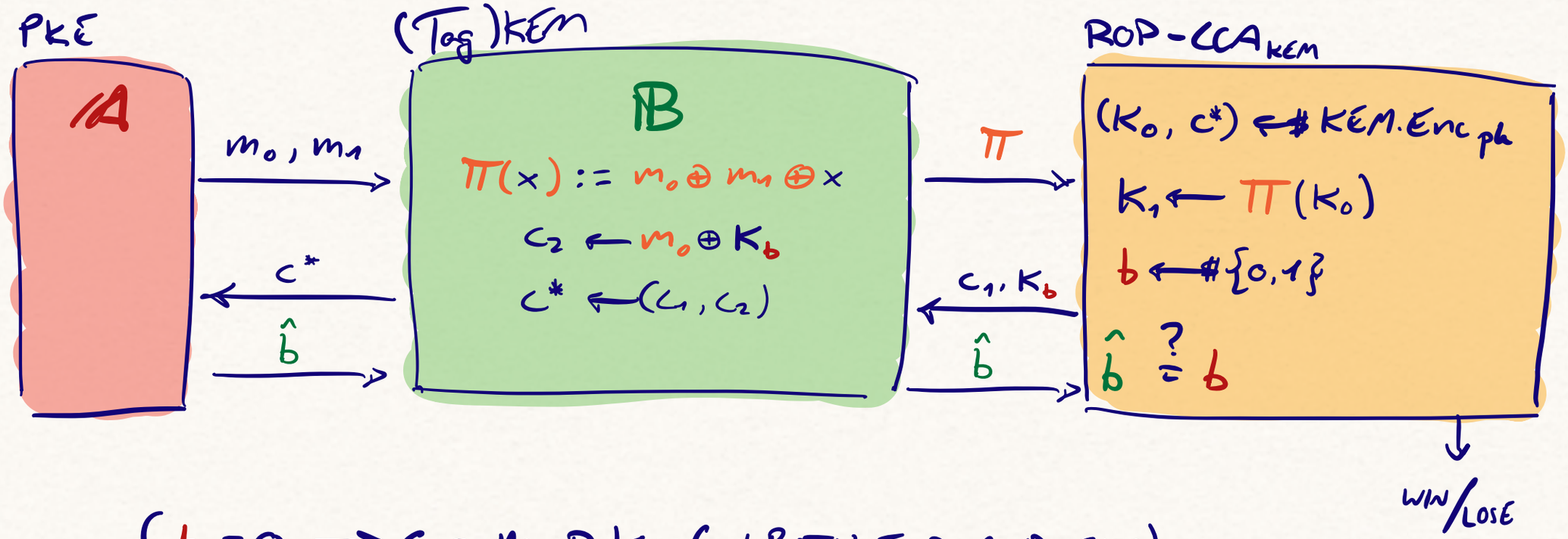


Simulating Left-or-Right IND-CCA



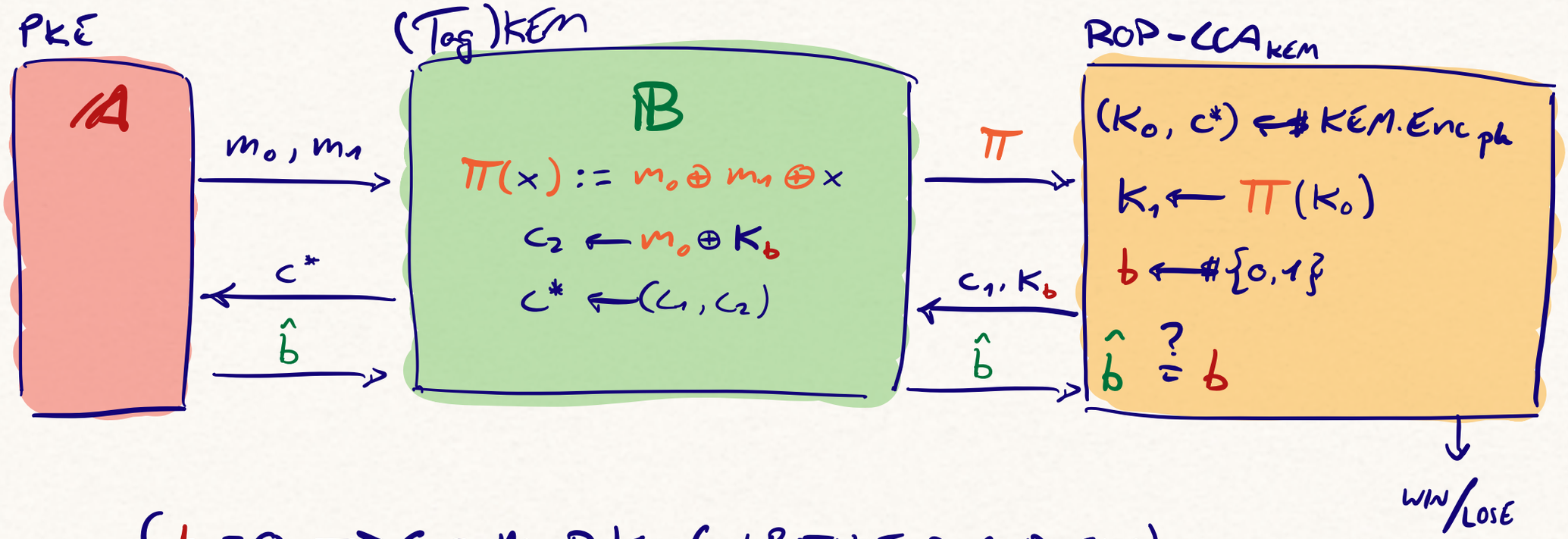
$\Longrightarrow$ $\left\{ b = 0 \longrightarrow c_2 = m_0 \oplus K_0 \text{ (IN BOTH EXP. AND SIM)} \right.$

Simulating Left-or-Right IND-CCA



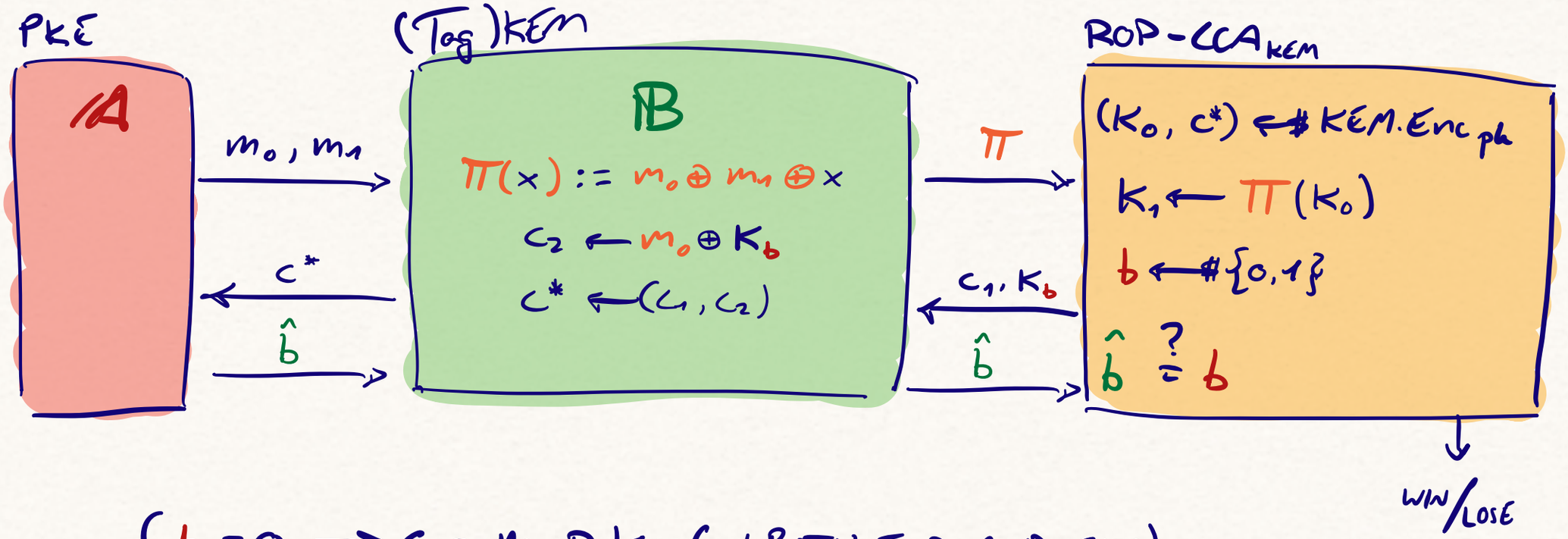
$$\Longrightarrow \begin{cases} b = 0 \longrightarrow c_2 = m_0 \oplus K_0 \text{ (IN BOTH EXP. AND SIM)} \\ b = 1 \begin{cases} \text{IND-CCA}: c_2 = m_1 \oplus K_0 \\ \text{SIM}: c_2 = m_0 \oplus K_1 \end{cases} \end{cases}$$

Simulating Left-or-Right IND-CCA



$$\Longrightarrow \begin{cases} b = 0 \longrightarrow c_2 = m_0 \oplus K_0 \text{ (IN BOTH EXP. AND SIM)} \\ b = 1 \begin{cases} \text{IND-CCA}: c_2 = m_1 \oplus K_0 \\ \text{SIM}: c_2 = m_0 \oplus K_1 = m_0 \oplus \pi(K_0) = m_0 \oplus m_0 \oplus m_1 \oplus K_0 \end{cases} \end{cases}$$

Simulating Left-or-Right IND-CCA



$$\Longrightarrow \begin{cases} b = 0 \longrightarrow c_2 = m_0 \oplus K_0 \text{ (IN BOTH EXP. AND SIM)} \\ b = 1 \begin{cases} \text{IND-CCA}: c_2 = m_1 \oplus K_0 \\ \text{SIM}: c_2 = m_0 \oplus K_1 = m_0 \oplus \pi(K_0) = \cancel{m_0} \oplus \cancel{m_0} \oplus m_1 \oplus K_0 = m_1 \oplus K_0 \end{cases} \end{cases}$$

3rd Attempt

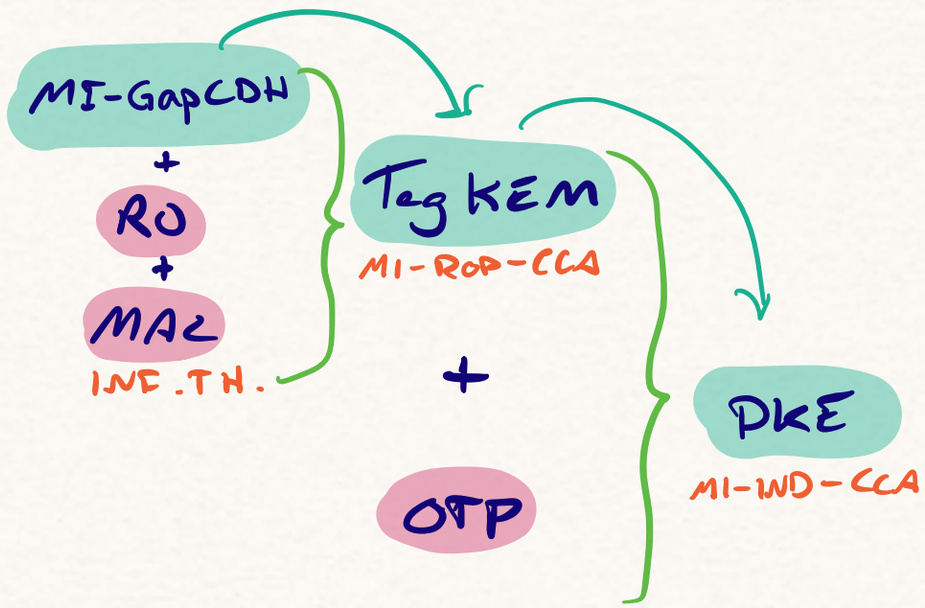
3. TagKEM + OTP ⇒ PKE ✓

MI-ROP-CCA OT-INF.TH.-CPA MI-IND-CCA

3rd Attempt

3. TagKEM + OTP ⇒ PKE

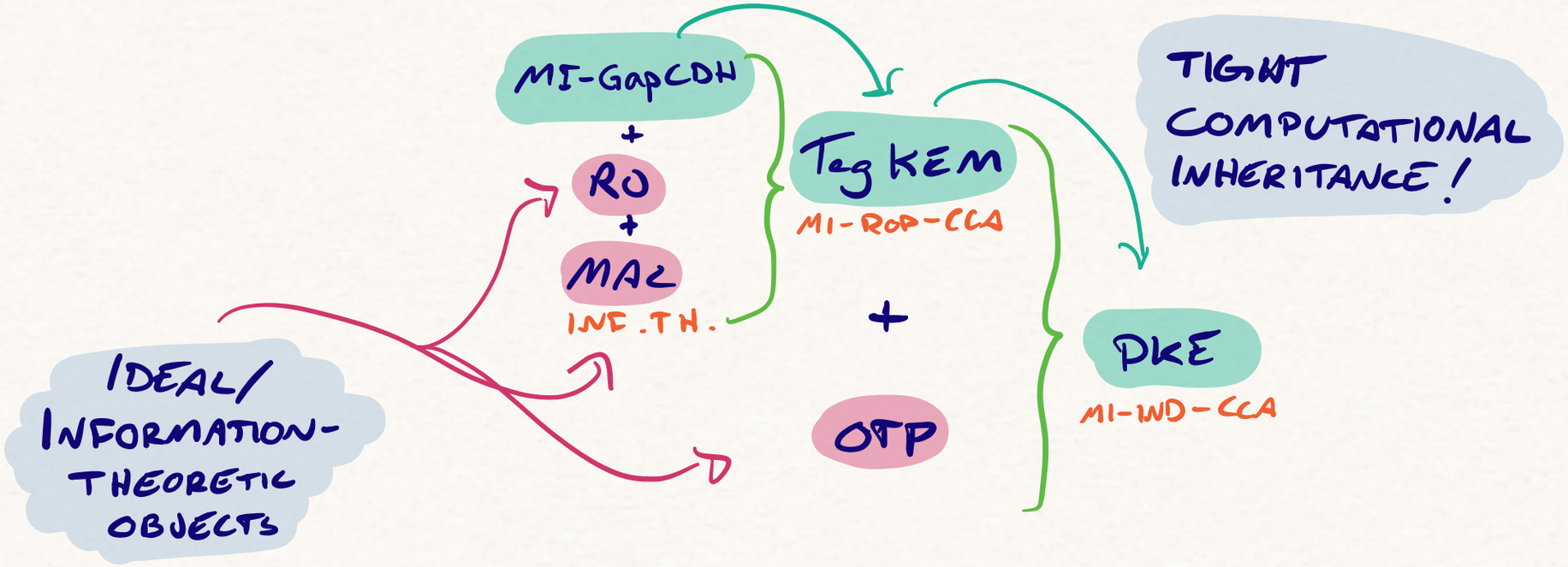
MI-ROP-CCA OT-INF.TH.-CPA MI-IND-CCA



3rd Attempt

3. TagKEM + OTP ⇒ PKE

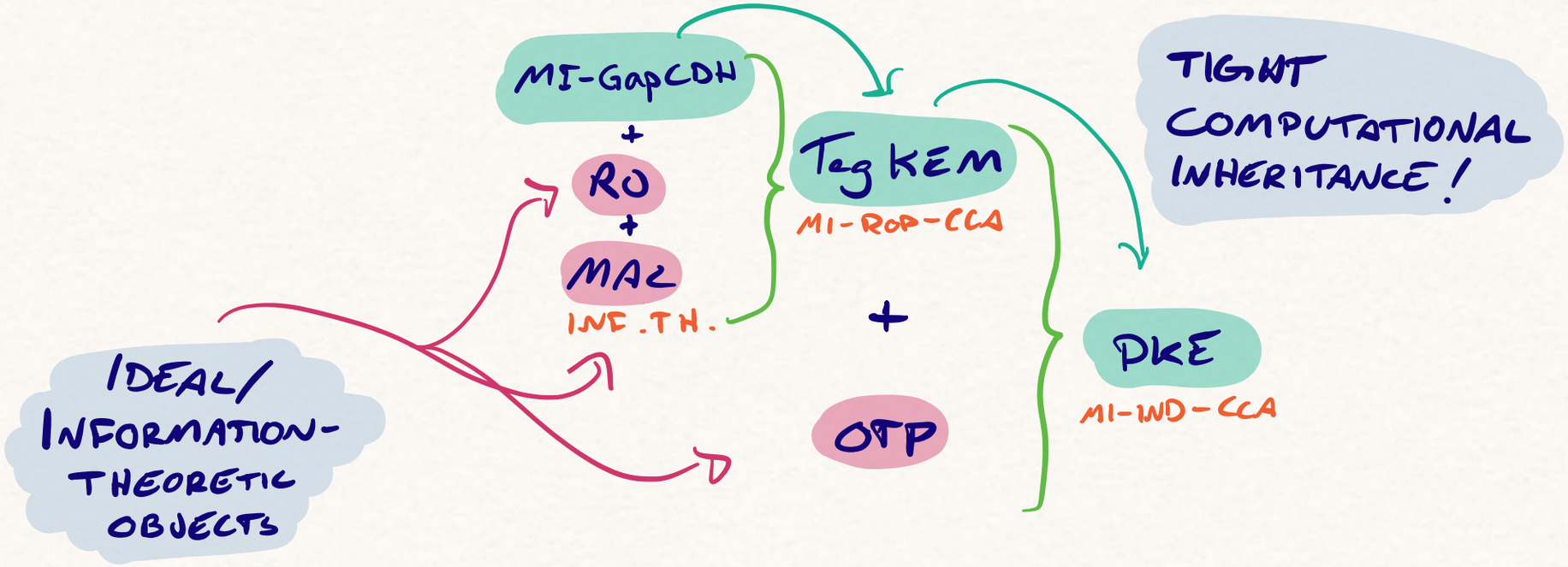
MI-ROP-CCA OT-INF.TH.-CPA MI-IND-CCA



3rd Attempt

3. TagKEM + OTP ⇒ PKE

MI-ROP-CCA OT-INF.TH.-CPA MI-IND-CCA



MAIN RESULT:

$$\mathrm{Adv}^{\text{MI-IND-CCA}}_{\mathrm{PKE}}(\mathbb{A}) \leq \mathrm{Adv}^{\text{MI-GapCDH}}(\mathbb{B}) + (\text{COLLISION TERM}) + (\text{MAC FORGERY})$$

CONCLUSION

- TIGHT MI-INHERITANCE FROM KEM TO PKE

CONCLUSION

- TIGHT MI-INHERITANCE FROM KEM TO PKE
- COROLLARY: PKE WITH OPTIMAL MULTI-INSTANCE RESISTANCE

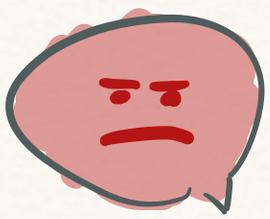
CONCLUSION

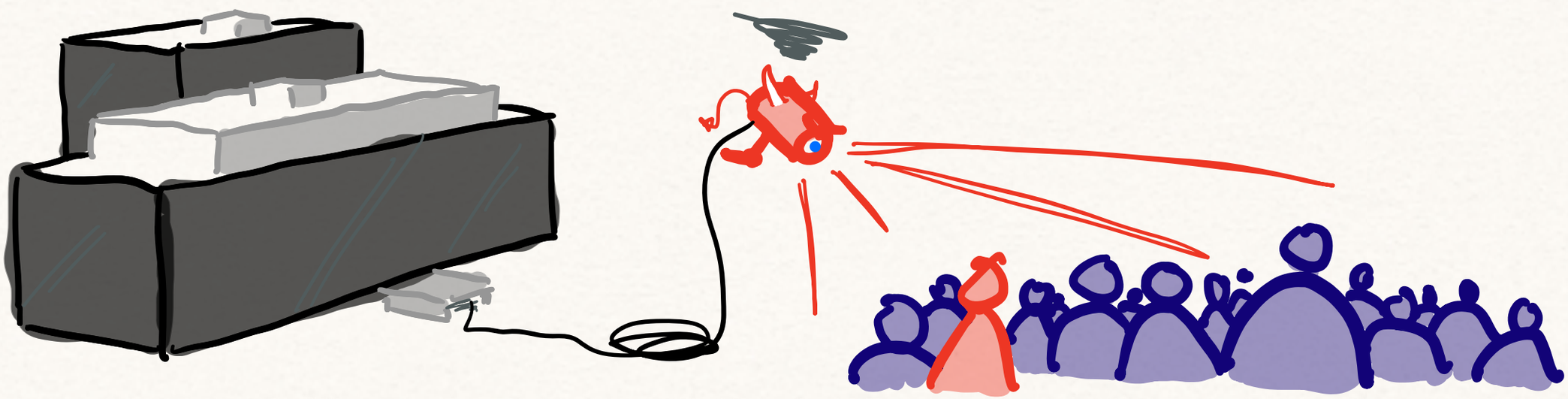
- TIGHT MI-INHERITANCE FROM KEM TO PKE
- COROLLARY: PKE WITH OPTIMAL MULTI-INSTANCE RESISTANCE

ALSO IN PAPER:

- NOVEL NOTION OF IMPERFECT CORRECTNESS
- NOVEL CCA-NOTION FOR IMPERFECT CORRECTNESS
- NOVEL NOTION OF MI KEY RECOVERY
- RELATIONS BETWEEN ALL RELEVANT NOTIONS
- EXTENDABLE-OUTPUT KEM/TAGKEM: "XEM/TAGXEM"
- (TAG)KEM + XOF = (TAG)XEM
- MORE CONSTRUCTIONS (CPA ONLY AND/OR MI-ROR ONLY)
- NOVEL NOTION OF MI-GAPCDH WITH CORRUPTIONS

Thank You!





HANS.HEUM@NTNU.NO