Resistance of Threshold Implementations against Statistical Ineffective Fault Attacks

Viet Sang Nguyen

June 18, 2024

Journée de la Recherche

joint work with Vincent Grosso and Pierre-Louis Cayrel

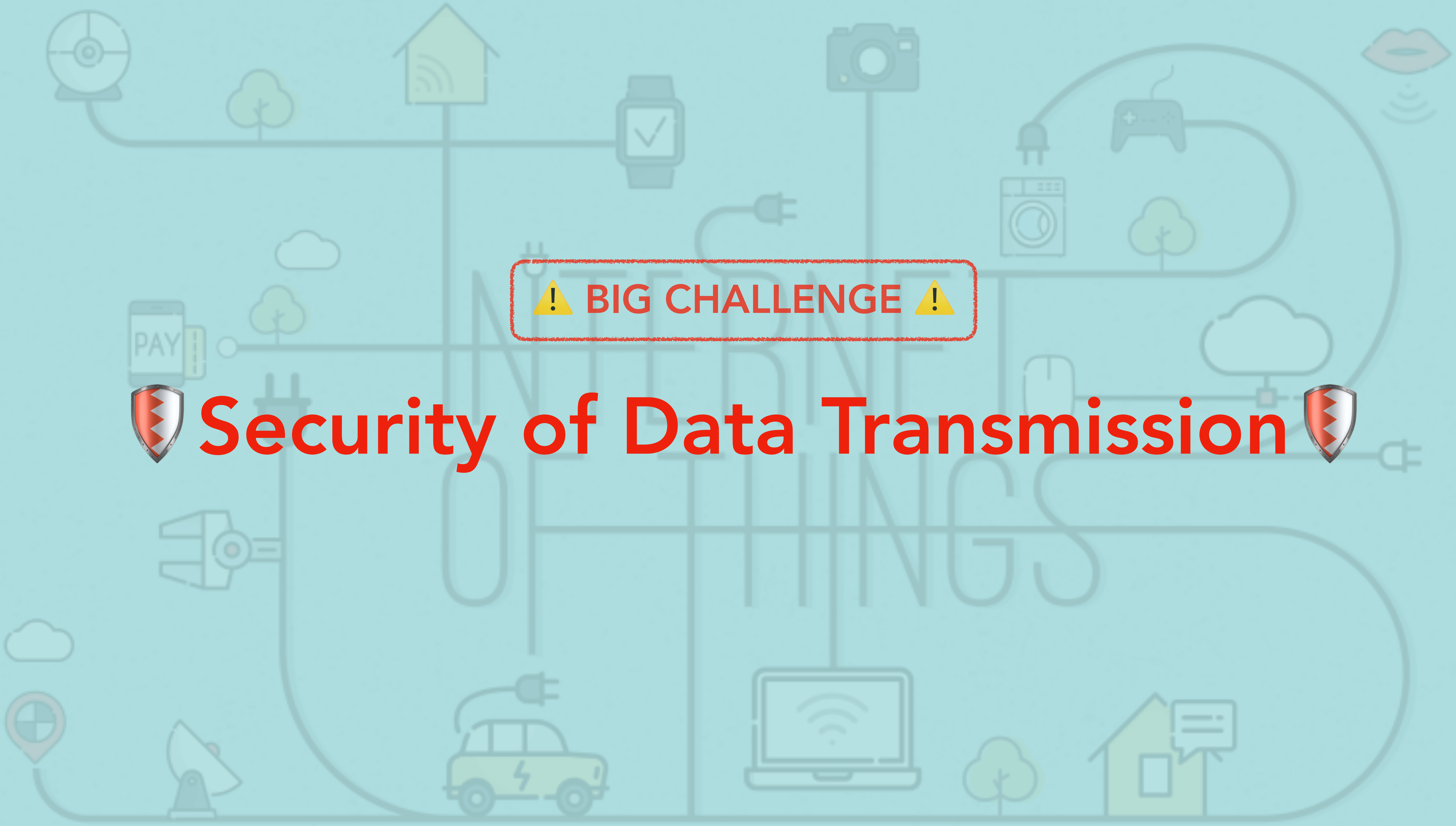
UNIVERSITÉ DE LYON

UNIVERSITÉ JEAN MONNET SAINT-ÉTIENNE

Laboratoire Hubert Curien
UMR • CNRS • 5516 • Saint-Étienne

anr®
PROPHY ANR-22-CE39-0008-01

ÉCOLE DOCTORALE 488
SIS
SCIENCES INGÉNIERIE SANTÉ
UNIVERSITÉ DE LYON

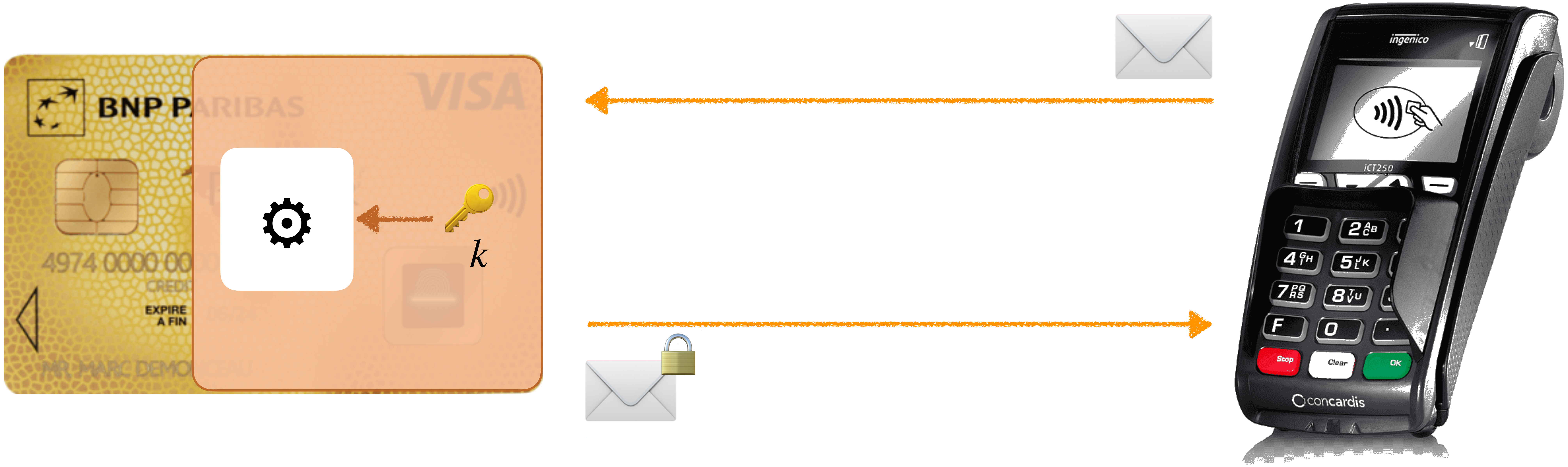


⚠️ BIG CHALLENGE ⚠️

🛡️ Security of Data Transmission 🛡️

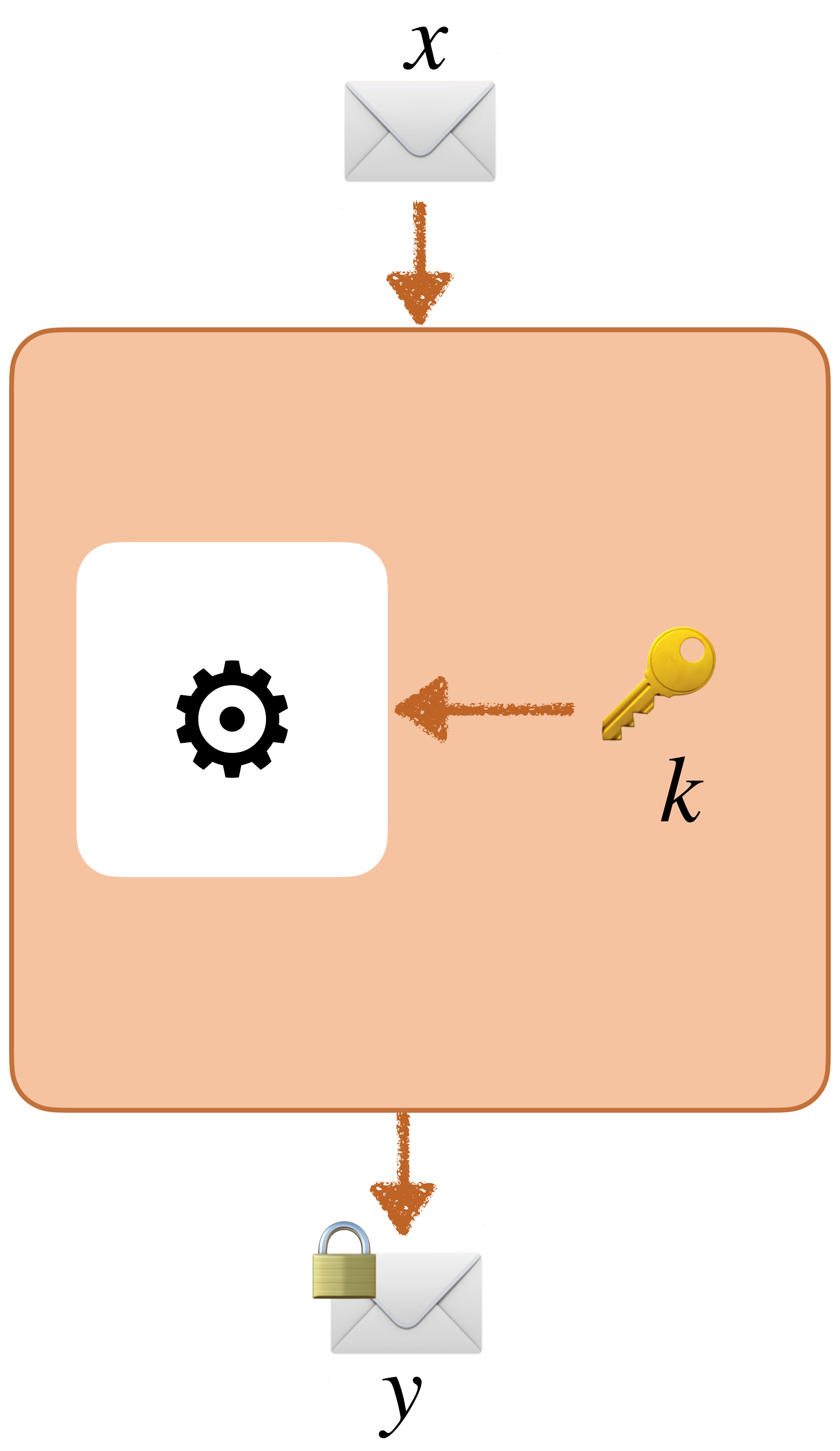
Viet Sang Nguyen

Payment Example



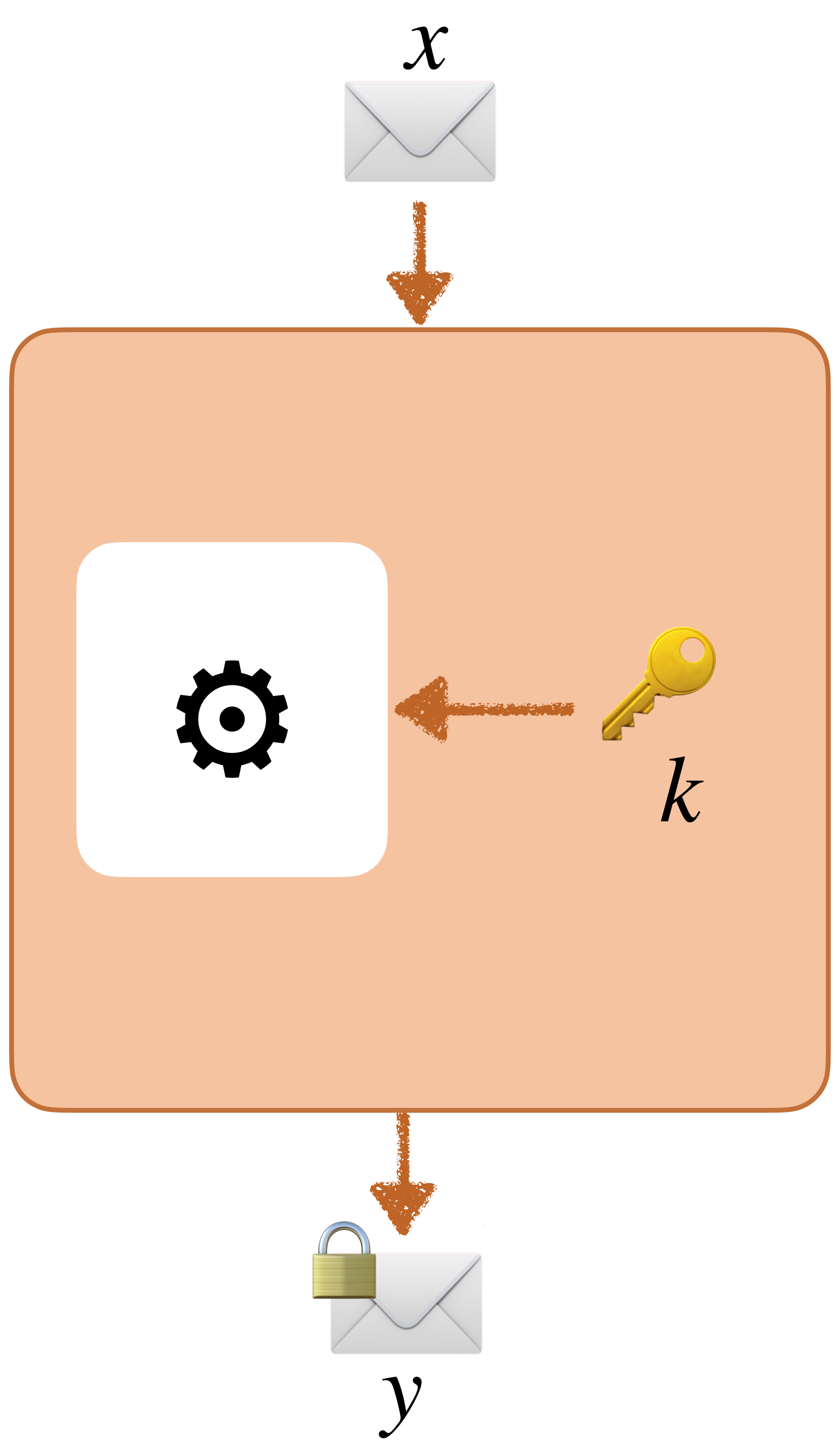
Viet Sang Nguyen

Cryptography



Viet Sang Nguyen

Battle… here it comes!



Attacker

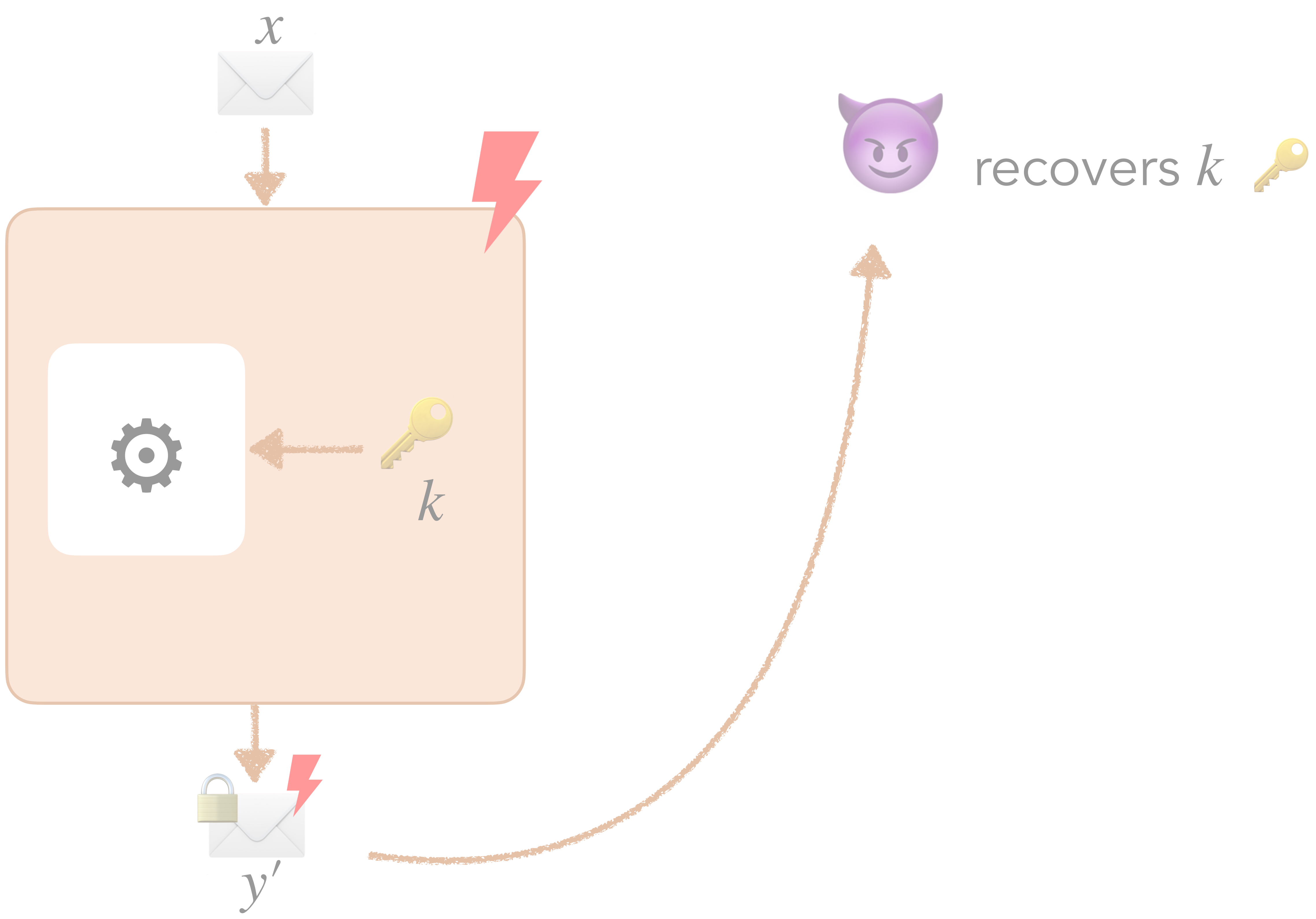
Designer

“I steal the key 🔑”

“I protect the key 🔑”

Viet Sang Nguyen

"I have fault attacks"



x

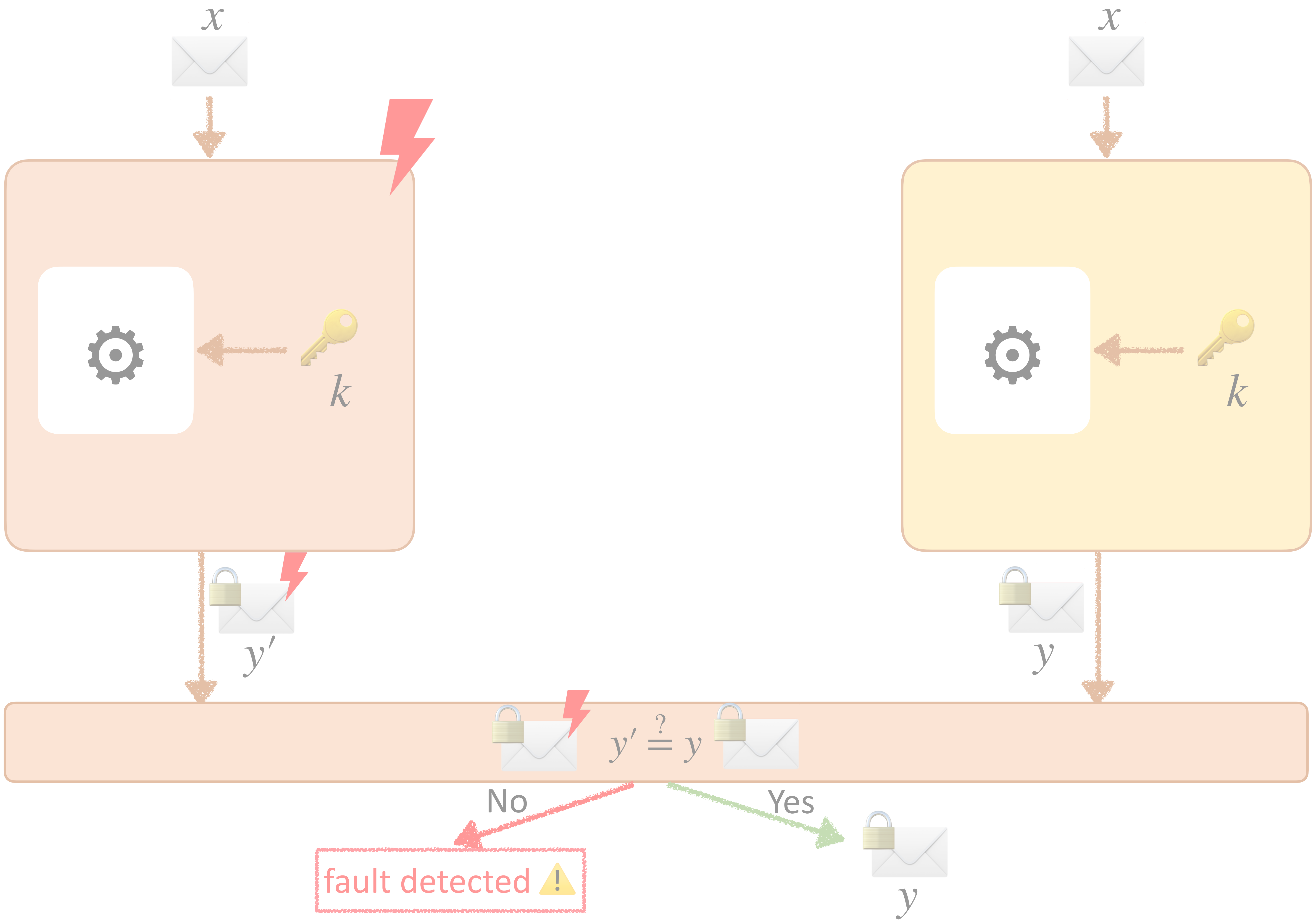
k

y'

recovers k

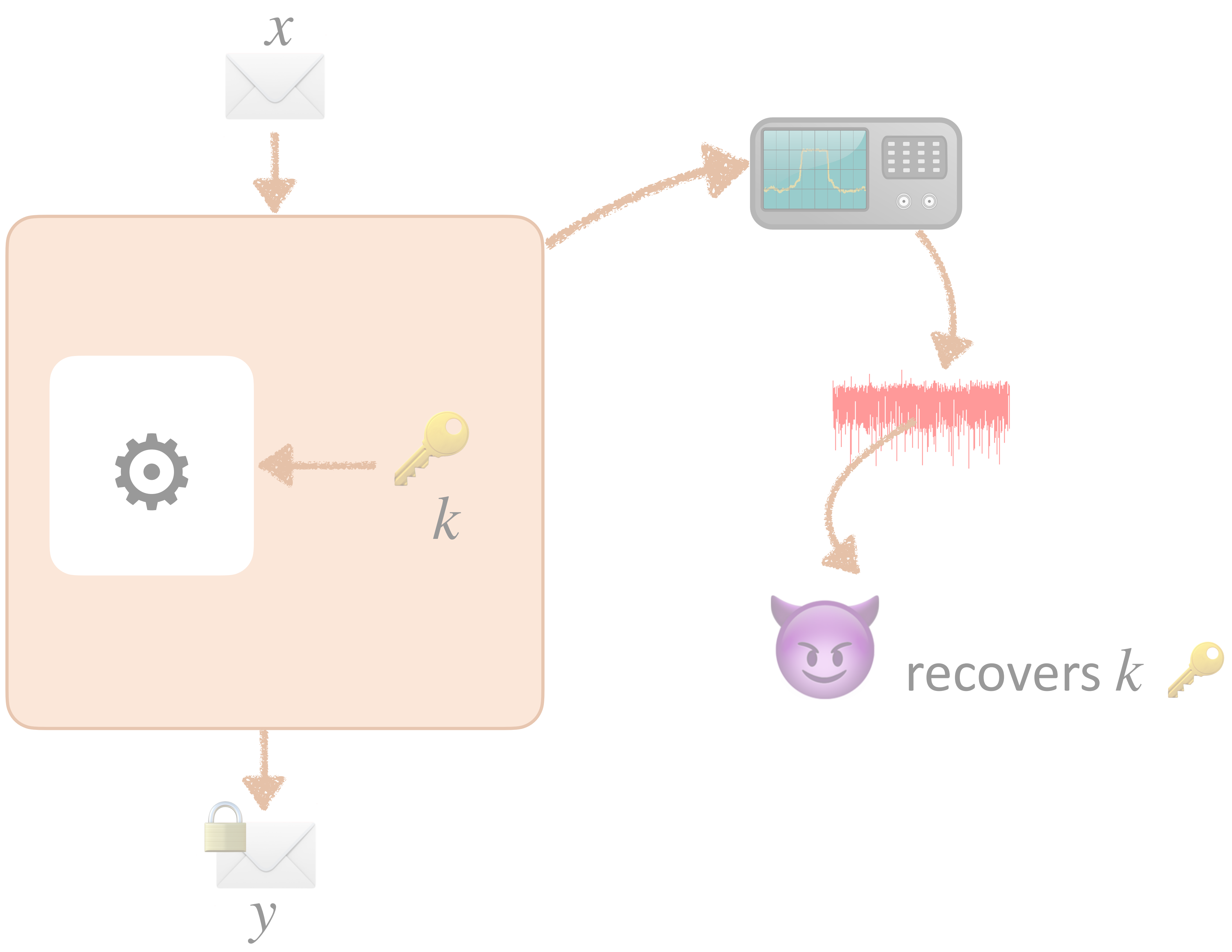
…

“I have countermeasure”



Viet Sang Nguyen

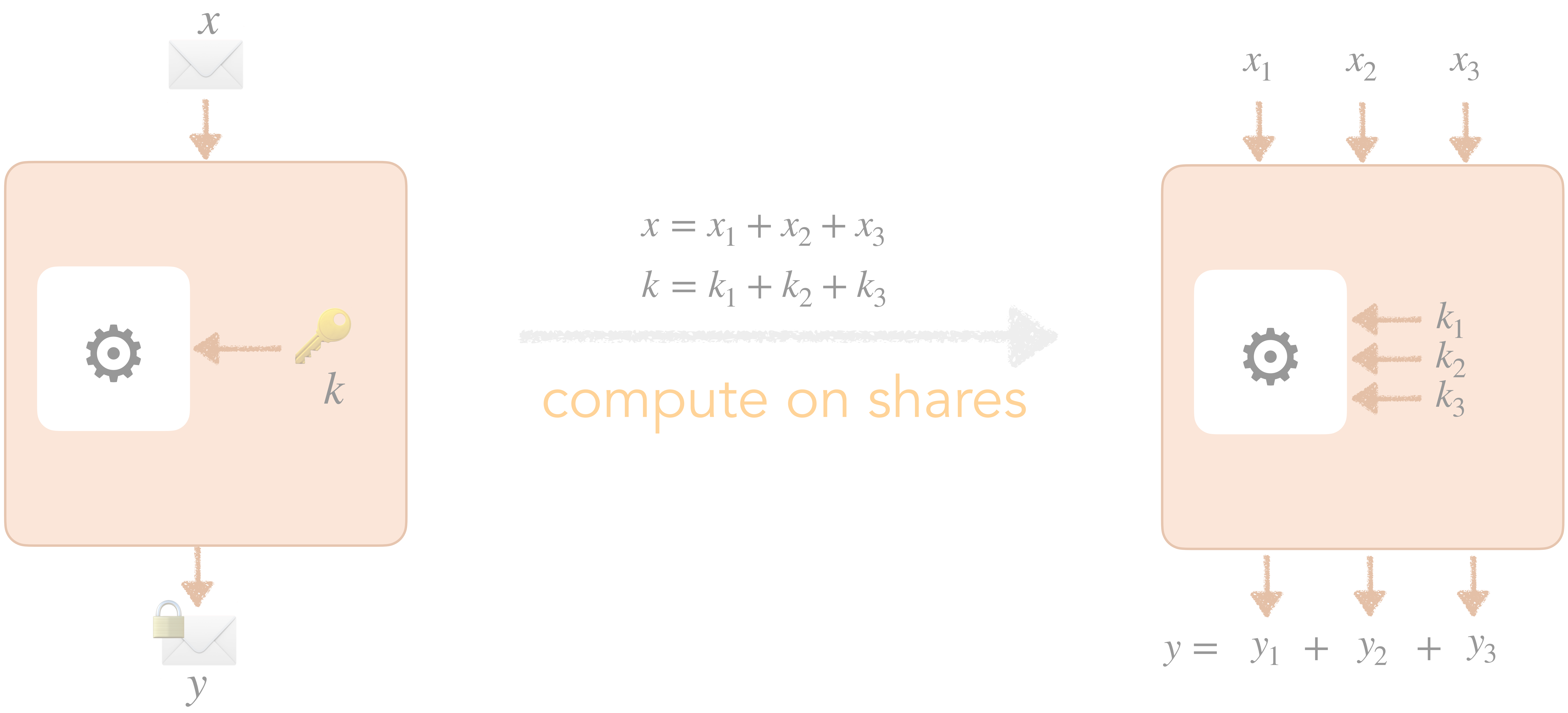
"I have side-channel attacks"



Viet Sang Nguyen

...

“I have countermeasure”



$$x = x_1 + x_2 + x_3$$

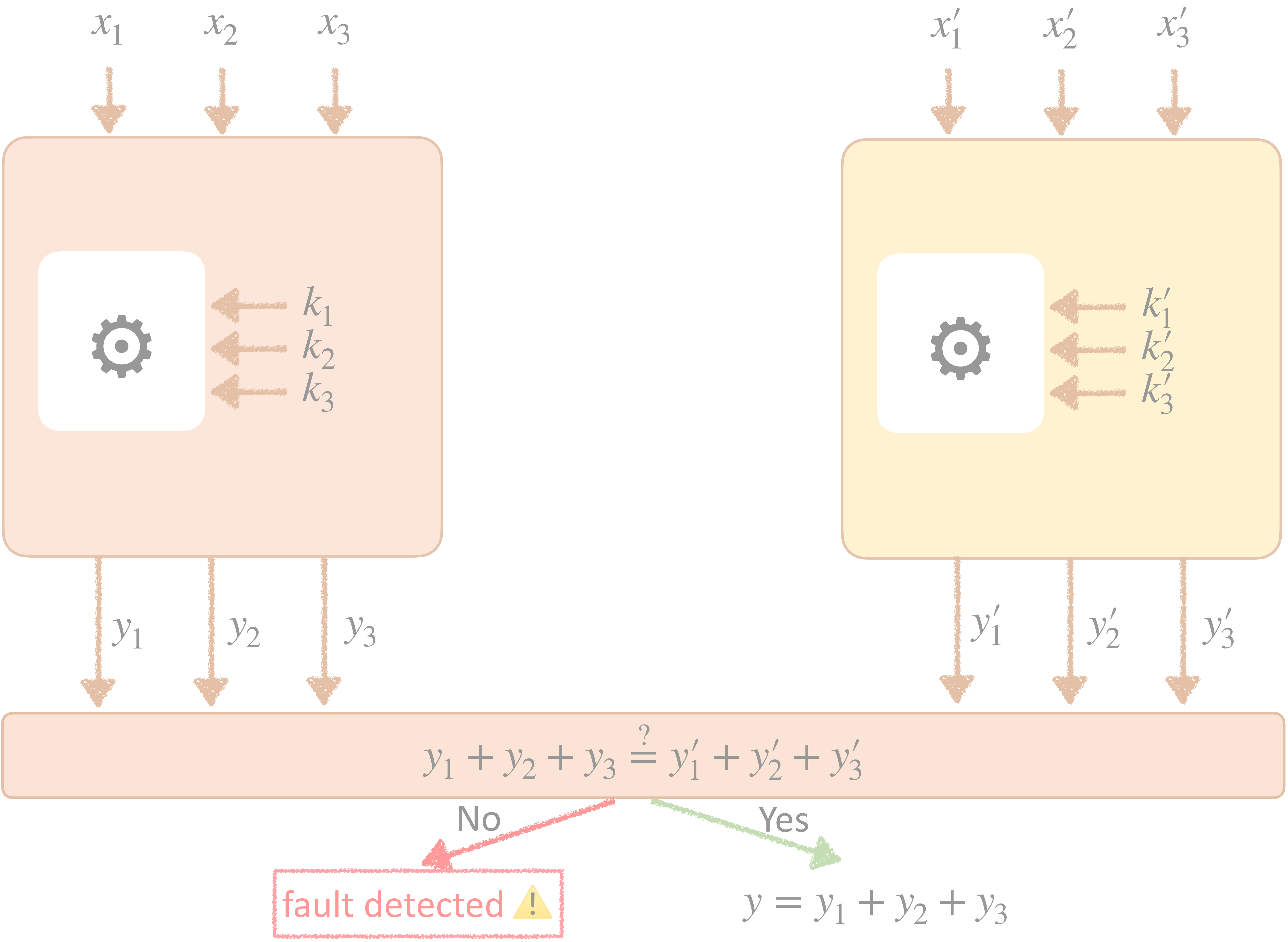
$$k = k_1 + k_2 + k_3$$

compute on shares

$$y = y_1 + y_2 + y_3$$

Viet Sang Nguyen

“This is combined countermeasure” 😇

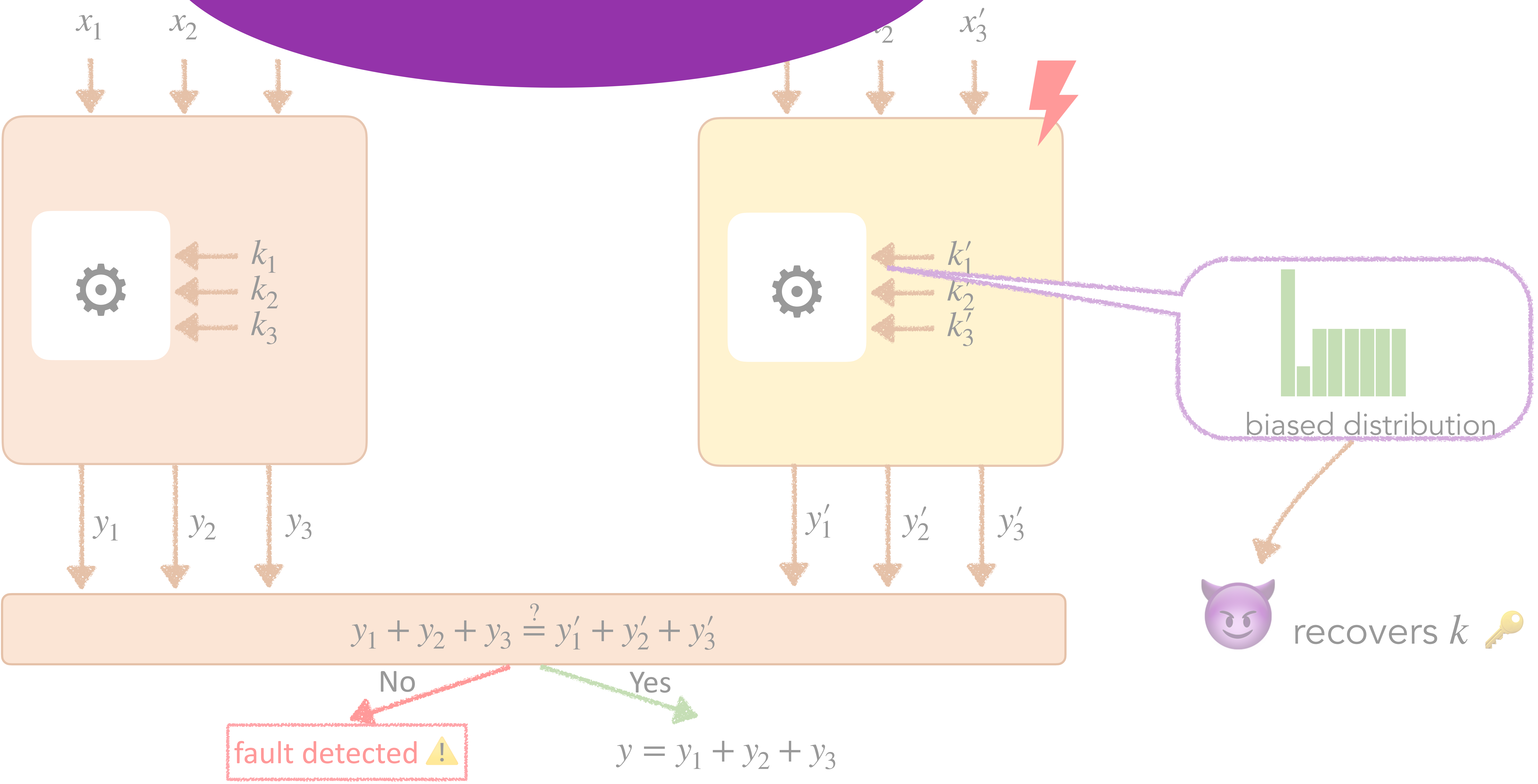


Viet Sang Nguyen

“I have stronger attack”

d countermeasure”

“This is state-of-the-art. Haha”

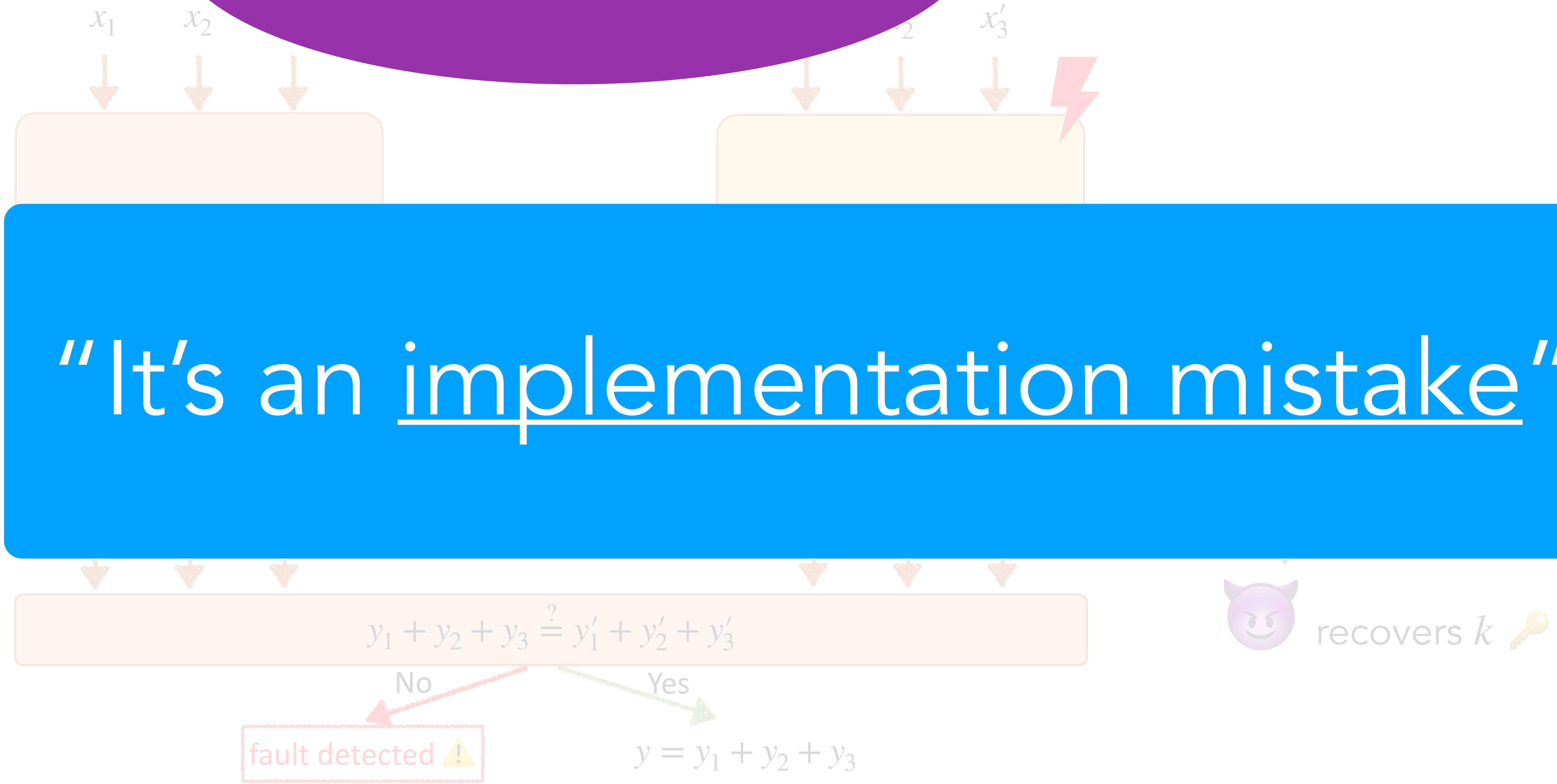


Viet Sang Nguyen

“I have str

“I know the reason”

“This is state-of-the-art. Haha”



“It’s an <u>implementation mistake</u>”

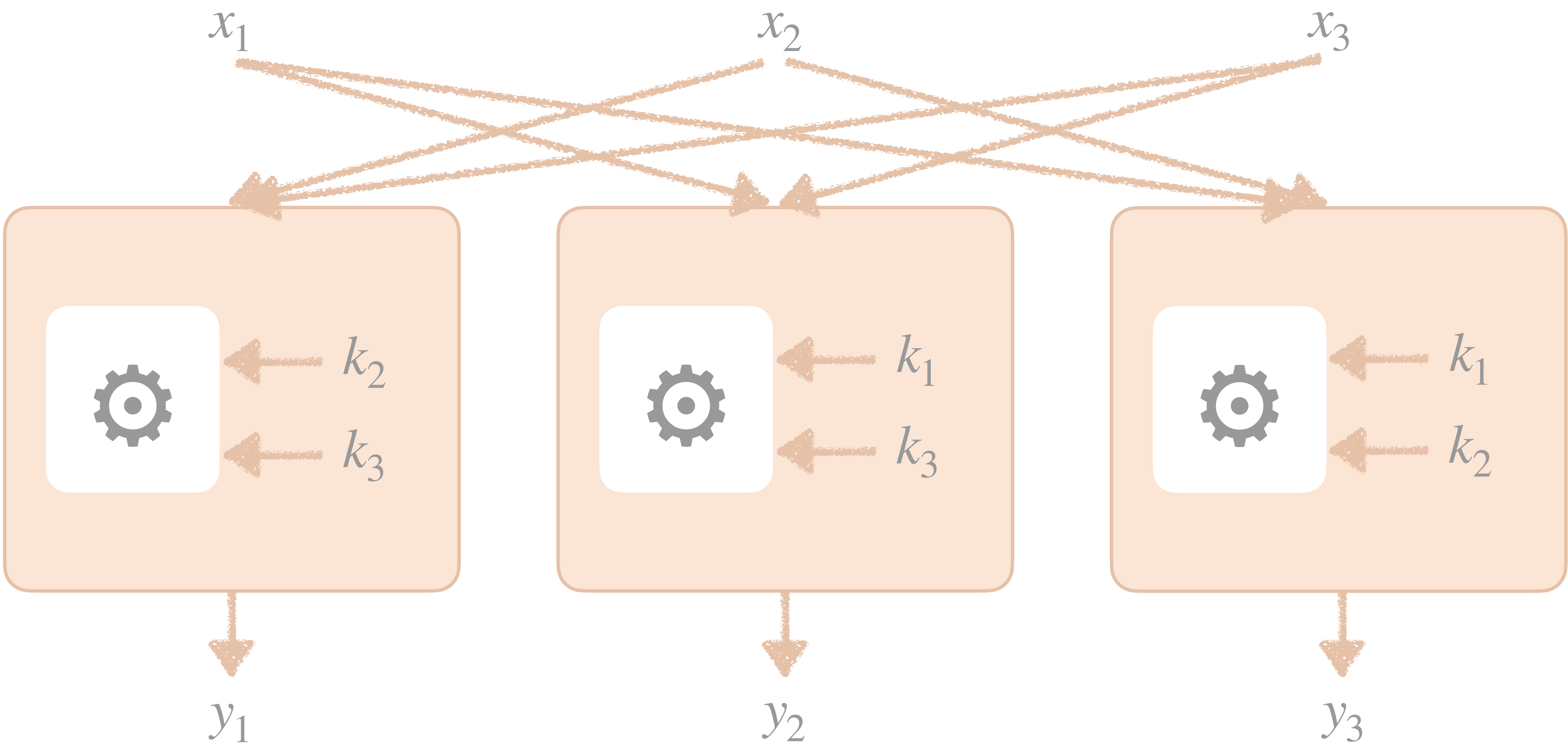
Viet Sang Nguyen

“I have str

“I know the reason”

“This is state-o

“I have countermeasure.
Let’s implement it properly!”



Viet Sang Nguyen

😈

“I have str

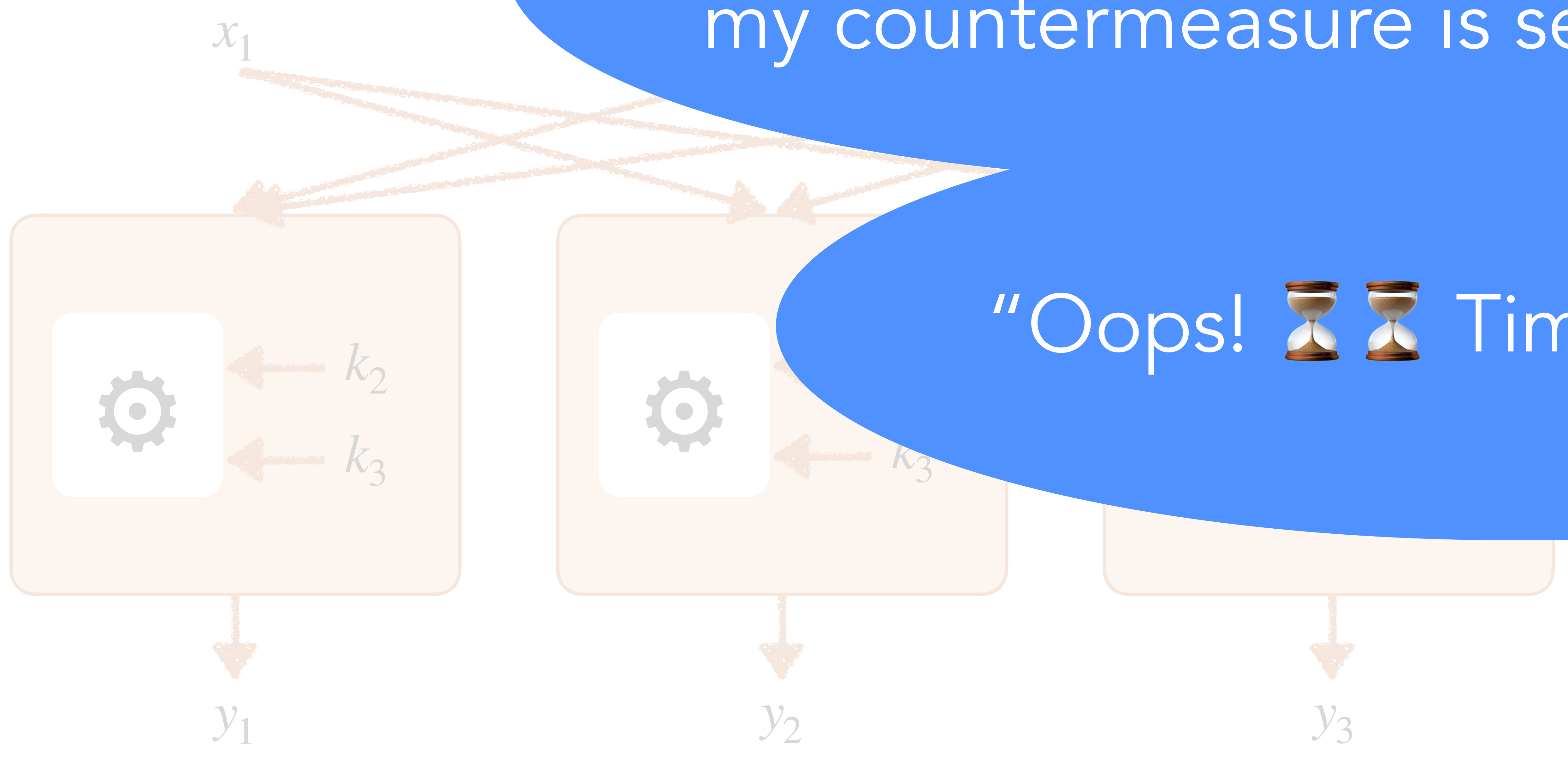
“This is state-o

“I know the reason”

“I have countermeasure.
Let’s implement it properly!”

“I can prove that
my countermeasure is secure”

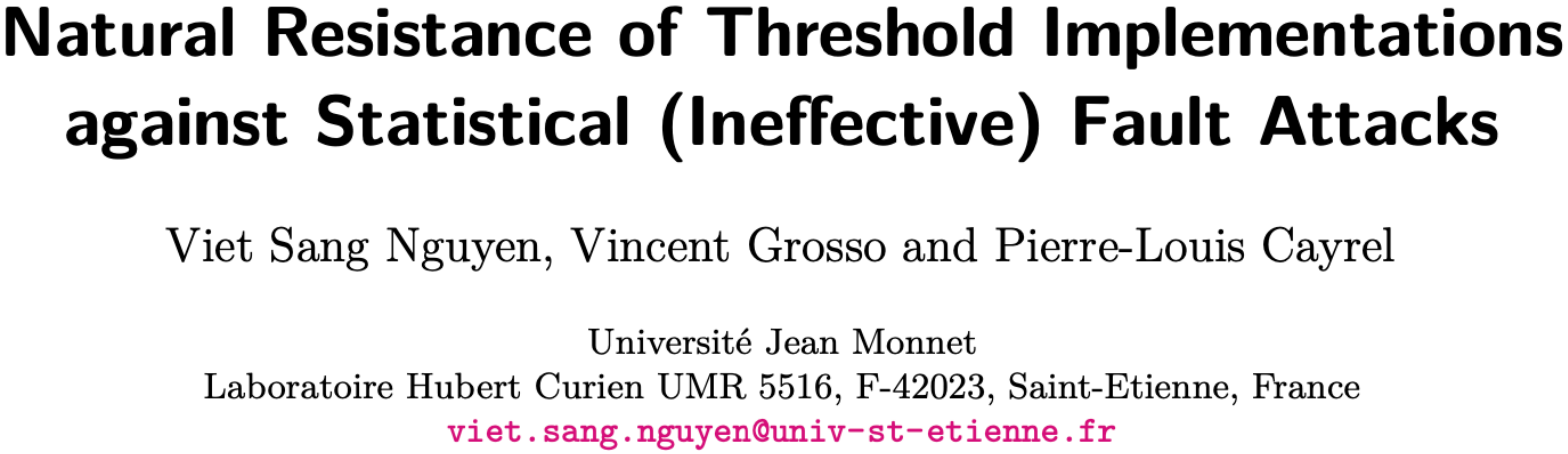
“Oops! ⏳⏳ Time’s up! ⏰⏰”



Viet Sang Nguyen

“You want to know more?
contact me 😉”

THANK YOU!



Natural Resistance of Threshold Implementations against Statistical (Ineffective) Fault Attacks

Viet Sang Nguyen, Vincent Grosso and Pierre-Louis Cayrel

Université Jean Monnet
Laboratoire Hubert Curien UMR 5516, F-42023, Saint-Etienne, France
viet.sang.nguyen@univ-st-etienne.fr