# Bounded Tamper Resilience: How to go beyond the Algebraic Barrier

Pratyay Mukherjee

Aarhus University

Asiacrypt 2013

Joint work with

Ivan Damgård, Sebastian Faust & Daniele Venturi

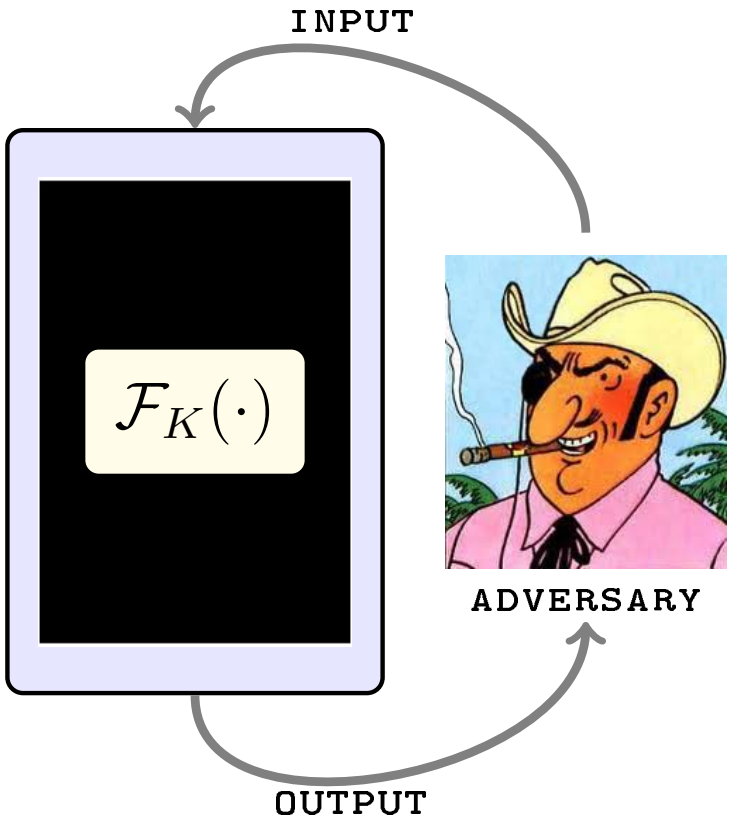
AARHUS UNIVERSITY

# Physical Attacks: Theory vs Reality

AARHUS UNIVERSITY

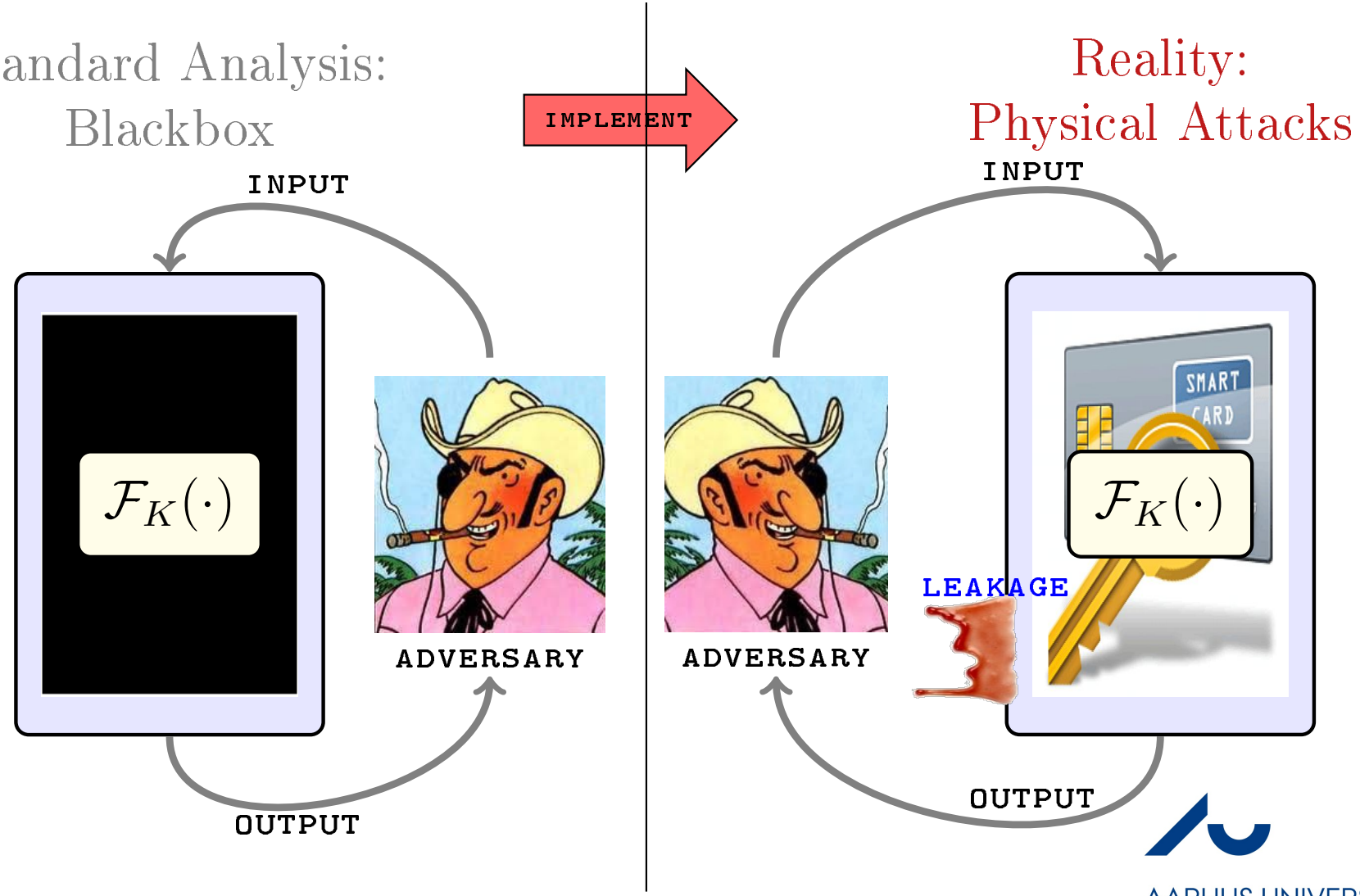
# Physical Attacks: Theory vs Reality

## Standard Analysis: Blackbox



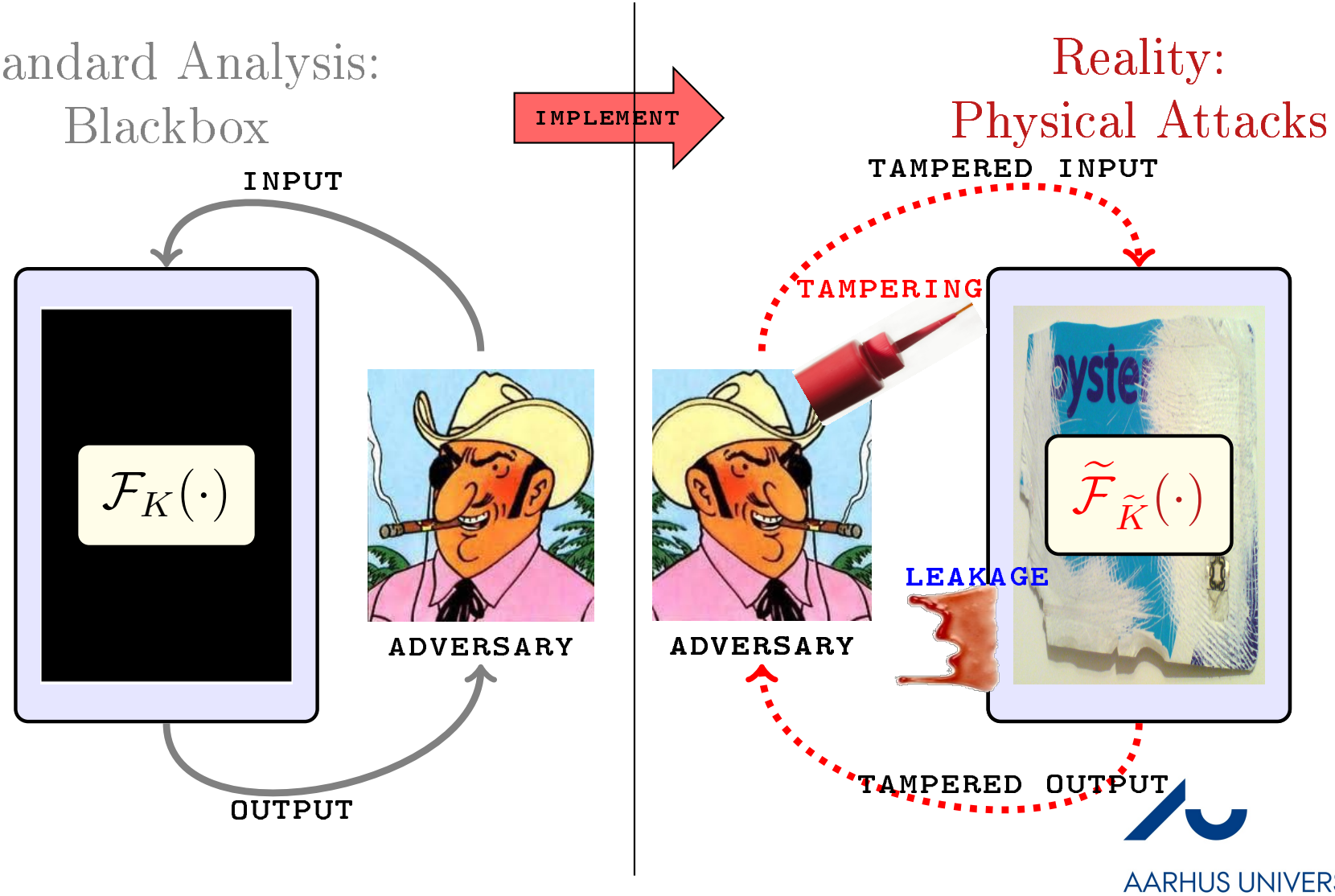

AARHUS UNIVERSITY

# Physical Attacks: Theory vs Reality

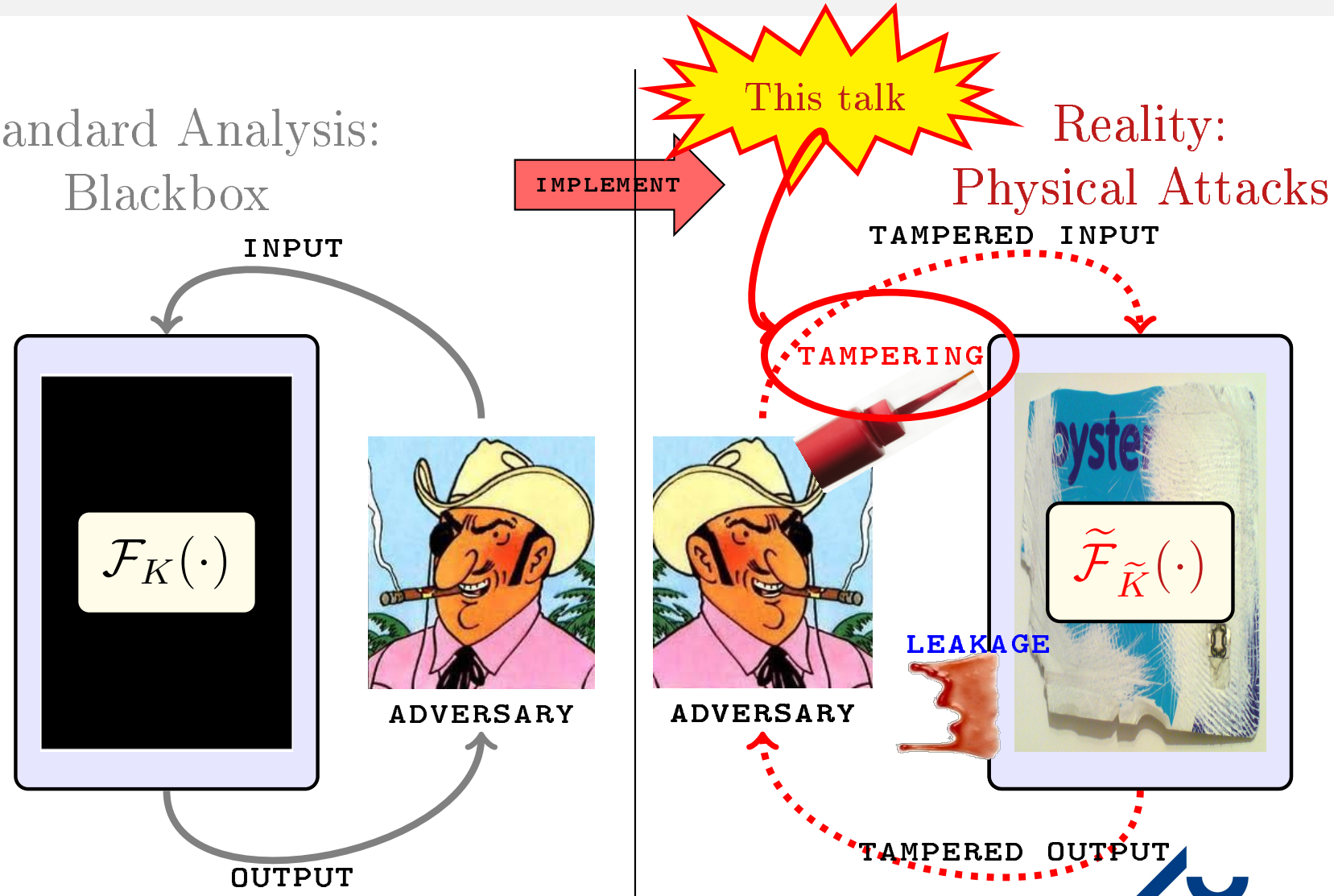



AARHUS UNIVERSITY

# Physical Attacks: Theory vs Reality



# Physical Attacks: Theory vs Reality



# Why care about Tampering ?

AARHUS UNIVERSITY

# Why care about Tampering ?

Captures Practical Attacks

Fault Attack!

AARHUS UNIVERSITY

# Why care about Tampering ?

Captures Practical Attacks

Fault Attack!

Example

Boneh et al. [JOC'01]: Inject single (random) fault to the signing-key of some type of RSA-sig $\Longrightarrow$ factor RSA-modulus !

AARHUS UNIVERSITY

# Why care about Tampering ?

Captures Practical Attacks

Fault Attack!

Example

Boneh et al. [JOC'01]: Inject single (random) fault to the signing-key of some type of RSA-sig $\Longrightarrow$ factor RSA-modulus !

Devastating !

AARHUS UNIVERSITY

# Why care about Tampering ?

Captures Practical Attacks

Fault Attack!

Example

Boneh et al. [JOC'01]: Inject single (random) fault to the signing-key of some type of RSA-sig $\Longrightarrow$ factor RSA-modulus !

Devastating !

More ...

Anderson & Kuhn [USENIX'96]
Skorobogatov et al. [CHES'02]
Coron et al. [CHES'09]
...

AARHUS UNIVERSITY

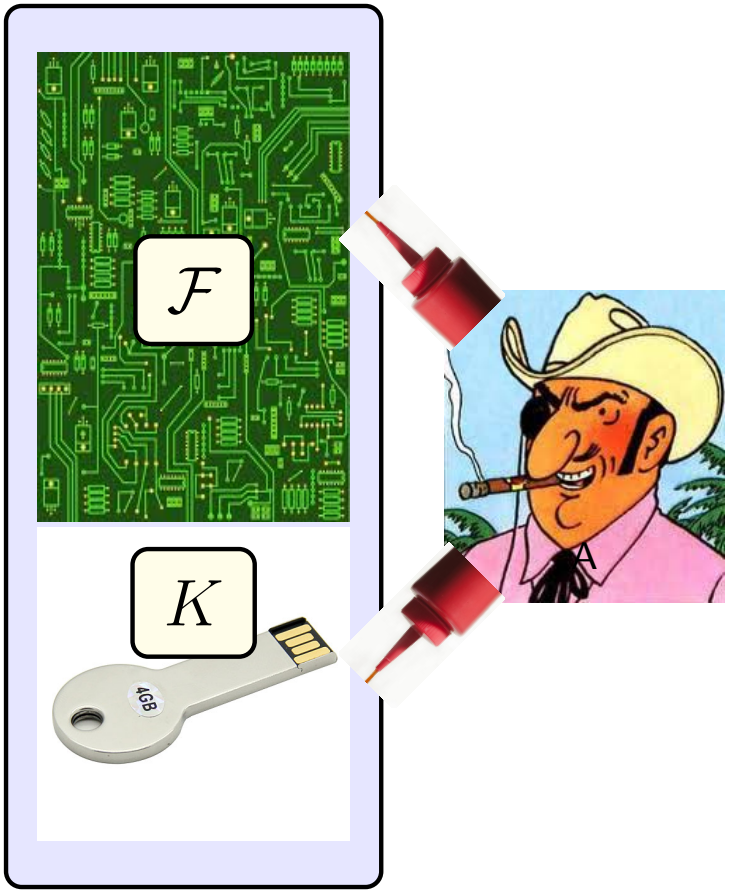
# Models of Tampering

AARHUS UNIVERSITY

# Models of Tampering

## Memory & Computation

(Ishai et al. [EUROCRYPT'06])

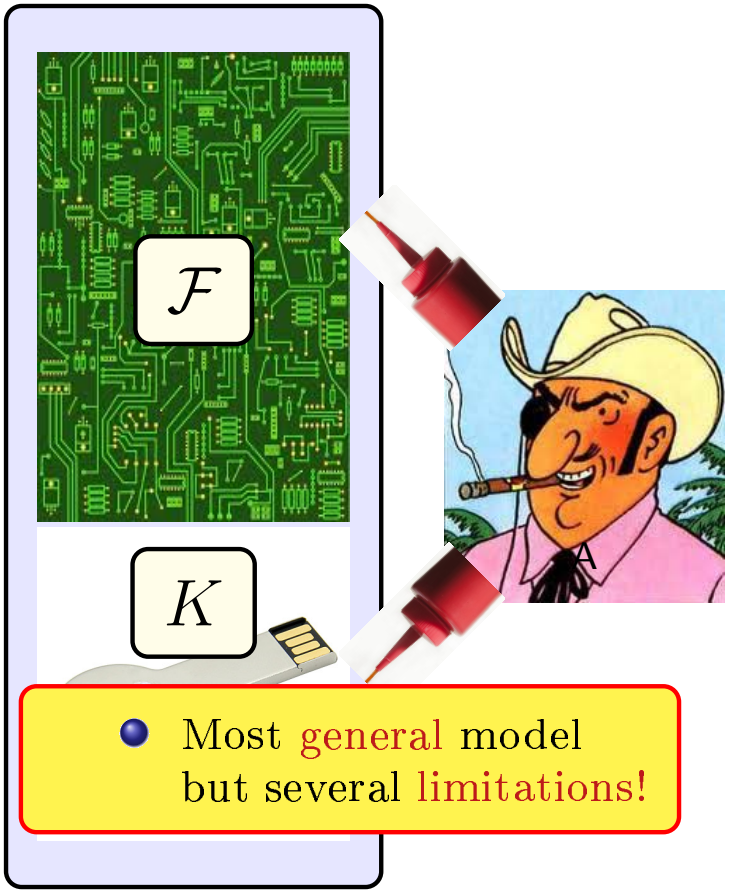



AARHUS UNIVERSITY

# Models of Tampering

## Memory & Computation

(Ishai et al. [EUROCRYPT'06])

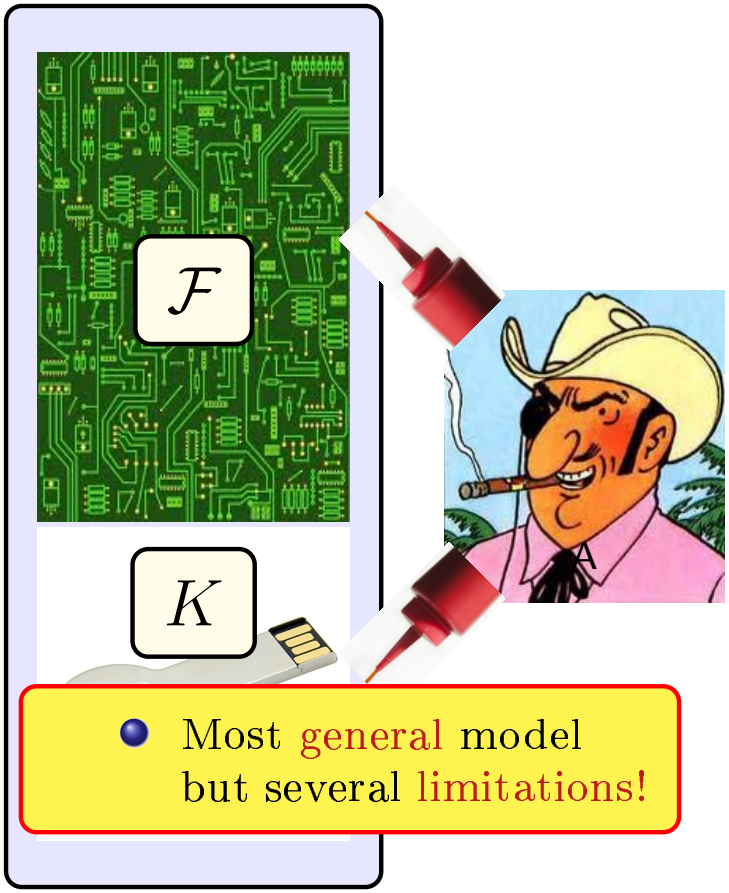



- Most general model but several limitations!

AARHUS UNIVERSITY

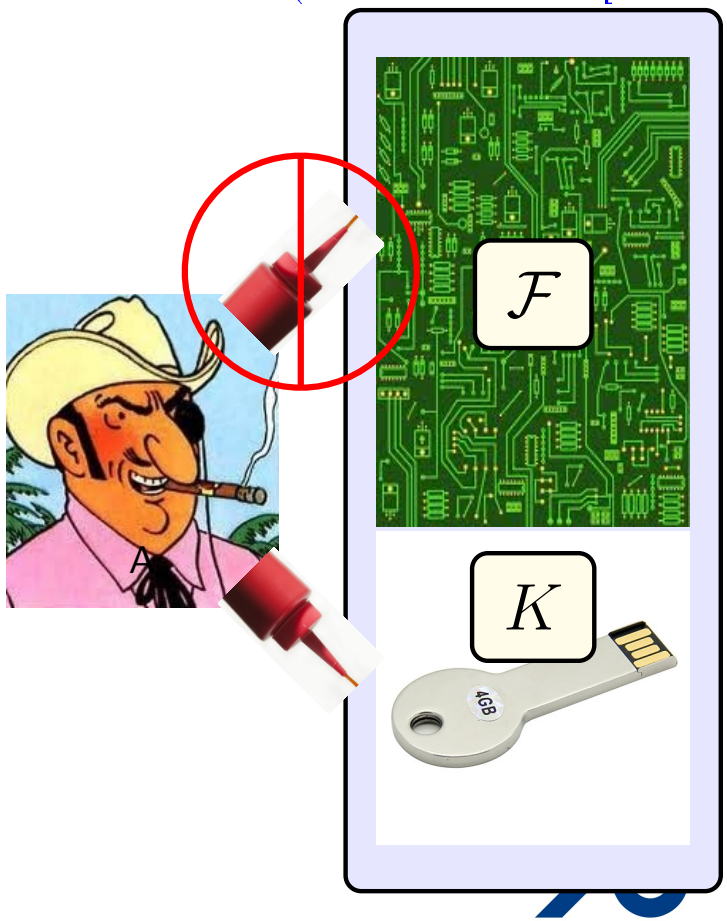
# Models of Tampering

## Memory & Computation
(Ishai et al. [EUROCRYPT'06])




- Most general model but several limitations!

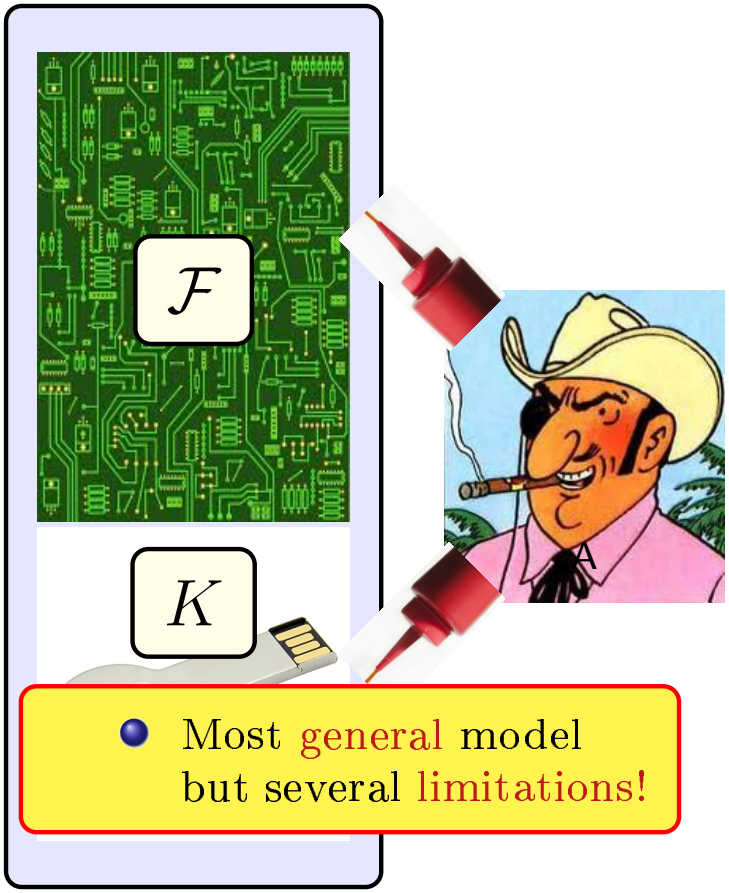
## Only Memory
(Gennaro et al. [TCC'04])




AARHUS UNIVERSITY

# Models of Tampering

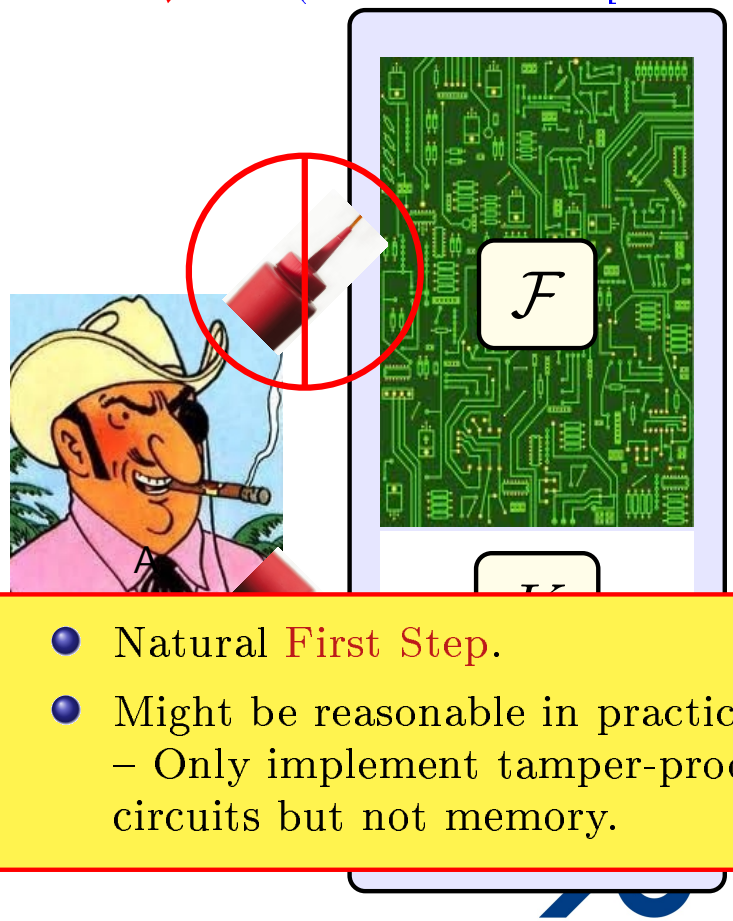
## Memory & Computation
(Ishai et al. [EUROCRYPT'06])




- Most general model but several limitations!

Our Focus

## Only Memory
(Gennaro et al. [TCC'04])

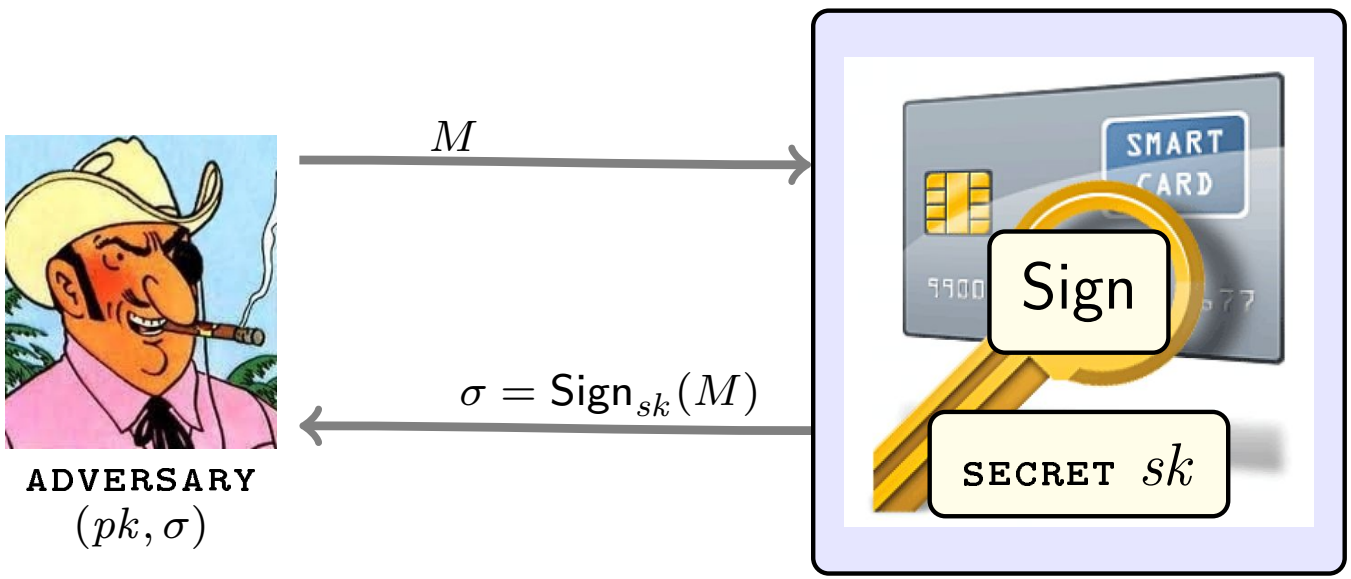



- Natural First Step.
- Might be reasonable in practice:
  – Only implement tamper-proof circuits but not memory.

AARHUS UNIVERSITY

# Memory Tampering: Illustrative Example

## Untampered Output




AARHUS UNIVERSITY

# Memory Tampering: Illustrative Example

Fix family $\Gamma$

$1 \leq i \leq t$
$(t = \mathsf{poly}(k))$

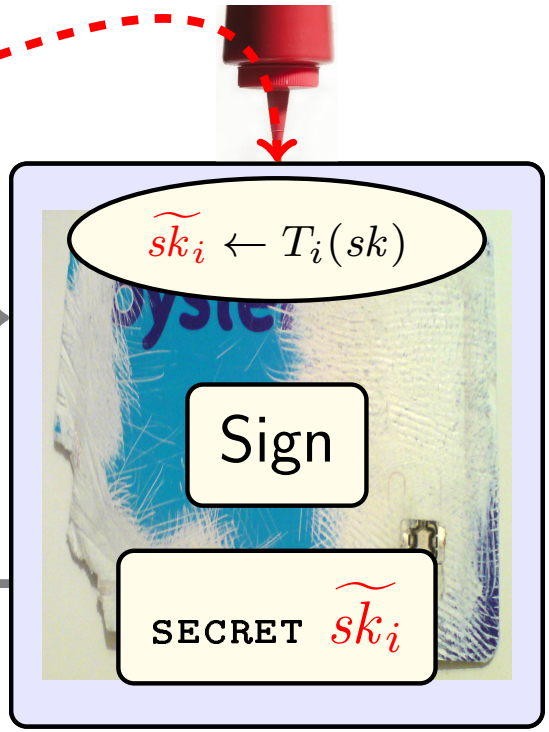
## Tampering

CHOOSE $T_i(\cdot) \leftarrow \Gamma$

$T_i(\cdot)$

$M$

ADVERSARY
$(pk, \sigma, \widetilde{\sigma_1}, \ldots, \widetilde{\sigma_i})$




$\widetilde{\sigma_i} = \mathsf{Sign}_{\widetilde{sk_i}}(M)$

AARHUS UNIVERSITY

# Memory Tampering: Illustrative Example

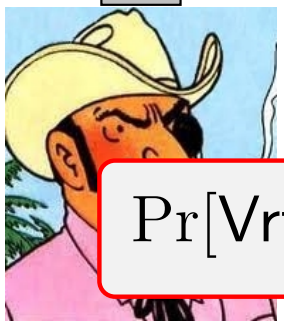
Fix family $\Gamma$

$1 \leq i \leq t$
$(t = \mathsf{poly}(k))$

Challenge

$M^\star, \sigma^\star$

Forge

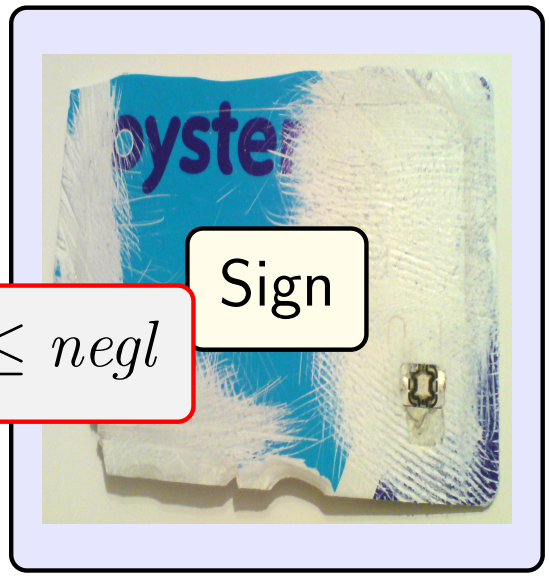


**ADVERSARY**

$(pk, \sigma, \widetilde{\sigma_1}, \ldots, \widetilde{\sigma_i}, \ldots, \widetilde{\sigma_t})$

Requirement

$$\Pr[\mathsf{Vrfy}_{pk}(M^\star, \sigma^\star) = 1] \leq negl$$




AARHUS UNIVERSITY

# Memory Tampering: Illustrative Example

Fix family $\Gamma$

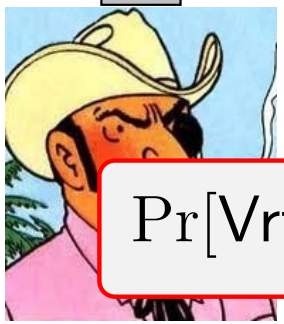
$1 \leq i \leq t$
$(t = \mathsf{poly}(k))$

a.k.a. RKA-model

## Challenge

$M^\star, \sigma^\star$

Forge

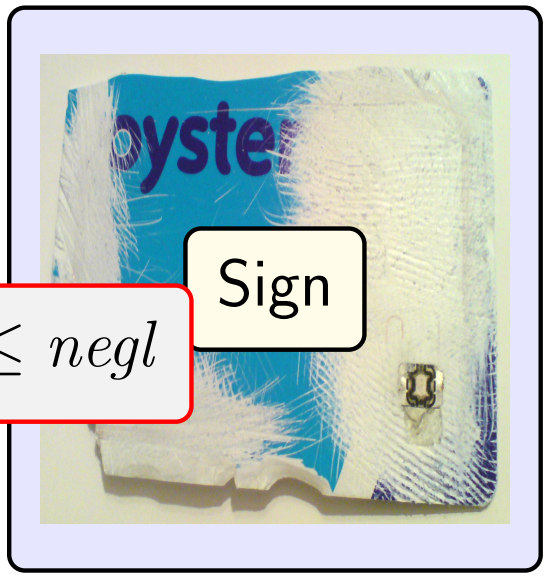


**ADVERSARY**

$(pk, \sigma, \widetilde{\sigma_1}, \ldots, \widetilde{\sigma_i}, \ldots, \widetilde{\sigma_t})$

Requirement

$$\Pr[\mathsf{Vrfy}_{pk}(M^\star, \sigma^\star) = 1] \leq negl$$




AARHUS UNIVERSITY

# Memory Tampering: Illustrative Example

Fix family $\Gamma$

$1 \leq i \leq t$
$(t = \mathsf{poly}(k))$

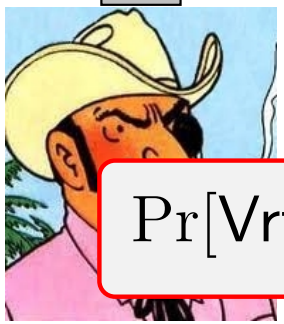
a.k.a. RKA-model

Challenge

Natural Goal:
Broaden $\Gamma$

$M^\star, \sigma^\star$

Forge

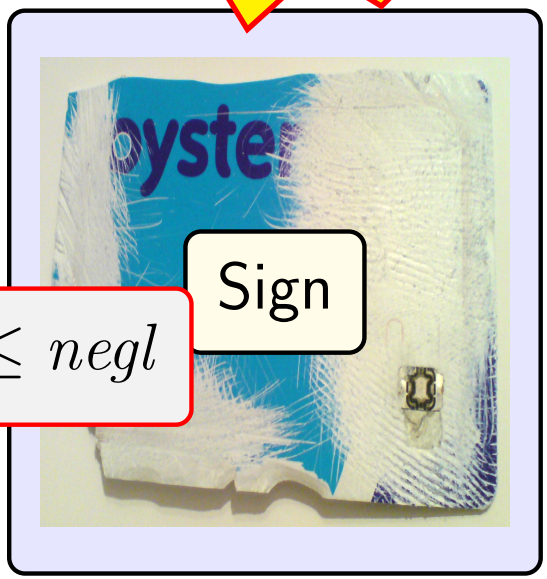


**ADVERSARY**

$(pk, \sigma, \widetilde{\sigma_1}, \ldots, \widetilde{\sigma_i}, \ldots, \widetilde{\sigma_t})$

Requirement

$$\Pr[\mathsf{Vrfy}_{pk}(M^\star, \sigma^\star) = 1] \leq negl$$




AARHUS UNIVERSITY

# ....RKA Model

AARHUS UNIVERSITY

# ....RKA Model

First model: Bellare and Kohno [EUROCRYPT'03].

AARHUS UNIVERSITY

# ....RKA Model

First model: Bellare and Kohno [EUROCRYPT'03].

More

Lucks[FSE'04], BC[CRYPTO'10], BCM[ASIACRYPT'11], BPT[ASIACRYPT'12], AHI[ICS'11], BR[FSE'13], GOR[TCC'11], Wee[PKC'12]...

AARHUS UNIVERSITY

# ....RKA Model

First model: Bellare and Kohno [EUROCRYPT'03].

More

Lucks[FSE'04], BC[CRYPTO'10], BCM[ASIACRYPT'11], BPT[ASIACRYPT'12], AHI[ICS'11], BR[FSE'13], GOR[TCC'11], Wee[PKC'12]...

## RKA(in short)

1. Unrestricted $t$ – any polynomial.

AARHUS UNIVERSITY

# ....RKA Model

First model: Bellare and Kohno [EUROCRYPT'03].

More

Lucks[FSE'04], BC[CRYPTO'10], BCM[ASIACRYPT'11], BPT[ASIACRYPT'12], AHI[ICS'11], BR[FSE'13], GOR[TCC'11], Wee[PKC'12]...

RKA(in short)

1. Unrestricted $t$ – any polynomial.
2. Restricted $\Gamma$. – Current-state-of-art considers $\Gamma$ as algebraic functions e.g. Affine function/polynomial over some field.

AARHUS UNIVERSITY

# ....RKA Model

First model: Bellare and Kohno [EUROCRYPT'03].

More

Lucks[FSE'04], BC[CRYPTO'10], BCM[ASIACRYPT'11], BPT[ASIACRYPT'12], AHI[ICS'11], BR[FSE'13], GOR[TCC'11], Wee[PKC'12]...

## RKA(in short)

1. Unrestricted $t$ – any polynomial.
2. Restricted $\Gamma$. – Current-state-of-art considers $\Gamma$ as algebraic functions e.g. Affine function/polynomial over some field.

## Drawback!

May NOT be realistic – arbitrary fault may not be captured by algebraic functions.

AARHUS UNIVERSITY

# This Work: An alternative Model

AARHUS UNIVERSITY

# This Work: An alternative Model

**Our Goal: Going beyond algebraic barrier**

We want tamper-resilience for unrestricted $\Gamma$.

AARHUS UNIVERSITY

# This Work: An alternative Model

**Our Goal: Going beyond algebraic barrier**

We want tamper-resilience for unrestricted $\Gamma$.

**Impossibility – Gennaro et al.[TCC'04]**

Both unrestricted and continuous tampering impossible!

AARHUS UNIVERSITY

# This Work: An alternative Model

**Our Goal: Going beyond algebraic barrier**

We want tamper-resilience for unrestricted $\Gamma$.

**Impossibility – Gennaro et al.[TCC'04]**

Both unrestricted and continuous tampering impossible!

**Our Solution: Bounded Tampering**

- Unrestricted $\Gamma$ – tamper with any efficient function !
- Bounded $t$ – tamper only bounded number of times.

AARHUS UNIVERSITY

# Our Contributions: Overview

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

## BLT-secure Public-key schemes

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

## BLT-secure Public-key schemes

Concrete schemes based on standard assumptions (DL, Factoring)

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

## BLT-secure Public-key schemes

Concrete schemes based on standard assumptions (DL, Factoring)

1. ID-schemes based on some class of $\Sigma$-protocols are BLT secure – e.g. Okamoto.

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

## BLT-secure Public-key schemes

Concrete schemes based on standard assumptions (DL, Factoring)

1. ID-schemes based on some class of $\Sigma$-protocols are BLT secure – e.g. Okamoto.
2. BHHO encryption scheme is BLT-secure.

AARHUS UNIVERSITY

# Our Contributions: Overview

## A new model: BLT

Bounded Leakage & Tampering – First model of Bounded Tampering.

–Analogous to Leakage-resilient Cryptography  - HOT!

## BLT-secure Public-key schemes

Concrete schemes based on standard assumptions (DL, Factoring)

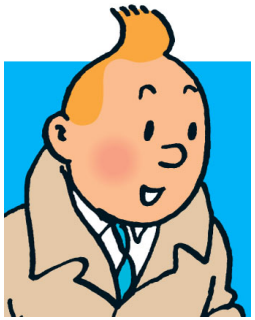
1. ID-schemes based on some class of $\Sigma$-protocols are BLT secure – e.g. Okamoto.
2. BHHO encryption scheme is BLT-secure.

## Moreover...

- Boost to Continuous Tampering using untamperable Floppy
- New Technique: Reduce tamper-resilience from leakage-resilience

# Recall: ID-Scheme

P wants to convince V that P knows secret $sk$ w.r.t $pk$

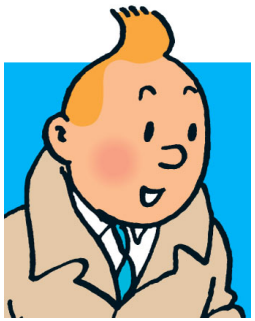


PROVER(P)
$(sk, pk)$

VERIFIER(V)
$(pk)$

# Recall: ID-Scheme

P wants to convince V that P knows secret $sk$ w.r.t $pk$



PROVER(P)
$(sk, pk)$

INTERACT

VERIFIER(V)
$(pk)$

Decision

ACCEPT/REJECT

Correctness

V accepts if P knows $sk$

AARHUS UNIVERSITY

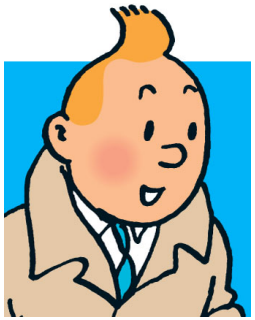
# BLT Model for ID-Schemes

AARHUS UNIVERSITY

# BLT Model for ID-Schemes

Parameter

$t$



PROVER(P)

$(sk)$

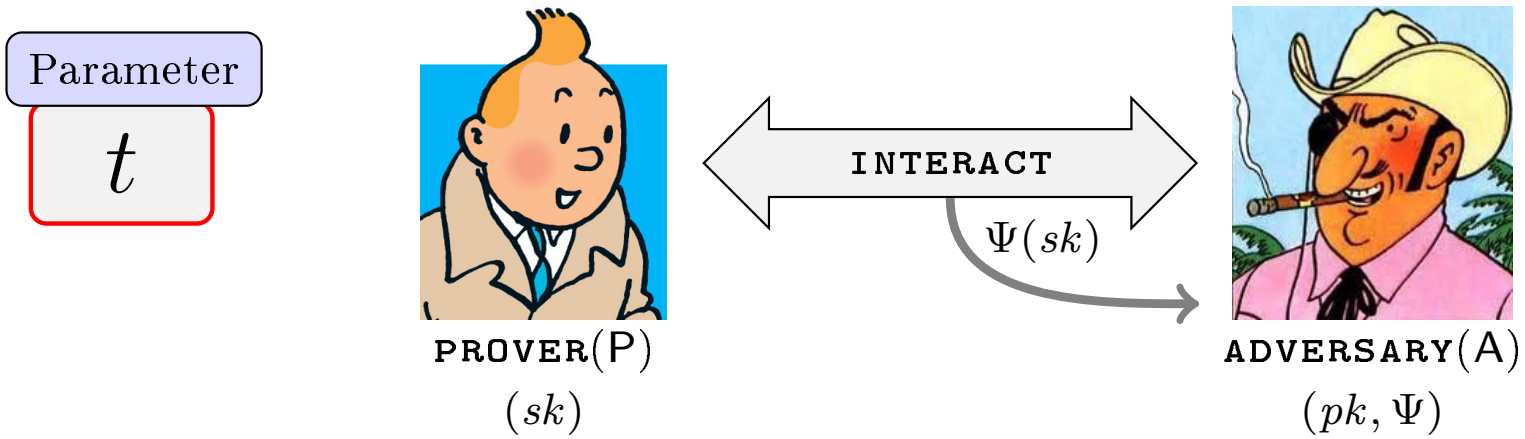
ADVERSARY(A)

$(pk)$

AARHUS UNIVERSITY

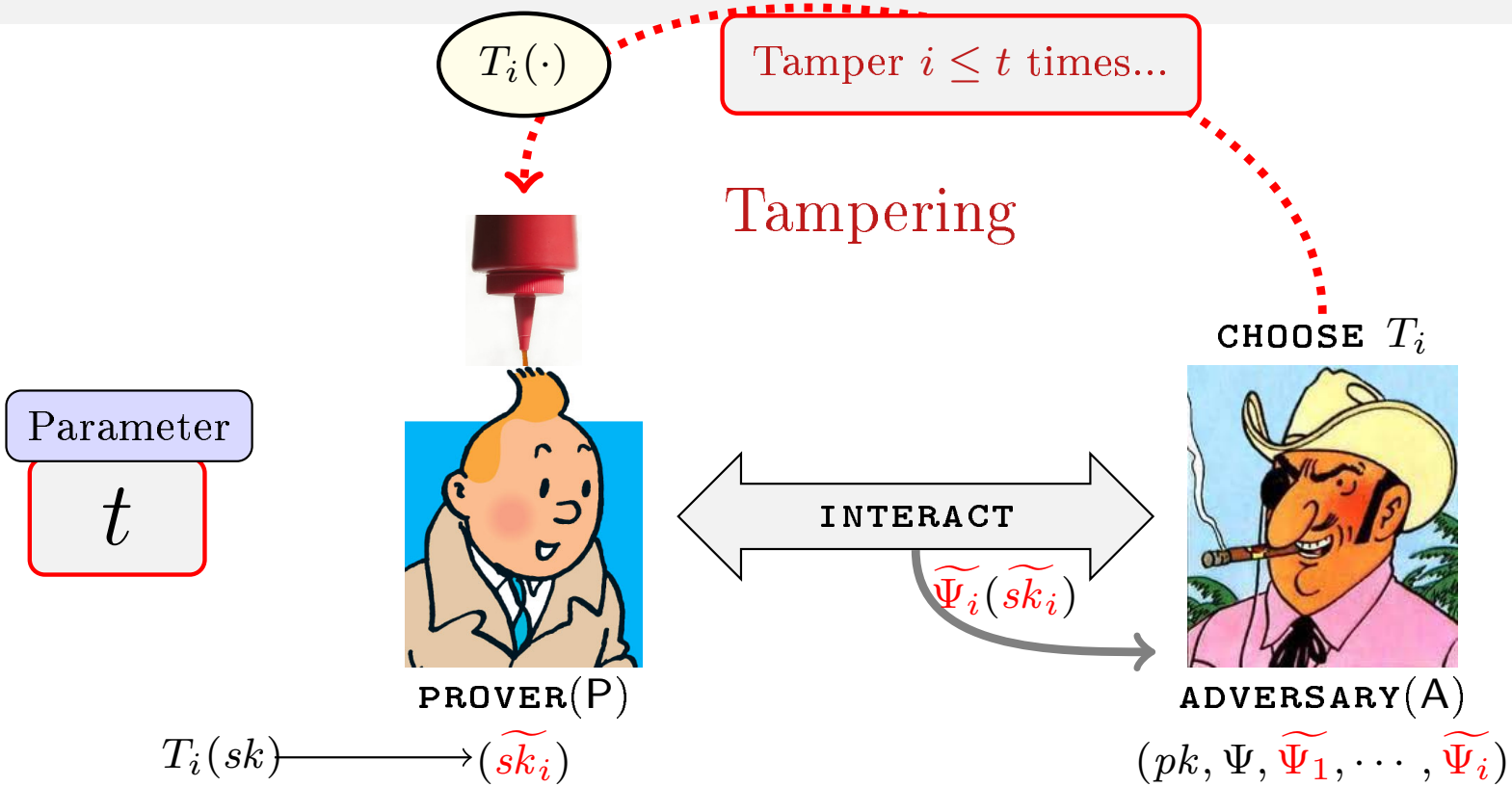
# BLT Model for ID-Schemes

Untampered Query




AARHUS UNIVERSITY

# BLT Model for ID-Schemes




AARHUS UNIVERSITY

# BLT Model for ID-Schemes

## Challenge Phase

Parameter

$t$

VERIFIER(V)

$(pk)$

INTERACT

ADVERSARY(A)

$(pk, \Psi, \widetilde{\Psi_1}, \cdots, \widetilde{\Psi_i}, \cdots, \widetilde{\Psi_t})$

Decision

ACCEPT/REJECT

Requirement

$\Pr[\text{V accepts}] \leq negl$

AARHUS UNIVERSITY

# ID-Scheme from $\Sigma$-protocol (Cramer '96)

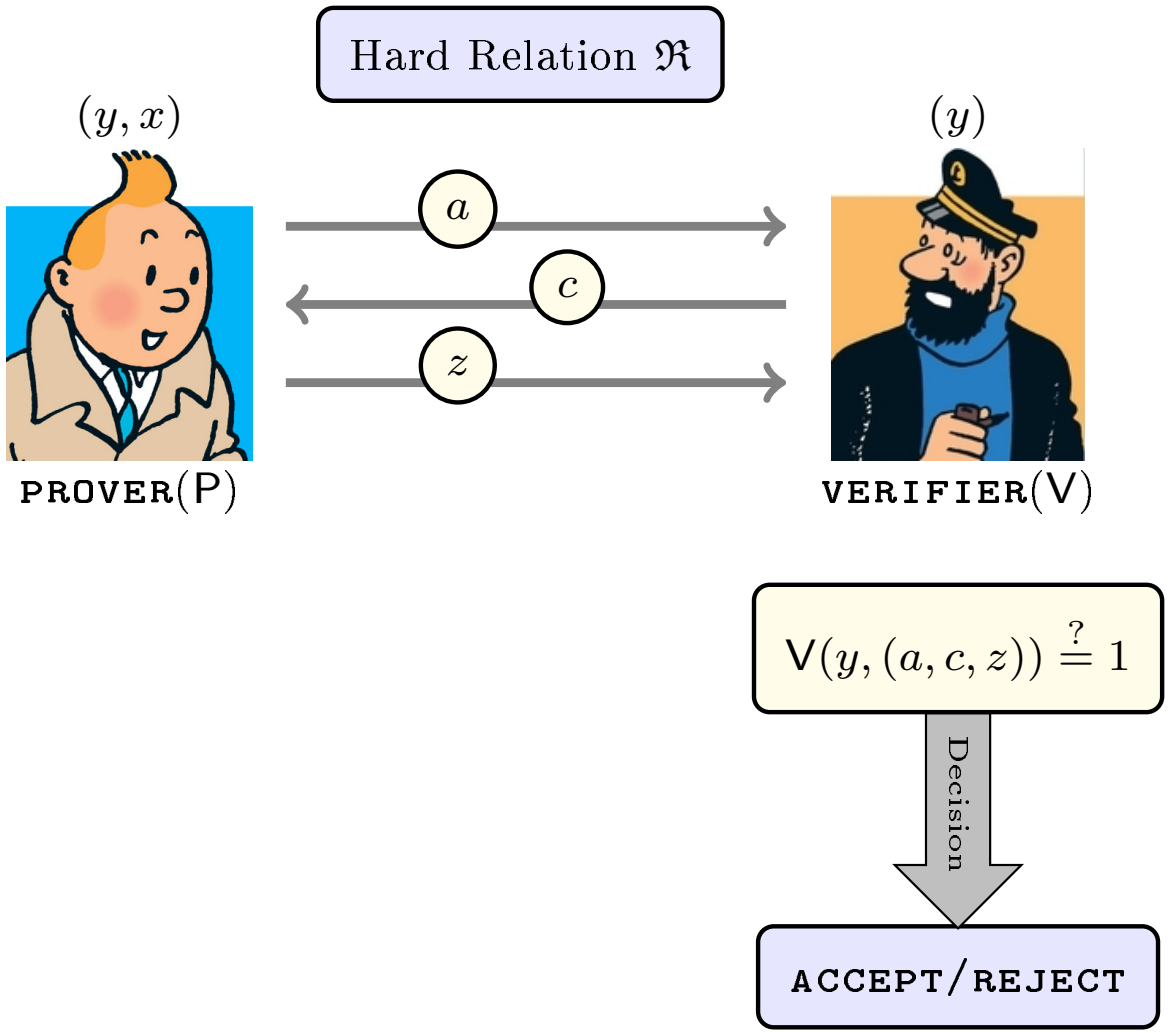
**Hard Relation $\mathfrak{R}$**

**Definition (informal)**

$\mathfrak{R}$ is hard if no PPT adversary can output $(y, x, x')$ such that $(y, x) \in \mathfrak{R} \wedge (y, x') \in \mathfrak{R}$.

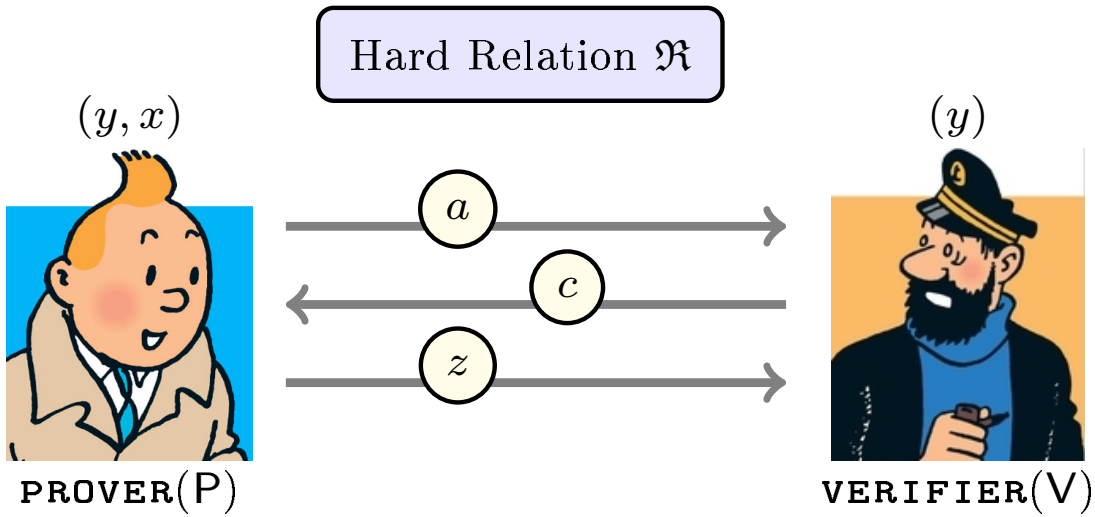
AARHUS UNIVERSITY

# ID-Scheme from Σ-protocol (Cramer '96)



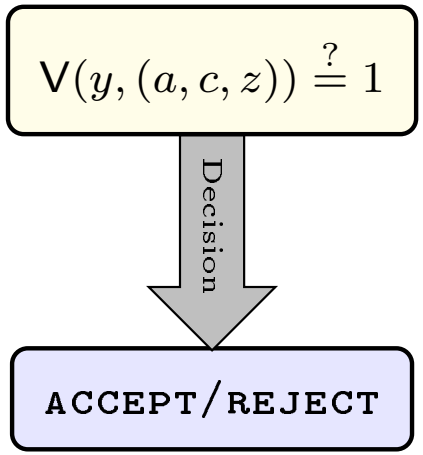

AARHUS UNIVERSITY

# ID-Scheme from Σ-protocol (Cramer '96)




**Theorem(informal)**

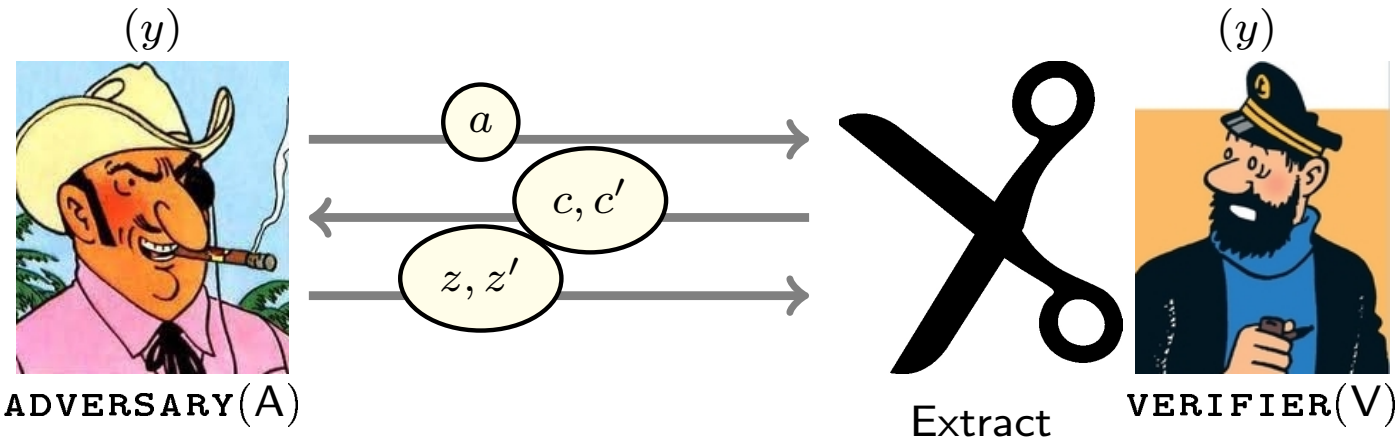
This is BLT-secure for $t \leq \frac{|x|}{|y|} - 1$




AARHUS UNIVERSITY

# ID-Scheme from Σ-protocol (Cramer '96)

Property-1: Special Soundness



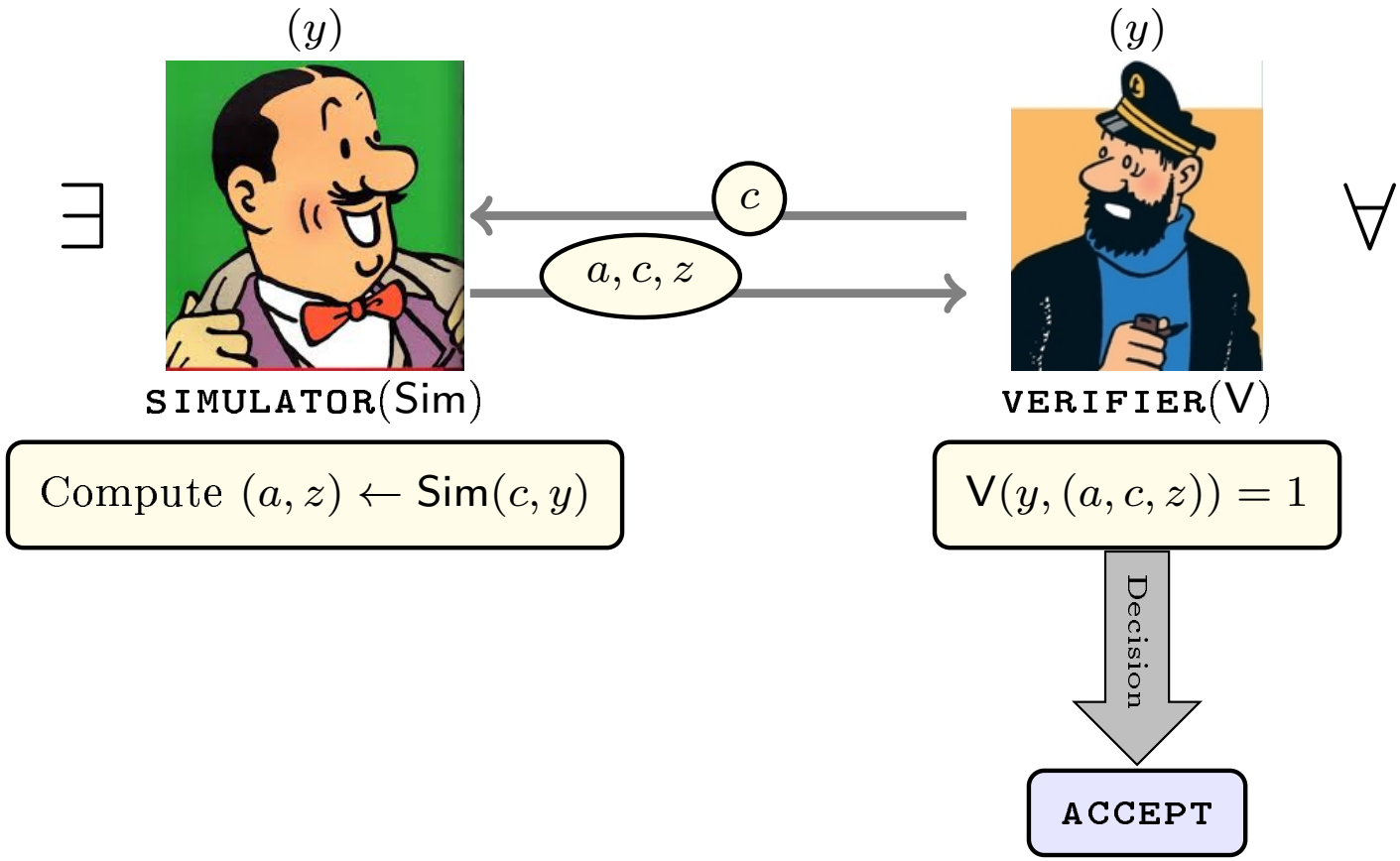

$$\mathsf{V}(y,(a,c,z)) = 1 \wedge \mathsf{V}(y,(a,c',z')) = 1$$

$$(y, x^\star) \in \mathfrak{R} : x^\star \leftarrow \mathsf{Extract}((a,c,z),(a,c',z'))$$

AARHUS UNIVERSITY

# ID-Scheme from Σ-protocol (Cramer '96)

Property-2: Honest Verifier ZK




AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)

Idea

Reduction from the Hard Relation $\mathfrak{R}$

CHALLENGER(C)

REDUCTION(B)

ADVERSARY(A)

AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)

Idea

Reduction from the Hard Relation $\mathfrak{R}$

Hardness Game w.r.t $\mathfrak{R}$

CHALLENGER(C)

REDUCTION(B)

ADVERSARY(A)

Goal: Find $(y, x, x^\star) : (y, x) \in \mathfrak{R} \wedge (y, x^\star) \in \mathfrak{R} \wedge (x \neq x^\star)$

Sample $(y, x) \in \mathfrak{R}$.

AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)

Idea

Reduction from the Hard Relation $\mathfrak{R}$

CHALLENGER(C)

Simulate BLT Game

$(x, y)$ $(y)$

$a$

$c$

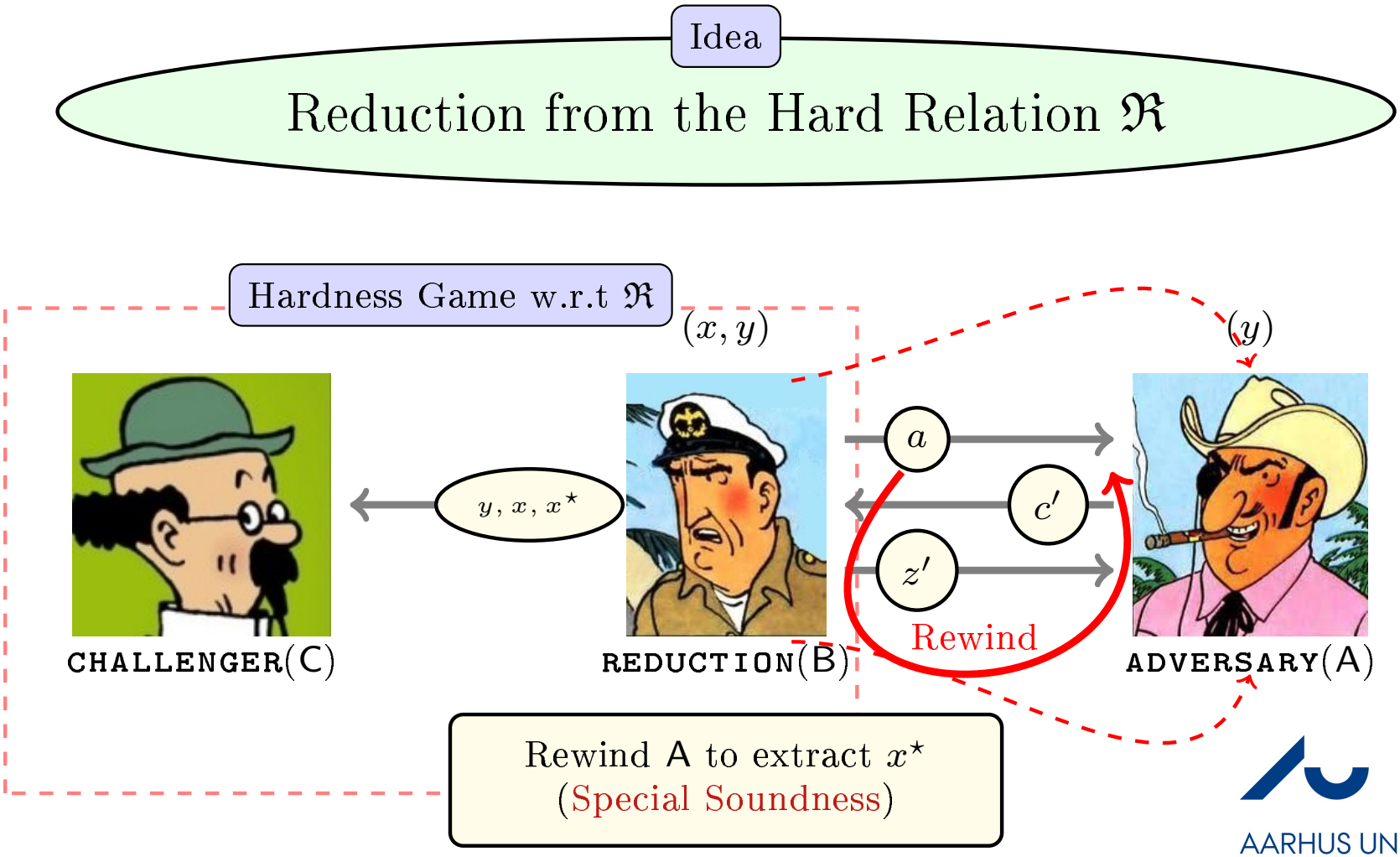
$z$

REDUCTION(B) ADVERSARY(A)

Easy to simulate

AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)




AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)

**Main Challenge**

Each tampering experiment outputs poly-many transcripts–HUGE!
To Prove: This does NOT leak much about $x$.

**Simulate BLT Game**

$(x, y)$

REDUCTION(B)

$(y)$

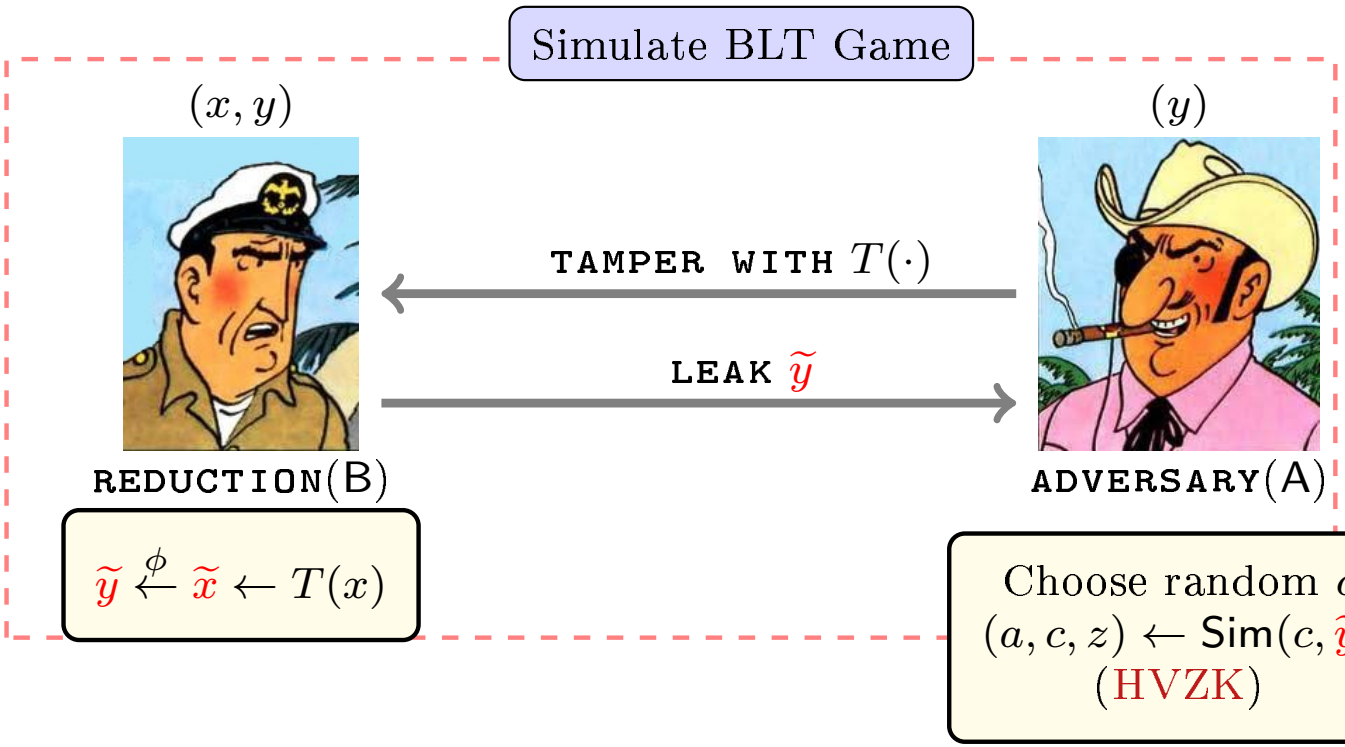
ADVERSARY(A)

AARHUS UNIVERSITY

# BLT-security (Proof Intuitions)

Technique

For each tampering:
LEAK tampered public statement
Only $|y|$ bits – SHORT!




AARHUS UNIVERSITY

# Concrete Instantiation and Signatures

AARHUS UNIVERSITY

# Concrete Instantiation and Signatures

- Generalized Okamoto ID-Scheme is bounded-leakage-resilient – Alwen et al. [CRYPTO'09].

AARHUS UNIVERSITY

# Concrete Instantiation and Signatures

- Generalized Okamoto ID-Scheme is bounded-leakage-resilient – Alwen et al. [CRYPTO'09].
- Also BLT-secure–this work.

AARHUS UNIVERSITY

# Concrete Instantiation and Signatures

- Generalized Okamoto ID-Scheme is bounded-leakage-resilient – Alwen et al. [CRYPTO'09].
- Also BLT-secure–this work.
- Additionally allows tampering with the public parameters (e.g. characteristic prime $p$) – but independently from $sk$! – impossible when tampering jointly.

AARHUS UNIVERSITY

# Concrete Instantiation and Signatures

- Generalized Okamoto ID-Scheme is bounded-leakage-resilient – Alwen et al. [CRYPTO'09].
- Also BLT-secure–this work.
- Additionally allows tampering with the public parameters (e.g. characteristic prime $p$) – but independently from $sk$! – impossible when tampering jointly.
- BLT-secure signatures using Fiat-Shamir transform. – requires random oracles.

AARHUS UNIVERSITY

# IND-CCA-BLT

AARHUS UNIVERSITY

# IND-CCA-BLT

Parameter

$t$

CHALLENGER(C)

$(sk)$

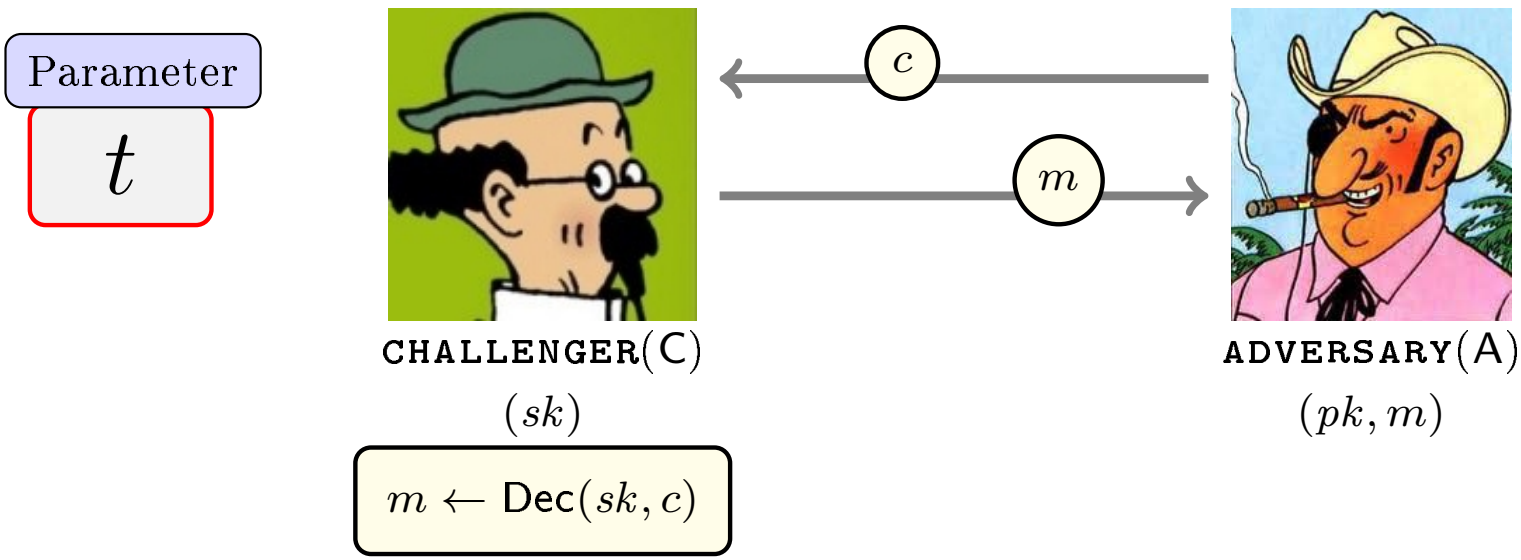
ADVERSARY(A)

$(pk)$

AARHUS UNIVERSITY

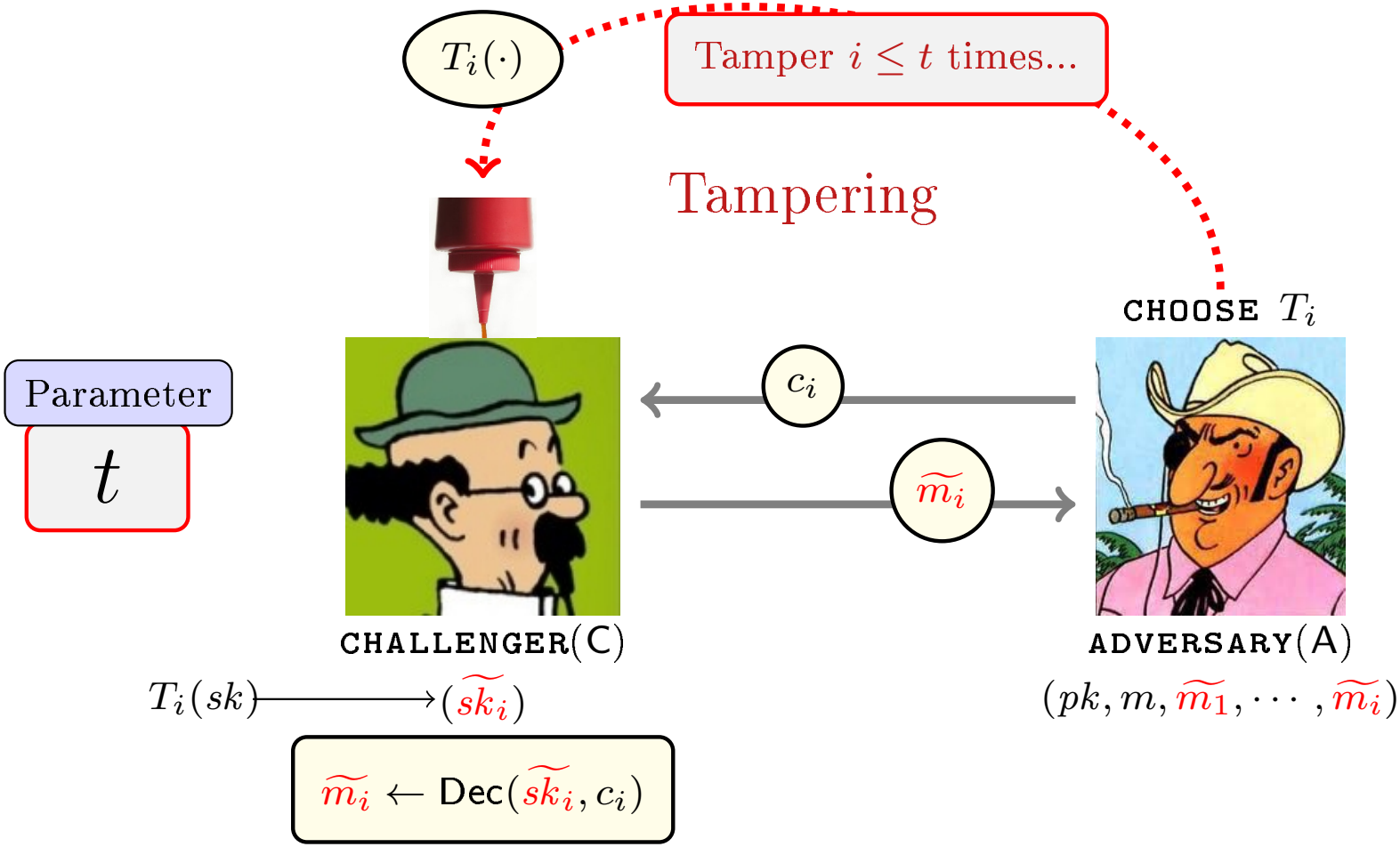
# IND-CCA-BLT

Untampered Query




AARHUS UNIVERSITY

# IND-CCA-BLT




AARHUS UNIVERSITY

# IND-CCA-BLT

## Challenge Phase

Parameter

$t$

$m_0, m_i$

$c^\star$

$b'$

CHALLENGER(C)

ADVERSARY(A)

$(pk, m, \widetilde{m_1}, \cdots, \widetilde{m_i}, \cdots, \widetilde{m_t})$

Choose $b \xleftarrow{\$} \{0,1\}$
$c^\star \leftarrow \mathsf{Enc}(pk, m_b)$

Requirement

$$\left|\Pr[b = b'] - \tfrac{1}{2}\right| \leq negl$$

AARHUS UNIVERSITY

# Results: BLT-secure PKE

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.
2. IND-CPA-BLT $\Longrightarrow$ IND-CCA-BLT – using a tSE-NIZK (similar to Dodis et al.[ASIACRYPT'10])

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.
2. IND-CPA-BLT $\Longrightarrow$ IND-CCA-BLT – using a tSE-NIZK (similar to Dodis et al.[ASIACRYPT'10])

## Concrete Instantiation

BHHO (Boneh et al. [CRYPTO'08])

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.
2. IND-CPA-BLT $\Longrightarrow$ IND-CCA-BLT – using a tSE-NIZK (similar to Dodis et al.[ASIACRYPT'10])

## Concrete Instantiation

BHHO (Boneh et al. [CRYPTO'08])

(Bounded-leakage-resilient– Naor & Segev [CRYPTO'09]).

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.
2. IND-CPA-BLT $\Longrightarrow$ IND-CCA-BLT – using a tSE-NIZK (similar to Dodis et al.[ASIACRYPT'10])

## Concrete Instantiation

BHHO (Boneh et al. [CRYPTO'08])

(Bounded-leakage-resilient– Naor & Segev [CRYPTO'09]).

Idea (similar to ID): simulate tampering queries by additional leakage.

AARHUS UNIVERSITY

# Results: BLT-secure PKE

## A general transformation

Two Steps.

1. A weaker model: IND-CPA-BLT.
2. IND-CPA-BLT $\Longrightarrow$ IND-CCA-BLT – using a tSE-NIZK (similar to Dodis et al.[ASIACRYPT'10])

## Concrete Instantiation

BHHO (Boneh et al. [CRYPTO'08])

(Bounded-leakage-resilient– Naor & Segev [CRYPTO'09]).

Idea (similar to ID): simulate tampering queries by additional leakage.

## Limitation!

Can not tamper(or leak) after challenge phase.

# Continuous tamper-resilience: Floppy Model

Each user has a

AARHUS UNIVERSITY

# Continuous tamper-resilience: Floppy Model

Each user has a

$\mathcal{CS}(sk)$
BLT-secure

$\mathsf{A}(pk)$

AARHUS UNIVERSITY

# Continuous tamper-resilience: Floppy Model

Each user has a

$\mathcal{CS}(sk)$
BLT-secure

$\mathsf{A}(pk)$

**Floppy**

Holds secret update key $uk$
Sample fresh randomness $r$
Update $(sk') \leftarrow \mathsf{Refresh}(uk, r)$

$\mathsf{A}(pk)$

AARHUS UNIVERSITY

# Continuous tamper-resilience: Floppy Model

Each user has a

$\mathcal{CS}(sk)$
BLT-secure

$\mathsf{A}(pk)$

**Floppy**

Holds secret update key $uk$
Sample fresh randomness $r$
Update $(sk') \leftarrow \mathsf{Refresh}(uk, r)$

$\mathsf{A}(pk)$

$\mathcal{CS}(sk')$
BLT-secure

$\mathsf{A}(pk)$

AARHUS UNIVERSITY

# Continuous tamper-resilience: Floppy Model

Each user has a

$\mathcal{CS}(sk)$
BLT-secure

$\mathsf{A}(pk)$

**Floppy**

Holds secret update key $uk$
Sample fresh randomness $r$
Update $(sk') \leftarrow \mathsf{Refresh}(uk, r)$

$\mathsf{A}(pk)$

$\mathcal{CS}(sk')$
BLT-secure

$\mathsf{A}(pk)$

**Results**

1. ID: A general transformation: any BLT-ID + cma-Sig $\Longrightarrow$ Floppy-ID.
2. PKE: A concrete construction from BHHO.

# Continuous tamper-resilience: Floppy Model

Each user has a

$\mathcal{CS}(sk)$
BLT-secure

$\mathsf{A}(pk)$

Floppy

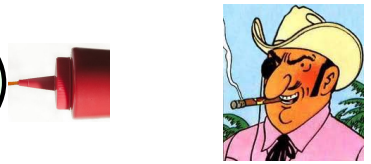
Holds secret update key $uk$
Sample fresh randomness $r$
Update $(sk') \leftarrow \mathsf{Refresh}(uk, r)$

$\mathsf{A}(pk)$

More on Floppy:
by Agrawal et al.
[ASIACRYPT 2013]
Tomorrow...

Hang ON !

$\mathcal{CS}(sk')$
BLT-secure



$\mathsf{A}(pk)$

**Results**

1. ID: A general transformation: any BLT-ID + cma-Sig $\Longrightarrow$ Floppy-ID.
2. PKE: A concrete construction from BHHO.

# Conclusion

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.
- Public-Key Schemes based on Standard Assumptions.

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.
- Public-Key Schemes based on Standard Assumptions.
- New techniques to reduce tamper-resilience from leakage-resilience.

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.
- Public-Key Schemes based on Standard Assumptions.
- New techniques to reduce tamper-resilience from leakage-resilience.
- Open Questions.

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.
- Public-Key Schemes based on Standard Assumptions.
- New techniques to reduce tamper-resilience from leakage-resilience.
- Open Questions.
  - Boosting to continuous tampering model without Floppy.

AARHUS UNIVERSITY

# Conclusion

- First model of Bounded Tamper Resilience.
- Public-Key Schemes based on Standard Assumptions.
- New techniques to reduce tamper-resilience from leakage-resilience.
- Open Questions.
  - Boosting to continuous tampering model without Floppy.
  - Post-challenge tampering for BLT-PKE.

AARHUS UNIVERSITY

# THANK YOU !

Question(s)?

AARHUS UNIVERSITY