Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability

Peter Pessl, Stefan Mangard
IAIK, Graz University of Technology, Austria

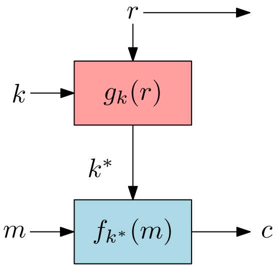
CT-RSA 2016, San Francisco, 3rd March 2016

Overview

- New side-channel attack on Fresh Re-Keying and binary-field multiplication
  - Connection to Learning Parity with Noise (LPN) problem
  - Extensive use of bit reliabilities in order to decrease runtime
- Attack a protected Fresh Re-Keying implementation
  - Using only 512 traces
  - With reasonable runtime

Fresh Re-Keying [MSGR10, MPR+11]

- Goal: SCA protection for low-cost devices
- Combine an encryption function f
- With a re-keying function g
- *Fresh* session key k^* per invocation
    - f is SPA secure
    - g is DPA secure, but not *cryptographically strong*



Re-Keying Function

- Polynomial multiplication modulo $y^{16} + 1$ over GF(2^8)
  - Good diffusion
  - Easy to protect (masking, shuffling)
- Rewrite as matrix-vector product over bytes and bits
  - Linear equation in master-key bits
  - Risk in SCA setting (SPA security?)

$$\begin{pmatrix} r_0 & r_{15} & r_{14} & \cdots & r_1 \\ r_1 & r_0 & r_{15} & \cdots & r_2 \\ r_2 & r_1 & r_0 & \cdots & r_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{15} & r_{14} & r_{13} & \cdots & r_0 \end{pmatrix} \begin{pmatrix} k_0 \\ k_1 \\ k_2 \\ \vdots \\ k_{15} \end{pmatrix} = \begin{pmatrix} k_0^* \\ k_1^* \\ k_2^* \\ \vdots \\ k_{15}^* \end{pmatrix}$$

SCA of Binary-Field Multiplication

Attacks of Belaïd et al. [BFG14, BCF+15]

- Multiplication in GF(2^n)
- Noisy Hamming weight of each n-bit product
  - With, e.g., $n = 128$
  - Round to either 0 or $2^n - 1$
- Linear equations in bits, but with errors

LPN - Learning Parity with Noise

Definition: Learning Parity with Noise

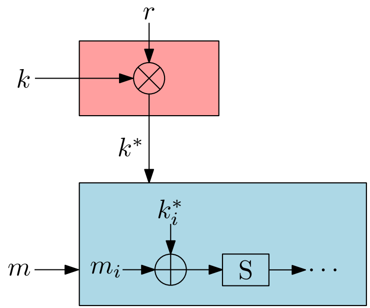
- ν equations $b_i = \langle \mathbf{a}_i, \mathbf{k} \rangle + e_i$
- Secret **k**, public random $\mathbf{a}_i$ (n-bit vectors), $\mathrm{P}(e_i = 1) = \epsilon$
- find **k**

Solving algorithms

- BKW-based (high ν, sub-exponential runtime) (used by Belaïd et al.)
- Linear decoding (low ν, exponential runtime)

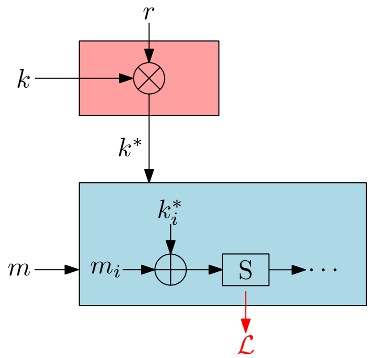
Our Attack

Chosen Target



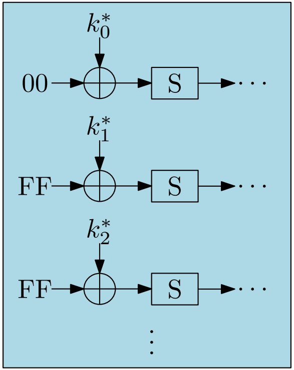
- Protected Fresh Re-Keying implementation (8-bit software) [MPR+11]
- Multiplication: masked and shuffled
- AES: shuffled

Template Attack on the S-box



- Product k^* is used in AES
  - AES *only* SPA secure
- Templates on S-box
- Probability vector for key-bytes
- Turn them into bit-wise probabilities

Countering the Shuffling



- Application: challenge-response auth.
  - Verifier choses plaintexts
- Chosen fixed plaintext: $(00)||(FF)^{15}$
- Templates for both cases
  - Reveal one position
  - Independent of permutation generation

Outcome of the physical attack

- Vector of probabilities for session-key bits b
  - $p_b = \mathrm{P}(b = 1)$, bias $\tau_b = |p_b - 0.5|$
  - Classification: $b = \lfloor p_b \rceil$, $\epsilon_b = 0.5 - \tau_b$
- Each entry an LPN sample
  - but with additional information (ϵ_b)

A New LPN Variant

Definition: Learning Parity with Variable Noise

- ν equations $b_i = \langle \mathbf{a}_i, \mathbf{k} \rangle + e_i$
- Secret **k**, public random **a** (bit vectors)
- $\mathrm{P}(e_i = 1) = \epsilon_i$, ϵ_i sampled from meta-distribution ψ
- Find **k**

Incorporation of ϵ_i might lead to faster algorithms.

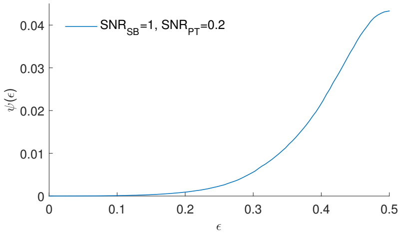
Our LPVN algorithm

Filtering

- Discard samples with high ϵ_b
- Similar to Belaïd et al., but bit-wise

Linear Decoding

- Tweaked algorithm incorporating probabilities



Typical meta-probability $\psi(\epsilon)$

LPN and Decoding

Decoding problem:

- Given a generator matrix $\mathbf{G}$ and noisy word $\mathbf{y} = \mathbf{G}^\mathsf{T}\mathbf{k} + \mathbf{e}$
- find $\mathbf{e}$ or $\mathbf{k}$

Syndrome decoding:

- Check matrix $\mathbf{H}$ and syndrome $\mathbf{s} = \mathbf{H}\mathbf{y} = \mathbf{H}\mathbf{e}$
- Search for $\mathbf{e}$ (w columns of $\mathbf{H}$ with sum $\mathbf{s}$)

Stern’s Algorithm for Random Linear Codes

- Randomly partition columns of **H** into sets $\mathcal{Q}, \mathcal{I}$
- Transform $\mathcal{I}$ to identity, search for errors of particular form
- Optimization: swap columns between $\mathcal{Q}$ and $\mathcal{I}$ [BLP08]

$$\mathbf{H}_p = (\mathcal{Q}|\mathcal{I}) = \begin{array}{c} \begin{array}{ccc} \overbrace{\hphantom{1 \quad 0 \quad 0 \cdots}}^{p \text{ err.}} & \overbrace{\hphantom{\cdots 0 \quad 1 \quad 0}}^{p \text{ err.}} & \overbrace{\hphantom{1 \quad 1 \quad 1}}^{0 \text{ err.}} \hphantom{\quad 1 \quad 1} \end{array} \\ \left(\begin{array}{cccccc|ccccc} 1 & 0 & 0 \cdots & \cdots 0 & 1 & 0 & 1 & & & & \\ 1 & 1 & 0 \cdots & \cdots 0 & 0 & 0 & & 1 & & & \\ 0 & 1 & 1 \cdots & \cdots 1 & 1 & 1 & & & 1 & & \\ & & \vdots & \vdots & & & & & & \ddots & \\ 0 & 1 & 1 \cdots & \cdots 1 & 0 & 1 & & & & & 1 \end{array}\right) \end{array}$$

Tweaked Stern

- Each entry of **e** / column of **H** corresponds to LPVN sample
  - with attached probability
- Reliability-guided swapping of columns
  - Rejection sampling based on bias
  - Keep number of errors in $\mathcal{Q}$ low
  - While still behaving randomly

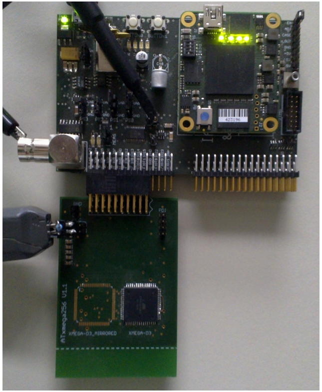
Attack Results

Simulation

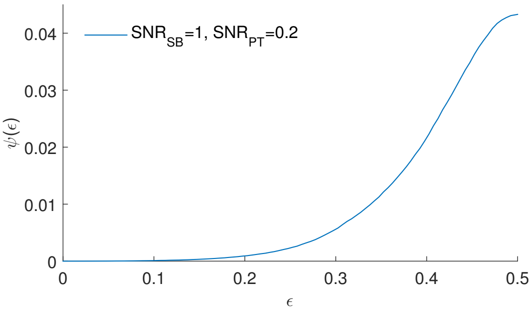
- 8-bit with shuffling countermeasure
- Noisy Hamming weights

Real device

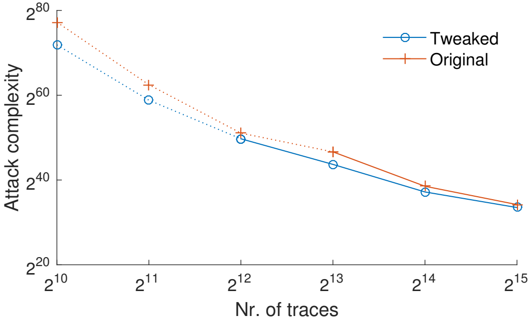
- Power measurements
- Profiling



Results - Simulation

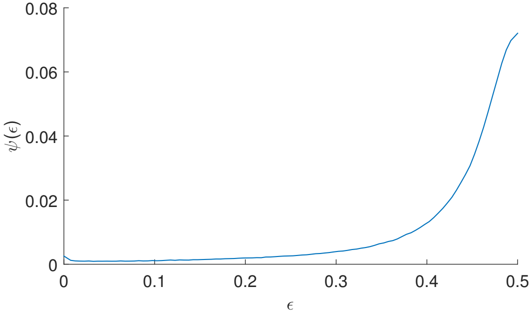


Meta-probability $\psi(\epsilon)$

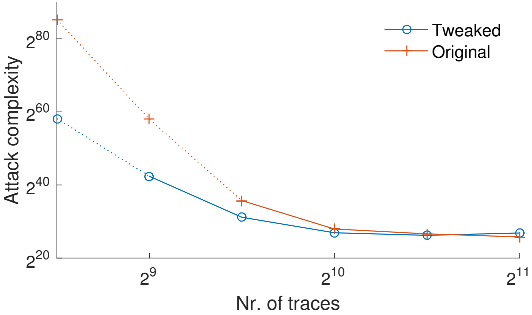


Runtime complexity

Results - Real Device



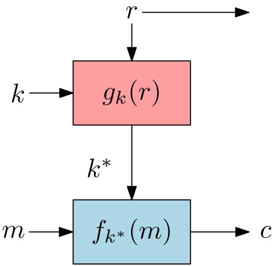
Meta-probability $\psi(\epsilon)$



Runtime complexity

Conclusions

- Attack with small trace count and reasonable runtime
  - Without violating the constraints of Fresh Re-Keying
  - AES still SPA secure
- Implications for Fresh Re-Keying
  - Separations of responsibilities not trivial
  - Protect re-keying output in all stages



Enhancing Side-Channel Analysis of Binary-Field Multiplication with Bit Reliability

Peter Pessl, Stefan Mangard
IAIK, Graz University of Technology, Austria

CT-RSA 2016, San Francisco, 3rd March 2016

Bibliography I

[BCF+15] Sonia Belaïd, Jean-Sébastien Coron, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff. Improved Side-Channel Analysis of Finite-Field Multiplication. *IACR Cryptology ePrint Archive*, 2015:542, 2015. note: to appear at CHES 2015.

[BFG14] Sonia Belaïd, Pierre-Alain Fouque, and Benoît Gérard. Side-Channel Analysis of Multiplications in GF(2^{128}) - Application to AES-GCM. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014*, volume 8874 of *Lecture Notes in Computer Science*, pages 306–325. Springer, 2014.

[BLP08] Daniel J. Bernstein, Tanja Lange, and Christiane Peters. Attacking and Defending the McEliece Cryptosystem. In Johannes A. Buchmann and Jintai Ding, editors, *Post-Quantum Cryptography, Second International Workshop, PQCrypto 2008*, volume 5299 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2008.

[MPR+11] Marcel Medwed, Christophe Petit, Francesco Regazzoni, Mathieu Renauld, and François-Xavier Standaert. Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks. In Emmanuel Prouff, editor, *Smart Card Research and Advanced Applications - 10th IFIP WG 8.8/11.2 International Conference, CARDIS 2011*, volume 7079 of *Lecture Notes in Computer Science*, pages 115–132. Springer, 2011.

[MSGR10] Marcel Medwed, François-Xavier Standaert, Johann Großschädl, and Francesco Regazzoni. Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In Daniel J. Bernstein and Tanja Lange, editors, *Progress in Cryptology - AFRICACRYPT 2010*, volume 6055 of *Lecture Notes in Computer Science*, pages 279–296. Springer, 2010.

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CRYP-R03

Towards a Unified Security Model for Physically Unclonable Functions

Daisuke Moriyama
Researcher
NICT

#RSAC

Authors of this paper




Frederik Armknecht (University of Mannheim)

Daisuke Moriyama (NICT)

Ahmad-Reza Sadeghi (TU Darmstadt)

Moti Yung (Google/Columbia Univ)

Introduction



Which is iPhone ?




Which is Louis Vuitton's product?

Introduction

We need unique identification of device/goods for IoT world

- Device ID or RFID tag is useless if the internal information is copied

⇩

Physical uniqueness during fabrication is useful !

Yield variance is not bad effect but uniqueness!

⇩

Physically Unclonable Functions (PUFs)

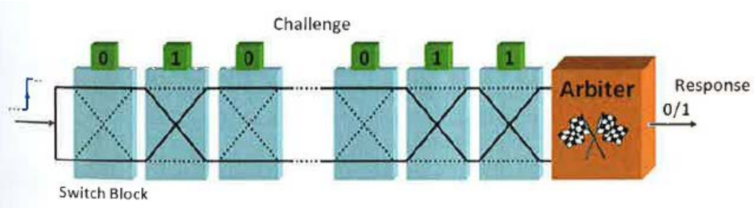
Cryptographic Brief Definition of PUFs

Input → PUF → Output

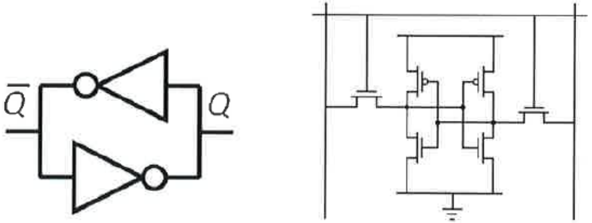
1. Given an input, it is easy to evaluate the output

2. It is difficult to produce another device which the two devices respond the same output from the same input.

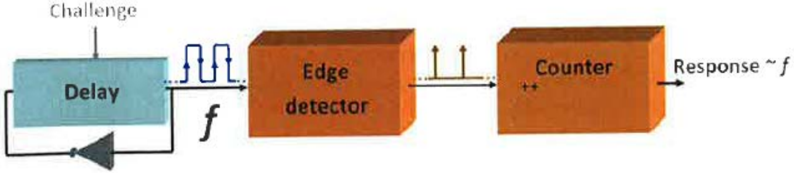
Example PUF constructions



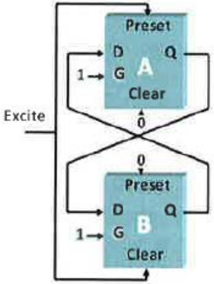
Arbiter PUFs



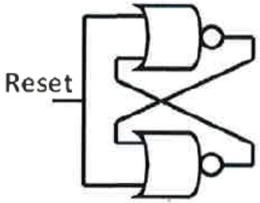
SRAM PUFs



Ring Oscillator PUFs



Butterfly PUFs

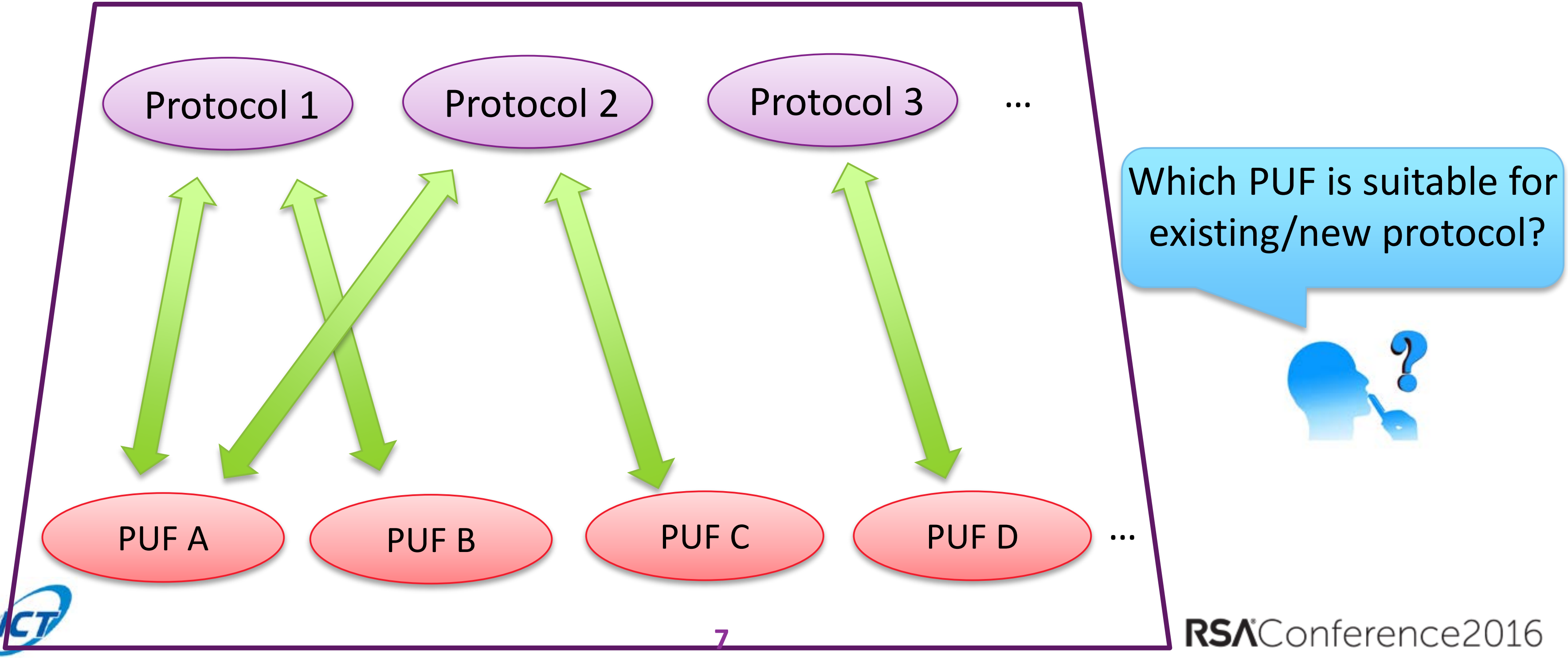


Latch PUFs

New constructions are discovered almost every year !!!

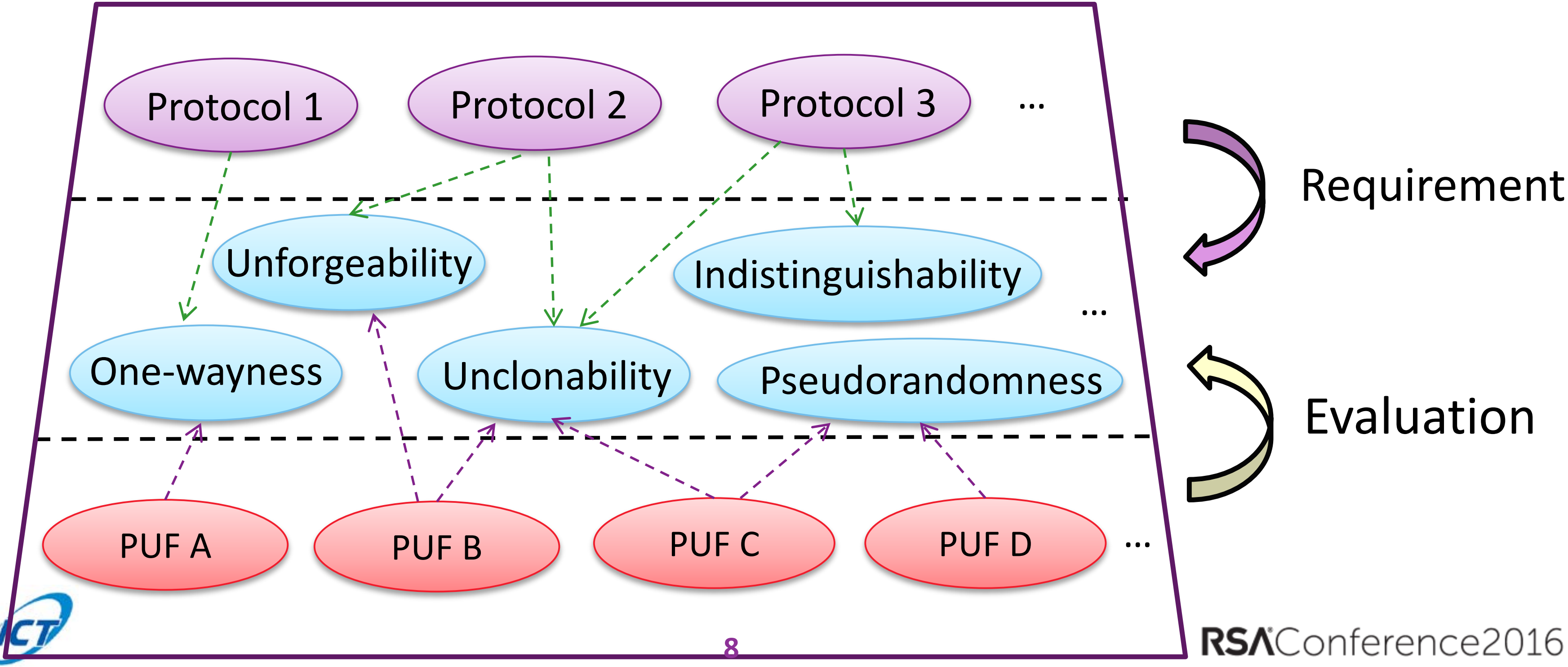
Application of PUFs in Cryptography

- PUF is expected to be used in cryptographic protocols…



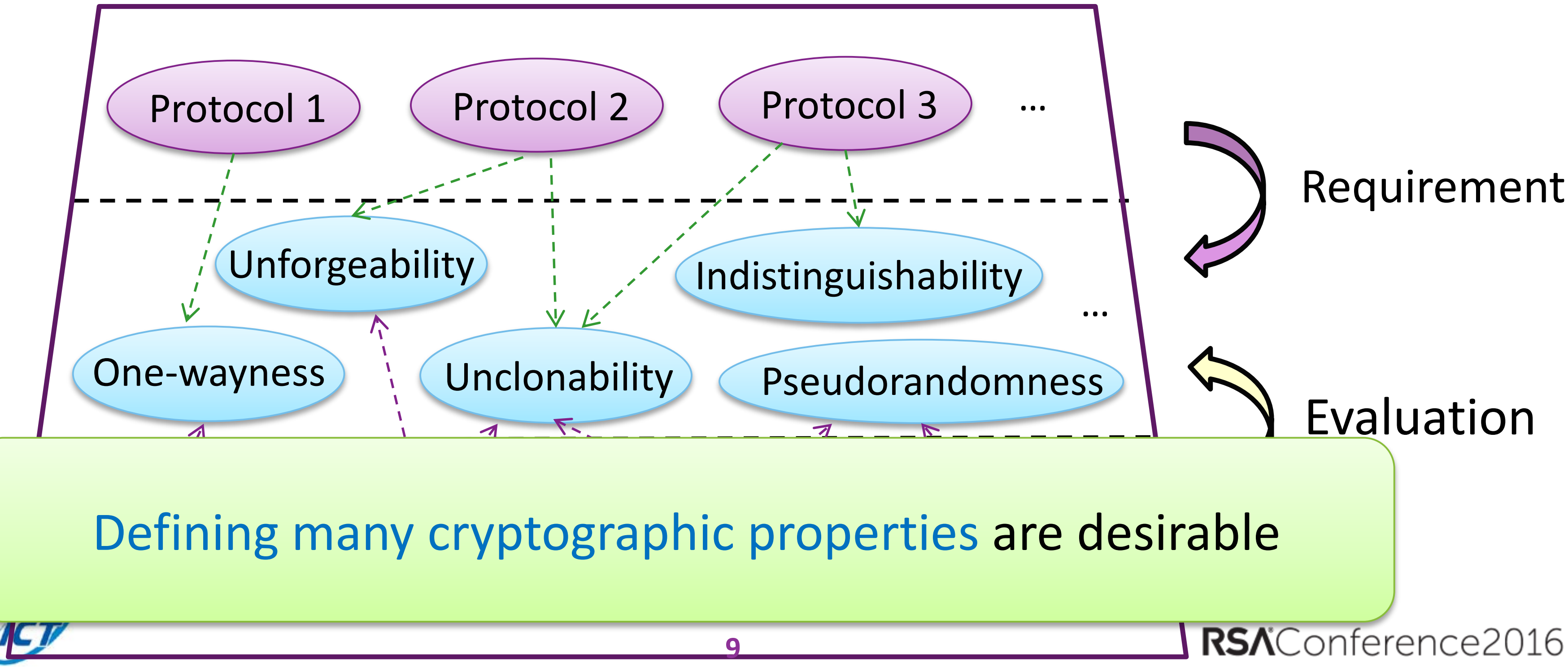
What we think

- Bridge them by security model !!



What we think

- Bridge them by security model !!

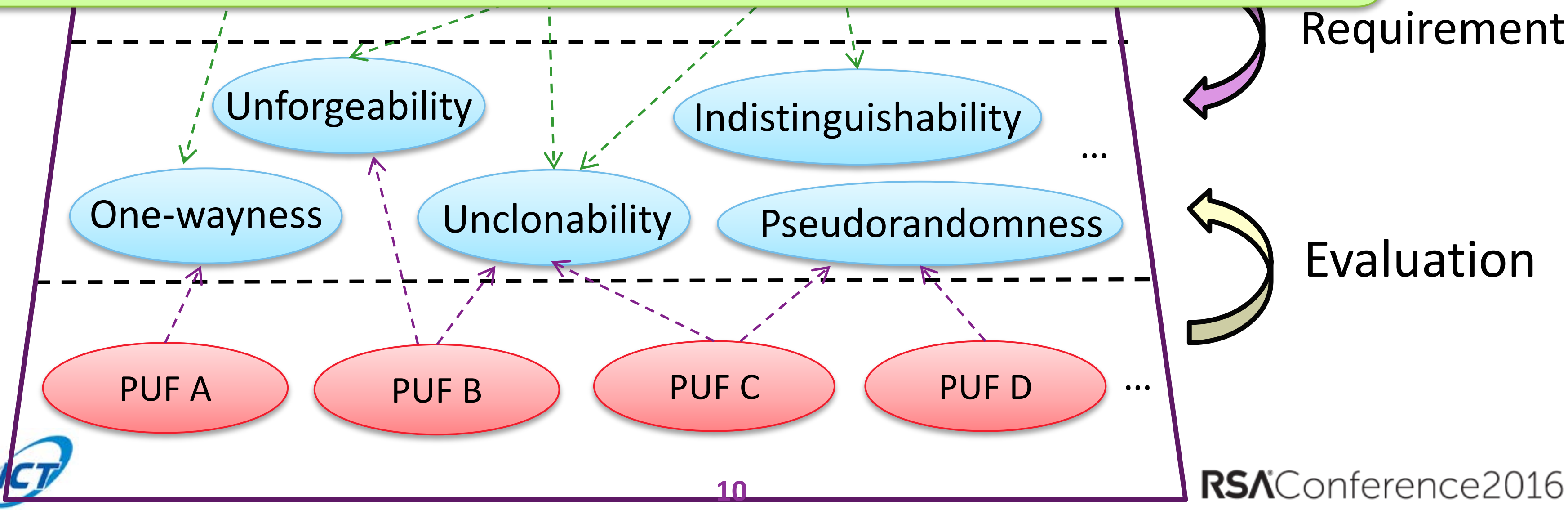


Defining many cryptographic properties are desirable

What we think

- Bridge them by security model !!

We cannot ignore real effects caused in physical device
(noisy outputs, correlation among devices, etc...)



Security model

Our *Unified* Security Model for PUFs

Security model: Manufacturing

PUF is denoted as function $f : \mathcal{D} \to \mathcal{R}$

But we should not simply say like “XXX PUF is good”…

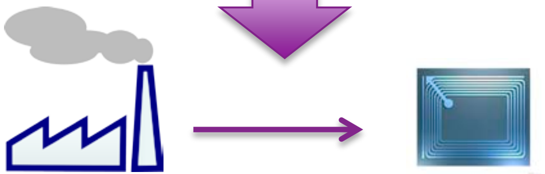
- 130nm process
- 90nm process
- 65nm process
- ⋮

- FPGA (Xillinx,Altera,…)
- Custom ASIC
- SRAM (ISSI,Micron,…)
- ⋮

- Made in USA
- Made in China
- Made in Japan
- ⋮

…

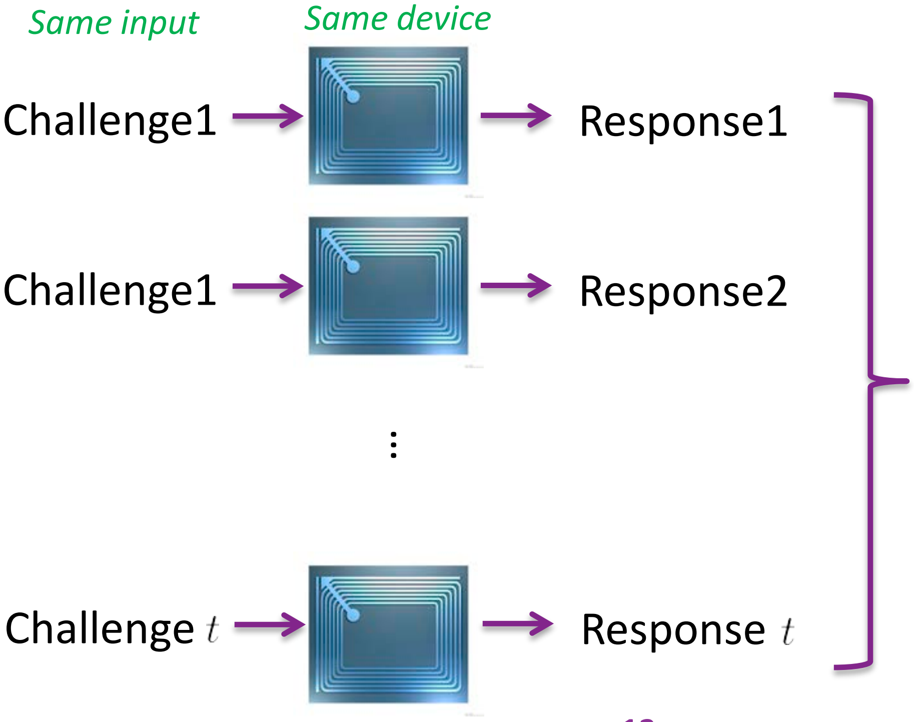
We treat



$\mathcal{MP}(param)$ f

Security model: Output distribution

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, t, \ell, n, \delta_1, \delta_2, \delta_3, \epsilon)$-variance and $(\mathcal{MP}, n, \ell, \delta_4, \epsilon)$-min-entropy if

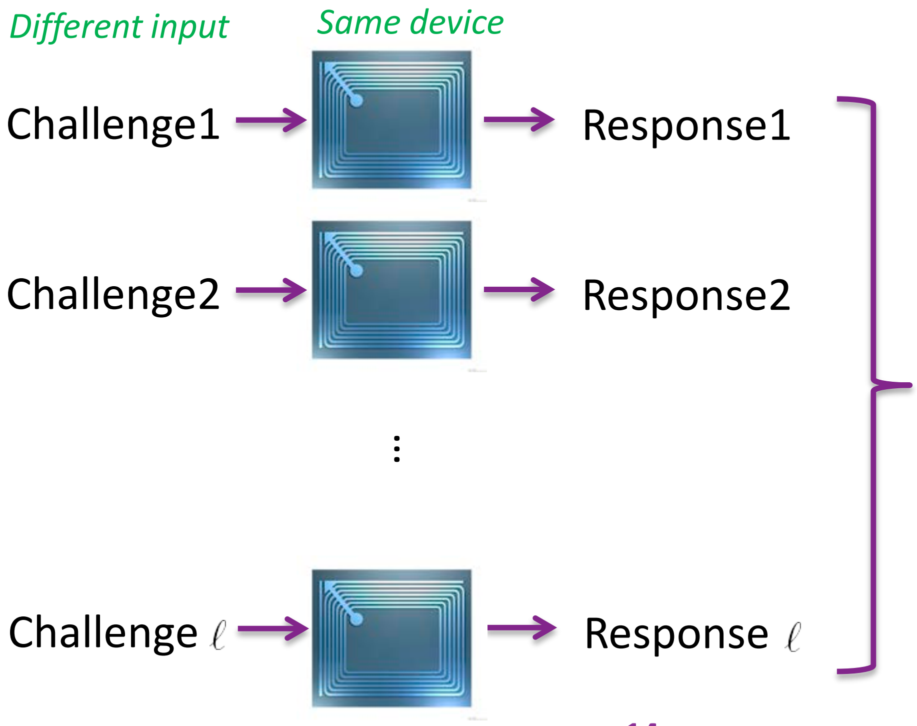


Distance among any pairs are smaller than δ_1

Intra-distance

Security model: Output distribution

$f : \mathcal{D} \rightarrow \mathcal{R}$ has $(\mathcal{MP}, t, \ell, n, \delta_1, \delta_2, \delta_3, \epsilon)$-variance and $(\mathcal{MP}, n, \ell, \delta_4, \epsilon)$-min-entropy if



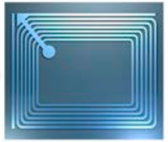
Distance among any pairs are larger than δ_2

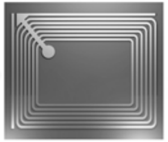
Inter-distance I

Security model: Output distribution

$f : \mathcal{D} \rightarrow \mathcal{R}$ has $(\mathcal{MP}, t, \ell, n, \delta_1, \delta_2, \delta_3, \epsilon)$-variance and $(\mathcal{MP}, n, \ell, \delta_4, \epsilon)$-min-entropy if

Same input *Different device*

Challenge1 →  → Response1

Challenge1 →  → Response2

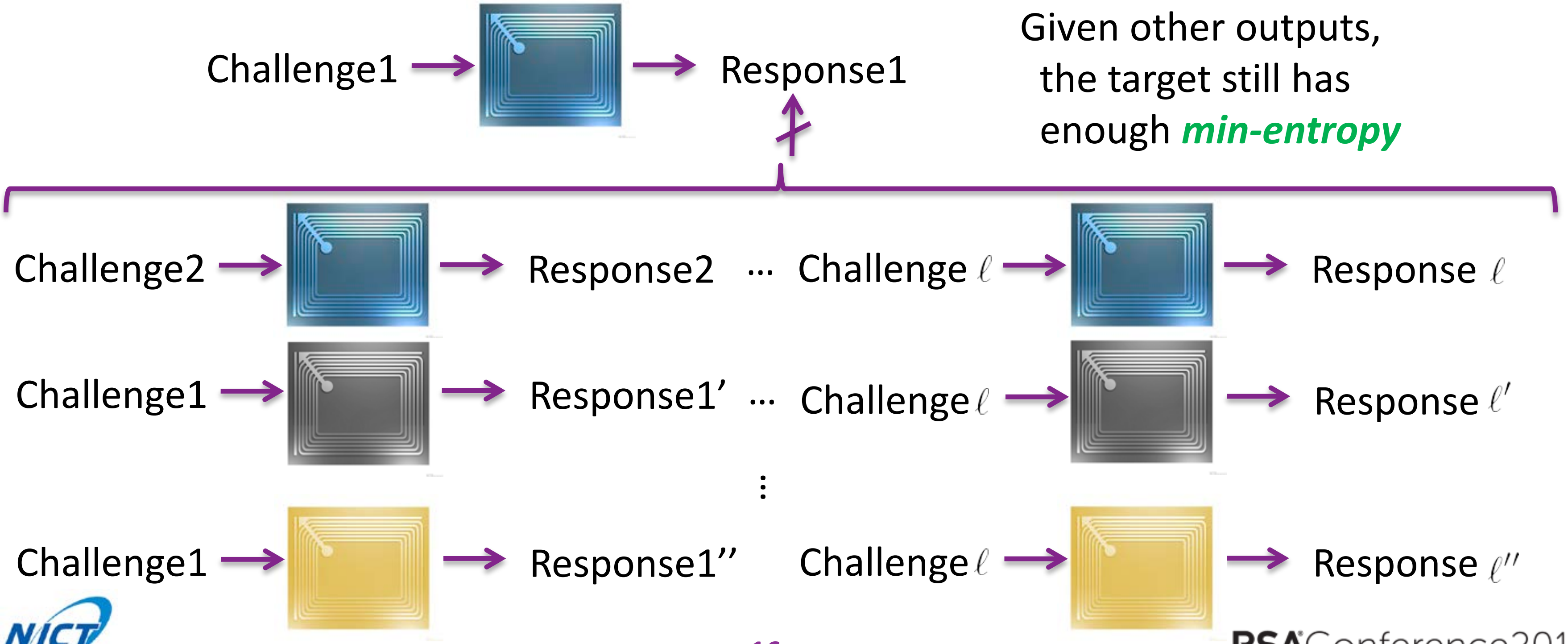
Challenge1 →  → Response n

Distance among any pairs are larger than δ_3

Inter-distance II

Security model: Output distribution

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, t, \ell, n, \delta_1, \delta_2, \delta_3, \epsilon)$-variance and $(\mathcal{MP}, n, \ell, \delta_4, \epsilon)$-min-entropy if



Given other outputs, the target still has enough ***min-entropy***

Security model: Output distribution

$f : \mathcal{D}$ ... py if

These are formal definitions provided in proceeding

Intra-distance:

$$\Pr\left[\max(\{\mathsf{Dist}(z_i, z_j)\}_{i \neq j}) \leq \delta_1 \mid \{z_i \mid x_1 \in \mathcal{K}, y_1 \in \mathcal{D}, z_i \xleftarrow{\mathsf{R}} f_1(y_1)\}_{1 \leq i \leq t}\right] = 1 - \epsilon(\lambda)$$

Inter-distance I:

$$\Pr\left[\min(\{\mathsf{Dist}(z_i, z_j)\}_{i \neq j}) \geq \delta_2 \mid \{z_i \mid x_1 \in \mathcal{K}, y_i \xleftarrow{\mathsf{U}} \mathcal{D}, z_i \xleftarrow{\mathsf{R}} f_1(y_i)\}_{1 \leq i \leq \ell}\right] = 1 - \epsilon(\lambda)$$

Inter-distance II:

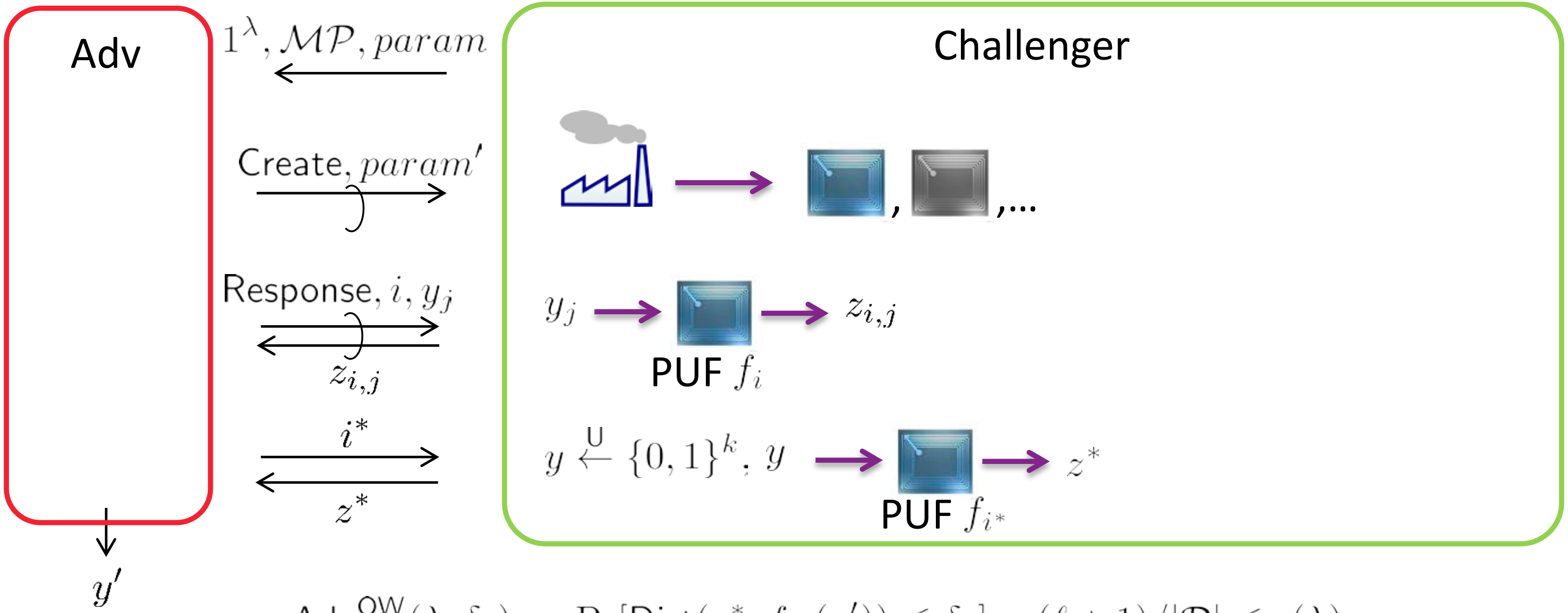
$$\Pr\left[\min(\{\mathsf{Dist}(z_i, z_j)\}_{i \neq j}) \geq \delta_3 \mid \{z_i \mid x_i \in \mathcal{K}, y_1 \in \mathcal{D}, z_i \xleftarrow{\mathsf{R}} f_i(y_1)\}_{1 \leq i \leq n}\right] = 1 - \epsilon(\lambda)$$

Min-entropy:

$$\Pr\left[\tilde{H}_\infty(z_1 \mid \mathcal{Z}_{i,j} \setminus z_1) \geq \delta_4 \;\middle|\; \begin{array}{l} x_1, \ldots, x_n \in \mathcal{K}, y_1, \ldots, y_\ell \in \mathcal{D}, \\ \mathcal{Z} := \{z_{i,j} \xleftarrow{\mathsf{R}} f_i(y_j)\}_{1 \leq i \leq n, 1 \leq j \leq \ell}, \mathcal{Z}_{i,j} := \mathcal{Z} \setminus z_{i,j} \end{array}\right] = 1 - \epsilon(\lambda)$$

Security model: One-wayness

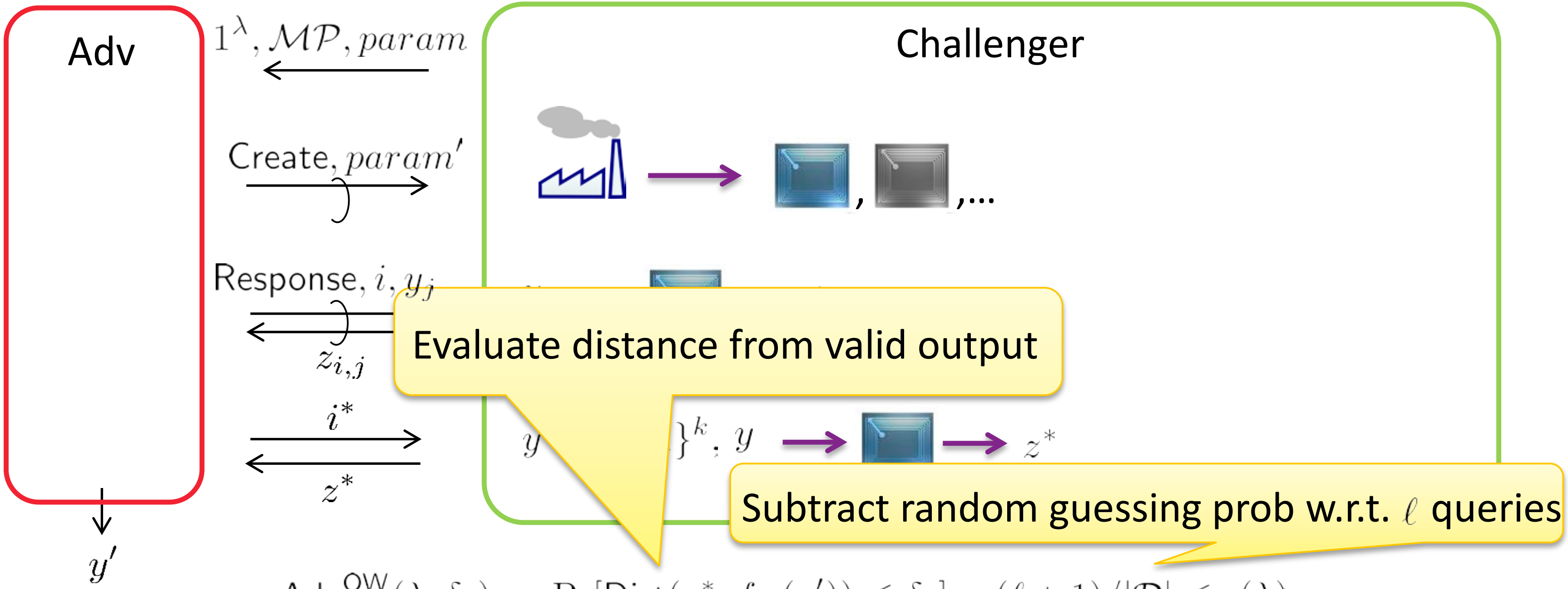
$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-one-wayness if



$$\mathsf{Adv}^{\mathsf{OW}}_{\mathcal{A}}(\lambda, \delta_1) := \Pr[\mathsf{Dist}(z^*, f_{i^*}(y')) \le \delta_1] - (\ell+1)/|\mathcal{D}| \le \epsilon(\lambda)$$

Security model: One-wayness

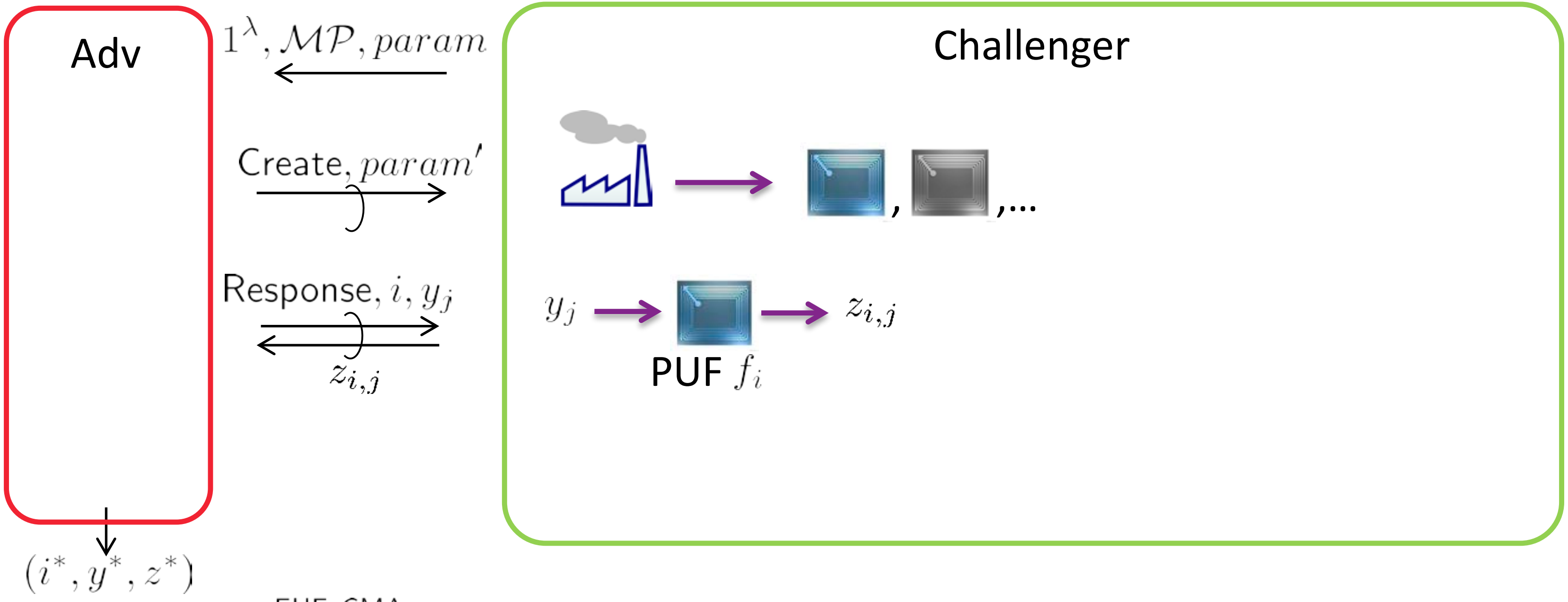
$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-one-wayness if



$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{OW}}(\lambda, \delta_1) := \Pr[\mathsf{Dist}(z^*, f_{i^*}(y')) \leq \delta_1] - (\ell + 1)/|\mathcal{D}| \leq \epsilon(\lambda)$$

Security model: Unforgeability

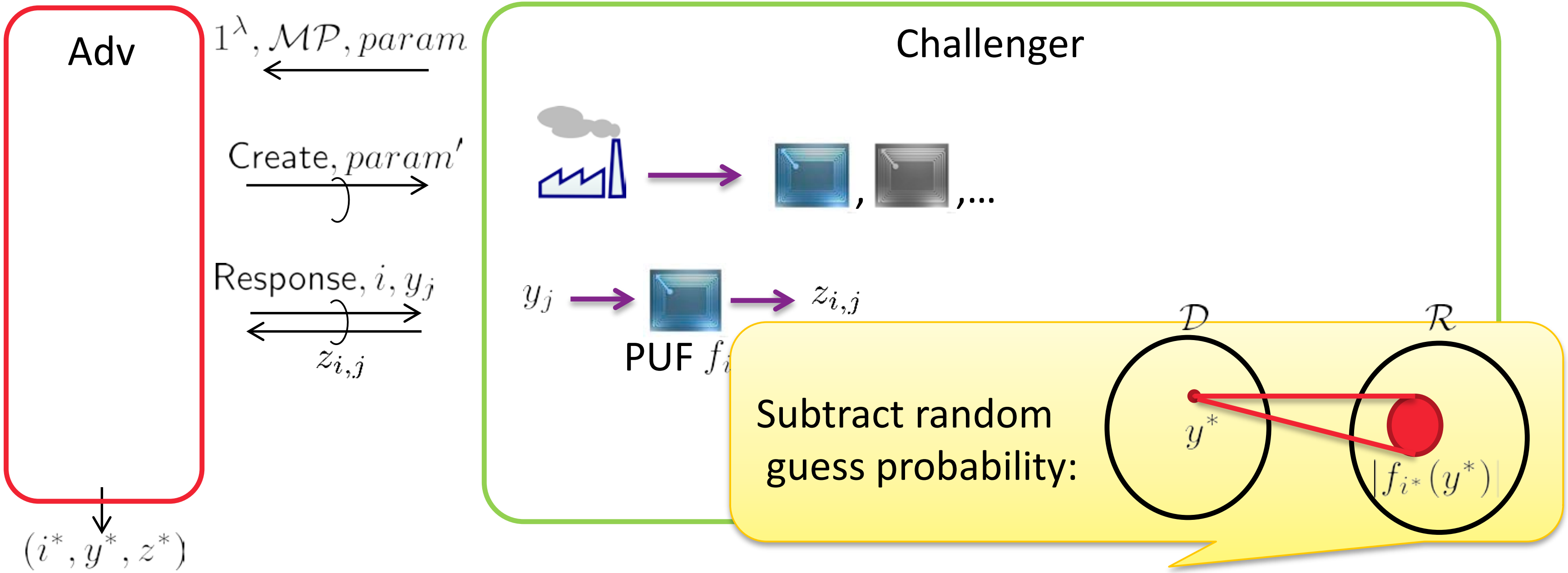
$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-EUF-CMA security if



$$\mathsf{Adv}_{\mathcal{A}}^{\text{EUF-CMA}}(\lambda, \delta_1) := \Pr\left[\mathsf{Dist}(z^*, f_{i^*}(y^*)) \leq \delta_1\right] - |f_{i^*}(y^*)|/|\mathcal{R}| \leq \epsilon(\lambda)$$

Security model: Unforgeability

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-EUF-CMA security if



$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{EUF\text{-}CMA}}(\lambda, \delta_1) := \Pr[\mathsf{Dist}(z^*, f_{i^*}(y^*)) \le \delta_1] - |f_{i^*}(y^*)|/|\mathcal{R}| \le \epsilon(\lambda)$$

Security model: Unforgeability

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-EUF-CMA security if

Pappu (PhD Thesis 2001)	$\longrightarrow$	$(\cdot, 1, 1, 0, \epsilon)$-UUF-KOA
Gassend et al. (ACMCCS 2002)	$\longrightarrow$	$(\cdot, 1, \text{poly}, 0, \epsilon)$-UUF-KMA
Guajardo et al. (CHES 2007)	$\longrightarrow$	$(\cdot, 1, 1, 0, \epsilon)$-UUF-OT-KMA, $(\cdot, 0, 0, 0, \epsilon)$-EUF-KOA
Armknecht et al. (IEEE S&P 2011)	$\longrightarrow$	$(\cdot, \text{poly}, \text{poly}, 0, \epsilon)$-UUF-KMA, $(\cdot, \text{poly}, \text{poly}, 0, \epsilon)$ -EUF-CMA
Brzuska et al. (CRYPTO 2011)	$\longrightarrow$	$(\cdot, 1, \text{poly}, 0, \epsilon)$-EUF-CMA

Our model is the *generalized* version

Security model: Unclonability

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \delta_1, \epsilon)$-unlonability if

Adv

$1^\lambda, \mathcal{MP}, param$

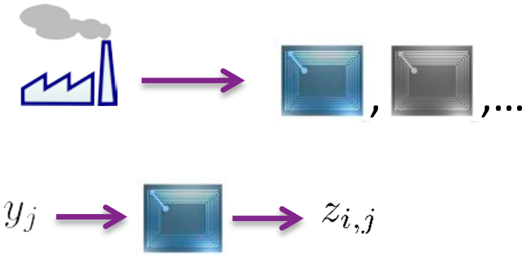
Create, $param'$

Response, i, y_j

$z_{i,j}$

(i^*, b^*, j^*)

Challenger



y_j $z_{i,j}$

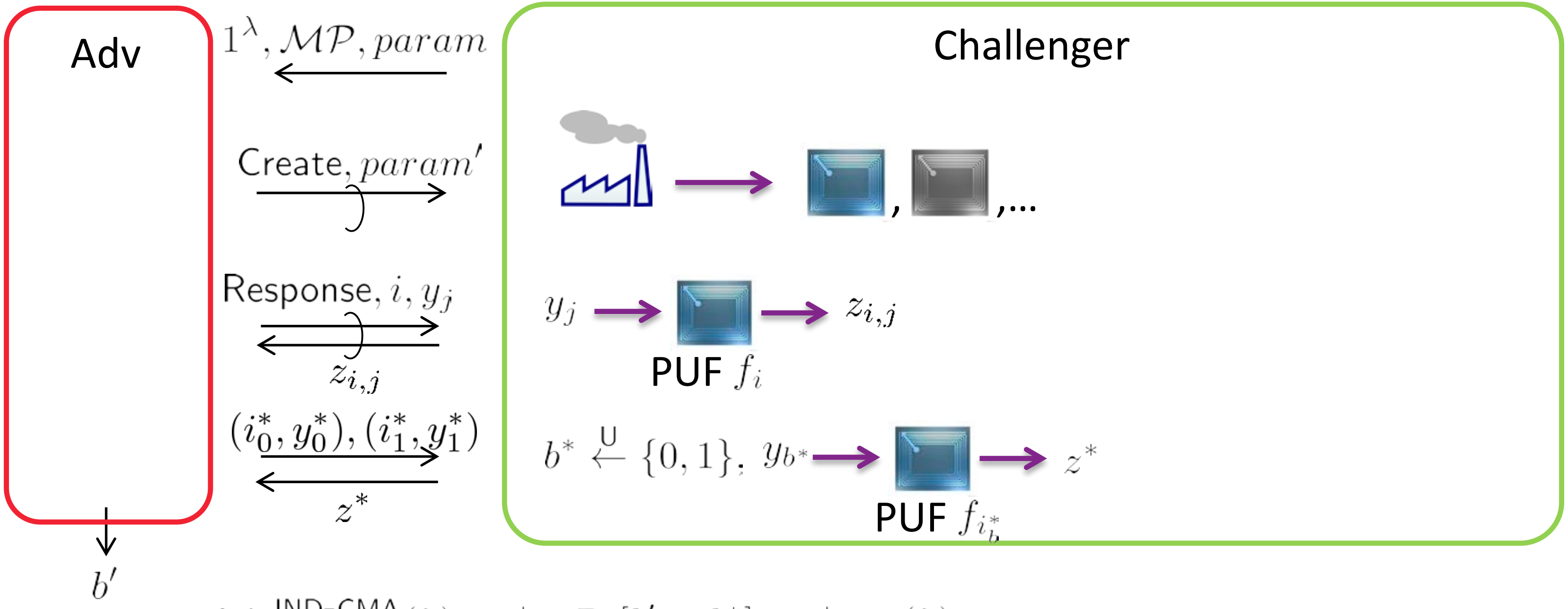
PUF f_i

f'_{j^*} behaves as f_{i^*}

$$\mathsf{Adv}_{\mathcal{A}}^{\mathsf{clone}}(\lambda, \delta_1) := \Pr\left[\forall y \in \mathcal{D}, \mathsf{Dist}(f_{i^*}(y), f'_{j^*}(y)) \leq \delta_1\right] \leq \epsilon(\lambda)$$

Security model: Indistinguishability

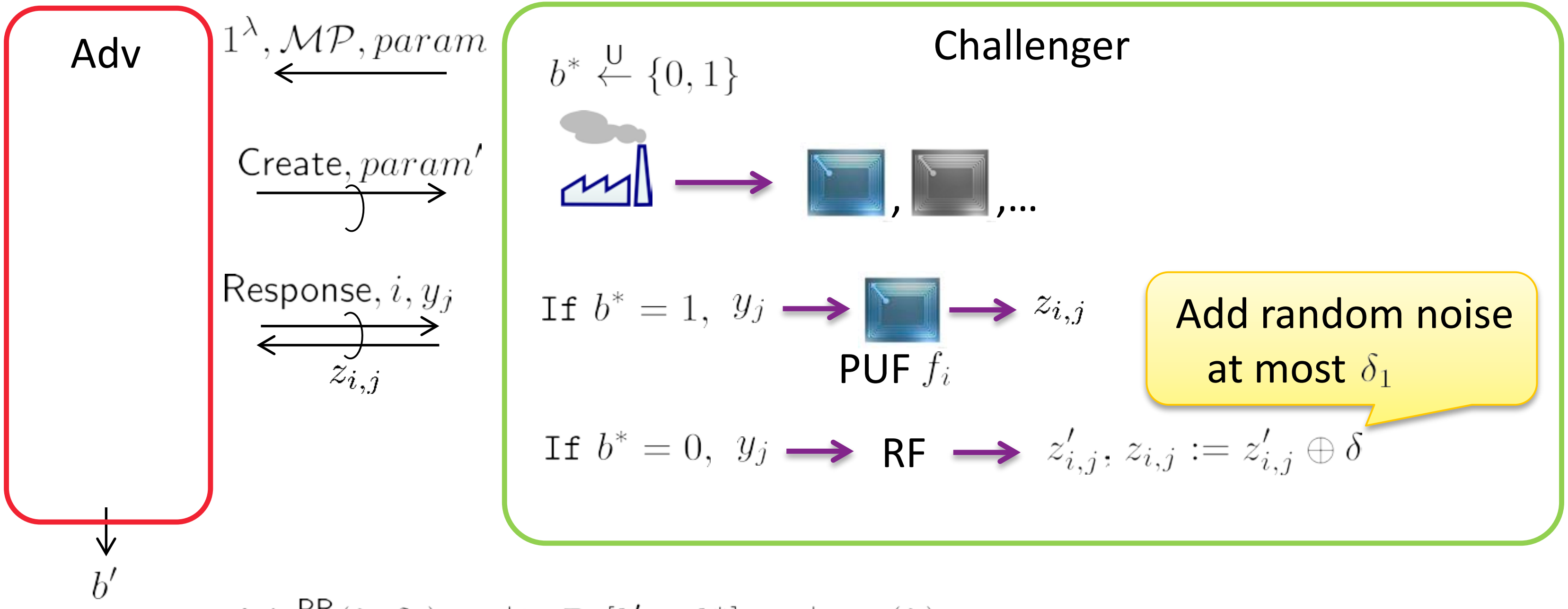
$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \epsilon)$-indistinguishablility if



$$\mathrm{Adv}_{\mathcal{A}}^{\text{IND-CMA}}(\lambda) := |2 \cdot \Pr[b' = b^*] - 1| \leq \epsilon(\lambda)$$

Security model: Pseudorandomness

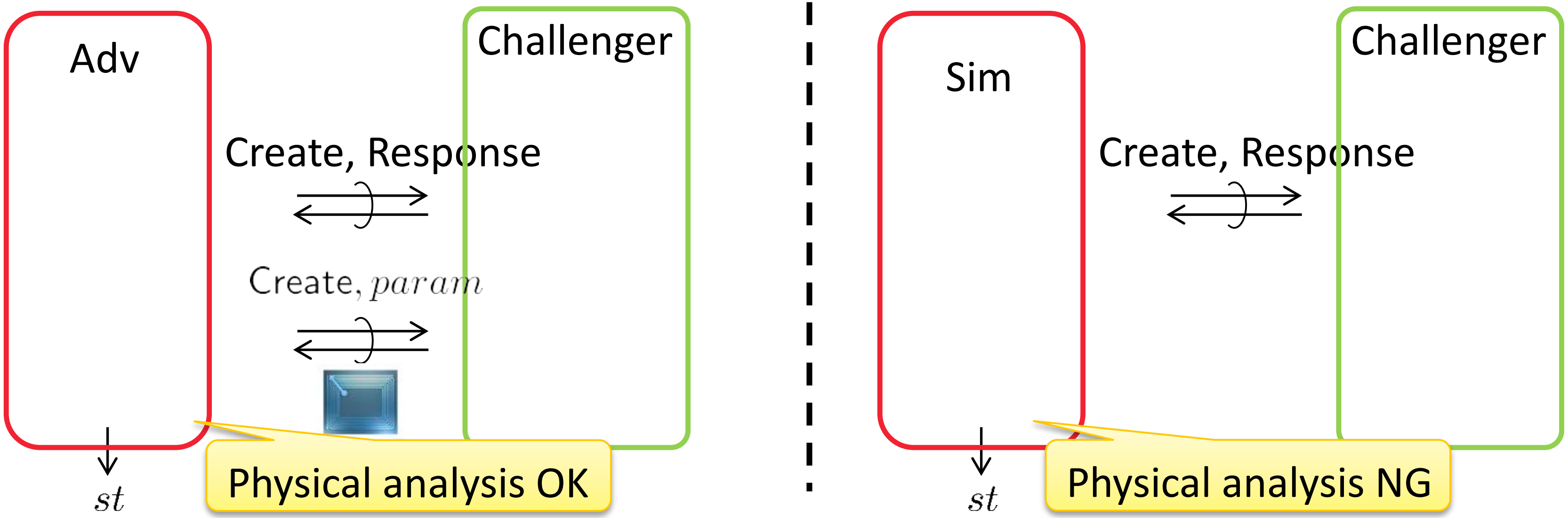
$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \epsilon)$-pseudorandomness if



$$\mathrm{Adv}^{\mathrm{PR}}_{\mathcal{A}}(\lambda, \delta_1) := |2 \cdot \Pr[b' = b^*] - 1| \le \epsilon(\lambda)$$

Security model: Tamper resilience

$f : \mathcal{D} \to \mathcal{R}$ has $(\mathcal{MP}, n, \ell, \epsilon)$-tamper resilience if



$$\mathsf{Adv}^{\mathsf{Tamp}}_{\mathcal{A},\mathcal{S},\mathcal{B}}(\lambda) := \left| \begin{array}{l} \Pr[\mathcal{B}(1^\lambda, st) \to 1 \mid st \xleftarrow{\mathsf{R}} \mathcal{A}^{\mathcal{O}}(1^\lambda, \mathcal{MP}, param, f_1, f_2, \ldots)] \\ - \Pr[\mathcal{B}(1^\lambda, st) \to 1 \mid st \xleftarrow{\mathsf{R}} \mathcal{S}^{\mathcal{O}}(1^\lambda, \mathcal{MP}, param)] \end{array} \right| \leq \epsilon(\lambda)$$

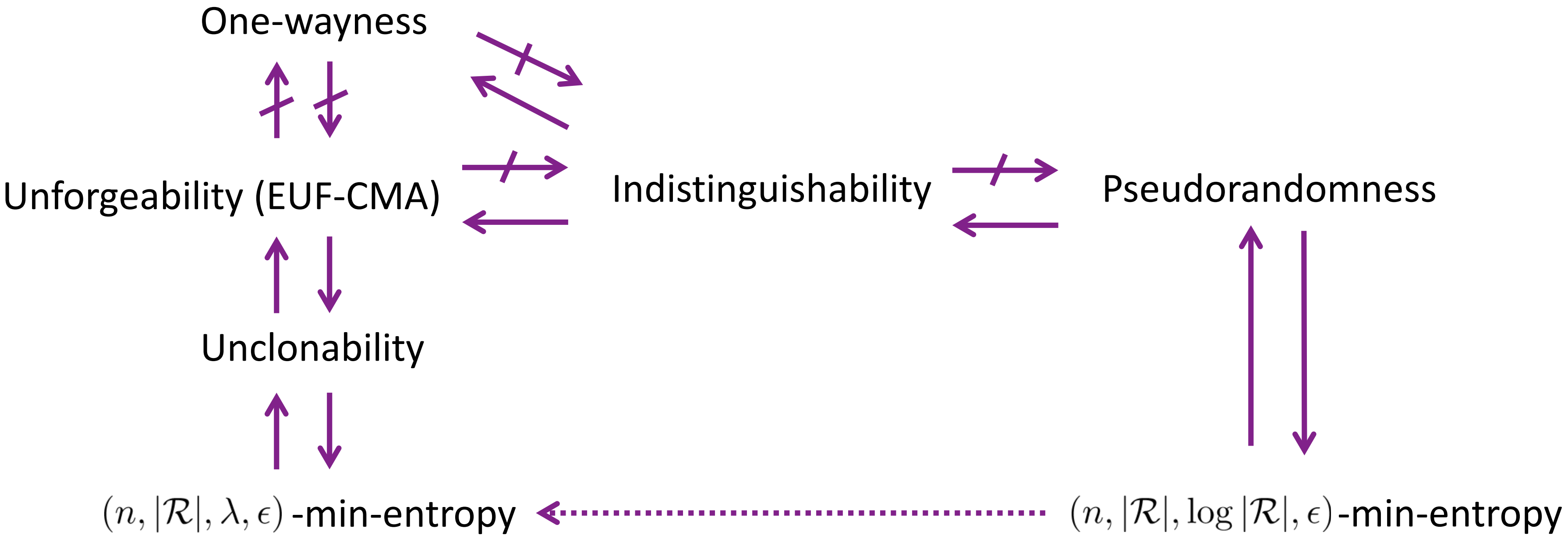
Comparison with Existing Works: Evaluation

	Intra-distance	Inter-distance I	Inter-distance II	Min-entropy	Number of PUFs	Number of Queries
Pappu	Yes	-	-	-	1	1
Gassend et al. (ACMCCS02)	Yes	Yes	-	-	1	poly
Guajardo et al. (CHES07)	Yes	-	-	-	1	1
Armknecht et al. (ASIACRYPT09)	Yes	-	-	Yes	1	poly
Armknecht et al. (IEEE S&P11)	Yes	-	-	Yes	poly	poly
Brzuska et al. (CRYPTO11)	Yes	-	-	Yes	1	poly
Maes	Yes	-	Yes	-	1	poly
Ours	Yes	Yes	Yes	Yes	poly	Yes

Comparison with Existing Works: Property

	Min-entropy	One-wayness	Unforgeability	Unclonability	Indistinguishability	Pseudo-randomness	Tamper Evidence
Pappu	-	Yes	UUF-KOA	-	-	-	-
Gassend et al. (ACMCCS02)	-	-	UUF-KMA	-	-	-	-
Guajardo et al. (CHES07)	-	-	UUF-OT-KMA EUF-KOA	-	-	-	-
Armknecht et al. (ASIACRYPT09)	Yes	-	-	Yes	-	-	-
Armknecht et al. (IEEE S&P11)	Yes	-	UUF-KMA, EUF-CMA	Yes	-	-	-
Brzuska et al. (CRYPTO11)	Yes	Yes	EUF-CMA	Yes	-	-	-
Maes		Yes	EUF-CMA	Yes	-	-	-
Ours	Yes	Yes	EUF-CMA	Yes	Yes	Yes	Yes

Relationship among Security Notions



See full version for formal proofs

Conclusion

- We provided a new security model for PUFs
  - Various security definitions (from crypto primitives) motivated by crypto primitives
  - Cover noise effect for formal definitions (caused from real PUFs!)
    - If ignored, adversarial advantage cannot be properly evaluated
  - Provide implication and separations

What Researchers Should DO NEXT

- Consider security proof for PUF-based protocols based on security model for PUFs (theory)
  - Whenever you propose a new protocol, think about requirements for PUFs toward provable security
- Consider evaluation s.t. which PUF satisfies which security property (implementation)
  - Whenever you propose a new PUF, think about the security properties your PUF can provide

Thank you for your attention !