Provable Security of the Sponge:
From Indifferentiability to Full-State Absorption

Damian Vizár (CSEM, Switzerland)

Advances in permutation-based cryptography 2018, Milan

This talk

- Introduction: provable security
- The evolution of bounds and full-state absorption

Why provable security

Context: symmetric crypto

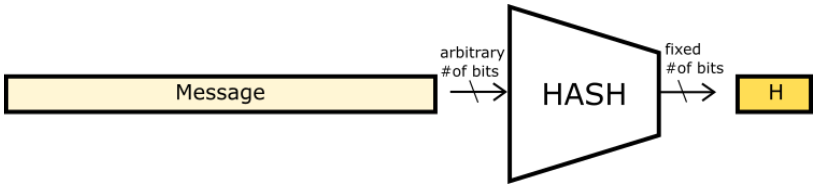
What we want:

Practical tools for all inputs

Why provable security

Context: symmetric crypto

What we want:

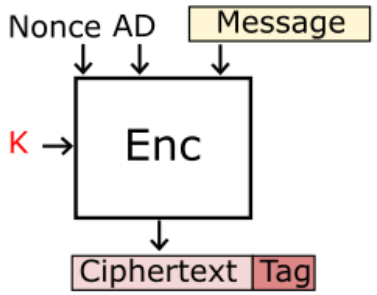


Practical tools for all inputs

Why provable security

Context: symmetric crypto

What we want:

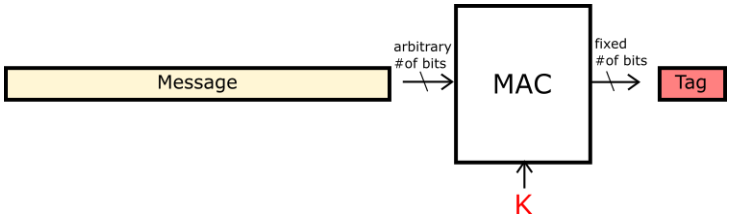


Practical tools for all inputs

Why provable security

Context: symmetric crypto

What we want:



Practical tools for all inputs

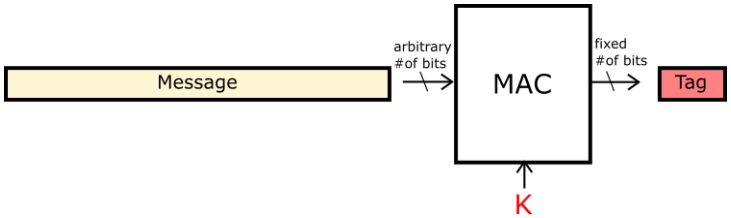
What we know how to do (well):

Not directly applicable

Why provable security

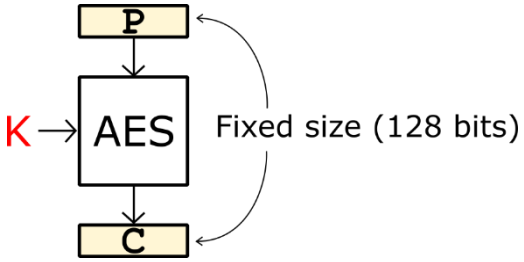
Context: symmetric crypto

What we want:



Practical tools for all inputs

What we know how to do (well):

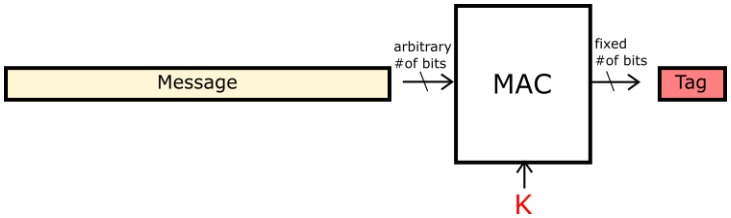


Not directly applicable

Why provable security

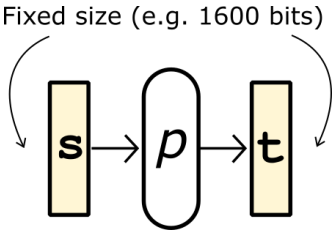
Context: symmetric crypto

What we want:



Practical tools for all inputs

What we know how to do (well):



Not directly applicable

What we (usually) do:

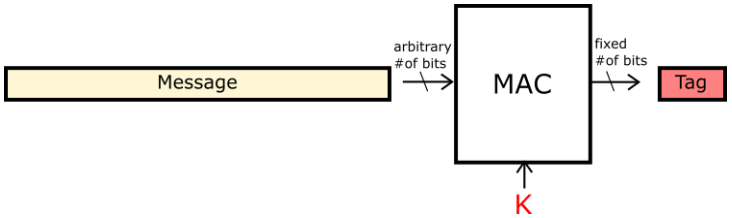
A mode of operation:

- Use primitive as blackbox

Why provable security

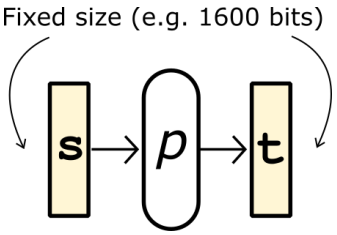
Context: symmetric crypto

What we want:



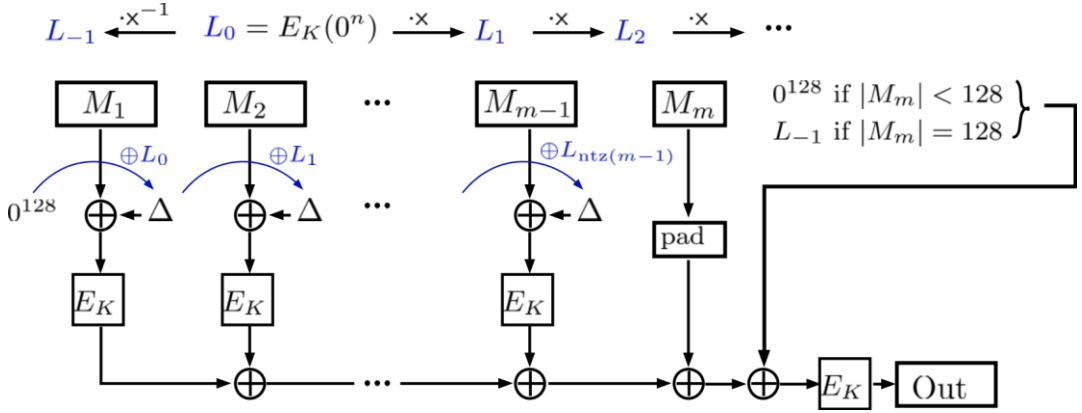
Practical tools for all inputs

What we know how to do (well):



Not directly applicable

What we (usually) do:



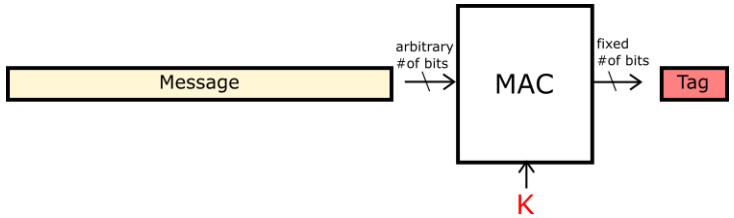
A mode of operation:

- Use primitive as blackbox

Why provable security

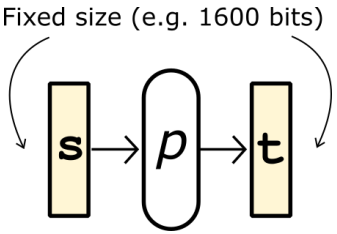
Context: symmetric crypto

What we want:



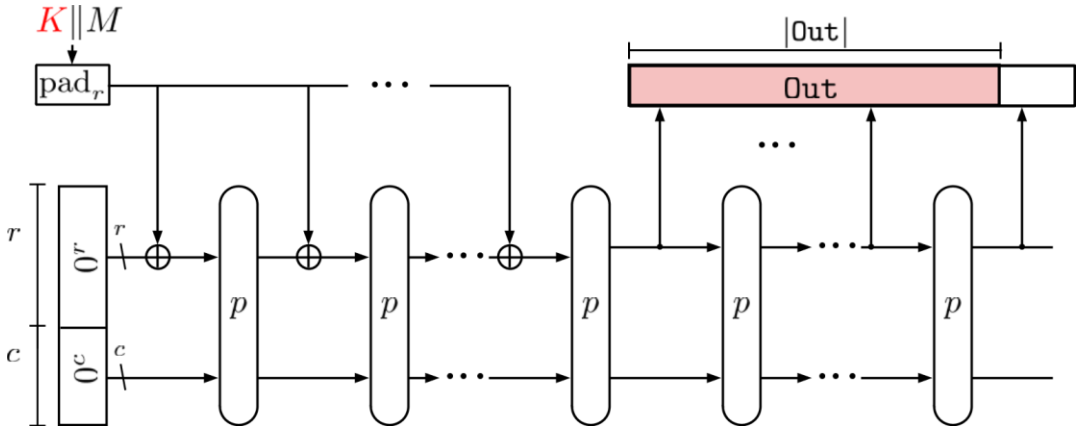
Practical tools for all inputs

What we know how to do (well):



Not directly applicable

What we (usually) do:



A mode of operation:

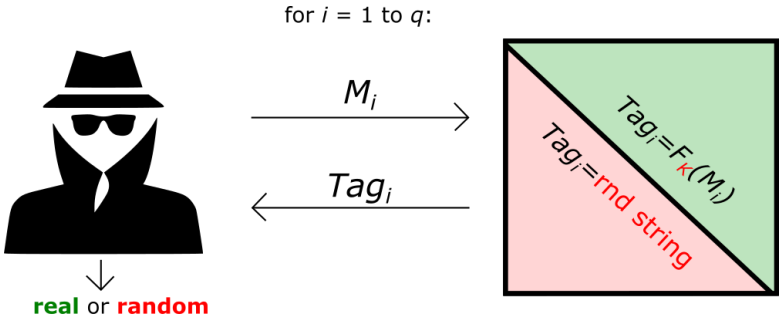
- Use primitive as blackbox

Provable security

Security-bridge between the primitives and the modes

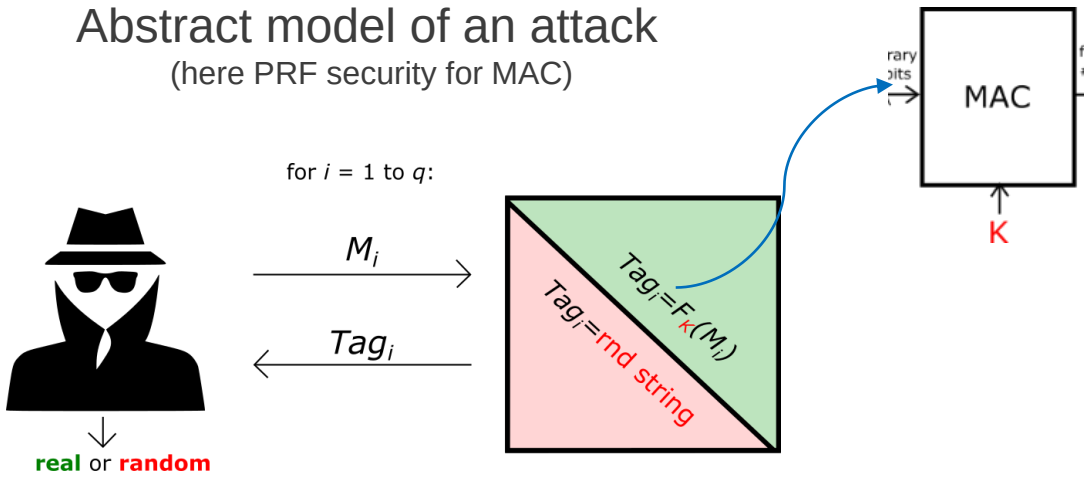
Abstract model of an attack
(here PRF security for MAC)

Messy reality



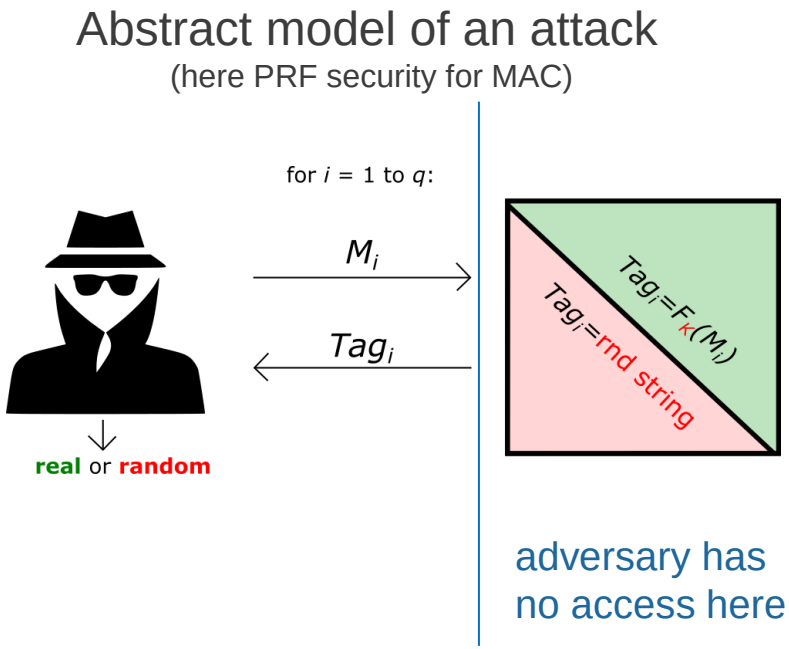
Provable security

Security-bridge between the primitives and the modes



Provable security

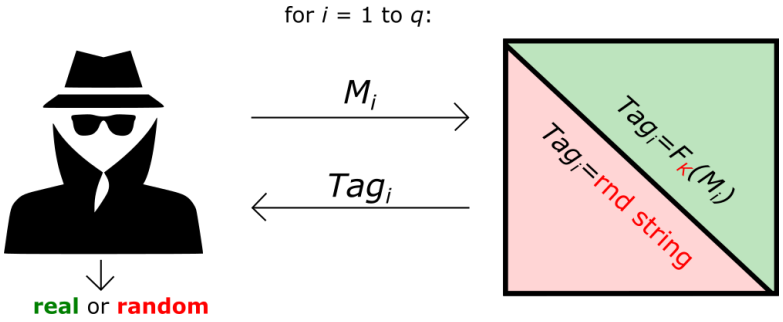
Security-bridge between the primitives and the modes



Provable security

Security-bridge between the primitives and the modes

Abstract model of an attack
(here PRF security for MAC)



Prove that

$$\Pr[\textbf{mode breaks}|\textbf{res.}] \leq \Pr[\textbf{primitive breaks}|\textbf{res.}] + f(\textbf{res.})$$

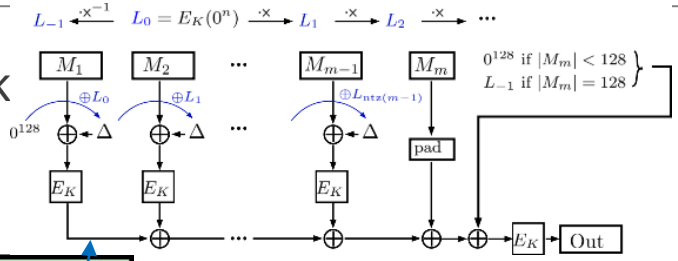
"Advantage"

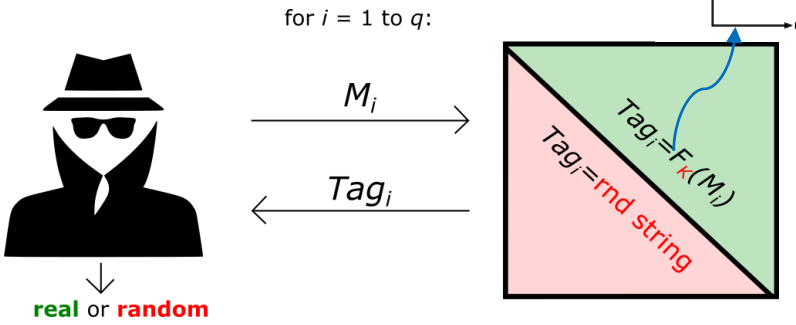
Provable security

Security-bridge between the primitives and the modes

Abstract model of an attack

(here PRF security for MAC)





Prove that

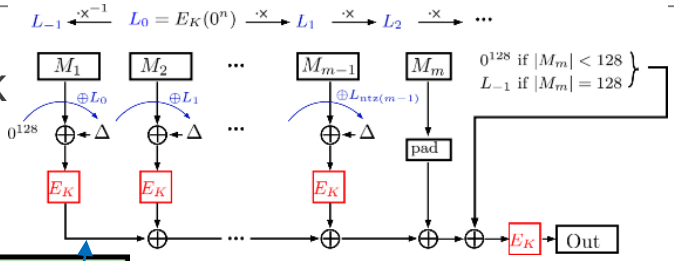
$$\Pr[\textbf{mode breaks}|\textbf{res.}] \leq \Pr[\textbf{primitive breaks}|\textbf{res.}] + f(\textbf{res.})$$

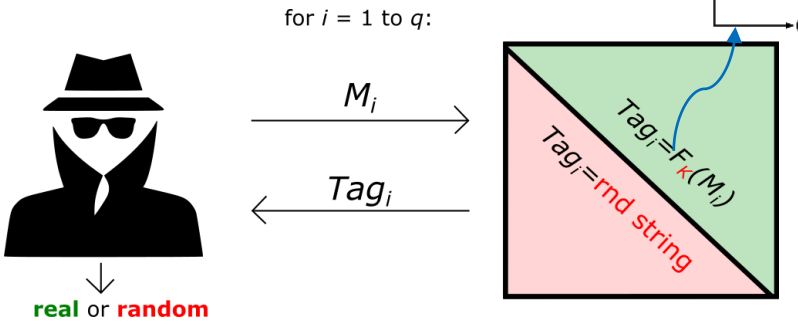
"Advantage"

Provable security

Security-bridge between the primitives and the modes

Abstract model of an attack
(here PRF security for MAC)





Prove that

$$\Pr[\text{mode breaks}|\text{res.}] \leq \Pr[\text{primitive breaks}|\text{res.}] + f(\text{res.})$$

"Advantage"

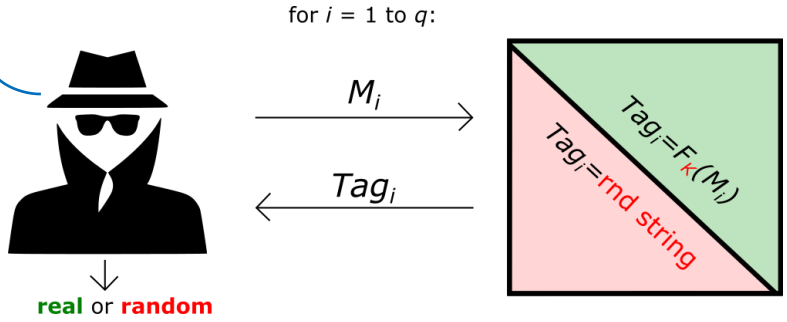
Provable security

Security-bridge between the primitives and the modes

Resources:

- max comp. power
- max #of queries (q)
- max #of total msg bits
- etc.

Abstract model of an attack
(here PRF security for MAC)



Prove that

$$\Pr[\textbf{mode breaks}|\textbf{res.}] \leq \Pr[\textbf{primitive breaks}|\textbf{res.}] + f(\textbf{res.})$$

"Advantage"

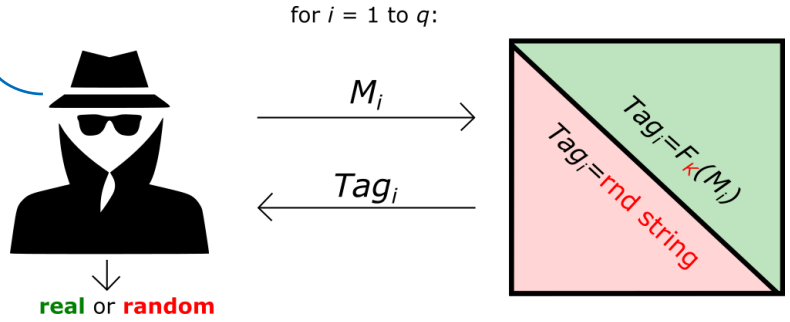
Provable security

Security-bridge between the primitives and the modes

Resources:

- max comp. power
- max #of queries (q)
- max #of total msg bits
- etc.

Abstract model of an attack
(here PRF security for MAC)



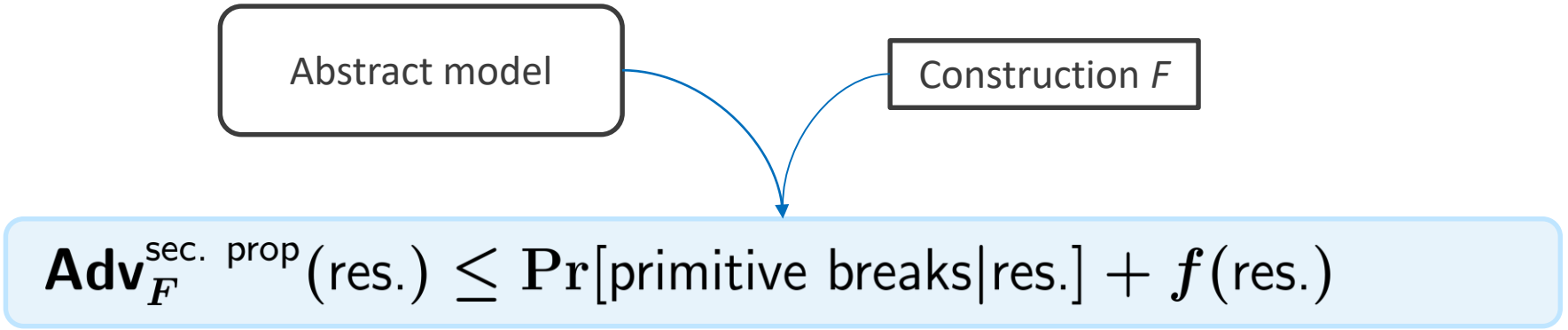
F secure if
$f(res) \sim 0$
for "reasonable" resources

Prove that

$$\Pr[\text{mode breaks}|\text{res.}] \leq \Pr[\text{primitive breaks}|\text{res.}] + f(\text{res.})$$

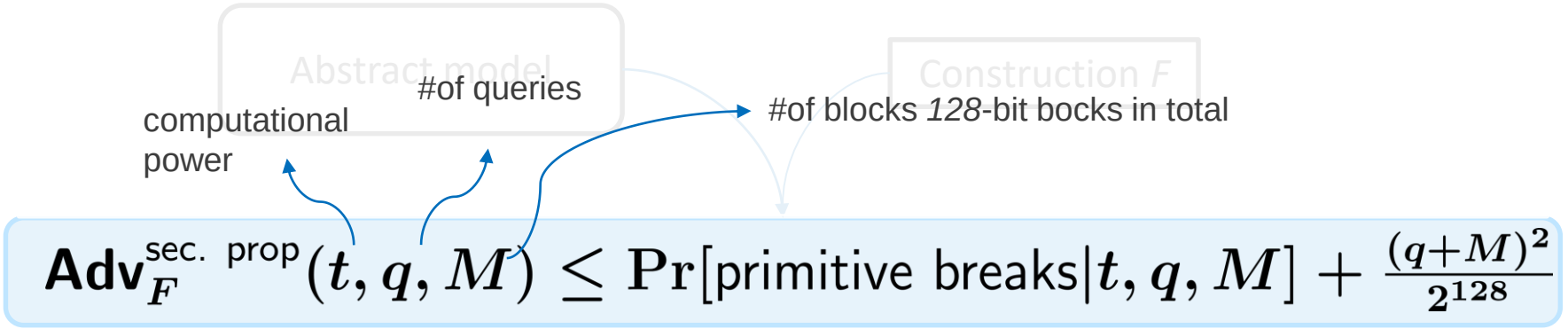
"Advantage"

Interpreting provable security



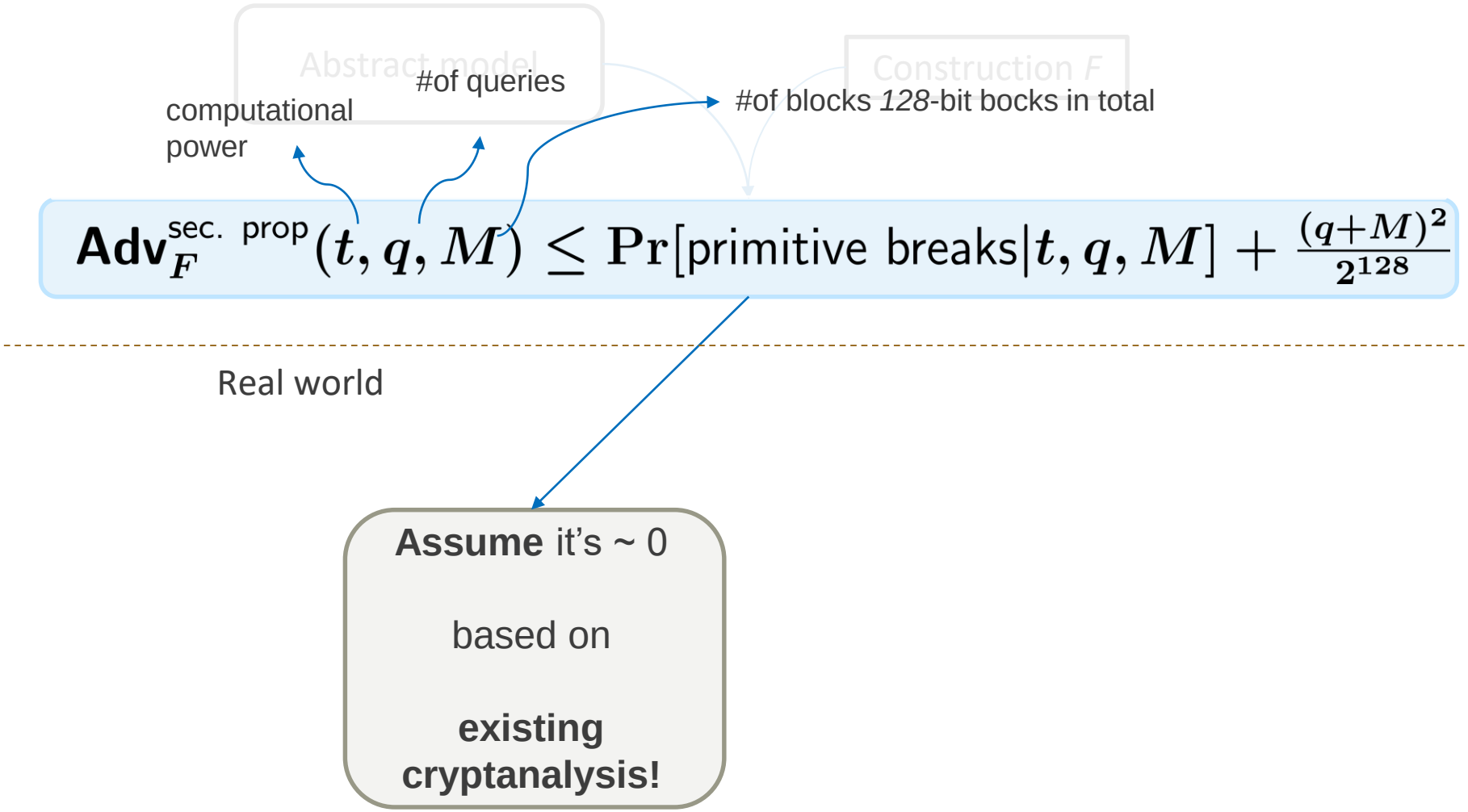
Real world

Interpreting provable security

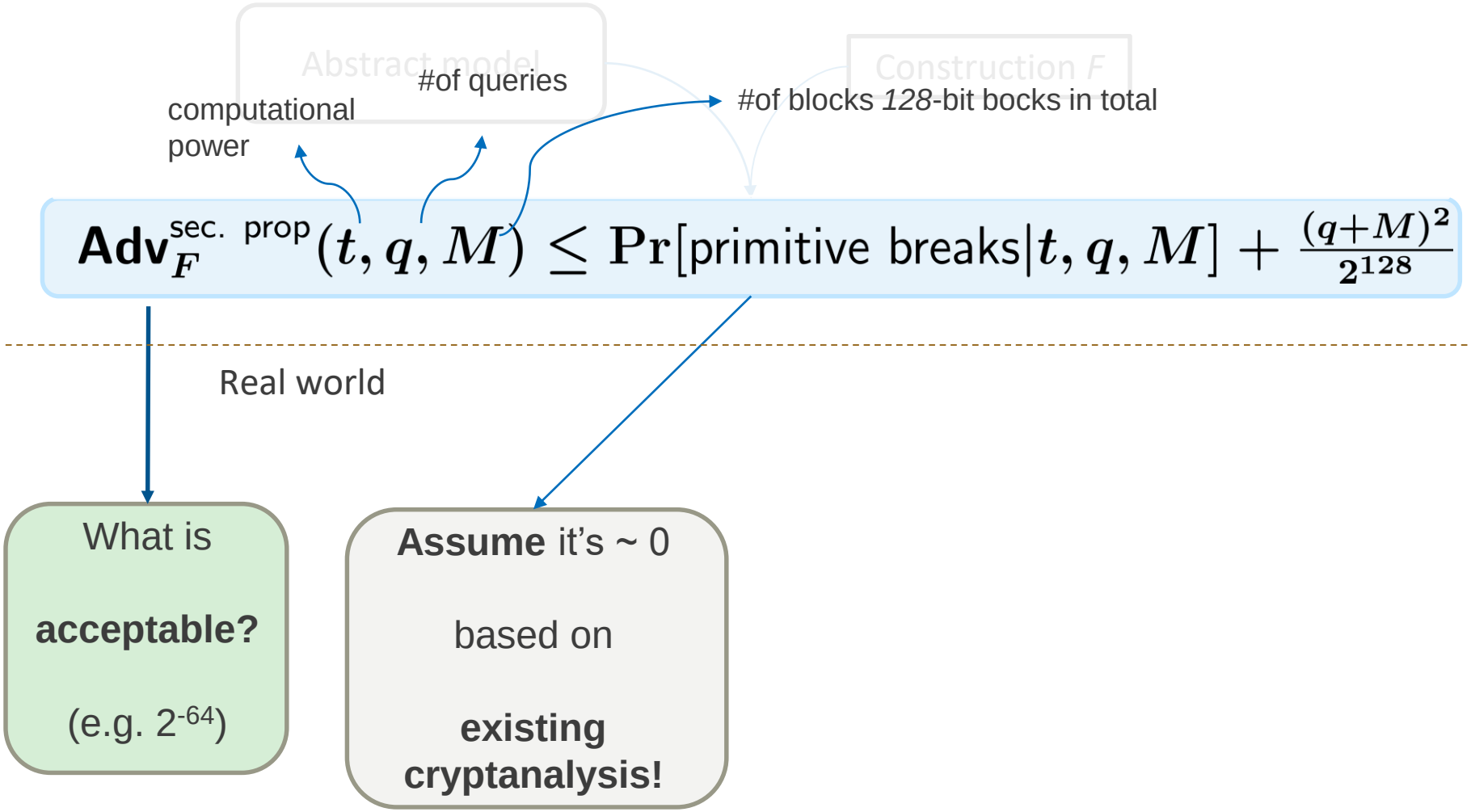


Real world

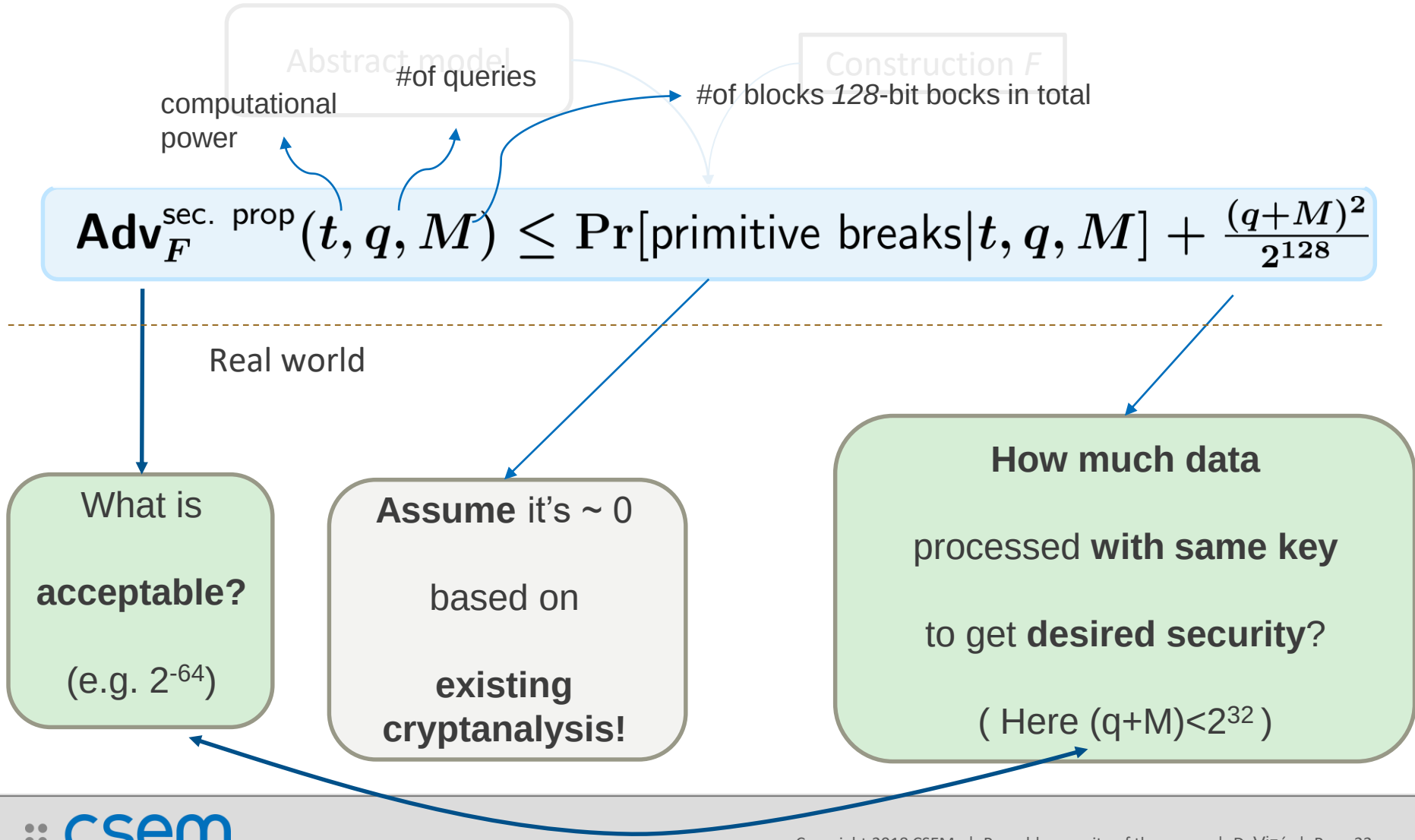
Interpreting provable security



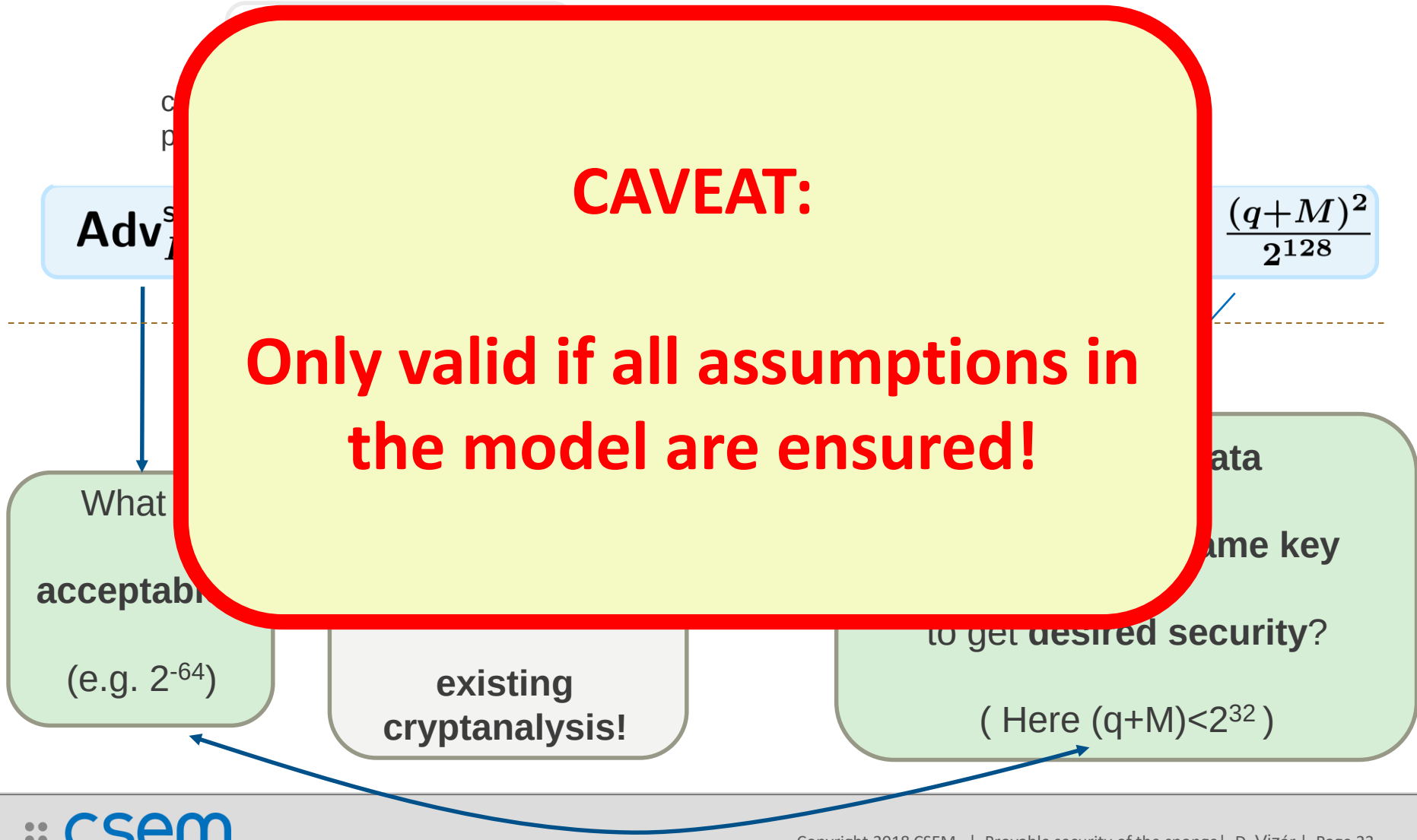
Interpreting provable security



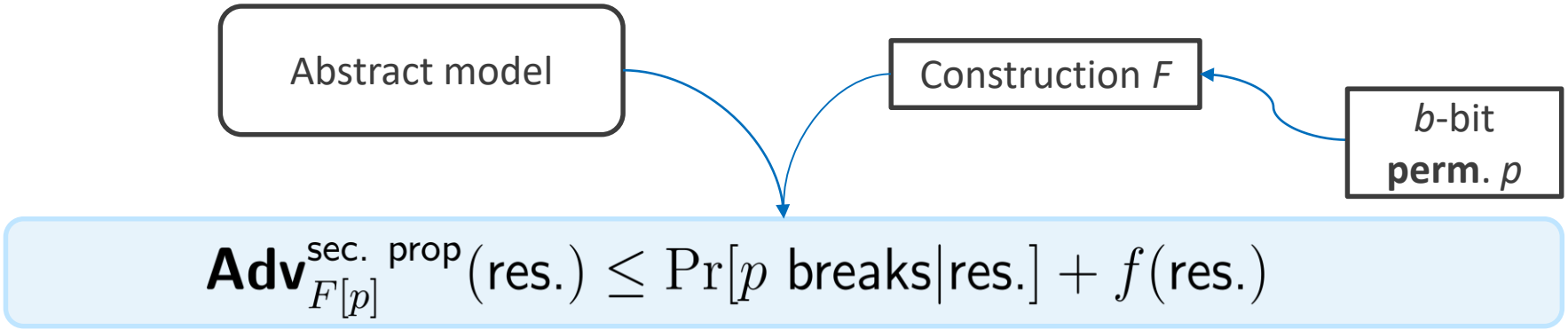
Interpreting provable security



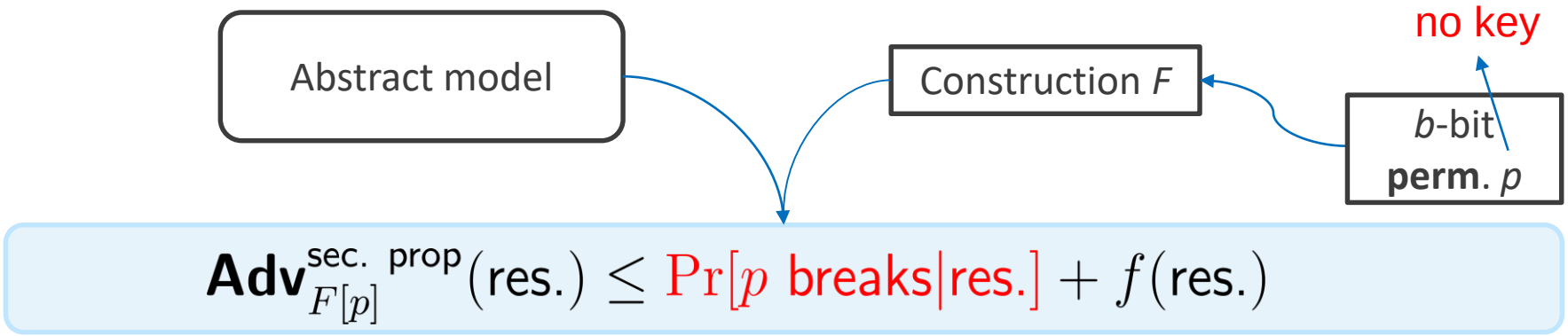
Interpreting provable security



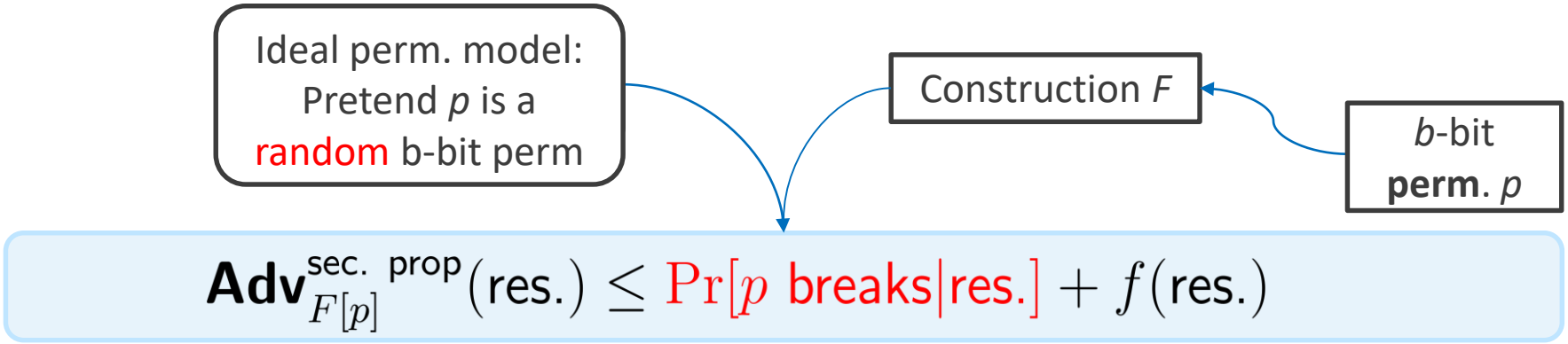
Ideal permutation model



Ideal permutation model

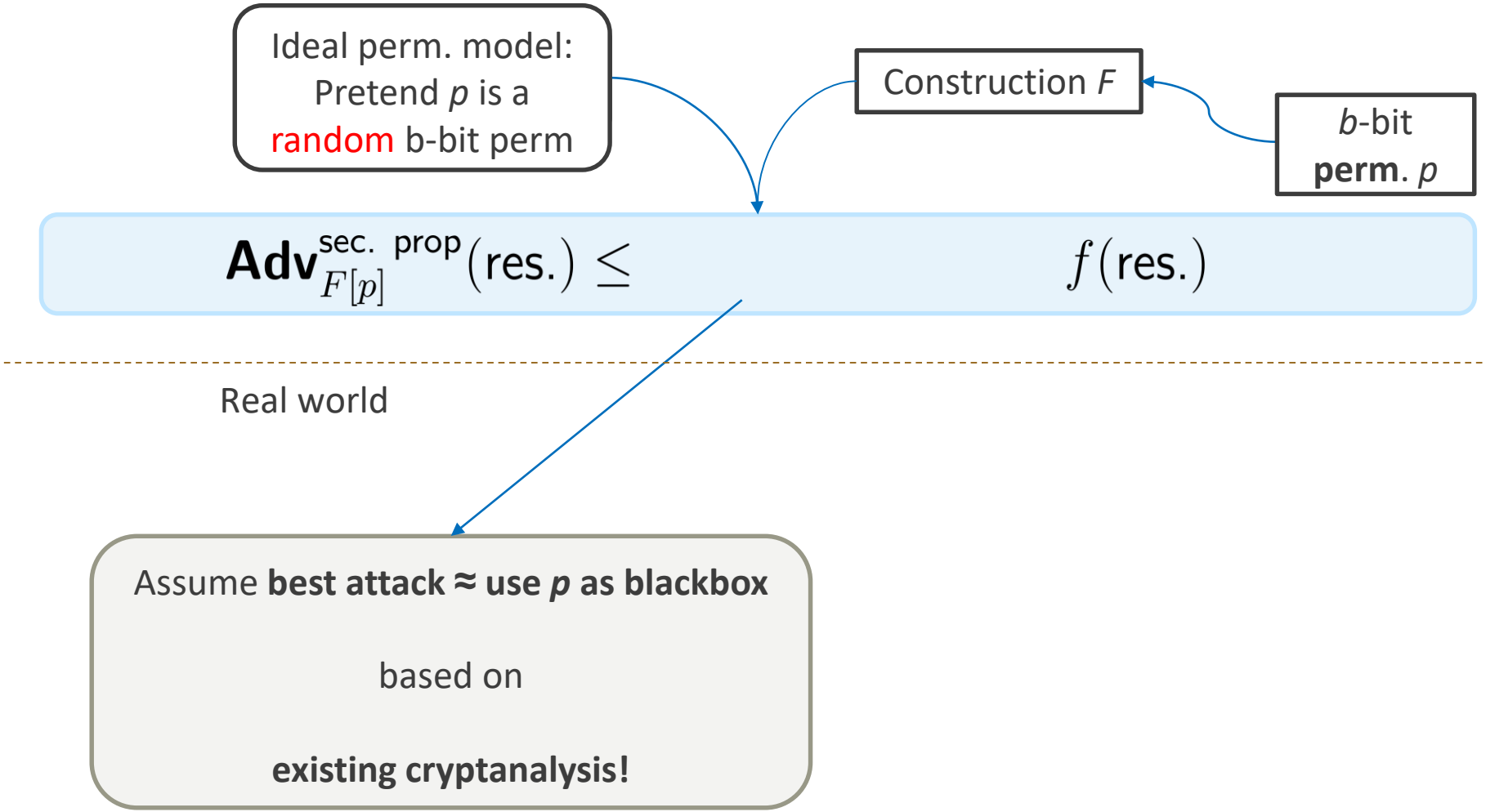


Ideal permutation model

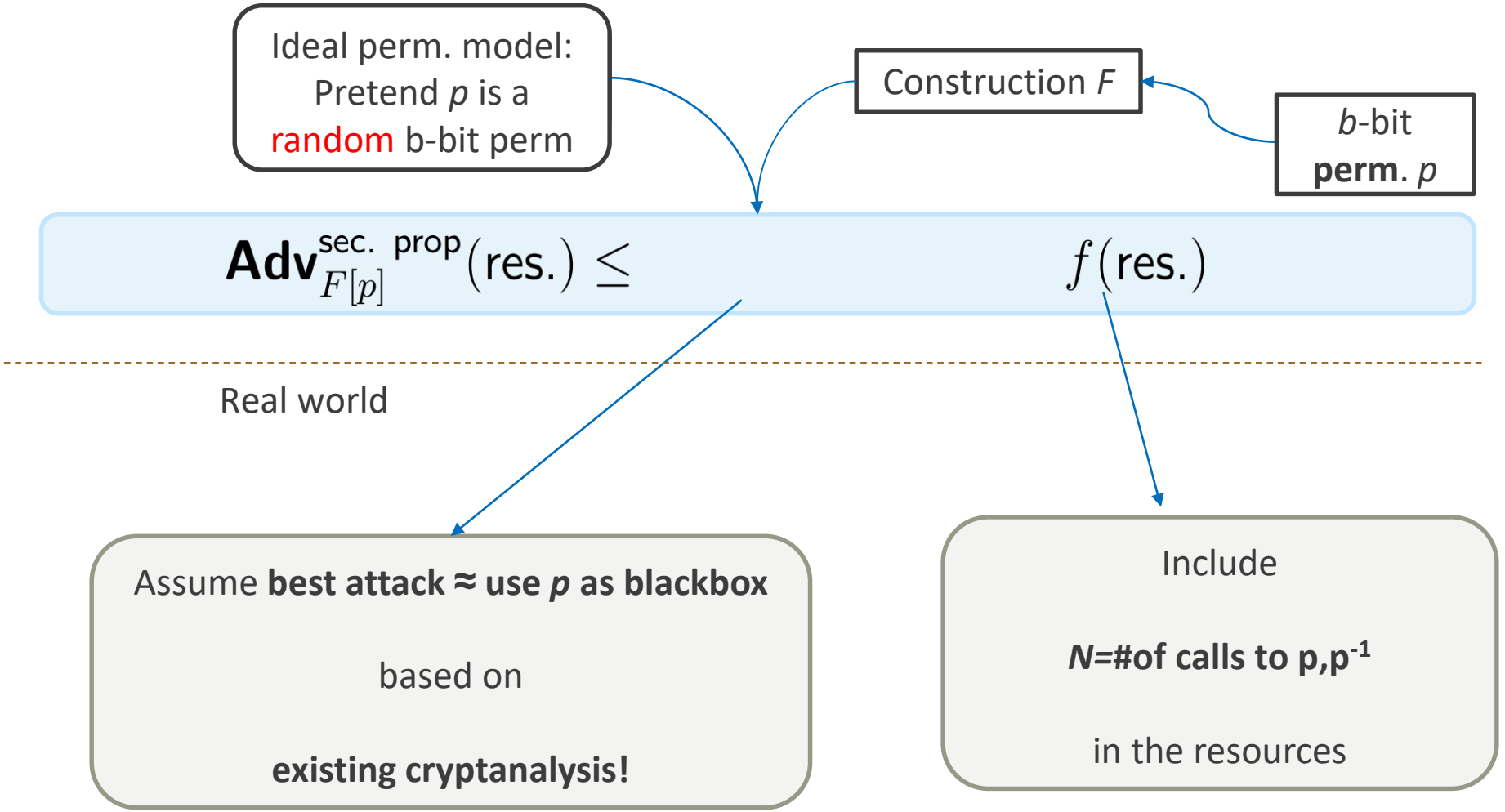


$$p \in_{\text{rnd}} \{\pi : \{0,1\}^b \to \{0,1\}^b | \pi \text{ is a permutation}\}$$

Ideal permutation model



Ideal permutation model



Evolution of bounds and full-state absorption

2008 Keyless sponge: indifferentiability [BDPV 08]

2011 Keyed sponge security [BDPV 11]

Duplex [BDPV 11]

2014 Improved bound: sponge AE [JLM 14]

2015 Keyed sponge revisited [ADMV 15]

Partially full-state sponge AE [SY 15]

(Limited) full-state keyed sponge [GPT 15]

Full-state keyed sponge [MRV 15]

2016 Keyed sponge revisited #2 [NY 16]

2017 Full-state keyed sponge revisited [DMV 17]

2018 Keyed sponge #4 [M 18]

Evolution of bounds and full-state absorption

2008 K

2011 K

Du

2014 In

2015 K

Pa

(L

Fu

2016 K

2017 Fu

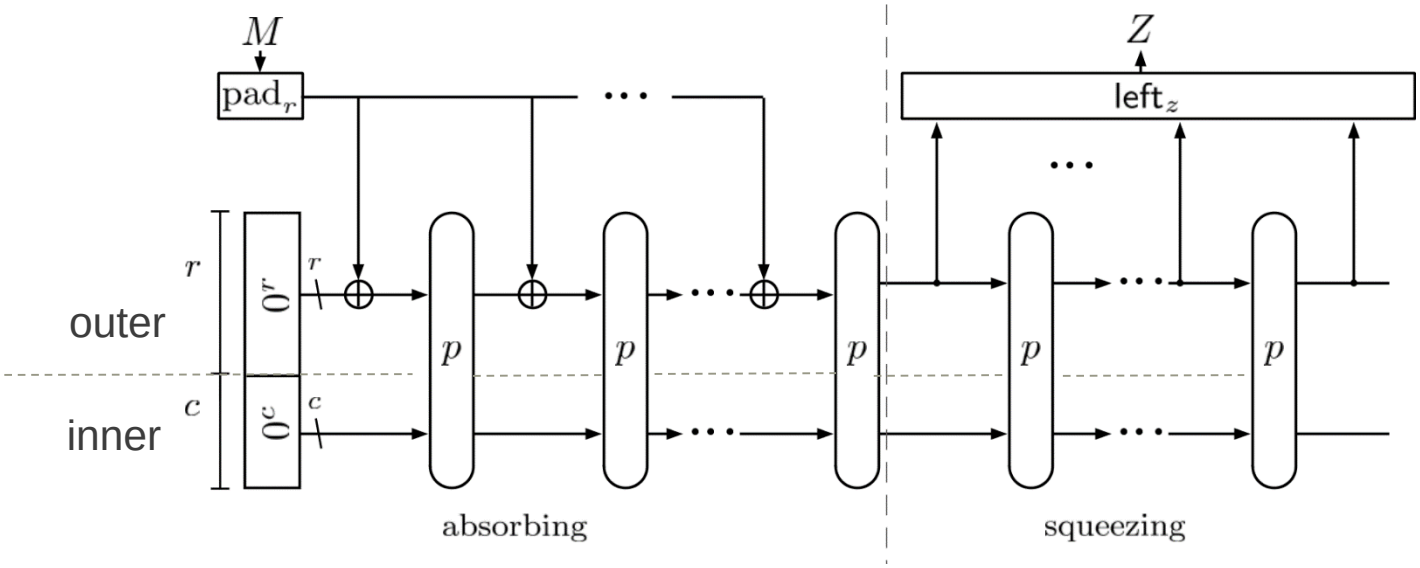
2018 K

Out of scope:

- **Other security models**
  - Weak perm. model [MP 15]
  - Public seed perm. [ST 17]
- **Multiuser security**
- **Sponge variants**
  - Sandwich sponge [N 16]
  - Prefix-free sponge [N 18]
- **Full proofs**

Sponge construction

Bertoni, Daemen, Peeters, Van Assche **2007**

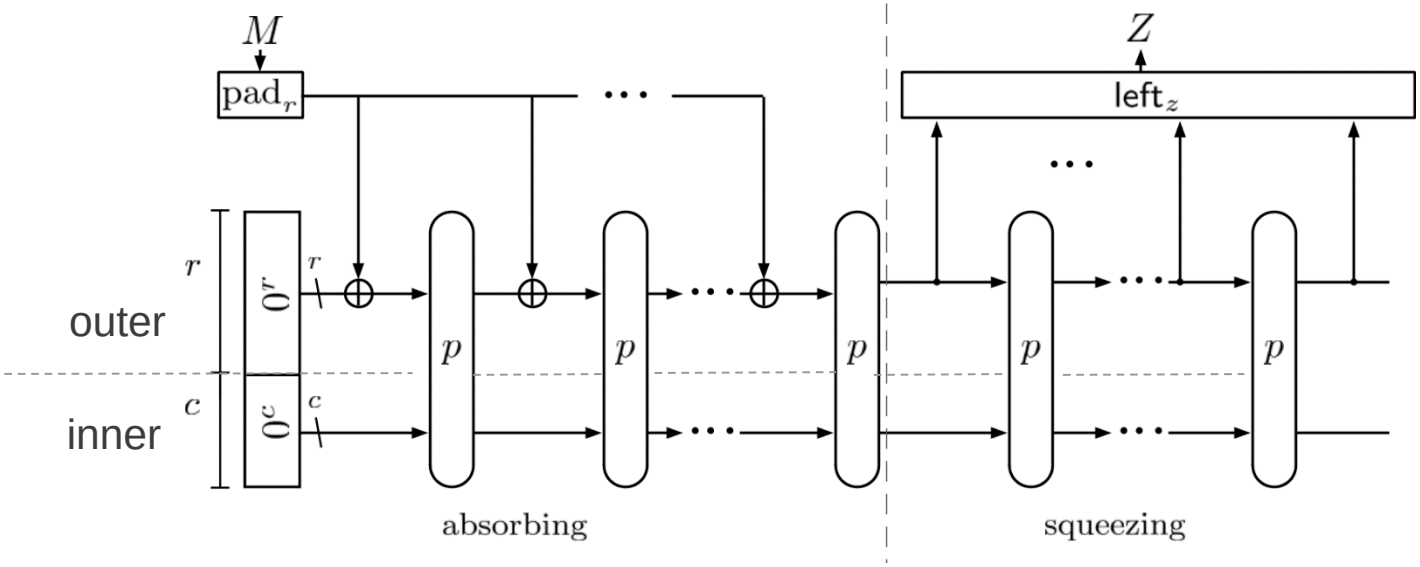


- Keyless crypto. permutation $p : \{0,1,\}^b \rightarrow \{0,1,\}^b$
- Crypto. hashing
  - What security to target?

Sponge construction

Bertoni, Daemen, Peeters, Van Assche **2007**

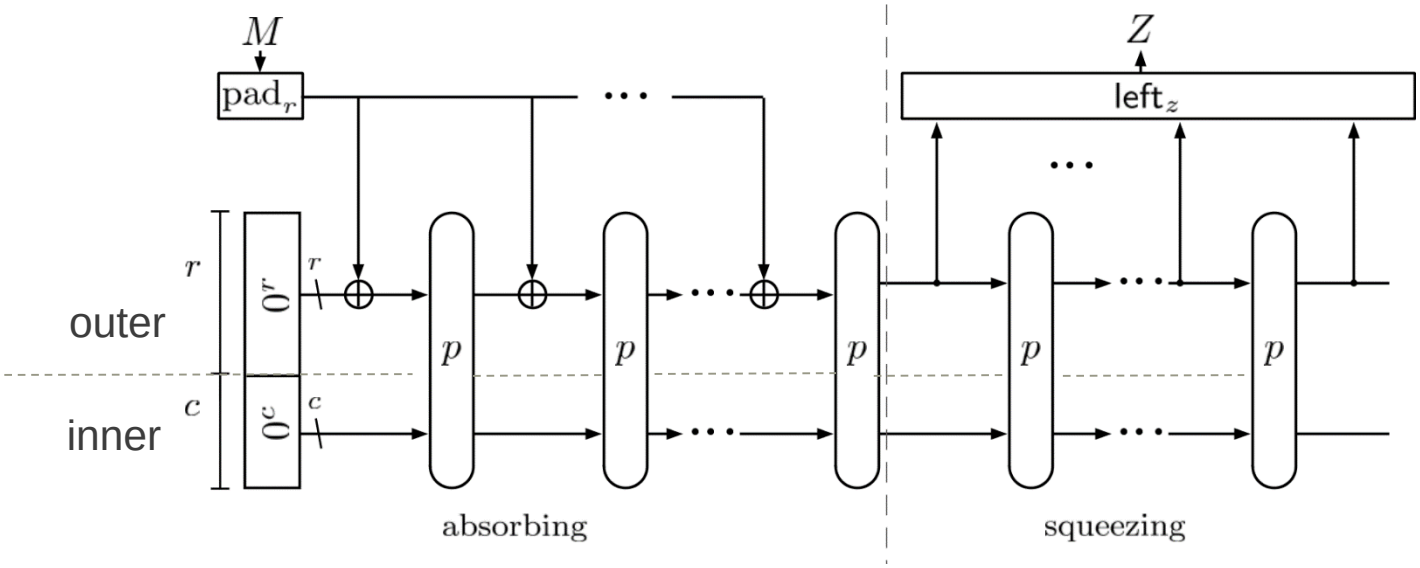
Z=Sponge(M,z): $\lceil |M|/r \rceil + \lfloor z/r \rfloor$ **calls to *p***



- Keyless crypto. permutation $p : \{0,1,\}^b \rightarrow \{0,1,\}^b$
- Crypto. hashing
  - What security to target?

Sponge construction

Bertoni, Daemen, Peeters, Van Assche **2007**

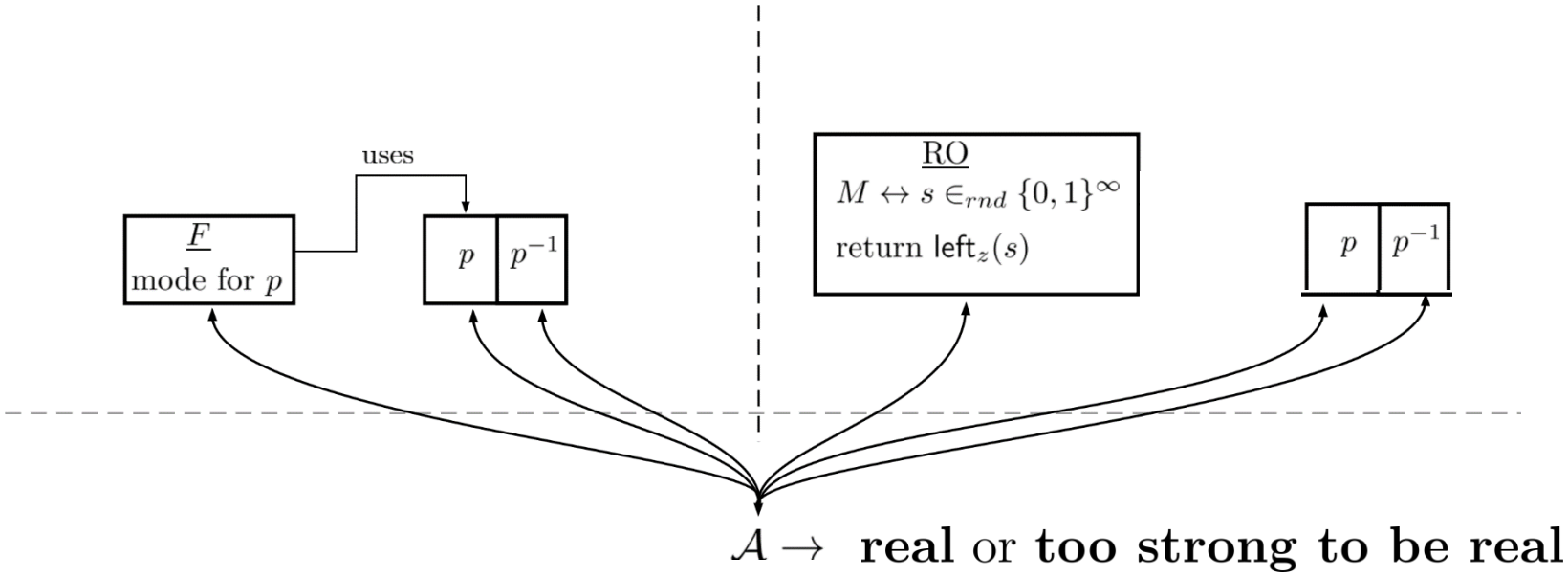


- Keyless crypto. permutation $p : \{0,1,\}^b \rightarrow \{0,1,\}^b$
- Crypto. hashing
  - What security to target?

For every *M*, output is “random”

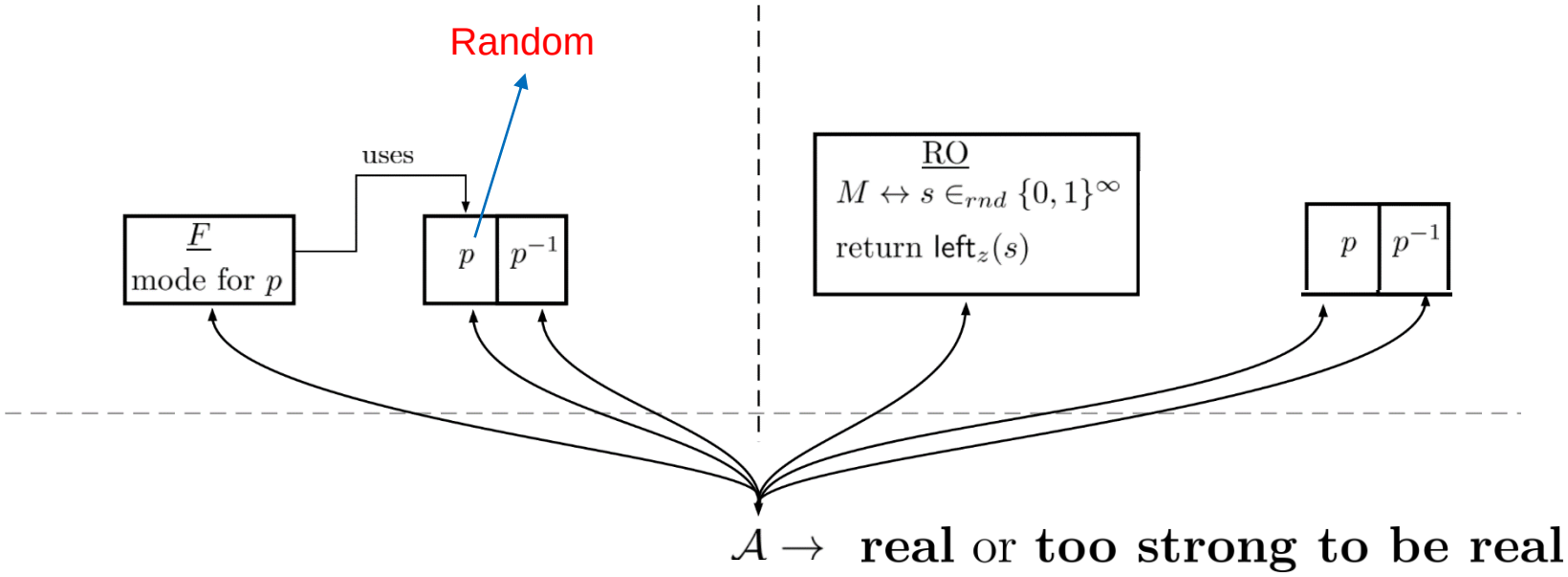
Indifferentiability

In ideal permutation model



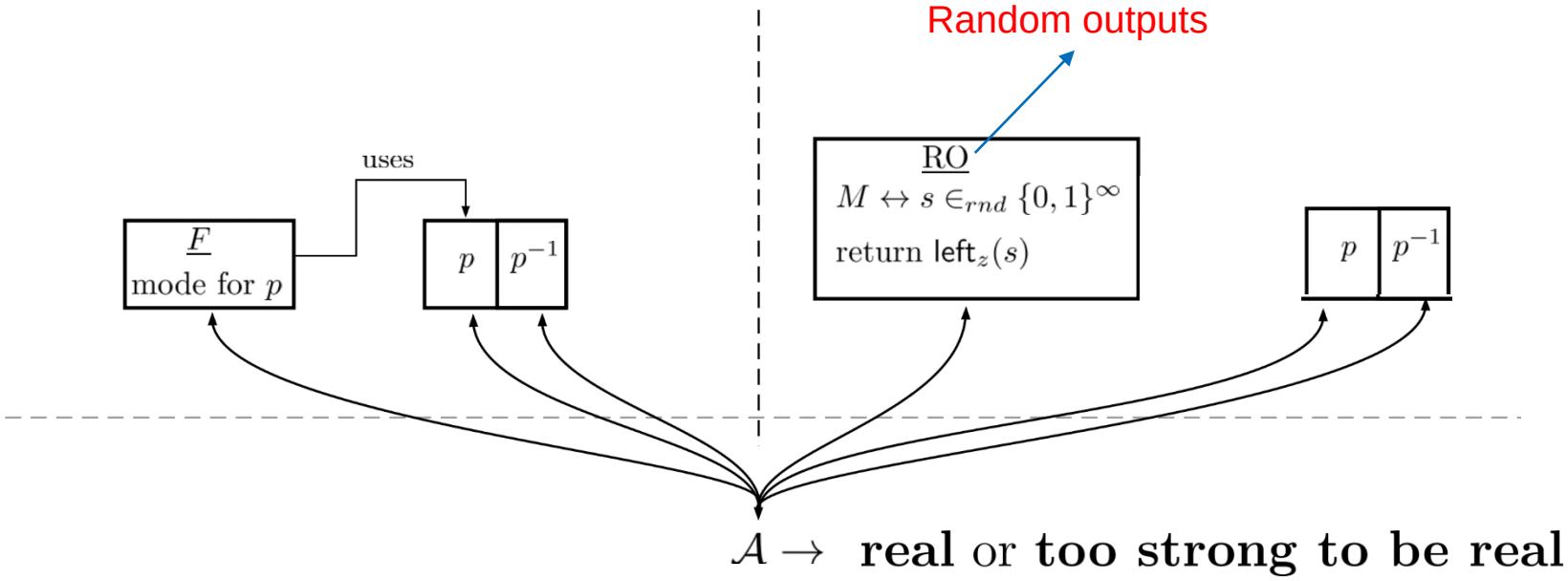
Indifferentiability

In ideal permutation model



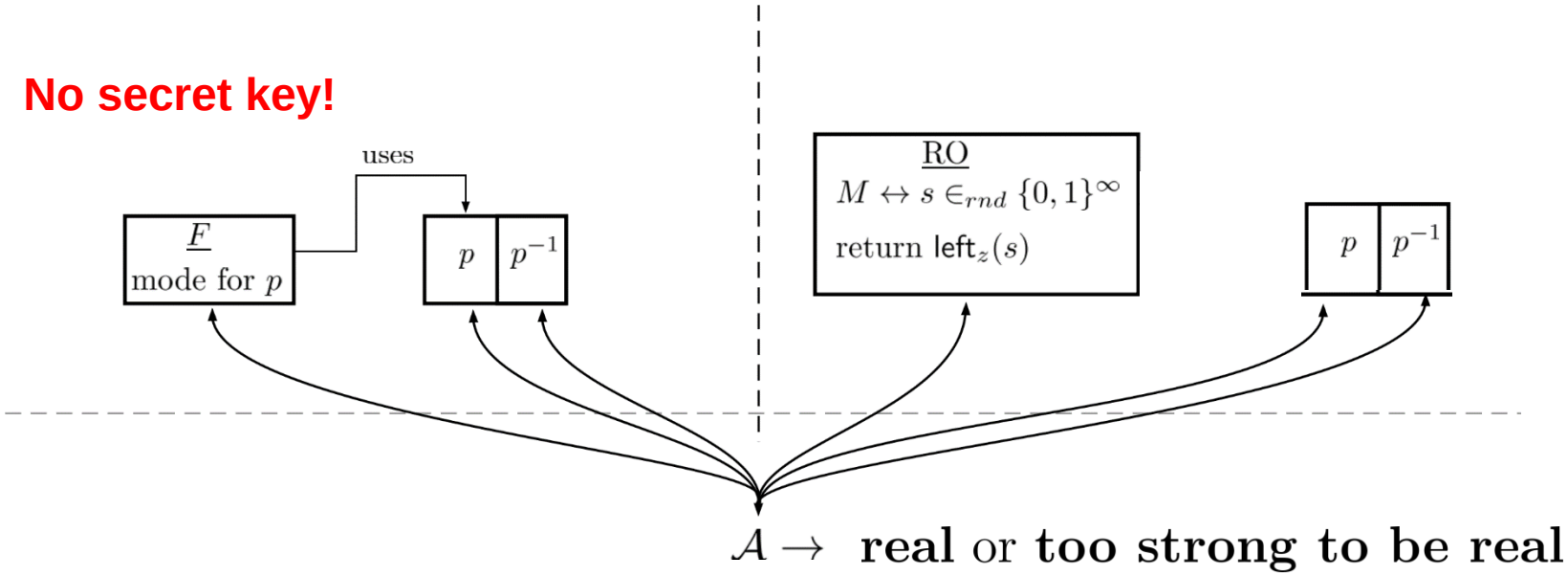
Indifferentiability

In ideal permutation model



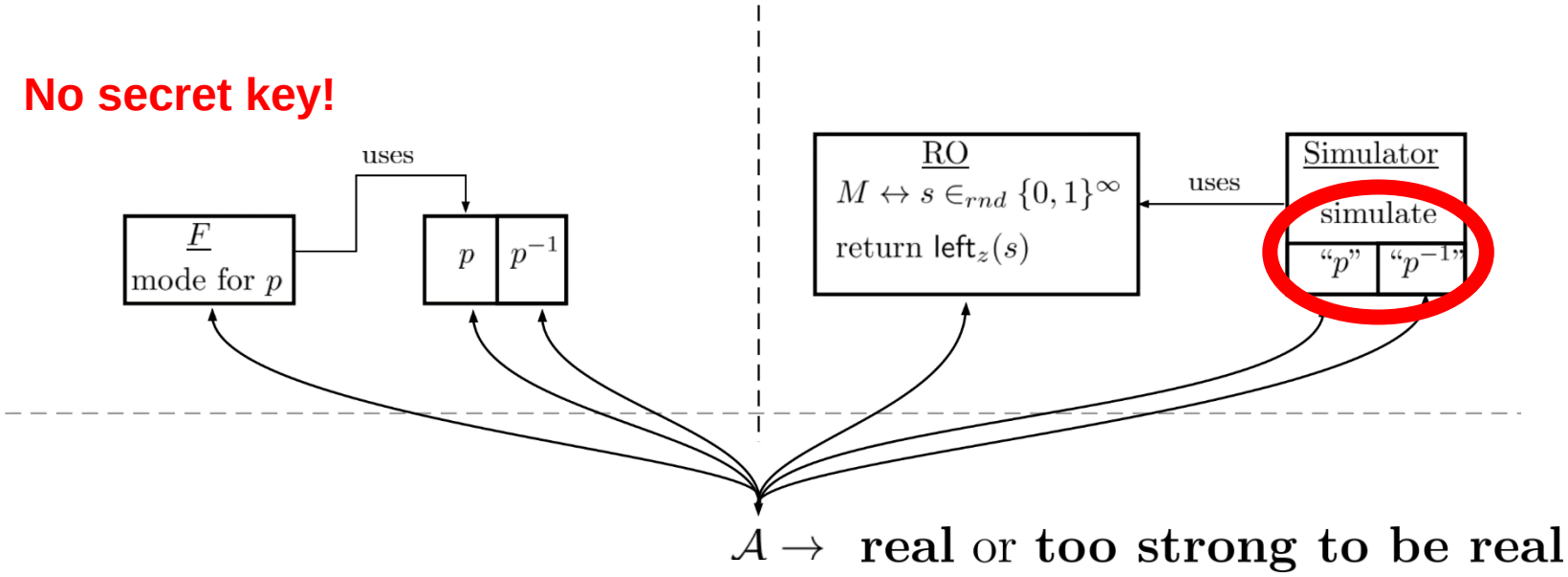
Indifferentiability

In ideal permutation model



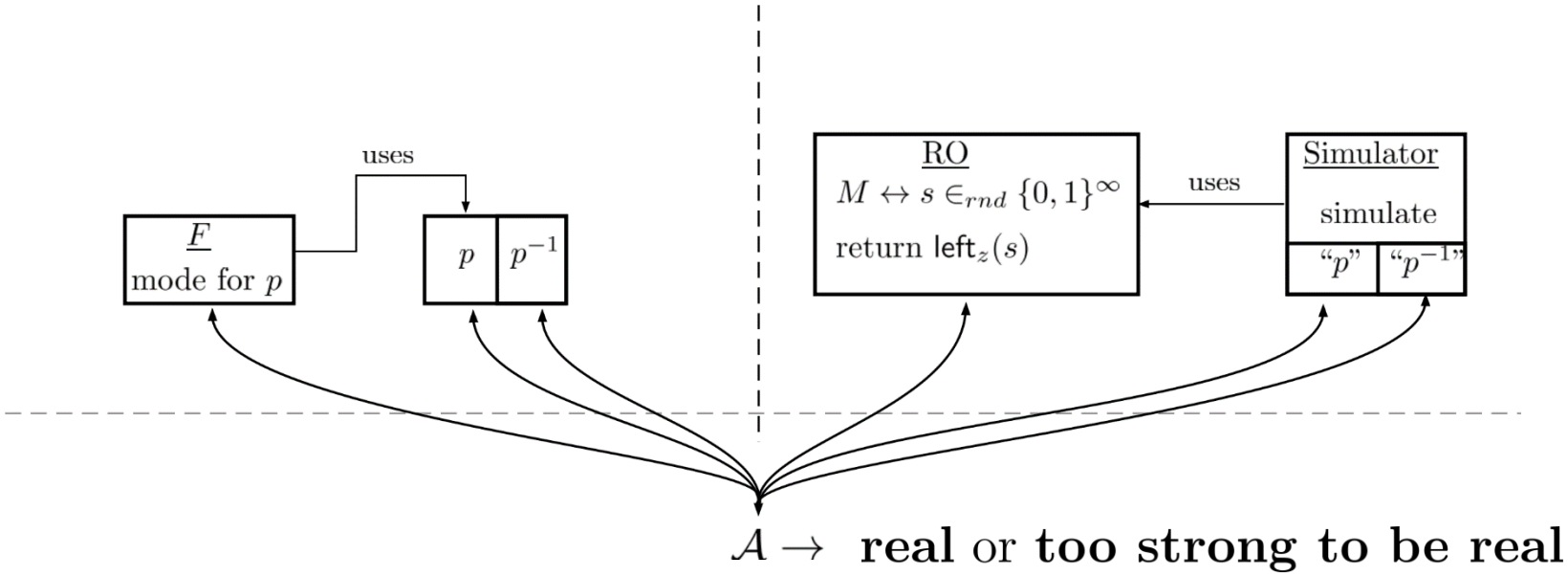
Indifferentiability

In ideal permutation model



Indifferentiability

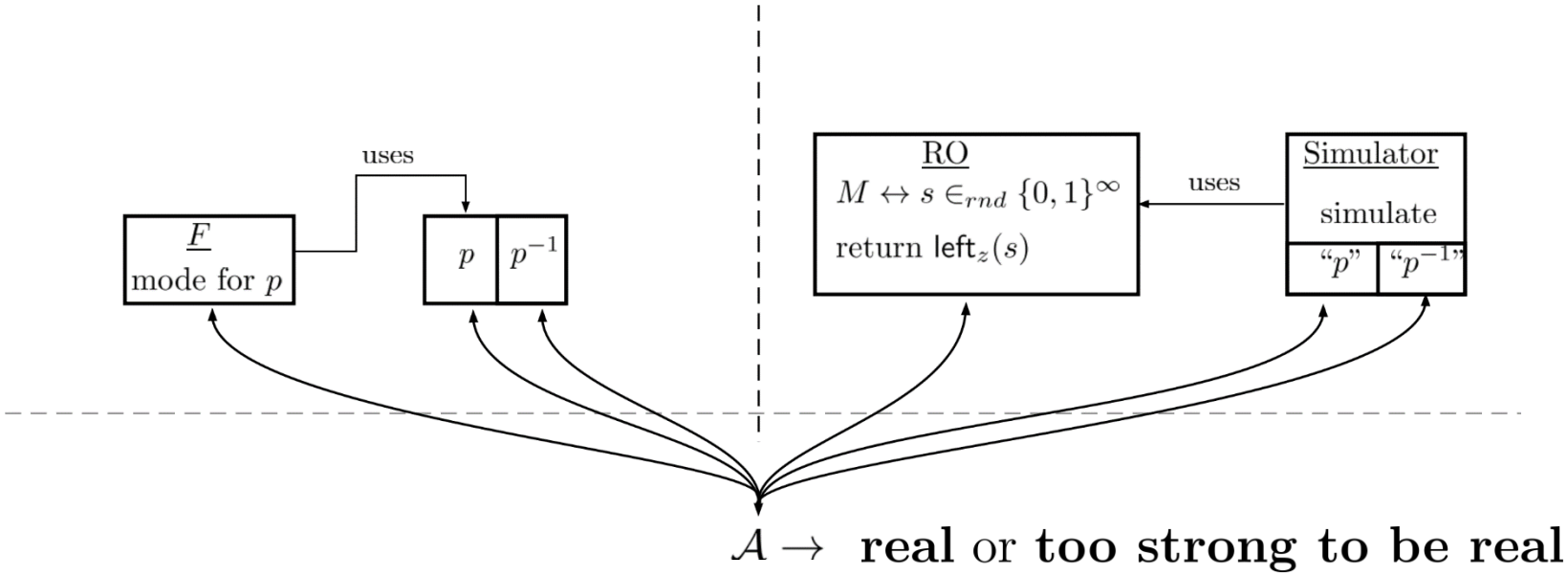
In ideal permutation model



$\mathbf{Adv}_{F}^{\mathsf{ind}}(\mathcal{A})$ = "how well can $\mathcal{A}$ tell them apart"

Indifferentiability

In ideal permutation model



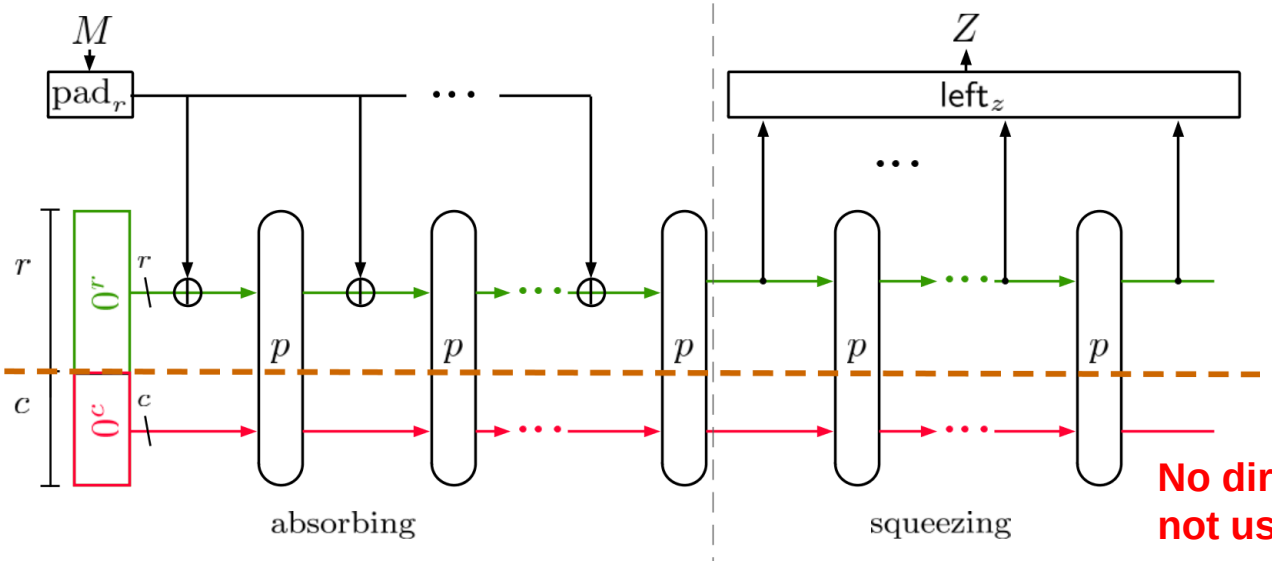
$$\mathbf{Adv}_{F}^{\text{ind}}(\mathcal{A}) = \text{“how well can } \mathcal{A} \text{ tell them apart”}$$

≈ 0 if attack not much better than random guess

- Proof = find **Sim** for which $\mathbf{Adv}_{F}^{\text{ind}} \approx 0$ for **all attackers** with certain resources

Indifferentiability of the sponge

Bertoni, Daemen, Peeters, Van Assche **2008**

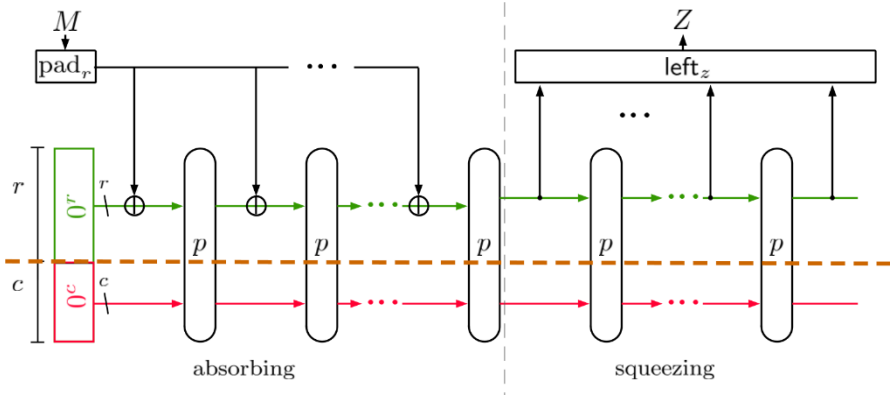


No direct control, not used for output

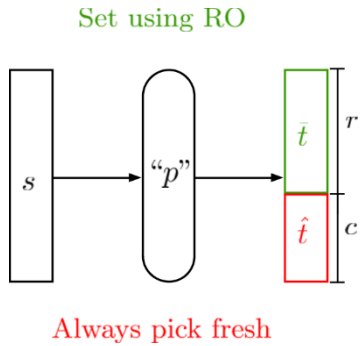
Indifferentiability of the sponge

Bertoni, Daemen, Peeters, Van Assche **2008**

Sponge:



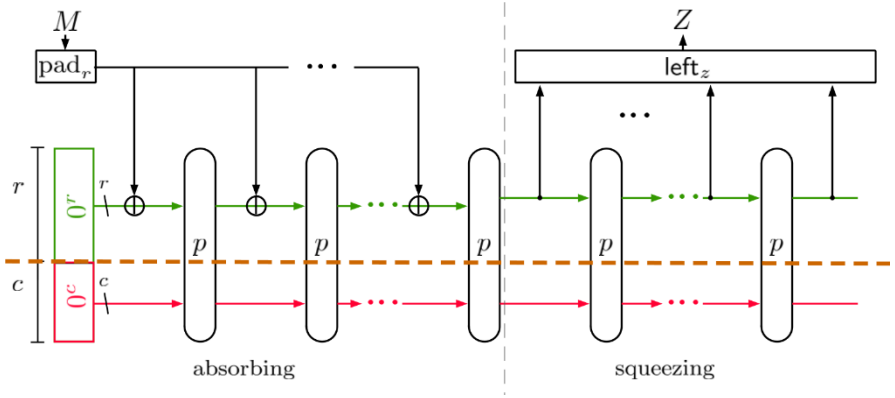
Simulator:



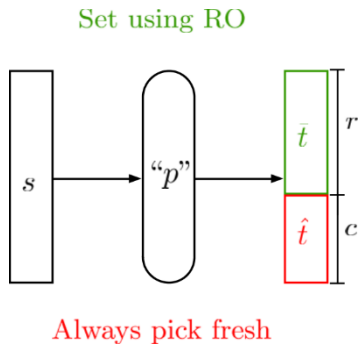
Indifferentiability of the sponge

Bertoni, Daemen, Peeters, Van Assche **2008**

Sponge:



Simulator:



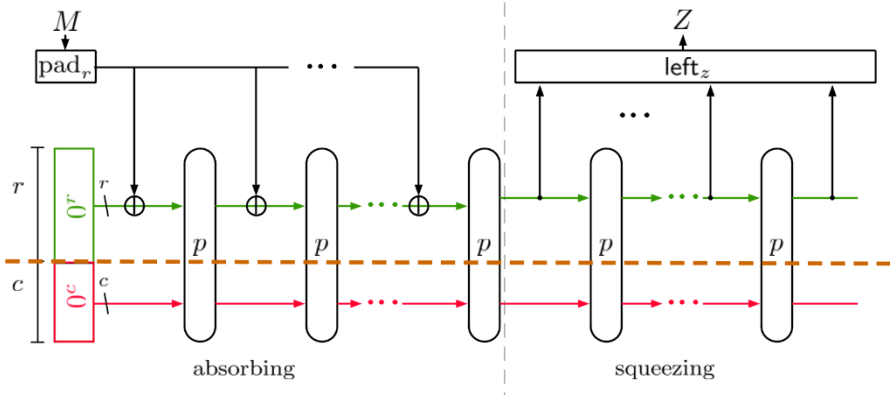
$$\mathbf{Adv}^{\mathrm{ind}}_{\mathrm{Sponge}}(N) \leq \frac{N^2}{2^c}$$

N = # of times *p* is evaluated in total
≈ time complexity

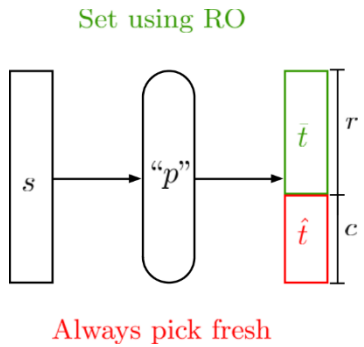
Indifferentiability of the sponge

Bertoni, Daemen, Peeters, Van Assche **2008**

Sponge:



Simulator:



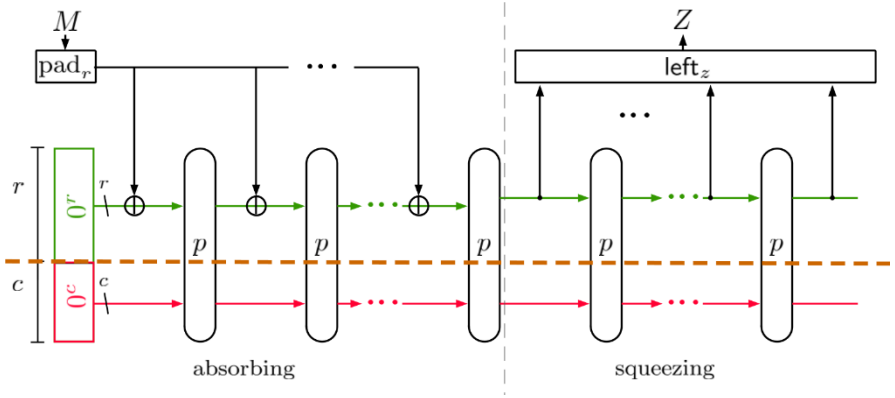
$$\mathbf{Adv}^{\mathrm{ind}}_{\mathrm{Sponge}}(N) \leq \frac{N^2}{2^c}$$

Real sponge+perm.:
Inner perm. part can **collide**

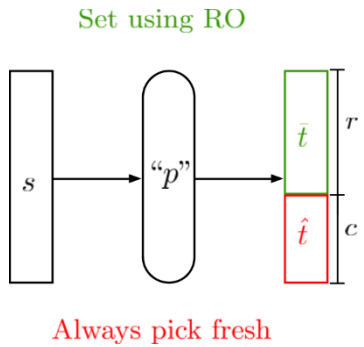
Indifferentiability of the sponge

Bertoni, Daemen, Peeters, Van Assche **2008**

Sponge:



Simulator:



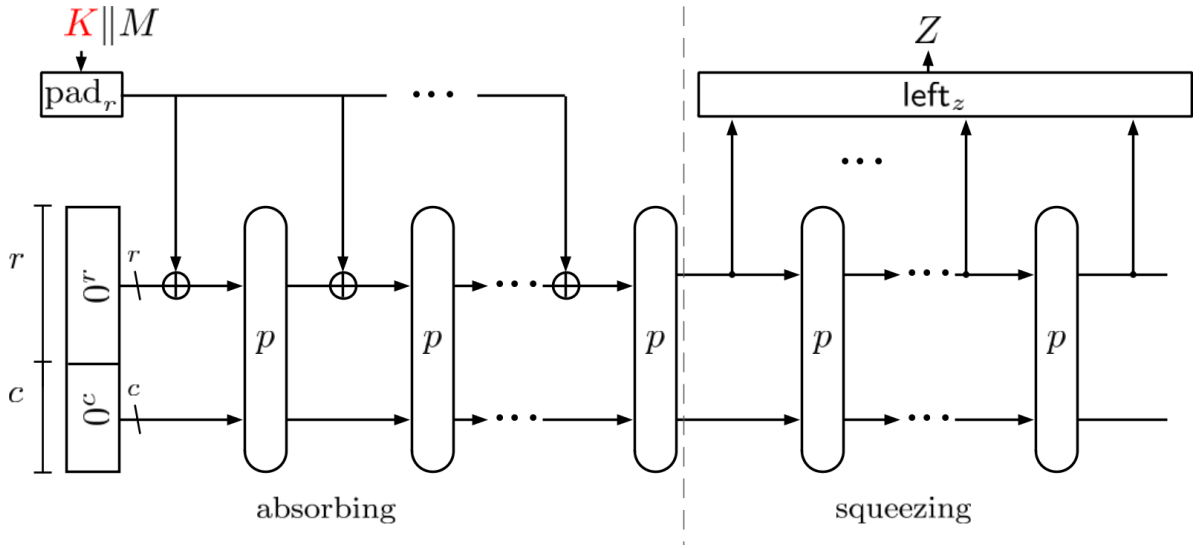
$$\mathbf{Adv}^{\mathsf{ind}}_{\mathrm{Sponge}}(N) \leq \frac{N^2}{2^c}$$

Implications:

- Time complexity of attack $N \approx 2^{\frac{c}{2}}$, so
- $c \geq 2 \cdot$ security level, e.g. $c = 160$ for 80-bit security

Keyed sponge security

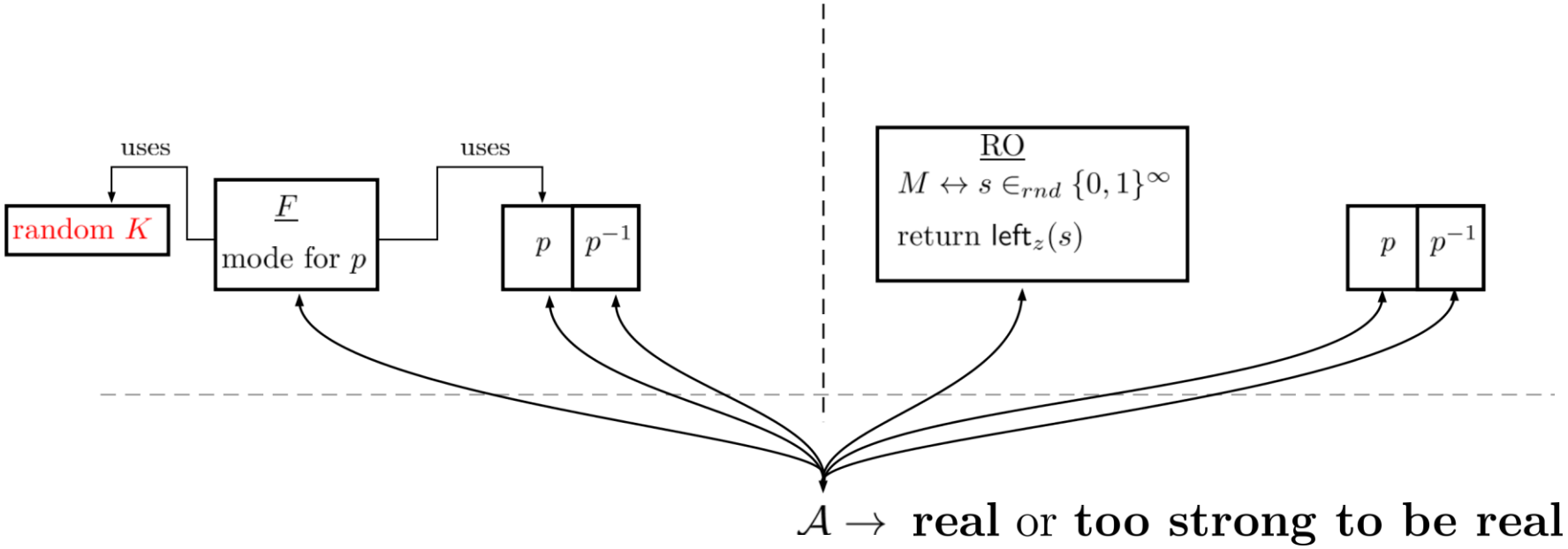
Bertoni, Daemen, Peeters, Van Assche **2011**



- Turn sponge into
  - a Message Authentication Code (MAC)
  - a Pseudorandom Function (PRF)
- Call it “Outer-keyed sponge”

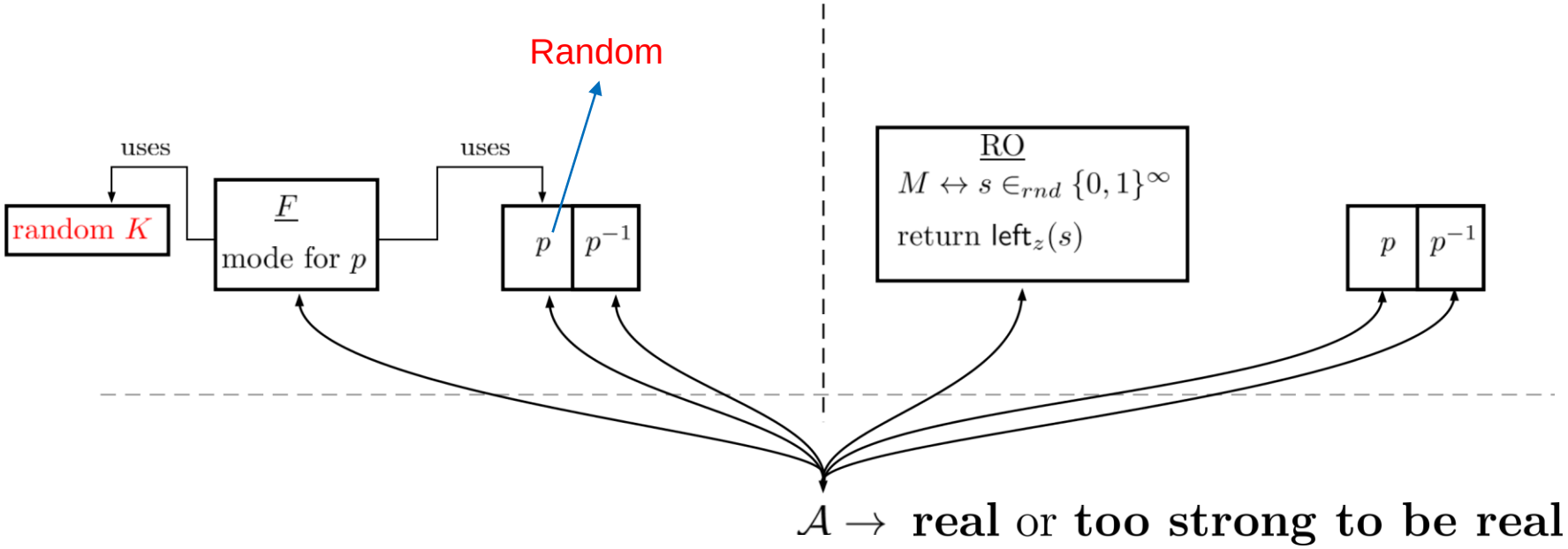
PRF security

Indistinguishability in ideal permutation model



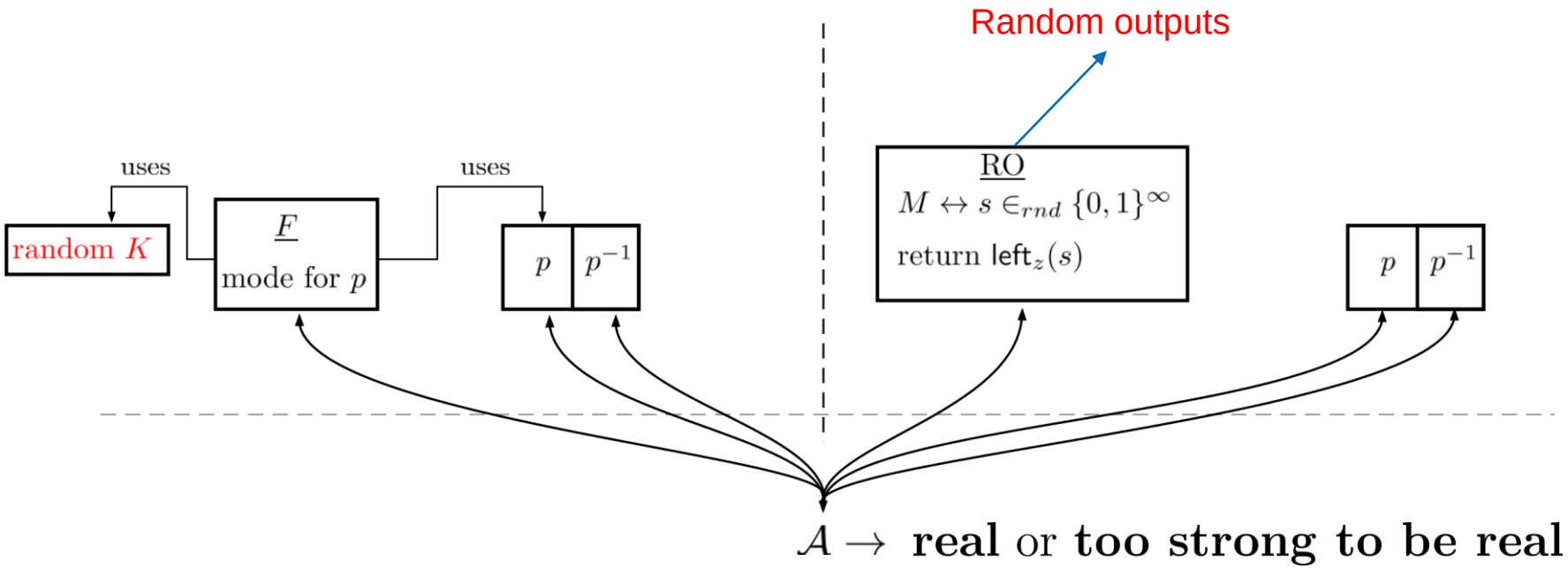
PRF security

Indistinguishability in ideal permutation model



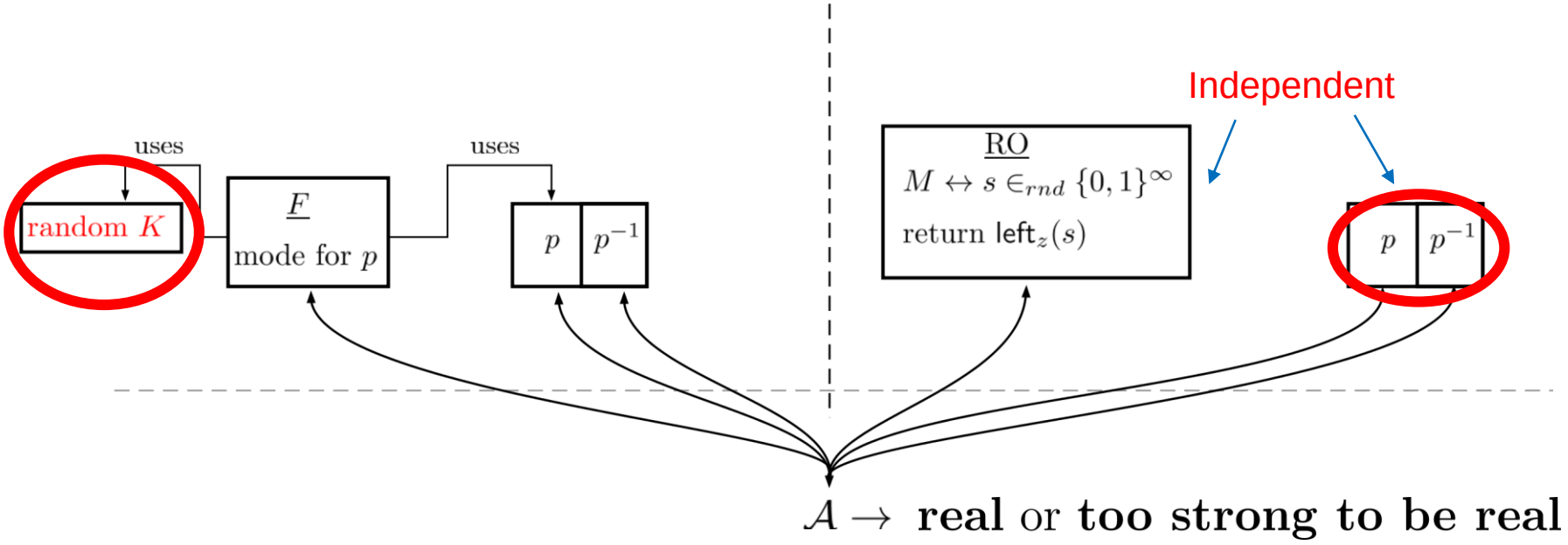
PRF security

Indistinguishability in ideal permutation model



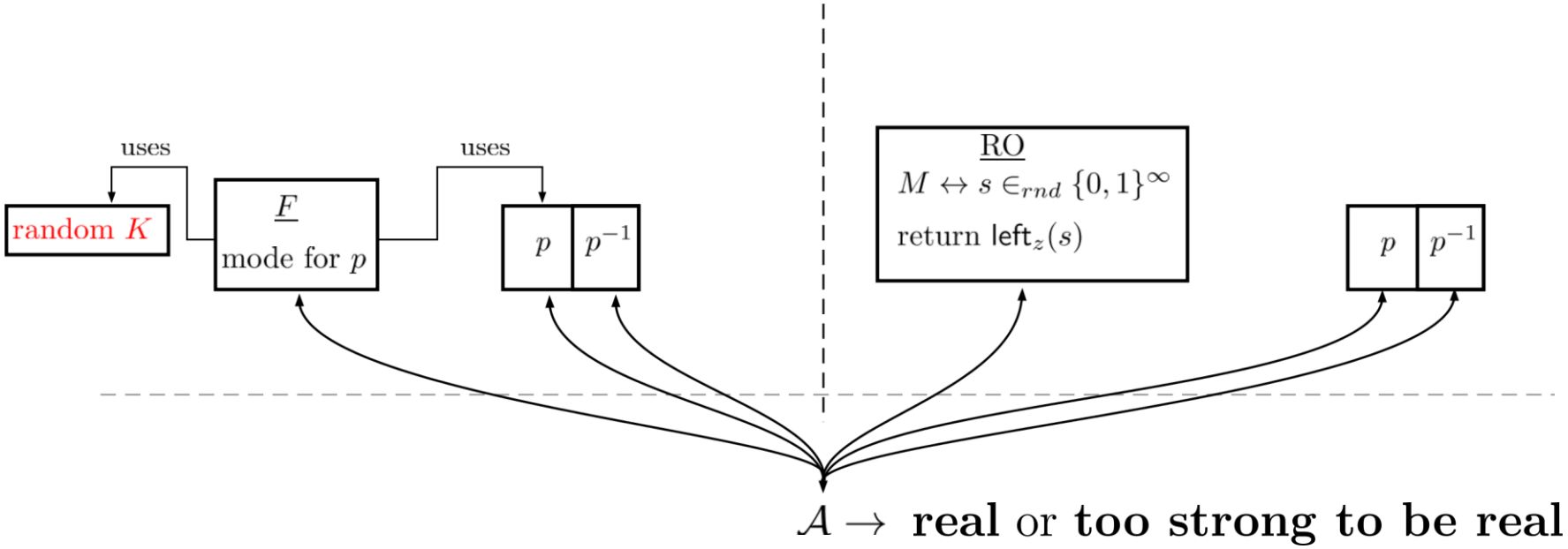
PRF security

Indistinguishability in ideal permutation model



PRF security

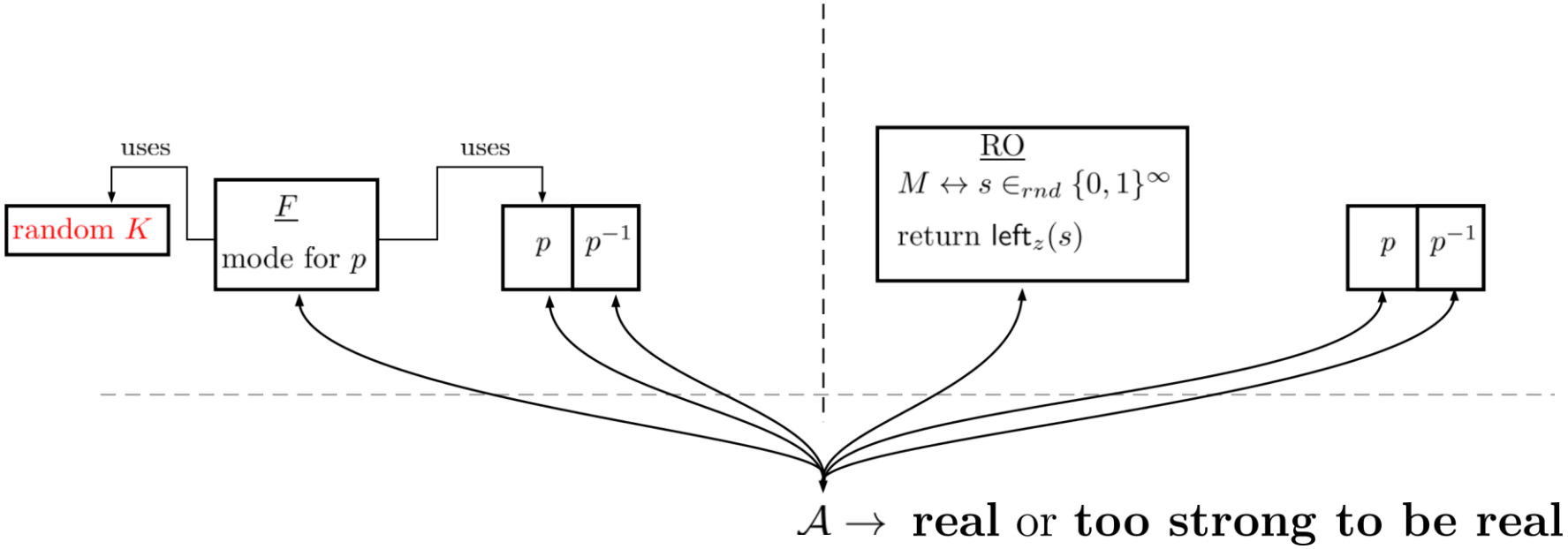
Indistinguishability in ideal permutation model



$$\mathbf{Adv}_{F}^{\mathsf{prf}}(\mathcal{A}) = \text{“how well can } \mathcal{A} \text{ tell them apart”}$$

PRF security

Indistinguishability in ideal permutation model



$$\mathbf{Adv}_{F}^{\mathrm{prf}}(\mathcal{A}) = \text{“how well can } \mathcal{A} \text{ tell them apart”}$$

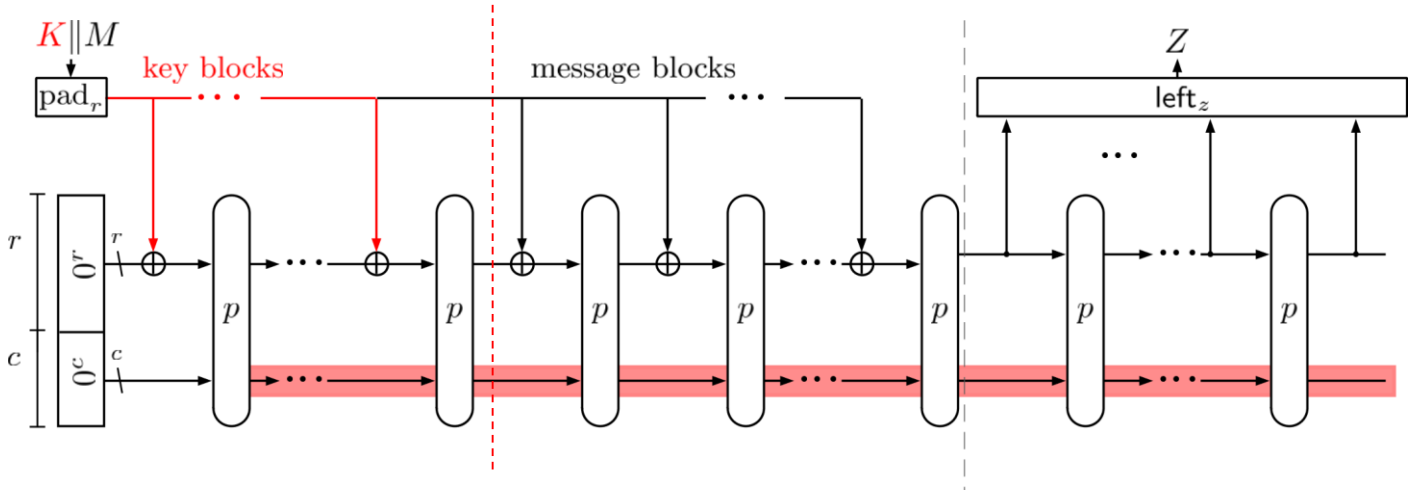
Resources:

- ***N*** **=** #of calls to p, p^{-1} **directly by attacker** ≈ time complexity
- ***M*** **=** #of calls to p **in the *F*-queries** ≈ data complexity

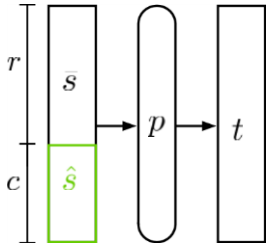
Security of outer-keyed sponge

Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



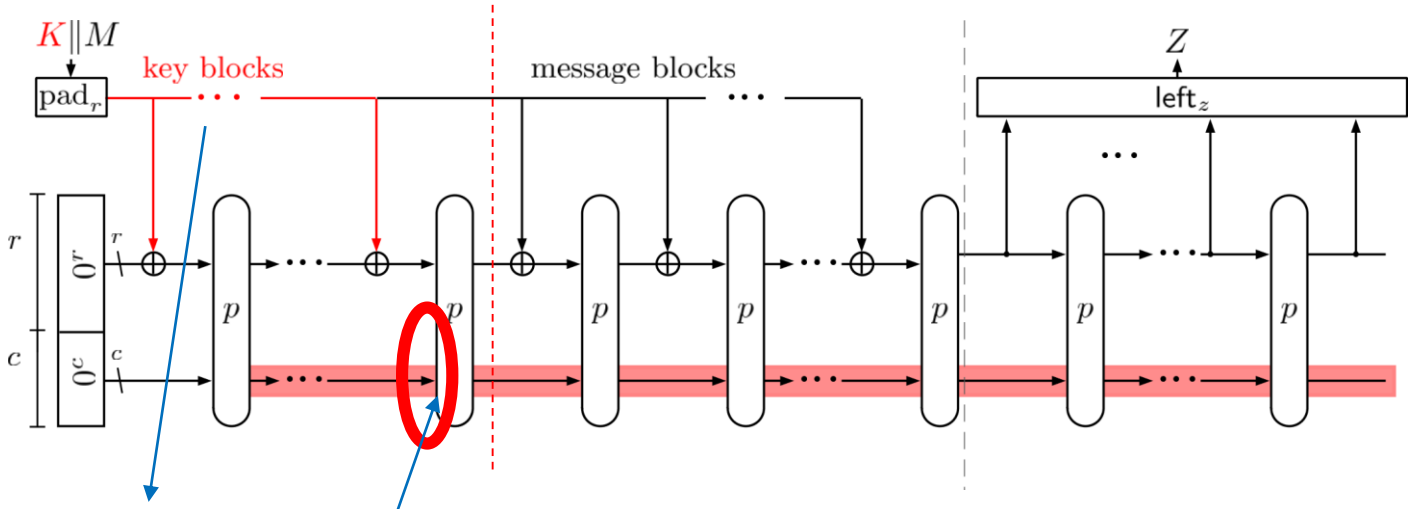
Perm. queries:



Security of outer-keyed sponge

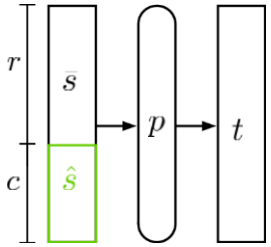
Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



no guess => unpredictable

Perm. queries:

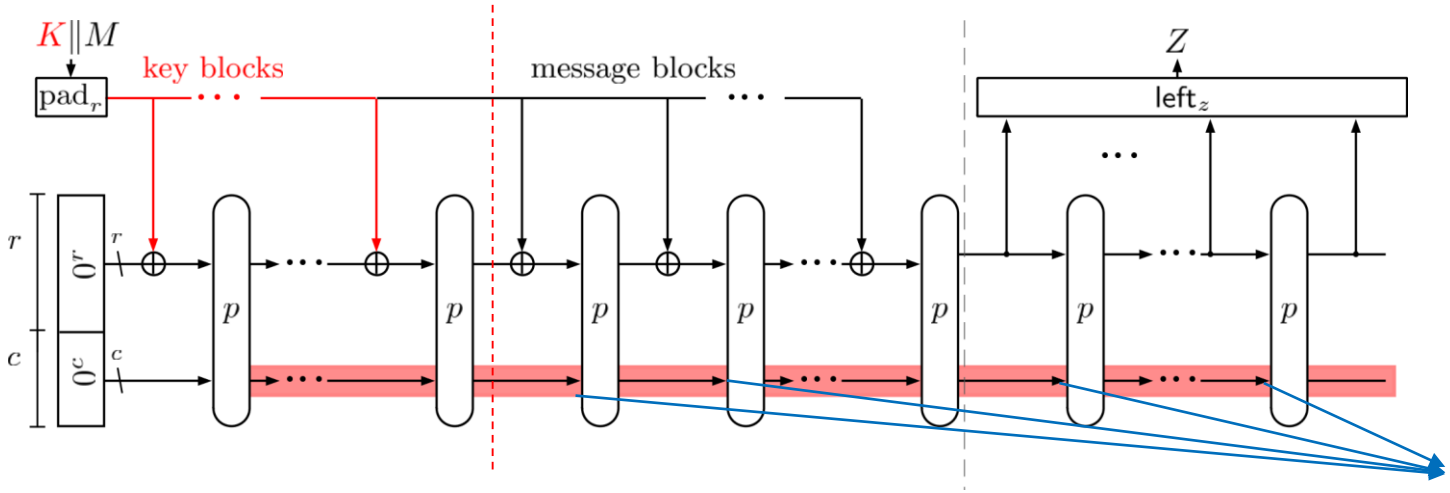


$$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K]$$

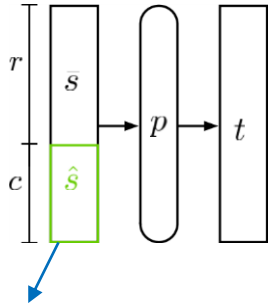
Security of outer-keyed sponge

Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



Perm. queries:



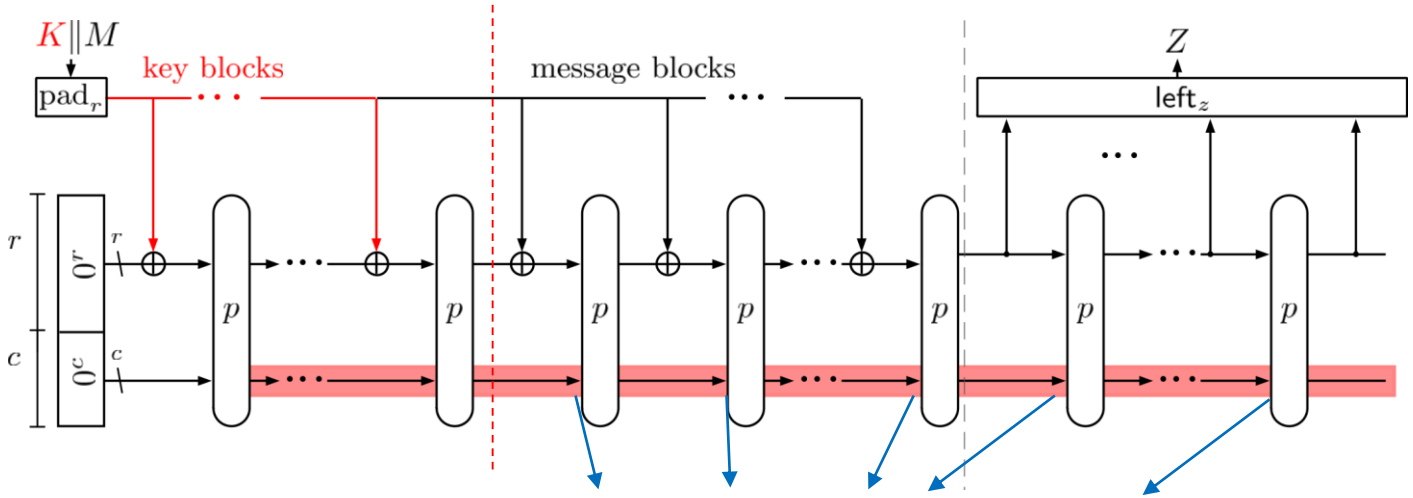
=> sponge output unpredictable

$$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c}$$

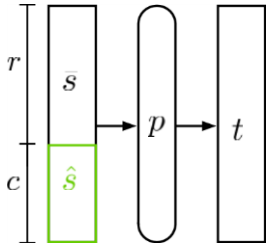
Security of outer-keyed sponge

Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



Perm. queries:



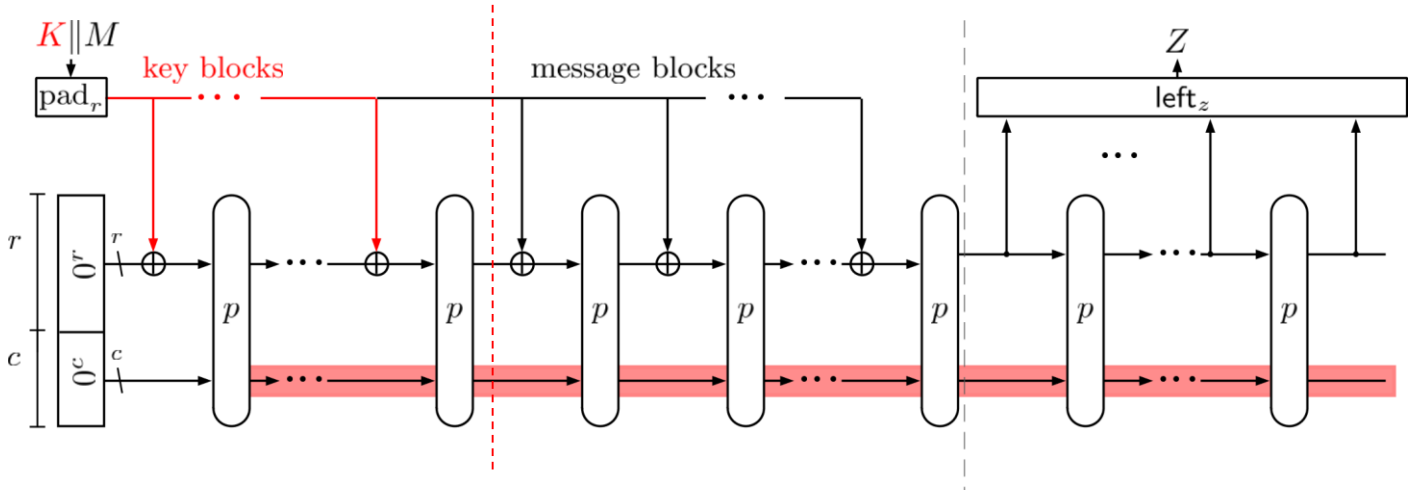
all unique => output “random”

$$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

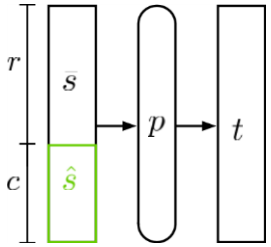
Security of outer-keyed sponge

Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



Perm. queries:



$$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M,N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

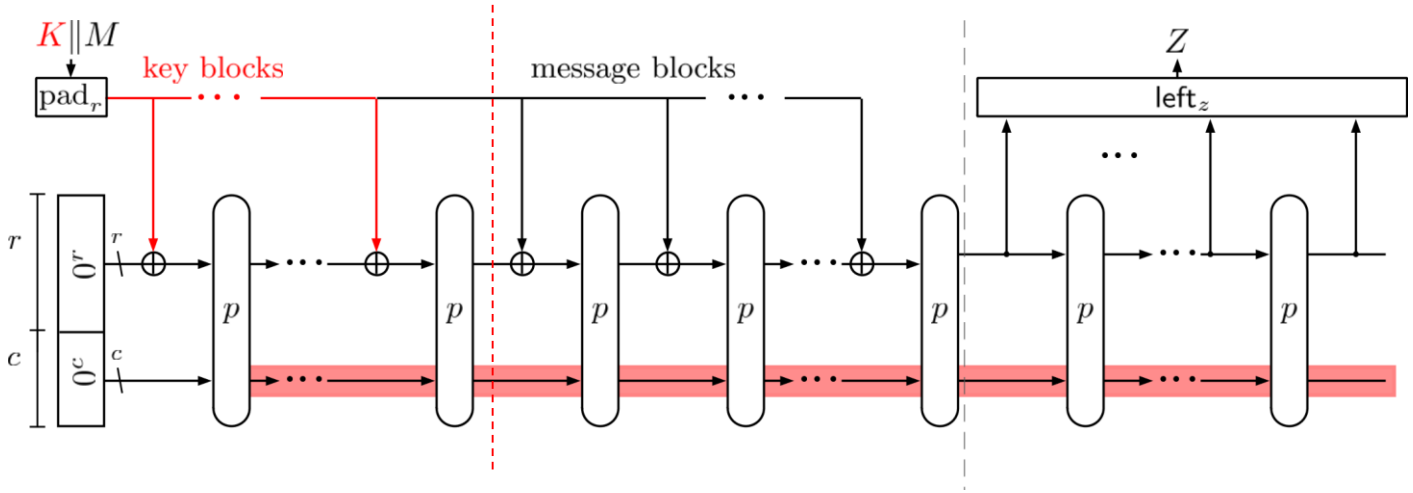
Implications:

$$\text{Time complexity } N \approx \min(2^c/M, 2^\kappa) \text{ if } M \ll 2^{\frac{c}{2}},\ \kappa \approx |K|$$

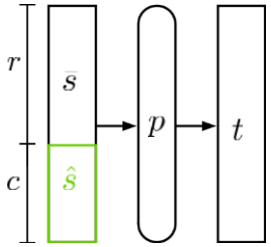
Security of outer-keyed sponge

Bertoni, Daemen, Peeters, Van Assche **2011**

Sponge queries:



Perm. queries:



$$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M,N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

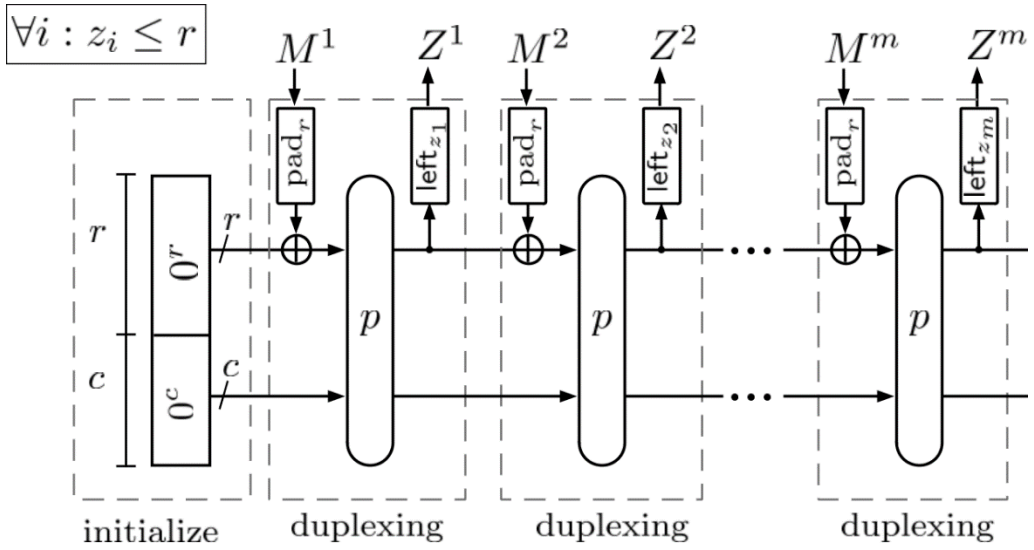
Implications:

Just estimated

Time complexity $N \approx \min(2^c/M, 2^\kappa)$ if $M \ll 2^{\frac{c}{2}}$, $\kappa \approx |K|$

Duplex construction

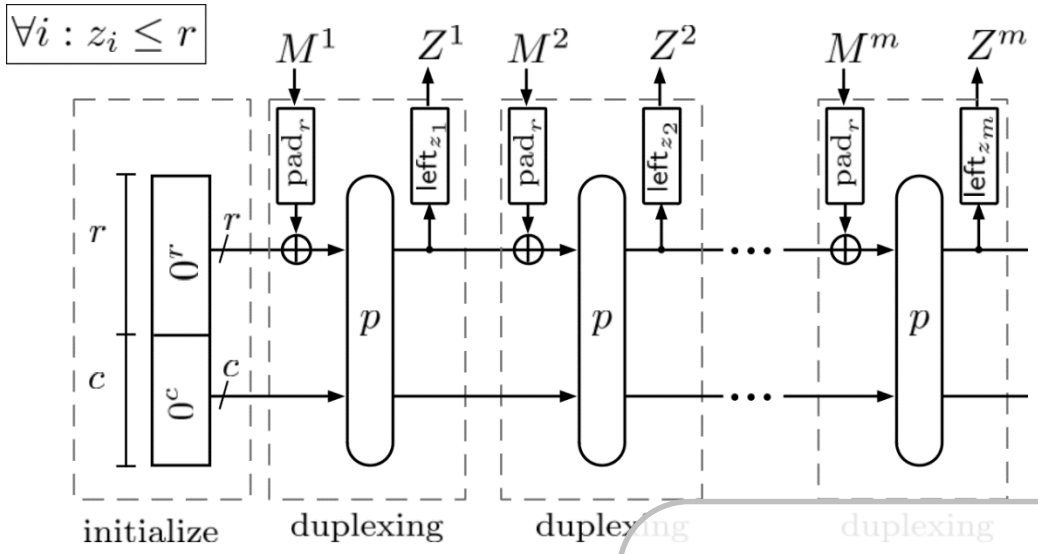
Bertoni, Daemen, Peeters, Van Assche **2011**



- "Stateful sponge"
- Interfaces: initialize & duplexing
- Security:

Duplex construction

Bertoni, Daemen, Peeters, Van Assche **2011**



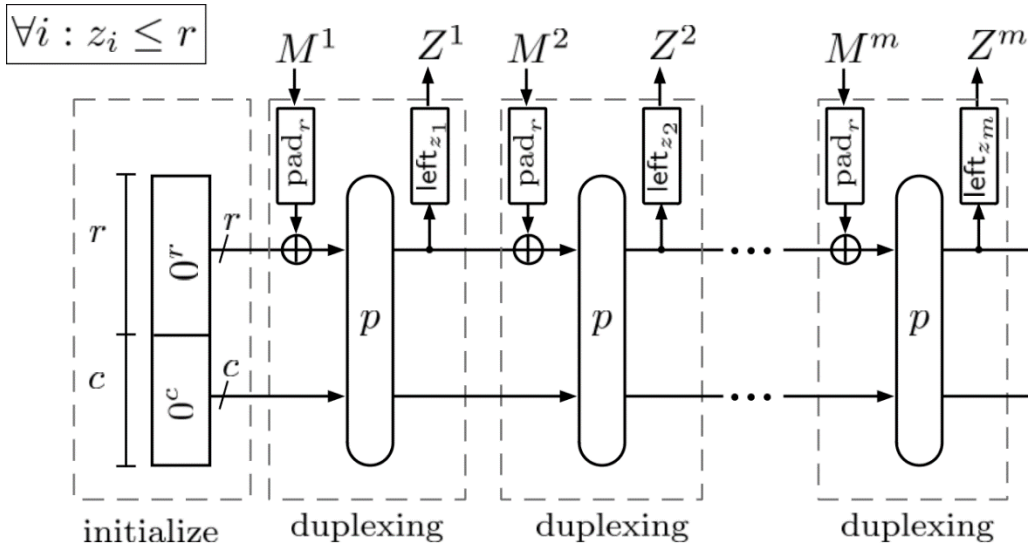
- "Stateful sponge"
- Interfaces: initialize & duplexing
- Security:

Equivalent with sponge:

$$Z_1 = \text{Sponge}(M_1, z_1)$$
$$Z_2 = \text{Sponge}(\text{pad}(M_1) \| M_2, z_2)$$
$$\dots$$

Duplex construction

Bertoni, Daemen, Peeters, Van Assche **2011**

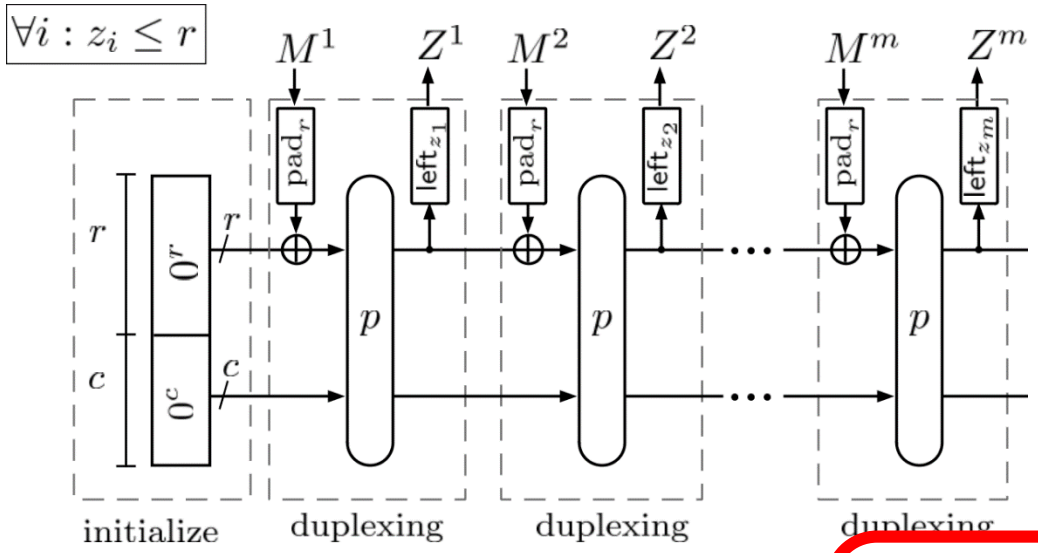


- "Stateful sponge"
- Interfaces: initialize & duplexing
- Security:

$$\mathbf{Adv}^{\text{prf}}_{\text{K.Duplex}}(M, N) \leq \mathbf{Pr}[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

Duplex construction

Bertoni, Daemen, Peeters, Van Assche **2011**



- "Stateful sponge"
- Interfaces: initialize & duplexing
- Security:

Duplex will return

$$\mathbf{Adv}^{\text{prf}}_{\text{K.Duplex}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

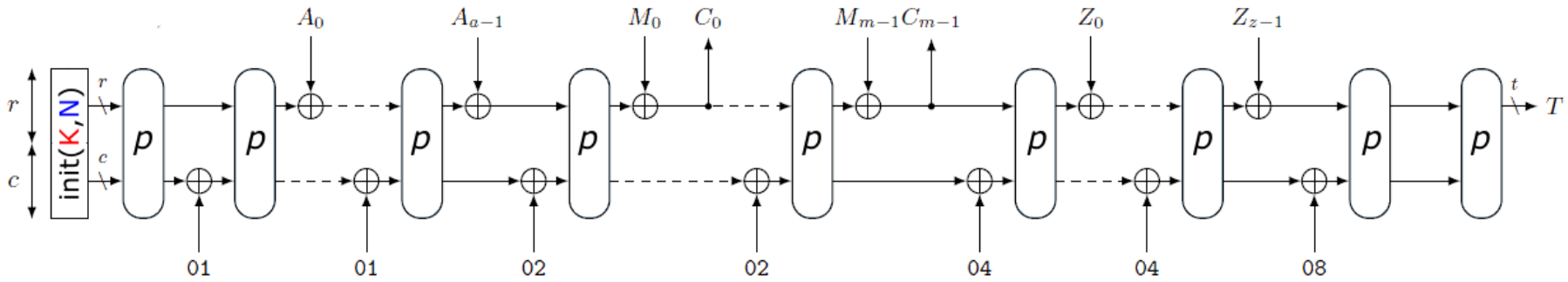
Summary 2008-2011

- Security given by inner state
- Keyless hashing
  - $N \approx 2^{c/2}$
- Keyed sponge
  - $N \approx \min(2^c/M, ???)$
  - must ensure $M \ll 2^{c/2}$

Security beyond $2^{c/2}$ in NORX

Jovanovic, Luykx, Mennink **2014**

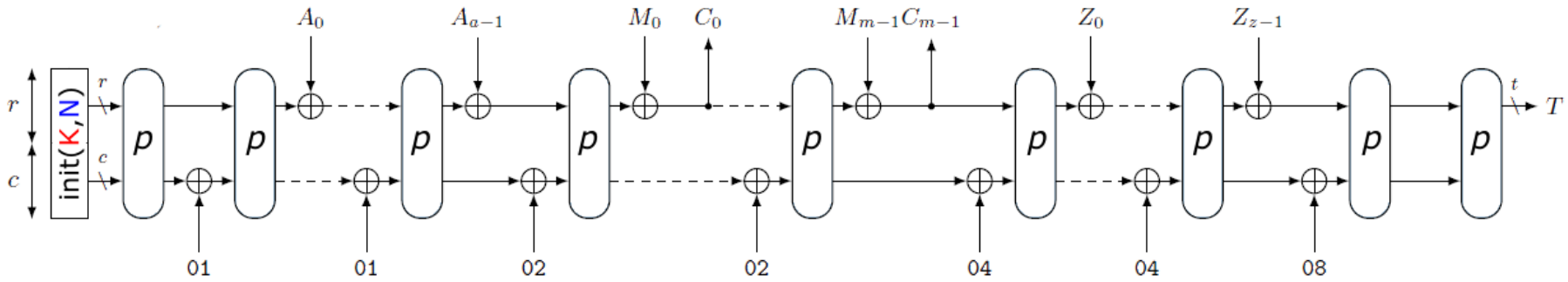
$C,T \leftarrow \text{Enc}(K,N,A,M,Z) \quad \approx \quad \text{Duplexing}(K||N,0) \rightarrow \text{Duplexing}(A_0,0)\ldots$



Security beyond $2^{c/2}$ in NORX

Jovanovic, Luykx, Mennink **2014**

C,T ← Enc(*K*,*N*,*A*,*M*,*Z*) ≈ Duplexing(*K*||*N*,*0*) →Duplexing(A_0,*0*)…



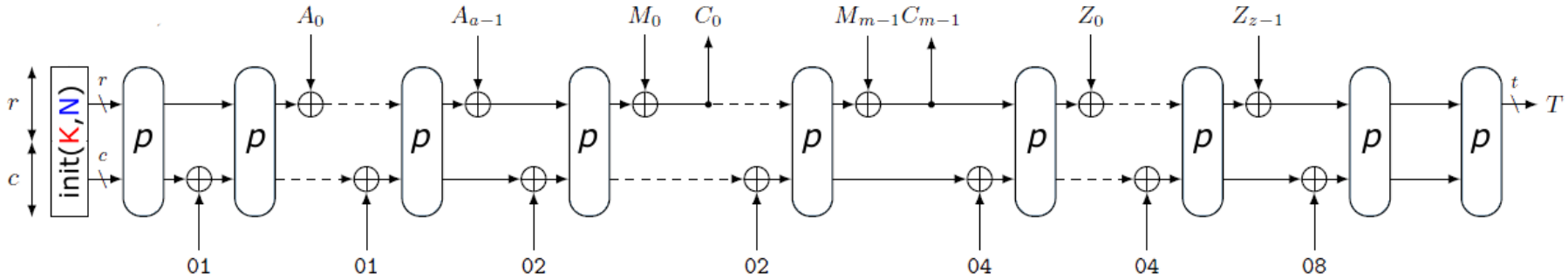
$$\mathbf{Adv}^{\approx\text{prf}}_{\text{NORX}}(M,N) \approx \frac{(M+N)^2}{2^{b+1}} + \frac{rN}{2^c} + \frac{N+M}{2^{|K|}}$$

Security beyond $2^{c/2}$ in NORX

Jovanovic, Luykx, Mennink **2014**

Main contribution:
foreshadow better bounds

C,T ← Enc(*K*,*N*,*A*,*M*,*Z*) ≈ Duplexing(*K*||*N*,*0*) →Duplexing(A_0,*0*)…



$$\mathbf{Adv}^{\approx\text{prf}}_{\text{NORX}}(M,N) \approx \frac{(M+N)^2}{2^{b+1}} + \frac{rN}{2^c} + \frac{N+M}{2^{|K|}}$$

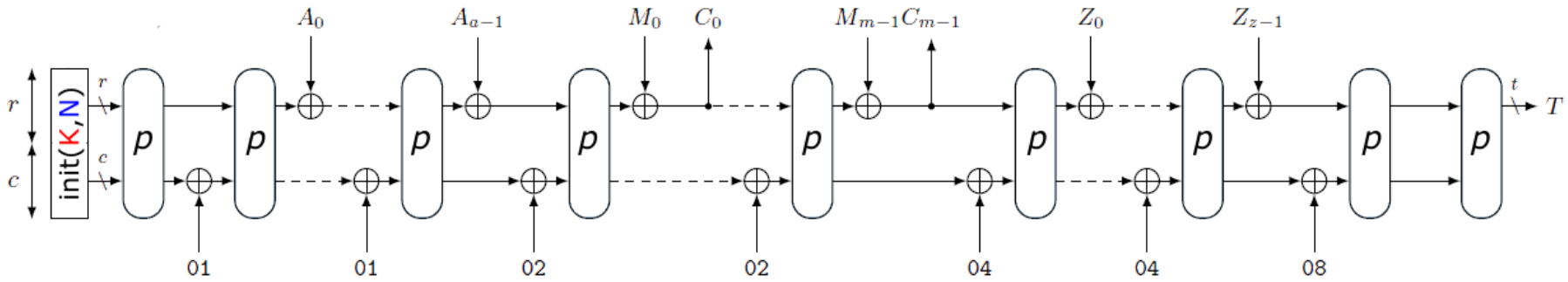
Time complexity $N \approx \min(2^{b/2} - M, 2^{|K|} - M, 2^c/r)$

Security beyond $2^{c/2}$ in NORX

Jovanovic, Luykx, Mennink **2014**

Main contribution:
foreshadow better bounds

$C,T \leftarrow \text{Enc}(K,N,A,M,Z) \quad \approx \quad \text{Duplexing}(K||N,0) \rightarrow \text{Duplexing}(A_0,0)\ldots$



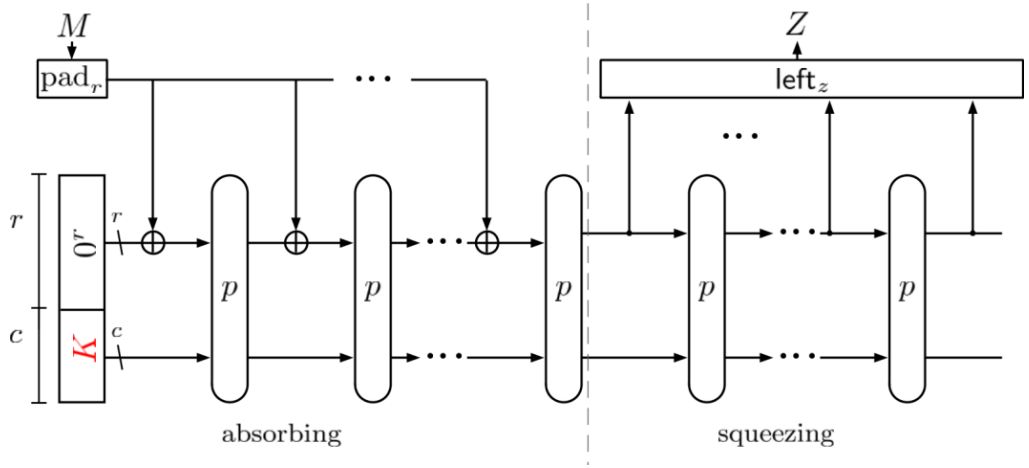
$$\mathbf{Adv}^{\approx\text{prf}}_{\text{NORX}}(M,N) \approx \frac{(M+N)^2}{2^{b+1}} + \frac{rN}{2^c} + \frac{N+M}{2^{|K|}}$$

Time complexity $N \approx \min(2^{b/2} - M, 2^{|K|} - M, 2^c/r)$

- Explicit key guessing, full security in *c* ☺
- Needs unique nonces, **specific to AE** ☹

Inner keyed sponge

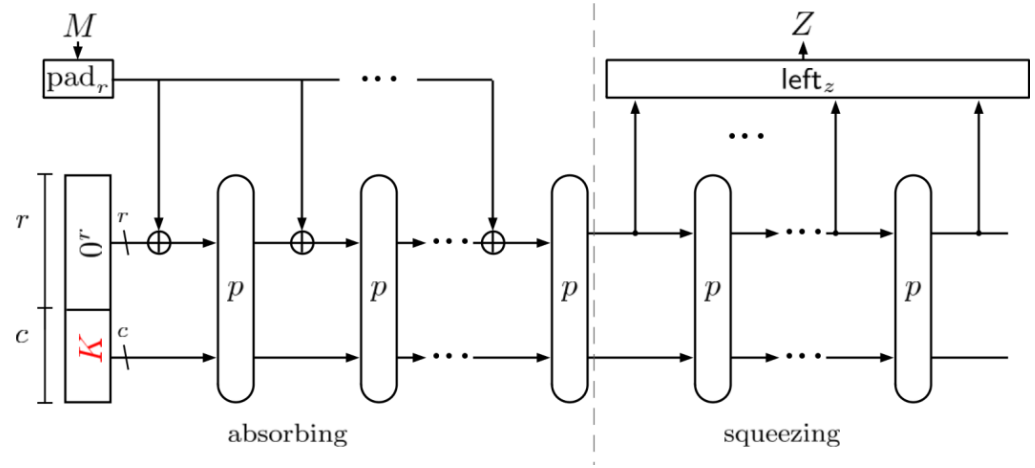
Chang, Dworkin, Hong, Kelsey, Nandi **2012**



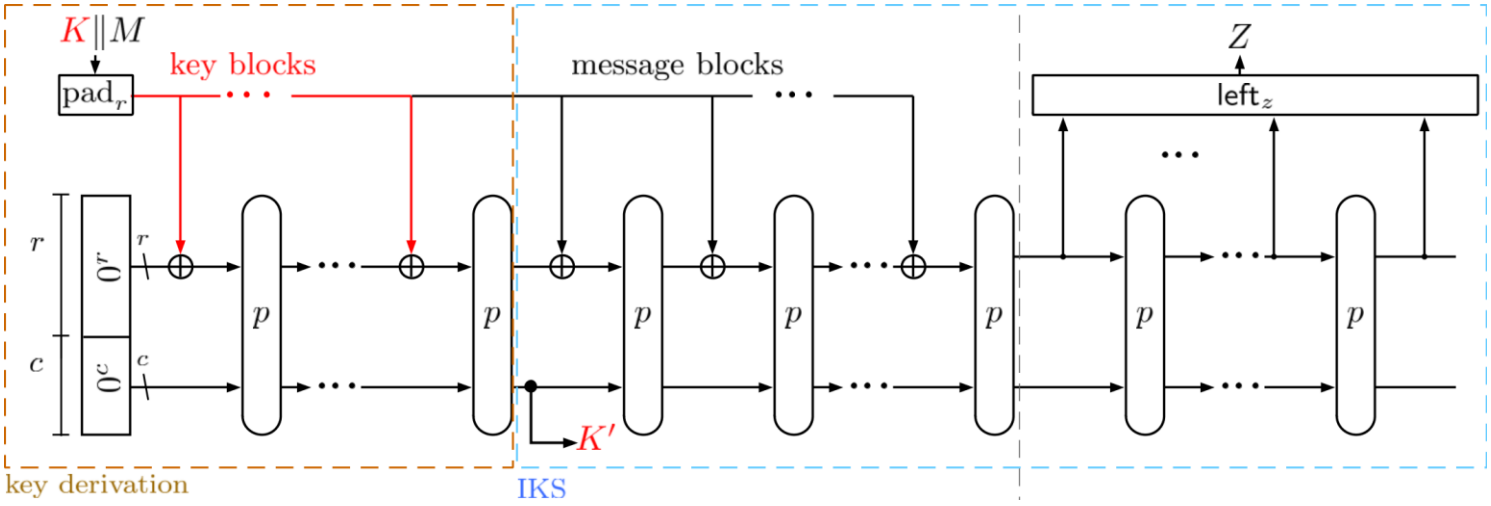
- Key in initial (inner) state

Inner keyed sponge

Chang, Dworkin, Hong, Kelsey, Nandi **2012**

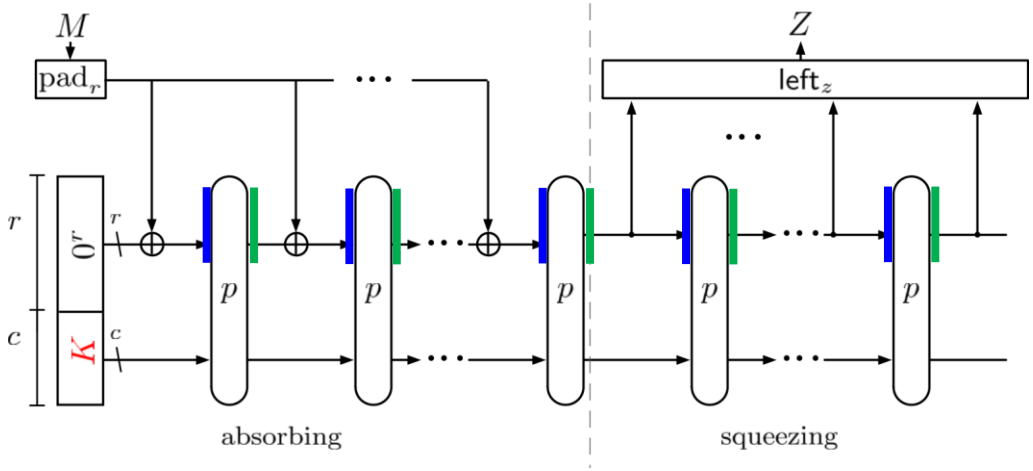


- Key in initial (inner) state
- Outer keyed vs IKS [ADMV 15]
  - OKS = key derivation + IKS



Security of the IKS

Andreeva, Daemen, Mennink, Van Assche **2015**



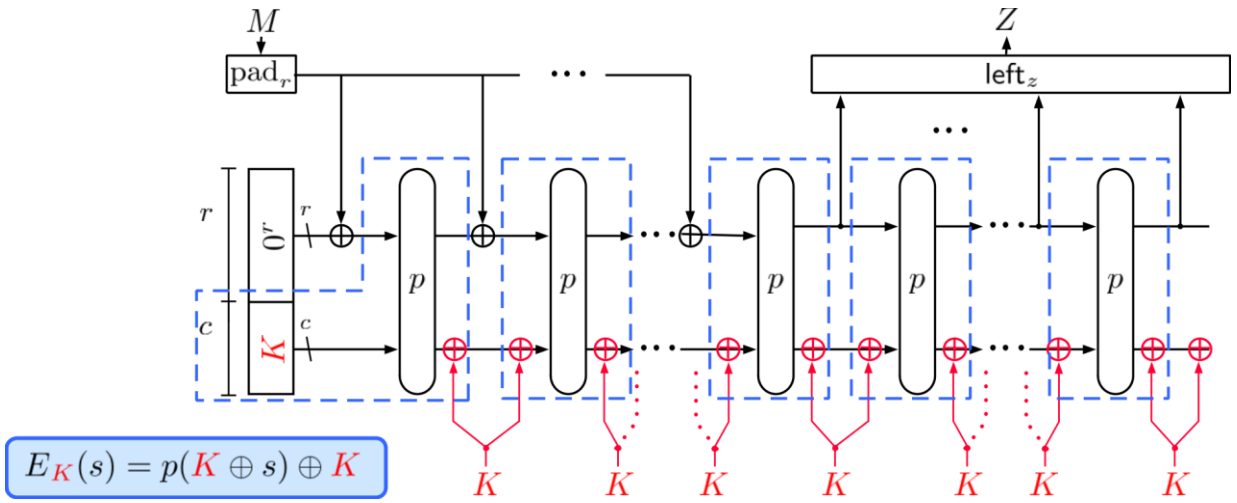
$1 \leq \mu \leq 2M$

- Multiplicity μ = max #{in states| same r-value} + max #{out states| same r-value}

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{IKS}}(M, N, \mu) \leq$$

Security of the IKS

Andreeva, Daemen, Mennink, Van Assche **2015**



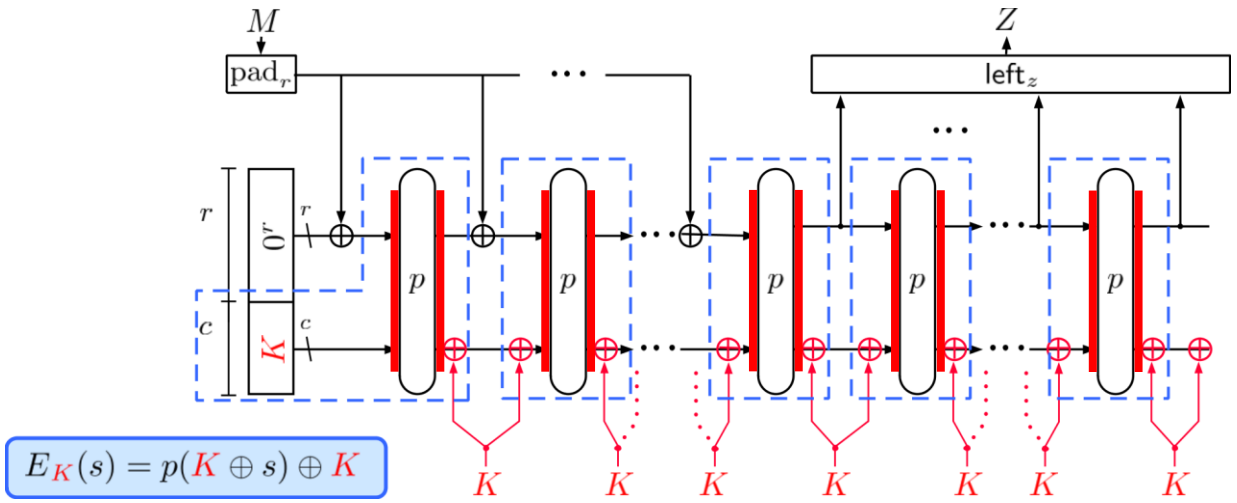
$E_K(s) = p(K \oplus s) \oplus K$

- Multiplicity μ = max #{in states| same r-value} + max #{out states| same r-value}
- $\mathrm{IKS}^p(K, M) = \mathrm{Sponge}^{E_K}(0^c, M)$

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{IKS}}(M, N, \mu) \leq$$

Security of the IKS

Andreeva, Daemen, Mennink, Van Assche **2015**

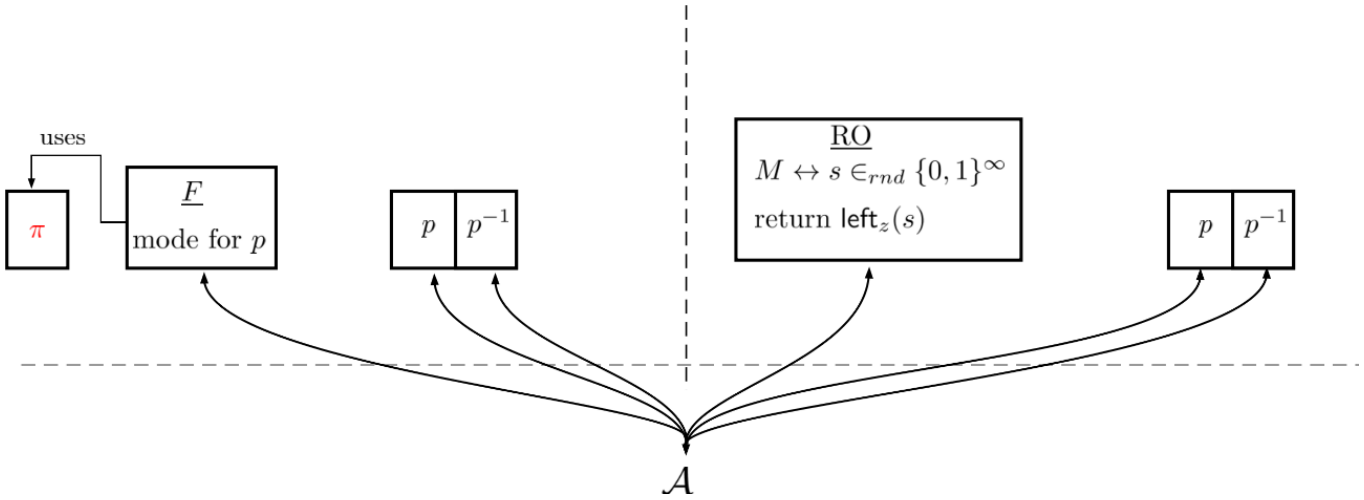


- Multiplicity μ = max #{in states| same r-value} + max #{out states| same r-value}
- $\mathrm{IKS}^p(K, M) = \mathrm{Sponge}^{E_K}(0^c, M)$ internal states secret => E_K ≈ secret permutation π

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{IKS}}(M, N, \mu) \leq \frac{\mu N}{2^c}$$

Security of the IKS

Andreeva, Daemen, Mennink, Van Assche **2015**

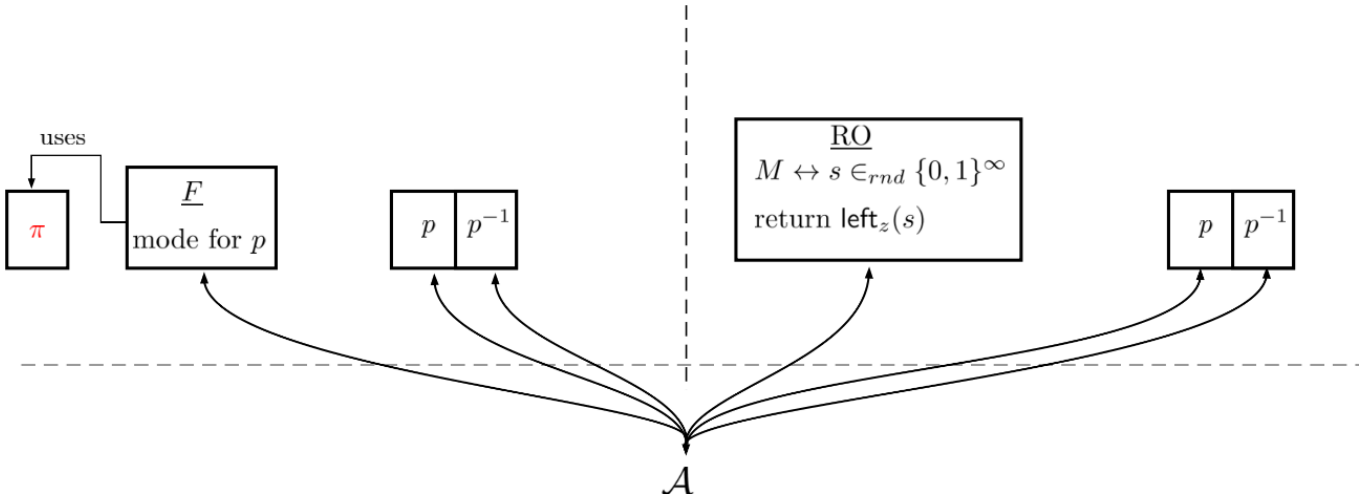


- Multiplicity μ = max #{in states| same r-value} + max #{out states| same r-value}
- $\mathrm{IKS}^{p}(K, M) = \mathrm{Sponge}^{E_K}(0^c, M)$ internal states secret => E_K ≈ secret permutation π

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{IKS}}(M, N, \mu) \leq \frac{\mu N}{2^c}$$

Security of the IKS

Andreeva, Daemen, Mennink, Van Assche **2015**



- Multiplicity μ = max #{in states| same r-value} + max #{out states| same r-value}
- $\mathrm{IKS}^{p}(K, M) = \mathrm{Sponge}^{E_K}(0^c, M)$
- Indifferentiability => secret-perm. sponge

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{IKS}}(M, N, \mu) \leq \frac{\mu N}{2^c} + \frac{M^2}{2^c}$$

Security of the OKS

Andreeva, Daemen, Mennink, Van Assche **2015**

NEW: $$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(M, N, \mu) \leq \frac{2\mu N}{2^c} + \lambda(N) + \frac{M^2}{2^c}$$

- Same as IKS + KDF security

Security of the OKS

Andreeva, Daemen, Mennink, Van Assche **2015**

NEW: $$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(M, N, \mu) \leq \frac{2\mu N}{2^c} + \lambda(N) + \frac{M^2}{2^c}$$

- Same as IKS + KDF security
- $\lambda(N) = \begin{cases} \frac{N}{2^{|K|}} & \text{if } K \equiv 0 (\mathrm{mod}\, r) \\ \frac{N}{2^{|K|/2}} & \text{else} \end{cases}$ [GPT 15]

Security of the OKS

Andreeva, Daemen, Mennink, Van Assche **2015**

Main contribution:
Better bound
(from $N \approx \min(2^c/M, 2^\kappa)$)

OLD: $$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

NEW: $$\mathbf{Adv}^{\text{prf}}_{\text{OKS}}(M, N, \mu) \leq \frac{2\mu N}{2^c} + \lambda(N) + \frac{M^2}{2^c}$$

- Same as IKS + KDF security
- $\lambda(N) = \begin{cases} \frac{N}{2^{|K|}} & \text{if } K \equiv 0 (\text{mod } r) \\ \frac{N}{2^{|K|/2}} & \text{else} \end{cases}$ [GPT 15]

Time complexity $N \approx \min\left(2^c/\mu, 2^{|K|/2}\right)$ with $1 \leq \mu \leq 2M$

Security of the OKS

Andreeva, Daemen, Mennink, Van Assche **2015**

Main contribution:
Better bound
(from $N \approx \min(2^c/M, 2^\kappa)$)

OLD: $$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

NEW: $$\mathbf{Adv}^{\text{prf}}_{\text{OKS}}(M, N, \mu) \leq \frac{2\mu N}{2^c} + \lambda(N) + \frac{M^2}{2^c}$$

- Same as IKS + KDF security
- $\lambda(N) = \begin{cases} \frac{N}{2^{|K|}} & \text{if } K \equiv 0 (\text{mod } r) \\ \frac{N}{2^{|K|/2}} & \text{else} \end{cases}$ [GPT 15]

Typically $\mu \approx M2^{-r}$

Time complexity $N \approx \min\left(2^c/\mu, 2^{|K|/2}\right)$ with $1 \leq \mu \leq 2M$

Security of the OKS

Andreeva, Daemen, Mennink, Van Assche **2015**

Main contribution:
Better bound
(from $N \approx \min(2^c/M, 2^\kappa)$)

OLD: $$\mathbf{Adv}^{\text{prf}}_{\text{K.Sponge}}(M, N) \leq \Pr[\mathcal{A} \text{ guesses } K] + \frac{2(M+1)(N+1)}{2^c} + \frac{M^2}{2 \cdot 2^c}$$

NEW: $$\mathbf{Adv}^{\text{prf}}_{\text{OKS}}(M, N, \mu) \leq \frac{2\mu N}{2^c} + \lambda(N) + \frac{M^2}{2^c}$$

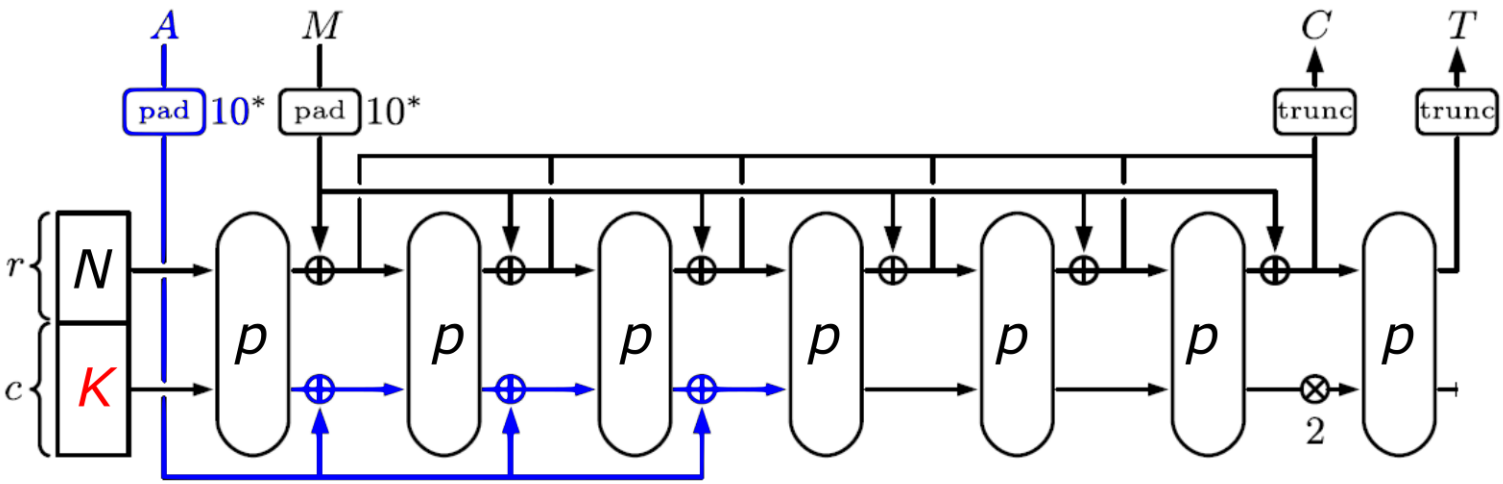
- Same as IKS + KDF security
- $\lambda(N) = \begin{cases} \frac{N}{2^{|K|}} & \text{if } K \equiv 0 (\text{mod } r) \\ \frac{N}{2^{|K|/2}} & \text{else} \end{cases}$ [GPT 15]
- no *M* in capacity term ☺ restriction on M<$2^{c/2}$ ☹

Typically $\mu \approx M2^{-r}$

Time complexity $N \approx \min\left(2^c/\mu, 2^{|K|/2}\right)$ with $1 \leq \mu \leq 2M$

(Partially) full-state sponge based AE

Sasaki, Yasuda **2015**

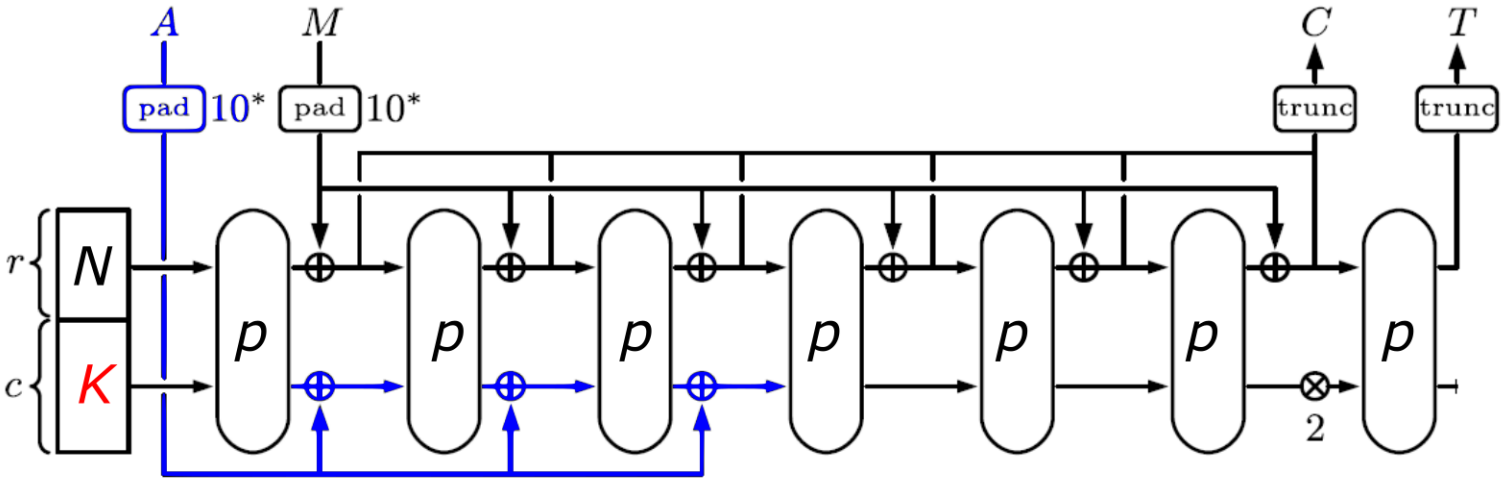


- Use **full state** to absorb => increased efficiency
- Similar bound as Jovanovic, Luykx and Mennink

(Partially) full-state sponge based AE

Sasaki, Yasuda **2015**

Main contribution:
Foreshadow full-state absorbtion

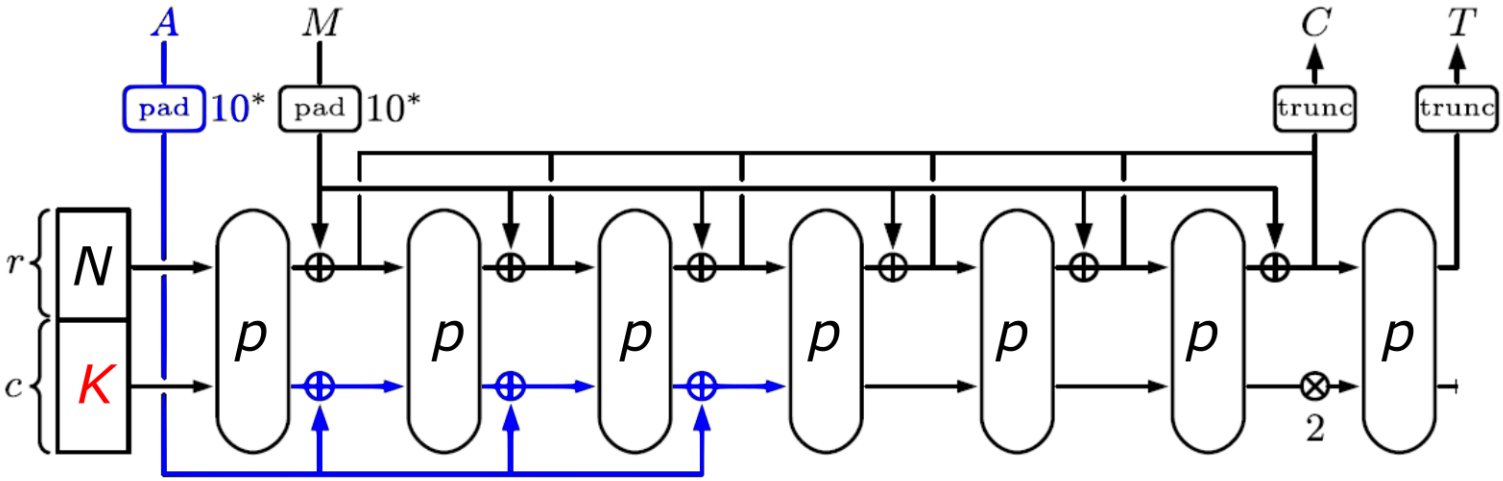


- Use **full state** to absorb => increased efficiency
- Similar bound as Jovanovic, Luykx and Mennink

(Partially) full-state sponge based AE

Sasaki, Yasuda **2015**

Main contribution:
Foreshadow full-state absorbtion

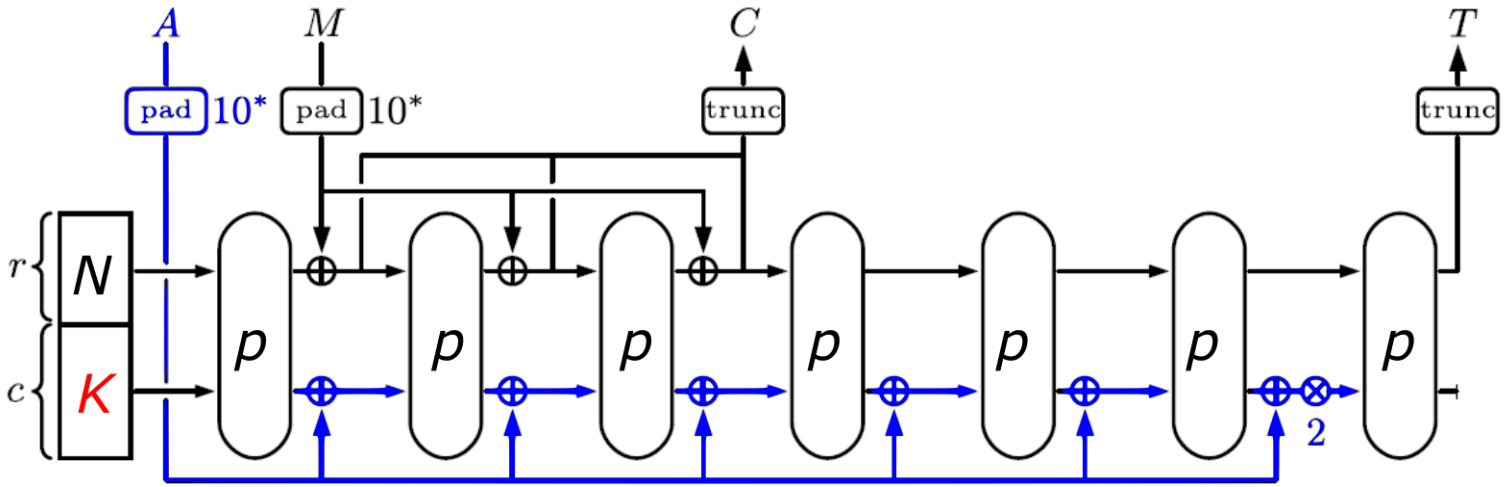


- Use **full state** to absorb => increased efficiency
- Similar bound as Jovanovic, Luykx and Mennink
- Specific to AE ☹

(Partially) full-state sponge based AE

Sasaki, Yasuda **2015**

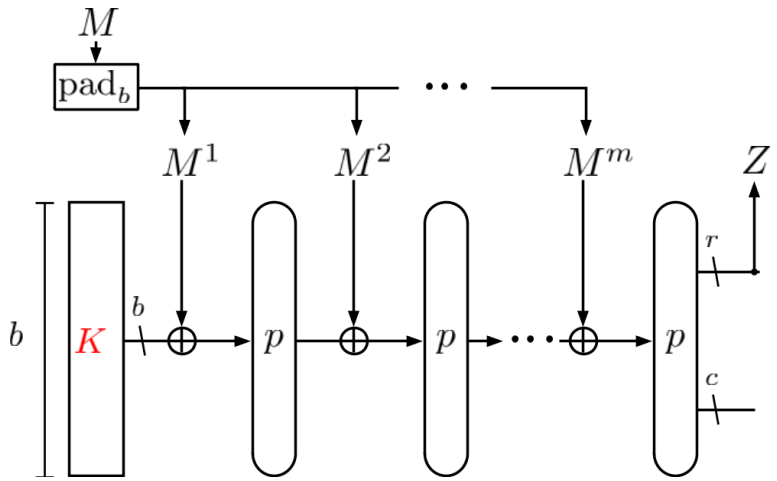
Main contribution:
Foreshadow full-state absorbtion



- Use **full state** to absorb => increased efficiency
- Similar bound as Jovanovic, Luykx and Mennink
- Specific to AE ☹
- Only partially full-state ☹
  - Lack of generic mechanism and analysis

Full-state sponge (fixed output size)

Gaži, Pietrzak, Tessaro **2015**



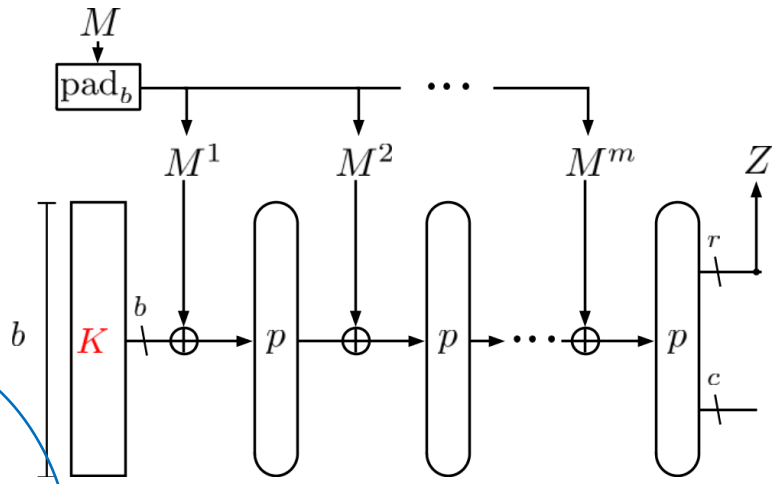
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}'}(q, N, \ell) \approx \frac{\ell q^2 + \ell q N}{2^b} + \frac{q^2 + \ell q + q N}{2^c} \qquad \text{if } \ell < 2^{n/4}$$

Full-state sponge (fixed output size)

Gaži, Pietrzak, Tessaro **2015**

max value of *m*

#of sponge queries

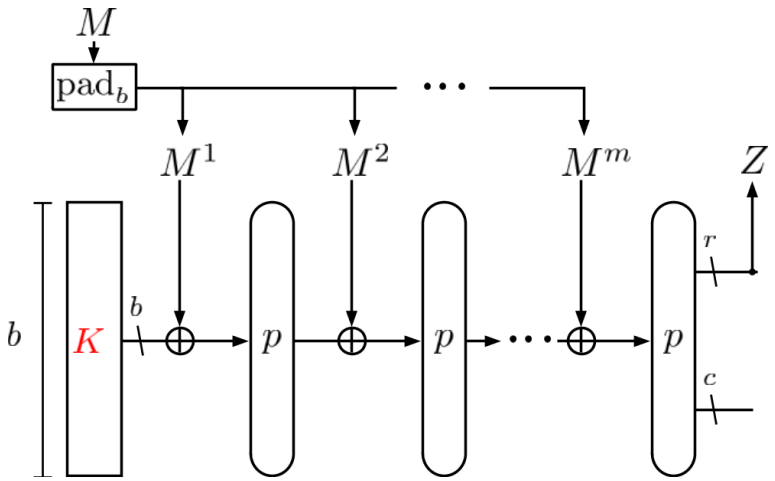


$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}'}(q, N, \ell) \approx \frac{\ell q^2 + \ell q N}{2^b} + \frac{q^2 + \ell q + q N}{2^c} \qquad \text{if } \ell < 2^{n/4}$$

Full-state sponge (fixed output size)

Gaži, Pietrzak, Tessaro **2015**

Main contribution:
Full-state(but limited output)
Improved bound (from $N \approx 2^c/\mu$)



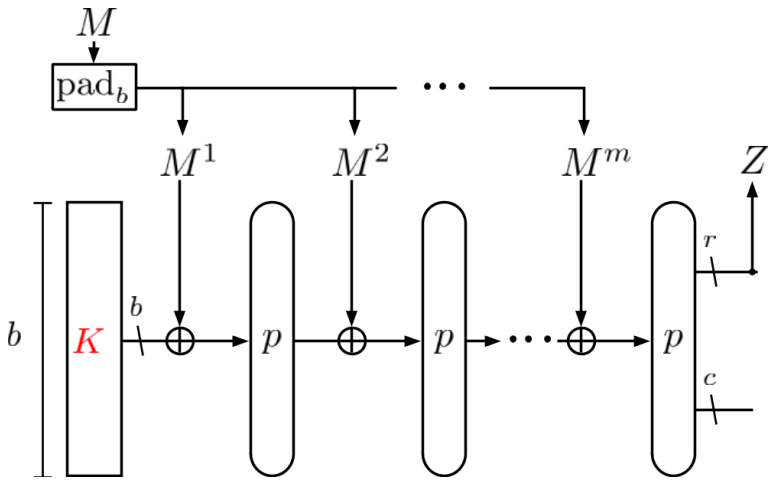
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}'}(q, N, \ell) \approx \frac{\ell q^2 + \ell q N}{2^b} + \frac{q^2 + \ell q + q N}{2^c} \qquad \text{if } \ell < 2^{n/4}$$

$$N \approx \min\left(2^b/(q\ell), 2^c/q\right) \qquad \text{if } \ell q^2 \ll 2^b,\ q^2 \ll 2^c \text{ and } \ell q \ll 2^c$$

Full-state sponge (fixed output size)

Gaži, Pietrzak, Tessaro **2015**

Main contribution:
Full-state(but limited output)
Improved bound (from $N \approx 2^c/\mu$)



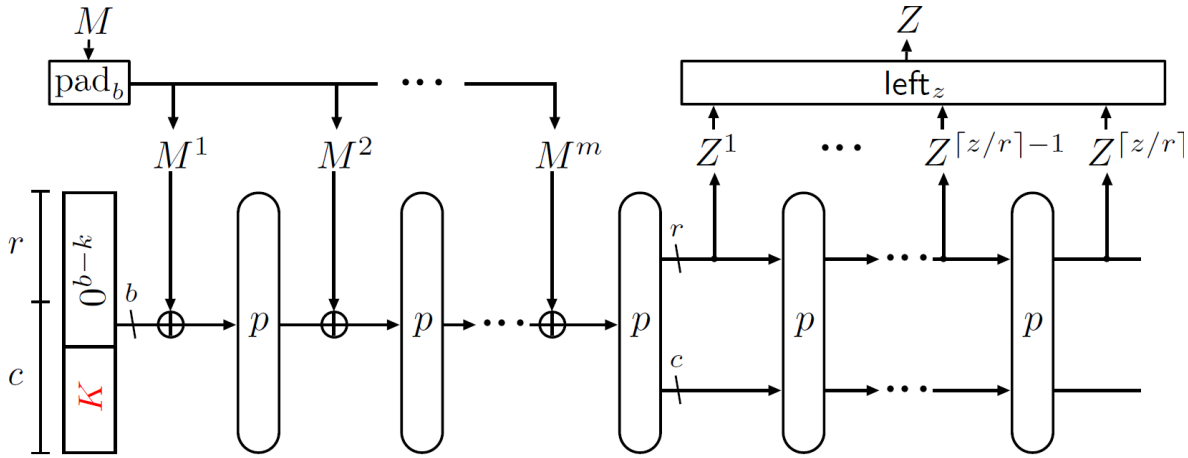
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}'}(q, N, \ell) \approx \frac{\ell q^2 + \ell q N}{2^b} + \frac{q^2 + \ell q + q N}{2^c} \qquad \text{if } \ell < 2^{n/4}$$

$$N \approx \min\left(2^b/(q\ell), 2^c/q\right) \qquad \text{if } \ell q^2 \ll 2^b,\ q^2 \ll 2^c \text{ and } \ell q \ll 2^c$$

- Full-state and tight bound ☺ (analysis complicated 😐)
- Does not cover variable output length ☹

Full state keyed sponge and duplex

Mennink, Reyhanitabar, Vizár **2015**



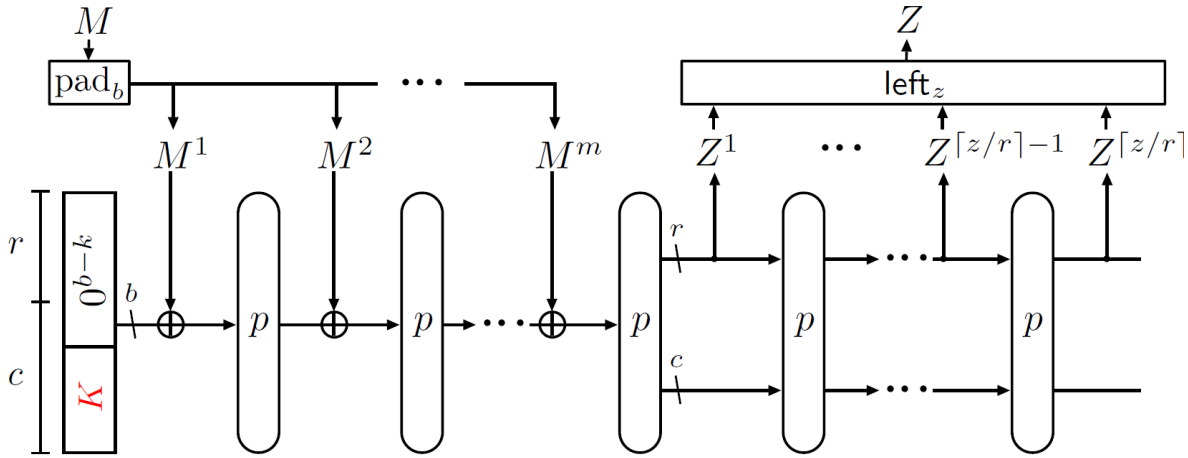
- General, variable output sponge ☺
  - Call it FKS
- Full-state absorption ☺

Full state keyed sponge and duplex

Mennink, Reyhanitabar, Vizár **2015**

The cost of Sponge(M,z):

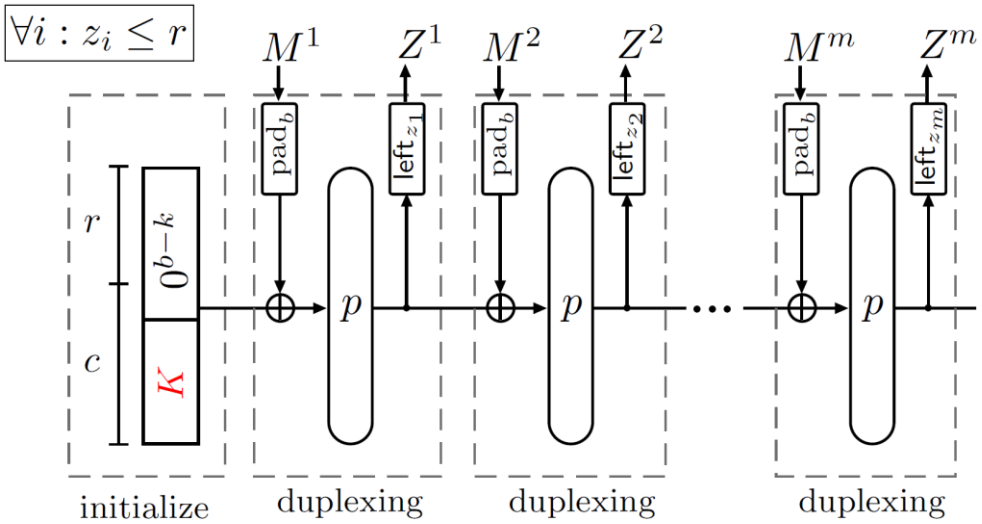
$\lceil |M|/b \rceil + \lfloor z/r \rfloor$ **calls to p**



- General, variable output sponge ☺
  - Call it FKS
- Full-state absorption ☺

Full state keyed sponge and duplex

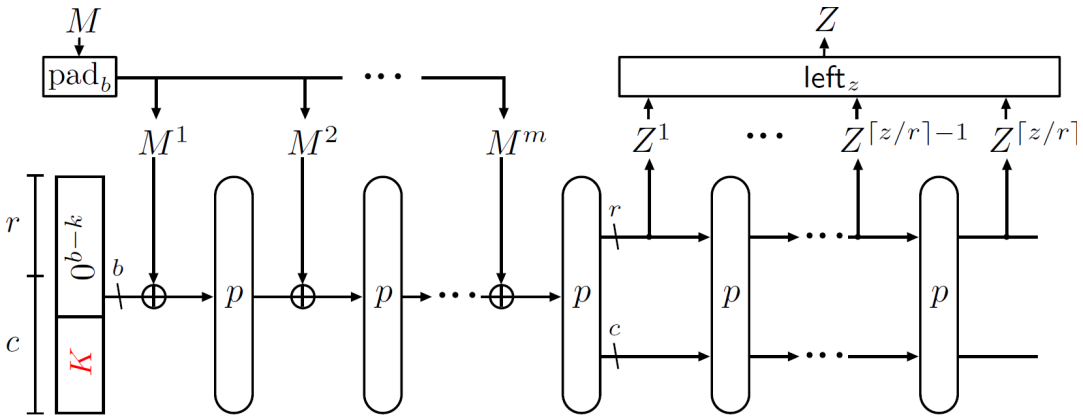
Mennink, Reyhanitabar, Vizár **2015**



- General, variable output sponge ☺
  - Call it FKS
- Full-state absorption ☺
- Also full-state duplex
  - Security reduced to sponge as before [BDPV 11]

Security of FKS

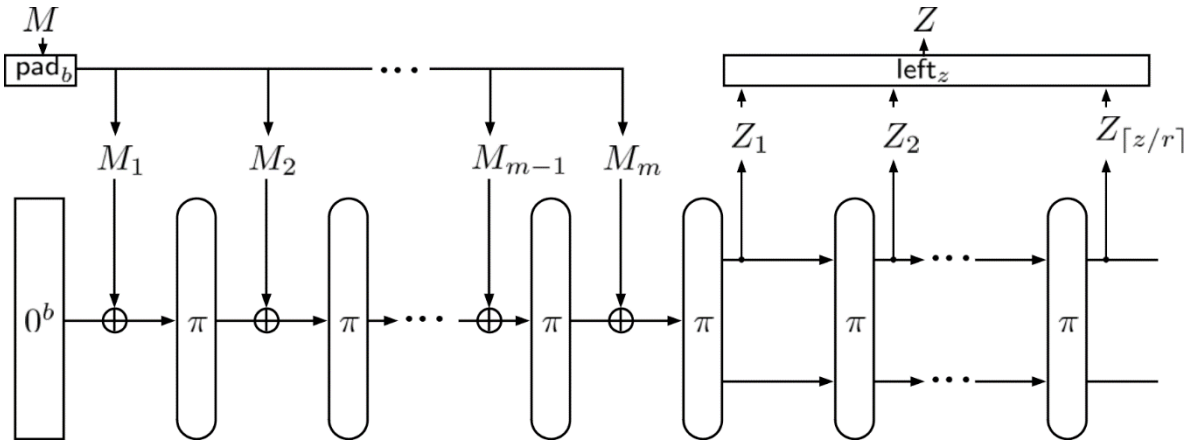
Mennink, Reyhanitabar, Vizár 2015



$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, \ell, \mu) \leq$$

Security of FKS

Mennink, Reyhanitabar, Vizár 2015

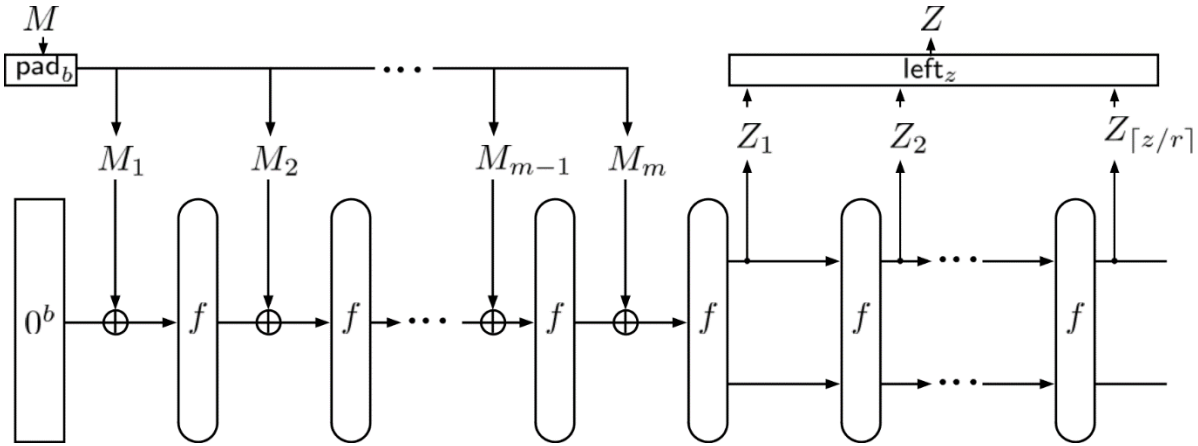


$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, \ell, \mu) \leq \frac{\mu N}{2^{|K|}}$$

- Blockcipher trick [ADMV 15] → secret perm.

Security of FKS

Mennink, Reyhanitabar, Vizár 2015



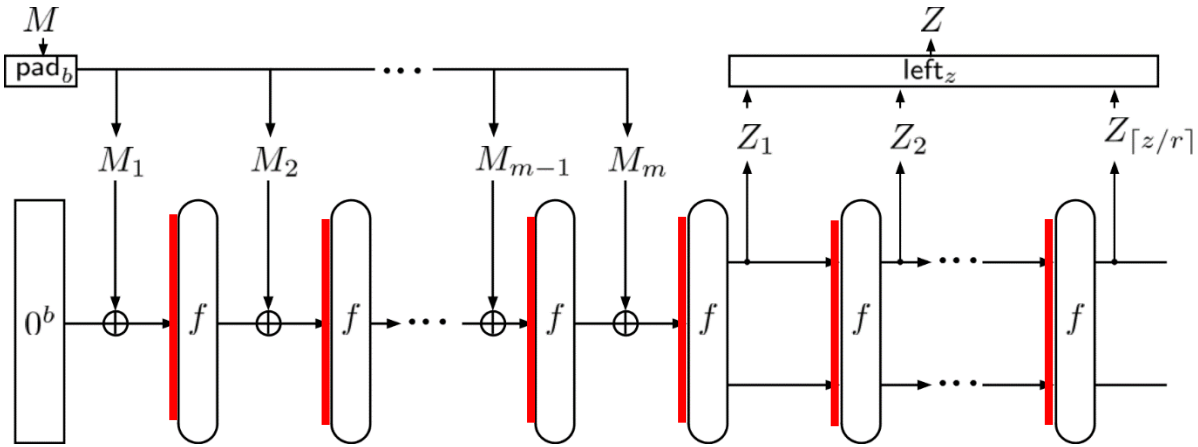
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, \ell, \mu) \leq \frac{\mu N}{2^{|K|}} + \frac{(q\ell)^2}{2^b}$$

- Blockcipher trick [ADMV 15] → secret perm.
- Secret perm. → secret function

Security of FKS

Mennink, Reyhanitabar, Vizár 2015

Only 2 states per query w/ Pr[coll]=2^{-c}



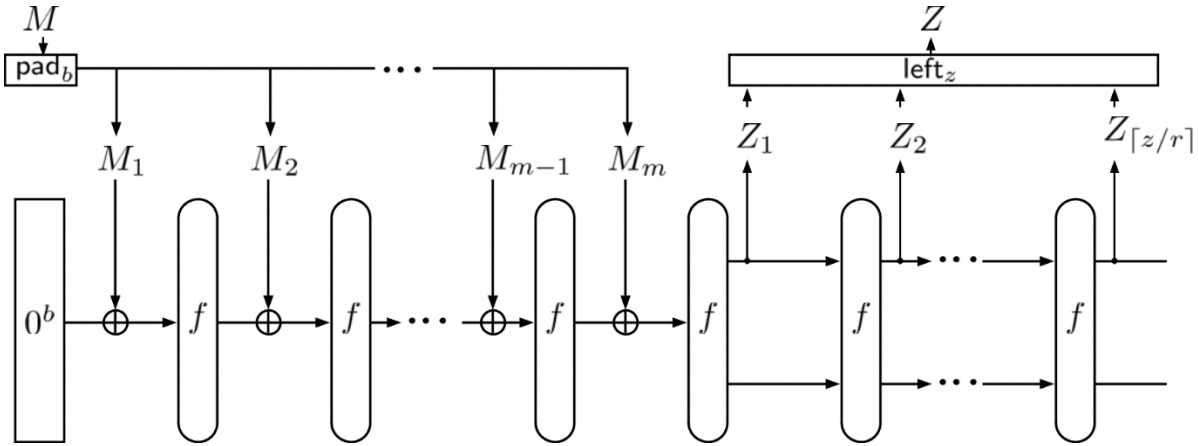
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, \ell, \mu) \leq \frac{\mu N}{2^{|K|}} + \frac{2(q\ell)^2}{2^b} + \frac{2q^2\ell}{2^c}$$

- Blockcipher trick [ADMV 15] → secret perm.
- Secret perm. → secret function
- **New analysis:** No internal collision => perfect security

Security of FKS

Mennink, Reyhanitabar, Vizár 2015

Main contribution:
Full state
Improved bound (for variable output len.)



$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, \ell, \mu) \leq \frac{\mu N}{2^{|K|}} + \frac{2(q\ell)^2}{2^b} + \frac{2q^2\ell}{2^c}$$

- Blockcipher trick [ADMV 15] → secret perm.
- Secret perm. → secret function
- **New analysis:** No internal collision => perfect security

$$N \approx 2^{|K|}/\mu \quad \text{if } (q\ell) \ll 2^{b/2} \text{ and } q^2\ell \ll 2^c$$

Improved security of outer keyed sponge

Naito, Yasuda 2016

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(q, N, \ell) \approx \frac{q^2+qN}{2^c} + \frac{\ell^2 q^2+qN+N}{2^b} + \lambda(N) \qquad \text{if } c \leq b/2$$

- Analysis of IKS and OKS
  - Variable length output ☺
- No full-state absorption ☹

Improved security of outer keyed sponge

Naito, Yasuda 2016

From Gaži et al. 2015

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(q, N, \ell) \approx \frac{q^2+qN}{2^c} + \frac{\ell^2 q^2+qN+N}{2^b} + \lambda(N) \qquad \text{if } c \leq b/2$$

- Analysis of IKS and OKS
  - Variable length output ☺
- No full-state absorption ☹

Improved security of outer keyed sponge

Naito, Yasuda 2016

From Gaži et al. 2015

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(q, N, \ell) \approx \frac{q^2+qN}{2^c} + \frac{\ell^2 q^2+qN+N}{2^b} + \lambda(N) \qquad \text{if } c \leq b/2$$

$$N \approx \min\left(2^c/q, 2^{|K|/2}\right) \qquad \text{if } \ell q \ll 2^{b/2} \text{ and } q^2 \ll 2^c$$

- Analysis of IKS and OKS
  - Variable length output ☺
- No full-state absorption ☹

Improved security of outer keyed sponge

Naito, Yasuda 2016

Main contribution:
Improved bound
(in corner-cases)

From Gaži et al. 2015

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{OKS}}(q, N, \ell) \approx \frac{q^2+qN}{2^c} + \frac{\ell^2 q^2+qN+N}{2^b} + \lambda(N) \qquad \text{if } c \leq b/2$$

$$N \approx \min\left(2^c/q, 2^{|K|/2}\right) \qquad \text{if } \ell q \ll 2^{b/2} \text{ and } q^2 \ll 2^c$$

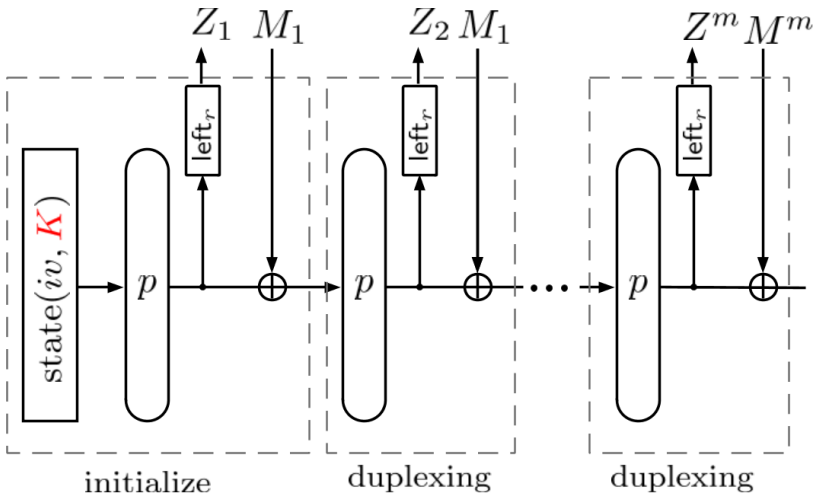
Gaži et al.:

$$N \approx \min\left(2^b/(q\ell), 2^c/q, 2^{|K|/2}\right) \qquad \text{if } q^2 \ll 2^c \text{ and } \ell q \ll 2^c$$

- Analysis of IKS and OKS
  - Variable length output ☺
- No full-state absorption ☹

Improved full-state keyed duplex

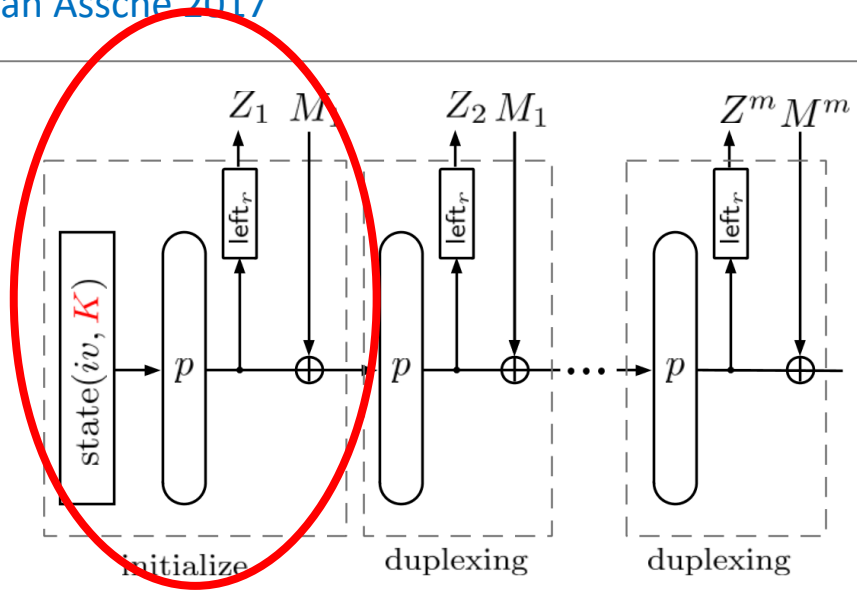
Daemen, Mennink, Van Assche 2017



- New definition of FKD
  - Init takes iv and inputblock
  - Commit to input block *before* seeing output

Improved full-state keyed duplex

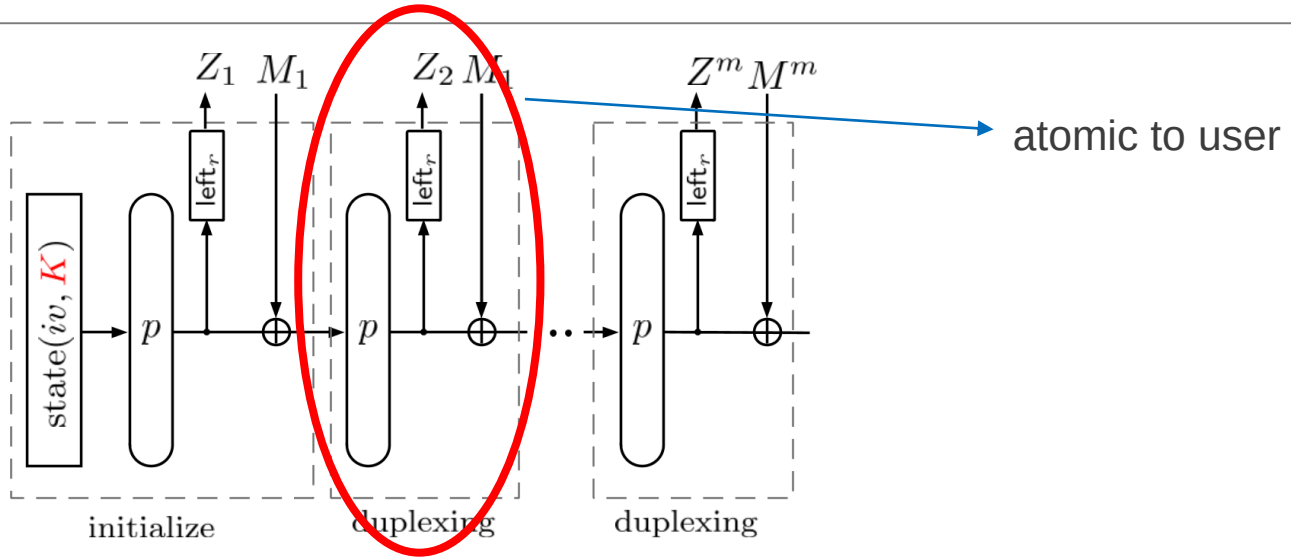
Daemen, Mennink, Van Assche 2017



- New definition of FKD
  - Init takes iv and inputblock
  - Commit to input block *before* seeing output

Improved full-state keyed duplex

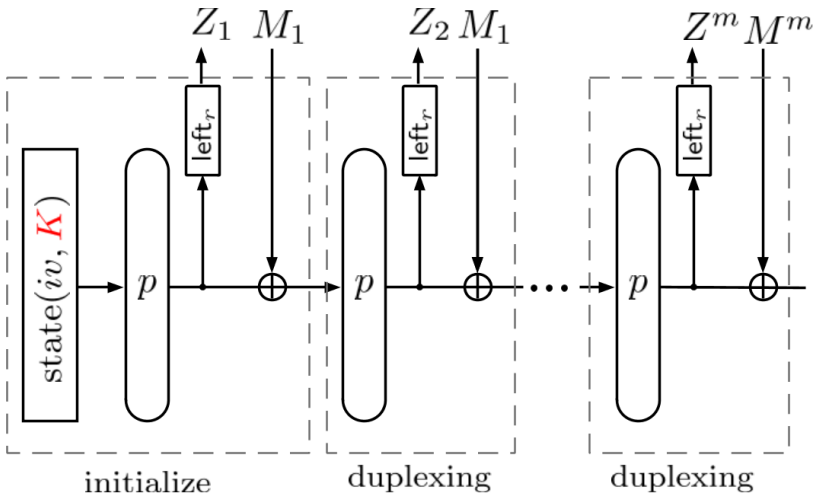
Daemen, Mennink, Van Assche 2017



- New definition of FKD
  - Init takes iv and inputblock
  - Commit to input block *before* seeing output

Improved full-state keyed duplex

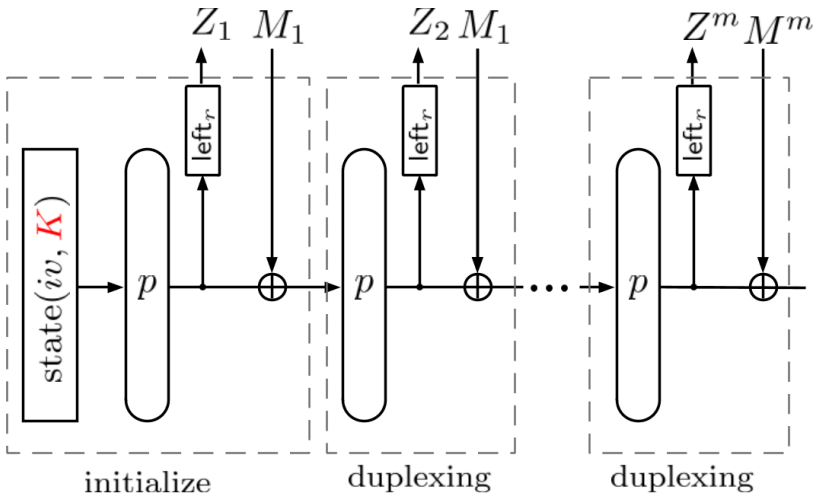
Daemen, Mennink, Van Assche 2017



- New definition of FKD
  - Init takes iv and inputblock
  - Commit to input block *before* seeing output
- Can simulate sponge!

Improved full-state keyed duplex

Daemen, Mennink, Van Assche 2017



- New definition of FKD
  - Init takes iv and inputblock
  - Commit to input block *before* seeing output
- Can simulate sponge!
- New resource: L = total #of inits with reused *iv*-s (i.e. q - #{uniq *iv*-s})

Improved FKS security (through FKD)

Daemen, Mennink, Van Assche 2017

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, M, L) \approx \frac{LN + L^2 + \mu(N)}{2^c} + \frac{N}{2^{|K|}} + \frac{qM}{2^{k+c-1}} + \frac{M^2}{2^b}$$

Improved FKS security (through FKD)

Daemen, Mennink, Van Assche 2017

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, M, L) \approx \frac{LN + L^2 + \mu(N)}{2^c} + \frac{N}{2^{|K|}} + \frac{qM}{2^{k+c-1}} + \frac{M^2}{2^b}$$

- Multi-collision limit $\mu(N)$: E[# states with r-collision]
  - $N/2$ if $r > 2\log_2(M)+c$ (large rate r)
  - $\approx NM/2^r$ otherwise (small rate r)

Improved FKS security (through FKD)

Daemen, Mennink, Van Assche 2017

Main contribution:
Improved bound
(Variable output, IKS only)

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, M, L) \approx \frac{LN+L^2+\mu(N)}{2^c} + \frac{N}{2^{|K|}} + \frac{qM}{2^{k+c-1}} + \frac{M^2}{2^b}$$

$$N \approx \min\left(2^c/L, 2^{|K|}\right) \quad \text{if } \ell q \ll 2^{b/2} \text{ and } q^2 \ll 2^c$$

- Multi-collision limit $\mu(N)$: E[# states with r-collision]
  - $N/2$ if $r > 2\log_2(M)+c$ (large rate r)
  - $\approx NM/2^r$ otherwise (small rate r)

Improved FKS security (through FKD)

Daemen, Mennink, Van Assche 2017

Main contribution:
Improved bound
(Variable output, IKS only)

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, M, L) \approx \frac{LN+L^2+\mu(N)}{2^c} + \frac{N}{2^{|K|}} + \frac{qM}{2^{k+c-1}} + \frac{M^2}{2^b}$$

$$N \approx \min\left(2^c/L, 2^{|K|}\right) \quad \text{if } \ell q \ll 2^{b/2} \text{ and } q^2 \ll 2^c$$

- Multi-collision limit $\mu(N)$: E[# states with r-collision]
  - $N/2$ if $r > 2\log_2(M)+c$ (large rate r)
  - $\approx NM/2^r$ otherwise (small rate r)
- Full state absorption, tight bound ☺

Improved FKS security (through FKD)

Daemen, Mennink, Van Assche 2017

Main contribution:
Improved bound
(Variable output, IKS only)

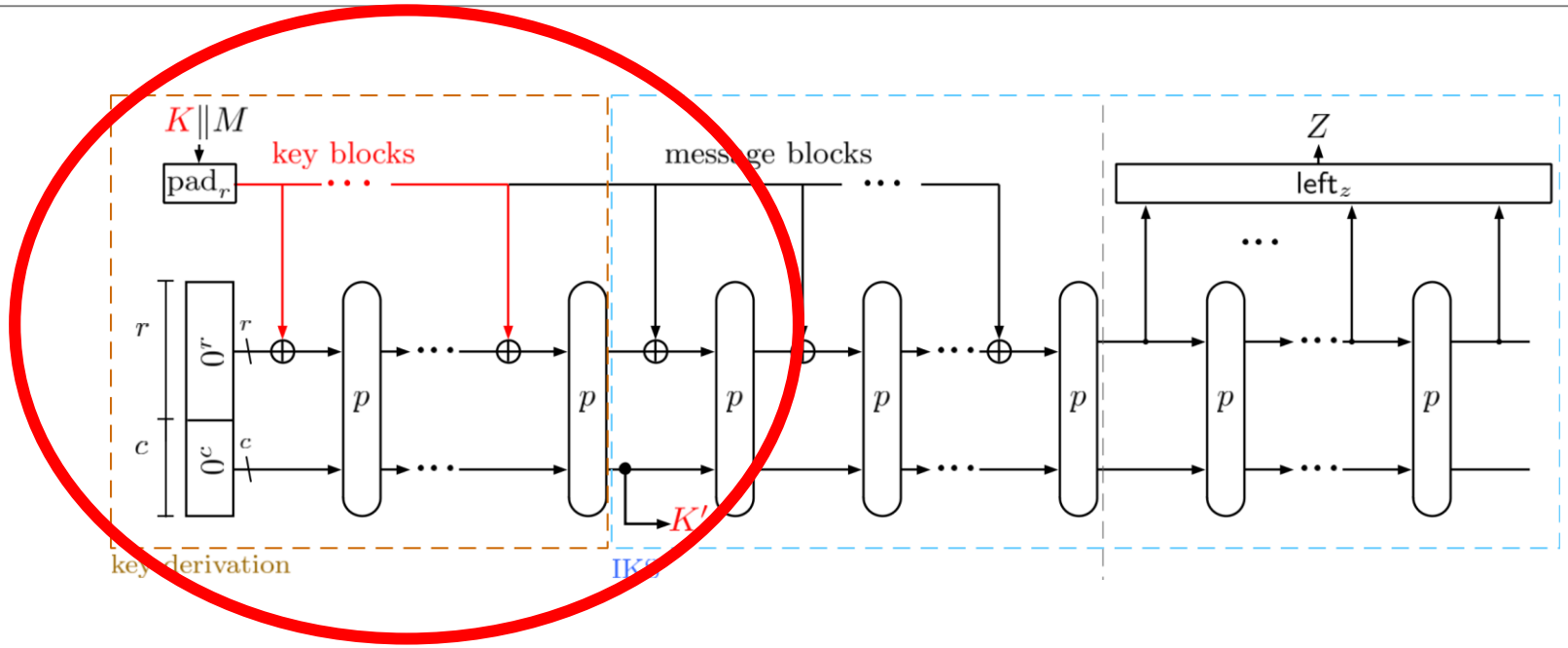
$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{FKS}}(q, N, M, L) \approx \frac{LN+L^2+\mu(N)}{2^c} + \frac{N}{2^{|K|}} + \frac{qM}{2^{k+c-1}} + \frac{M^2}{2^b}$$

$$N \approx \min\left(2^c/L, 2^{|K|}\right) \quad \text{if } \ell q \ll 2^{b/2} \text{ and } q^2 \ll 2^c$$

- Multi-collision limit $\mu(N)$: E[# states with r-collision]
  - $N/2$ if $r > 2\log_2(M)+c$ (large rate r)
  - $\approx NM/2^r$ otherwise (small rate r)
- Full state absorption, tight bound ☺
- Does not cover Outer keyed sponge 😐

Key prediction security

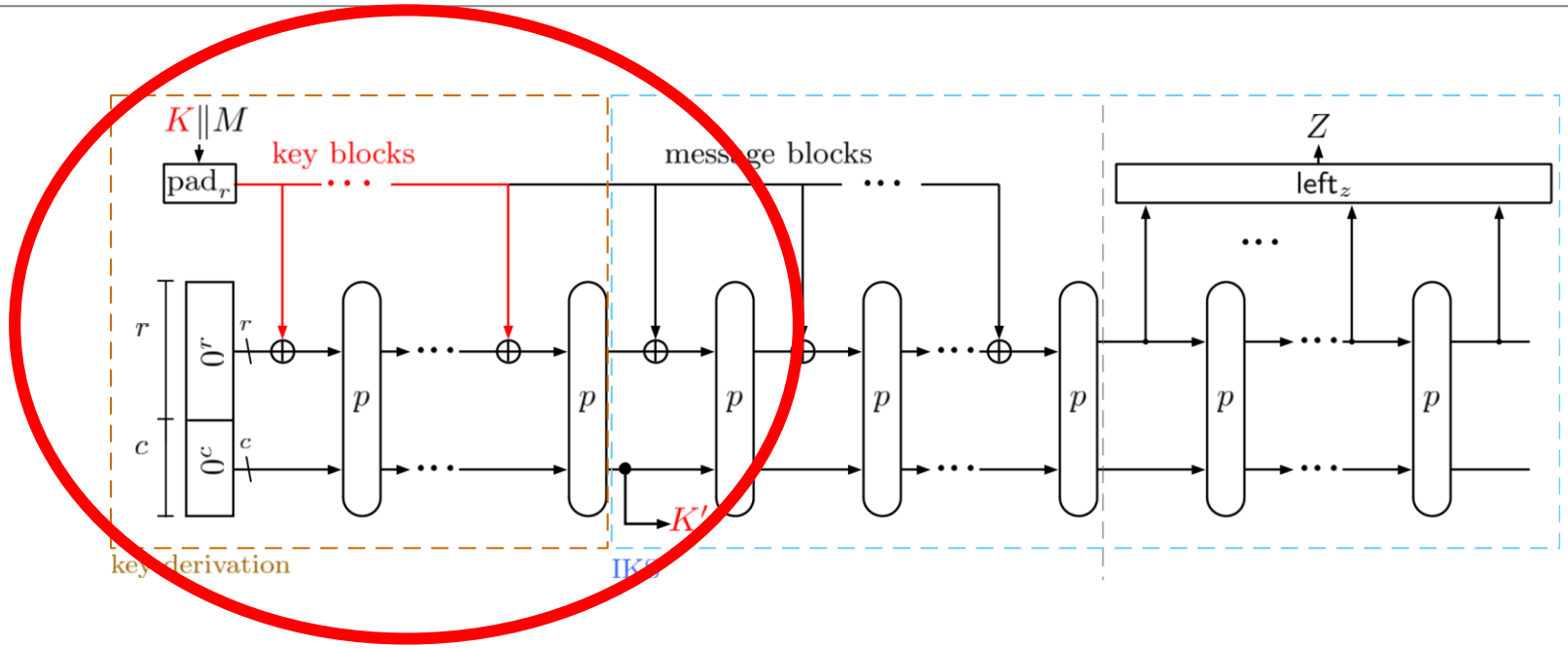
Mennink 2018



- Reconstructing key derivation vs |K|

Key prediction security

Mennink 2018

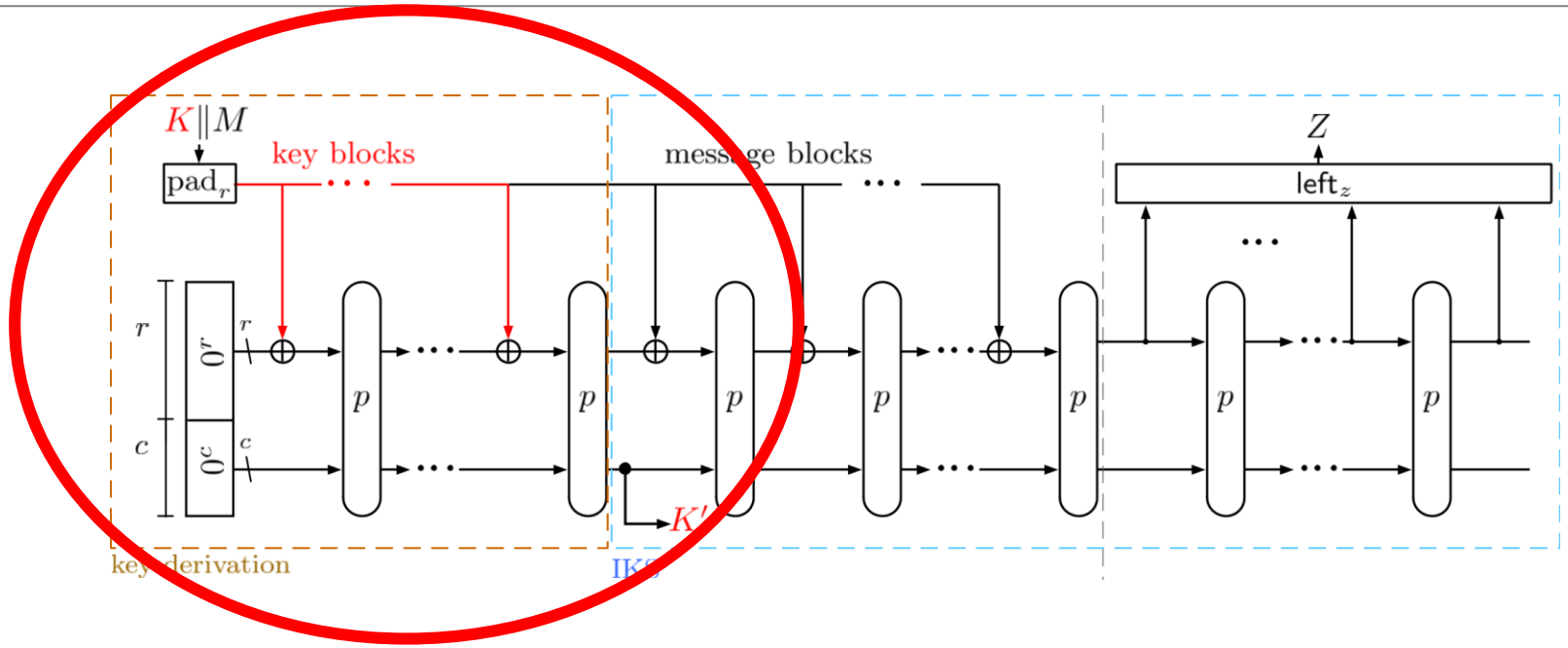


- Reconstructing key derivation vs |K|
- Previously: ≈ $\mathbf{2^{|K|/2}}$ (if |*K*| mod *r* ≠*0*) [GPT 15]

Key prediction security

Mennink 2018

Main contribution:
Improved bound
(OKS, last missing piece)



- Reconstructing key derivation vs |K|
- Previously: ≈ $2^{|K|/2}$ (if $|K|$ mod $r \neq 0$) [GPT 15]
- New result: ≈ $2^{|K|}$

Conclusion

The evolution of keyed sponge in a nutshell

With keyed sponge using a *b*-bit permutation, capacity *c*, rate *r=b-c*

- Before:
  - Only outer keying
  - Absorb data in *r*-bit blocks
  - Limit on data: $M \ll 2^{c/2}$
  - Security level: $\min(???), c - \log_2(M)$

Conclusion

The evolution of keyed sponge in a nutshell

With keyed sponge using a *b*-bit permutation, capacity *c*, rate *r=b-c*

- Before:
  - Only outer keying
  - Absorb data in *r*-bit blocks
  - Limit on data: $M \ll 2^{c/2}$
  - Security level: $\min(???), c - \log_2(M)$
- Today:
  - Both **outer and inner** keying
  - Absorb data using **full state**
  - Limit on data $\boldsymbol{M \ll 2^{b/2}}$
  - Security level: $\boldsymbol{min(|K|, b - log_2(M), c - log_2(L))}$

Conclusion

The evolution of keyed sponge in a nutshell

With keyed sponge using a *b*-bit permutation, capacity *c*, rate *r=b-c*

- Before:
  - Only outer keying
  - Absorb data in *r*-bit blocks
  - Limit on data: $M \ll 2^{c/2}$
  - Security level: $\min(???), c - \log_2(M)$

b=400, c=128, r=272, |K|=128

up to **2^{64} blocks**
at sec. level: **64**

- Today:
  - Both **outer and inner** keying
  - Absorb data using **full state**
  - Limit on data $\boldsymbol{M \ll 2^{b/2}}$
  - Security level: $\boldsymbol{min(|K|, b - log_2(M), c - log_2(L))}$

b=400, c=128, r=272, |K|=128

up to **2^{200} blocks** (if L=0)
at sec. level: **128**
save **≈1/3** of *p* evaluations

Thank you for your attention!

Follow us on

www.csem.ch