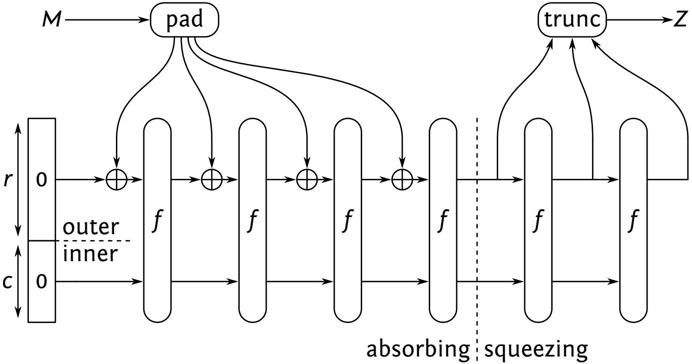
Security of Keyed Sponge Constructions Using a Modular Proof Approach

Elena Andreeva, Joan Daemen, Bart Mennink, Gilles Van Assche

KU Leuven, STMicroelectronics

Fast Software Encryption
March 10, 2015

Sponges



- Hashing
- Keyed applications

Keyed Sponges

Stream cipher encryption

- Squeezing $k = \text{Sponge}(K||\text{nonce})$
- Block-wise $k_i = \text{Sponge}(K||\text{nonce}||i)$

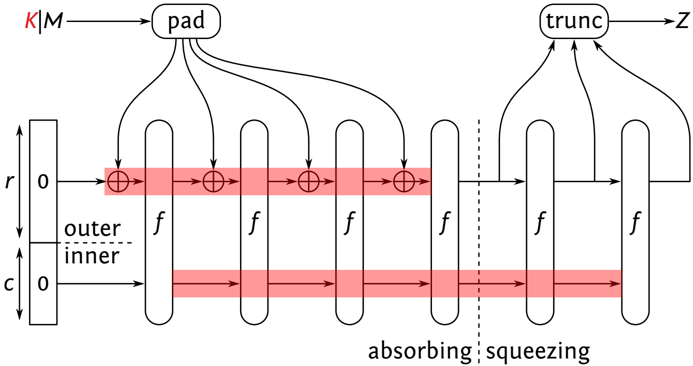
Authentication

- $\text{MAC} = \text{Sponge}(K||M)$

Authenticated encryption

- Duplexing the sponge

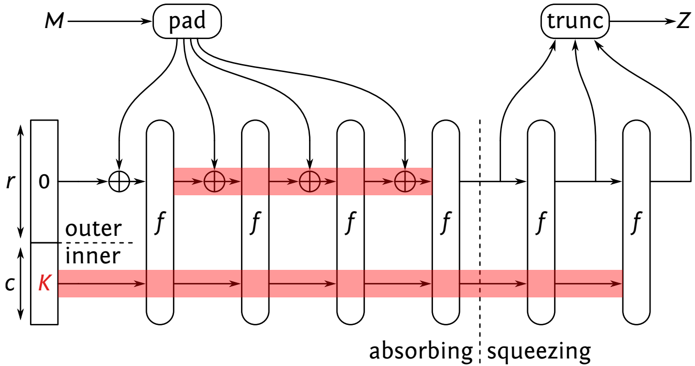
Outer-Keyed Sponge [BertoniDPV11]



$$\mathsf{OKS}^f_K(M) = \mathsf{Sponge}^f(K||M)$$

(K of length a multiple of r)

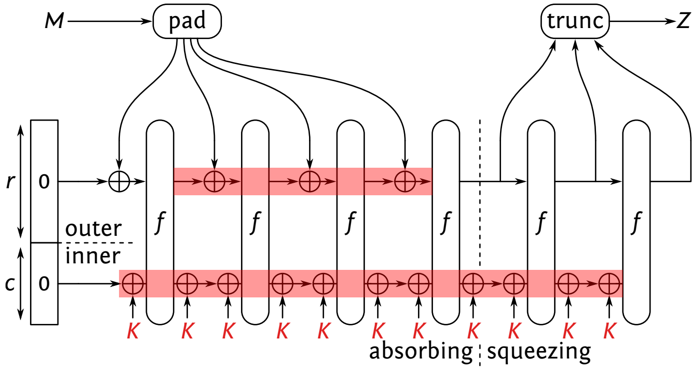
Inner-Keyed Sponge [ChangDHKN12]



$\mathsf{IKS}_{K}^{f}(M)$

(K of length c)

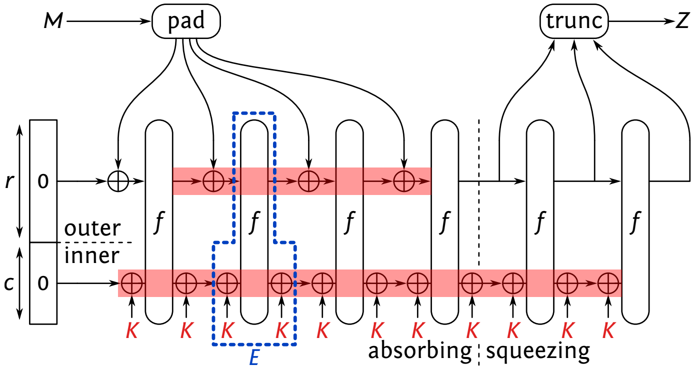
Inner-Keyed Sponge [ChangDHKN12]



$$\mathsf{IKS}^{f}_{K}(M)$$

(K of length c)

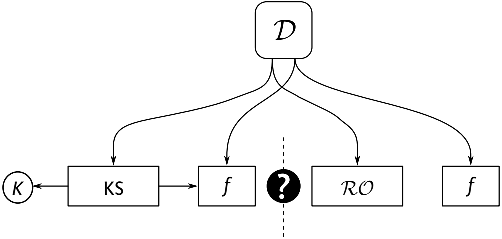
Inner-Keyed Sponge [ChangDHKN12]



$$\mathsf{IKS}_K^f(M) = \mathsf{Sponge}^{E_K^f}(M)$$

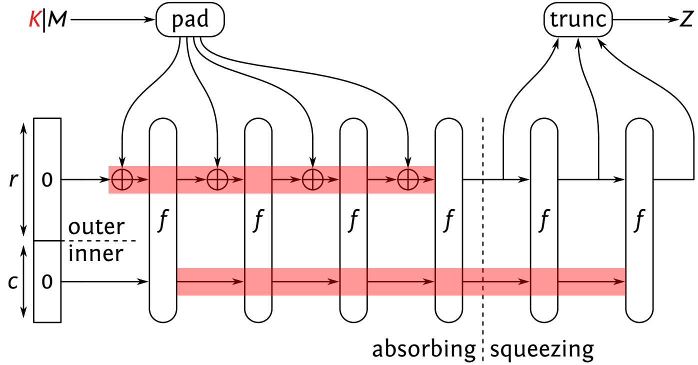
(K of length c)

Security Model



- M: online **data** complexity (blocks)
  - Calls to KS_K or $\mathcal{RO}$
- N: offline **time** complexity
  - Calls to f

Existing Distinguishing Bound [BertoniDPV11]



$$\mathbf{Adv}_{\mathsf{OKS}} \leq \frac{M^2}{2^{c+1}} + \frac{2MN}{2^c} + \frac{N}{2^k}$$

Existing Distinguishing Bound [BertoniDPV11]

Bad news

- Flaw in Lemma 1 of [BertoniDPV11]
- Easily fixable, but adds additional term

Existing Distinguishing Bound [BertoniDPV11]

Bad news

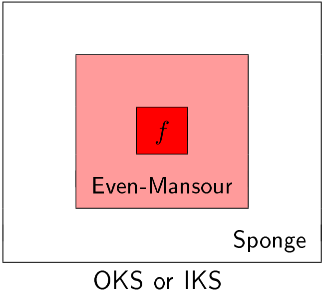
- Flaw in Lemma 1 of [BertoniDPV11]
- Easily fixable, but adds additional term

Good news

- Different proof approach leads to better results

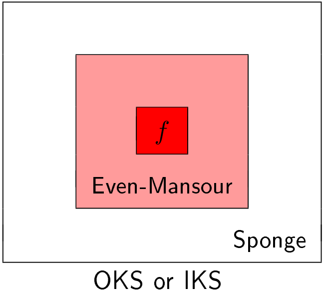
Modular Proof Approach

Proofs based on reduction to underlying primitives



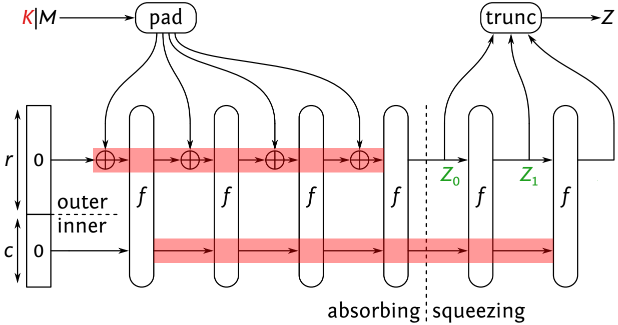
Modular Proof Approach

Proofs based on reduction to underlying primitives

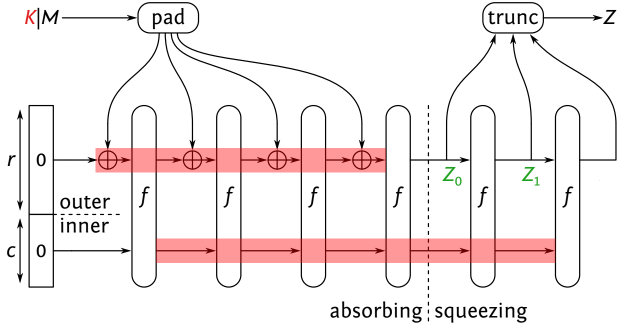


- Easier proofs
- Better bounds
- More general due to use of multiplicity

Multiplicity [BertoniDPV10]



Multiplicity [BertoniDPV10]



$$\mu_{\text{fw}} : \max_{Z_0} \text{ \# evaluations } f(Z_0||?) = (?||?)$$

$$\mu_{\text{bw}} : \max_{Z_1} \text{ \# evaluations } f(?||?) = (Z_1||?)$$

Multiplicity [BertoniDPV10]

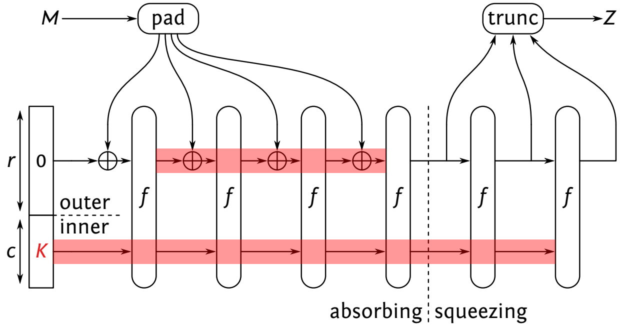
- Application to state recovery
  - Maximize probability of f-evaluation hitting state

Multiplicity [BertoniDPV10]

- Application to state recovery
  - Maximize probability of f-evaluation hitting state

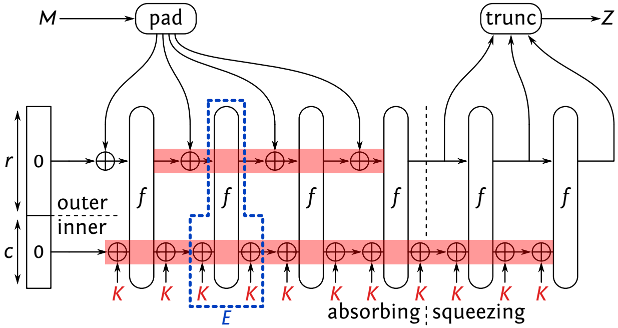
- $M/2^r \leq \mu_{\text{fw}}, \mu_{\text{bw}} \leq M$
  - General case: close to M
  - Constrained case (unique nonce): close to $M/2^r$

Inner-Keyed Sponge



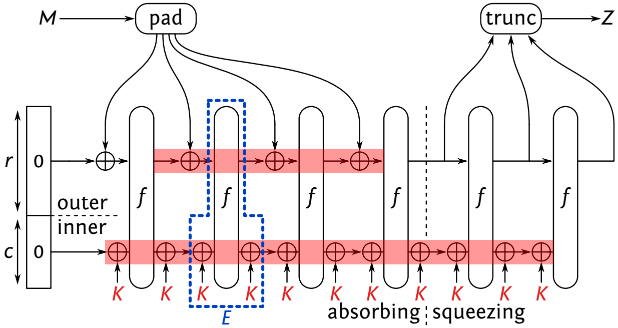
$$\mathbf{Adv}_{\mathsf{IKS}} = \Delta(\mathsf{IKS}_K^f, f; \mathcal{RO}, f)$$

Inner-Keyed Sponge



$$\mathbf{Adv}_{\mathsf{IKS}} = \Delta(\mathsf{IKS}_{K}^{f}, f; \mathcal{RO}, f)$$
$$= \Delta(\mathsf{Sponge}^{E_{K}^{f}}, f; \mathcal{RO}, f)$$

Inner-Keyed Sponge



$$
\begin{aligned}
\mathbf{Adv}_{\mathsf{IKS}} &= \Delta(\mathsf{IKS}^{f}_{K}, f; \mathcal{RO}, f) \\
&= \Delta(\mathsf{Sponge}^{E^{f}_{K}}, f; \mathcal{RO}, f) \\
&\leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{K}, f; \pi, f)
\end{aligned}
$$

Inner-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{IKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E_K^f, f; \pi, f)$$

Inner-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{IKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E_K^f, f; \pi, f)$$

$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f)$

- Independent of f
- Indifferentiability bound of sponge

Inner-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{IKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E_K^f, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Independent of f
- Indifferentiability bound of sponge

Inner-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{IKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E_K^f, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Independent of f
- Indifferentiability bound of sponge

$$\Delta(E_K^f, f; \pi, f)$$

- PRP-security of Even-Mansour with c-bit key
- Proof more general due to multiplicity

Inner-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{IKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E_K^f, f; \pi, f)$$

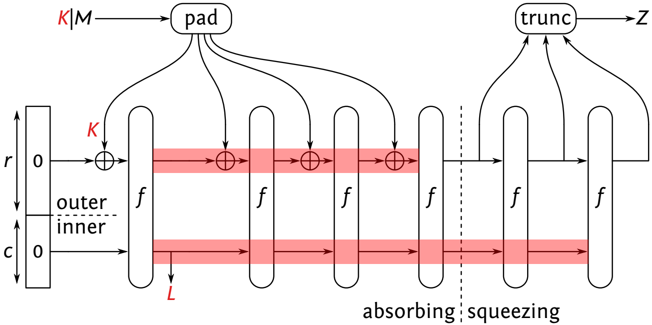
$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Independent of f
- Indifferentiability bound of sponge

$$\Delta(E_K^f, f; \pi, f) \leq \frac{(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c}$$

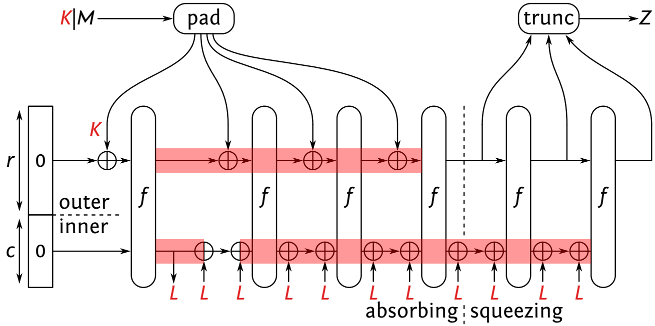
- PRP-security of Even-Mansour with c-bit key
- Proof more general due to multiplicity

Outer-Keyed Sponge



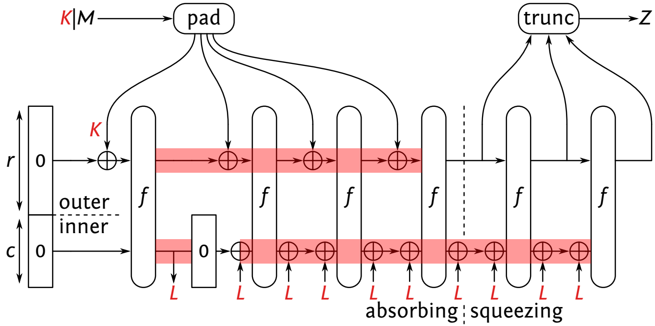
$$\mathbf{Adv}_{\mathsf{OKS}} = \Delta(\mathsf{OKS}_K^f, f; \mathcal{RO}, f)$$

Outer-Keyed Sponge



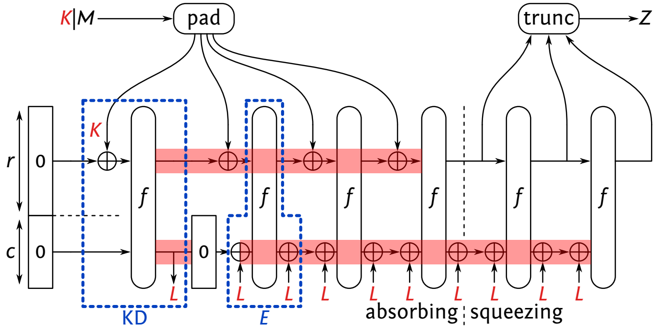
$$\mathbf{Adv}_{\mathsf{OKS}} = \Delta(\mathsf{OKS}_K^f, f; \mathcal{RO}, f)$$

Outer-Keyed Sponge



$$\mathbf{Adv}_{\mathsf{OKS}} = \Delta(\mathsf{OKS}_K^f, f; \mathcal{RO}, f)$$

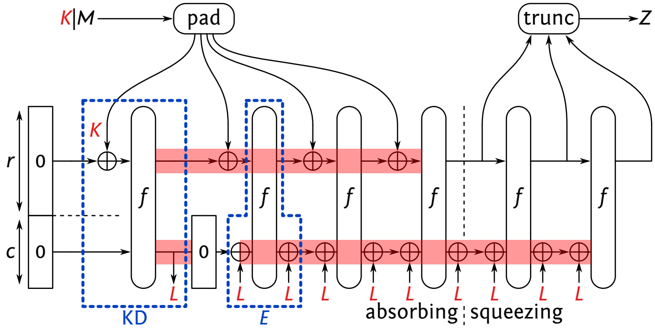
Outer-Keyed Sponge



$$\mathbf{Adv}_{\mathsf{OKS}} = \Delta(\mathsf{OKS}^f_K, f; \mathcal{RO}, f)$$

$$= \Delta(\mathsf{Sponge}^{E^f_{L=\mathsf{KD}^f(K)}}, f; \mathcal{RO}, f)$$

Outer-Keyed Sponge



$$\mathbf{Adv}_{\mathsf{OKS}} = \Delta(\mathsf{OKS}^f_K, f; \mathcal{RO}, f)$$
$$= \Delta(\mathsf{Sponge}^{E^f_{L=\mathsf{KD}^f(K)}}, f; \mathcal{RO}, f)$$
$$\leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^f_{L=\mathsf{KD}^f(K)}, f; \pi, f)$$

Outer-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{OKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{L=\mathsf{KD}^{f}(K)}, f; \pi, f)$$

Outer-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{OKS}} \le \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{L=\mathsf{KD}^f(K)}, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \le \frac{M^2}{2^c}$$

- Indifferentiability bound of sponge

Outer-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{OKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{L=\mathsf{KD}^{f}(K)}, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Indifferentiability bound of sponge

$$\Delta(E^{f}_{L=\mathsf{KD}^{f}(K)}, f; \pi, f)$$

- PRP-security of Even-Mansour with c-bit subkey
- Analysis more technical

Outer-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{OKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{L=\mathsf{KD}^f(K)}, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Indifferentiability bound of sponge

$$\Delta(E^{f}_{L=\mathsf{KD}^f(K)}, f; \pi, f) \leq \frac{2(\mu_{\text{fw}} + \mu_{\text{bw}})N}{2^c}$$

- PRP-security of Even-Mansour with c-bit subkey
- Analysis more technical
  - If all calls to f in $\mathsf{KD}^f(K)$ unique (term 1)

Outer-Keyed Sponge

$$\mathbf{Adv}_{\mathsf{OKS}} \leq \Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) + \Delta(E^{f}_{L=\mathsf{KD}^f(K)}, f; \pi, f)$$

$$\Delta(\mathsf{Sponge}^{\pi}, f; \mathcal{RO}, f) \leq \frac{M^2}{2^c}$$

- Indifferentiability bound of sponge

$$\Delta(E^{f}_{L=\mathsf{KD}^f(K)}, f; \pi, f) \leq \frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} + \frac{N}{2^k} + \frac{2(k/r)N}{2^{r+c}}$$

- PRP-security of Even-Mansour with c-bit subkey
- Analysis more technical
  - If all calls to f in $\mathsf{KD}^f(K)$ unique (term 1)
  - Probability an f-call in $\mathsf{KD}^f(K)$ collides (rest)

Interpretation

- Dominating term:

$$\mathbf{Adv}(M, \mu_{\mathrm{fw}}, \mu_{\mathrm{bw}}, N) \leq \frac{M^2}{2^c} + \frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} + \frac{N}{2^k}$$

Interpretation

- Dominating term:

$$\mathbf{Adv}(M, \mu_{\mathrm{fw}}, \mu_{\mathrm{bw}}, N) \leq \frac{M^2}{2^c} + \frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} + \frac{N}{2^k}$$

Limited data complexity $\begin{cases} M \leq 2^{\alpha} \\ \mu_{\mathrm{fw}} + \mu_{\mathrm{bw}} \leq 2^{\beta} \end{cases}$

Interpretation

- Dominating term:

$$\mathbf{Adv}(M, \mu_{\text{fw}}, \mu_{\text{bw}}, N) \leq \frac{M^2}{2^c} + \frac{2(\mu_{\text{fw}} + \mu_{\text{bw}})N}{2^c} + \frac{N}{2^k}$$

Limited data complexity $\begin{cases} M \leq 2^{\alpha} \\ \mu_{\text{fw}} + \mu_{\text{bw}} \leq 2^{\beta} \end{cases}$

$$\Downarrow$$

Time complexity is $\min\{2^{c-\beta-1}, 2^k\}$

Interpretation

$$\frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} \leq \frac{2(\mu_{\mathrm{fw}}^* + \mu_{\mathrm{bw}}^*)N}{2^c} + \Pr\left(\mu_{\mathrm{fw}} > \mu_{\mathrm{fw}}^*\right) + \Pr\left(\mu_{\mathrm{bw}} > \mu_{\mathrm{bw}}^*\right)$$

Interpretation

$$\frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} \le \frac{2(\mu^*_{\mathrm{fw}} + \mu^*_{\mathrm{bw}})N}{2^c} + \Pr\left(\mu_{\mathrm{fw}} > \mu^*_{\mathrm{fw}}\right) + \Pr\left(\mu_{\mathrm{bw}} > \mu^*_{\mathrm{bw}}\right)$$

General case

- μ_{fw} may be up to M (adversary has full control)
- μ_{bw} at most $\mathrm{const} \cdot \max\{1, M/2^r\}$
  - except with small probability

Interpretation

$$\frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} \leq \frac{2(\mu_{\mathrm{fw}}^* + \mu_{\mathrm{bw}}^*)N}{2^c} + \Pr\left(\mu_{\mathrm{fw}} > \mu_{\mathrm{fw}}^*\right) + \Pr\left(\mu_{\mathrm{bw}} > \mu_{\mathrm{bw}}^*\right)$$

General case

- μ_{fw} may be up to M (adversary has full control)
- μ_{bw} at most $\mathrm{const} \cdot \max\{1, M/2^r\}$
  - except with small probability
- Time complexity $\approx \min\{2^{c-\alpha-1}, 2^k\}$ if $M \leq 2^\alpha$

Interpretation

$$\frac{2(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c} \le \frac{2(\mu^*_{\mathrm{fw}} + \mu^*_{\mathrm{bw}})N}{2^c} + \Pr\left(\mu_{\mathrm{fw}} > \mu^*_{\mathrm{fw}}\right) + \Pr\left(\mu_{\mathrm{bw}} > \mu^*_{\mathrm{bw}}\right)$$

General case

- μ_{fw} may be up to M (adversary has full control)
- μ_{bw} at most $\mathrm{const} \cdot \max\{1, M/2^r\}$
  - except with small probability
- Time complexity $\approx \min\{2^{c-\alpha-1}, 2^k\}$ if $M \le 2^\alpha$

Constrained case

- $\mu_{\mathrm{fw}}, \mu_{\mathrm{bw}}$ both at most $\mathrm{const} \cdot \max\{1, M/2^r\}$
  - except with small probability

Interpretation

$$\frac{2(\mu_{\text{fw}} + \mu_{\text{bw}})N}{2^c} \leq \frac{2(\mu^*_{\text{fw}} + \mu^*_{\text{bw}})N}{2^c} + \Pr\left(\mu_{\text{fw}} > \mu^*_{\text{fw}}\right) + \Pr\left(\mu_{\text{bw}} > \mu^*_{\text{bw}}\right)$$

General case

- μ_{fw} may be up to M (adversary has full control)
- μ_{bw} at most $\text{const} \cdot \max\{1, M/2^r\}$
  - except with small probability
- Time complexity $\approx \min\{2^{c-\alpha-1}, 2^k\}$ if $M \leq 2^\alpha$

Constrained case

- $\mu_{\text{fw}}, \mu_{\text{bw}}$ both at most $\text{const} \cdot \max\{1, M/2^r\}$
  - except with small probability
- Time complexity $\approx \min\{2^{c-2}, 2^{r+c-\alpha-2}, 2^k\}$ if $M \leq 2^\alpha$

Interpretation (Ignoring 2^k Term)

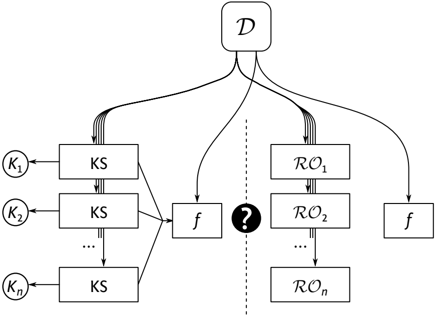
rate	capacity	data complexity	case	time complexity
r	c	$\leq 2^{\alpha}$	general	$2^{c-\alpha-1}$
			constrained	$\min\{2^{c-2}, 2^{r+c-\alpha-2}\}$
40	160	$\leq 2^{79}$	general	2^{80}
			constrained	2^{119}
548	252	$\leq 2^{123}$	general	2^{128}
			constrained	2^{250}

Multi-Target Security

- System with n independent keys
- Damage if any instance is broken

Multi-Target Security

- System with n independent keys
- Damage if any instance is broken



- $M = \sum_h M_h$: online **data** complexity (blocks)
- N: offline **time** complexity

Consequences for Bounds

- Technicalities for multi-target (subkey) Even-Mansour

Consequences for Bounds

- Technicalities for multi-target (subkey) Even-Mansour
- Cross-sponge inner collisions

$$\sum_{h} \frac{M_h^2}{2^c} + \sum_{h \neq h'} \frac{2M_h M_{h'}}{2^c} = \frac{M^2}{2^c}$$

Consequences for Bounds

- Technicalities for multi-target (subkey) Even-Mansour
- Cross-sponge inner collisions

$$\sum_{h} \frac{M_h^2}{2^c} + \sum_{h \neq h'} \frac{2 M_h M_{h'}}{2^c} = \frac{M^2}{2^c}$$

- Interpretation of multiplicity: over all n online accesses

$$\frac{(\mu_{\mathrm{fw}} + \mu_{\mathrm{bw}})N}{2^c}$$

Consequences for Bounds

- Technicalities for multi-target (subkey) Even-Mansour
- Cross-sponge inner collisions

$$\sum_{h} \frac{M_h^2}{2^c} + \sum_{h \neq h'} \frac{2M_h M_{h'}}{2^c} = \frac{M^2}{2^c}$$

- Interpretation of multiplicity: over all n online accesses

$$\frac{(\mu_{\text{fw}} + \mu_{\text{bw}})N}{2^c}$$

- Exhaustive key search speed-up

$$\frac{N}{2^k} \quad \longrightarrow \quad \frac{nN}{2^k}$$

Conclusion

Thanks for your attention!

Questions?