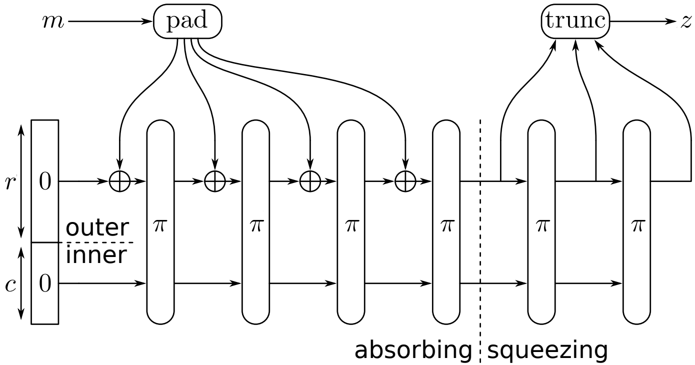
Key Prediction Security of Keyed Sponges

Bart Mennink
Radboud University (The Netherlands)

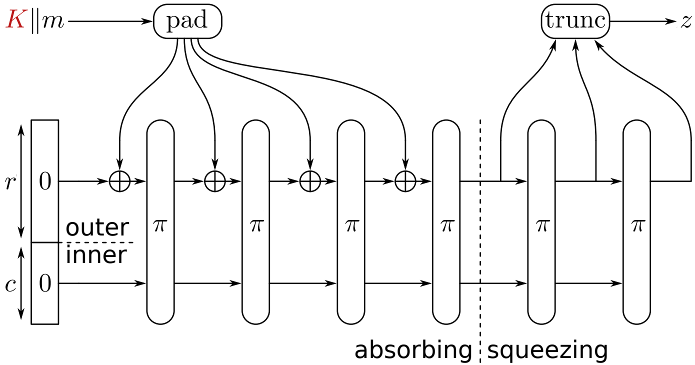
Fast Software Encryption 2019
March 26, 2019

Sponges [BDPV07]



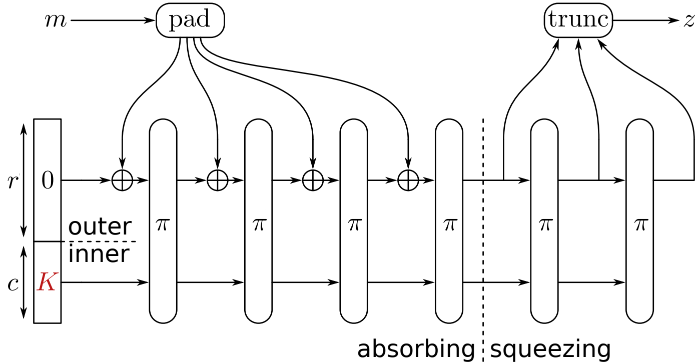
- Cryptographic hash function
- SHA-3, XOFs, lightweight hashing, . . .
- Behaves as RO up to query complexity $\approx 2^{c/2}$ [BDPV08]

Keyed Sponges



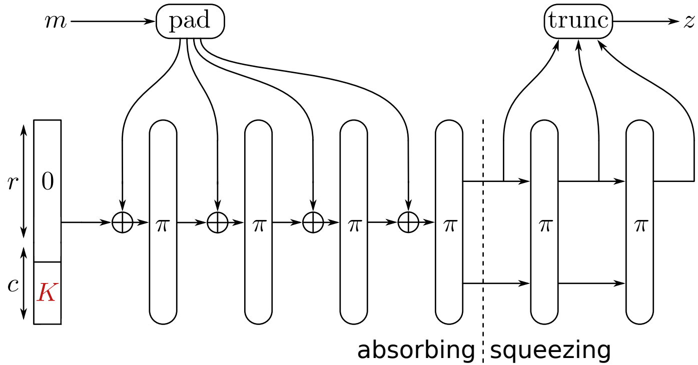
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16]

Keyed Sponges



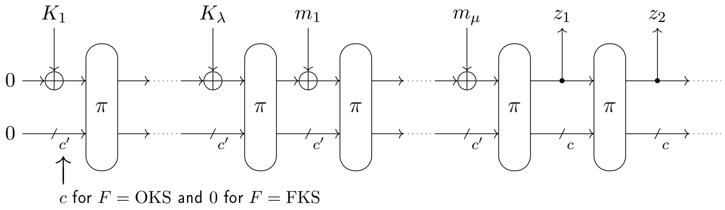
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]

Keyed Sponges



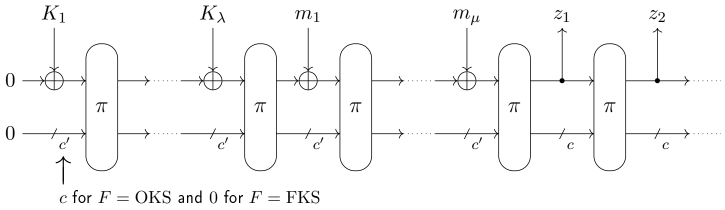
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]
- Full-Keyed Sponge [BDPV12,GPT15,MRV15]

Security of Keyed Sponge



- $F \in \{\text{OKS}, \text{FKS}\}$

Security of Keyed Sponge

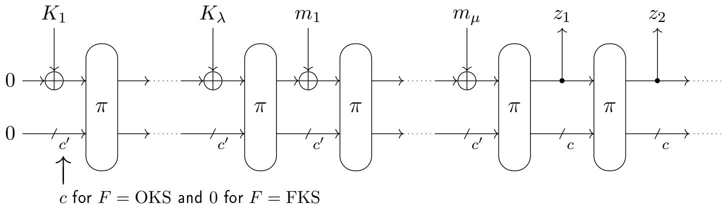


- $F \in \{\text{OKS}, \text{FKS}\}$
- M: data (construction) complexity
- N: time (primitive) complexity

Simplified Security Bound

$$\frac{M^2}{2^c} + \frac{MN}{2^c} + \mathbf{Adv}_F^{\text{key-pre}}(N)$$

Security of Keyed Sponge



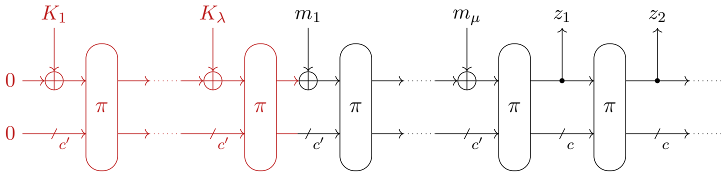
- $F \in \{\text{OKS}, \text{FKS}\}$
- M: data (construction) complexity
- N: time (primitive) complexity

Simplified Security Bound

$$\frac{M^2}{2^c} + \frac{MN}{2^c} + \mathbf{Adv}_F^{\text{key-pre}}(N)$$

probability that adversary predicts key

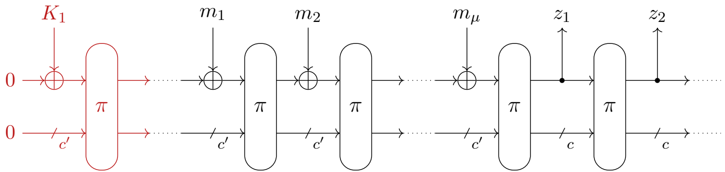
Key Prediction Security



$\mathbf{Adv}_F^{\text{key-pre}}(N)$

- Adversary makes N queries to π
- Key K randomly drawn
- Adversary wins if query history "covers K"

Key Prediction Security: Existing Bounds

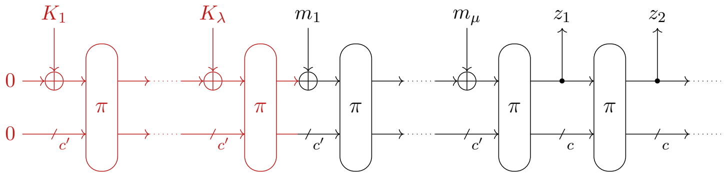


One Key Block

- Adversary makes N queries
- Query history covers at most N keys

$$\mathbf{Adv}_F^{\text{key-pre}}(N) \leq \frac{N}{2^k}$$

Key Prediction Security: Existing Bounds



One Key Block

- Adversary makes N queries
- Query history covers at most N keys

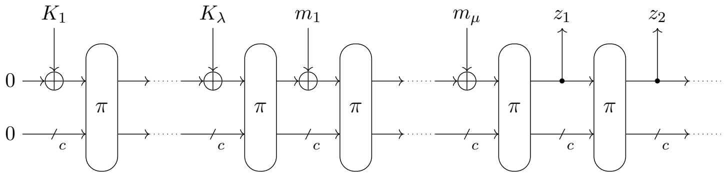
$$\mathbf{Adv}_F^{\text{key-pre}}(N) \le \frac{N}{2^k}$$

More Than One Key Block

- By Gaži et al. [GPT15]
- Used in many sponge proofs

$$\mathbf{Adv}_F^{\text{key-pre}}(N) \lesssim \frac{b^\lambda N}{2^{k/2}}$$

Key Prediction Security: Implication for OKS



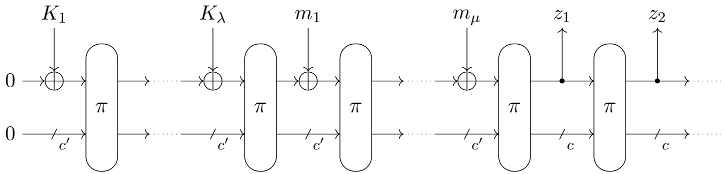
Case of $(b, c, r, k) = (320, 256, 64, 64)$

$$\frac{M^2}{2^c} + \frac{MN}{2^c} + \frac{N}{2^k} = \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{64}}$$

Case of $(b, c, r, k) = (320, 256, 64, 128)$

$$\frac{M^2}{2^c} + \frac{MN}{2^c} + \frac{N}{2^{k/2}} = \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{64}}$$

New Analysis

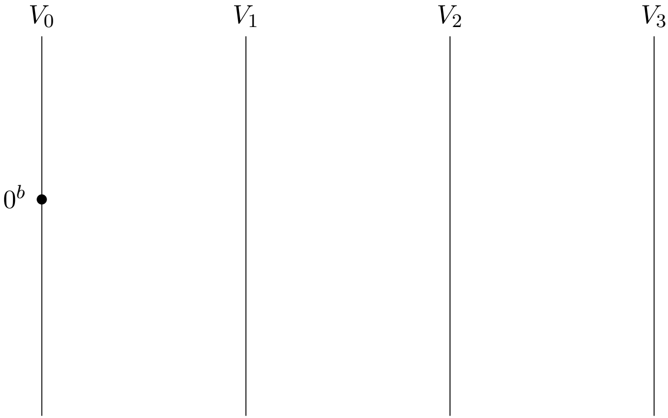


$$\mathbf{Adv}_F^{\text{key-pre}}(N) \lesssim \frac{c^{\lambda-1}N}{2^k}$$

- Loss c due to lucky multi-collisions (in old bound: b)
- 2^k in denominator (in old bound: $2^{k/2}$)
- Best attack: around 2^k queries

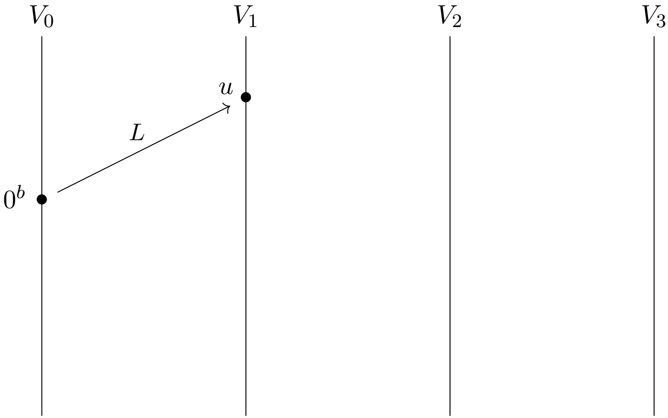
Proof Idea

- Tree-based approach (as in [GPT15])



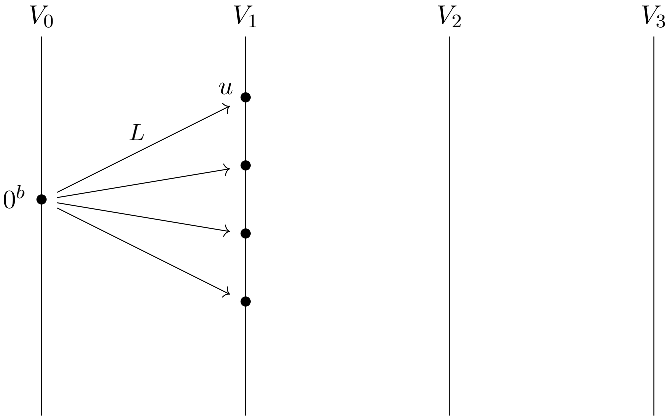
Proof Idea

- Tree-based approach (as in [GPT15])



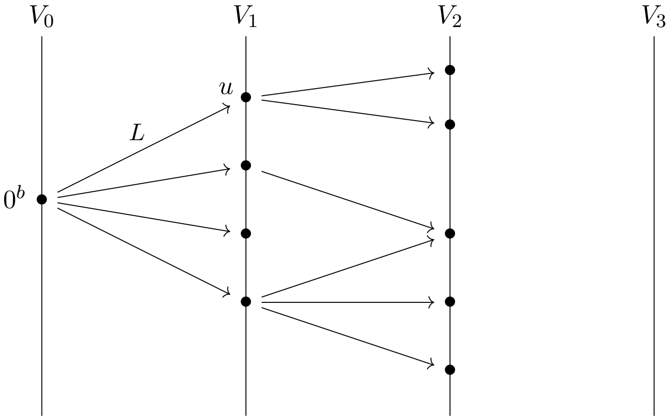
Proof Idea

- Tree-based approach (as in [GPT15])



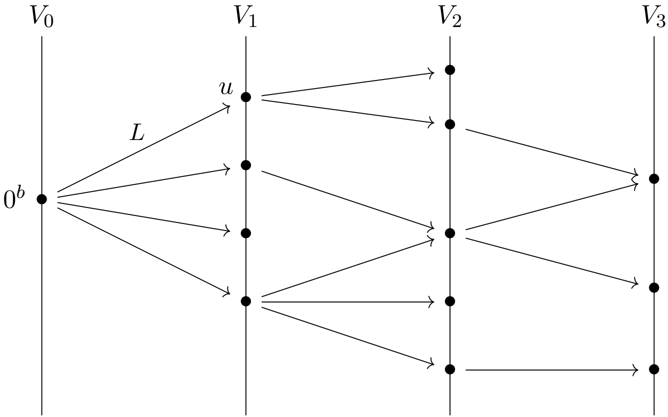
Proof Idea

- Tree-based approach (as in [GPT15])



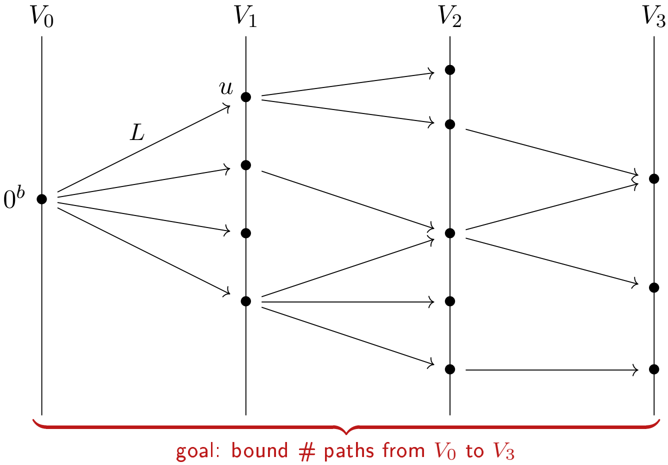
Proof Idea

- Tree-based approach (as in [GPT15])



Proof Idea

- Tree-based approach (as in [GPT15])

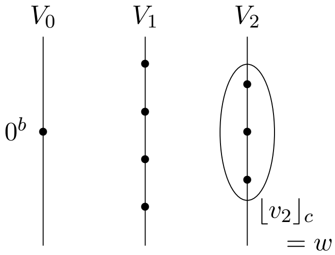


Proof Idea

- Fix any query from V_2 to V_3: N options

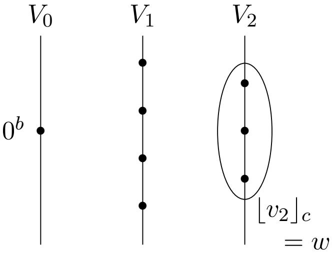
Proof Idea

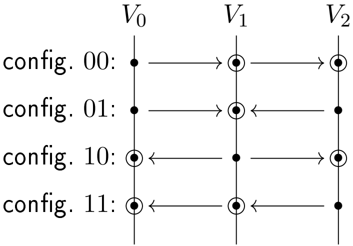
- Fix any query from V_2 to V_3: N options
- This query fixes inner part of second-last layer



Proof Idea

- Fix any query from V_2 to V_3: N options
- This query fixes inner part of second-last layer

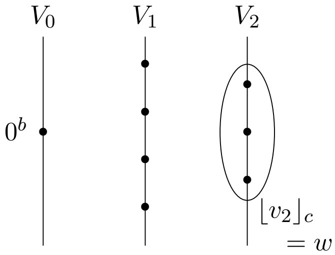


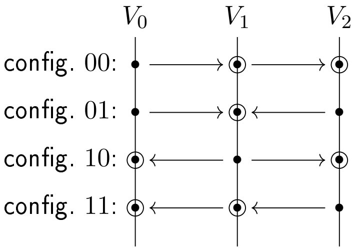


- Consider configurations for these layers
  - Arrows indicate query direction, circles indicate inner collisions

Proof Idea

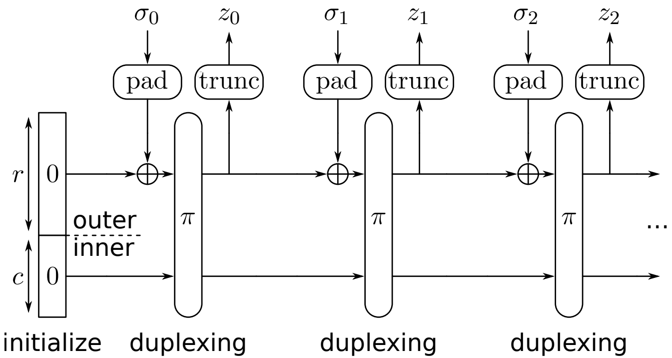
- Fix any query from V_2 to V_3: N options
- This query fixes inner part of second-last layer





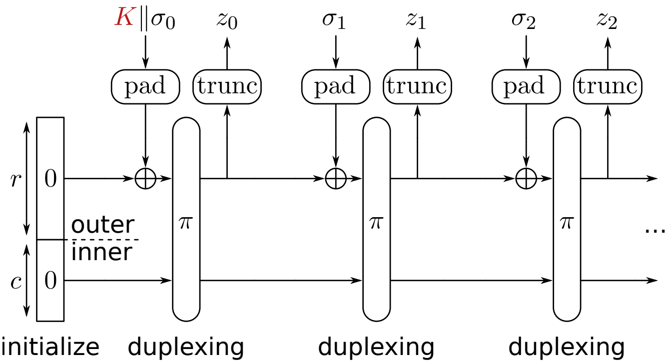
- Consider configurations for these layers
  - Arrows indicate query direction, circles indicate inner collisions
- Inductive reasoning on non-occurrence of α^i-fold collisions

Further Application to Duplex



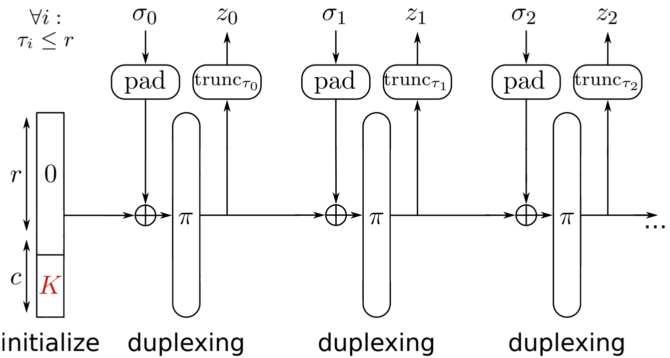
- Unkeyed Duplex [BDPV11]

Further Application to Duplex



- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]

Further Application to Duplex



- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]
- Full-Keyed Duplex [MRV15,DMV17]

Application to Duplex

Bounds Reduce Bi-Directionally [MRV15,DMV17]

$$\text{OKS and OKD:} \qquad \frac{M^2}{2^c} + \frac{MN}{2^c} + \mathbf{Adv}^{\text{key-pre}}_{\text{OKS}}(N)$$

$$\text{FKS and FKD:} \qquad \frac{M^2}{2^c} + \frac{MN}{2^c} + \mathbf{Adv}^{\text{key-pre}}_{\text{FKS}}(N)$$

Same for Nonce-Respecting Setting [JLM14,DMV17]

$$\text{OKS and OKD:} \qquad \frac{M^2}{2^b} + \frac{N}{2^c} + \mathbf{Adv}^{\text{key-pre}}_{\text{OKS}}(N)$$

$$\text{FKS and FKD:} \qquad \frac{M^2}{2^b} + \frac{N}{2^c} + \mathbf{Adv}^{\text{key-pre}}_{\text{FKS}}(N)$$

Application to CAESAR

CAESAR Competition

- Four third-round candidates based on duplex

scheme	b	c	r	k
Ascon [DEMS16]	320	256	64	128
	320	192	128	128
Ketje [BDP+16]	200	184	16	92
	400	368	32	128
Keyak [BDP+16]	800	256	544	128..224
	1600	256	1344	128..224
NORX [AJN16]	512	128	384	128
	1024	256	768	256

Application to CAESAR

CAESAR Competition

- Four third-round candidates based on duplex

scheme	b	c	r	k
Ascon [DEMS16]	320	256	64	128
	320	192	128	128
Ketje [BDP+16]	200	184	16	92
	400	368	32	128
Keyak [BDP+16]	800	256	544	128..224
	1600	256	1344	128..224
NORX [AJN16]	512	128	384	128
	1024	256	768	256

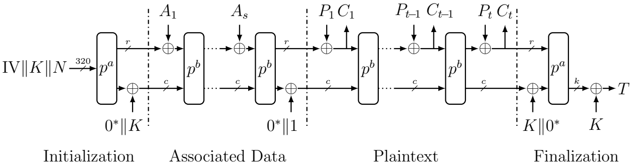
- Initialize entire state using key (FKS for key)

Application to CAESAR Portfolio: Ascon

Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1.2

1.4 Mode of Operation

The mode of operation of Ascon is based on duplex sponge modes like MonkeyDuplex [13], but uses a stronger keyed initialization and keyed finalization function. The core permutations p^a and p^b operate on a sponge state S of size 320 bits, with a rate of r bits and a capacity of $c = 320 - r$ bits. For a more convenient notation, the rate and capacity parts of the state S are denoted by S_r and S_c, respectively. The encryption and decryption operations are illustrated in Figure 1a and Figure 1b and specified in Algorithm 1.



(a) Encryption

Application to CAESAR Portfolio: Ascon-128 Parameters*

$(b, c, r, k) = (320, 256, 64, 128)$

Old Bound (Simplified)

$$\frac{M^2}{2^{320}} + \frac{N}{2^{256}} + \frac{N}{2^{64}}$$

- If $M \leq 2^{160}$, security as long as $N \leq 2^{64}$

New Bound (Simplified)

$$\frac{M^2}{2^{320}} + \frac{N}{2^{256}} + \frac{N}{2^{128}}$$

- If $M \leq 2^{160}$, security as long as $N \leq 2^{128}$

* Reasoning does not apply to Ascon-128 itself

Application to STROBE

STROBE Protocol Framework [Ham17]

- Lightweight framework for network protocols
- Goal: simple framework with small code size

Application to STROBE

STROBE Protocol Framework [Ham17]

- Lightweight framework for network protocols
- Goal: simple framework with small code size
- Hashing, authentication, and encryption:
  all using sponge and outer-keyed sponge/duplex

Application to STROBE

STROBE Protocol Framework [Ham17]

- Lightweight framework for network protocols
- Goal: simple framework with small code size
- Hashing, authentication, and encryption:
  all using sponge and outer-keyed sponge/duplex

scheme	b	c	r	k
STROBE-128/1600	1600	256	1344	256
STROBE-256/1600	1600	512	1088	256
STROBE-128/800	800	256	544	256
STROBE-256/800	800	512	288	256
STROBE-128/400	400	256	144	256

Application to STROBE-128/400

$(b, c, r, k) =$
$(400, 256, 144, 256)$

Old Bound (Simplified)

$$\frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{128}}$$

- If $M \leq 2^{100} =: 2^a$, security as long as $N \leq 2^{128}$

New Bound (Simplified)

$$\frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{256}}$$

- If $M \leq 2^{100} =: 2^a$, security as long as $N \leq 2^{156}$

Conclusion

Tight Key Prediction Security

- Last "missing link" in keyed sponge proofs
- Close to optimal bound

Applications

- Every use of outer-keyed sponge/duplex with $k > r$
- HMAC-SHA-3 [NY16] and sandwich sponge [Nai16]
- STROBE protocol framework
- Lightweight permutations

Thank you for your attention!