Full-State Keyed Duplex With Built-In Multi-User Support

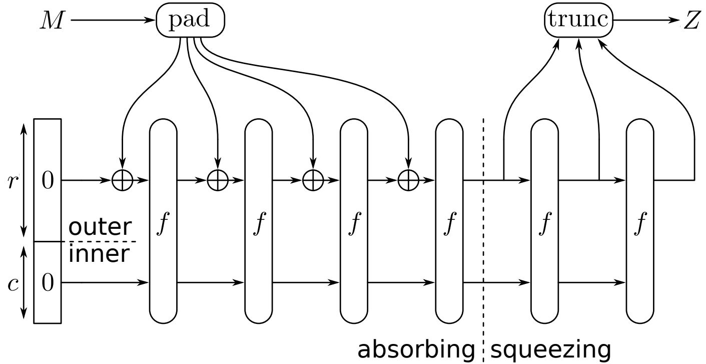
Joan Daemen, Bart Mennink, Gilles Van Assche

Radboud University (The Netherlands),
STMicroelectronics (Belgium)

ASIACRYPT 2017

December 6, 2017

Sponges [BDPV07]



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

Keying the Sponges

Keyed Sponge

- $\text{PRF}(K, M) = \text{Sponge}(K \| M)$
- Message authentication
- Keystream generation

Keying the Sponges

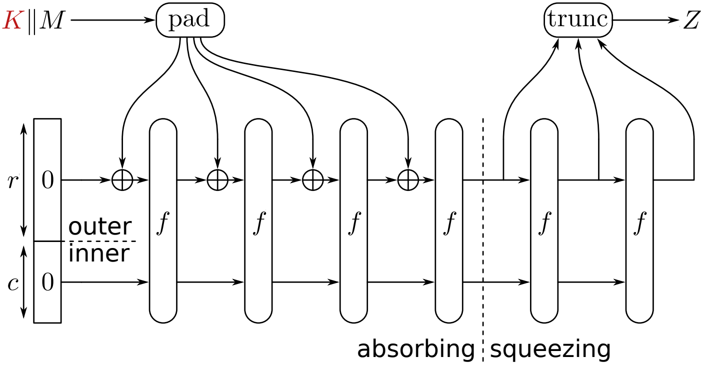
Keyed Sponge

- $\mathsf{PRF}(K, M) = \mathsf{Sponge}(K \| M)$
- Message authentication
- Keystream generation

Keyed Duplex

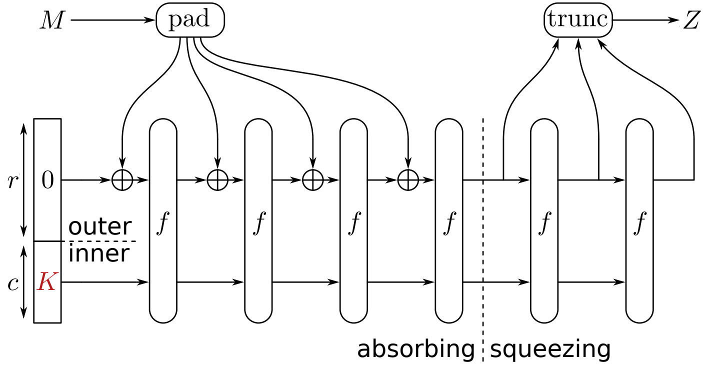
- Authenticated encryption
- Multiple CAESAR submissions

Evolution of Keyed Sponges



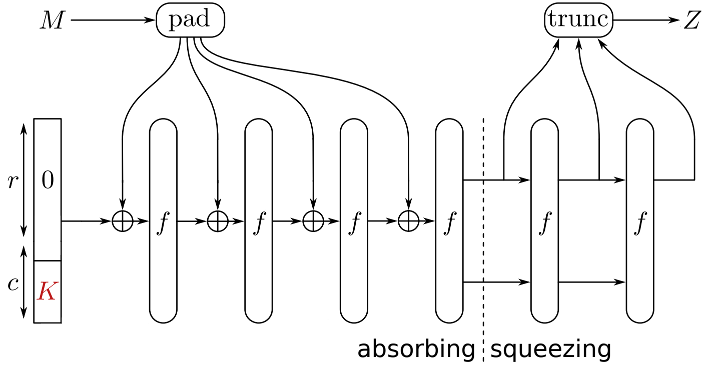
- Outer Keyed Sponge [BDPV11,ADMV15,NY16]

Evolution of Keyed Sponges



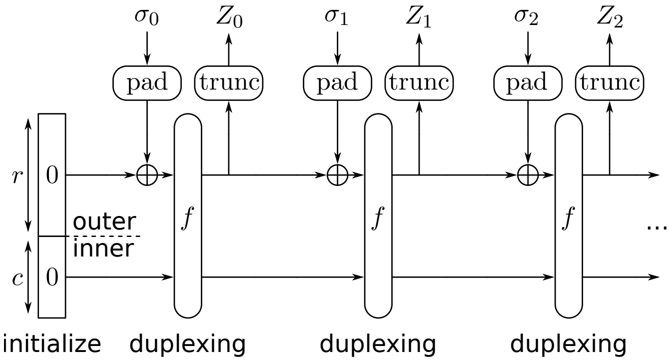
- Outer Keyed Sponge [BDPV11,ADMV15,NY16]
- Inner Keyed Sponge [CDHKN12,ADMV15,NY16]

Evolution of Keyed Sponges



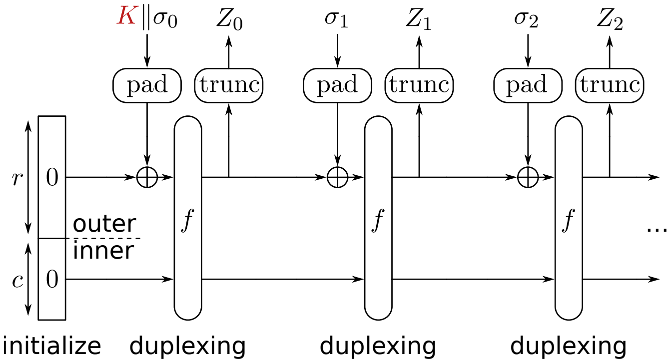
- Outer Keyed Sponge [BDPV11,ADMV15,NY16]
- Inner Keyed Sponge [CDHKN12,ADMV15,NY16]
- Full-State Keyed Sponge [BDPV12,GPT15,MRV15]

Evolution of Keyed Duplexes



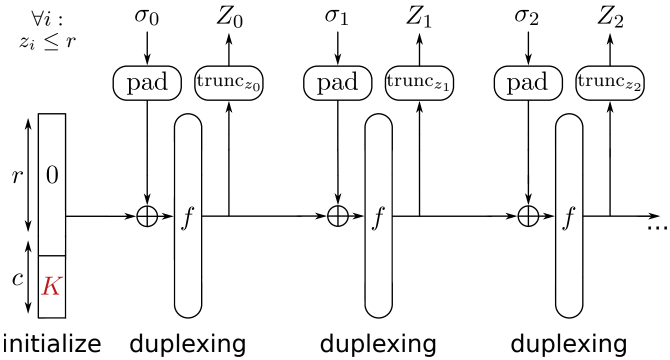
- Unkeyed Duplex [BDPV11]

Evolution of Keyed Duplexes



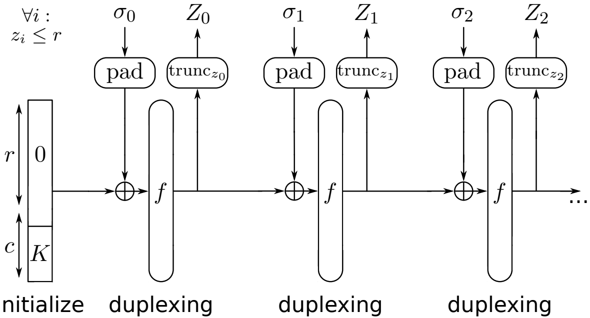
- Unkeyed Duplex [BDPV11]
- Outer Keyed Duplex [BDPV11]

Evolution of Keyed Duplexes



- Unkeyed Duplex [BDPV11]
- Outer Keyed Duplex [BDPV11]
- Full-State Keyed Duplex [MRV15]

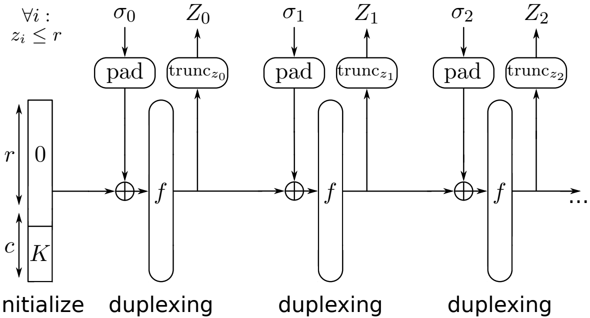
Full-State Keyed Duplex [MRV15]



$$\text{Security} \approx \frac{\mu N}{2^k} + \frac{M^2}{2^c}$$

- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- $\mu \leq 2M$: multiplicity ("maximum outer collision of f")

Full-State Keyed Duplex [MRV15]

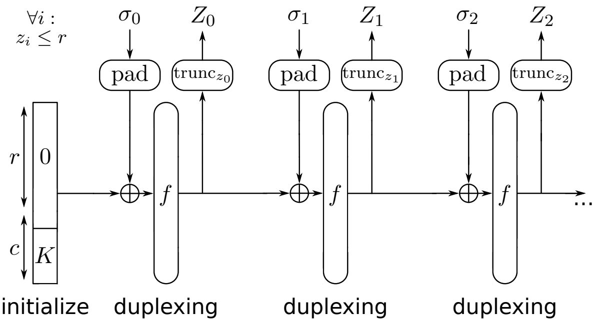


$$\text{Security} \approx \frac{\mu N}{2^k} + \frac{M^2}{2^c}$$

similar bound for full-state keyed sponge

- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- $\mu \leq 2M$: multiplicity ("maximum outer collision of f")

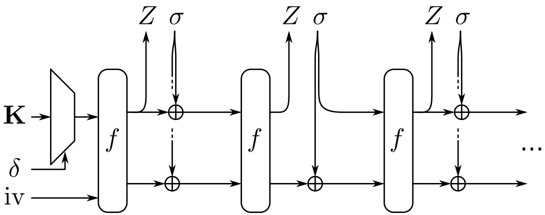
Full-State Keyed Duplex [MRV15]



Limitations

- Dominating term $\mu N/2^k$ rather than $\mu N/2^c$
- Multiplicity μ only known a posteriori
- No multi-user security
- Limited flexibility in modeling adversarial power

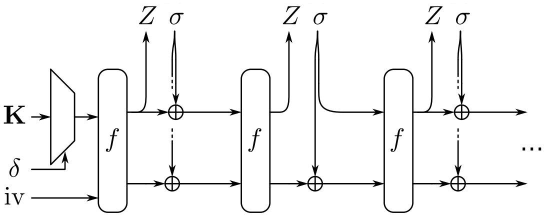
New Core: Full-State Keyed Duplex



Features

- Multi-user by design: index δ specifies key in array
- Initial state: concatenation of $\mathbf{K}[\delta]$ and iv
- Full-state absorption, no padding
- Re-phasing: f, Z, σ instead of σ, f, Z
- Refined adversarial strength

Security Result



$$\text{Security} \approx \frac{q_{\text{iv}} N}{2^k} + \frac{(L + \Omega + \nu_{r,c}^{M}) N}{2^c}$$

- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- q_{iv}: max # init queries with same iv
- L: # queries with repeated path (e.g., nonce-violation)
- Ω: # queries with overwriting outer part (e.g., RUP)
- $\nu_{r,c}^{M}$: some multicollision coefficient $\rightarrow$ often small constant

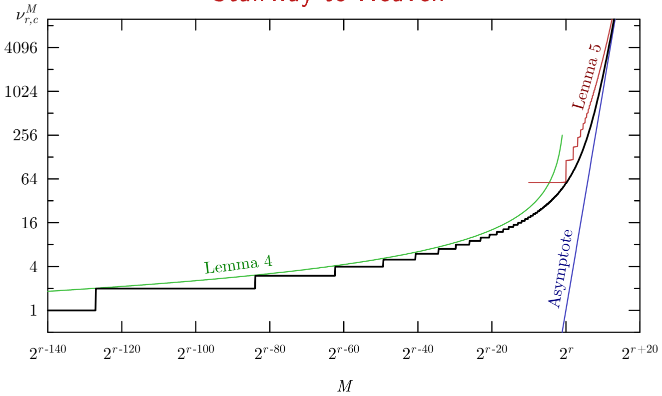
Multicollision Coefficient $\nu_{r,c}^{M}$

- M balls, 2^r bins
- $\nu_{r,c}^{M}$ is smallest x such that $\Pr\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

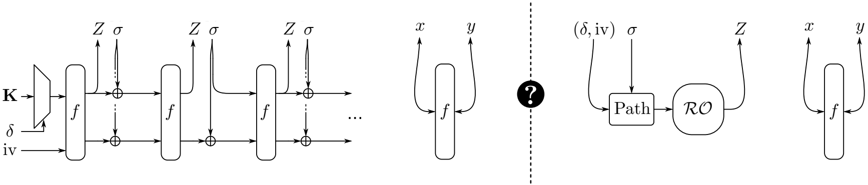
Multicollision Coefficient $\nu_{r,c}^M$

- M balls, 2^r bins
- $\nu_{r,c}^M$ is smallest x such that $\Pr(|\text{fullest bin}| > x) \leq \frac{x}{2^c}$
- For $r + c = 256$, $\nu_{r,c}^M$ versus proven upper bounds:

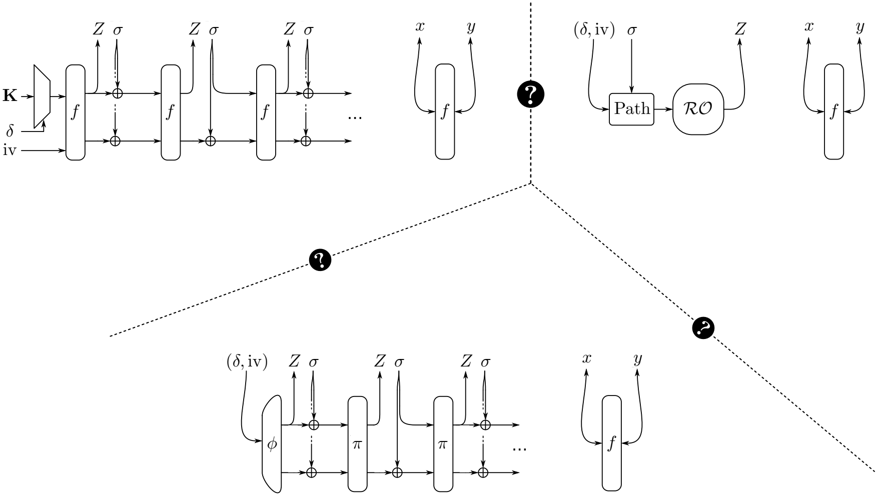
Stairway to Heaven



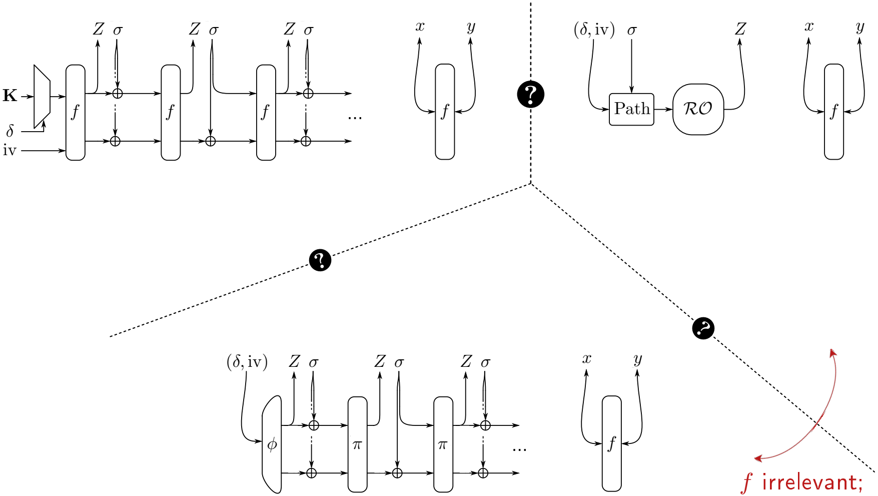
Security in Hybrid Argument



Security in Hybrid Argument

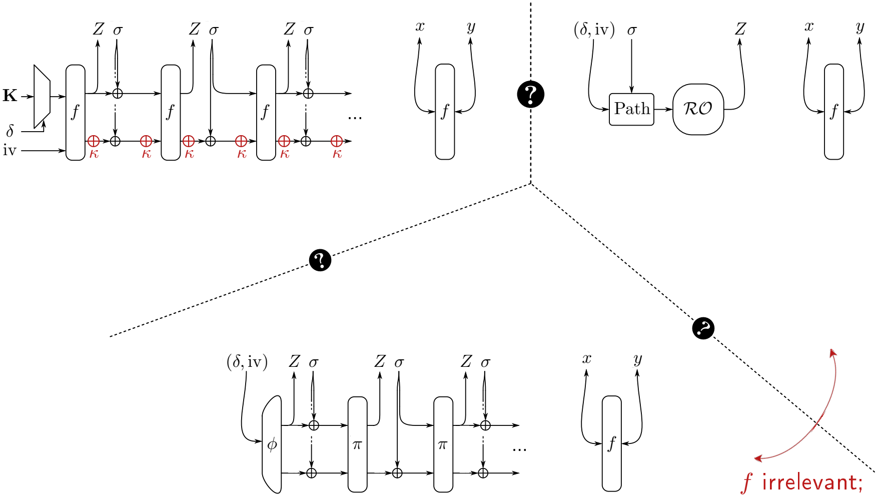


Security in Hybrid Argument



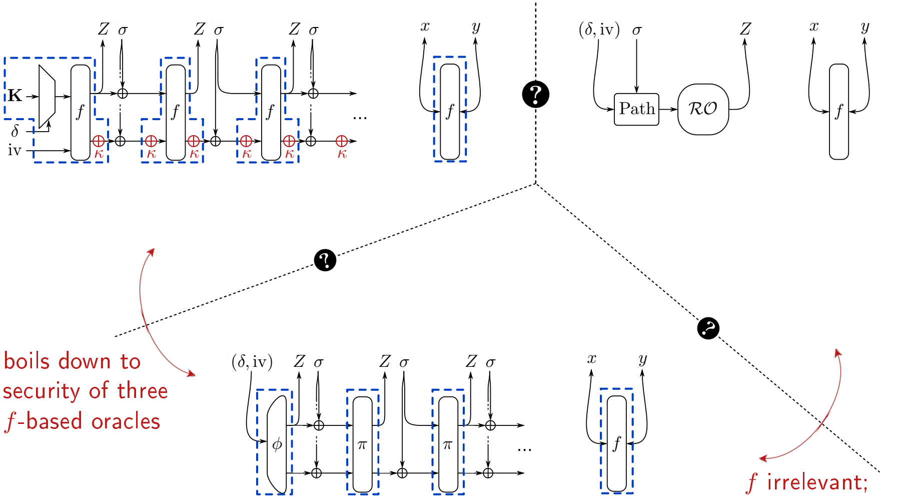
f irrelevant;
security of
random duplex

Security in Hybrid Argument



f irrelevant;
security of
random duplex

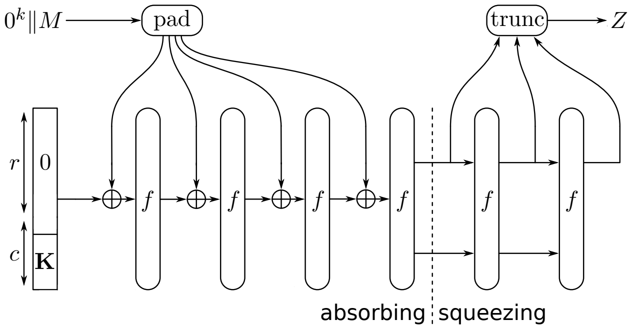
Security in Hybrid Argument



boils down to security of three f-based oracles

f irrelevant; security of random duplex

Application to Full-State Keyed Sponge



- Overwrites possible and no nonce restriction
- $L + \Omega \leq M/2$, $\nu_{r,c}^{M}$ is negligible, $q_{\text{iv}} \leq u$

$$\text{Security} \approx \frac{uN}{2^k} + \frac{MN}{2^c}$$

- Improves [MRV15]: better bound and multi-user support

Application to Authenticated Encryption

General Bound (Nonce-Violating)

- $L + \Omega \leq M/2$
- $\nu_{r,c}^{M}$ is negligible

$$\text{Security} \approx \frac{q_{\text{iv}} N}{2^k} + \frac{MN}{2^c}$$

Application to Authenticated Encryption

General Bound (Nonce-Violating)

- $L + \Omega \leq M/2$
- $\nu_{r,c}^{M}$ is negligible

$$\text{Security} \approx \frac{q_{\text{iv}} N}{2^k} + \frac{MN}{2^c}$$

Nonce-Respecting and No RUP

- $L = \Omega = 0$
- Second term dominated by $\nu_{r,c}^{M}$

$$\text{Security} \approx \frac{q_{\text{iv}} N}{2^k} + \frac{\nu_{r,c}^{M} N}{2^c}$$

Application to Authenticated Encryption

- Security strength if $Mr \leq 2^a$:

Scheme		Parameters b	c	r	nonce-violating	nonce-respecting
Ketje	Jr.	200	184	16	$189–a$	$\min\{196–a, 177\}$
	Sr.	400	368	32	$374–a$	$\min\{396–a, 360\}$
Ascon	128	320	256	64	$263–a$	$\min\{317–a, 248\}$
	128a	320	192	128	$200–a$	$\min\{318–a, 184\}$
NORX	32	512	128	384	$137–a$	127
	64	1024	256	768	$266–a$	255
Keyak	River	800	256	544	$266–a$	255
	Lake	1600	256	1344	$267–a$	255

Conclusion

Full-Stated Keyed Duplex

- Versatile primitive
- Flexible bound covering many use cases
- Makes life easier for sponge mode designer

Conclusion

Full-State Keyed Duplex

- Versatile primitive
- Flexible bound covering many use cases
- Makes life easier for sponge mode designer

Looking Forward

- Generalized FSKD found adoption in Keyak v2
- Further applications of tight multi-collision analysis

Thank you for your attention!

SUPPORTING SLIDES

Comparison of Schemes

- "Pure bound" means that derived security bound is expressed purely as a function of the adversary's capabilities.

	Full state absorption	Extendable output	Multi-target	Pure bound
Bertoni et al. [BDPV11]	—	✓	—	✓
Bertoni et al. [BDPV11]	—	✓	—	✓
Chang et al. [CDHKN12]	—	✓	—	✓
Andreeva et al. [ADMV15]	—	✓	✓	—
Gaži et al. [GPT15]	✓	—	—	✓
Mennink et al. [MRV15]	✓	✓	—	—
Naito and Yasuda [NY16]	—	✓	—	✓
This work	✓	✓	✓	✓