Leakage Resilience of the ISAP Mode: a Vulgarized Summary

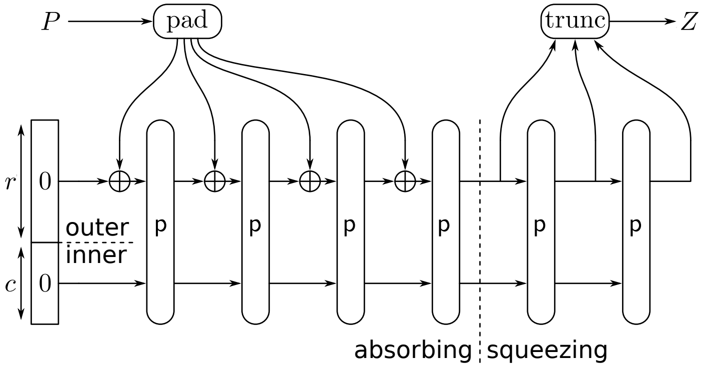
Christoph Dobraunig, Bart Mennink *

Radboud University (The Netherlands)

NIST Lightweight Cryptography Workshop 2019
November 6, 2019

* Thanks to the ISAP team!

Sponges [BDPV07]



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

Keying Sponges

Keyed Sponge

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

Keying Sponges

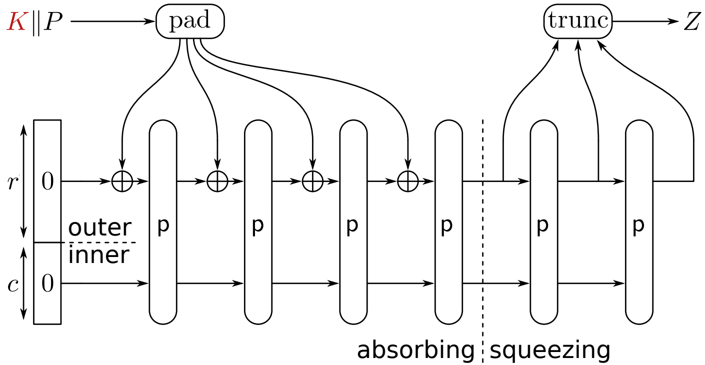
Keyed Sponge

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

Keyed Duplex

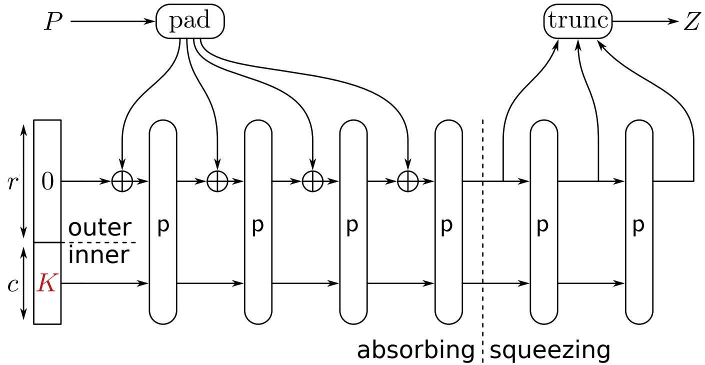
- Authenticated encryption
- Multiple CAESAR and NIST LWC submissions

Evolution of Keyed Sponges



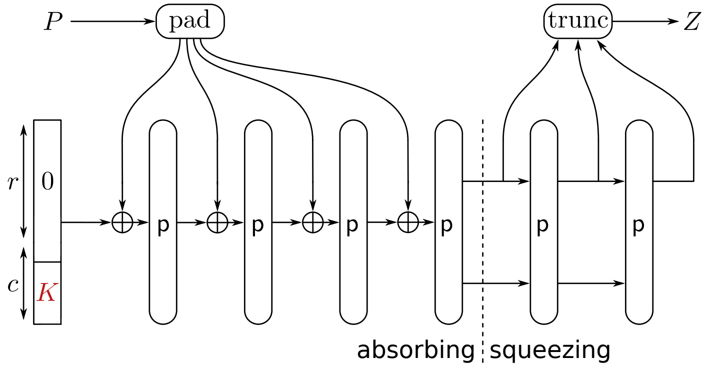
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]

Evolution of Keyed Sponges



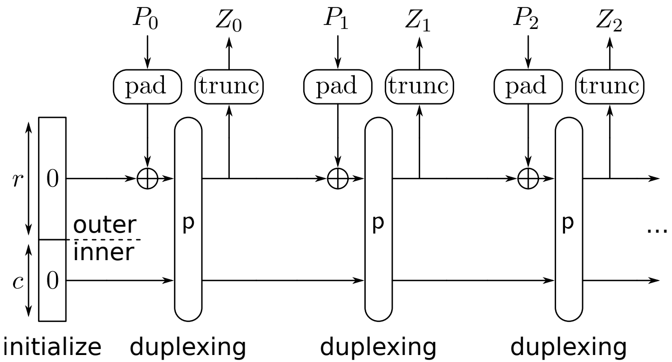
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]

Evolution of Keyed Sponges



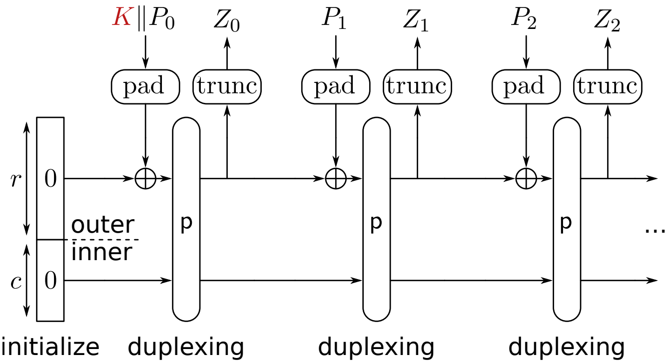
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]
- Full-Keyed Sponge [BDPV12,GPT15,MRV15]

Evolution of Keyed Duplexes



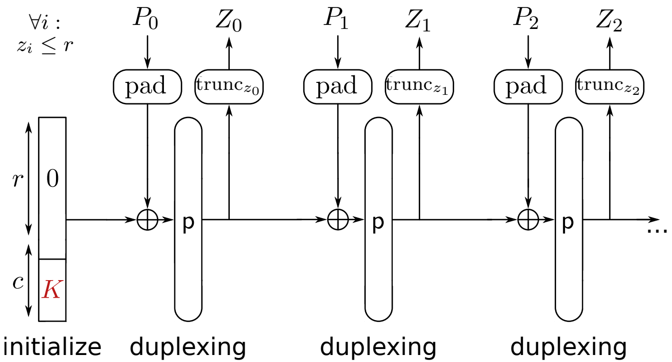
- Unkeyed Duplex [BDPV11]

Evolution of Keyed Duplexes



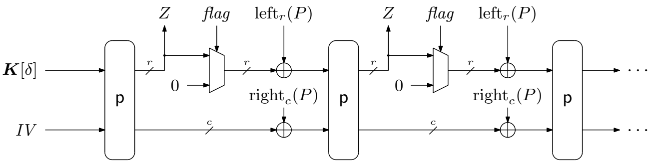
- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]

Evolution of Keyed Duplexes

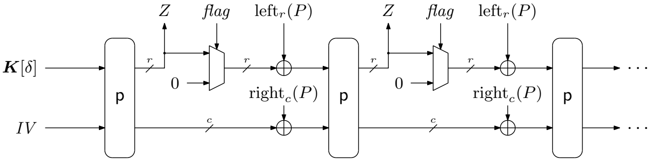


- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]
- Full-Keyed Duplex [MRV15,DMV17]

Security of Generalized Keyed Duplex [DMV17]



Security of Generalized Keyed Duplex [DMV17]



- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- q_{IV}: max # init calls for single 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

Simplified Security Bound

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

Outline

Leakage Resilience of the Duplex Construction

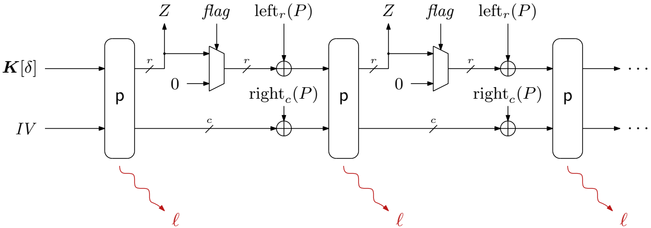
Security of the Suffix Keyed Sponge

Application to ISAP

Conclusion

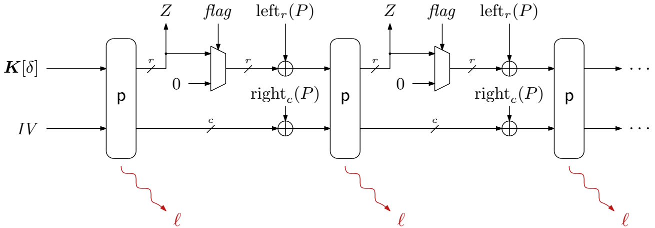
Outline

Leakage Resilience of Keyed Duplex



- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

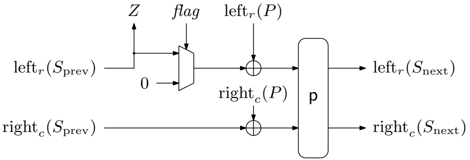
Leakage Resilience of Keyed Duplex



- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

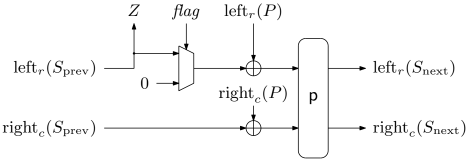
Is keyed duplex secure under leakage?

Formalizing Leakage



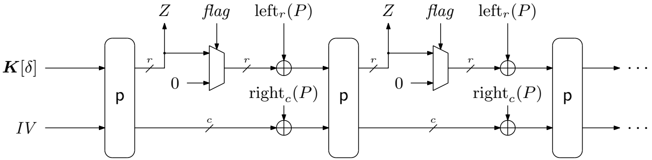
- L is any fixed leakage function (non-adaptive leakage)
- For each evaluation of p: L leaks λ bits of $(S_{\text{prev}}, S_{\text{next}})$

Influence of Leakage



- Suppose S_{prev} invoked at most R times
- At most $R+1$ leakages of S_{prev}
- Min-entropy of S_{prev}: at least $c-(R+1)\lambda$

Leakage Resilience of Keyed Duplex



- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- q_{IV}: max # init calls for single IV
- q_δ: maximum # init calls for single δ
- L: # queries with repeated path (e.g., nonce-violation)
- Ω: # queries with overwriting outer part (e.g., RUP)
- R: max # duplexing calls for single non-empty subpath
- $\nu_{r,c}^M$: some multicollision coefficient $\rightarrow$ often small constant

Simplified Security Bound

$$\frac{q_{IV} N}{2^{k - q_\delta \lambda}} + \frac{(L + \Omega + \nu_{r,c}^M) N}{2^{c - (R+1)\lambda}}$$

Application: Managing Leakage

Simplified Security Bound

$$\frac{q_{IV} N}{2^{k - q_\delta \lambda}} + \frac{(L + \Omega + \nu_{r,c}^{M}) N}{2^{c - (R+1)\lambda}}$$

Application: Managing Leakage

Simplified Security Bound

$$\frac{q_{IV} N}{2^{k - q_\delta \lambda}} + \frac{(L + \Omega + \nu^M_{r,c}) N}{2^{c-(R+1)\lambda}}$$

$q_\delta \leq$ **# allowed** IV**'s**

Application: Managing Leakage

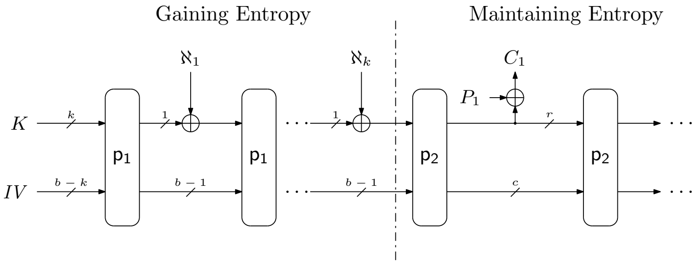
Simplified Security Bound

$$\frac{q_{IV} N}{2^{k - q_\delta \lambda}} + \frac{(L + \Omega + \nu^M_{r,c}) N}{2^{c-(R+1)\lambda}}$$

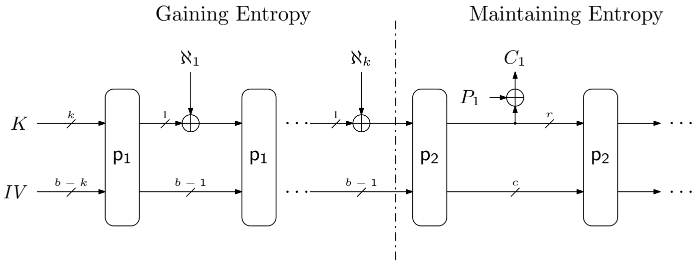
$q_\delta \leq$ # **allowed** IV**'s**

Limit $L + \Omega$ **or limit** R**?**

Application: Leakage Resilient Encryption (1)

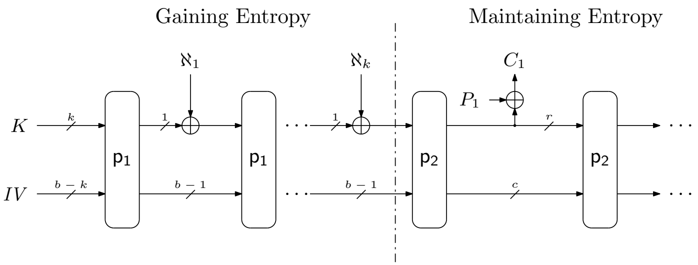


Application: Leakage Resilient Encryption (1)



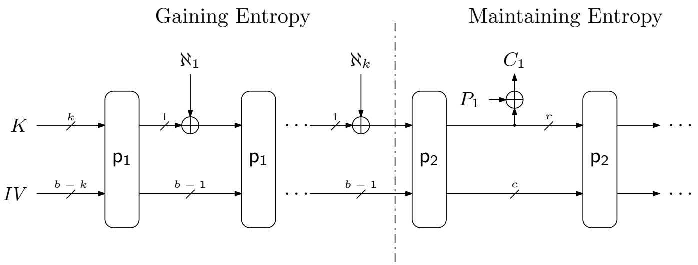
- Gain entropy in KD_1 from nonce at small rate

Application: Leakage Resilient Encryption (1)



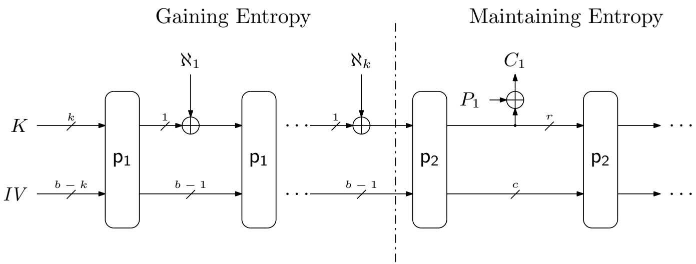
- Gain entropy in KD_1 from nonce at small rate
- Final state of KD_1 has high entropy (w.h.p.)

Application: Leakage Resilient Encryption (1)



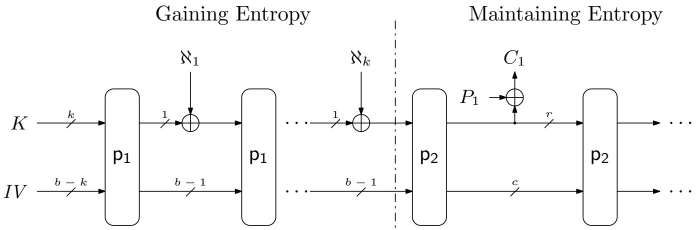
- Gain entropy in KD_1 from nonce at small rate
- Final state of KD_1 has high entropy (w.h.p.)
- Inner part of state of KD_1 forms key to KD_2

Application: Leakage Resilient Encryption (1)



- Gain entropy in KD_1 from nonce at small rate
- Final state of KD_1 has high entropy (w.h.p.)
- Inner part of state of KD_1 forms key to KD_2
- Encrypt in KD_2 at high rate while maintaining high entropy (w.h.p.)

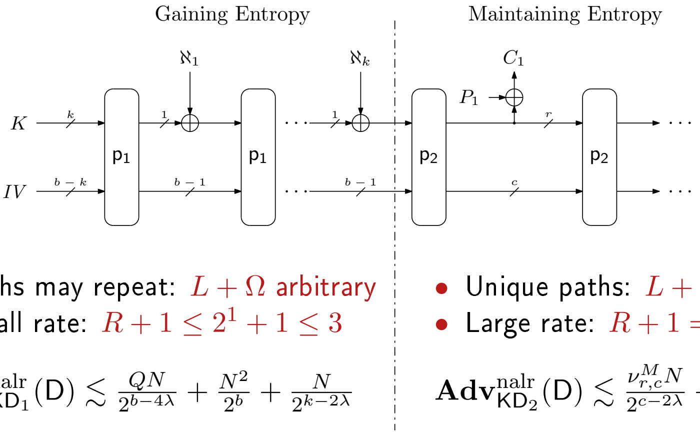
Application: Leakage Resilient Encryption (2)



- Paths may repeat: $L + \Omega$ arbitrary
- Small rate: $R + 1 \leq 2^1 + 1 \leq 3$

- Unique paths: $L + \Omega = 0$
- Large rate: $R + 1 = 2$

Application: Leakage Resilient Encryption (2)



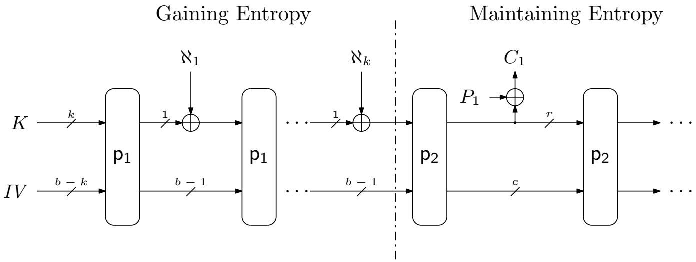
- Paths may repeat: $L + \Omega$ arbitrary
- Small rate: $R + 1 \leq 2^1 + 1 \leq 3$

$$\mathbf{Adv}^{\text{nalr}}_{\mathsf{KD}_1}(\mathsf{D}) \lesssim \frac{QN}{2^{b-4\lambda}} + \frac{N^2}{2^b} + \frac{N}{2^{k-2\lambda}}$$

- Unique paths: $L + \Omega = 0$
- Large rate: $R + 1 = 2$

$$\mathbf{Adv}^{\text{nalr}}_{\mathsf{KD}_2}(\mathsf{D}) \lesssim \frac{\nu^M_{r,c} N}{2^{c-2\lambda}} + \frac{QN}{2^{b-4\lambda}} + \frac{N^2}{2^b}$$

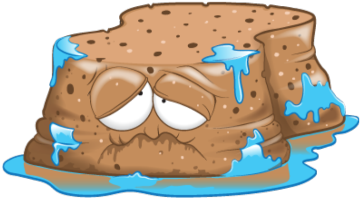
Application: Leakage Resilient Encryption (3)

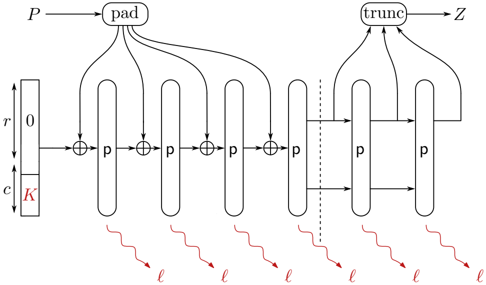


$$\mathbf{Adv}_{\mathcal{E}}^{\text{nalr-cpa}}(\mathsf{D}) \leq 4 \cdot \mathbf{Adv}_{\mathsf{KD}_1}^{\text{nalr}}(\mathsf{D}') + 2 \cdot \mathbf{Adv}_{\mathsf{KD}_2}^{\text{nalr}}(\mathsf{D}'')$$

Outline

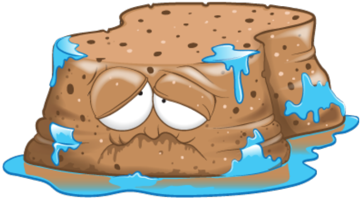
Leakage Resilience of Keyed Sponges

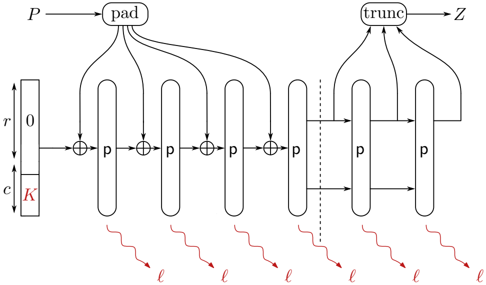




- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

Leakage Resilience of Keyed Sponges

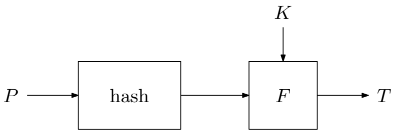




- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

Minimizing leakage of keyed sponge?

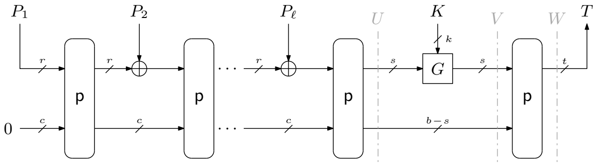
Hash-then-MAC



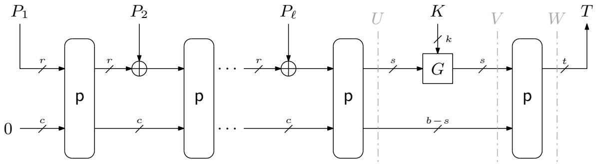
Typical Approach

- Hash function is unkeyed $\rightarrow$ nothing to be protected
- Keyed function F applied to fixed-size input
- Hash output (hence F input) must be at least $2k$ bits for k-bit security

Suffix Keyed Sponge



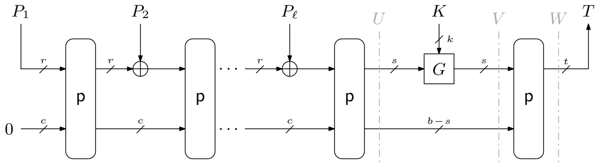
Suffix Keyed Sponge



SuKS versus Full-Keyed Sponge

- No full-state absorption
- Side-channel leakage limited
- s, t arbitrary (typical: $s = t = c/2$)

Suffix Keyed Sponge



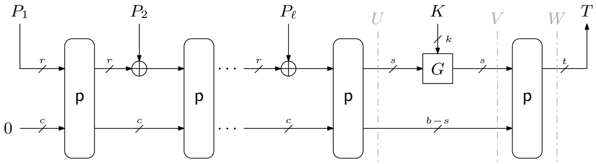
SuKS versus Full-Keyed Sponge

- No full-state absorption
- Side-channel leakage limited
- s, t arbitrary (typical: $s = t = c/2$)

SuKS versus Hash-then-MAC

- State of keyed function half as large
- G need not be cryptographically strong (a XOR suffices)
- Single cryptographic primitive needed

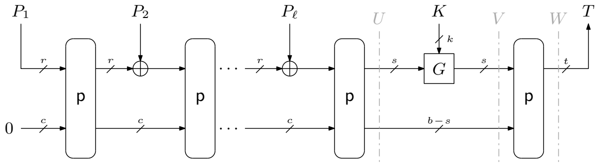
Security of SuKS



- $k, s, t \leq b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

Security of SuKS

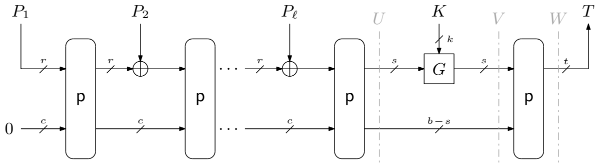


- $k, s, t \leq b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

inner collision

Security of SuKS



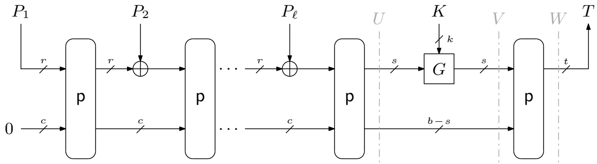
- $k, s, t \leq b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

inner collision

"break at G", bounds primitive queries with same inner part

Security of SuKS



- $k, s, t \leq b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

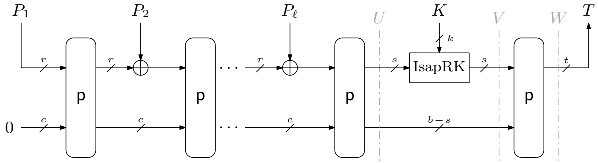
$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

inner collision

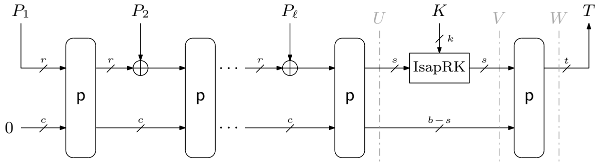
"break at G", bounds primitive queries with same inner part

"break at T", bounds construction queries with same tag

Application to MAC Part of ISAP [DEMMMPU19]



Application to MAC Part of ISAP [DEMMMPU19]

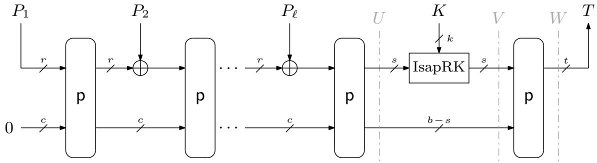


$(b, c, r, k) = (400, 256, 144, 128)$

- $\nu_{b-s,s}^{2(N-q)} = \mu_{272,128}^{2^{129}} \leq 3$
- $\nu_{t,b-t}^{q} = \mu_{128,272}^{2^{128}} \leq 80$

$$\mathbf{Adv}_{\text{IsapMAC}}^{\text{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^{256}} + \frac{3N}{2^{128}} + \frac{80N}{2^{272}}$$

Application to MAC Part of ISAP [DEMMMPU19]



$(b, c, r, k) = (400, 256, 144, 128)$

- $\nu_{b-s,s}^{2(N-q)} = \mu_{272,128}^{2^{129}} \leq 3$
- $\nu_{t,b-t}^{q} = \mu_{128,272}^{2^{128}} \leq 80$

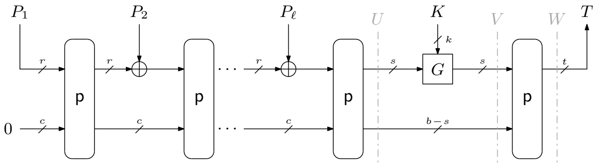
$$\mathbf{Adv}_{\text{IsapMAC}}^{\text{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^{256}} + \frac{3N}{2^{128}} + \frac{80N}{2^{272}}$$

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

- $\nu_{b-s,s}^{2(N-q)} = \mu_{192,128}^{2^{129}} \leq 5$
- $\nu_{t,b-t}^{q} = \mu_{128,192}^{2^{128}} \leq 67$

$$\mathbf{Adv}_{\text{IsapMAC}}^{\text{prf}}(\mathsf{D}) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{272}}$$

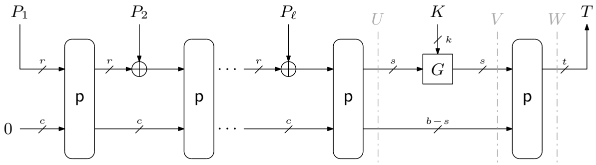
Leakage Resilience of SuKS



- $k, s, t \leq b$
- G is strongly protected, $2^{-\delta}$-uniform, and $2^{-\epsilon}$-universal

$$\mathbf{Adv}_F^{\text{nalr-prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{s,b-s}^{2(N-q)}}{2^{b-s}} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\} - \nu_{s,b-s}^{2(N-q)} \lambda}} + \frac{\nu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

Leakage Resilience of SuKS



- $k, s, t \leq b$
- G is strongly protected, $2^{-\delta}$-uniform, and $2^{-\epsilon}$-universal

$$\mathbf{Adv}_F^{\text{nalr-prf}}(\mathsf{D}) \leq \frac{2N^2}{2^c} + \frac{\nu_{s,b-s}^{2(N-q)}}{2^{b-s}} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\} - \nu_{s,b-s}^{2(N-q)}\lambda}} + \frac{\nu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$

bounds the number of repeated leakages on same $G(K, X)$

Outline

Leakage Resilience of the Duplex Construction

Security of the Suffix Keyed Sponge

Application to ISAP

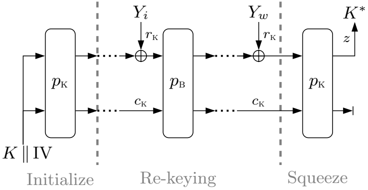
Conclusion

ISAP

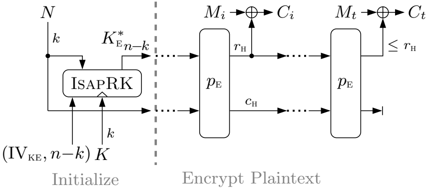
- LWC candidate [DEMMMPU19]

- Originally proposed at FSE 2017 [DEMMU17]
- Sponge/duplex-based authenticated encryption mode
- Instantiation:
  - Keccak-p$[400]$
  - Ascon-p
- Carefully selected capacities and rates:
  - Protection against DPA
  - Hardening against fault attacks: DFA, SFA, SIFA

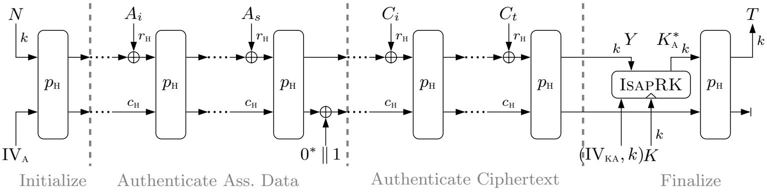
Security of ISAP Mode



IsapRK

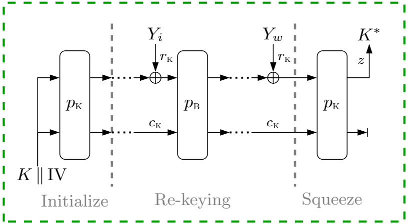


IsapEnc



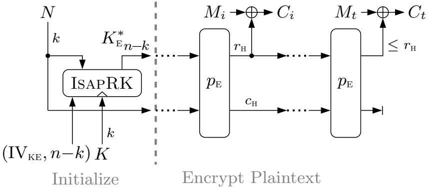
IsapMAC

Security of ISAP Mode

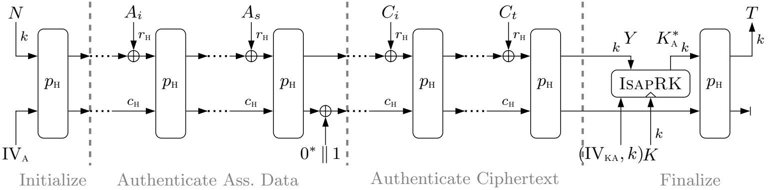


IsapRK

KD$_1$ with small rate

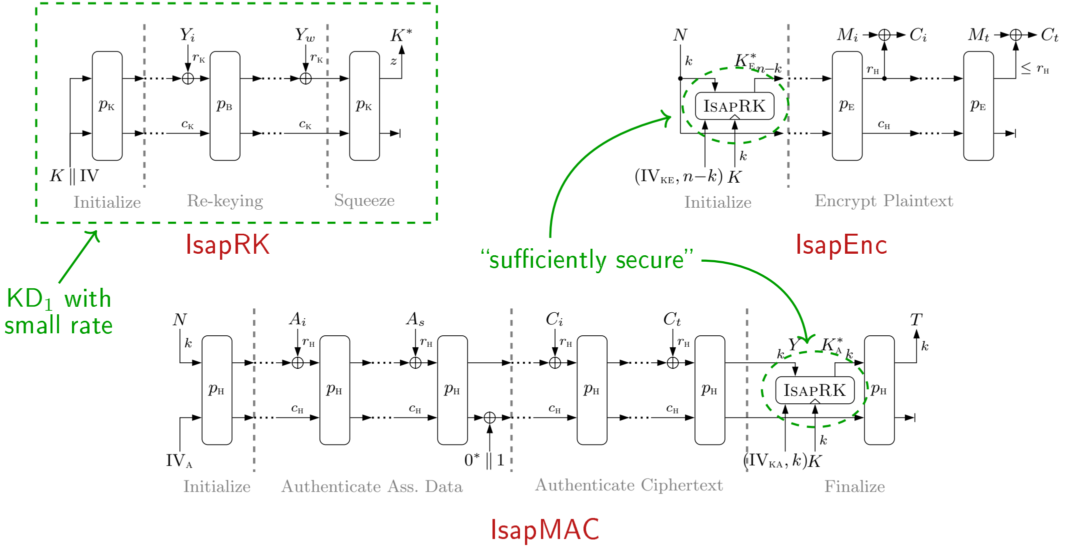


IsapEnc

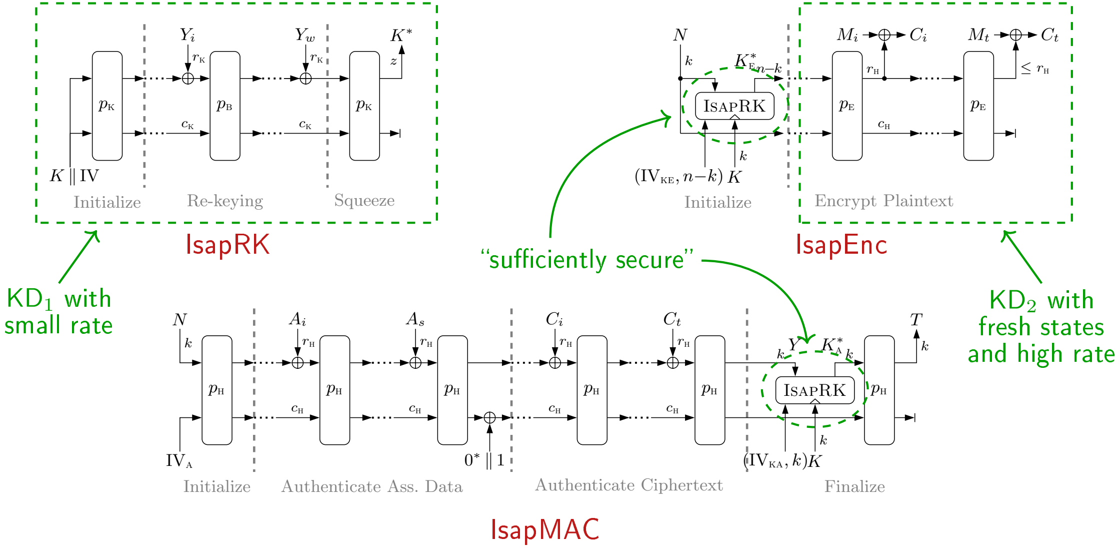


IsapMAC

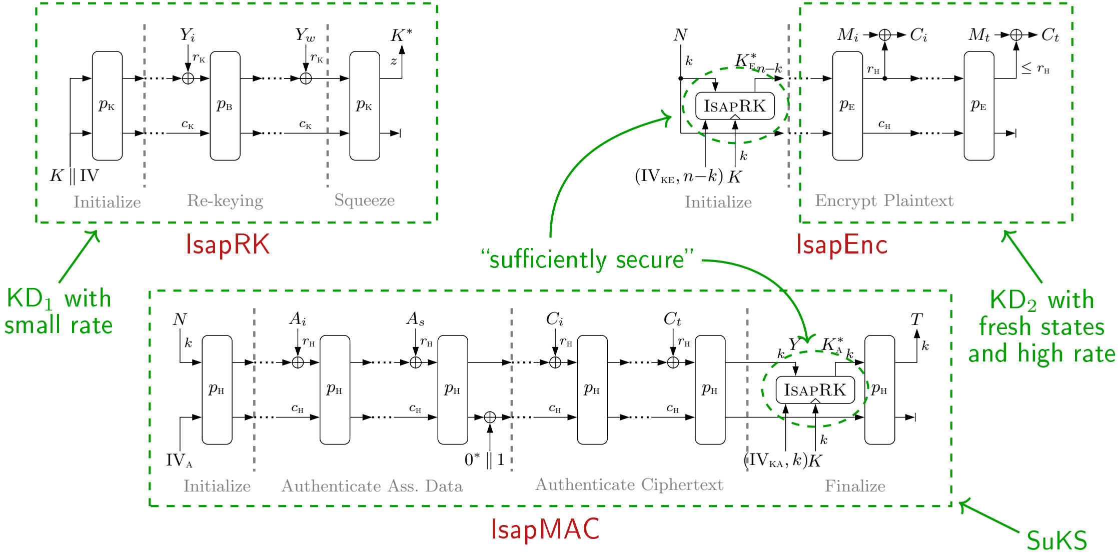
Security of ISAP Mode



Security of ISAP Mode



Security of ISAP Mode



Outline

Conclusion

ISAP

- Built-in security against side-channel and fault attacks
- Higher order security without higher order masking!

Conclusion

ISAP

- Built-in security against side-channel and fault attacks
- Higher order security without higher order masking!

Leakage Resilience

- Follows from:
  - Leakage resilience of Keyed Duplex [DM19a]
  - Leakage resilience of Suffix Keyed Sponge [DM19b]
- Proof in alternative model given by Guo et al. [GPPS19]

Thank you for your attention!