Leakage Resilience of the Duplex Construction

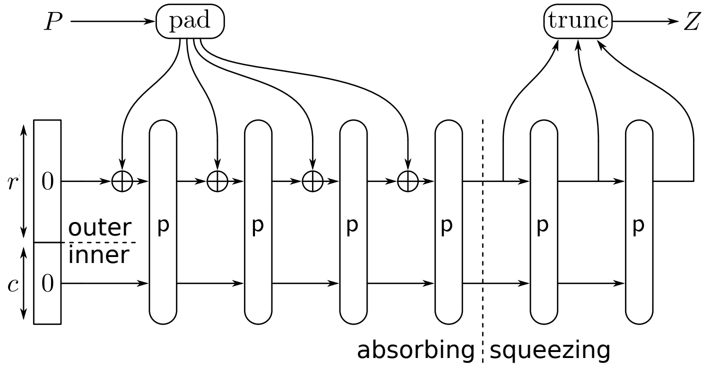
Christoph Dobraunig, Bart Mennink

Radboud University (The Netherlands)

ASIACRYPT 2019

December 11, 2019

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

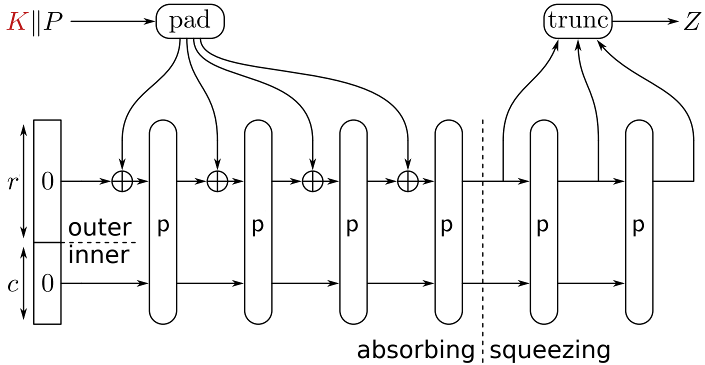
Keyed Sponge

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

Keyed Duplex

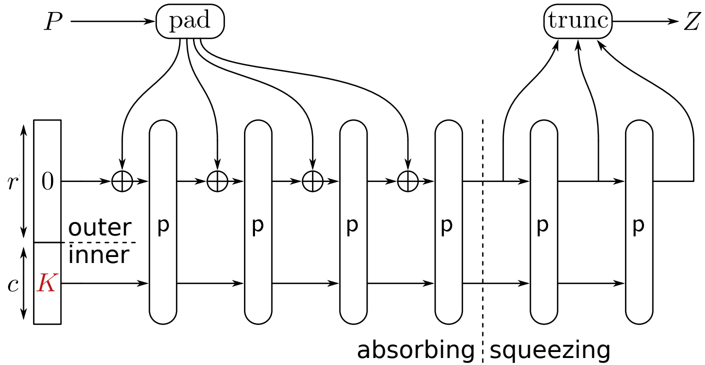
- Authenticated encryption
- Multiple CAESAR and NIST LWC submissions

Evolution of Keyed Sponges



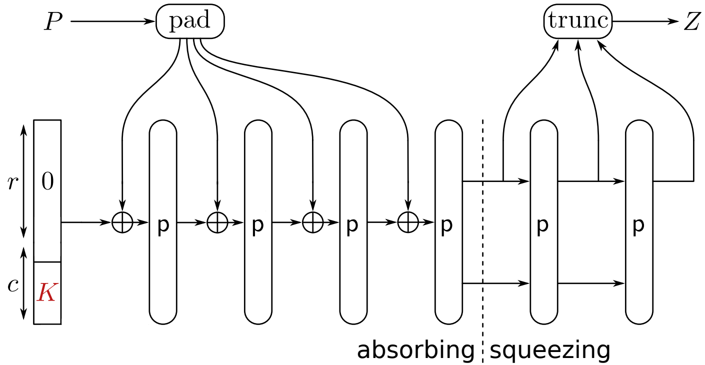
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]

Evolution of Keyed Sponges



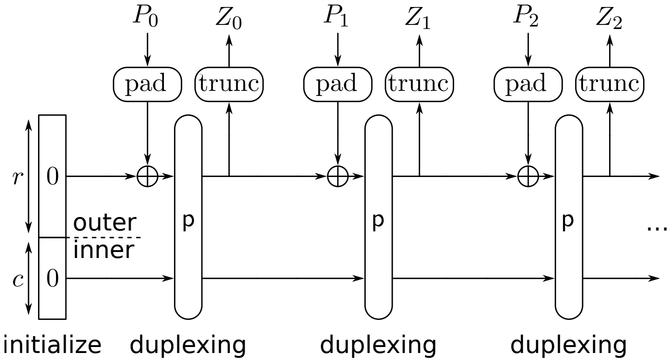
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]

Evolution of Keyed Sponges



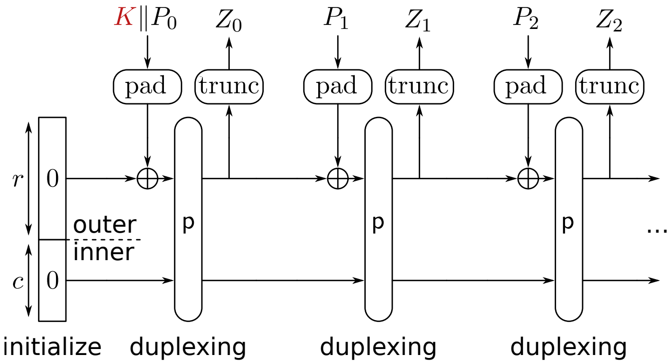
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]
- Full-Keyed Sponge [BDPV12,GPT15,MRV15]

Evolution of Keyed Duplexes



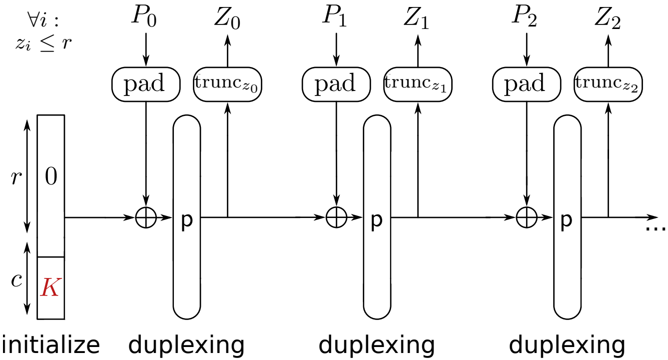
- Unkeyed Duplex [BDPV11]

Evolution of Keyed Duplexes



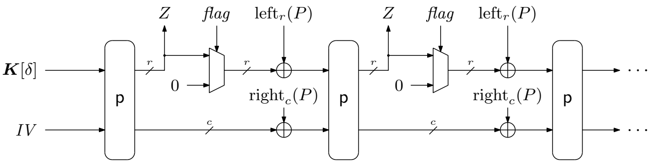
- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]

Evolution of Keyed Duplexes

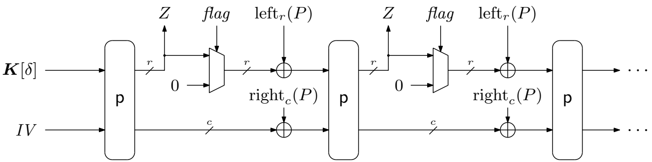


- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]
- Full-Keyed Duplex [MRV15,DMV17]

Security of Generalized Keyed Duplex [DMV17]



Security of Generalized Keyed Duplex [DMV17]

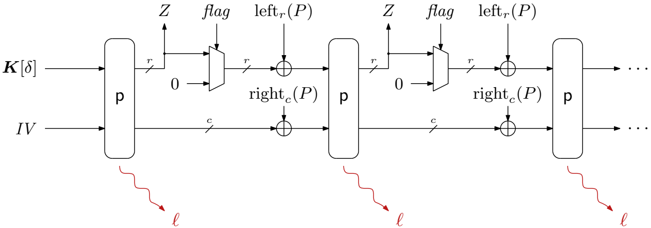


- M: data complexity (calls to construction)
- N: time complexity (calls to primitive)
- q_{IV}: max # init calls for single IV
- L: # queries with repeated path (e.g., nonce-violation)
- Ω: # queries with overwriting outer part (e.g., RUP)
- $\nu_{r,c}^{M}$: some multicollision coefficient $\rightarrow$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

Simplified Security Bound

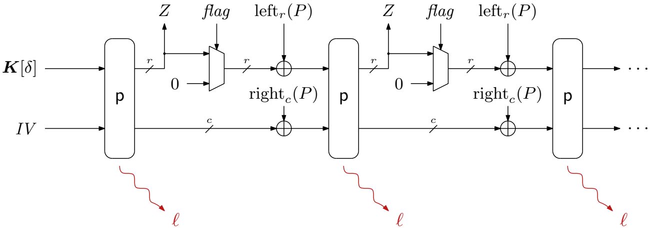
$$\frac{q_{IV}N}{2^k} + \frac{(L+\Omega+\nu_{r,c}^{M})N}{2^c}$$

Leakage Resilience of Keyed Duplex



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

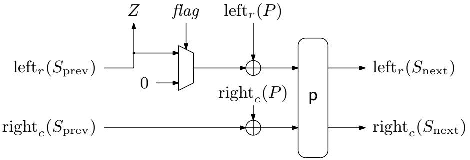
Leakage Resilience of Keyed Duplex



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

Is keyed duplex secure under leakage?

Leakage Resilience of Keyed Duplex: Formalizing Leakage



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

Leakage Resilience of Keyed Duplex: Model

- Re-phasing: P, p, Z [MRV15] $\longrightarrow$ p, Z, P [DMV17] $\longrightarrow$ Z, P, p

Algorithm $\mathsf{KD}[\mathsf{p}]_{\boldsymbol{K}}$

Interface: KD.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{p}(S)$
return $\varnothing$

Interface: KD.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$

$Z \leftarrow \mathrm{left}_r(S)$
$S \leftarrow S \oplus [\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P$
$S \leftarrow \mathsf{p}(S)$
return Z

Leakage Resilience of Keyed Duplex: Model

- Re-phasing: P, p, Z [MRV15] $\longrightarrow$ p, Z, P [DMV17] $\longrightarrow$ Z, P, p

Algorithm $\mathsf{KD}[\mathsf{p}]_{\boldsymbol{K}}$

Interface: KD.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{p}(S)$
return $\varnothing$

Interface: KD.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$

$Z \leftarrow \mathrm{left}_r(S)$
$S \leftarrow S \oplus [\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P$
$S \leftarrow \mathsf{p}(S)$
return Z

Algorithm $\mathsf{AIXIF}[\mathsf{ro}]_{\boldsymbol{K}}$

Interface: AIXIF.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$\mathit{path} \leftarrow \mathsf{encode}[\delta] \parallel IV$
$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$
return $\varnothing$

Interface: AIXIF.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$

$Z \leftarrow \mathrm{left}_r(S)$
$\mathit{path} \leftarrow \mathit{path} \parallel ([\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$
return Z

Leakage Resilience of Keyed Duplex: Model

- Re-phasing: P, p, Z [MRV15] $\longrightarrow$ p, Z, P [DMV17] $\longrightarrow$ Z, P, p

Algorithm $\mathsf{KD}[\mathsf{p}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: KD.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{p}(S)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: KD.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$
$Z \leftarrow \mathrm{left}_r(S)$
$S \leftarrow S \oplus [\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P$
$S \leftarrow \mathsf{p}(S)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

Algorithm $\mathsf{AIXIF}[\mathsf{ro}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: AIXIF.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$
$\mathit{path} \leftarrow \mathsf{encode}[\delta] \parallel IV$
$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: AIXIF.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$
$Z \leftarrow \mathrm{left}_r(S)$
$\mathit{path} \leftarrow \mathit{path} \parallel ([\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

Leakage Resilience of Keyed Duplex: Model

- Re-phasing: P, p, Z [MRV15] $\longrightarrow$ p, Z, P [DMV17] $\longrightarrow$ Z, P, p

Algorithm $\mathsf{KD}[\mathsf{p}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: KD.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{p}(S)$ $\triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: KD.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$
$Z \leftarrow \text{left}_r(S)$
$S \leftarrow S \oplus [\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P$
$S \leftarrow \mathsf{p}(S)$ $\triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

Algorithm $\mathsf{AIXIF}[\mathsf{ro}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: AIXIF.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$
$\mathit{path} \leftarrow \mathsf{encode}[\delta] \parallel IV$
$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: AIXIF.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$
$Z \leftarrow \text{left}_r(S)$
$\mathit{path} \leftarrow \mathit{path} \parallel ([\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

$$\mathbf{Adv}^{\mathrm{naLR}}_{\mathsf{KD}}(\mathsf{D}) = \max_{\mathsf{L} \in \mathcal{L}} \Delta_{\mathsf{D}} \left(\mathsf{KD}[\mathsf{p}]^{\mathsf{L}}_{\boldsymbol{K}}, \mathsf{p}^{\pm} \; ; \; \mathsf{AIXIF}[\mathsf{ro}]^{\mathsf{L}}_{\boldsymbol{K}}, \mathsf{p}^{\pm} \right)$$

Leakage Resilience of Keyed Duplex: Model

- Re-phasing: P, p, Z [MRV15] $\longrightarrow$ p, Z, P [DMV17] $\longrightarrow$ Z, P, p

Algorithm $\mathsf{KD}[\mathsf{p}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: KD.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{p}(S)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: KD.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$

$Z \leftarrow \mathrm{left}_r(S)$
$S \leftarrow S \oplus [\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P$
$S \leftarrow \mathsf{p}(S)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

Algorithm $\mathsf{AIXIF}[\mathsf{ro}]^{\mathsf{L}}_{\boldsymbol{K}}$

Interface: AIXIF.init
Input: $(\delta, IV) \in [1, u] \times \mathcal{IV}$
Output: $\varnothing$

$\mathit{path} \leftarrow \mathsf{encode}[\delta] \parallel IV$
$S \leftarrow \mathsf{rot}_\alpha(\boldsymbol{K}[\delta] \parallel IV)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return $\varnothing$

Interface: AIXIF.duplex
Input: $(\mathit{flag}, P) \in \{\mathit{true}, \mathit{false}\} \times \{0,1\}^b$
Output: $Z \in \{0,1\}^r$

$Z \leftarrow \mathrm{left}_r(S)$
$\mathit{path} \leftarrow \mathit{path} \parallel ([\mathit{flag}] \cdot (Z \| 0^{b-r}) \oplus P)$
$S \leftarrow \mathsf{ro}(\mathit{path}, b)$ $\quad \triangleright$ leaks $\mathsf{L}(S_{\text{prev}}, S_{\text{next}})$
return Z

$$\mathbf{Adv}^{\mathrm{naLR}}_{\mathsf{KD}}(\mathsf{D}) = \max_{\mathsf{L} \in \mathcal{L}} \Delta_{\mathsf{D}} \left(\mathsf{KD}[\mathsf{p}]^{\mathsf{L}}_{\boldsymbol{K}}, \mathsf{p}^{\pm} \; ; \; \mathsf{AIXIF}[\mathsf{ro}]^{\mathsf{L}}_{\boldsymbol{K}}, \mathsf{p}^{\pm} \right)$$

- No leakage $\longrightarrow$ original model of [DMV17] retained

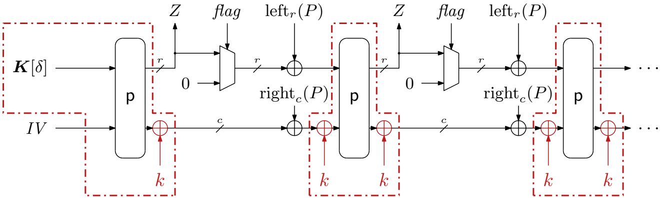
Proof Rationale: Typical Leakage Resilience Proof

- Iterates a weak PRF with output size n
- Relies on HILL-pseudoentropy
- Procedure:
  - Input sufficiently high min-entropy $\longrightarrow$ output pseudorandom
  - λ bits of output leaked $\longrightarrow$ HILL-pseudoentropy $n - 2\lambda$
  - HILL-pseudoentropy $n - 2\lambda$ $\longrightarrow$ replace state with min-entropy $n - 2\lambda$
  - ... (iterate)

Application to Our Case

- Ideal permutation: HILL not needed
- Simplifies readability and comprehensibility

Proof Rationale: Typical Sponge/Duplex Proof

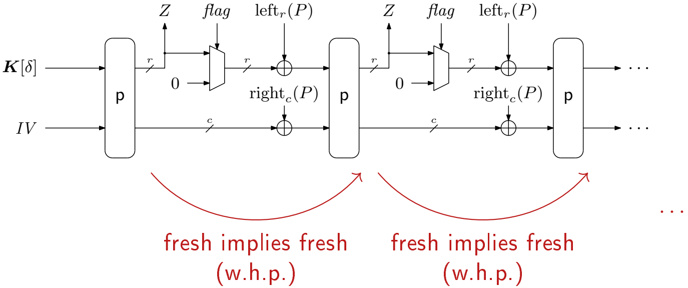


- Add phantom c-bit keys k
- Isolate "Even-Mansour" and analyze simplified construction

Application to Our Case

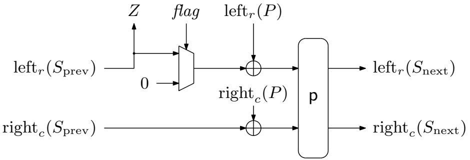
- Tricky in combination with leakage
- Requires explicit split of input and output leakage

Proof Rationale: Our Approach



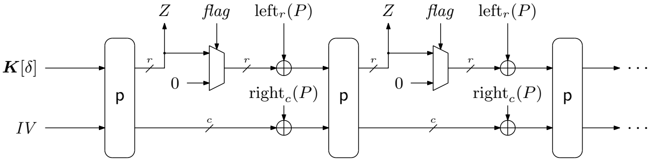
- Inductive reasoning
- Leakage influences min-entropy of states
- Subsequently influences adversarial guessing advantages

Proof Rationale: 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 $\to$ 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

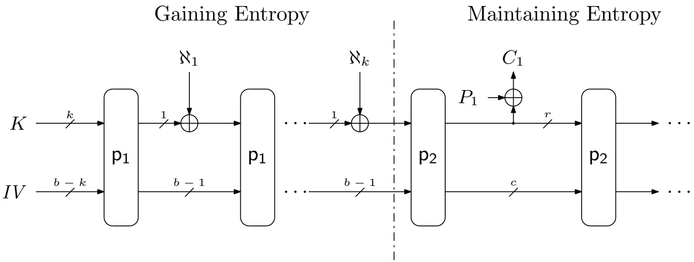
Simplified Security Bound

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

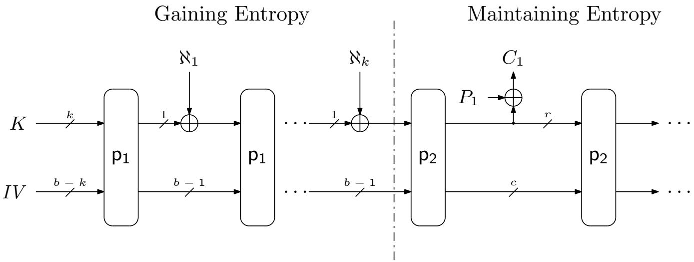
$q_\delta \leq \#$ **allowed** IV**'s**

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

Application: Leakage Resilient Encryption (1)

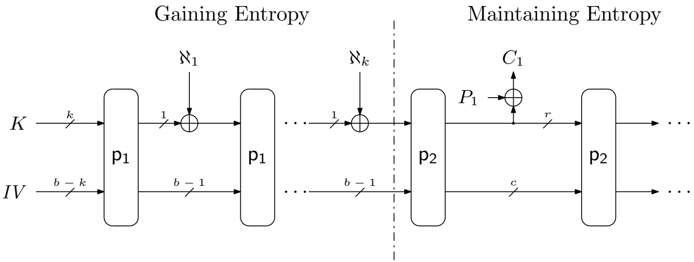


Application: Leakage Resilient Encryption (1)



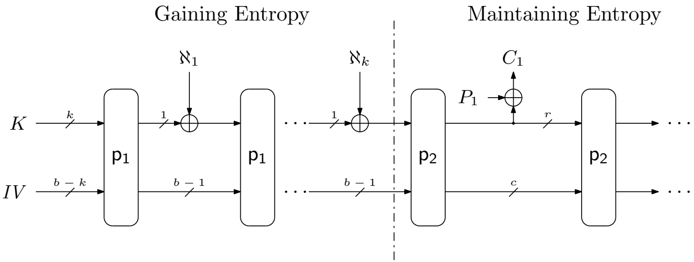
- Gain entropy in KD_1 from nonce at small rate

Application: Leakage Resilient Encryption (1)



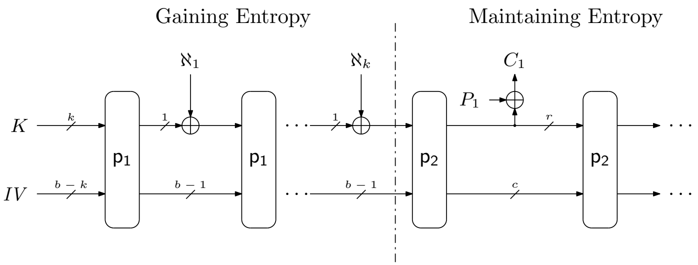
- Gain entropy in KD_1 from nonce at small rate
- Final state of KD_1 has high entropy (w.h.p.)

Application: Leakage Resilient Encryption (1)



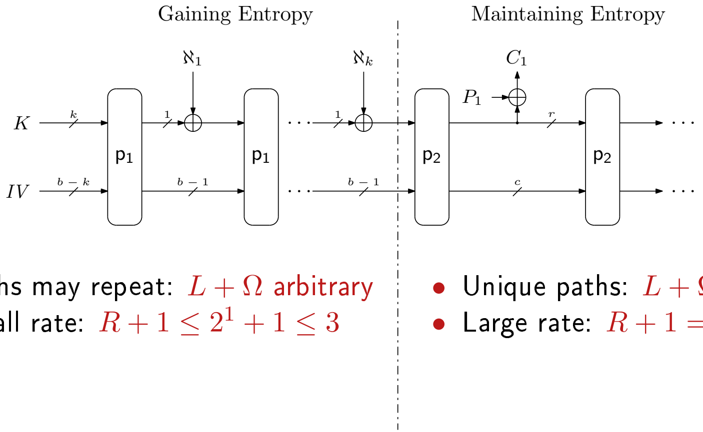
- Gain entropy in KD_1 from nonce at small rate
- Final state of KD_1 has high entropy (w.h.p.)
- Inner part of state of KD_1 forms key to KD_2

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.)

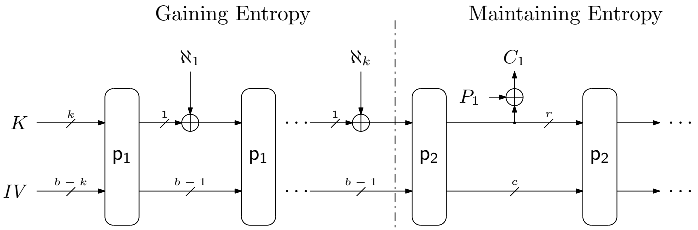
Application: Leakage Resilient Encryption (2)



- 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)



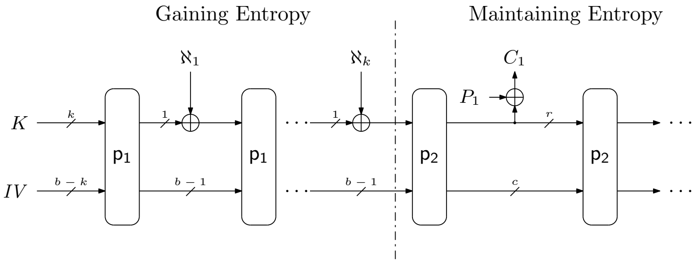
- Paths may repeat: $L + \Omega$ arbitrary
- Small rate: $R + 1 \leq 2^1 + 1 \leq 3$

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

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

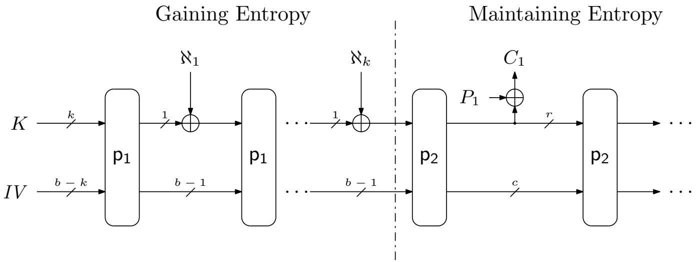
$$\mathbf{Adv}^{\mathrm{naLR}}_{\mathsf{KD}_2}(\mathsf{D}) \lesssim \frac{\nu^M_{r,c} N}{2^{c-2\lambda}} + \frac{QN}{2^{b-4\lambda}} + \frac{N^2}{2^b}$$

Application: Leakage Resilient Encryption (3)



$$\mathbf{Adv}_{\mathcal{E}}^{\text{naLR-cpa}}(\mathsf{D}) = \max_{\mathsf{L}\in\mathcal{L}} \Delta_{\mathsf{D}}\left(\mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K^{\mathsf{L}},\ \mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K,\ \mathsf{p}_1^{\pm},\ \mathsf{p}_2^{\pm}\ ;\ \mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K^{\mathsf{L}},\ \$,\ \mathsf{p}_1^{\pm},\ \mathsf{p}_2^{\pm}\right)$$

Application: Leakage Resilient Encryption (3)



$$\begin{aligned}\mathbf{Adv}_{\mathcal{E}}^{\text{naLR-cpa}}(\mathsf{D}) &= \max_{\mathsf{L}\in\mathcal{L}} \Delta_{\mathsf{D}}\left(\mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K^{\mathsf{L}}\,,\ \mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K\,,\ \mathsf{p}_1^{\pm}\,,\ \mathsf{p}_2^{\pm}\ ;\ \mathcal{E}[\mathsf{p}_1,\mathsf{p}_2]_K^{\mathsf{L}}\,,\ \$\,,\ \mathsf{p}_1^{\pm}\,,\ \mathsf{p}_2^{\pm}\right)\\ &\leq 4\cdot\mathbf{Adv}_{\mathsf{KD}_1}^{\text{naLR}}(\mathsf{D}')+2\cdot\mathbf{Adv}_{\mathsf{KD}_2}^{\text{naLR}}(\mathsf{D}'')\end{aligned}$$

Conclusion

Keyed Duplex

- Leakage resilience: model and analysis
- Building block for leakage resilient ENC/MAC/AE

ISAP

- LWC candidate [DEMMMPU19]
- Sponge/duplex-based authenticated encryption mode
- LR of duplex + LR of suffix sponge [DM19b] $\Longrightarrow$ LR of ISAP mode

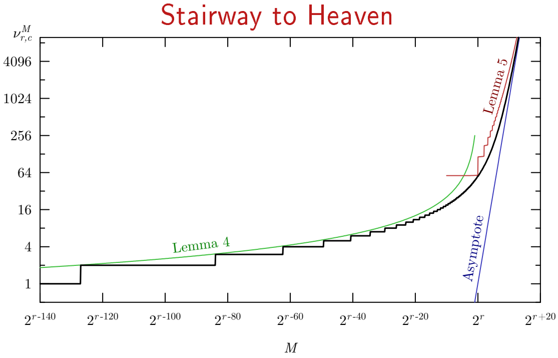
Thank you for your attention!

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

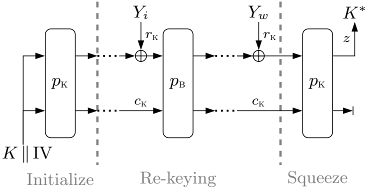
- M balls, 2^r bins
- $\nu_{r,c}^{M}$ is smallest x such that $\Pr\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

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

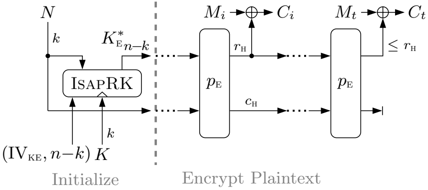
- M balls, 2^r bins
- $\nu_{r,c}^{M}$ is smallest x such that $\Pr\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$
- For $r + c = 256$, $\nu_{r,c}^{M}$ versus proven upper bounds:



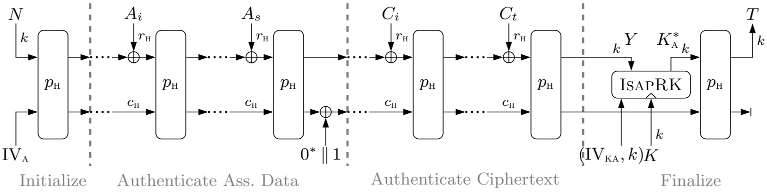
Supporting Slide: Security of ISAP Mode



IsapRK

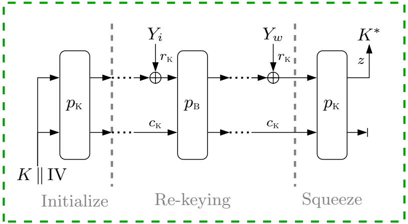


IsapEnc



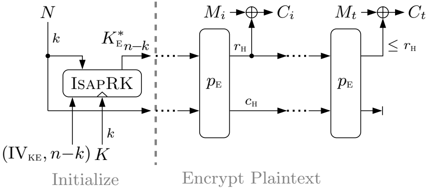
IsapMAC

Supporting Slide: Security of ISAP Mode

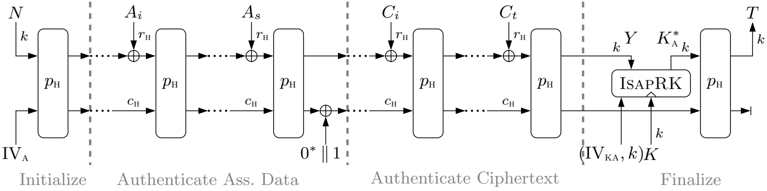


IsapRK

KD_1 with small rate

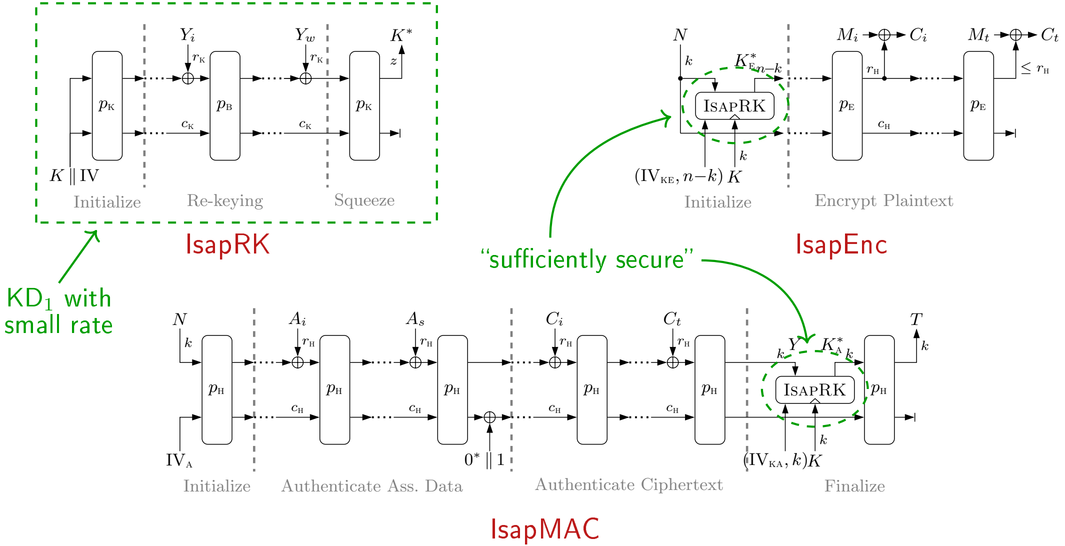


IsapEnc

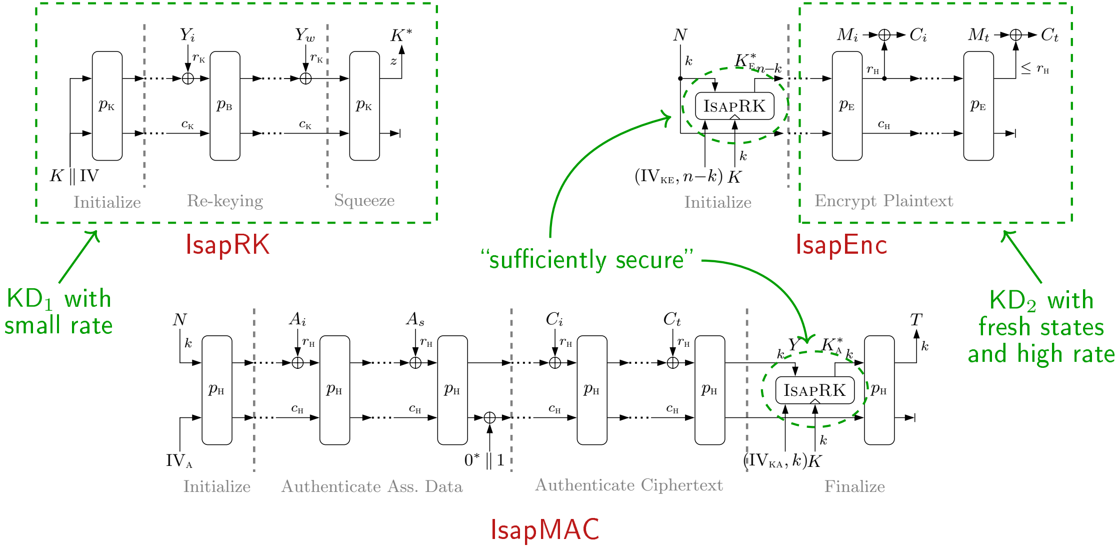


IsapMAC

Supporting Slide: Security of ISAP Mode



Supporting Slide: Security of ISAP Mode



Supporting Slide: Security of ISAP Mode