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 \[\text{[BDPV07]}\]

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

Keyed Sponge

- \( \text{PRF}(K, P) = \text{Sponge}(K \| P) \)
- Message authentication
- Keystream generation
Keying Sponges

Keyed Sponge

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

Keyed Duplex

- Authenticated encryption
- Multiple CAESAR and NIST LWC submissions
Evolution of Keyed Sponges

- Inner-Keyed Sponge \([\text{CDHKN12,ADMV15,NY16}]\)
- Full-Keyed Sponge \([\text{BDPV12,GPT15,MRV15}]\)

- Outer-Keyed Sponge \([\text{BDPV11,ADMV15,NY16,Men18}]\)
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

- **Outer-Keyed Duplex**
- **Full-Keyed Duplex** [MRV15, DMV17]

![Diagram of duplexing process]

- **Unkeyed Duplex** [BDPV11]
Evolution of Keyed Duplexes

- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]
Evolution of Keyed Duplexes

\[ \forall i : z_i \leq r \]

- **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)
- $\Omega$: # 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 the Duplex Construction

Security of the Suffix Keyed Sponge

Application to ISAP

Conclusion
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 $\lambda$ bits of $(S_{\text{prev}}, S_{\text{next}})$
Influence of Leakage

- Suppose $S_{\text{prev}}$ invoked at most $R$ times
- At most $R + 1$ leakages of $S_{\text{prev}}$
- Min-entropy of $S_{\text{prev}}$: 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 $IV$
- $q_{\delta}$: maximum # init calls for single $\delta$
- $L$: # queries with repeated path (e.g., nonce-violation)
- $\Omega$: # 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

\[
\frac{q IV \cdot N}{2^{k-\delta} \lambda} + \frac{(L + \Omega + \nu^{M}_{r,c}) \cdot N}{2^{c-(R+1)\lambda}}
\]
Application: Managing Leakage

Simplified Security Bound

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

\(q_\delta \leq \# \text{ allowed IV’s}\)
Application: Managing Leakage

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

\[ q_{\delta} \leq \# \text{ allowed IV’s} \quad \text{Limit } L + \Omega \text{ or limit } R? \]
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 $\mathbf{KD}_1$ from nonce at small rate
- Final state of $\mathbf{KD}_1$ has high entropy (w.h.p.)
- Inner part of state of $\mathbf{KD}_1$ forms key to $\mathbf{KD}_2$
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: \( R + 1 \leq 2^{1 \log_2 N} + 1 \leq 3 \)
- Unique paths: \( L + \Omega = 0 \)
- Large rate: \( R + 1 = 2 \)

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

\[
\text{Adv}_{\text{KD}_2}^{\text{nalr}}(D) \lesssim \frac{\nu_{r,c}^M N}{2^{c-2\lambda}} + \frac{QN}{2^{b-4\lambda}} + \frac{N^2}{2^b}
\]
Application: Leakage Resilient Encryption (3)

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

Leakage Resilience of the Duplex Construction

Security of the Suffix Keyed Sponge

Application to ISAP

Conclusion
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?
Typical Approach

- Hash function is unkeyed → 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
SuKS versus Full-Kei ded 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
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 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

$$\text{Adv}_{F}^{\text{prf}}(D) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta, \epsilon\}}} + \frac{\nu_{t,b-t}^q \cdot N}{2^{b-t}}$$
Security of SuKS

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

\[
\text{Adv}_{F}^{\text{prf}}(D) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta, \epsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}
\]

inner collision
Security of SuKS

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

$$\text{Adv}^\text{prf}_F(D) \leq \frac{2N^2}{2^c} + \frac{2(N-q)}{2^{\min\{\delta, \epsilon\}}} N + \frac{\nu_{q+b-t} \cdot N}{2^{b-t}}$$

“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

$$\text{Adv}^\text{prf}_F(D) \leq \frac{2N^2}{2^c} + \frac{2(N-q)}{2\min\{\delta, \epsilon\}} \cdot N + \frac{\nu^q_{t, b-t}}{2^{b-t}} \cdot N$$

• “break at $T$”, bounds construction queries with same tag
• “break at $G$”, bounds primitive queries with same inner part
Application to MAC Part of ISAP [DEMMMPU19]
Application to MAC Part of ISAP [DEMMMPU19]

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

- \( \nu_{b-s,s}^{2(N-q)} = \mu_{272,128}^{2129} \leq 3 \)
- \( \nu_{t,b-t}^{q} = \mu_{128,272}^{128} \leq 80 \)

\[ \text{Adv}_{\text{IsapMAC}}^{\text{prf}}(D) \leq \frac{2N^2}{2256} + \frac{3N}{2128} + \frac{80N}{2272} \]
Application to MAC Part of ISAP [DEMMMPU19]

\[(b, c, r, k) = (400, 256, 144, 128)\]

- \(\nu_{b-s,s}^{2(N-q)} = \mu_{272,128}^{2129} \leq 3\)
- \(\nu_{t,b-t}^{q} = \mu_{128,272}^{128} \leq 80\)

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

\[(b, c, r, k) = (320, 256, 64, 128)\]

- \(\nu_{b-s,s}^{2(N-q)} = \mu_{192,128}^{2129} \leq 5\)
- \(\nu_{t,b-t}^{q} = \mu_{128,192}^{128} \leq 67\)

\[\text{Adv}_{\text{IsapMAC}}^{\text{prf}}(D) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{272}}\]
Leakage Resilience of SuKS

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

$$\text{Adv}_{F}^{\text{nahr-prf}}(D) \leq \frac{2N^2}{2c} + \frac{\nu_{s,b-s}^{2(N-q)}(N-q)}{2^{b-s}} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\epsilon\}} - \nu_{s,b-s}^{2(N-q)} \cdot \lambda} + \frac{\nu_{t,b-t}^{2q} \cdot N}{2^{b-t-\lambda}}$$
Leakage Resilience of SuKS

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

$$\text{Adv}_{F}^{\text{nalr-prf}}(D) \leq \frac{2N^2}{2c} + \frac{2(N-q)}{2^{b-s} \nu_{s,b-s}} + \frac{2(N-q)}{2^{b-t} \nu_{t,b-t}} \cdot N + \frac{2q}{2^{b-t-\lambda} \nu_{s,b-s}} \cdot N$$

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
• **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
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix keyed sponge accumulate to the leakage resilience of the suffix keyed sponge security in Section 4. The main result on the mode. The ingredients of keyed duplex security are summarized in Section 3, and those on the then-MAC design.

Encryption

\[ \begin{align*}
K \parallel IV & \\
\text{Initialize} & \\
Y_i & \rightarrow r_k \rightarrow p_K \\
Y_w & \rightarrow r_k \rightarrow p_B \\
& \rightarrow p_k \\
& \rightarrow c_k \\
& \rightarrow \text{Re-keying} \\
Y & \rightarrow K^* \\
& \rightarrow c_k \\
& \rightarrow \text{Squeeze} \\
\end{align*} \]

IsapRK

\[ \begin{align*}
N & \rightarrow k \\
A_i & \rightarrow r_n \rightarrow p_n \\
A_s & \rightarrow r_n \rightarrow p_n \\
C_i & \rightarrow r_n \rightarrow p_n \\
C_t & \rightarrow r_n \rightarrow p_n \\
& \rightarrow 0^* \parallel 1 \\
\text{Initialize} & \\
\text{Authenticate Ass. Data} & \\
\text{Authenticate Ciphertext} & \\
\text{Finalize} & \\
T & \rightarrow k \\
& \rightarrow Y \\
& \rightarrow K^* \\
& \rightarrow (IV_{KA}, k)K \\
\end{align*} \]

IsapMAC

\[ \begin{align*}
N & \rightarrow k \\
K & \rightarrow K_{e_n-k} \\
& \rightarrow (IV_{KB}, n-k)K \\
\text{Initialize} & \\
\text{Encrypt Plaintext} & \\
M_i & \rightarrow C_i \\
M_t & \rightarrow C_t \\
& \leq r_n \\
\end{align*} \]

IsapEnc

Isapauthenticated encryption

(c) IsapMAC

Fig. 1: Isap authenticated encryption
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix keyed sponge accumulate to the leakage resilience of the suffix keyed sponge security in Section 4. The main result on the mode. The ingredients of keyed duplex security are summarized in Section 3, and those on

The hashing capacity satisfies $k \in \{0, 1\}$. It outputs a ciphertext as function of these.

Finally, we remark that Guo et al. (GPPS) [11] independently constructed a security argument for a key

The compression in $\mathcal{H}$ occurs at

where $n$ is sufficiently secure

Security of ISAP Mode

where $n$ is depicted in Figure 1b and message authentication

Authenticated encryption of

Authenticated Ass. Data

Authenticated Ciphertext

Finalize

$K \parallel IV$

Re-keying

Squeeze

Initialize

IsapRK

IsapEnc

IsapMAC
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix accumulate to the leakage resilience of the suffix keyed sponge security in Section 4. The main result on the mode. The ingredients of keyed duplex security are summarized in Section 3, and those on the Isap authenticated encryption.

Security of ISAP Mode

IsapRK with small rate

KD with small rate

IsapEnc

“sufficiently secure”
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix keyed sponge accumulate to the leakage resilience of the suffix keyed sponge in Section 4. The main result on the mode is stated and the ingredients of keyed duplex security are summarized in Section 3, and those on then-MAC design. Encryption IsapEnc comes with four variants, two of which have rate subsequently satisfies $r_k = 1$. The hashing capacity satisfies $k = 1$. The compression in $k = 256$ for all variants, and the hashing specification of is depicted in Figure 1a. We remark that, although we have sticked to the figures of the in Figure 1c. Both functions internally use a rekeying function $r_{k^*}$, with $(IV_{k^*}, n-k) K$. Finally, we remark that Guo et al. (GPPS) [11] independently constructed a security argument for Isap. It follows a different strategy, and henceforth resulted in different bounds $K_1$ with KD1 with small rate $K_2$ with fresh states and high rate "sufficiently secure"
In this brief note, we show how the leakage resilience of the keyed duplex and the leakage resilience of the suffix keyed sponge accumulate to the leakage resilience of the mode. The ingredients of keyed duplex security are summarized in Section 3, and those on the key specification of ISAP comes with four variants, two of which have $K^*$ as parameters, and a message gets as input $K_{K^*}^{\ast}$. Authenticated encryption of Isap gets as input $K_{K^*}^{\ast}$. Authenticated Ass. Data $K_{K^*}^{\ast}$, associated data $K_{K^*}^{\ast}$, and a message $K_{K^*}^{\ast}$. Authenticated Ciphertext $K_{K^*}^{\ast}$, and a message $K_{K^*}^{\ast}$. Finalize

(c) IsapMAC

Fig. 1: Isap authenticated encryption

Security of ISAP Mode

IsapRK

"sufficiently secure"

IsapEnc

KD$_1$ with small rate

KD$_2$ with fresh states and high rate

SuKS

IV$_k$ $|$ $K$

Initialize

Re-keying

Squeeze

$K_e$ $|$ $IV$

$Y_i$ $r_k$

$K^*$ $z$

$K_{K^*}^\ast$

$C$

IsapRK

N $k$

$M_i$ $C_i$

Encrypt Plaintext

$M_t$ $\leq r_n$

$C_t$

IsapEnc

IV$_n$ $| k$

Initialize

Authenticate Ass. Data

Authenticate Ciphertext

(IV$_{K^*}$, $n-k$) $K$

Initialize

Finalize

$T_k$

$K^*$

0$^*$ $\parallel$ 1

IsapMAC

$0^*$ $\parallel$ 1

$0^*$ $\parallel$ 1

$0^*$ $\parallel$ 1
Outline

Leakage Resilience of the Duplex Construction

Security of the Suffix Keyed Sponge

Application to ISAP

Conclusion
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!