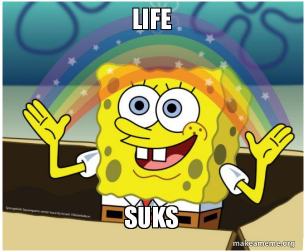
Security of the Suffix Keyed Sponge

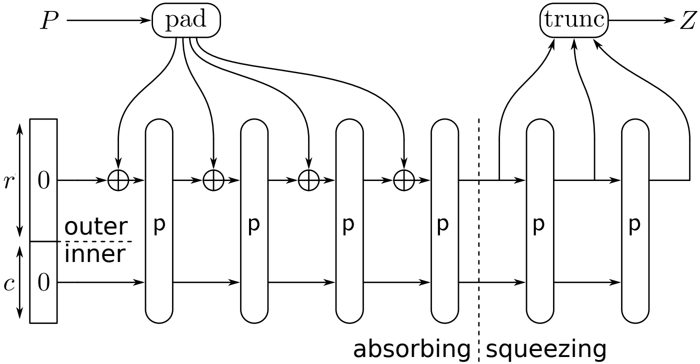


Christoph Dobraunig, Bart Mennink
Radboud University (The Netherlands)

Fast Software Encryption 2020
November 9, 2020

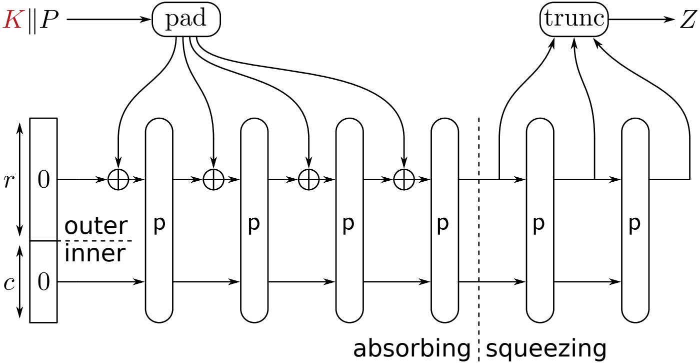
ESCADA

Sponges [BDPV07]



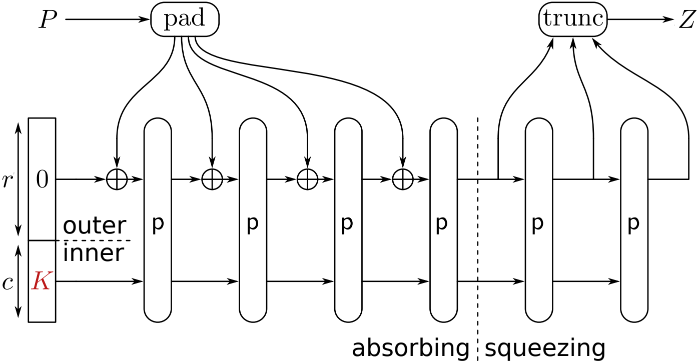
- Cryptographic hash function
- SHA-3, XOFs, lightweight hashing, . . .
- Behaves as RO up to query complexity $\approx 2^{c/2}$ [BDPV08]

Keyed Sponges



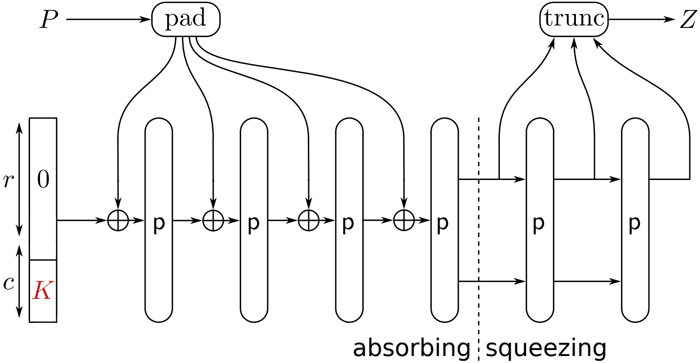
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]

Keyed Sponges



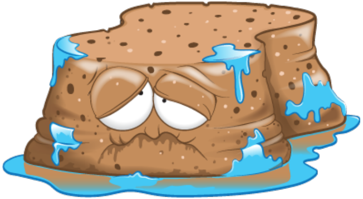
- Outer-Keyed Sponge [BDPV11,ADMV15,NY16,Men18]
- Inner-Keyed Sponge [CDHKN12,ADMV15,NY16]

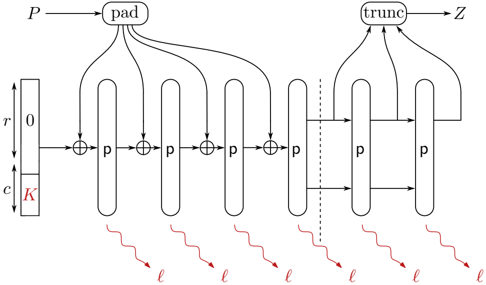
Keyed Sponges



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

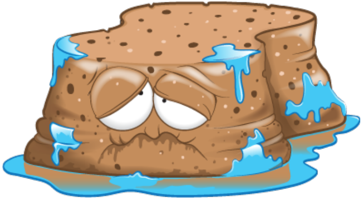
Leakage Resilience of Keyed Sponges

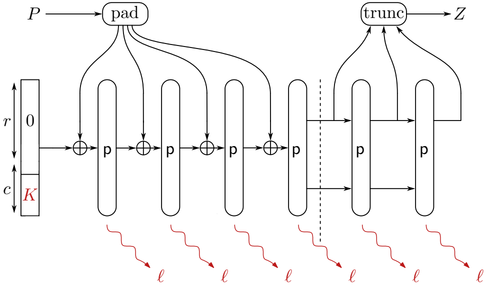




- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

Leakage Resilience of Keyed Sponges

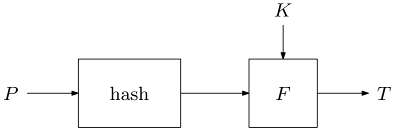




- Permutation p repeatedly evaluated on secret state
- Any evaluation of p may leak information

Minimizing leakage of keyed sponge?

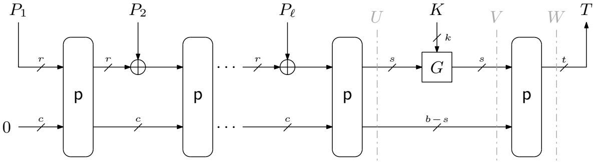
Hash-then-MAC



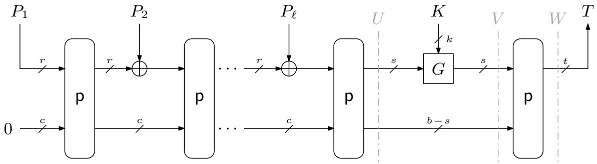
Typical Approach

- Hash function is unkeyed → 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



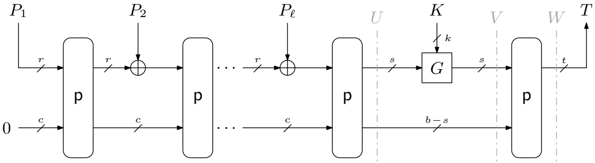
Suffix Keyed Sponge



SuKS versus Full-Keyed Sponge

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

Suffix Keyed Sponge



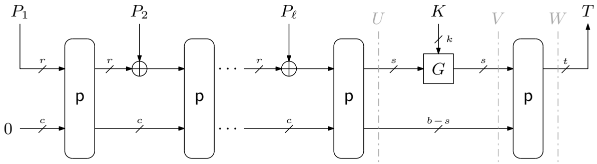
SuKS versus Full-Keyed Sponge

- 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 with Restricted Parameters



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

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SuKS}}(\mathcal{A}) \leq \frac{N^2+N}{2^c} + \frac{N}{2^\delta}$$

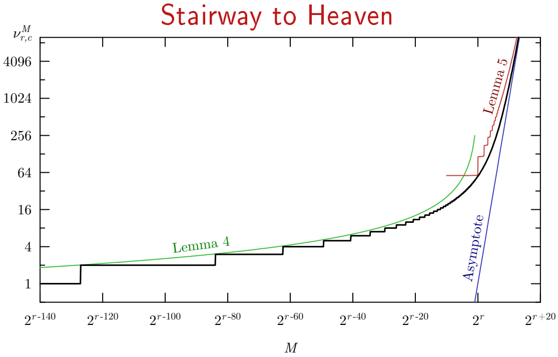
- Proof relies on indifferentiability of sponge [BDPV08]

Intermezzo: Multicollision Limit Function

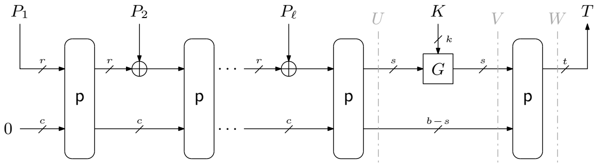
- M balls, 2^r bins
- $\nu_{r,c}^{M}$ is smallest x such that $\Pr\left(|\text{fullest bin}| > x\right) \leq \frac{x}{2^c}$

Intermezzo: Multicollision Limit Function

- 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:



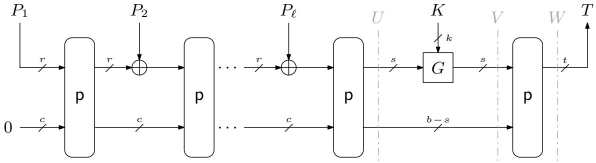
Security of SuKS with Unrestricted Parameters



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

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

Security of SuKS with Unrestricted Parameters

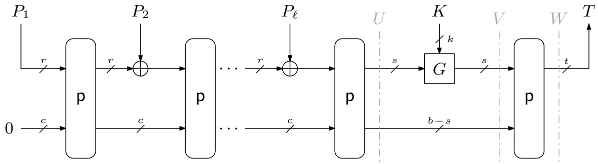


- $k, s, t \le b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

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

inner collision

Security of SuKS with Unrestricted Parameters



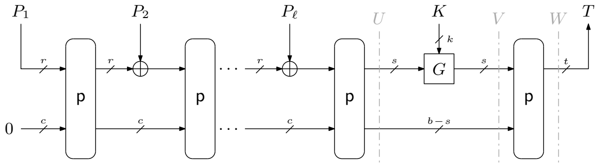
- $k, s, t \leq b$
- G is $2^{-\delta}$-uniform and $2^{-\epsilon}$-universal

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

inner collision

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

Security of SuKS with Unrestricted Parameters



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

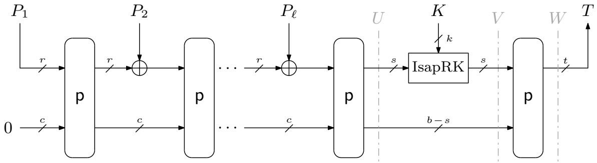
$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^c} + \frac{\nu_{b-s,s}^{2(N-q)} \cdot N}{2^{\min\{\delta,\varepsilon\}}} + \frac{\nu_{t,b-t}^{q} \cdot N}{2^{b-t}}$$

inner collision

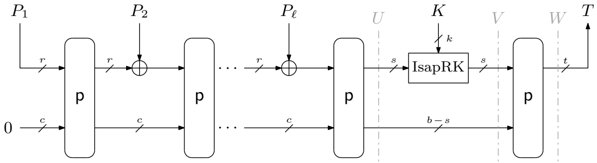
"break at T", bounds construction queries with same tag

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

Application to MAC Part of ISAP [DEMMMPU19]



Application to MAC Part of ISAP [DEMMMPU19]

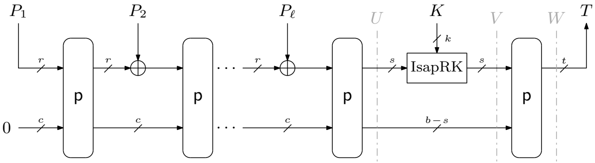


$(b, c, r, k) = (400, 256, 144, 128)$

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

$$\mathbf{Adv}_{\mathrm{IsapMAC}}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{3N}{2^{128}} + \frac{80N}{2^{272}}$$

Application to MAC Part of ISAP [DEMMMPU19]



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

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

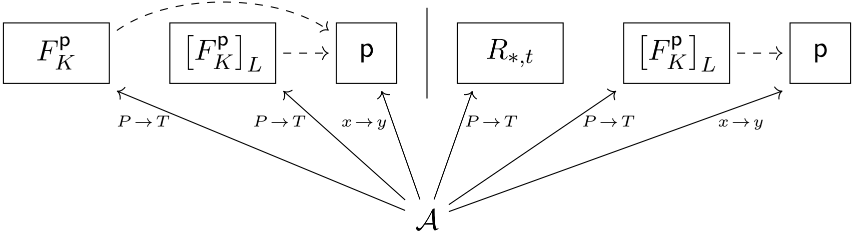
$$\mathbf{Adv}_{\mathrm{IsapMAC}}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{3N}{2^{128}} + \frac{80N}{2^{272}}$$

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

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

$$\mathbf{Adv}_{\mathrm{IsapMAC}}^{\mathrm{prf}}(\mathcal{A}) \leq \frac{2N^2}{2^{256}} + \frac{5N}{2^{128}} + \frac{67N}{2^{192}}$$

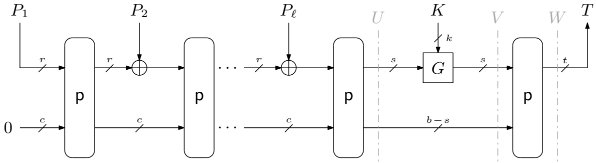
Leakage Resilience



$$\mathbf{Adv}_F^{\text{nalr-prf}}(\mathcal{A}) = \max_{L \in \mathcal{L}} \Delta_{\mathcal{A}} \left(\left[F_K^{\mathsf{p}}\right]_L, F_K^{\mathsf{p}}, \mathsf{p} \, ; \, \left[F_K^{\mathsf{p}}\right]_L, R_{*,t}, \mathsf{p} \right)$$

- Non-adaptive leakage resilience
- Bounded leakage model

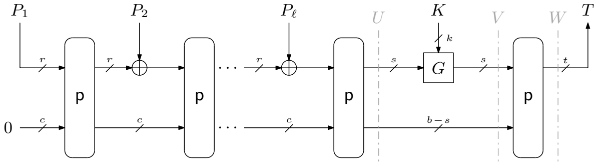
Leakage Resilience of SuKS



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

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

Leakage Resilience of SuKS



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

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

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

Conclusion

Suffix Keyed Sponge

- Easy-to-protect message authentication
- Strong security bound
- Beneficial over full-keyed sponge and Hash-then-MAC

ISAP

- Uses suffix keyed sponge for message authentication
- Leakage resilient AE security of ISAP follows from [DM19a] and [DM19b]

Thank you for your attention!