Key Prediction Security of Keyed Sponges

Bart Mennink
Radboud University (The Netherlands)

Fast Software Encryption 2019
March 26, 2019
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]
Keyed Sponges

- **Outer-Keyed Sponge** [BDPV11, ADMV15, NY16]
- **Inner-Keyed Sponge** [CDHKKN12, ADMV15, NY16]
Keyed Sponges

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

- $F \in \{\text{OKS, FKS}\}$
Security of Keyed Sponge

\[ F \in \{\text{OKS, FKS}\} \]

- \( M \): data (construction) complexity
- \( N \): time (primitive) complexity

\[ \frac{M^2}{2^c} + \frac{MN}{2^c} + \text{Adv}_{F}^{\text{key-pre}}(N) \]

Diagram: Sponge function with keys and messages.
Security of Keyed Sponge

- $F \in \{\text{OKS}, \text{FKS}\}$
- $M$: data (construction) complexity
- $N$: time (primitive) complexity

Simplified Security Bound

$$\frac{M^2}{2^c} + \frac{MN}{2^c} + \text{Adv}^\text{key-pre}_F(N)$$

probability that adversary predicts key
Adv$_F^{key-pre}(N)$

- Adversary makes $N$ queries to $\pi$
- Key $K$ randomly drawn
- Adversary wins if query history “covers $K$”
Key Prediction Security: Existing Bounds

**One Key Block**
- Adversary makes $N$ queries
- Query history covers at most $N$ keys

\[ \text{Adv}^\text{key-pre}_F(N) \leq \frac{N}{2^k} \]
Key Prediction Security: Existing Bounds

One Key Block
- Adversary makes $N$ queries
- Query history covers at most $N$ keys

More Than One Key Block
- By Gaži et al. [GPT15]
- Used in many sponge proofs

$\text{Adv}^{\text{key-pre}}_F(N) \leq \frac{N}{2^k}$

$\text{Adv}^{\text{key-pre}}_F(N) \lesssim \frac{b^\lambda N}{2^{k/2}}$
Key Prediction Security: Implication for OKS

Case of \((b, c, r, k) = (320, 256, 64, 64)\)

\[
\frac{M^2}{2^c} + \frac{MN}{2^c} + \frac{N}{2^k} = \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{64}}
\]

Case of \((b, c, r, k) = (320, 256, 64, 128)\)

\[
\frac{M^2}{2^c} + \frac{MN}{2^c} + \frac{N}{2^{k/2}} = \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{64}}
\]
Adv_{key-pre}^F(N) \lesssim \frac{c^{\lambda-1}N}{2^k}

- Loss $c$ due to lucky multi-collisions (in old bound: $b$)
- $2^k$ in denominator (in old bound: $2^{k/2}$)
- Best attack: around $2^k$ queries
Proof Idea

- Tree-based approach (as in [GPT15])
Proof Idea

- Tree-based approach (as in [GPT15])

\[ V_0 \xrightarrow{L} V_1 \xrightarrow{u} V_3 \]
Proof Idea

- Tree-based approach (as in [GPT15])

![Diagram of tree-based approach](image-url)
Proof Idea

- Tree-based approach (as in [GPT15])
Proof Idea

- Tree-based approach (as in [GPT15])
Proof Idea

- Tree-based approach (as in [GPT15])

---

goal: bound # paths from $V_0$ to $V_3$
Proof Idea

- Fix any query from $V_2$ to $V_3$: $N$ options
Proof Idea

- Fix any query from $V_2$ to $V_3$: $N$ options
- This query fixes inner part of second-last layer

Consider configurations for these layers

Arrows indicate query direction, circles indicate inner collisions

Inductive reasoning on non-occurrence of $\alpha_i$-fold collisions
Proof Idea

- Fix any query from $V_2$ to $V_3$: $N$ options
- This query fixes inner part of second-last layer

Consider configurations for these layers
- Arrows indicate query direction, circles indicate inner collisions
Proof Idea

- Fix any query from $V_2$ to $V_3$: $N$ options
- This query fixes inner part of second-last layer

Consider configurations for these layers
- Arrows indicate query direction, circles indicate inner collisions
- Inductive reasoning on non-occurrence of $\alpha^i$-fold collisions
Further Application to Duplex

- **Unkeyed Duplex** [BDPV11]

![Diagram of Duplexing Process](attachment:image.png)
Further Application to Duplex

- Unkeyed Duplex [BDPV11]
- Outer-Keyed Duplex [BDPV11]
Further Application to Duplex

∀i : \( \tau_i \leq r \)

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

Bounds Reduce Bi-Directionally [MRV15, DMV17]

\[
\begin{align*}
\text{OKS and OKD:} & \quad \frac{M^2}{2^c} + \frac{MN}{2^c} + \text{Adv}_{\text{key-pre}}^{\text{OKS}}(N) \\
\text{FKS and FKD:} & \quad \frac{M^2}{2^c} + \frac{MN}{2^c} + \text{Adv}_{\text{key-pre}}^{\text{FKS}}(N)
\end{align*}
\]

Same for Nonce-Respecting Setting [JLM14, DMV17]

\[
\begin{align*}
\text{OKS and OKD:} & \quad \frac{M^2}{2^b} + \frac{N}{2^c} + \text{Adv}_{\text{key-pre}}^{\text{OKS}}(N) \\
\text{FKS and FKD:} & \quad \frac{M^2}{2^b} + \frac{N}{2^c} + \text{Adv}_{\text{key-pre}}^{\text{FKS}}(N)
\end{align*}
\]
Application to CAESAR

CAESAR Competition

- Four third-round candidates based on duplex

<table>
<thead>
<tr>
<th>scheme</th>
<th>b</th>
<th>c</th>
<th>r</th>
<th>k</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascon [DEMS16]</td>
<td>320</td>
<td>256</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>320</td>
<td>192</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Ketje [BDP+16]</td>
<td>200</td>
<td>184</td>
<td>16</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>400</td>
<td>368</td>
<td>32</td>
<td>128</td>
</tr>
<tr>
<td>Keyak [BDP+16]</td>
<td>800</td>
<td>256</td>
<td>544</td>
<td>128..224</td>
</tr>
<tr>
<td></td>
<td>1600</td>
<td>256</td>
<td>1344</td>
<td>128..224</td>
</tr>
<tr>
<td>NORX [AJN16]</td>
<td>512</td>
<td>128</td>
<td>384</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td>256</td>
<td>768</td>
<td>256</td>
</tr>
</tbody>
</table>
Application to CAESAR

CAESAR Competition

- Four third-round candidates based on duplex

<table>
<thead>
<tr>
<th>scheme</th>
<th>$b$</th>
<th>$c$</th>
<th>$r$</th>
<th>$k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ascon [DEMS16]</td>
<td>320</td>
<td>256</td>
<td>64</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>320</td>
<td>192</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Ketje [BDP+16]</td>
<td>200</td>
<td>184</td>
<td>16</td>
<td>92</td>
</tr>
<tr>
<td></td>
<td>400</td>
<td>368</td>
<td>32</td>
<td>128</td>
</tr>
<tr>
<td>Keyak [BDP+16]</td>
<td>800</td>
<td>256</td>
<td>544</td>
<td>128..224</td>
</tr>
<tr>
<td></td>
<td>1600</td>
<td>256</td>
<td>1344</td>
<td>128..224</td>
</tr>
<tr>
<td>NORX [AJN16]</td>
<td>512</td>
<td>128</td>
<td>384</td>
<td>128</td>
</tr>
<tr>
<td></td>
<td>1024</td>
<td>256</td>
<td>768</td>
<td>256</td>
</tr>
</tbody>
</table>

- Initialize entire state using key (FKS for key)
1.4 Mode of Operation

The mode of operation of Ascon is based on duplex sponge modes like MonkeyDuplex [13], but uses a stronger keyed initialization and keyed finalization function. The core permutations $p^a$ and $p^b$ operate on a sponge state $S$ of size 320 bits, with a rate of $r$ bits and a capacity of $c = 320 - r$ bits. For a more convenient notation, the rate and capacity parts of the state $S$ are denoted by $S_r$ and $S_c$, respectively. The encryption and decryption operations are illustrated in Figure 1a and Figure 1b and specified in Algorithm 1.
Application to CAESAR Portfolio: Ascon-128 Parameters*  

Old Bound (Simplified)

\[ \frac{M^2}{2^{320}} + \frac{N}{2^{256}} + \frac{N}{2^{64}} \]

- If \( M \leq 2^{160} \), security as long as \( N \leq 2^{64} \)

New Bound (Simplified)

\[ \frac{M^2}{2^{320}} + \frac{N}{2^{256}} + \frac{N}{2^{128}} \]

- If \( M \leq 2^{160} \), security as long as \( N \leq 2^{128} \)

* Reasoning does not apply to Ascon-128 itself
STROBE Protocol Framework [Ham17]

- Lightweight framework for network protocols
- Goal: simple framework with small code size
Application to STROBE

**STROBE Protocol Framework [Ham17]**

- Lightweight framework for network protocols
- Goal: simple framework with small code size
- Hashing, authentication, and encryption: all using sponge and outer-keyed sponge/duplex
Application to STROBE

STROBE Protocol Framework [Ham17]

- Lightweight framework for network protocols
- Goal: simple framework with small code size
- Hashing, authentication, and encryption: all using sponge and outer-keyed sponge/duplex

<table>
<thead>
<tr>
<th>scheme</th>
<th>$b$</th>
<th>$c$</th>
<th>$r$</th>
<th>$k$</th>
</tr>
</thead>
<tbody>
<tr>
<td>STROBE-128/1600</td>
<td>1600</td>
<td>256</td>
<td>1344</td>
<td>256</td>
</tr>
<tr>
<td>STROBE-256/1600</td>
<td>1600</td>
<td>512</td>
<td>1088</td>
<td>256</td>
</tr>
<tr>
<td>STROBE-128/800</td>
<td>800</td>
<td>256</td>
<td>544</td>
<td>256</td>
</tr>
<tr>
<td>STROBE-256/800</td>
<td>800</td>
<td>512</td>
<td>288</td>
<td>256</td>
</tr>
<tr>
<td>STROBE-128/400</td>
<td>400</td>
<td>256</td>
<td>144</td>
<td>256</td>
</tr>
</tbody>
</table>
Application to STROBE-128/400

Old Bound (Simplified)

\[ \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{128}} \]

- If \( M \leq 2^{100} =: 2^a \), security as long as \( N \leq 2^{128} \)

New Bound (Simplified)

\[ \frac{M^2}{2^{256}} + \frac{MN}{2^{256}} + \frac{N}{2^{256}} \]

- If \( M \leq 2^{100} =: 2^a \), security as long as \( N \leq 2^{156} \)
Conclusion

Tight Key Prediction Security
- Last “missing link” in keyed sponge proofs
- Close to optimal bound

Applications
- Every use of outer-keyed sponge/duplex with $k > r$
- HMAC-SHA-3 [NY16] and sandwich sponge [Nai16]
- STROBE protocol framework
- Lightweight permutations

Thank you for your attention!