Full-State Keyed Duplex With Built-In Multi-User Support

Joan Daemen, Bart Mennink, Gilles Van Assche

Radboud University (The Netherlands),
STMicroelectronics (Belgium)

ASIACRYPT 2017
December 6, 2017
Sponges [BDPV07]

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

**Keyed Sponge**

- \( \text{PRF}(K, M) = \text{Sponge}(K \parallel M) \)
- Message authentication
- Keystream generation
Keying the Sponges

**Keyed Sponge**

- PRF($K, M$) = Sponge($K || M$)
- Message authentication
- Keystream generation

**Keyed Duplex**

- Authenticated encryption
- Multiple CAESAR submissions
Evolution of Keyed Sponges

- Outer Keyed Sponge [BDPV11, ADMV15, NY16]
Evolution of Keyed Sponges

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

- **Outer Keyed Sponge** [BDPV11, ADMV15, NY16]
- **Inner Keyed Sponge** [CDHKN12, ADMV15, NY16]
- **Full-State 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

\( \forall i : z_i \leq r \)

- Unkeyed Duplex [BDPV11]
- Outer Keyed Duplex [BDPV11]
- Full-State Keyed Duplex [MRV15]
Full-State Keyed Duplex [MRV15]

∀i : \( z_i \leq r \)

\[
\begin{align*}
\sigma_0 & \quad Z_0 \\
\text{pad} & \quad \text{trunc}_{z_0} \\
\sigma_1 & \quad Z_1 \\
\text{pad} & \quad \text{trunc}_{z_1} \\
\sigma_2 & \quad Z_2 \\
\text{pad} & \quad \text{trunc}_{z_2} \\
\end{align*}
\]

initialize \quad duplexing \quad duplexing \quad duplexing

\[
\begin{align*}
0 & \quad f & \quad f & \quad f \\
\end{align*}
\]

\[
\text{Security} \approx \frac{\mu N}{2^k} + \frac{M^2}{2^c}
\]

- \( M \): data complexity (calls to construction)
- \( N \): time complexity (calls to primitive)
- \( \mu \leq 2M \): multiplicity ("maximum outer collision of \( f \)")
Full-State Keyed Duplex [MRV15]

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

\[
\begin{array}{cccc}
\sigma_0 & Z_0 & \text{pad} & \text{trunc}_{z_0} \\
\sigma_1 & Z_1 & \text{pad} & \text{trunc}_{z_1} \\
\sigma_2 & Z_2 & \text{pad} & \text{trunc}_{z_2} \\
\end{array}
\]

\[ r \]

\[ c \]

initialize \hspace{1cm} duplexing \hspace{1cm} duplexing \hspace{1cm} duplexing

Security \approx \frac{\mu N}{2^k} + \frac{M^2}{2^c}

- \( M \): data complexity (calls to construction)
- \( N \): time complexity (calls to primitive)
- \( \mu \leq 2M \): multiplicity (“maximum outer collision of \( f \)”)

similar bound for full-state keyed sponge
Full-State Keyed Duplex \cite{MRV15}

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

\[
\sigma_0 Z_0 \quad \sigma_1 Z_1 \quad \sigma_2 Z_2
\]

\[
pad\quad \text{trunc}_{z_0}\quad pad\quad \text{trunc}_{z_1}\quad pad\quad \text{trunc}_{z_2}
\]

\[
 minden initialize\quadplexing\quadplexing\quadplexing\quad ...
\]

Limitations

- Dominating term \(\mu N/2^k\) rather than \(\mu N/2^c\)
- Multiplicity \(\mu\) only known a posteriori
- No multi-user security
- Limited flexibility in modeling adversarial power
New Core: Full-State Keyed Duplex

Features

- Multi-user by design: index $\delta$ specifies key in array
- Initial state: concatenation of $K[\delta]$ and $iv$
- Full-state absorption, no padding
- Re-phasing: $f, Z, \sigma$ instead of $\sigma, f, Z$
- Refined adversarial strength
Security Result

Security \approx \frac{q_{iv}N}{2^k} + \frac{(L + \Omega + \nu_{r,c}M)N}{2^c}

- $M$: data complexity (calls to construction)
- $N$: time complexity (calls to primitive)
- $q_{iv}$: max \# init queries with same 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
Multicollision Coefficient $\nu_{r,c}^M$

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

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

Stairway to Heaven
Security in Hybrid Argument

[Diagram with symbols and arrows representing the flow of data and processes related to security in a hybrid argument context.]
Security in Hybrid Argument

\[(\delta, \text{iv}) \sigma \]

\[\text{Path} \rightarrow \mathcal{RO} \]

\[x \quad y \]

\[f \]
Security in Hybrid Argument

$f$ irrelevant; security of random duplex
Security in Hybrid Argument

\( \text{(δ, iv)} \sigma \)

Path \( \mathcal{R} \) \( \mathcal{O} \)

\( f \) irrelevant; security of random duplex
Security in Hybrid Argument

boils down to security of three $f$-based oracles

$f$ irrelevant; security of random duplex
Application to Full-State Keyed Sponge

- Overwrites possible and no nonce restriction
- $L + \Omega \leq M/2$, $\nu_{r,c}^M$ is negligible, $q_{iv} \leq u$

\[
\text{Security} \approx \frac{uN}{2^k} + \frac{MN}{2^c}
\]

- Improves [MRV15]: better bound and multi-user support
Application to Authenticated Encryption

General Bound (Nonce-Violating)

- $L + \Omega \leq M/2$
- $\nu_{r,c}^M$ is negligible

$$\text{Security} \approx \frac{q_{iv}N}{2^k} + \frac{MN}{2^c}$$
Application to Authenticated Encryption

General Bound (Nonce-Violating)

- \( L + \Omega \leq M/2 \)
- \( \nu_{r,c}^M \) is negligible

\[
\text{Security} \approx \frac{q_{iv}N}{2^k} + \frac{MN}{2^c}
\]

Nonce-Respecting and No RUP

- \( L = \Omega = 0 \)
- Second term dominated by \( \nu_{r,c}^M \)

\[
\text{Security} \approx \frac{q_{iv}N}{2^k} + \nu_{r,c}^M \frac{N}{2^c}
\]
Application to Authenticated Encryption

- Security strength if $Mr \leq 2^a$:

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Parameters</th>
<th>nonce-violating</th>
<th>nonce-respecting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ketje Jr.</td>
<td>200 184 16</td>
<td>189–a</td>
<td>min{196–a, 177}</td>
</tr>
<tr>
<td>Sr.</td>
<td>400 368 32</td>
<td>374–a</td>
<td>min{396–a, 360}</td>
</tr>
<tr>
<td>Ascon 128</td>
<td>320 256 64</td>
<td>263–a</td>
<td>min{317–a, 248}</td>
</tr>
<tr>
<td>Ascon 128a</td>
<td>320 192 128</td>
<td>200–a</td>
<td>min{318–a, 184}</td>
</tr>
<tr>
<td>NORX 32</td>
<td>512 128 384</td>
<td>137–a</td>
<td>127</td>
</tr>
<tr>
<td>NORX 64</td>
<td>1024 256 768</td>
<td>266–a</td>
<td>255</td>
</tr>
<tr>
<td>Keyak River</td>
<td>800 256 544</td>
<td>266–a</td>
<td>255</td>
</tr>
<tr>
<td>Keyak Lake</td>
<td>1600 256 1344</td>
<td>267–a</td>
<td>255</td>
</tr>
</tbody>
</table>
Conclusion

Full-Stated Keyed Duplex

- Versatile primitive
- Flexible bound covering many use cases
- Makes life easier for sponge mode designer

Looking Forward

- Generalized FSKD found adoption in Keyak v2
- Further applications of tight multi-collision analysis

Thank you for your attention!
Conclusion

Full-Stated Keyed Duplex

- Versatile primitive
- Flexible bound covering many use cases
- Makes life easier for sponge mode designer

Looking Forward

- Generalized FSKD found adoption in Keyak v2
- Further applications of tight multi-collision analysis

Thank you for your attention!
Supporting Slides

SUPPORTING SLIDES
Comparison of Schemes

- “Pure bound” means that derived security bound is expressed purely as a function of the adversary’s capabilities.

<table>
<thead>
<tr>
<th></th>
<th>Full state absorption</th>
<th>Extendable output</th>
<th>Multi-target</th>
<th>Pure bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bertoni et al. [BDPV11]</td>
<td>—</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Bertoni et al. [BDPV11]</td>
<td>—</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Chang et al. [CDHKN12]</td>
<td>—</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Andreeva et al. [ADMV15]</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
</tr>
<tr>
<td>Gaži et al. [GPT15]</td>
<td>✓</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Mennink et al. [MRV15]</td>
<td>✓</td>
<td>✓</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Naito and Yasuda [NY16]</td>
<td>—</td>
<td>✓</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>This work</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>