Updates on Elephant

Tim Beyne\textsuperscript{1}, Yu Long Chen\textsuperscript{1}, Christoph Dobr"{a}unig\textsuperscript{2}, Bart Mennink\textsuperscript{2}

\textsuperscript{1} KU Leuven (Belgium) \quad \textsuperscript{2} Radboud University (The Netherlands)

NIST Lightweight Cryptography Workshop 2020
October 19, 2020
Our goal: minimize state size and complexity of design while still meeting expected security strength and limit on online complexity.

Lightweight Authenticated Encryption

- nonce-based?
- suitable primitive
- RUP/LR/...?
- math beyond primitive
- hardware/software
- parallelism
Lightweight Authenticated Encryption

Our goal: minimize state size and complexity of design while still meeting expected security strength $2^{112}$ and limit on online complexity $2^{50}$ bytes.
Permutation is the best suited choice

What Primitive?

Tweakable Block Cipher  Block Cipher  Permutation
What Primitive?

Tweakable Block Cipher  Block Cipher  Permutation

Permutation is the best suited choice
Our Approach

• Parallel evaluation of the permutation \( \rightarrow \) requires proper masking
• Evaluating it in forward direction only \( \rightarrow \) requires proper mode of use
• Goal: minimize permutation size

\[
\begin{align*}
\text{What Mode?} \\
\text{Established Approach} \\
\quad \text{• Keyed duplex/sponge} \\
\quad \quad [\text{BDPV11, MRV15, DMV17}] \\
\quad \text{• Inherently sequential}
\end{align*}
\]
What Mode?

Established Approach

• Keyed duplex/sponge
  [BDPV11,MRV15,DMV17]
• Inherently sequential

Our Approach

• Parallel evaluation of the permutation
  → requires proper masking
• Evaluating it in forward direction only
  → requires proper mode of use
• Goal: minimize permutation size
What Mask?

Simplified Version of MEM [GJMN16]

- $\varphi_1$ is fixed LFSR, $\varphi_2 = \varphi_1 \oplus \text{id}$
- $\text{mask}_{K}^{a,b} = \varphi_2^b \circ \varphi_1^a \circ P(K\|0^{n-k})$
What Mask?

Simplified Version of MEM [GJMN16]

- $\varphi_1$ is fixed LFSR, $\varphi_2 = \varphi_1 \oplus \text{id}$
- $\text{mask}^{a,b}_K = \varphi_2^b \circ \varphi_1^a \circ P(K\|0^{n-k})$

Features

- Constant-time
- Simple to implement
- More efficient than alternatives
Elephant Authenticated Encryption Mode

$$\text{mask}_{a,b}^K = \varphi_2^b \circ \varphi_1^a \circ P(K\|0^{n-k})$$

$$\text{mask}_{K}^{0,0}$$

$$P$$

$$N\|0^{n-m}$$

$$\text{mask}_{K}^{0,0}$$

$$P$$

$$N\|0^{n-m}$$

$$M_1$$

$$C_1$$

$$\ldots$$

$$M_{\ell_M}$$

$$C_{\ell_M}$$

$$\text{mask}_{K}^{\ell_M-1,0}$$

$$P$$

$$\text{mask}_{0,1}$$

$$P$$

$$\text{mask}_{K}^{\ell_C-1,1}$$

$$P$$

$$A_1$$

$$A_{\ell_A}$$

$$C_1$$

$$C_{\ell_C}$$

$$\text{mask}_{K}^{\ell_A-1,2}$$

$$\text{mask}_{K}^{0.2}$$

$$P$$

$$\text{mask}_{K}^{\ell_C-1,1}$$

$$P$$

$$\text{mask}_{K}^{\ell_A-1,2}$$

$$\text{mask}_{K}^{0.2}$$

$$P$$

$$\ldots$$

$$\ldots$$

$$[\cdot]_t \rightarrow T$$

$$\text{mask}_{K}^{0.1}$$

$$\text{mask}_{K}^{\ell_C-1,1}$$

$$\text{mask}_{K}^{\ell_A-1,2}$$

$$\text{mask}_{K}^{0.2}$$

$$P$$

$$\text{mask}_{K}^{\ell_C-1,1}$$

$$P$$

$$\text{mask}_{K}^{\ell_A-1,2}$$

$$\text{mask}_{K}^{0.2}$$

$$P$$
Elephant Authenticated Encryption Mode

Encryption

- Nonce $N$ input to all $P$ calls
- $K$ and counter in mask
- Padding $M_1 \ldots M_{\ell M} \leftarrow M$
- Ciphertext $C \leftarrow [C_1 \ldots C_{\ell M}]_M$
Elephant Authenticated Encryption Mode

Encryption

- Nonce $N$ input to all $P$ calls
- $K$ and counter in mask
- Padding $M_1 \ldots M_{\ell_M} \leftarrow M$
- Ciphertext $C \leftarrow [C_1 \ldots C_{\ell_M}]_M$

Authentication

- Padding $A_1 \ldots A_{\ell_A} \leftarrow N||A||1$
- Padding $C_1 \ldots C_{\ell_C} \leftarrow C||1$
- $K$ and counter in mask
- Tag $T$ truncated to $t$ bits
Elephant Authenticated Encryption Mode

Mode Properties

- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

\[
\text{mask}_{K}^{a,b} = \varphi_{2}^{b} \circ \varphi_{1}^{a} \circ P(K||0^{n-k})
\]

\[
m_{i}^{0,0} \xrightarrow{} \text{mask}_{K}^{0,0} \xrightarrow{} \text{P} \xrightarrow{} M_{1} \xrightarrow{} C_{1} \xrightarrow{} \ldots \xrightarrow{} M_{\ell M} \xrightarrow{} C_{\ell M}
\]

\[
m_{i}^{0,1} \xrightarrow{} \text{mask}_{K}^{0,1} \xrightarrow{} \text{P} \xrightarrow{} \cdot \cdot \cdot \xrightarrow{} \cdot \cdot \cdot \xrightarrow{} [.]_{t} \xrightarrow{} T
\]
Elephant Authenticated Encryption Mode

\[ \text{mask}^a_b = \varphi^b_2 \circ \varphi^a_1 \circ P(K||0^{n-k}) \]

Mode Properties
- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties
- Mask can be easily updated
Elephant Authenticated Encryption Mode

Mode Properties

- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties

- Mask can be easily updated
- \( \text{mask}_{K}^{i,0} = \varphi_{1} \circ \text{mask}_{K}^{i-1,0} \)
Elephant Authenticated Encryption Mode

Mode Properties

- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive $P$
- $P$ in forward direction only

Mask Properties

- Mask can be easily updated
- $\text{mask}^{i-1,0}_K = \varphi_1 \circ \text{mask}^{i-1,0}_K$
- $\text{mask}^{i-1,0}_K \oplus \text{mask}^{i-1,1}_K = \text{mask}^{i,0}_K$

$\text{mask}^{a,b}_K = \varphi_b \circ \varphi_1 \circ P(K||0^{n-k})$
Security of Mode

\[ \text{Adv}_{\text{Elephant}}^{\text{ae}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n} \]

- \( \sigma \) is online complexity, \( p \) is offline complexity
- Assumptions:
  - \( P \) is random permutation
  - \( \varphi_1 \) has maximal length and \( \varphi_2^b \circ \varphi_1^a \neq \varphi_2^{b'} \circ \varphi_1^{a'} \) for \((a, b) \neq (a', b')\)
  - \( \mathcal{A} \) is nonce-based adversary
Security of Mode

\[ \text{Adv}_{\text{Elephant}}^{\text{ae}}(A) \lesssim \frac{4\sigma p}{2^n} \]

- \( \sigma \) is online complexity, \( p \) is offline complexity
- Assumptions:
  - \( P \) is random permutation
  - \( \varphi_1 \) has maximal length and \( \varphi_2^b \circ \varphi_1^a \neq \varphi_2^{b'} \circ \varphi_1^{a'} \) for \( (a, b) \neq (a', b') \)
  - \( A \) is nonce-based adversary

Parameters of NIST lightweight call can be met with a 160-bit permutation!
Dumbo

- Spongent-$\pi$[160]
- Minimalist design
  - Time complexity $2^{112}$
  - Data complexity $2^{46}$

Instantiation
Delirium

• Keccak-f

• High security

• Time complexity $2^{127}$

• Data complexity $2^{70}$

• Specified in NIST standard

Instantiation

Dumbo

• Spongent-$\pi[160]$

• Minimalist design
  • Time complexity $2^{112}$
  • Data complexity $2^{46}$

Jumbo

• Spongent-$\pi[176]$

• Conservative design
  • Time complexity $2^{127}$
  • Data complexity $2^{46}$

• ISO/IEC standardized
Instantiation

Dumbo
- Spongent-$\pi$[160]
- Minimalist design
  - Time complexity $2^{112}$
  - Data complexity $2^{46}$

Jumbo
- Spongent-$\pi$[176]
- Conservative design
  - Time complexity $2^{127}$
  - Data complexity $2^{46}$
- ISO/IEC standardized

Delirium
- Keccak-$f$[200]
- High security
  - Time complexity $2^{127}$
  - Data complexity $2^{70}$
- Specified in NIST standard
Technical Specification of Instances

<table>
<thead>
<tr>
<th>instance</th>
<th>$k$</th>
<th>$m$</th>
<th>$n$</th>
<th>$t$</th>
<th>$P$</th>
<th>$\varphi_1$</th>
<th>expected security strength</th>
<th>limit on online complexity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dumbo</td>
<td>128</td>
<td>96</td>
<td>160</td>
<td>64</td>
<td>80-round Spongent-$\pi$[160]</td>
<td>$\varphi_{\text{Dumbo}}$</td>
<td>$2^{112}$</td>
<td>$2^{50}/(n/8)$</td>
</tr>
<tr>
<td>Jumbo</td>
<td>128</td>
<td>96</td>
<td>176</td>
<td>64</td>
<td>90-round Spongent-$\pi$[176]</td>
<td>$\varphi_{\text{Jumbo}}$</td>
<td>$2^{127}$</td>
<td>$2^{50}/(n/8)$</td>
</tr>
<tr>
<td>Delirium</td>
<td>128</td>
<td>96</td>
<td>200</td>
<td>128</td>
<td>18-round Keccak-$f$[200]</td>
<td>$\varphi_{\text{Delirium}}$</td>
<td>$2^{127}$</td>
<td>$2^{74}/(n/8)$</td>
</tr>
</tbody>
</table>

- All LFSRs operate on 8-bit words:
  \[
  \begin{align*}
  \varphi_{\text{Dumbo}} : (x_0, \ldots, x_{19}) & \mapsto (x_1, \ldots, x_{19}, x_0 \lll 3 \oplus x_3 \lll 7 \oplus x_{13} \gg 7) \\
  \varphi_{\text{Jumbo}} : (x_0, \ldots, x_{21}) & \mapsto (x_1, \ldots, x_{21}, x_0 \lll 1 \oplus x_3 \lll 7 \oplus x_{19} \gg 7) \\
  \varphi_{\text{Delirium}} : (x_0, \ldots, x_{24}) & \mapsto (x_1, \ldots, x_{24}, x_0 \lll 1 \oplus x_2 \lll 1 \oplus x_{13} \ll 1)
  \end{align*}
  \]

- All have maximal length and $\varphi_2^b \circ \varphi_1^a \neq \varphi_2^{b'} \circ \varphi_1^{a'}$ for $(a, b) \neq (a', b')$
Tweak Proposal

\[ \text{mask}_{K}^{a,b} = \varphi_{2}^{b} \circ \varphi_{1}^{a} \circ P(K||0^{n-k}) \]
Tweak Proposal

\[ \text{mask}_{K}^{a,b} = \varphi_{2}^{b} \circ \varphi_{1}^{a} \circ P(K||0^{n-k}) \]

Changes to v1

- Authentication via protected counter sum
- Slight change in roles of mask parameters
Tweak Proposal

\[ \text{mask}^{a,b}_K = \varphi^b_2 \circ \varphi^a_1 \circ P(K||0^{n-k}) \]

**Changes to v1**
- Authentication via protected counter sum
- Slight change in roles of mask parameters

**Security and Efficiency**
- v2 retains all good properties of v1
- Bonus: authenticity under nonce-reuse
Tweak Proposal: Security in a Nutshell

\[ \text{mask}_{K}^{a,b} = \varphi_{2}^{b} \circ \varphi_{1}^{a} \circ P(K||0^{n-k}) \]

---

<table>
<thead>
<tr>
<th>Security</th>
<th>Elephant v1.1</th>
<th></th>
<th>Elephant v2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>confidentiality</td>
<td>authenticity</td>
<td>confidentiality</td>
</tr>
<tr>
<td>nonce-respecting</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>nonce-misuse</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
</tbody>
</table>
Implementation Update

• Implementations of Elephant can and should exploit parallelism so far only used in Delirium implementation of Campos et al. [CJL+20] (unoptimized Keccak-f)

• New parallel reference implementation for Delirium
  • Processes up to 8 blocks in parallel using modified Keccak-f[1600] implementation
  • Speedup between 8 and 80 (depending on compilation options)
  • Other word sizes: same approach with different number of blocks

  https://github.com/TimBeyne/Elephant

• Dumbo and Jumbo
  • Hardware: exploit parallelism to achieve better trade-offs
  • Software: bitslicing (reuse techniques developed for Present and GIFT)
Conclusion

Elephant

- Parallel lightweight AE with small state
- Mode: provably secure in random permutation model
- Primitives: standardized and well-studied
- Dumbo and Jumbo for hardware
- Delirium for software

Thank you for your attention!