Dumbo, Jumbo, and Delirium: Parallel AEAD for the Lightweight Circus

Tim Beyne\textsuperscript{1}, Yu Long Chen\textsuperscript{1}, Christoph Dobraunig\textsuperscript{2}, Bart Mennink\textsuperscript{2}

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

NIST Lightweight Cryptography Workshop 2019
November 6, 2019
Authenticated Encryption

Encryption

No outsider can learn anything about data

Authentication

No outsider can manipulate data

Authenticated Encryption

A

B

2 / 14
Authenticated Encryption
Authenticated Encryption

Encryption

- No outsider can learn anything about data
Authenticated Encryption

Encryption
- No outsider can learn anything about data

Authentication
- No outsider can manipulate data
Authenticated Encryption

- Ciphertext $C$ encryption of message $M$
- Tag $T$ authenticates associated data $A$ and message $M$
Authenticated Encryption

- Ciphertext $C$ encryption of message $M$
- Tag $T$ authenticates associated data $A$ and message $M$
- Nonce $N$ randomizes the scheme
Authenticated Decryption

- Authenticated decryption needs to satisfy that
  - Message disclosed if tag is correct
  - Message is not leaked if tag is incorrect
Authenticated Decryption

- Authenticated decryption needs to satisfy that
  - Message disclosed if tag is **correct**
  - Message is not leaked if tag is **incorrect**
Authenticated Decryption

- Authenticated decryption needs to satisfy that
  - Message disclosed if tag is correct
  - Message is not leaked if tag is incorrect
- Correctness: $AD_k(N, A, AE_k(N, A, M)) = M$
Our goal: minimize state size and complexity of design while still meeting expected security strength and limit on online complexity by 50 bytes.

Lightweight Authenticated Encryption

nonce-based? suitable primitive

RUP/LR/...? math beyond primitive

hardware/software parallelism
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.
What Primitive?

- **Tweakable Block Cipher**
- **Block Cipher**
- **Permutation**
What Primitive?

Tweakable Block Cipher  Block Cipher  Permutation

Permutation is the best suited choice
What Mode?

Established Approach

- Keyed duplex/sponge
  [BDPV11, MRV15, DMV17]
- Inherently sequential
What Mode?

Established Approach

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

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
What Mask?

**Simplified Version of MEM [GJMN16]**

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

**Simplified Version of MEM [GJMN16]**

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

**Features**

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

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

\[ \begin{align*}
\text{mask}_{K}^{0,0} & \rightarrow P \\
M_1 & \rightarrow C_1 \\
\ldots & \\
M_{\ell_M} & \rightarrow C_{\ell_M}
\end{align*} \]

\[ \begin{align*}
\text{mask}_{K}^{0,1} & \rightarrow P \\
\text{mask}_{K}^{0,2} & \rightarrow P \\
\ldots & \\
\text{mask}_{K}^{\ell_M-1,1} & \rightarrow P
\end{align*} \]

\[ \cdot \cdot \cdot \rightarrow T \]
Elephant Authenticated Encryption Mode

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

**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 $M_1 \ldots M_{\ell_M} \leftarrow^n M$
- Ciphertext $C \leftarrow [C_1 \ldots C_{\ell_M}]_M$

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

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

Mode Properties

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

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

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**

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

**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
- \(\text{mask}_K^{i,0} = \varphi_1 \circ \text{mask}_K^{i-1,0}\)
Elephant Authenticated Encryption Mode

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

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
- \( \text{mask}^{i,0}_K = \varphi^i_1 \circ \text{mask}^{i-1,0}_K \)
- \( \text{mask}^{i-1,0}_K \oplus \text{mask}^{i-1,1}_K = \text{mask}^{i,0}_K \)
Security of Mode

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

- \( \sigma \) is online complexity, \( p \) is offline complexity
- Assumptions:
  - \( P \) is random permutation
  - \( \varphi_1 \) has maximal length and \( \varphi^b_2 \circ \varphi^a_1 \neq \varphi^{b'}_2 \circ \varphi^{a'}_1 \) 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!
Instantiation

- Spongent-π\([160]\]
- Minimalist design
  - Time complexity \(2^{112}\)
  - Data complexity \(2^{46}\)
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 \(2^{70}\)
- NIST standardized
## Technical Specification of Instances

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

- All LFSRs operate on 8-bit words:
  - $\varphi_{\text{Dumbo}}: (x_0, \ldots, x_{19}) \mapsto (x_1, \ldots, x_{19}, x_0 \lll 3 \oplus x_{3} \lll 7 \oplus x_{13} \ggg 7)$
  - $\varphi_{\text{Jumbo}}: (x_0, \ldots, x_{21}) \mapsto (x_1, \ldots, x_{21}, x_0 \lll 1 \oplus x_{3} \lll 7 \oplus x_{19} \ggg 7)$
  - $\varphi_{\text{Delirium}}: (x_0, \ldots, x_{24}) \mapsto (x_1, \ldots, x_{24}, x_0 \lll 1 \oplus x_{2} \lll 1 \oplus x_{13} \lll 1)$

- All have maximal length and $\varphi_{b}^{b} \circ \varphi_{a}^{a} \neq \varphi_{b}^{b'} \circ \varphi_{a}^{a'}$ for $(a, b) \neq (a', b')$
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!