Dumbo, Jumbo, and Delirium: Parallel Authenticated Encryption for the Lightweight Circus

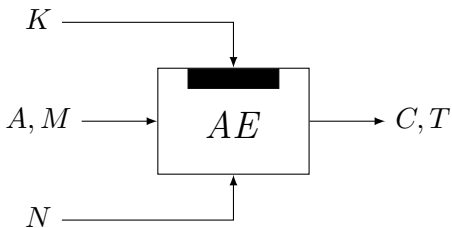
Tim Beyne[1], Yu Long Chen[1], Christoph Dobraunig[2], Bart Mennink[2]

[1] KU Leuven (Belgium) [2] Radboud University (The Netherlands)

Fast Software Encryption 2020
November 9, 2020

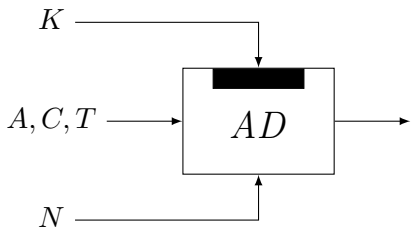
Authenticated Encryption

Authenticated Encryption



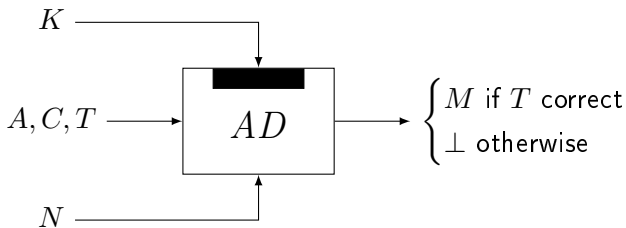
- Ciphertext C encryption of message M
- Tag T authenticates associated data A and message M
- Nonce N randomizes the scheme

Authenticated Decryption



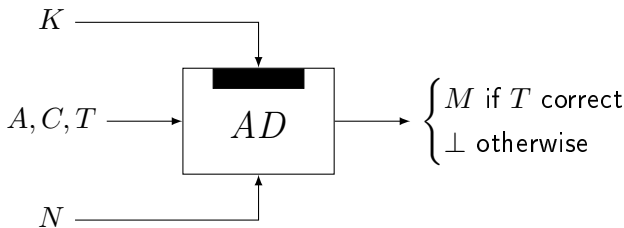
- Authenticated decryption needs to satisfy that

Authenticated Decryption



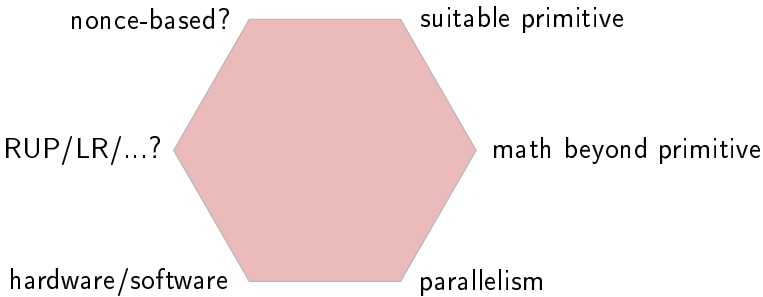
- Authenticated decryption needs to satisfy that
  - Message disclosed if tag is correct
  - Message is not leaked if tag is incorrect

Authenticated Decryption

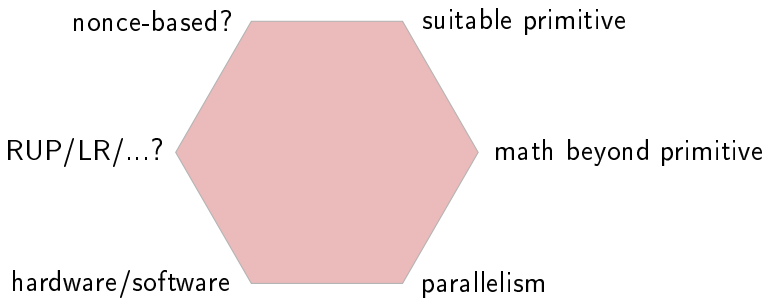


- Authenticated decryption needs to satisfy that
  - Message disclosed if tag is correct
  - Message is not leaked if tag is incorrect
- Correctness: $AD_k(N, A, AE_k(N, A, M)) = M$

Lightweight Authenticated Encryption



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

What Primitive?

Tweakable Block Cipher

Block Cipher

Permutation

What Primitive?

Tweakable Block Cipher

Block Cipher

Permutation

What Primitive?

Tweakable Block Cipher

Block Cipher

Permutation

What Primitive?

Tweakable Block Cipher

Block Cipher

Permutation

What Primitive?

Tweakable Block Cipher

Block Cipher

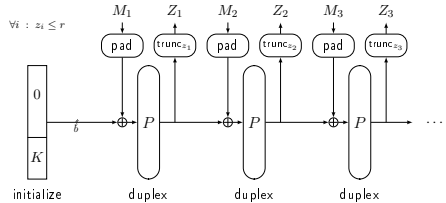
Permutation

Permutation is the best suited choice

What Mode?

Established Approach

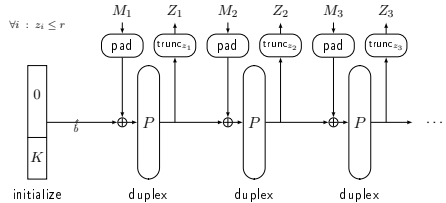
- Keyed duplex/sponge [BDPV11,MRV15,DMV17]
- Inherently sequential



What Mode?

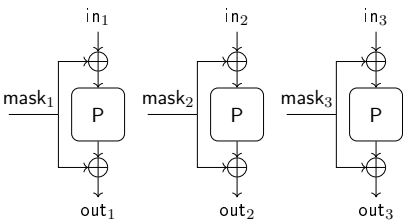
Established Approach

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



Our Approach

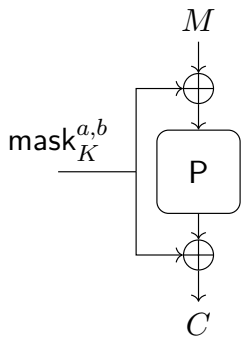
- Parallel evaluation of the permutation
  $\rightarrow$ requires proper masking
- Evaluating it in forward direction only
  $\rightarrow$ requires proper mode of use
- Goal: minimize permutation size



What Mask?

Simplified Version of MEM [GJMN16]

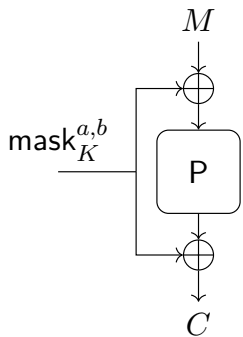
- φ_1 is fixed LFSR, $\varphi_2 = \varphi_1 \oplus \mathsf{id}$
- $\mathsf{mask}_K^{a,b} = \varphi_2^b \circ \varphi_1^a \circ \mathsf{P}(K \| 0^{n-k})$



What Mask?

Simplified Version of MEM [GJMN16]

- φ_1 is fixed LFSR, $\varphi_2 = \varphi_1 \oplus \mathsf{id}$
- $\mathsf{mask}_K^{a,b} = \varphi_2^b \circ \varphi_1^a \circ \mathsf{P}(K \| 0^{n-k})$

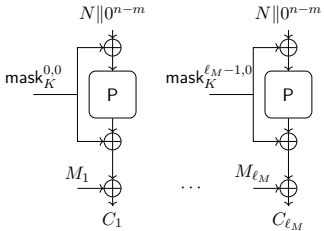


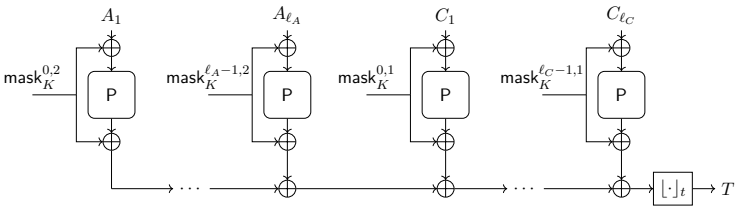
Features

- Constant-time
- Simple to implement
- More efficient than alternatives

Elephant Authenticated Encryption Mode

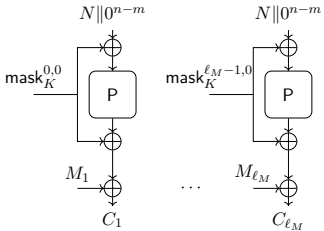
$$\mathsf{mask}_K^{a,b} = \varphi_2^b \circ \varphi_1^a \circ \mathsf{P}(K \| 0^{n-k})$$





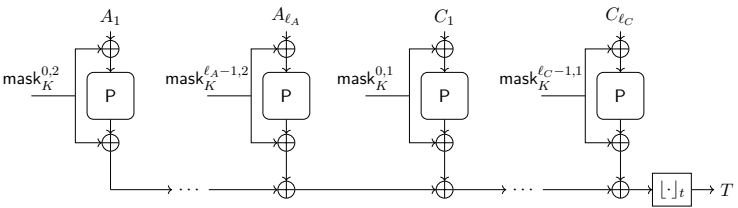
Elephant Authenticated Encryption Mode

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



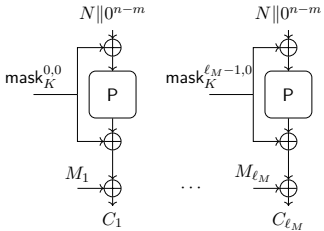
Encryption

- Nonce N input to all P calls
- K and counter in mask
- Padding $M_1 \dots M_{\ell_M} \xleftarrow{n} M$
- Ciphertext $C \leftarrow \lfloor C_1 \dots C_{\ell_M} \rfloor_{|M|}$



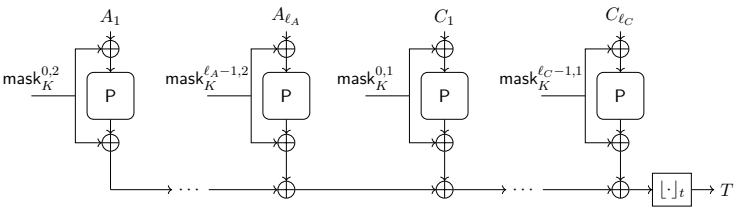
Elephant Authenticated Encryption Mode

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



Encryption

- Nonce N input to all P calls
- K and counter in mask
- Padding $M_1 \dots M_{\ell_M} \xleftarrow{n} M$
- Ciphertext $C \leftarrow \lfloor C_1 \dots C_{\ell_M} \rfloor_{|M|}$

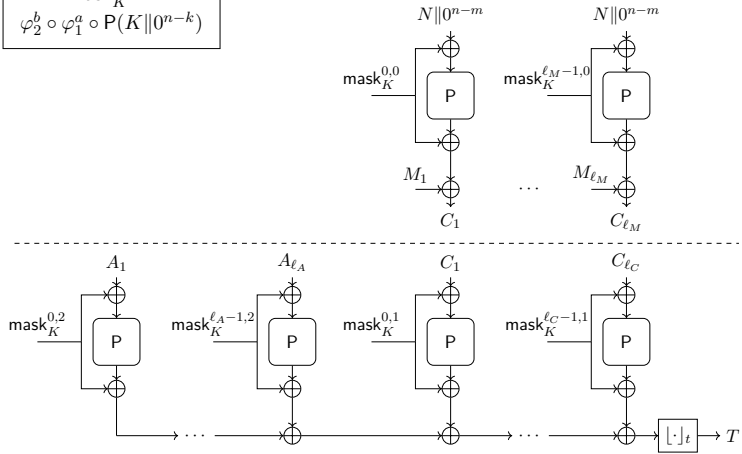


Authentication

- Padding $A_1 \dots A_{\ell_A} \xleftarrow{n} N\|A\|1$
- Padding $C_1 \dots C_{\ell_C} \xleftarrow{n} C\|1$
- K and counter in mask
- Tag T truncated to t bits

Elephant Authenticated Encryption Mode

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

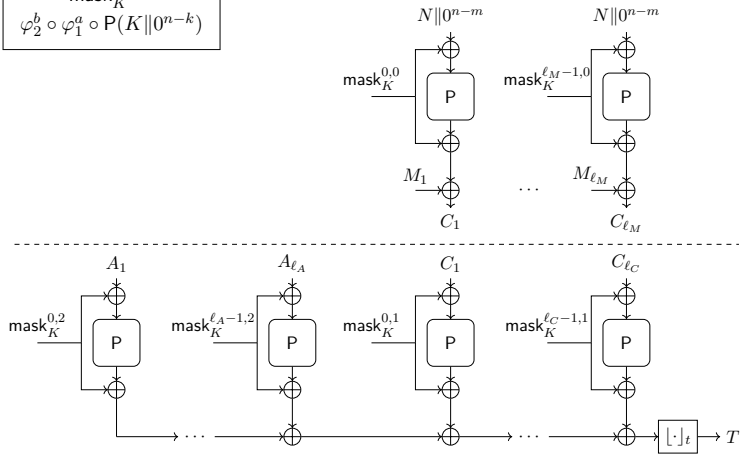


Mode Properties

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

Elephant Authenticated Encryption Mode

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



Mode Properties

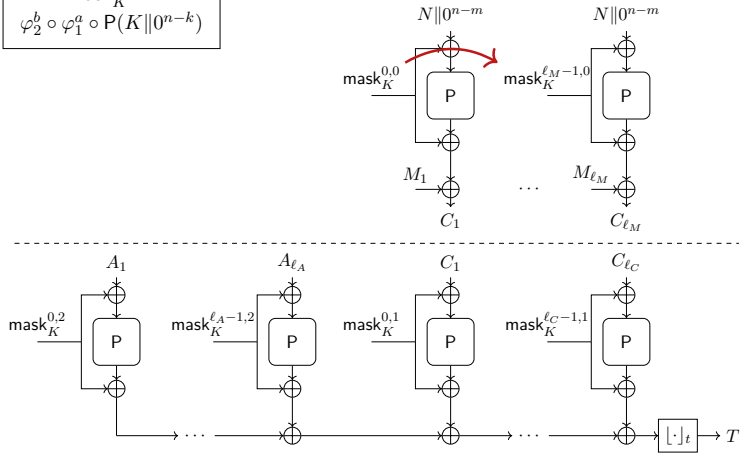
- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties

- Mask can be easily updated

Elephant Authenticated Encryption Mode

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



Mode Properties

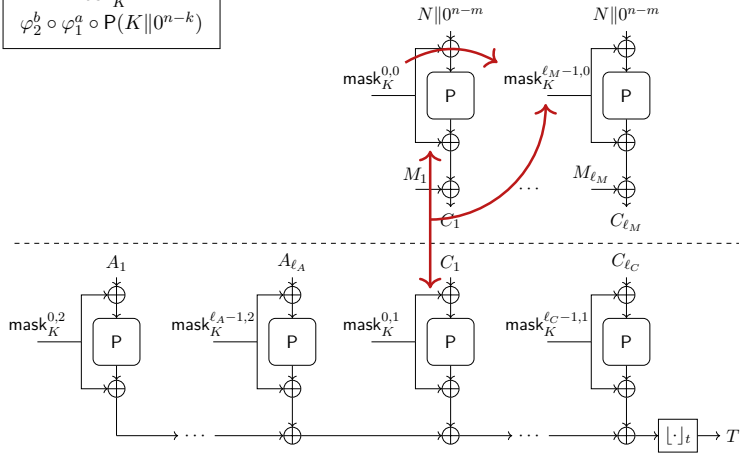
- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties

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

Elephant Authenticated Encryption Mode

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



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
- $\mathsf{mask}_K^{i,0} = \varphi_1 \circ \mathsf{mask}_K^{i-1,0}$
- $\mathsf{mask}_K^{i-1,0} \oplus \mathsf{mask}_K^{i-1,1} = \mathsf{mask}_K^{i,0}$

Security of Mode

$$\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{Elephant}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n}$$

- σ is online complexity, p is offline complexity
- Assumptions:
  - P is random permutation
  - φ_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

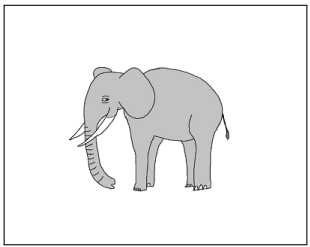
Security of Mode

$$\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{Elephant}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n}$$

- σ is online complexity, p is offline complexity
- Assumptions:
  - P is random permutation
  - φ_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

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

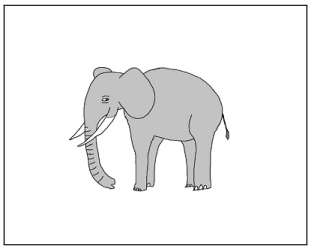
Instantiation



Dumbo

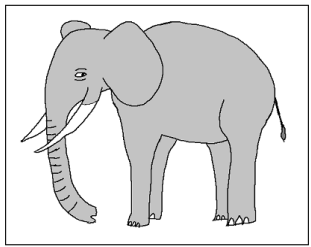
- Spongent-$\pi[160]$
- Minimalist design
  - Time complexity 2^{112}
  - Data complexity 2^{46}

Instantiation



Dumbo

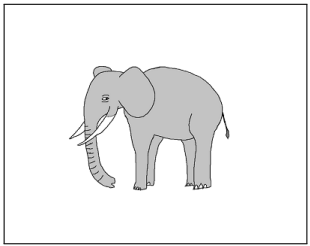
- Spongent-$\pi[160]$
- Minimalist design
  - Time complexity 2^{112}
  - Data complexity 2^{46}



Jumbo

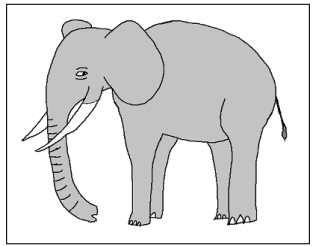
- Spongent-$\pi[176]$
- Conservative design
  - Time complexity 2^{127}
  - Data complexity 2^{46}
- ISO/IEC standardized

Instantiation



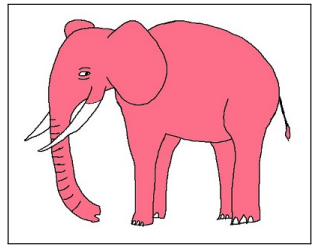
Dumbo

- 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}
- Specified in NIST standard

Technical Specification of Instances

instance	k	m	n	t	P	φ_1	expected security strength	limit on online complexity
Dumbo	128	96	160	64	80-round Spongent-π[160]	φ_{Dumbo}	2^{112}	$2^{50}/(n/8)$
Jumbo	128	96	176	64	90-round Spongent-π[176]	φ_{Jumbo}	2^{127}	$2^{50}/(n/8)$
Delirium	128	96	200	128	18-round Keccak-f[200]	$\varphi_{\text{Delirium}}$	2^{127}	$2^{74}/(n/8)$

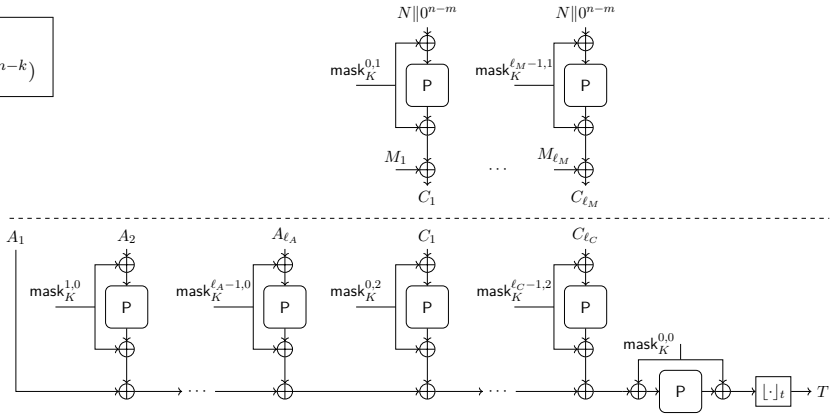
- All LFSRs operate on 8-bit words:

$$\varphi_{\text{Dumbo}}\colon (x_0,\ldots,x_{19}) \mapsto (x_1,\ldots,x_{19},x_0 \lll 3 \oplus x_3 \ll 7 \oplus x_{13} \gg 7)$$
$$\varphi_{\text{Jumbo}}\colon (x_0,\ldots,x_{21}) \mapsto (x_1,\ldots,x_{21},x_0 \lll 1 \oplus x_3 \ll 7 \oplus x_{19} \gg 7)$$
$$\varphi_{\text{Delirium}}\colon (x_0,\ldots,x_{24}) \mapsto (x_1,\ldots,x_{24},x_0 \lll 1 \oplus x_2 \lll 1 \oplus x_{13} \ll 1)$$

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

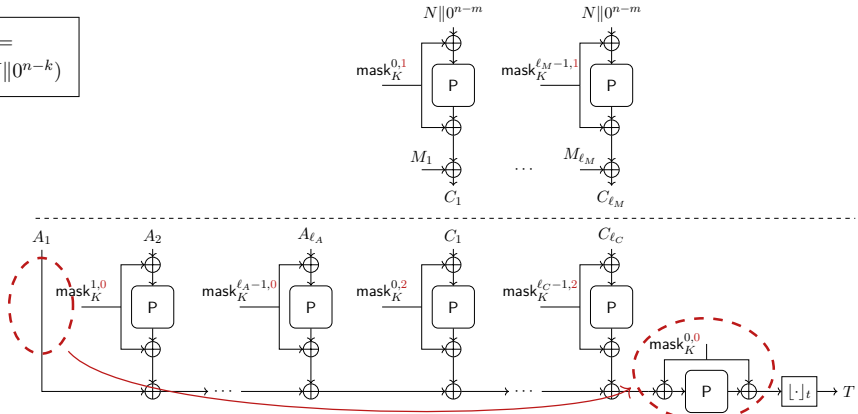
Tweak Proposal

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



Tweak Proposal

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

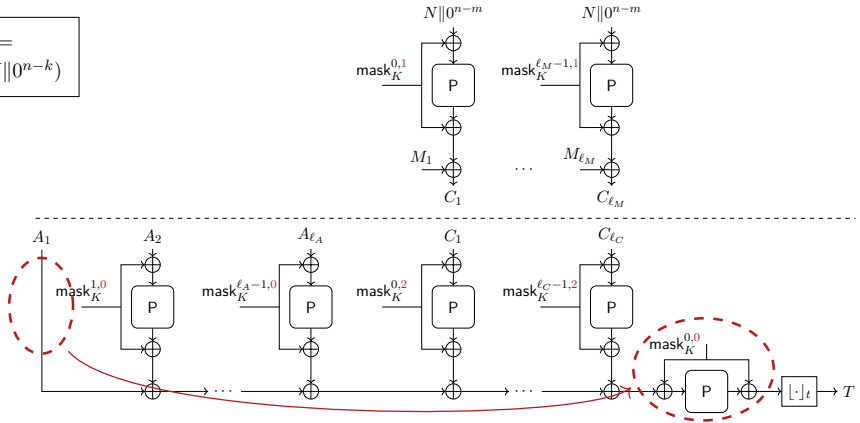


Changes to v1

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

Tweak Proposal

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



Changes to v1

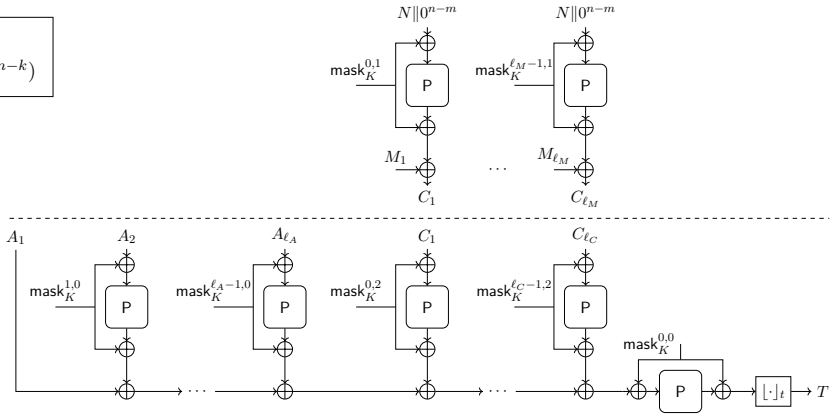
- Authentication via protected counter sum
- Slight change in roles of mask parameters

Security and Efficiency

- v2 retains all good properties of v1
- Bonus: authenticity under nonce-reuse

Tweak Proposal: Security in a Nutshell

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



	Elephant v1.1		Elephant v2	
security	confidentiality	authenticity	confidentiality	authenticity
nonce-respecting	✓	✓	✓	✓
nonce-misuse	✗	✗	✗	✓

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!