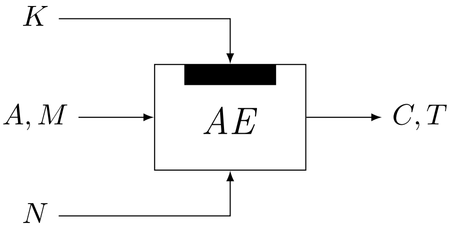
Multi-User Security of the Elephant v2 Authenticated Encryption Mode

Tim Beyne[1], Yu Long Chen[1], Christoph Dobraunig[2], Bart Mennink[3]

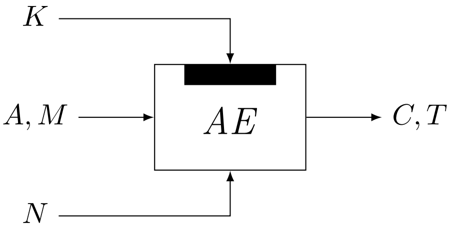
[1] KU Leuven (Belgium)
[2] Lamarr Security (Austria)
[3] Radboud University (The Netherlands)

Selected Areas in Cryptography
September – October 2021

Authenticated Encryption

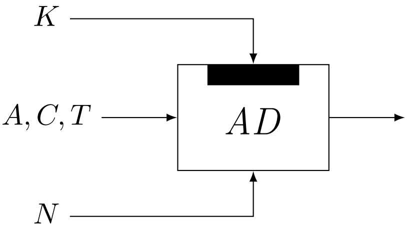


Authenticated Encryption



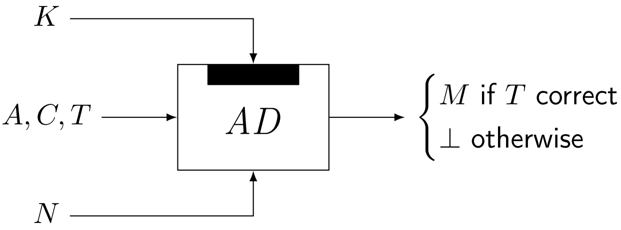
- Ciphertext C encryption of message M
- Tag T authenticates associated data A and message M
- Nonce N randomizes the scheme

Authenticated Decryption



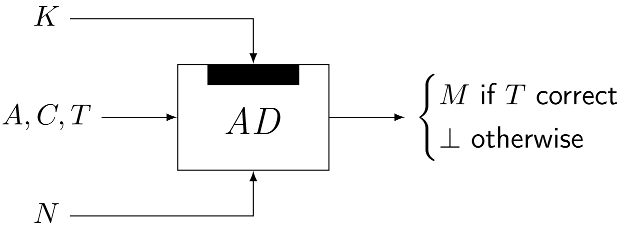
- Authenticated decryption needs to satisfy that

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: $AD_K(N, A, AE_K(N, A, M)) = M$

NIST Lightweight Cryptography Competition

Goal and Current Status

- Authenticated encryption (and optional hashing)
- Minimal security strength: 2^{112} if data complexity $\leq 2^{50}$ bytes

NIST Lightweight Cryptography Competition

Goal and Current Status

- Authenticated encryption (and optional hashing)
- Minimal security strength: 2^{112} if data complexity $\leq 2^{50}$ bytes
- February 2019: 56 first round candidates
- August 2019: 32 second round candidates
- March 2021: 10 third round (final) candidates

NIST Lightweight Cryptography Competition

Goal and Current Status

- Authenticated encryption (and optional hashing)
- Minimal security strength: 2^{112} if data complexity $\leq 2^{50}$ bytes
- February 2019: 56 first round candidates
- August 2019: 32 second round candidates
- March 2021: 10 third round (final) candidates

Elephant

- Third round candidate by Beyne, Chen, Dobraunig, Mennink [BCDM19]
- Permutation-based parallelizable authenticated encryption mode

NIST Lightweight Cryptography Competition

Goal and Current Status

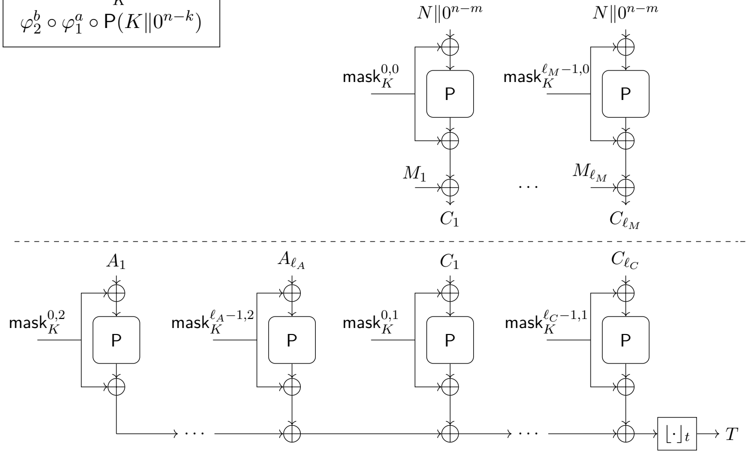
- Authenticated encryption (and optional hashing)
- Minimal security strength: 2^{112} if data complexity $\leq 2^{50}$ bytes
- February 2019: 56 first round candidates
- August 2019: 32 second round candidates
- March 2021: 10 third round (final) candidates

Elephant

- Third round candidate by Beyne, Chen, Dobraunig, Mennink [BCDM19]
- Permutation-based parallelizable authenticated encryption mode
- Design goal: simple scheme with smallest possible permutation

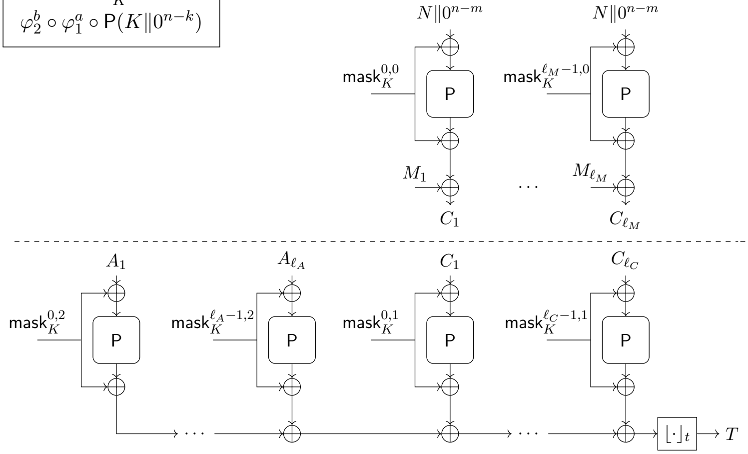
Elephant v1 Authenticated Encryption Mode (Round 1&2)

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



Elephant v1 Authenticated Encryption Mode (Round 1&2)

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

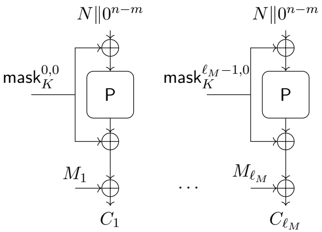


Encryption

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

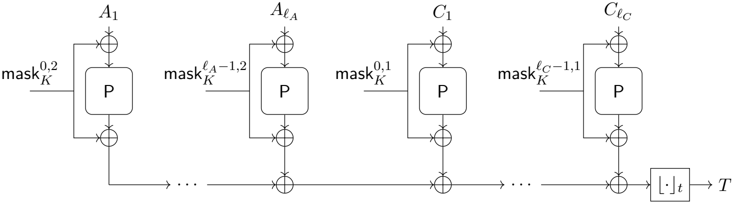
Elephant v1 Authenticated Encryption Mode (Round 1&2)

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



Encryption

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

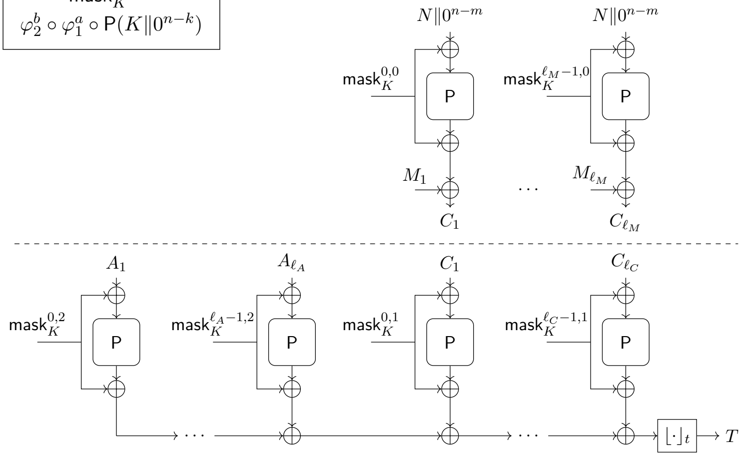


Authentication

- 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 v1 Authenticated Encryption Mode (Round 1&2)

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

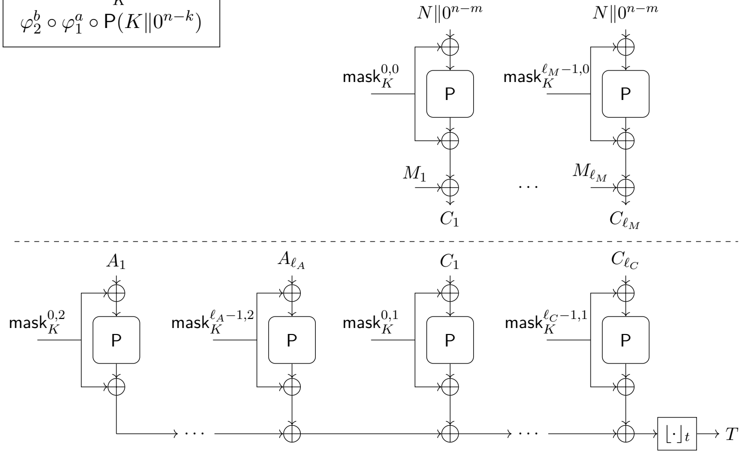


Mode Properties

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

Elephant v1 Authenticated Encryption Mode (Round 1&2)

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



Mode Properties

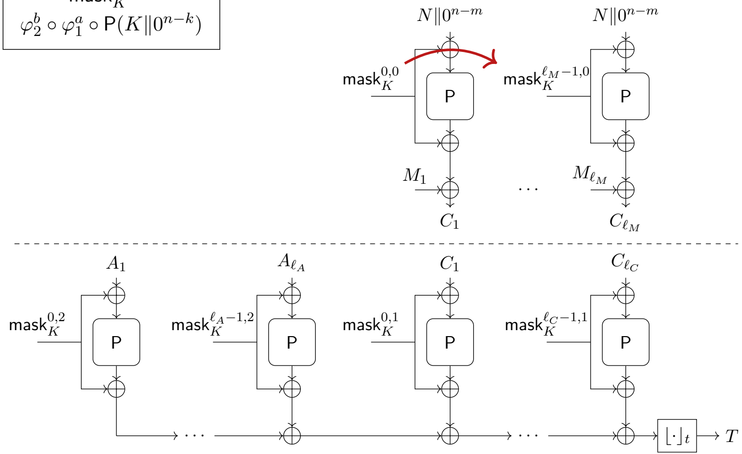
- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties

- Mask can be easily updated

Elephant v1 Authenticated Encryption Mode (Round 1&2)

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



Mode Properties

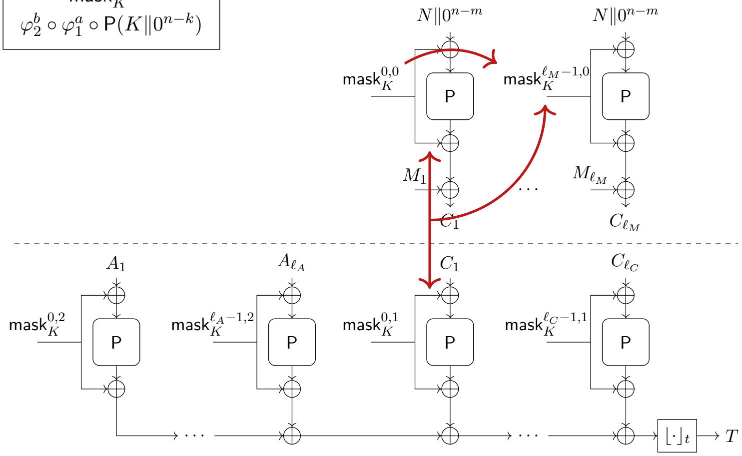
- Encrypt-then-MAC
  - CTR encryption
  - Wegman-Carter-Shoup
- Fully parallelizable
- Uses single primitive P
- P in forward direction only

Mask Properties

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

Elephant v1 Authenticated Encryption Mode (Round 1&2)

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



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 Elephant v1 Mode [BCDM20]

$$\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{Elephant\text{-}v1}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n}$$

- 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 Elephant v1 Mode [BCDM20]

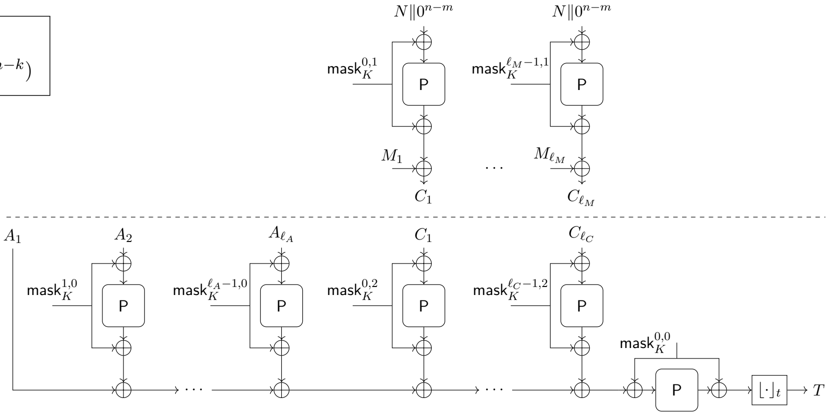
$$\mathbf{Adv}^{\mathrm{ae}}_{\text{Elephant-v1}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n}$$

- 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!

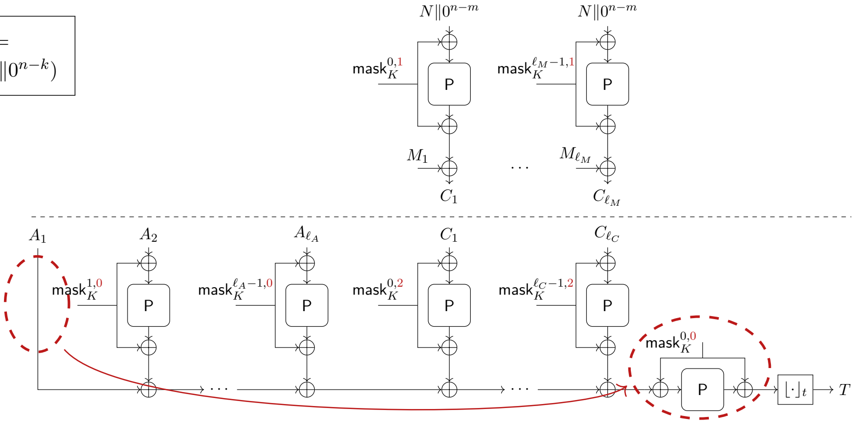
Elephant v2 Authenticated Encryption Mode (Round 3)

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



Elephant v2 Authenticated Encryption Mode (Round 3)

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

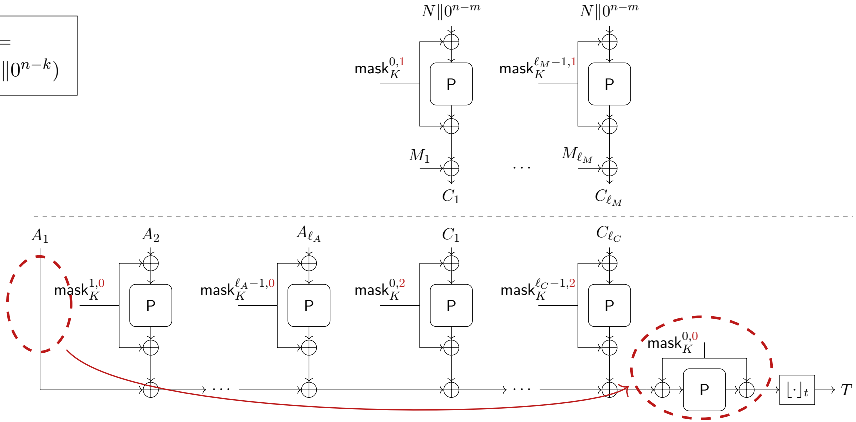


Changes to v1

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

Elephant v2 Authenticated Encryption Mode (Round 3)

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



Changes to v1

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

Claimed Security and Efficiency

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

This Work: Security of Elephant v2 Mode

This Work: Security of Elephant v2 Mode

1. Security guarantees of Elephant v1 are preserved
(confidentiality and authenticity against nonce-based adversaries $\mathcal{A}$)

This Work: Security of Elephant v2 Mode

1. Security guarantees of Elephant v1 are preserved
   (confidentiality and authenticity against nonce-based adversaries $\mathcal{A}$)
2. Elephant v2 additionally achieves authenticity under nonce-misuse

This Work: Security of Elephant v2 Mode

1. Security guarantees of Elephant v1 are preserved
   (confidentiality and authenticity against nonce-based adversaries $\mathcal{A}$)
2. Elephant v2 additionally achieves authenticity under nonce-misuse
3. These results even hold in multi-user setting

This Work: Security of Elephant v2 Mode

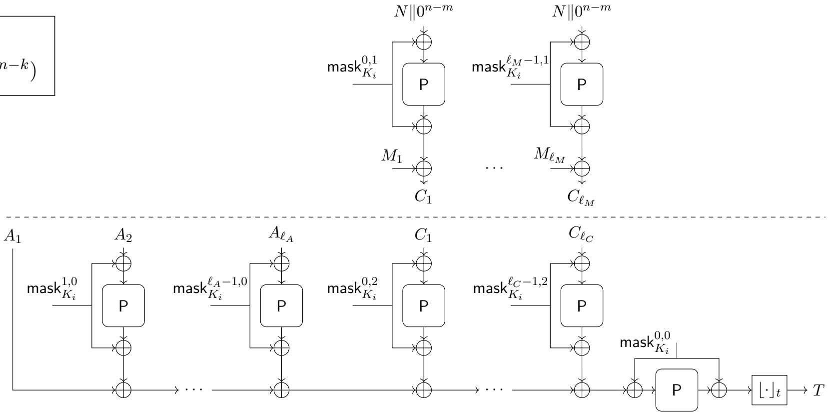
1. Security guarantees of Elephant v1 are preserved
(confidentiality and authenticity against nonce-based adversaries $\mathcal{A}$)
2. Elephant v2 additionally achieves authenticity under nonce-misuse
3. These results even hold in multi-user setting

$$\mathbf{Adv}^{\mu\text{-ae}}_{\textsf{Elephant-v2}}(\mathcal{A}) \lesssim \frac{4\sigma p}{2^n} \qquad \mathbf{Adv}^{\mu\text{-auth}}_{\textsf{Elephant-v2}}(\mathcal{B}) \lesssim \frac{4\sigma p}{2^n}$$

- σ is online complexity, p is offline complexity, μ is number of users
- 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, $\mathcal{B}$ is bdversary that may reuse nonces

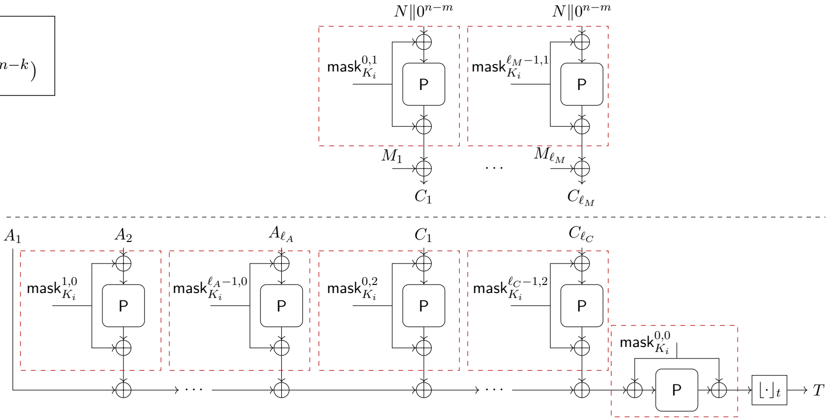
Proof Idea (1/3)

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



Proof Idea (1/3)

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

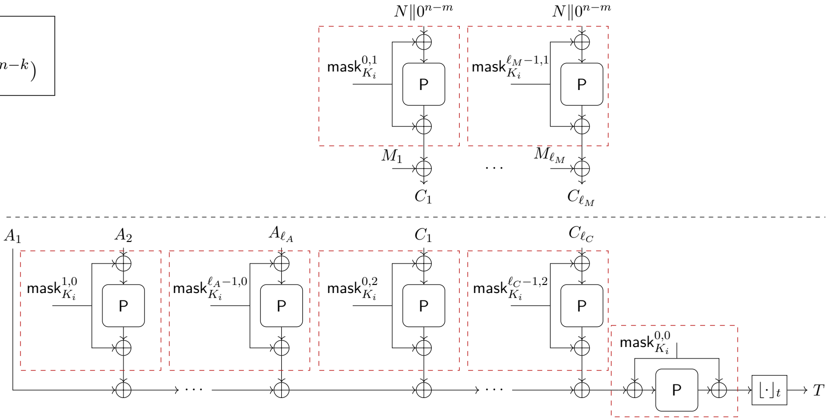


Step 1

- Isolate Simplified Masked Even-Mansour (SiMEM)

Proof Idea (1/3)

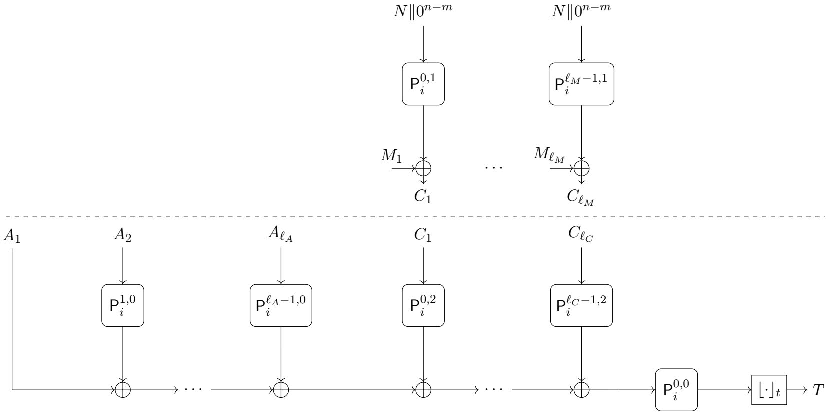
$$\text{mask}_{K_i}^{a,b} = \varphi_2^b \circ \varphi_1^a \circ \mathsf{P}(K_i \| 0^{n-k})$$



Step 1

- Isolate Simplified Masked Even-Mansour (SiMEM)
- Multi-user security analysis of SiMEM

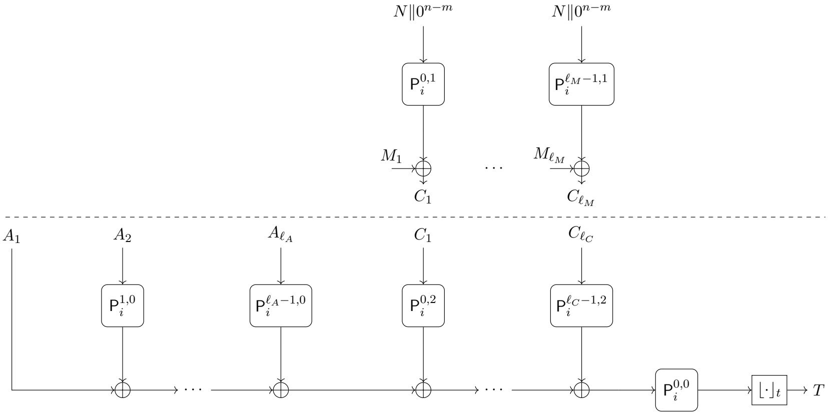
Proof Idea (1/3)



Step 1

- Isolate Simplified Masked Even-Mansour (SiMEM)
- Multi-user security analysis of SiMEM
- Replace SiMEM instances by independent random permutations

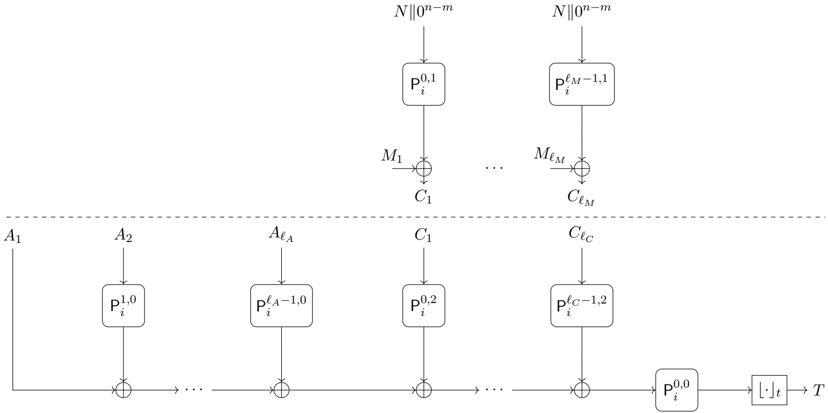
Proof Idea (2/3)



Step 2

- We obtained μ independent instances of Elephant v2
- Multi-user security: sum over μ independent single-user adversaries

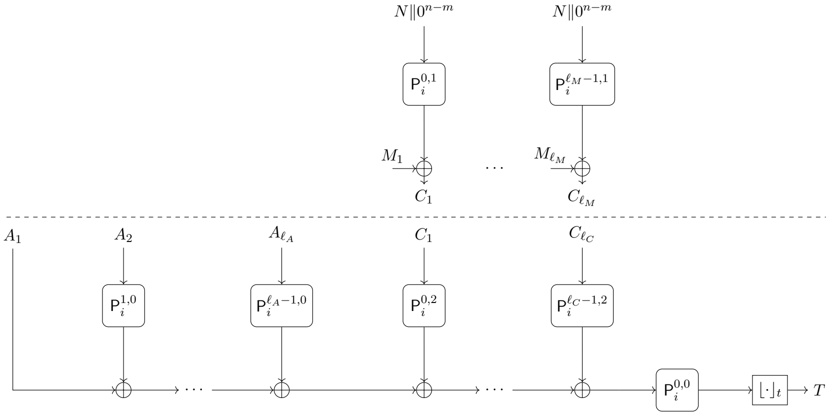
Proof Idea (2/3)



Step 2

- We obtained μ independent instances of Elephant v2
- Multi-user security: sum over μ independent single-user adversaries
- Focus on single-user case

Proof Idea (3/3)



Step 3

- Nonce-based encryption part
- Nonce-independent authentication part

Conclusion

- Elephant v1 achieved confidentiality and authenticity in nonce-respecting setting [BCDM20]

Conclusion

- Elephant v1 achieved confidentiality and authenticity in nonce-respecting setting [BCDM20]
- We proved that Elephant v2:
  - preserves all security properties of v1 (up to comparable bound)
  - additionally achieves authenticity in nonce-misuse setting

	Elephant v1 [BCDM20]		Elephant v2 (proven now)	
security	confidentiality	authenticity	confidentiality	authenticity
nonce-respecting	✓	✓	✓	✓
nonce-misuse	✗	✗	✗	✓

Conclusion

- Elephant v1 achieved confidentiality and authenticity in nonce-respecting setting [BCDM20]
- We proved that Elephant v2:
  - preserves all security properties of v1 (up to comparable bound)
  - additionally achieves authenticity in nonce-misuse setting

	Elephant v1 [BCDM20]		Elephant v2 (proven now)	
security	confidentiality	authenticity	confidentiality	authenticity
nonce-respecting	✓	✓	✓	✓
nonce-misuse	✗	✗	✗	✓

- Our results even hold in the multi-user setting
  - Number of users only affects minor terms in the security bound

Conclusion

- Elephant v1 achieved confidentiality and authenticity in nonce-respecting setting [BCDM20]
- We proved that Elephant v2:
  - preserves all security properties of v1 (up to comparable bound)
  - additionally achieves authenticity in nonce-misuse setting

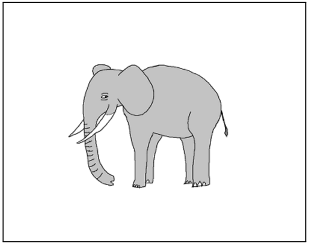
	Elephant v1 [BCDM20]		Elephant v2 (proven now)	
security	confidentiality	authenticity	confidentiality	authenticity
nonce-respecting	✓	✓	✓	✓
nonce-misuse	✗	✗	✗	✓

- Our results even hold in the multi-user setting
  - Number of users only affects minor terms in the security bound

Thank you for your attention!

SUPPORTING SLIDES

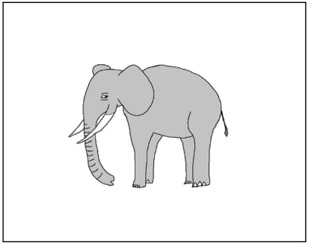
Instantiation



Dumbo

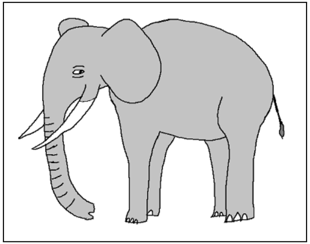
- Spongent-$\pi[160]$
- Minimalist design
  - Time complexity 2^{112}
  - Data complexity 2^{46}

Instantiation



Dumbo

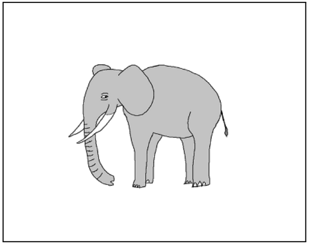
- Spongent-$\pi[160]$
- Minimalist design
  - Time complexity 2^{112}
  - Data complexity 2^{46}



Jumbo

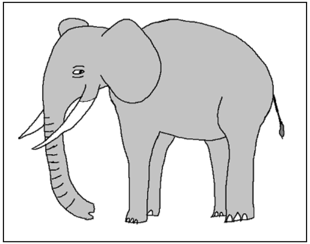
- Spongent-$\pi[176]$
- Conservative design
  - Time complexity 2^{127}
  - Data complexity 2^{46}
- ISO/IEC standardized

Instantiation



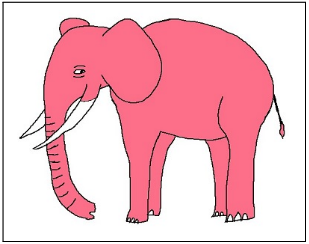
Dumbo

- 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-$\pi[160]$	φ_{Dumbo}	2^{112}	$2^{50}/(n/8)$
Jumbo	128	96	176	64	90-round Spongent-$\pi[176]$	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:

$$\varphi_{\text{Dumbo}} : (x_0, \ldots, x_{19}) \mapsto (x_1, \ldots, x_{19}, x_0 \lll 3 \oplus x_3 \ll 7 \oplus x_{13} \gg 7)$$

$$\varphi_{\text{Jumbo}} : (x_0, \ldots, x_{21}) \mapsto (x_1, \ldots, x_{21}, x_0 \lll 1 \oplus x_3 \ll 7 \oplus x_{19} \gg 7)$$

$$\varphi_{\text{Delirium}} : (x_0, \ldots, x_{24}) \mapsto (x_1, \ldots, x_{24}, x_0 \lll 1 \oplus x_2 \lll 1 \oplus x_{13} \ll 1)$$

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