Generic Security of the Ascon Mode: On the Power of Key Blinding

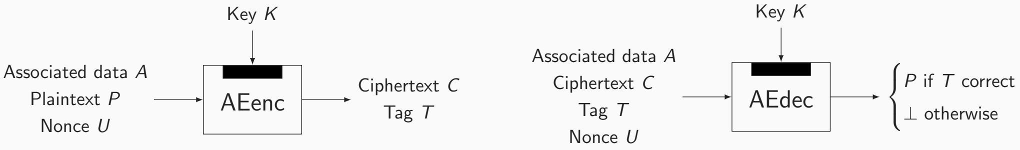
Charlotte Lefevre, Bart Mennink

Radboud University (The Netherlands)

Selected Areas in Cryptography

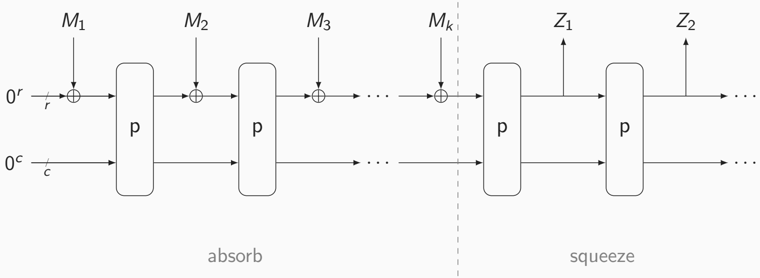
30 August 2024

Authenticated Encryption with Associated Data



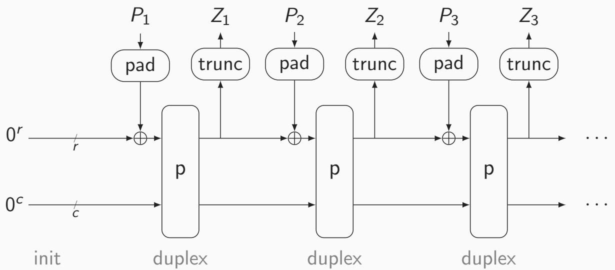
Conventional security: confidentiality (indistinguishability of ciphertexts) and authenticity (unforgeability)

The Sponge Construction [BDPV07]

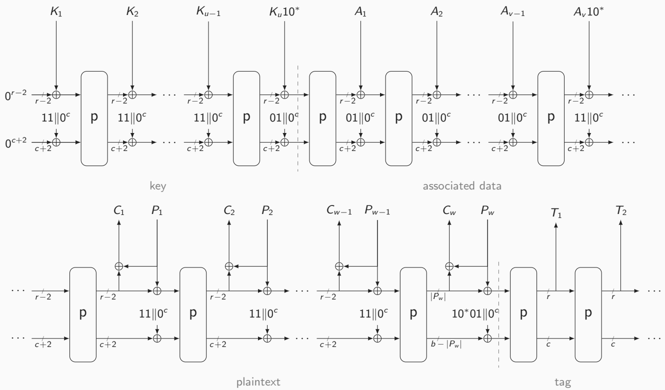


- State of size $b = r + c$
- $M_1 \| \cdots \| M_k$ is the message injectively padded into r-bit blocks

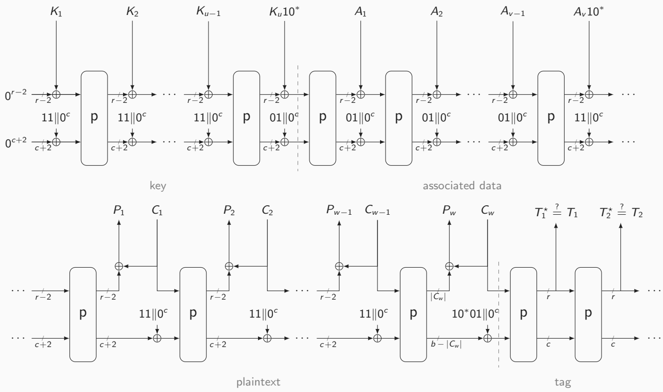
The Duplex Construction [BDPV11]



Interleaved absorption and squeezing phases

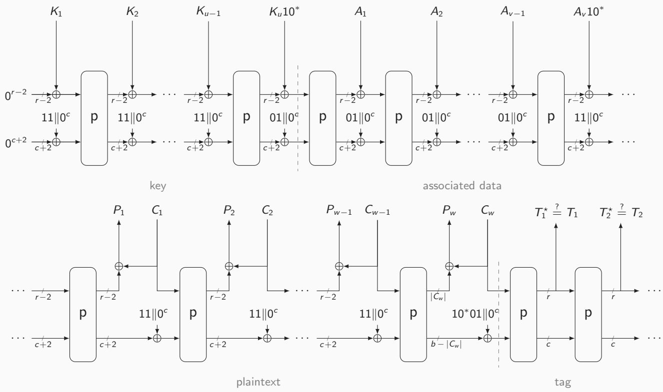


- Key, associated data, plaintext fed into duplex with domain separators
- Encryption: outer parts used as one-time pad



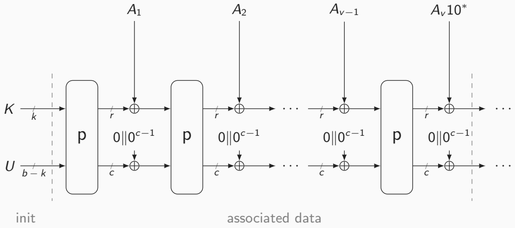
- Key, associated data, plaintext fed into duplex with domain separators
- Encryption: outer parts used as one-time pad
- Decryption: ciphertext overwrites outer part of the state

Application: SpongeWrap [BDPV11]

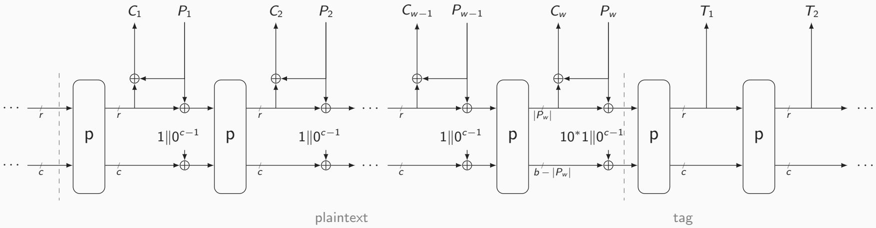


- Key, associated data, plaintext fed into duplex with domain separators
- Encryption: outer parts used as one-time pad
- Decryption: ciphertext overwrites outer part of the state
- Security derived from the indifferentiability of the sponge [BDPV08]

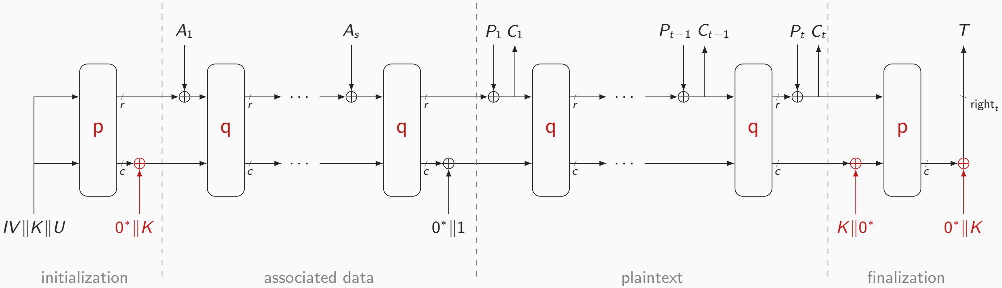
Application: MonkeySpongeWrap [Men23]



- Closer to modern duplex-based AEADs
- State initialized with key and nonce
- Security follows from a generic analysis done in [DMV17]



Ascon-AEAD Mode



- Additional key blindings at initialization and finalization
- Outer and inner permutations p and q differ

Security of Ascon-AEAD Mode

- Generic results on the duplex [DMV17] do not cover Ascon-AEAD mode

- Generic results on the duplex [DMV17] do not cover Ascon-AEAD mode

This Work

- Multi-user analysis of confidentiality of Ascon-AEAD mode
- Multi-user analysis of authenticity of Ascon-AEAD mode:
  - Nonce-respecting setting
  - Nonce-misuse setting

- Generic results on the duplex [DMV17] do not cover Ascon-AEAD mode

This Work

- Multi-user analysis of confidentiality of Ascon-AEAD mode
- Multi-user analysis of authenticity of Ascon-AEAD mode:
  - Nonce-respecting setting
  - Nonce-misuse setting
  - Under state recovery with a tailored security model

Security of Ascon-AEAD Mode

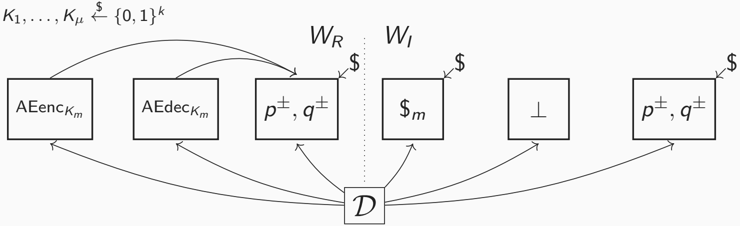
- Generic results on the duplex [DMV17] do not cover Ascon-AEAD mode

This Work

- Multi-user analysis of confidentiality of Ascon-AEAD mode
- Multi-user analysis of authenticity of Ascon-AEAD mode:
  - Nonce-respecting setting
  - Nonce-misuse setting
  - Under state recovery with a tailored security model

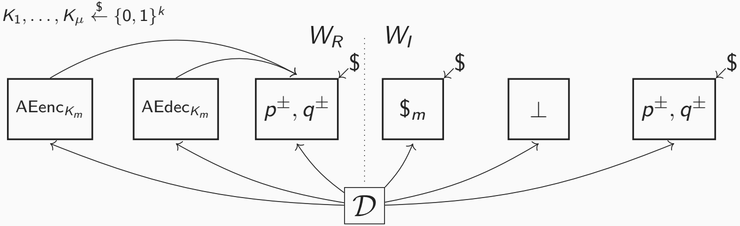
Independent Work

- Chakraborty et al. [CDN23]: tight bound on confidentiality and authenticity in the nonce-respecting case ($p = q$)



- Distinguishing advantage: $\mathbf{Adv}^{\mu\text{-ae}}_{\text{Ascon}}(\mathcal{D})$

Security Model: Nonce-Based AE Security



- Distinguishing advantage: $\mathbf{Adv}^{\mu\text{-ae}}_{\text{Ascon}}(\mathcal{D})$
- Resources of the adversary:
  - Q_E encryption queries with M_E blocks
  - Q_D decryption queries with M_D blocks
  - $M = M_E + M_D$
  - N primitive queries

Security Model: Separation into Confidentiality and Authenticity

- Confidentiality: remove oracle access to $(\mathrm{AEdec}_{K_m})_m / \perp$
- Authenticity: $\mathbf{Pr}\left(\mathcal{D}\left[\left(\mathsf{AEenc}_{K_m}^{p,q}\right)_m, \left(\mathsf{AEdec}_{K_m}^{p,q}\right)_m, (p^{\pm}, q^{\pm})\right] \text{ forges}\right)$

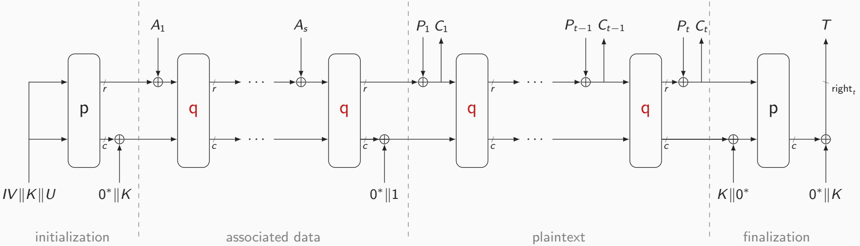
Security Model: Separation into Confidentiality and Authenticity

- Confidentiality: remove oracle access to $(\mathrm{AEdec}_{K_m})_m / \perp$
- Authenticity: $\mathbf{Pr}\left(\mathcal{D}\left[\left(\mathsf{AEenc}^{p,q}_{K_m}\right)_m, \left(\mathsf{AEdec}^{p,q}_{K_m}\right)_m, (p^{\pm}, q^{\pm})\right] \text{ forges}\right)$
- We have

$$\mathbf{Adv}^{\mu\text{-ae}}_{\mathrm{Ascon}}(\mathcal{D}) \leq \mathbf{Adv}^{\mu\text{-conf}}_{\mathrm{Ascon}}(\mathcal{D}') + \mathbf{Adv}^{\mu\text{-auth}}_{\mathrm{Ascon}}(\mathcal{D}'')$$

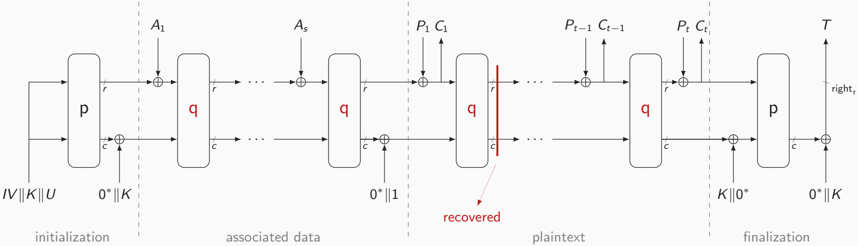
with $\mathcal{D}'$ and $\mathcal{D}''$ having similar complexities than $\mathcal{D}$

Security Model: Authenticity Under State Recovery (1)



Attack Setting

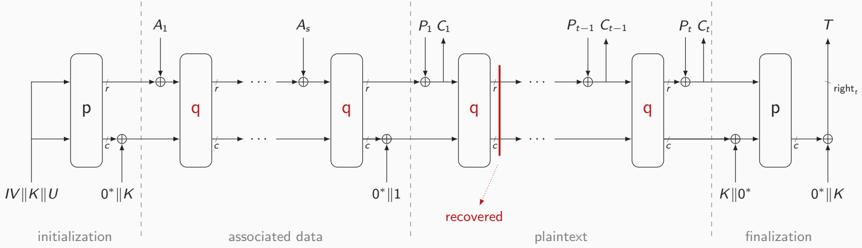
- Adversary may somehow recover any inner state



Attack Setting

- Adversary may somehow recover any inner state

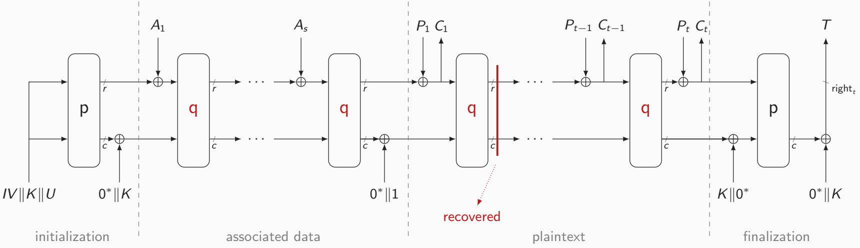
Security Model: Authenticity Under State Recovery (1)



Attack Setting

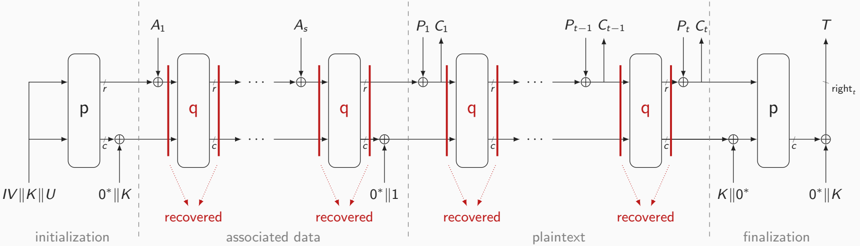
- Adversary may somehow recover any inner state
- Ascon-AEAD designed to still achieve authenticity in this setting

Authenticity Under State Recovery (2)



Model

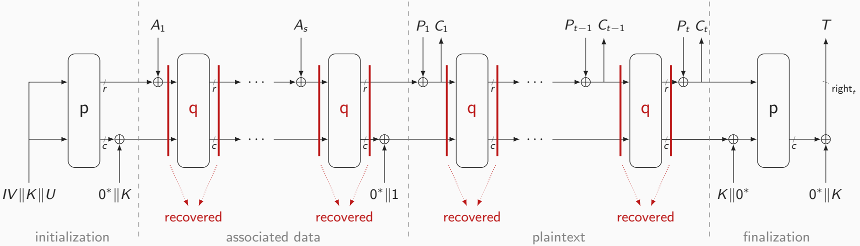
- Model inspired by permutation-based leakage resilience [DM19a, DM19b]



Model

- Model inspired by permutation-based leakage resilience [DM19a, DM19b]
- Without loss of generality: every encryption/decryption query leaks the entire b-bit state of all evaluations of inner permutation q

Authenticity Under State Recovery (2)



Model

- Model inspired by permutation-based leakage resilience [DM19a, DM19b]
- Without loss of generality: every encryption/decryption query leaks the entire b-bit state of all evaluations of inner permutation q
- MonkeySpongeWrap-style AEAD does not guarantee security in this setting

Security Results

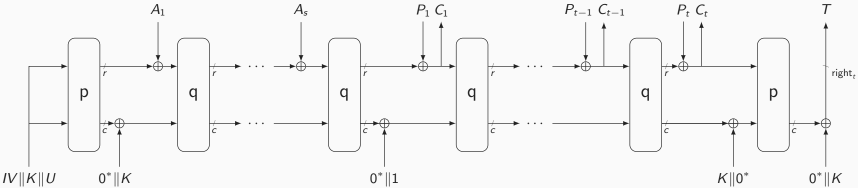
Property	Setting	Security bound (simplified)
Confidentiality	nonce-respecting	$\mathcal{O}\left(\frac{\mu(N+\mu)}{2^k} + \frac{N^2}{2^b} + \frac{N}{2^c}\right)$
	nonce-misuse	—
	state recovery	
Authenticity	nonce-respecting	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{M_E N}{2^b} + \frac{M_D N}{2^c}\right)$
	nonce-misuse	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{MN}{2^c}\right)$
	state recovery	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{N^2}{2^c}\right)$

- Nonce-misuse and state recovery authenticity degrade in the last terms

Security Results

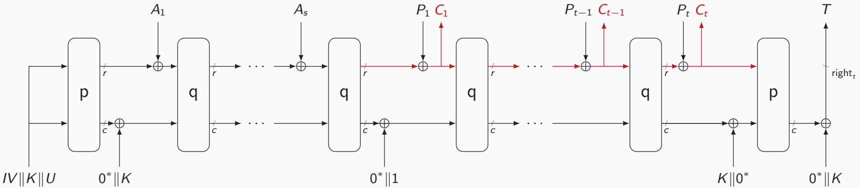
Property	Setting	Security bound (simplified)
Confidentiality	nonce-respecting	$\mathcal{O}\left(\frac{\mu(N+\mu)}{2^k} + \frac{NM}{2^b} + \frac{N}{2^c}\right)$
	nonce-misuse	—
	state recovery	
Authenticity	nonce-respecting	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{MN}{2^b} + \frac{N}{2^c}\right)$
	nonce-misuse	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{MN}{2^c}\right)$
	state recovery	$\mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k} + \frac{N^2}{2^c}\right)$

- Nonce-misuse and state recovery authenticity degrade in the last terms
- Improvement from Chakraborty et al. [CDN23] in nonce-based security



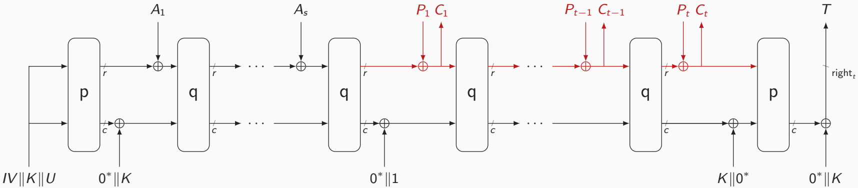
Modular Proof

- Some bad events are kept unchanged $\implies \mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k}\right)$
- Others are adjusted, depending on the setting:



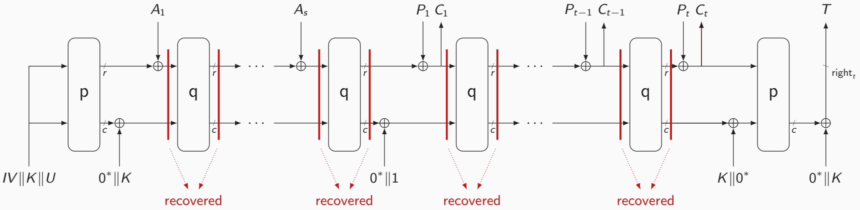
Modular Proof

- Some bad events are kept unchanged $\Longrightarrow \mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k}\right)$
- Others are adjusted, depending on the setting:
  - Nonce-respecting: inner states secret, but adversary has access to the outer parts $\Longrightarrow \mathcal{O}\left(\frac{M_E N}{2^b} + \frac{M_D N}{2^c}\right)$



Modular Proof

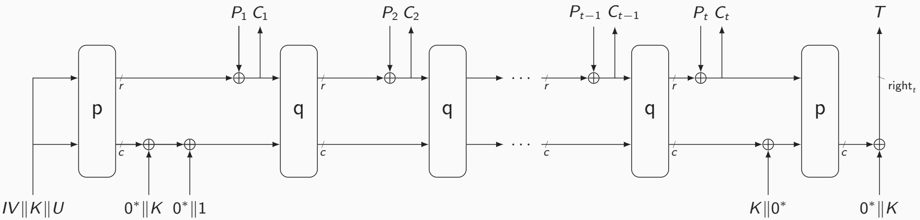
- Some bad events are kept unchanged $\Longrightarrow \mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k}\right)$
- Others are adjusted, depending on the setting:
  - Nonce-misuse: inner states secret, but adversary has access to and can overwrite the outer parts $\Longrightarrow \mathcal{O}\left(\frac{MN}{2^c}\right)$



Modular Proof

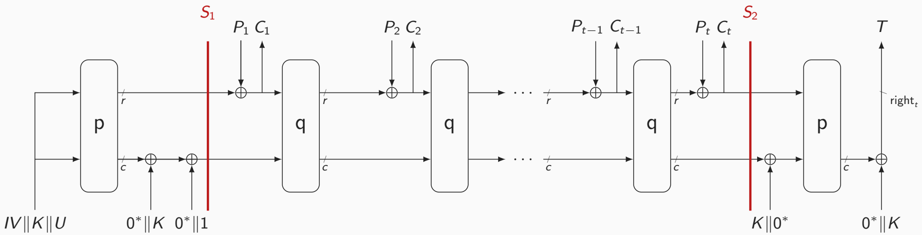
- Some bad events are kept unchanged $\implies \mathcal{O}\left(\frac{Q_D}{2^t} + \frac{\mu(N+\mu)}{2^k}\right)$
- Others are adjusted, depending on the setting:
  - State recovery: inner states fully leak, thus permutation queries may correspond later to construction queries $\implies \mathcal{O}\left(\frac{N^2}{2^c}\right)$

Authenticity Under State Recovery: Matching Attack



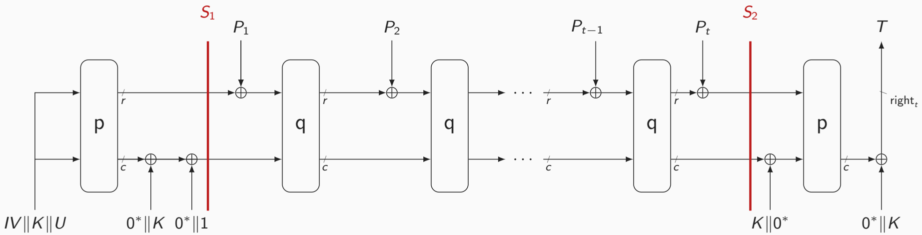
- Make an encryption query with empty associated data

Authenticity Under State Recovery: Matching Attack



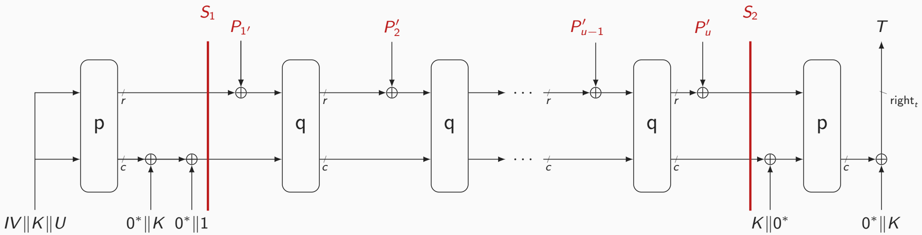
- Make an encryption query with empty associated data
- Get state after first initialization S_1, and right before finalization S_2

Authenticity Under State Recovery: Matching Attack



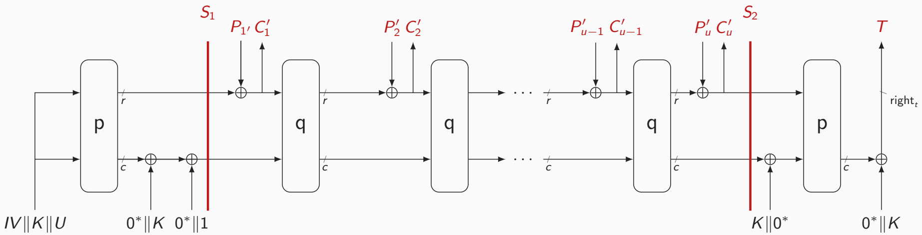
- Make an encryption query with empty associated data
- Get state after first initialization S_1, and right before finalization S_2
- View S_1 as initial state of a sponge, S_2 as a state obtained with the preimage $P_1, \ldots, P_t$

Authenticity Under State Recovery: Matching Attack



- Make an encryption query with empty associated data
- Get state after first initialization S_1, and right before finalization S_2
- View S_1 as initial state of a sponge, S_2 as a state obtained with the preimage $P_1, \ldots, P_t$
- Apply a second preimage attack, i.e. find $P'_1, \ldots, P'_u \neq P_1, \ldots, P_t$ that reaches $S_2 \implies$ costs $2^{c/2}$ q-evaluations

Authenticity Under State Recovery: Matching Attack



- Make an encryption query with empty associated data
- Get state after first initialization S_1, and right before finalization S_2
- View S_1 as initial state of a sponge, S_2 as a state obtained with the preimage $P_1, \ldots, P_t$
- Apply a second preimage attack, i.e. find $P_1', \ldots, P_u' \neq P_1, \ldots, P_t$ that reaches $S_2 \implies$ costs $2^{c/2}$ q-evaluations
- Submit a forgery with the associated ciphertext and T

Application to Ascon-AEAD Parameters

- $(k, b, c, r, t) = \begin{cases} (128, 320, 256, 64, 128) \text{ for Ascon-128} \\ (128, 320, 192, 128, 128) \text{ for Ascon-128a} \\ (160, 320, 256, 64, 128) \text{ for Ascon-80pq} \end{cases}$
- Assume number of users $\mu \ll 2^{64}$
- Assume online complexity $Q, M \ll 2^{64}$

Application to Ascon-AEAD Parameters

- $(k, b, c, r, t) = \begin{cases} (128, 320, 256, 64, 128) \text{ for Ascon-128} \\ (128, 320, 192, 128, 128) \text{ for Ascon-128a} \\ (160, 320, 256, 64, 128) \text{ for Ascon-80pq} \end{cases}$
- Assume number of users $\mu \ll 2^{64}$
- Assume online complexity $Q, M \ll 2^{64}$

$\Longrightarrow$ Ascon-128: in all cases, generic security as long as $N \ll 2^{128}/\mu$

$\Longrightarrow$ Ascon-80pq: in all cases, generic security as long as $N \ll 2^{160}/\mu$

$\Longrightarrow$ Ascon-128a: nonce-respecting/misusing generic security as long as $N \ll 2^{128}/\mu$, authenticity under state recovery as long as additionally $N \ll 2^{96}$

Conclusion

- General security analysis of Ascon-AEAD mode
- Main focus on role of key blindings
- Caution: the results hold in ideal permutation model (e.g. see [BCP22] for attack in nonce-misuse setting on concrete instantiation)

Conclusion

- General security analysis of Ascon-AEAD mode
- Main focus on role of key blindings
- Caution: the results hold in ideal permutation model (e.g. see [BCP22] for attack in nonce-misuse setting on concrete instantiation)

Thank you for your attention!

- Jules Baudrin, Anne Canteaut, and Léo Perrin.
  Practical cube attack against nonce-misused ascon.
  IACR Trans. Symmetric Cryptol., 2022(4):120–144, 2022.
- Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
  Sponge functions.
  Ecrypt Hash Workshop 2007, May 2007.
- Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
  On the Indifferentiability of the Sponge Construction.
  In Nigel P. Smart, editor, *EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

References ii

- Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
  Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications.
  In Ali Miri and Serge Vaudenay, editors, *SAC 2011*, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.
- Bishwajit Chakraborty, Chandranan Dhar, and Mridul Nandi.
  Exact security analysis of ASCON.
  In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023*, volume 14440 of *Lecture Notes in Computer Science*, pages 346–369. Springer, 2023.

Christoph Dobraunig and Bart Mennink.
Leakage Resilience of the Duplex Construction.
In Steven D. Galbraith and Shiho Moriai, editors, *ASIACRYPT 2019, Part III*, volume 11923 of *LNCS*, pages 225–255. Springer, 2019.

Christoph Dobraunig and Bart Mennink.
Security of the Suffix Keyed Sponge.
IACR Trans. Symmetric Cryptol., 2019(4):223–248, 2019.

Joan Daemen, Bart Mennink, and Gilles Van Assche.
Full-State Keyed Duplex with Built-In Multi-user Support.
In Tsuyoshi Takagi and Thomas Peyrin, editors, *ASIACRYPT 2017, Part II*, volume 10625 of *LNCS*, pages 606–637. Springer, 2017.

Bart Mennink.
Understanding the Duplex and Its Security.
IACR Trans. Symmetric Cryptol., 2023(2):1–46, 2023.