SoK: Security of the Ascon Modes

Charlotte Lefevre, Bart Mennink

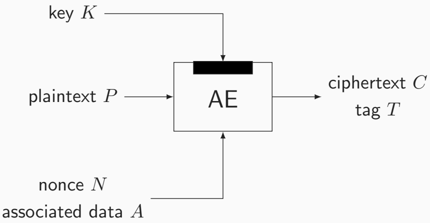
Radboud University

FSE 2025

March 17, 2025

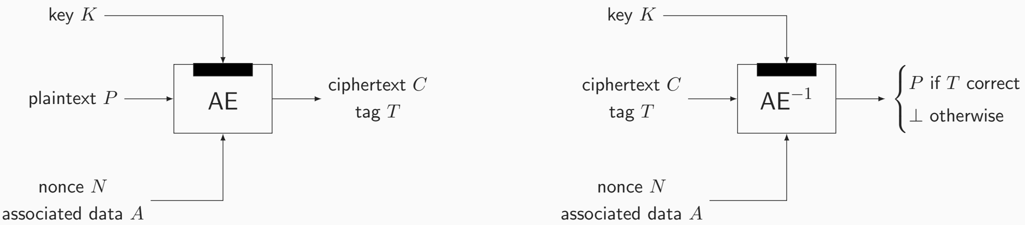
Introduction

Authenticated Encryption



- Using key K:
  - Ciphertext C encrypts plaintext P
  - Tag T authenticates (N, A, P)

Authenticated Encryption



- Using key K:
  - Ciphertext C encrypts plaintext P
  - Tag T authenticates (N, A, P)
- Unwrapping needs to satisfy that
  - Plaintext disclosed if tag is correct
  - Plaintext is not leaked if tag is incorrect

CAESAR Competition

- 2014–2019
- Call for authenticated encryption scheme
- 57 submissions (of which $\approx$ 10 sponge/duplex-based)
- Ascon selected as winner in category lightweight applications

CAESAR Competition

- 2014–2019
- Call for authenticated encryption scheme
- 57 submissions (of which $\approx$ 10 sponge/duplex-based)
- Ascon selected as winner in category lightweight applications

NIST Lightweight Cryptography Competition

- 2019–2023
- Call for authenticated encryption scheme and, optionally, hash function
- 57 submissions (of which $\approx$ 22 sponge/duplex-based)
- Ascon selected as winner

Ascon [DEMS21]

Ascon [DEMS21]

Authenticated Encryption

- Duplex-based but with additional key blindings

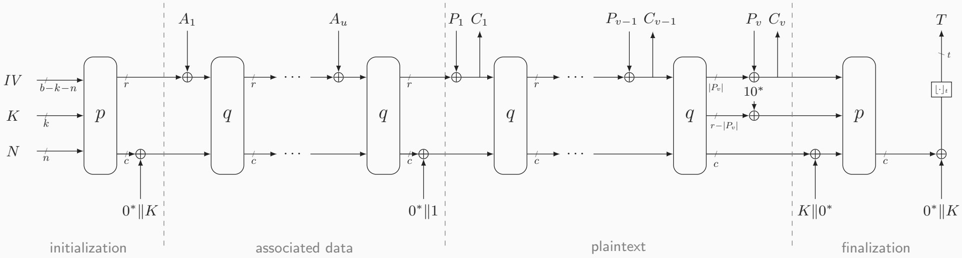
Authenticated Encryption

- Duplex-based but with additional key blindings

Hashing

- Sponge-based hashing and XOFing
- Only included in NIST Lightweight Cryptography submission

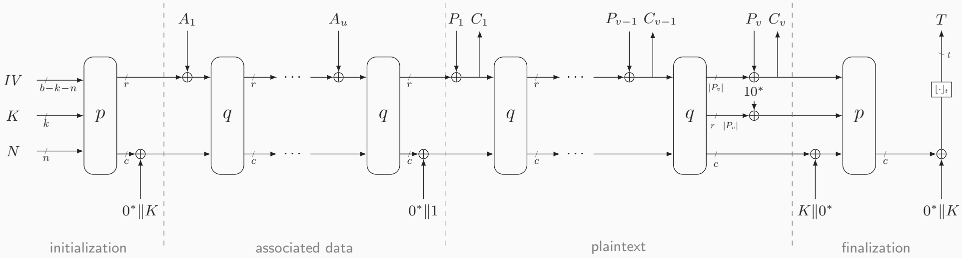
Ascon-AE



Variant of SpongeWrap [BDPV11]

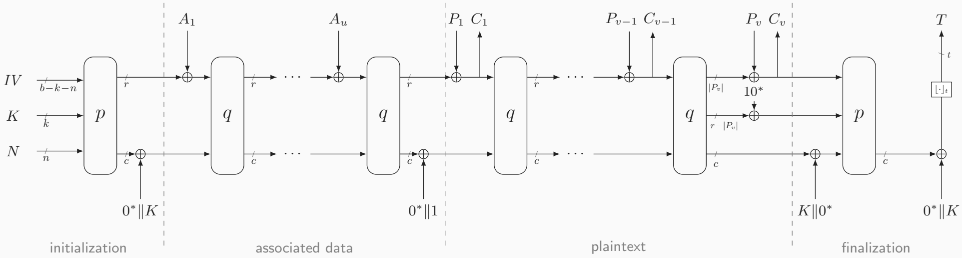
- Outer permutation p and inner permutation q, both on b bits
  - r is the rate, c is the capacity (security parameter)

Ascon-AE



Variant of SpongeWrap [BDPV11]

- Outer permutation p and inner permutation q, both on b bits
  - r is the rate, c is the capacity (security parameter)
- Additional key blindings around "outer" permutations



Variant of SpongeWrap [BDPV11]

- Outer permutation p and inner permutation q, both on b bits
  - r is the rate, c is the capacity (security parameter)
- Additional key blindings around "outer" permutations
- Domain separation simplified and spilled-over into inner part

SpongeWrap and Similar

History of Generic Security Results (1/2)

SpongeWrap and Similar

2011 Bertoni et al. [BDPV11]
Duplex and SpongeWrap

History of Generic Security Results (1/2)

SpongeWrap and Similar

2011 Bertoni et al. [BDPV11]
Duplex and SpongeWrap

2015 Mennink et al. [MRV15]
Full-state duplex and SpongeWrap

History of Generic Security Results (1/2)

SpongeWrap and Similar

2011 — Bertoni et al. [BDPV11]
Duplex and SpongeWrap

2015 — Mennink et al. [MRV15]
Full-state duplex and SpongeWrap

2017 — Daemen et al. [DMV17]
Generalized duplex

History of Generic Security Results (1/2)

SpongeWrap and Similar

2011 Bertoni et al. [BDPV11]
Duplex and SpongeWrap

2015 Mennink et al. [MRV15]
Full-state duplex and SpongeWrap

2017 Daemen et al. [DMV17]
Generalized duplex

2019 Dobraunig and Mennink [DM19]
Leakage resilience of generalized duplex

SpongeWrap and Similar

- 2011 — Bertoni et al. [BDPV11]
  Duplex and SpongeWrap
- 2015 — Mennink et al. [MRV15]
  Full-state duplex and SpongeWrap
- 2017 — Daemen et al. [DMV17]
  Generalized duplex
- 2019 — Dobraunig and Mennink [DM19]
  Leakage resilience of generalized duplex
- 2023 — Mennink [Men23]
  Duplex guide and MonkeySpongeWrap

History of Generic Security Results (1/2)

SpongeWrap and Similar

- 2011 — Bertoni et al. [BDPV11]
  Duplex and SpongeWrap
- 2014 — Jovanovic et al. [JLM14]
  Security of NORX with claim on Ascon
- 2015 — Mennink et al. [MRV15]
  Full-state duplex and SpongeWrap
- 2017 — Daemen et al. [DMV17]
  Generalized duplex
- 2019 — Dobraunig and Mennink [DM19]
  Leakage resilience of generalized duplex
- 2023 — Mennink [Men23]
  Duplex guide and MonkeySpongeWrap

History of Generic Security Results (1/2)

SpongeWrap and Similar

2011 Bertoni et al. [BDPV11]
Duplex and SpongeWrap

2014 Jovanovic et al. [JLM14]
Security of NORX with claim on Ascon

2015 Mennink et al. [MRV15]
Full-state duplex and SpongeWrap

2017 Daemen et al. [DMV17]
Generalized duplex

2019 Dobraunig and Mennink [DM19]
Leakage resilience of generalized duplex

2023 Mennink [Men23]
Duplex guide and MonkeySpongeWrap

none of these results deals with additional key blindings

Dedicated Ascon Analysis

Dedicated Ascon Analysis

2023 Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

Dedicated Ascon Analysis

2023 Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

2024 Lefevre and Mennink [LM24]
Multi-user security in nonce-respecting and nonce-misuse setting

Dedicated Ascon Analysis

2023 — Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

2024 — Lefevre and Mennink [LM24]
Multi-user security in nonce-respecting and nonce-misuse setting

2024 — Chakraborty et al. [CDN24]
Extended [CDN23] to multi-user security and nonce-misuse setting

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

2019 Guo et al. [GPPS19]
Multi-user security in nonce-misuse resilience setting

2023 Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

2024 Lefevre and Mennink [LM24]
Multi-user security in nonce-respecting and nonce-misuse setting

2024 Chakraborty et al. [CDN24]
Extended [CDN23] to multi-user security and nonce-misuse setting

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

- 2019 — Guo et al. [GPPS19]
  - Multi-user security in nonce-misuse resilience setting
  - Multi-user security under leakage resilience
- 2023 — Chakraborty et al. [CDN23]
  - Single-user security in nonce-respecting setting
- 2024 — Lefevre and Mennink [LM24]
  - Multi-user security in nonce-respecting and nonce-misuse setting
- 2024 — Chakraborty et al. [CDN24]
  - Extended [CDN23] to multi-user security and nonce-misuse setting

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

- 2019 — Guo et al. [GPPS19]
  - Multi-user security in nonce-misuse resilience setting
  - Multi-user security under leakage resilience
- 2023 — Chakraborty et al. [CDN23]
  - Single-user security in nonce-respecting setting
- 2024 — Lefevre and Mennink [LM24]
  - Multi-user security in nonce-respecting and nonce-misuse setting
  - Multi-user security under state recovery
- 2024 — Chakraborty et al. [CDN24]
  - Extended [CDN23] to multi-user security and nonce-misuse setting

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

- **2019** Guo et al. [GPPS19]
  - Multi-user security in nonce-misuse resilience setting
  - Multi-user security under leakage resilience
  - only "proof sketches"
  - contain gaps [LM24]
- **2023** Chakraborty et al. [CDN23]
  - Single-user security in nonce-respecting setting
- **2024** Lefevre and Mennink [LM24]
  - Multi-user security in nonce-respecting and nonce-misuse setting
  - Multi-user security under state recovery
- **2024** Chakraborty et al. [CDN24]
  - Extended [CDN23] to multi-user security and nonce-misuse setting

Dedicated Ascon Analysis

2019 Guo et al. [GPPS19]
Multi-user security in nonce-misuse resilience setting
Multi-user security under leakage resilience

only "proof sketches"
contain gaps [LM24]

2023 Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

2024 Lefevre and Mennink [LM24]
Multi-user security in nonce-respecting and nonce-misuse setting
Multi-user security under state recovery

equal versus independent p, q

2024 Chakraborty et al. [CDN24]
Extended [CDN23] to multi-user security and nonce-misuse setting

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

2019 Guo et al. [GPPS19]

Multi-user security in nonce-misuse resilience setting

Multi-user security under leakage resilience

only "proof sketches"

contain gaps [LM24]

2023 Chakraborty et al. [CDN23]

Single-user security in nonce-respecting setting

equal versus independent p, q

2024 Lefevre and Mennink [LM24]

Multi-user security in nonce-respecting and nonce-misuse setting

Multi-user security under state recovery

2024 Chakraborty et al. [CDN24]

Extended [CDN23] to multi-user security and nonce-misuse setting

contains mistake (this work)

History of Generic Security Results (2/2)

Dedicated Ascon Analysis

2019 Guo et al. [GPPS19]
Multi-user security in nonce-misuse resilience setting
Multi-user security under leakage resilience

only "proof sketches"
contain gaps [LM24]

2023 Chakraborty et al. [CDN23]
Single-user security in nonce-respecting setting

2024 Lefevre and Mennink [LM24]
Multi-user security in nonce-respecting and nonce-misuse setting
Multi-user security under state recovery

equal versus independent p, q

2024 Chakraborty et al. [CDN24]
Extended [CDN23] to multi-user security and nonce-misuse setting

contains mistake (this work)

2025 Lefevre and Mennink (this work)
Let's clean this up!

Complete Overview of Generic Security of the Ascon-AE Mode

Complete Overview of Generic Security of the Ascon-AE Mode

- Three flavors of conventional security:
  1. Nonce-respecting security [BN00]
  2. Nonce-misuse resistance [RS06]
  3. Nonce-misuse resilience [ADL17]

Complete Overview of Generic Security of the Ascon-AE Mode

- Three flavors of conventional security:
  1. Nonce-respecting security [BN00]
  2. Nonce-misuse resistance [RS06]
  3. Nonce-misuse resilience [ADL17]
- Three flavors of leaky security:
  1. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  2. State-recovery security [LM24]
  3. Security under release of unverified plaintext [ABL+14]

Complete Overview of Generic Security of the Ascon-AE Mode

- Three flavors of conventional security:
  1. Nonce-respecting security [BN00]
  2. Nonce-misuse resistance [RS06]
  3. Nonce-misuse resilience [ADL17]
- Three flavors of leaky security:
  1. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  2. State-recovery security [LM24]
  3. Security under release of unverified plaintext [ABL+14]
- We categorize existing lower and upper bounds
- We derive new security bounds and matching attacks where needed

Complete Overview of Generic Security of the Ascon-AE Mode

- Three flavors of conventional security:
  1. Nonce-respecting security [BN00]
  2. Nonce-misuse resistance [RS06]
  3. Nonce-misuse resilience [ADL17]
- Three flavors of leaky security:
  1. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  2. State-recovery security [LM24]
  3. Security under release of unverified plaintext [ABL+14]
- We categorize existing lower and upper bounds
- We derive new security bounds and matching attacks where needed
- All results assume that $p = q$ is a random permutation

Overview of Results on Ascon-AE

nonce-respecting security
confidentiality
authenticity

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

bounds of [CDN23, CDN24]
carry over
new: matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

bounds of [CDN23, CDN24]
carry over
new: matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

μ number of users
$Q_E/\mathcal{M}_E$ encryption queries/complexity
$Q_D/\mathcal{M}_D$ decryption queries/complexity
$Q/\mathcal{M}$ construction queries/complexity
$\mathcal{N}$ permutation queries

new: flaw in proof of [CDN24]
new: transformation of [LM24] to $p = q$ setting
new: matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

analysis of [GPPS19] incomplete
new: security bounds
and matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

analysis of [GPPS19] incomplete

new: security bounds

and matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

leakage resilience, no leakage	
confidentiality	
authenticity	

leakage resilience, limited	
confidentiality	
authenticity	

leakage resilience, unlimited	
confidentiality	
authenticity	

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{MN}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{MN}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

$\Updownarrow$

leakage resilience, no leakage	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{MN}}{2^c}$

follows by equivalence

leakage resilience, limited	
confidentiality	
authenticity	

leakage resilience, unlimited	
confidentiality	
authenticity	

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

core term $(\star)$

$\Updownarrow$

leakage resilience, no leakage	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

leakage resilience, limited	
confidentiality	
authenticity	

analysis of [GPPS19] incomplete
and in different model
new: security bounds
and matching attacks

leakage resilience, unlimited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

nonce-respecting security $\Longleftarrow$ nonce-misuse resilience $\Longleftarrow$ nonce-misuse resistance

nonce-misuse resilience $\Updownarrow$ leakage resilience, no leakage

leakage resilience, no leakage	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Uparrow$

leakage resilience, limited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

$\Uparrow \quad \Downarrow\cap$

leakage resilience, unlimited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

follows by implication

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Updownarrow$

leakage resilience, no leakage	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Uparrow$

leakage resilience, limited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

$\Uparrow \quad \Downarrow$

leakage resilience, unlimited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

$\Longleftarrow$

state-recovery security	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{N}^2}{2^c}$

new: transformation of [LM24] to $p = q$ setting

new: matching attacks

Overview of Results on Ascon-AE

nonce-respecting security	
confidentiality	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resilience	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Longleftarrow$

nonce-misuse resistance	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

core term $(\star)$

μ	number of users
$Q_E/\mathcal{M}_E$	encryption queries/complexity
$Q_D/\mathcal{M}_D$	decryption queries/complexity
$Q/\mathcal{M}$	construction queries/complexity
$\mathcal{N}$	permutation queries

$\Updownarrow$

leakage resilience, no leakage	
confidentiality	$(\star) + \frac{\mathcal{M}_E\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Uparrow$

leakage resilience, limited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

RUP security	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

$\Uparrow$ $\Downarrow^{c}$

$\Uparrow^{\text{auth}}$

leakage resilience, unlimited	
confidentiality	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c} + \min\left\{\frac{\mathcal{N}^2}{2^c}, \frac{Q\mathcal{N}}{2^k}\right\}$

$\Longleftarrow$

state-recovery security	
confidentiality	1
authenticity	$(\star) + \frac{\mathcal{N}^2}{2^c}$

new: security bounds
and matching attacks

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting		
nonce-misuse resilience		
nonce-misuse resistance		
state-recovery security		

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}, Q_D \ll 2^t$
nonce-misuse resilience		
nonce-misuse resistance		
state-recovery security		

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}, Q_D \ll 2^t$
nonce-misuse resilience	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
nonce-misuse resistance		
state-recovery security		

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}, Q_D \ll 2^t$
nonce-misuse resilience	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
nonce-misuse resistance	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
state-recovery security		

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}, Q_D \ll 2^t$
nonce-misuse resilience	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
nonce-misuse resistance	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
state-recovery security	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^{c/2}\}, \quad Q_D \ll 2^t$

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$, $Q_D \ll 2^t$
nonce-misuse resilience	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$, $Q_D \ll 2^t$
nonce-misuse resistance	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$, $Q_D \ll 2^t$
state-recovery security	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^{c/2}\}$, $Q_D \ll 2^t$

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 online complexity of $Q, \mathcal{M} \ll 2^{64}$ (could be taken higher)

Simplified Numerical Interpretation

setting	confidentiality as long as	authenticity as long as
nonce-respecting	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^b/\mathcal{M}, 2^c\}, Q_D \ll 2^t$
nonce-misuse resilience	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
nonce-misuse resistance	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
state-recovery security	—	$\mathcal{N} \ll \min\{2^k/\mu, 2^{c/2}\}, \quad Q_D \ll 2^t$

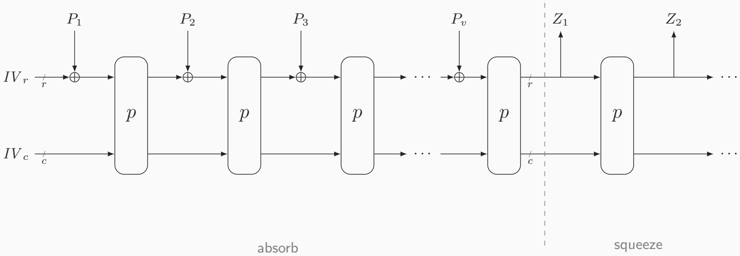
Application to Ascon-AEAD Parameters

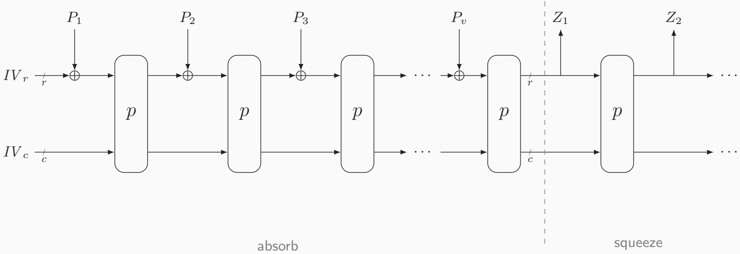
- $(k, b, c, r, t) = \begin{cases} (128, 320, 256, 64, 128) \text{ for Ascon-128} \\ (128, 320, 192, 128, 128) \text{ for Ascon-128a} \\ (160, 320, 256, 64, 128) \text{ for Ascon-80pq} \end{cases}$
- Assume online complexity of $Q, \mathcal{M} \ll 2^{64}$ (could be taken higher)
- Generic security as long as $\mathcal{N} \ll 2^{128}/\mu$

(exceptions: $\mathcal{N} \ll 2^{160}/\mu$ for Ascon-80pq; $\mathcal{N} \ll 2^{96}$ for Ascon-128a under state-recovery)

Ascon-Hash/Ascon-(C)XOF

Ascon-Hash/Ascon-(C)XOF





Sponge [BDPV07]

- Permutation p on b bits
  - r is the rate
  - c is the capacity (security parameter)
- Output of ν bits (256 for Ascon-Hash, unlimited for the XOFs)

Generic Security of the Sponge

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]

Generic Security of the Sponge

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]
- Security of sponge truncated to ν bits against classical attacks [AMP10]:

Collision resistance:	$\mathcal{N}^2/2^c + \mathcal{N}^2/2^{\nu+1}$
Second preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^\nu$
Preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^\nu$

Generic Security of the Sponge

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]
- Security of sponge truncated to ν bits against classical attacks [AMP10]:

Collision resistance:	$\mathcal{N}^2/2^c + \mathcal{N}^2/2^{\nu+1}$
Second preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$
Preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$

distance from sponge to RO
($\mathcal{N}$ is # primitive evaluations)

classical attacks against RO
($\mathcal{N}$ is # oracle evaluations)

Generic Security of the Sponge

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]
- Security of sponge truncated to ν bits against classical attacks [AMP10]:

Collision resistance:	$\mathcal{N}^2/2^c + \mathcal{N}^2/2^{\nu+1}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu/2}\}$
Second preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu}\}$
Preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$	

distance from sponge to RO
($\mathcal{N}$ is # primitive evaluations)

classical attacks against RO
($\mathcal{N}$ is # oracle evaluations)

- Attacks already described in [BDPV07]

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]
- Security of sponge truncated to ν bits against classical attacks [AMP10]:

Collision resistance:	$\mathcal{N}^2/2^c + \mathcal{N}^2/2^{\nu+1}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu/2}\}$
Second preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu}\}$
Preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$	$\leftarrow$ attack in $\min\{2^{\nu-r} + 2^{c/2}, 2^{\nu}\}$

distance from sponge to RO
($\mathcal{N}$ is # primitive evaluations)

classical attacks against RO
($\mathcal{N}$ is # oracle evaluations)

- Attacks already described in [BDPV07]

Generic Security of the Sponge

- Sponge indifferentiable from random up to bound $\mathcal{N}^2/2^c$ [BDPV08]
- Security of sponge truncated to ν bits against classical attacks [AMP10]:

Collision resistance:	$\mathcal{N}^2/2^c + \mathcal{N}^2/2^{\nu+1}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu/2}\}$
Second preimage resistance:	$\mathcal{N}^2/2^c + \mathcal{N}/2^{\nu}$	$\leftarrow$ attack in $\min\{2^{c/2}, 2^{\nu}\}$
~~Preimage resistance:~~	$\cancel{\underbrace{\mathcal{N}^2/2^c}_{\uparrow} + \underbrace{\mathcal{N}/2^{\nu}}_{\uparrow}}$	~~$\leftarrow$ attack in $\min\{2^{\nu-r} + 2^{c/2}, 2^{\nu}\}$~~

distance from sponge to RO ($\mathcal{N}$ is # primitive evaluations)

classical attacks against RO ($\mathcal{N}$ is # oracle evaluations)

- Attacks already described in [BDPV07]
- Tightened preimage resistance bound by Lefevre and Mennink [LM22]:

Preimage resistance: $\min\{\mathcal{N}/2^{\nu-r}, \mathcal{N}/2^{c/2}\} + \mathcal{N}/2^{\nu}$ $\leftarrow$ attack in $\min\{2^{\nu-r} + 2^{c/2}, 2^{\nu}\}$

Application to Ascon-Hash and Ascon-(C)XOF Parameters

- $(b, c, r, \nu) = \begin{cases} (320, 256, 64, 256) \text{ for Ascon-Hash} \\ (320, 256, 64, \infty) \text{ for Ascon-XOF} \\ (320, 256, 64, \infty) \text{ for Ascon-CXOF} \end{cases}$

Application to Ascon-Hash and Ascon-(C)XOF Parameters

- $(b, c, r, \nu) = \begin{cases} (320, 256, 64, 256) \text{ for Ascon-Hash} \\ (320, 256, 64, \infty) \text{ for Ascon-XOF} \\ (320, 256, 64, \infty) \text{ for Ascon-CXOF} \end{cases}$
- Generic collision resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu/2}\}$

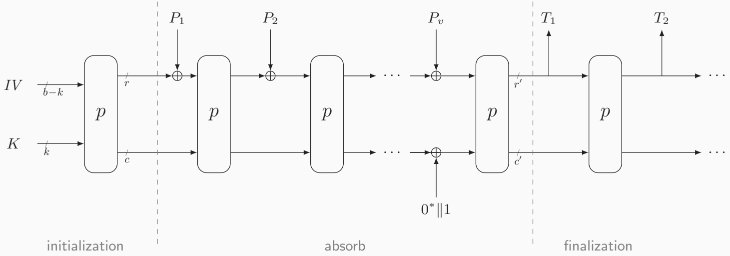
Application to Ascon-Hash and Ascon-(C)XOF Parameters

- $(b, c, r, \nu) = \begin{cases} (320, 256, 64, 256) \text{ for Ascon-Hash} \\ (320, 256, 64, \infty) \text{ for Ascon-XOF} \\ (320, 256, 64, \infty) \text{ for Ascon-CXOF} \end{cases}$
- Generic collision resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu/2}\}$
- Generic second preimage resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu}\}$

Application to Ascon-Hash and Ascon-(C)XOF Parameters

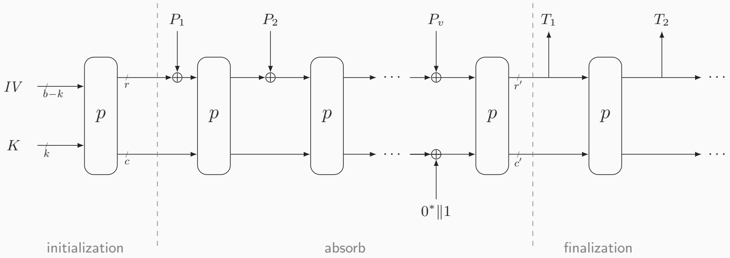
- $(b, c, r, \nu) = \begin{cases} (320, 256, 64, 256) \text{ for Ascon-Hash} \\ (320, 256, 64, \infty) \text{ for Ascon-XOF} \\ (320, 256, 64, \infty) \text{ for Ascon-CXOF} \end{cases}$
- Generic collision resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu/2}\}$
- Generic second preimage resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu}\}$
- Generic preimage resistance as long as $\mathcal{N} \ll \min\{2^{192}, 2^{\nu}\}$

Bonus: Ascon-PRF



Variant of Full-State Keyed Sponge [BDPV12, MRV15]

- Permutation p on b bits
  - r is the rate, c is the capacity (security parameter)



Variant of Full-State Keyed Sponge [BDPV12, MRV15]

- Permutation p on b bits
  - r is the rate, c is the capacity (security parameter)
- Domain separation to avoid squeezed tags being misused in absorption

FSKS and Ascon-PRF

FSKS and Ascon-PRF

2015 — Mennink et al. [MRV15]

Security of FSKS but with proof-inherent “multiplicity term”

FSKS and Ascon-PRF

2015 — Mennink et al. [MRV15]
Security of FSKS but with proof-inherent "multiplicity term"

2017 — Daemen et al. [DMV17]
Generalized duplex
Applies to Ascon-PRF but with non-tight term $\mathcal{M}\mathcal{N}/2^c$

Generic Security of Ascon-PRF (1/2)

FSKS and Ascon-PRF

2015 Mennink et al. [MRV15]
Security of FSKS but with proof-inherent "multiplicity term"

2017 Daemen et al. [DMV17]
Generalized duplex
Applies to Ascon-PRF but with non-tight term $\mathcal{M}\mathcal{N}/2^c$

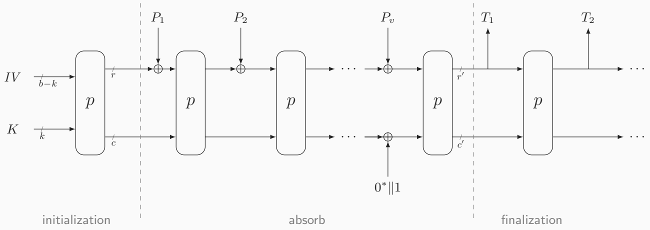
2019 Dobraunig and Mennink [DM19]
Leakage resilience of generalized duplex
Applies to Ascon-PRF

FSKS and Ascon-PRF

- 2015 — Mennink et al. [MRV15]
  Security of FSKS but with proof-inherent "multiplicity term"
- 2017 — Daemen et al. [DMV17]
  Generalized duplex
  Applies to Ascon-PRF but with non-tight term $\mathcal{M}\mathcal{N}/2^c$
- 2019 — Dobraunig and Mennink [DM19]
  Leakage resilience of generalized duplex
  Applies to Ascon-PRF
- 2023 — Mennink [Men23]
  Duplex guide and improved analysis of Ascon-PRF

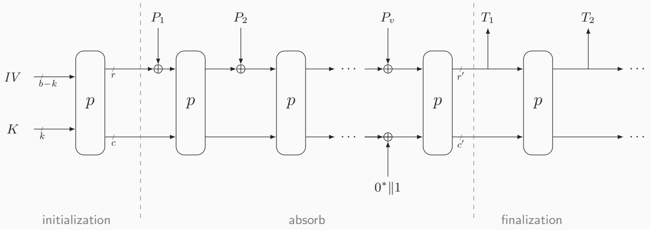
FSKS and Ascon-PRF

- 2015 Mennink et al. [MRV15]
  Security of FSKS but with proof-inherent “multiplicity term”
- 2017 Daemen et al. [DMV17]
  Generalized duplex
  Applies to Ascon-PRF but with non-tight term $\mathcal{M}\mathcal{N}/2^c$
- 2019 Dobraunig and Mennink [DM19]
  Leakage resilience of generalized duplex
  Applies to Ascon-PRF
- 2023 Mennink [Men23]
  Duplex guide and improved analysis of Ascon-PRF
- 2025 Lefevre and Mennink (this work)
  Adapt bound of [Men23] with improved multicollision strategy



Generic Security Bound

- Ascon-PRF is multi-user secure up to bound $\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{N}}{2^{c'}} + \frac{\mathcal{M}\mathcal{N}}{2^b}$

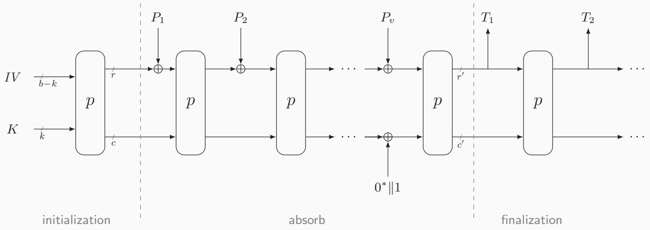


Generic Security Bound

- Ascon-PRF is multi-user secure up to bound $\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{N}}{2^{c'}} + \frac{\mathcal{M}\mathcal{N}}{2^b}$

Application to Ascon-PRF Parameters

- $(k, b, c, r, c', r', t) = (128, 320, 64, 256, 192, 128, \infty)$
- Assume online complexity of $\mathcal{M} \ll 2^{64}$ (could be taken higher)



Generic Security Bound

- Ascon-PRF is multi-user secure up to bound $\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{N}}{2^{c'}} + \frac{\mathcal{M}\mathcal{N}}{2^b}$

Application to Ascon-PRF Parameters

- $(k, b, c, r, c', r', t) = (128, 320, 64, 256, 192, 128, \infty)$
- Assume online complexity of $\mathcal{M} \ll 2^{64}$ (could be taken higher)
- Generic security as long as $\mathcal{N} \ll 2^{128}/\mu$

Conclusion

Conclusion

More in Paper: https://eprint.iacr.org/2024/1969

- Exact security models, settings, and discussions
- Discussion on multicollision bounding, assumption on $p, q, \ldots$
- All proofs and generic attacks

Conclusion

More in Paper: `https://eprint.iacr.org/2024/1969`

- Exact security models, settings, and discussions
- Discussion on multicollision bounding, assumption on $p, q, \ldots$
- All proofs and generic attacks

What We Did Not Cover

- Related-key security and security for arbitrary key distributions
- Security under fault attacks
- Variant with nonce masking [DM24]
- Committing security $\longrightarrow$ next talk!

Conclusion

More in Paper: `https://eprint.iacr.org/2024/1969`

- Exact security models, settings, and discussions
- Discussion on multicollision bounding, assumption on $p, q, \ldots$
- All proofs and generic attacks

What We Did Not Cover

- Related-key security and security for arbitrary key distributions
- Security under fault attacks
- Variant with nonce masking [DM24]
- Committing security $\longrightarrow$ next talk!

Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda.
How to Securely Release Unverified Plaintext in Authenticated Encryption.
In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 105–125. Springer, 2014.

Tomer Ashur, Orr Dunkelman, and Atul Luykx.
Boosting Authenticated Encryption Robustness with Minimal Modifications.
In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 3–33. Springer, 2017.

Elena Andreeva, Bart Mennink, and Bart Preneel.
Security Reductions of the Second Round SHA-3 Candidates.
In Mike Burmester, Gene Tsudik, Spyros S. Magliveras, and Ivana Ilic, editors, *Information Security - 13th International Conference, ISC 2010, Boca Raton, FL, USA, October 25-28, 2010, Revised Selected Papers*, volume 6531 of *Lecture Notes in Computer Science*, pages 39–53. Springer, 2010.

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, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

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, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011,*

Revised Selected Papers, volume 7118 of *Lecture Notes in Computer Science*, pages 320–337. Springer, 2011.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche.
Permutation-based encryption, authentication and authenticated encryption.
Directions in Authenticated Ciphers, July 2012.

Mihir Bellare and Chanathip Namprempre.
Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm.
In Tatsuaki Okamoto, editor, *Advances in Cryptology - ASIACRYPT 2000, 6th International Conference on the Theory and Application of Cryptology and*

Information Security, Kyoto, Japan, December 3-7, 2000, Proceedings, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer, 2000.

Bishwajit Chakraborty, Chandranan Dhar, and Mridul Nandi.
Exact Security Analysis of ASCON.
In Jian Guo and Ron Steinfeld, editors, *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III*, volume 14440 of *Lecture Notes in Computer Science*, pages 346–369. Springer, 2023.

Bishwajit Chakraborty, Chandranan Dhar, and Mridul Nandi.
Tight Multi-user Security of Ascon and Its Large Key Extension.
In Tianqing Zhu and Yannan Li, editors, *Information Security and Privacy - 29th Australasian Conference, ACISP 2024, Sydney, NSW, Australia, July 15-17, 2024, Proceedings, Part I*, volume 14895 of *Lecture Notes in Computer Science*, pages 57–76. Springer, 2024.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon v1.2: Lightweight Authenticated Encryption and Hashing.
J. Cryptol., 34(3):33, 2021.

Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer.
Ascon MAC, PRF, and Short-Input PRF - Lightweight, Fast, and Efficient Pseudorandom Functions.
In Elisabeth Oswald, editor, *Topics in Cryptology - CT-RSA 2024 - Cryptographers' Track at the RSA Conference 2024, San Francisco, CA, USA, May 6-9, 2024, Proceedings*, volume 14643 of *Lecture Notes in Computer Science*, pages 381–403. Springer, 2024.

Christoph Dobraunig and Bart Mennink.
Leakage Resilience of the Duplex Construction.
In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part III*, volume 11923 of *Lecture Notes in Computer Science*, pages 225–255. Springer, 2019.

Christoph Dobraunig and Bart Mennink.
Generalized Initialization of the Duplex Construction.
In Christina Pöpper and Lejla Batina, editors, *Applied Cryptography and Network Security - 22nd International Conference, ACNS 2024, Abu Dhabi, United Arab Emirates, March 5-8, 2024, Proceedings, Part II*, volume 14584 of *Lecture Notes in Computer Science*, pages 460–484. Springer, 2024.

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, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017,*

Proceedings, Part II, volume 10625 of *Lecture Notes in Computer Science*, pages 606–637. Springer, 2017.

- Stefan Dziembowski and Krzysztof Pietrzak.
Leakage-Resilient Cryptography.
In *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*, pages 293–302. IEEE Computer Society, 2008.

- Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction.
Cryptology ePrint Archive, Report 2019/193, 2019.
`http://eprint.iacr.org/2019/193` (full version of [GPPS20]).

Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert.
Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction.
IACR Trans. Symmetric Cryptol., 2020(1):6–42, 2020.

Philipp Jovanovic, Atul Luykx, and Bart Mennink.
Beyond $2^{c/2}$ Security in Sponge-Based Authenticated Encryption Modes.
In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 85–104. Springer, 2014.

Charlotte Lefevre and Bart Mennink.
Tight Preimage Resistance of the Sponge Construction.
In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part IV*, volume 13510 of *Lecture Notes in Computer Science*, pages 185–204. Springer, 2022.

Charlotte Lefevre and Bart Mennink.
Generic Security of the Ascon Mode: On the Power of Key Blinding.
In Maria Eichlseder and Sébastien Gambs, editors, *Selected Areas in Cryptography, 31st International Workshop, SAC 2024, Montréal, Quebec, Canada, August 26-27, Revised Selected Papers*, Lecture Notes in Computer Science. Springer, 2024.
to appear.

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

Bart Mennink, Reza Reyhanitabar, and Damian Vizár.
Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption.
In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 465–489. Springer, 2015.

Olivier Pereira, François-Xavier Standaert, and Srinivas Vivek.
Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives.
In Indrajit Ray, Ninghui Li, and Christopher Kruegel, editors, *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015*, pages 96–108. ACM, 2015.

Phillip Rogaway and Thomas Shrimpton.
A Provable-Security Treatment of the Key-Wrap Problem.
In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 373–390. Springer, 2006.