SoK: Security of the Ascon Modes

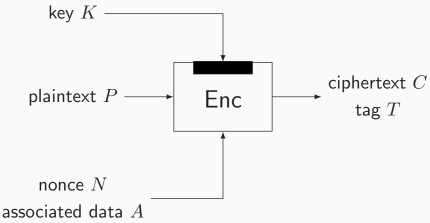
Charlotte Lefevre, Bart Mennink
Radboud University

GAPS 2025

September 4, 2025

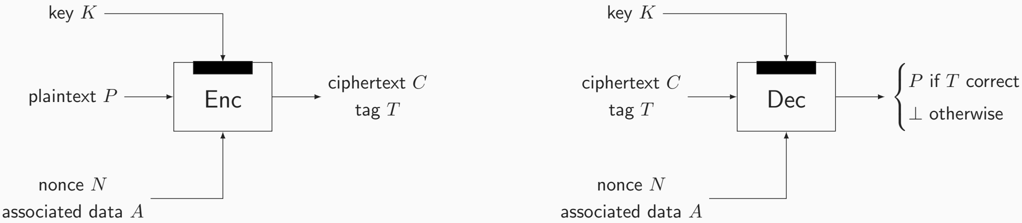
Introduction

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

Cryptographic Competitions

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

Ascon [DEMS21]

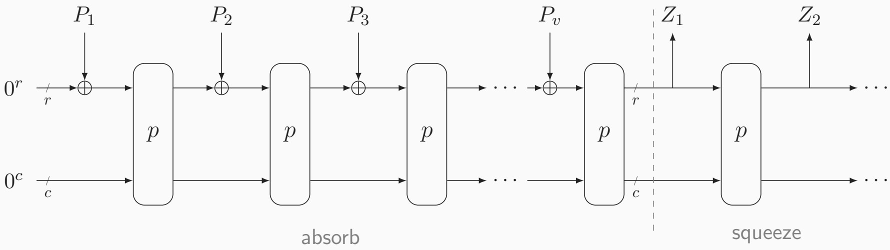
Authenticated Encryption

- Duplex-based but with additional key blindings

Hashing

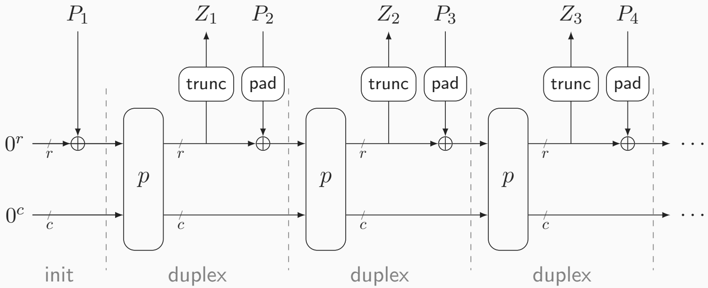
- Sponge-based hashing and XOFing
- Only included in NIST Lightweight Cryptography submission

Ascon-AE



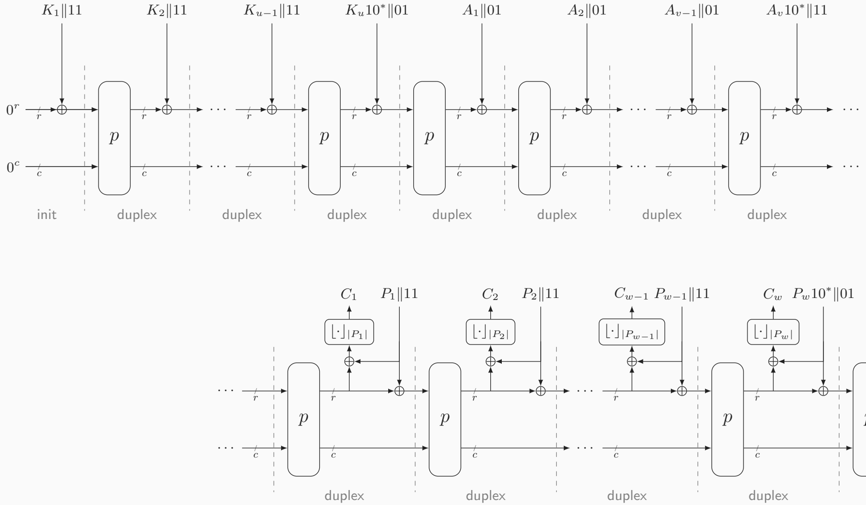
- Extendable Output Function (variable-length digest)
- State of size $b = r + c$ bits:
  - rate r (efficiency parameter)
  - capacity c (security parameter)
- $P_1 \| \cdots \| P_v$ is the message padded into r-bit blocks (e.g., 10^* padding)

The Duplex Construction [BDPV11]



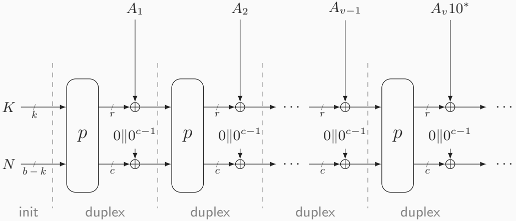
- Stateful version of sponge
- Interleaved absorb and squeeze
- Main application: authenticated encryption

SpongeWrap [BDPV11]

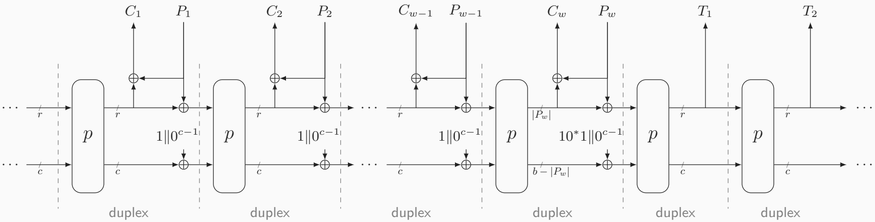


- SpongeWrap embeds duplex

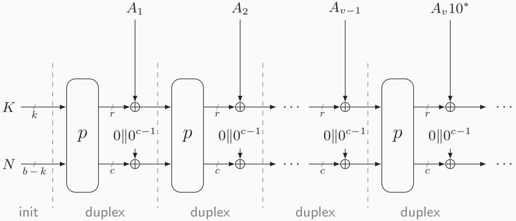
MonkeySpongeWrap [Men23]



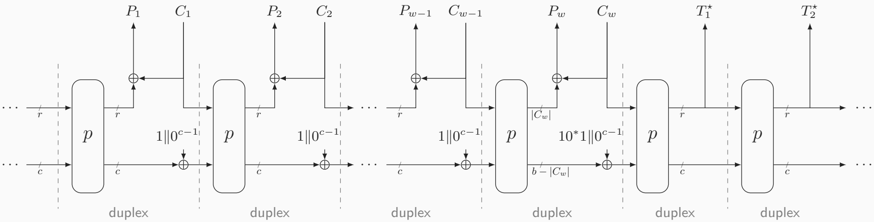
- State initialized using key and nonce
- Cleaned-up and synchronized domain separation
- Spill-over into inner part



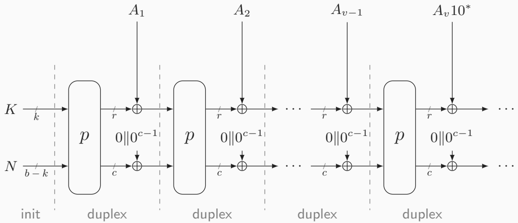
MonkeySpongeWrap [Men23]



- State initialized using key and nonce
- Cleaned-up and synchronized domain separation
- Spill-over into inner part
- Decryption similar to encryption

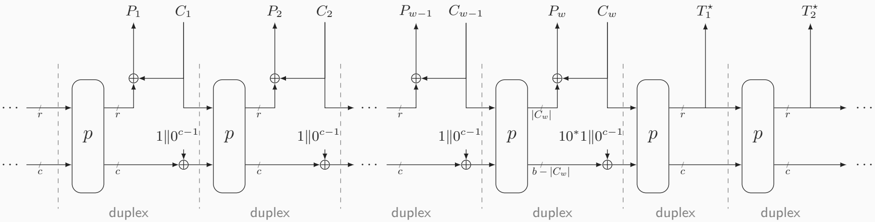


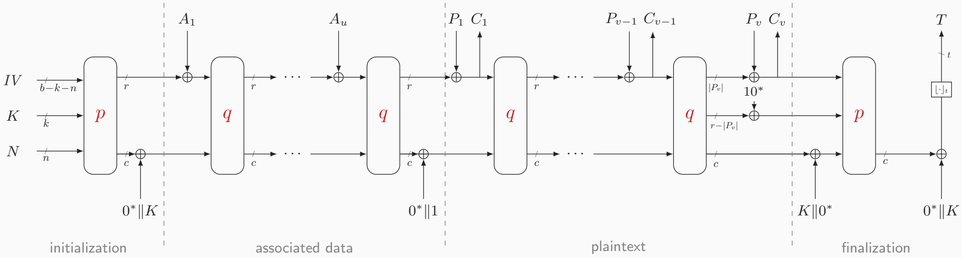
MonkeySpongeWrap [Men23]



- State initialized using key and nonce
- Cleaned-up and synchronized domain separation
- Spill-over into inner part
- Decryption similar to encryption

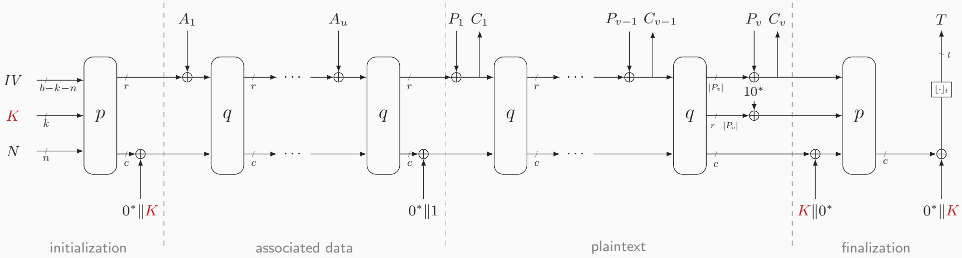
security depends on permutation strength, nonce conditions, and parameters





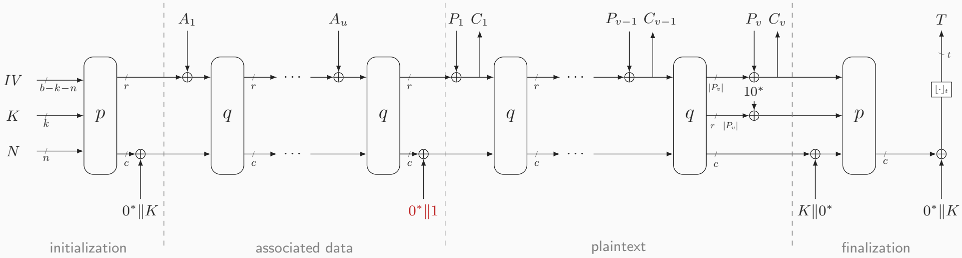
Variant of (Monkey-)SpongeWrap [BDPV11, Men23]

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



Variant of (Monkey-)SpongeWrap [BDPV11, Men23]

- 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 (Monkey-)SpongeWrap [BDPV11, Men23]

- 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

SpongeWrap and Similar

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

SpongeWrap and Similar

2011 Bertoni et al. [BDPV11]
Duplex and SpongeWrap

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

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

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
- 2023 — Mennink [Men23]
  Duplex guide and MonkeySpongeWrap

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

History of Generic Security Results (2/2)

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

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

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

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

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

Our Contribution

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. Security under release of unverified plaintext [ABL+14]
  2. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  3. State-recovery security [LM24]

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. Security under release of unverified plaintext [ABL+14]
  2. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  3. State-recovery security [LM24]
- 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. Security under release of unverified plaintext [ABL+14]
  2. Bounded leakage resilience in leveled implementation [DP08, PSV15]
  3. State-recovery security [LM24]
- 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

Conventional Security

1. **Nonce-respecting security** [BN00]
   - Confidentiality: distance $\left(\mathsf{Enc}_K^p, p\,;\, \$, p\right)$
   - Authenticity: $\mathbf{Pr}\left(\mathcal{A}\left[\mathsf{Enc}_K^p, \mathsf{Dec}_K^p, p\right] \text{ forges}\right)$
   - $\mathcal{A}$ never repeats the same nonce for encryption queries

Conventional Security

1. **Nonce-respecting security** [BN00]
   - Confidentiality: distance $\left(\text{Enc}_K^p, p\,;\,\$, p\right)$
   - Authenticity: $\mathbf{Pr}\left(\mathcal{A}\left[\text{Enc}_K^p, \text{Dec}_K^p, p\right]\text{ forges}\right)$
   - $\mathcal{A}$ never repeats the same nonce for encryption queries
2. **Nonce-misuse resistance** [RS06]
   - Same, but $\mathcal{A}$ may repeat the same nonce for encryption queries
   - Ascon does not achieve nonce-misuse confidentiality
   - In general, not achievable by one-pass AEs
   - Authenticity still achievable

❷ **Nonce-misuse resilience** [ADL17]

- Idea: challenge oracles for non-reused nonces only (but $\mathcal{A}$ may still repeat nonces in leaky oracles)
- Confidentiality: distance $\left(\mathsf{Enc}_K^p, \mathsf{LEnc}_K^p, p\,;\, \$, \mathsf{LEnc}_K^p, p\right)$
- Authenticity: $\mathbf{Pr}\left(\mathcal{A}\left[\mathsf{Enc}_K^p, \mathsf{LEnc}_K^p, \mathsf{Dec}_K^p, p\right] \text{ forges}\right)$

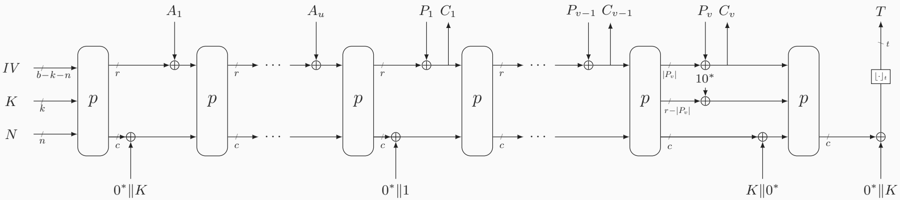
❷ **Nonce-misuse resilience** [ADL17]

- Idea: challenge oracles for non-reused nonces only (but $\mathcal{A}$ may still repeat nonces in leaky oracles)
- Confidentiality: distance $\left(\mathsf{Enc}_K^p, \mathsf{LEnc}_K^p, p\,;\,\$, \mathsf{LEnc}_K^p, p\right)$
- Authenticity: $\mathbf{Pr}\left(\mathcal{A}\left[\mathsf{Enc}_K^p, \mathsf{LEnc}_K^p, \mathsf{Dec}_K^p, p\right] \text{ forges}\right)$

Leaky Security

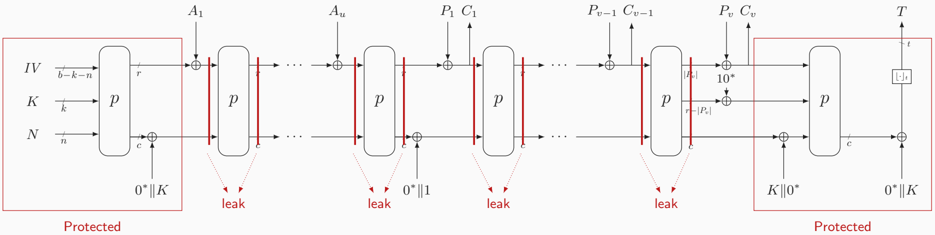
❶ **Security under release of unverified plaintext** [ABL+14]

- Confidentiality is covered by plaintext awareness
  - Ascon does not achieve plaintext awareness
  - In general, not achievable by nonce-based length-preserving AEs
- Authenticity still achievable



- Ascon was designed to provide some security even if the internal permutation evaluations leak (e.g., via side channels)

Security Model (3/3)

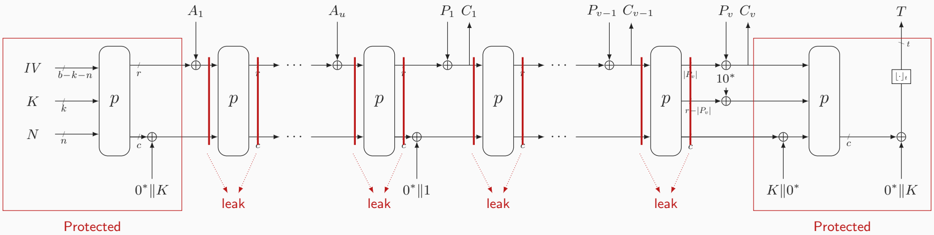


- Ascon was designed to provide some security even if the internal permutation evaluations leak (e.g., via side channels)

❷ **Leakage resilience**: inner evaluations leak information via a leakage function

- Outer evaluations do not leak (leveled implementation setup [DP08, PSV15])
- Adverary's oracle access is similar to nonce-misuse resilience, where LEnc/LDec additionally leak leakage function's output

Security Model (3/3)



- Ascon was designed to provide some security even if the internal permutation evaluations leak (e.g., via side channels)

❷ **Leakage resilience**: inner evaluations leak information via a leakage function
- Outer evaluations do not leak (leveled implementation setup [DP08, PSV15])
- Adverary's oracle access is similar to nonce-misuse resilience, where LEnc/LDec additionally leak leakage function's output

❸ **State recovery**: the entire inner b-bit states leaks, adversary may reuse nonces

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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
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	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$

$\Longleftarrow$

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

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	$\frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$
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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
authenticity	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$

leakage resilience, limited	
confidentiality	
authenticity	

leakage resilience, unlimited	
confidentiality	
authenticity	

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 equivalence

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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
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	$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$
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	$\frac{\mu\mathcal{N}}{2^k}+\frac{\mathcal{MN}}{2^b}+\frac{\mathcal{N}}{2^c}$
authenticity	$\frac{Q_D}{2^t}+\frac{\mu\mathcal{N}}{2^k}+\frac{\mathcal{MN}}{2^b}+\frac{\mathcal{N}}{2^c}$

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	$(\star)+\frac{\mathcal{MN}}{2^c}$
authenticity	$(\star)+\frac{\mathcal{MN}}{2^c}$

$\Longleftarrow$

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

$\Updownarrow$

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

$\Uparrow$

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

$\Uparrow \quad \Downarrow$

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

follows by implication

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	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

$\Longleftarrow$

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

$\Longleftarrow$

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

$\Updownarrow$

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

$\Uparrow$

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

$\Uparrow \quad \Downarrow$

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

$\Longleftarrow$

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

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

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	$\frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$

core term $(\star)$

$\Longleftarrow$

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

$\Longleftarrow$

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

$\Updownarrow$

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

$\Uparrow$

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

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

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

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

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

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

$\Longleftarrow$

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: 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	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
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	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}$	$\mathcal{N} \ll \min\{2^k/\mu, 2^c/\mathcal{M}\}, \quad Q_D \ll 2^t$
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 $Q, \mathcal{M} \ll 2^{64} \cdot \mu$

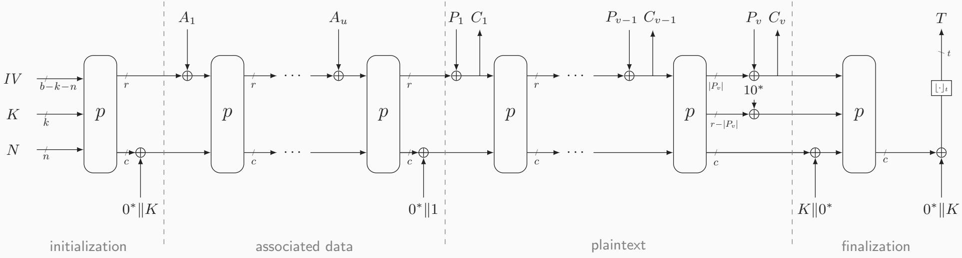
Simplified Numerical Interpretation

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

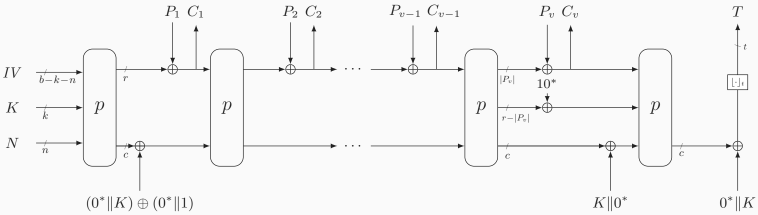
- $(k, b, c, r, t) = \begin{cases} (128, 320, 256, 64, 128) \text{ for Ascon-128} \\ (128, 320, 192, 128, 128) \text{ for Ascon-128a} \\ (160, 320, 256, 64, 128) \text{ for Ascon-80pq} \end{cases}$
- Assume online complexity of $Q, \mathcal{M} \ll 2^{64} \cdot \mu$
- Generic security as long as $\mathcal{N}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

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



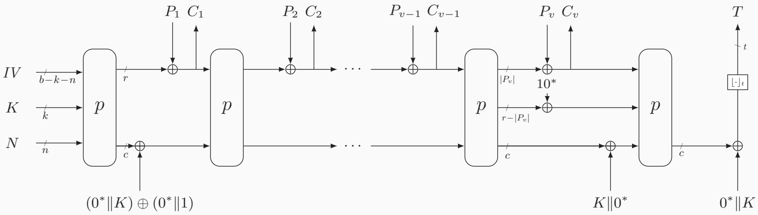
General Goal: Forgery

- Observe multiple evaluations $\mathsf{Enc}_K(N, A, P) = (C, T)$
- Output a new tuple (N, A, C, T) for which Dec_K does not return $\perp$



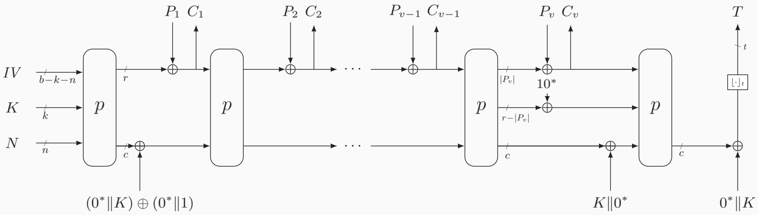
General Setup

- Adversary ignores associated data



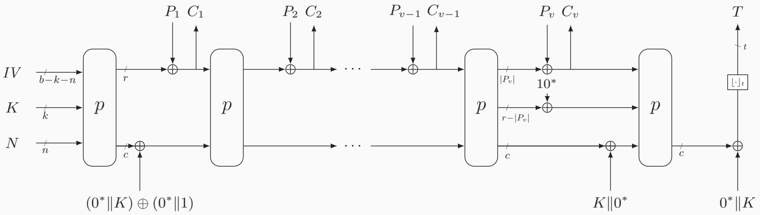
General Setup

- Adversary ignores associated data
- Adversary can make $\mathcal{N}$ queries to p,
  $\mathcal{M}$ construction queries,
  Q_D forgery attempts



Nonce-Respecting Adversary

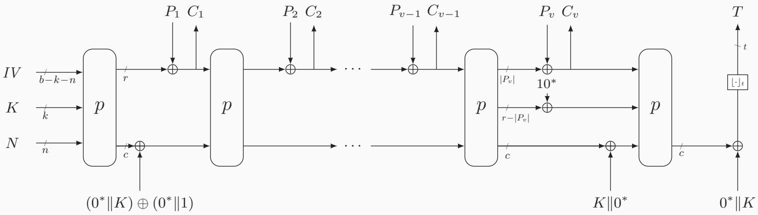
$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$



$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

Nonce-Respecting Adversary

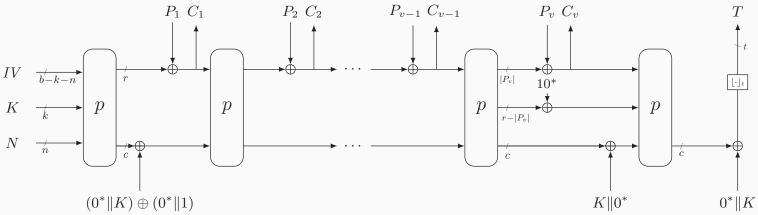
- First term corresponds to random tag guessing:
  - Any guess succeeds with probability $1/2^t$



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

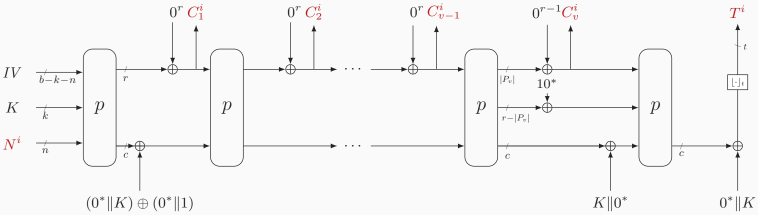
- First term corresponds to random tag guessing:
  - Any guess succeeds with probability $1/2^t$
- Second term corresponds to random key guessing:
  - Any guess succeeds with probability $\mu/2^k$ (as there are μ keys)



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

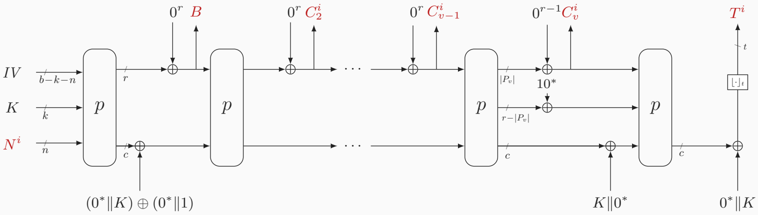
- Last two terms correspond to following attack:



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

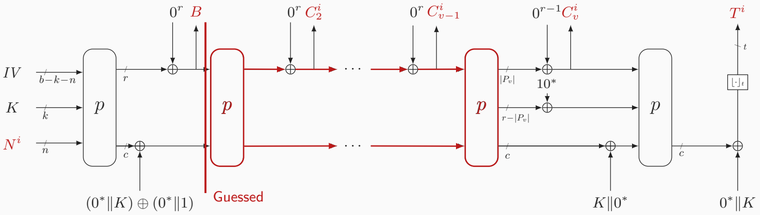
- Last two terms correspond to following attack:
  - Make $\mathcal{M}$ queries for plaintext 0^{rv-1}, get ciphertexts $C_1^i\|\cdots\|C_v^i$
  - Looking ahead, v is a logarithmic factor



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

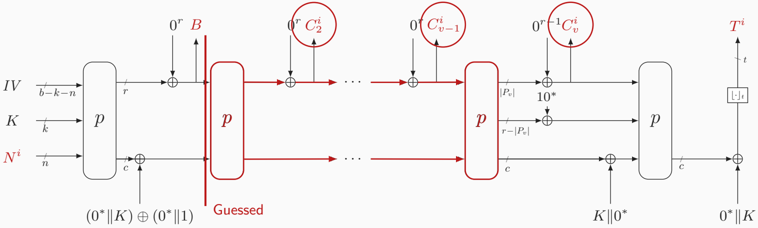
- Last two terms correspond to following attack:
  - Let $B \in \{0,1\}^r$ be the most frequent ciphertext block C_1^i
  - Query $p^f(B\|X_j)$, for $f = 1, \ldots, v-1$ and $\mathcal{N}$ random $X_j \in \{0,1\}^c$
  - Total cost: $\mathcal{N} \times (v-1)$ permutation queries (can be simplified)



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$$

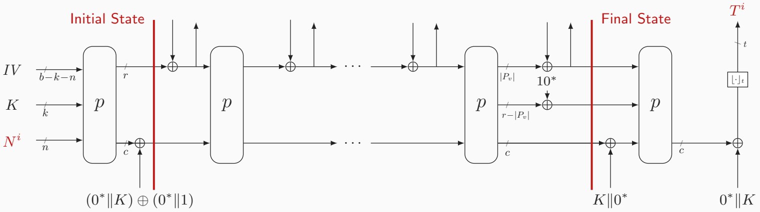
- Last two terms correspond to following attack:
  - With probability $\approx \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$, adversary guesses internal state



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$$

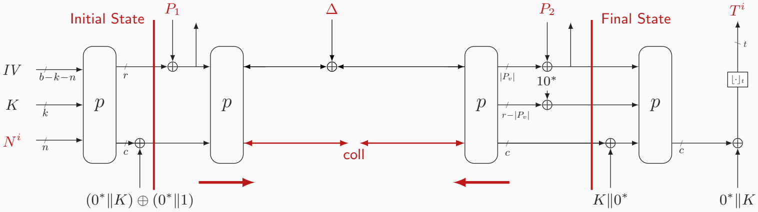
- Last two terms correspond to following attack:
  - With probability $\approx \frac{\mathcal{MN}}{2^b} + \frac{\mathcal{N}}{2^c}$, adversary guesses internal state
  - If v is large enough (e.g., $\approx \lceil b/r \rceil$), false positives can be discarded with high probability



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

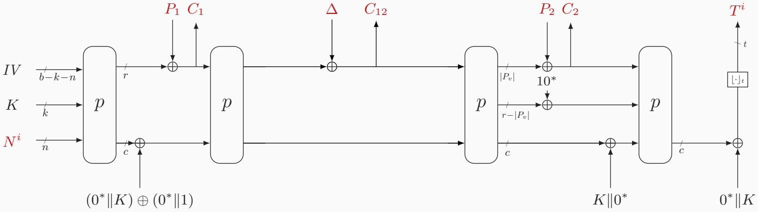
- Last two terms correspond to following attack:
  - Final step: connect initial and final states with a different plaintext



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

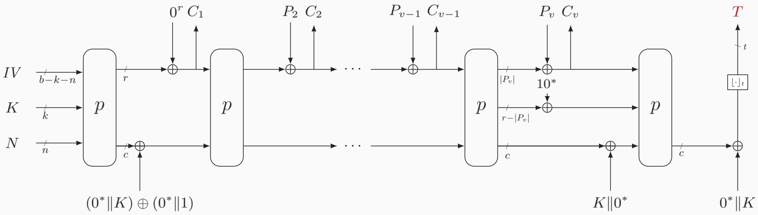
- Last two terms correspond to following attack:
  - Final step: connect initial and final states with a different plaintext
  - Boils down to finding inner collisions, success probability $\approx \frac{\mathcal{N}(\mathcal{N}-1)}{2^{c+1}}$



Nonce-Respecting Adversary

$$(\star) = \frac{Q_D}{2^t} + \frac{\mu\mathcal{N}}{2^k} + \frac{\mathcal{M}\mathcal{N}}{2^b} + \frac{\mathcal{N}}{2^c}$$

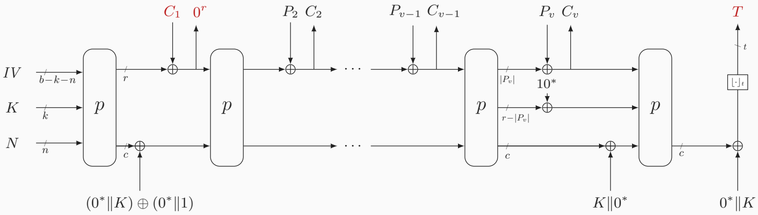
- Last two terms correspond to following attack:
  - Final step: connect initial and final states with a different plaintext
  - Boils down to finding inner collisions, success probability $\approx \frac{\mathcal{N}(\mathcal{N}-1)}{2^{c+1}}$
  - The input $(N^i, (C_1\|C_{12}\|C_2), T^i)$ is a valid forgery



Nonce-Misuse Resistance Adversary

$$(\star) + \frac{\mathcal{M}\mathcal{N}}{2^c}$$

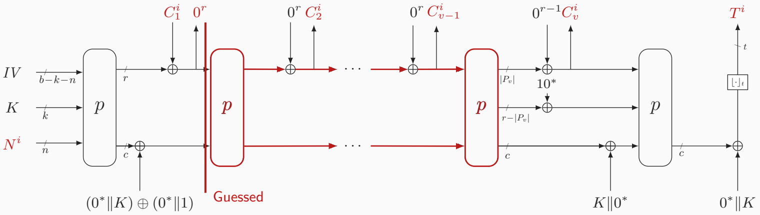
- This time the adversary can re-use nonces



Nonce-Misuse Resistance Adversary

$$(\star) + \frac{\mathcal{MN}}{2^c}$$

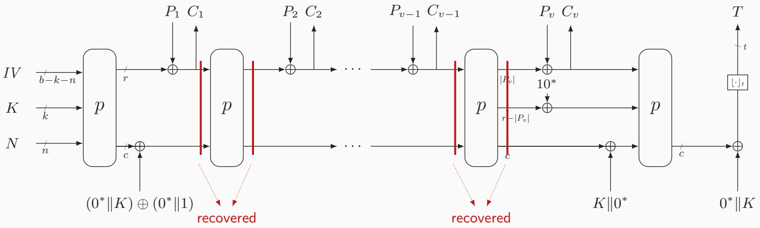
- This time the adversary can re-use nonces
- Allows overwriting the outer parts to a value of its choice



Nonce-Misuse Resistance Adversary

$$(\star) + \frac{\mathcal{MN}}{2^c}$$

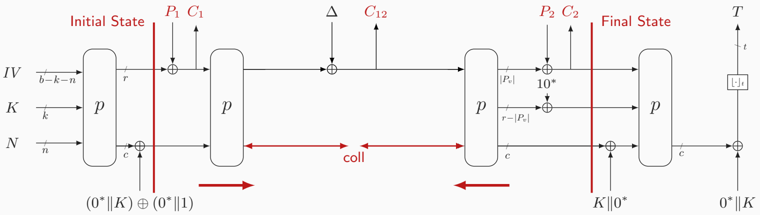
- This time the adversary can re-use nonces
- Allows overwriting the outer parts to a value of its choice
- Same strategy as before can be applied, but state guessing step sped up
  - Success probability of $\approx \frac{\mathcal{MN}}{2^c}$



State-Recovery Adversary

$$(\star) + \frac{\mathcal{N}^2}{2^c}$$

- The internal states leak

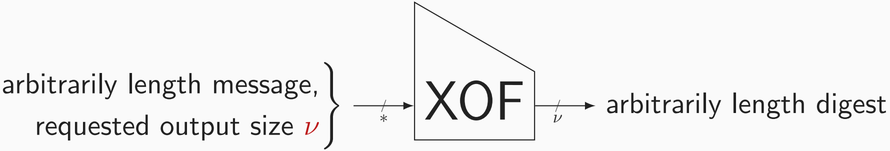


$$(\star) + \frac{\mathcal{N}^2}{2^c}$$

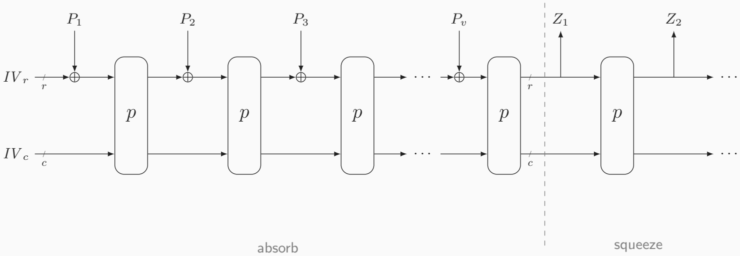
State-Recovery Adversary

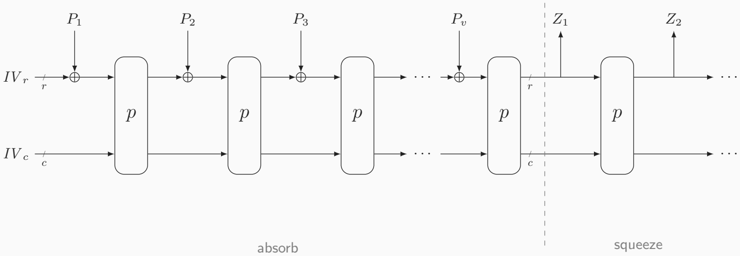
- The internal states leak
- It just remains to apply the last step of previous attacks
  - Success probability $\approx \frac{\mathcal{N}(\mathcal{N}-1)}{2^{c+1}}$

Ascon-Hash/Ascon-(C)XOF



- Function XOF from $\{0,1\}^*$ to $\{0,1\}^\infty$
  - Variable-length input
  - Variable-length output
  - User specifies output length ν when calling the function


P_1
P_2
P_3
P_v
Z_1
Z_2
IV_r
IV_c
r
c
p
absorb
squeeze



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:	$\mathcal{N}^2/2^c + \mathcal{N}/2^\nu$

- 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:	$\mathcal{N}^2/2^c + \mathcal{N}/2^\nu$	

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

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

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

$\uparrow$ 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:~~	$\cancel{\mathcal{N}^2/2^c + \mathcal{N}/2^\nu}$	~~$\leftarrow$ 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]
- Tightened preimage resistance bound by Lefevre and Mennink [LM22]:

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

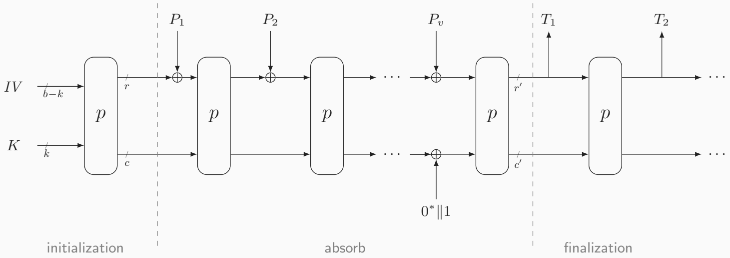
- $(b, c, r, \nu) = \begin{cases} (320, 256, 64, 256) \text{ for Ascon-Hash} \\ (320, 256, 64, \infty) \text{ for Ascon-XOF} \\ (320, 256, 64, \infty) \text{ for Ascon-CXOF} \end{cases}$
- Generic collision resistance as long as $\mathcal{N} \ll \min\{2^{128}, 2^{\nu/2}\}$
- Generic second preimage resistance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

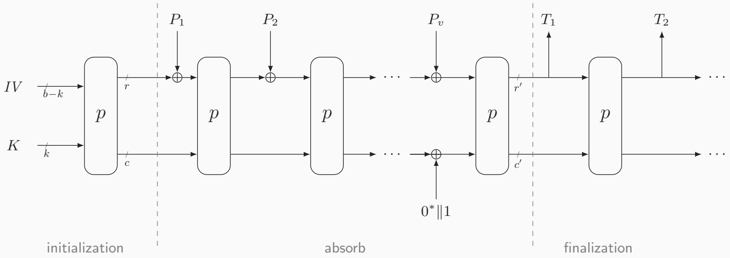
Bonus: Ascon-PRF [DEMS24]



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

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

Bonus: Ascon-PRF [DEMS24]



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

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”

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 $\mathcal{M}\mathcal{N}/2^c$

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

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

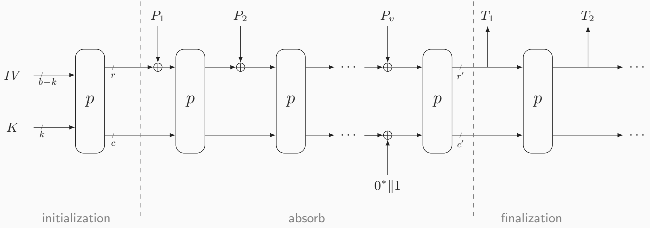
2023 Mennink [Men23]
Duplex guide and improved analysis of Ascon-PRF

Generic Security of Ascon-PRF (1/2)

FSKS and Ascon-PRF

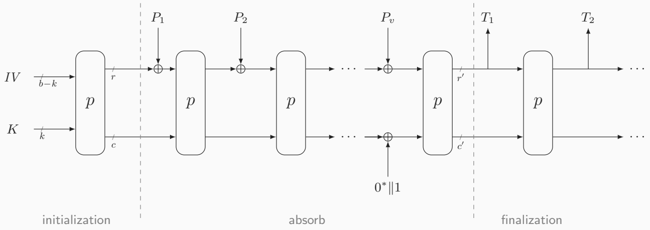
- 2015 — Mennink et al. [MRV15]
  Security of FSKS but with proof-inherent “multiplicity term”
- 2017 — Daemen et al. [DMV17]
  Generalized duplex
  Applies to Ascon-PRF but with non-tight term $\mathcal{M}\mathcal{N}/2^c$
- 2019 — Dobraunig and Mennink [DM19]
  Leakage resilience of generalized duplex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



Generic Security Bound

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

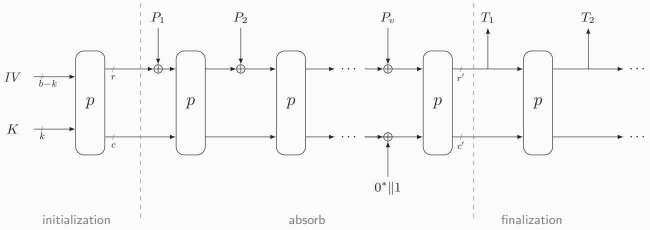


Generic Security Bound

- 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 $\mathcal{M} \ll 2^{64} \cdot \mu$ (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 $\mathcal{M} \ll 2^{64} \cdot \mu$ (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

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

Thank you for your attention!

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.