NTNU
Norwegian University of
Science and Technology

"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER
SCIENCE AND ENGINEERING

# π-CIPHER V2.0

Danilo Gligoroski, ITEM, NTNU, Norway
Hristina Mihajloska, FCSE, UKIM, Macedonia
Simona Samardjiska, FCSE, UKIM, Macedonia
Håkon Jacobsen, ITEM, NTNU, Norway
Mohamed El-Hadedy, University of Virginia, USA
Rune Erlend Jensen, IDI, NTNU, Norway
Daniel Otte, RUB, Germany

# About $\pi$ - Cipher

- Nonce-based authenticated encryption cipher with associated data
- Sponge based
  - key-less permutation function based on ARX operations
  - supports 16, 32 and 64-bit words
- Security in the range of 96 to 256 bits
- Uses secret message number (SMN)

# What is new!?

- Padding rule
  - Gaëtan Leurent and Thomas Fuhr

  *Observation on picipher. Message on the cryptocompetitions mailing list, Nov, 2014*

- The rule is now simple:
  - "Append 1 in any case, and fill the rest of the block with 0s"

| | | | | |
|---|---|---|---|---|
| $M_1$ | $M_2$ | . . . | $M_m$ | 10* |

# What is changed?

- The number of rounds R
- Now R = 3
  (previously it was R = 4)

# What is changed in explanation?

- From v2.0 $\pi$ -Cipher supports the concept of **"open authorship"**
  - it gives opportunity to all people that contribute anyhow in the development of $\pi$ -Cipher:
    - a tweak is introduced due to an analysis of the cipher,
    - a new mode of operation is proposed,
    - a new significantly different and improved implementation is given
  - if they want, they can be added to the list of designers for new versions or variants of $\pi$ -Cipher.

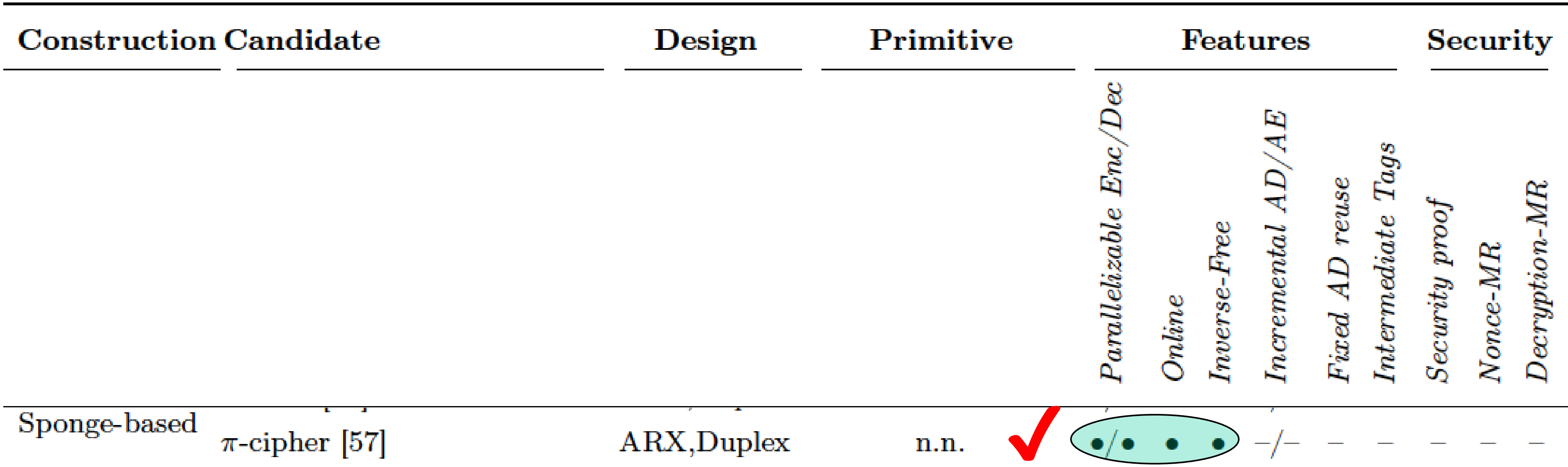
# What is changed in explanation?

- New parts in the documentation of $\pi$ -Cipher:
  - **The security proof of $\pi$ -Cipher**
  - Explanation of how to use tweakable parameter N for wide blocks
  - Explanation of how to securely use incremental property of $\pi$ -Cipher
  - Rational why we consider $\pi$ -Cipher to be STREAM OAE2+ design

# How $\pi$ - Cipher is perceived and what are its actual properties

- F. Abed, C. Forler and S. Lucks, "*General Overview of the Authenticated Schemes for the First Round of the CAESAR Competition*", Cryptology ePrint Archive, Report 2014/792

# How $\pi$ - Cipher is perceived and what are its actual properties

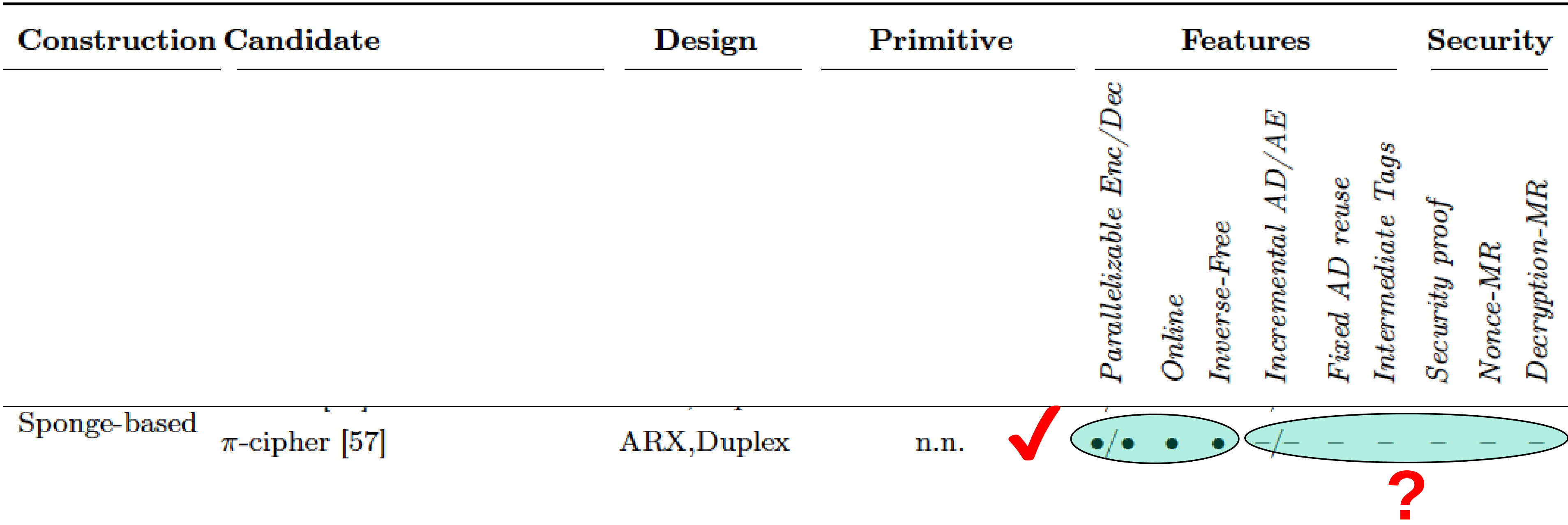


| Construction | Candidate | Design | Primitive | | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ✓ | •/• | • | • | –/– | – | – | – | – | – |

# Functional characteristics

1. Parallelizable
   - $\pi$ -Cipher is parallelizable in both encryption and decryption phases
2. Online
   - Encryption of the *i*-th input message block $M_i$ depends only on the common state *CIS*, *i* and $M_i$.
3. Inverse free
   - $\pi$ -Cipher does not use $\pi^{-1}$ of underlying permutation

# How $\pi$ - Cipher is perceived and what are its actual properties

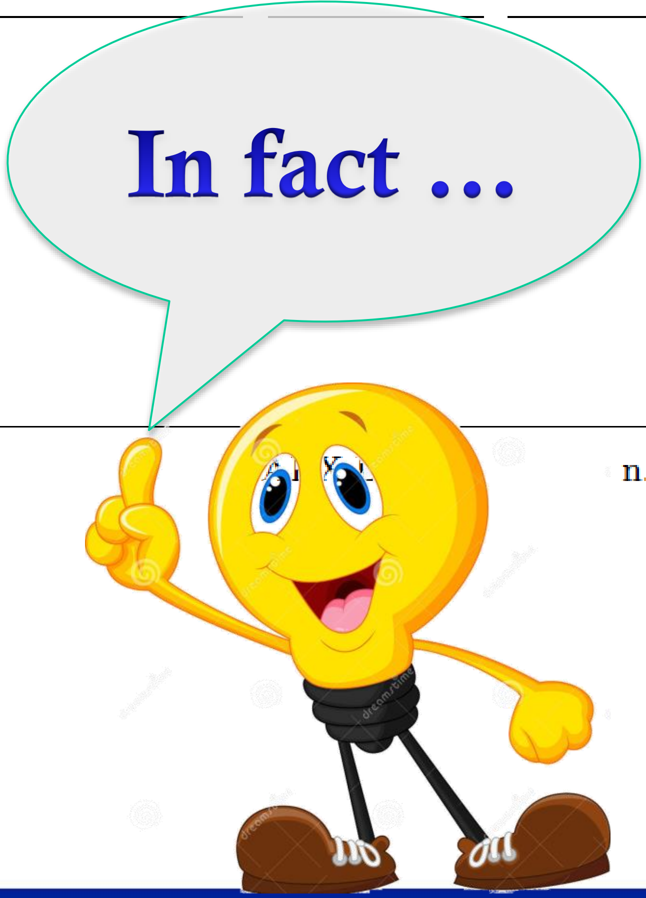


| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

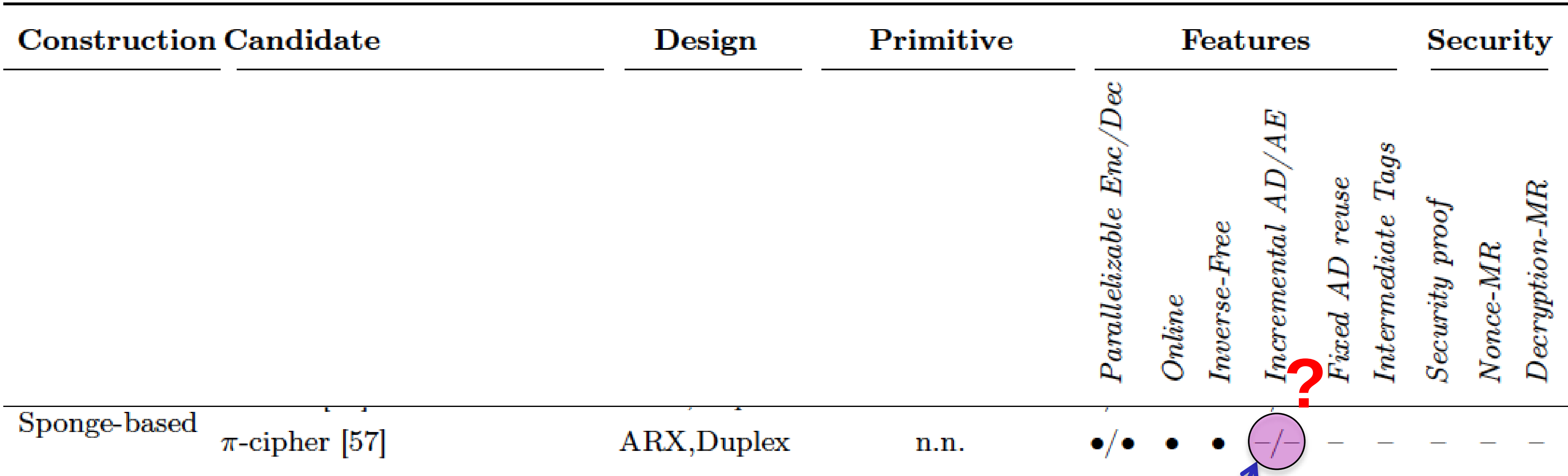
# How $\pi$ - Cipher is perceived and what are its actual properties

| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | | n.n. ✓ | ●/● | ● | ● | –/– | – | – | – | – | – |

?



# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | •/• | • | • | –/– | – | – | – | – | – |

?

Yes, with additional metadata for the plaintext (overhead), in which case it is secure even with complete
NONCE = (PMN, SMN) REUSE

# Incremental feature of $\pi$ - Cipher

- Incremental schemes have advantage over standard one when longer messages are used (ex. encrypting data in rest)
- In $\pi$ - Cipher incrementality and NMR are achieved with additional **metadata** overhead of 64 bits per block
  - Update counter *UpdCtr* that records the history of updates for every data block

# Incremental feature of $\pi$ - Cipher

- Adding 64 bits of metadata to existing data blocks of π-Cipher (128, 256 and 512 bits) is unacceptable big overhead
- We need bigger blocks!
- How to do that?
  - Change the length of the state
  - In our case it is doable by changing the parameter N
  - Make π-Cipher a wide block cipher

Another extra feature

# $\pi$ - Cipher as a wide block cipher

- Permutation state can be from 512B to 16KB
- Keeps the same security level even with 2 rounds

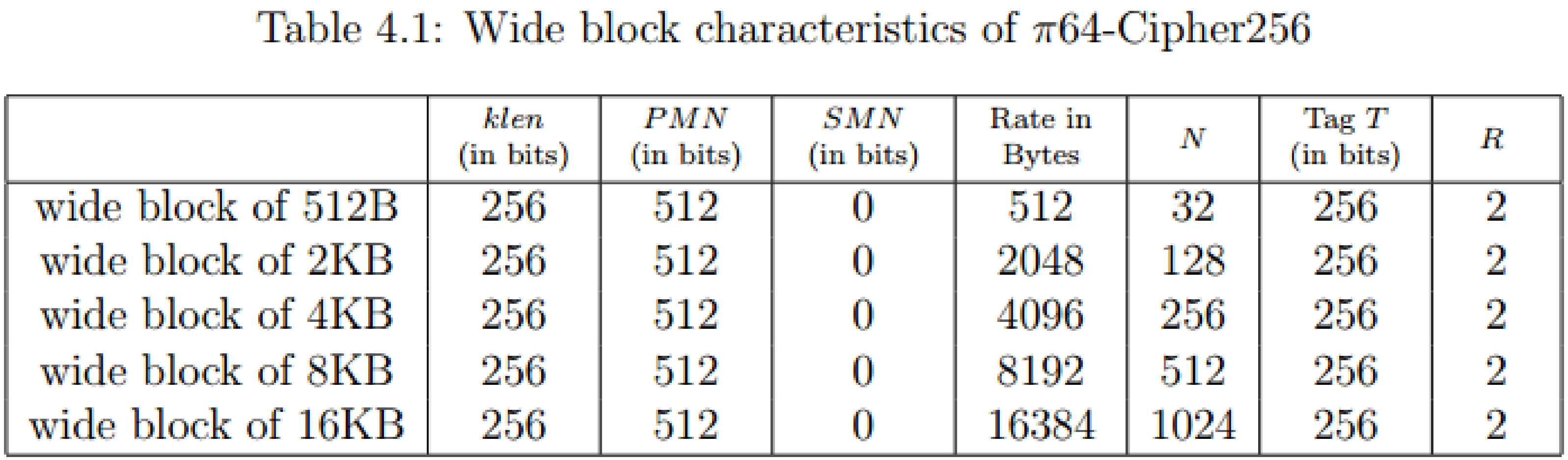
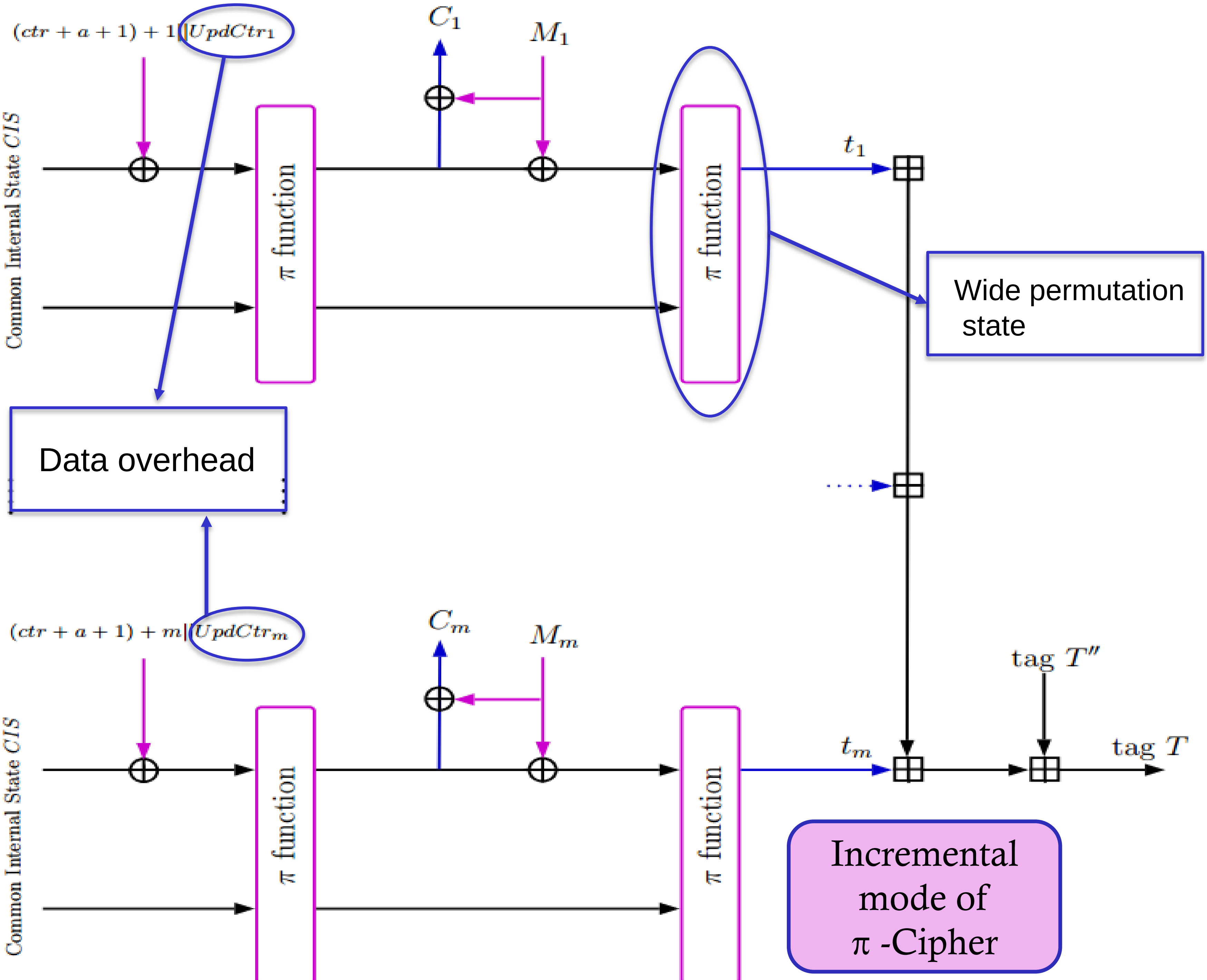


Table 4.1: Wide block characteristics of $\pi$64-Cipher256

| | $klen$ (in bits) | $PMN$ (in bits) | $SMN$ (in bits) | Rate in Bytes | $N$ | Tag $T$ (in bits) | $R$ |
|---|---|---|---|---|---|---|---|
| wide block of 512B | 256 | 512 | 0 | 512 | 32 | 256 | 2 |
| wide block of 2KB | 256 | 512 | 0 | 2048 | 128 | 256 | 2 |
| wide block of 4KB | 256 | 512 | 0 | 4096 | 256 | 256 | 2 |
| wide block of 8KB | 256 | 512 | 0 | 8192 | 512 | 256 | 2 |
| wide block of 16KB | 256 | 512 | 0 | 16384 | 1024 | 256 | 2 |

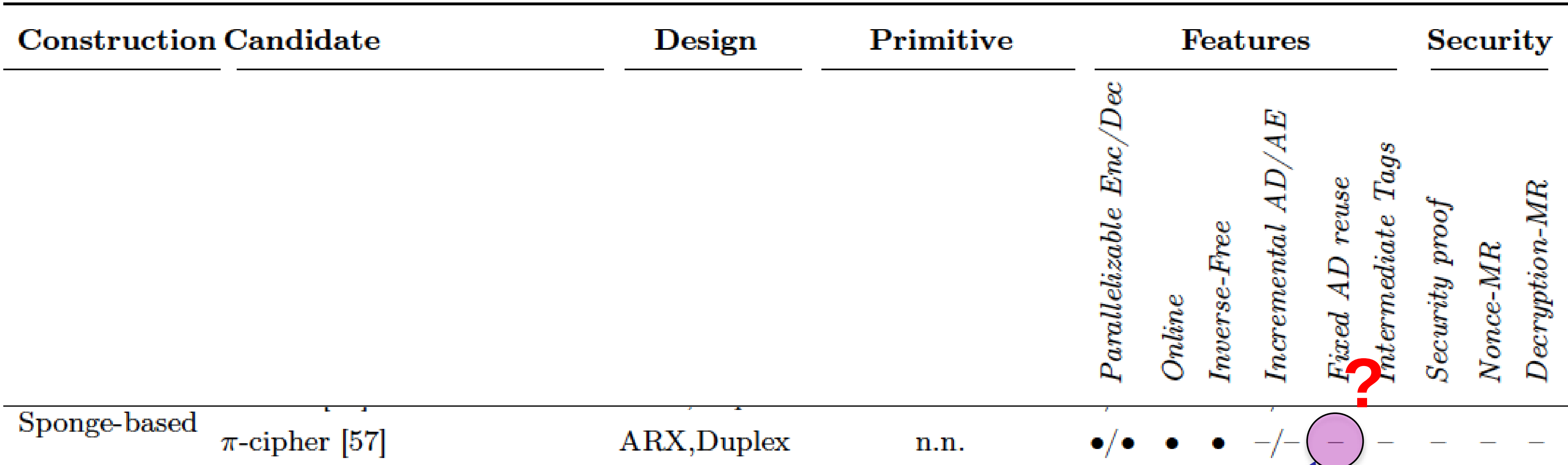

$(ctr + a + 1) + 1 \| UpdCtr_1$
$C_1$
$M_1$
Common Internal State $CIS$
$\pi$ function
$\pi$ function
$t_1$
$(ctr + a + 1) + m \| UpdCtr_m$
$C_m$
$M_m$
Common Internal State $CIS$
$\pi$ function
$\pi$ function
$t_m$
tag $T''$
tag $T$

Data overhead

Wide permutation state

Incremental mode of π -Cipher

# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | •/• | • | • | –/– | – | – | – | – | – |

?

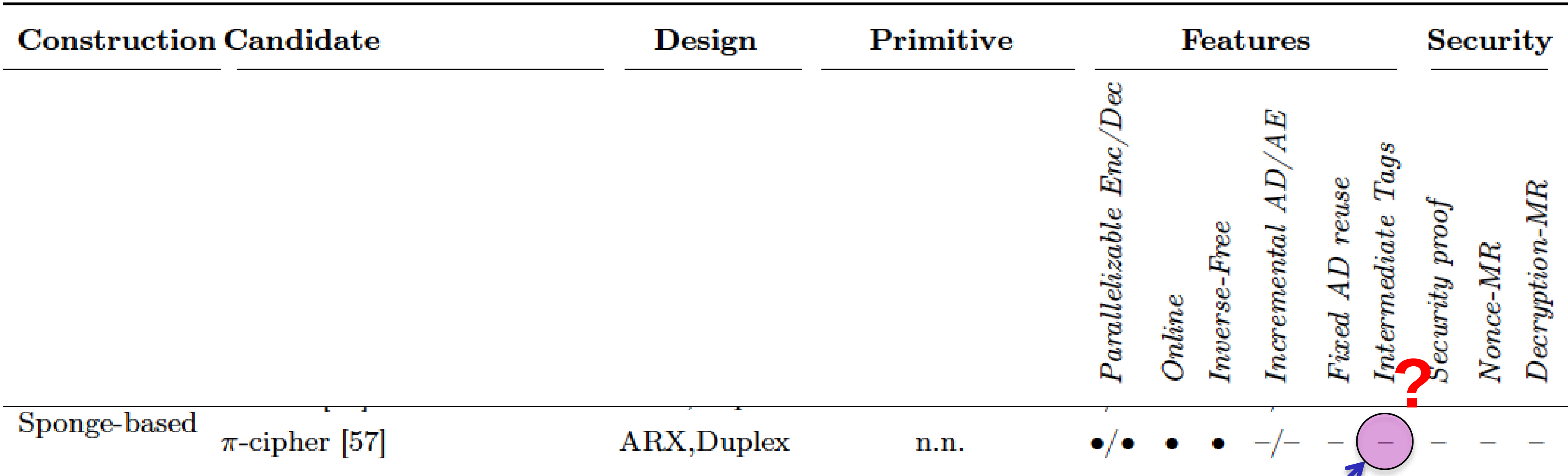
Yes, when PMN is reused but SMN is different

# Functional characteristics …

4. Fixed Associated Data Reuse

- It is possible in the case where PMN is the same and SMN is different
- Allows considerable speed-up (Initialization phase and Processing the AD are skipped)
    - A typical use-case scenario would be a secure communication between devices in Internet Of Things. They run the initial setup procedure once where AD is used, and then they send only short encrypted messages.

# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | •/• | • | • | –/– | – | – | – | – | – |

?

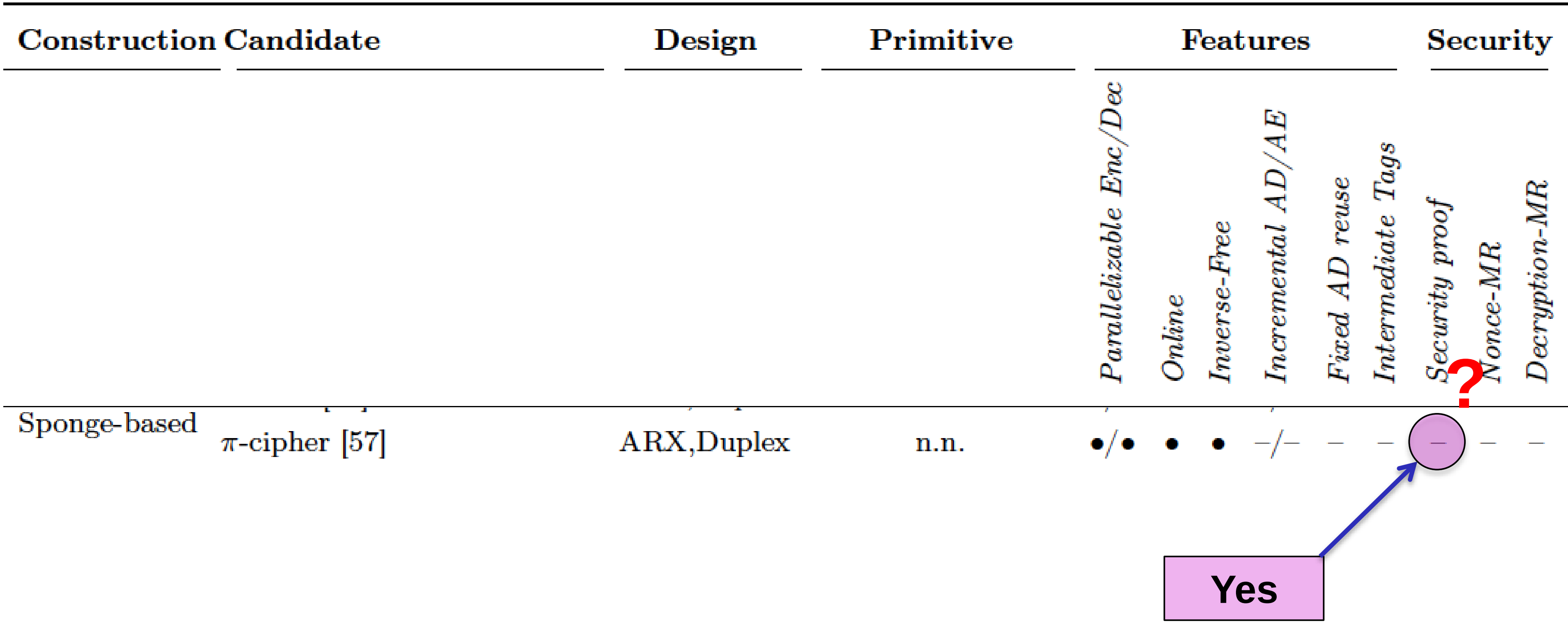
**Yes, π- Cipher always computes intermediate tags for every block. It is just a matter of a mode of operation to use them. Additionally, with the wide-block feature, the relative overhead of having intermediate tags goes to zero.**

# Functional characteristics …

5. By default, $\pi$ - Cipher has no ciphertext expansion

- The length of the ciphertext is the same as the length of the message before padding + the length of the SMN
- But, as a mode of operation, it is possible to output intermediate tags for every block. Security of the cipher is not affected by publishing these intermediate tags.
- In order to reduce the relative overhead of having intermediate tags, the wide-block feature of $\pi$ - Cipher should be used.

# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | •/• | • | • | –/– | – | – | – | – | – |

?

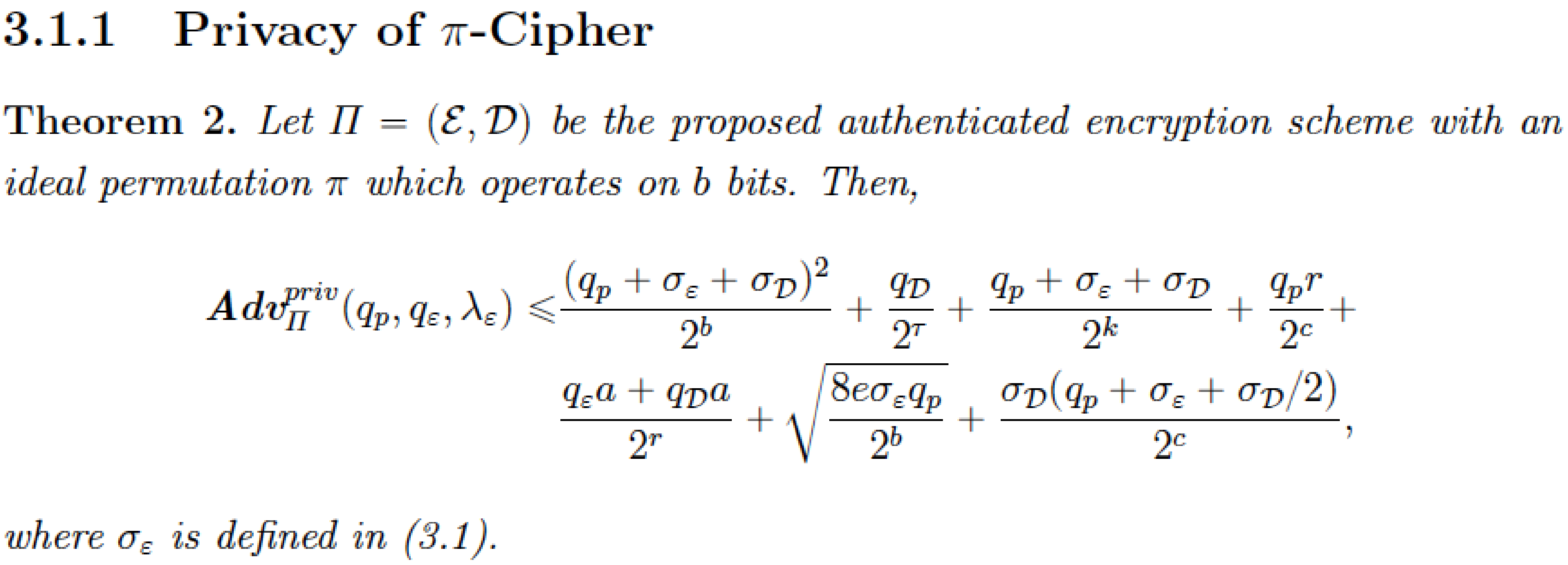
Yes

# Security proof of $\pi$ - Cipher

- Ensuring both privacy and authenticity for encrypted messages at the same time
  - Data privacy (IND-CPA)
  - Ciphertext integrity against forgery (INT-CTXT)

- $\pi$ - Cipher security proof is based on the proof for the sponge based authenticated ciphers given by P. Jovanovic, A. Luykx, B. Mennink in the ASIACRYPT 2014 paper "*Beyond $2^{c/2}$ security in sponge based authenticated encryption modes*"

# IND-CPA



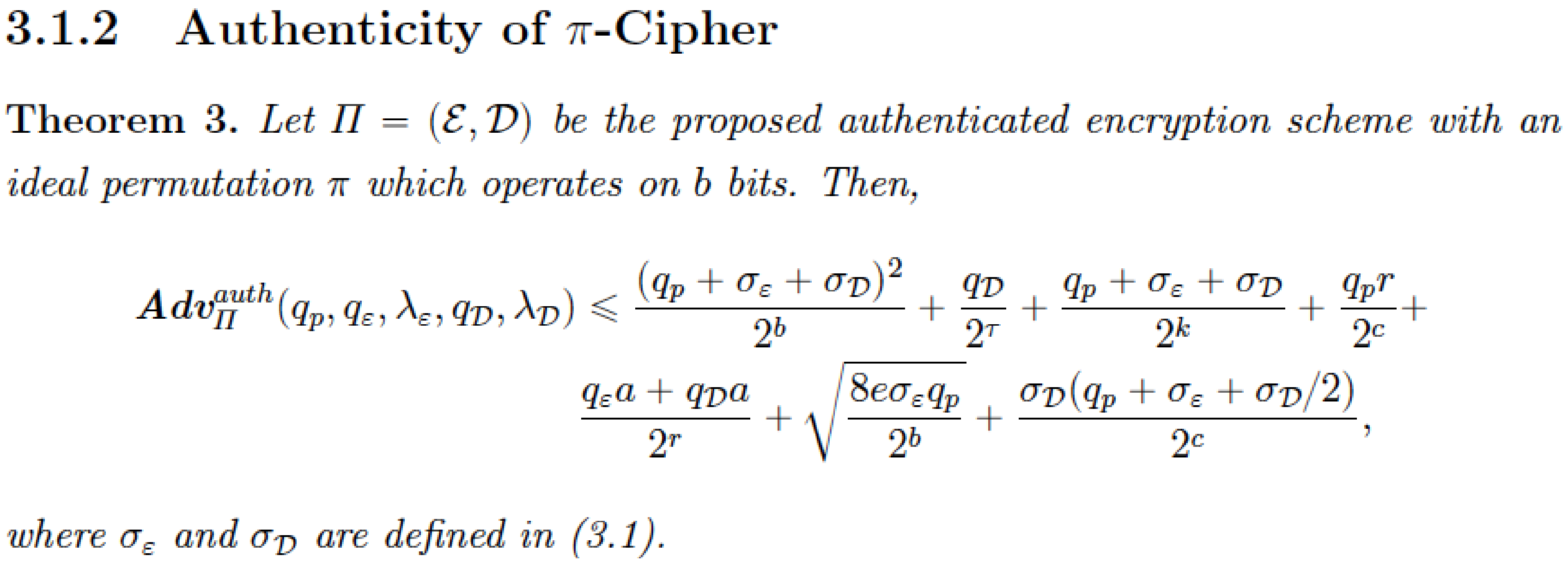
### 3.1.1 Privacy of $\pi$-Cipher

**Theorem 2.** *Let $\Pi = (\mathcal{E}, \mathcal{D})$ be the proposed authenticated encryption scheme with an ideal permutation $\pi$ which operates on $b$ bits. Then,*

$$\boldsymbol{Adv}_{\Pi}^{priv}(q_p, q_\varepsilon, \lambda_\varepsilon) \leqslant \frac{(q_p + \sigma_\varepsilon + \sigma_\mathcal{D})^2}{2^b} + \frac{q_\mathcal{D}}{2^\tau} + \frac{q_p + \sigma_\varepsilon + \sigma_\mathcal{D}}{2^k} + \frac{q_p r}{2^c} + \frac{q_\varepsilon a + q_\mathcal{D} a}{2^r} + \sqrt{\frac{8e\sigma_\varepsilon q_p}{2^b}} + \frac{\sigma_\mathcal{D}(q_p + \sigma_\varepsilon + \sigma_\mathcal{D}/2)}{2^c},$$

*where $\sigma_\varepsilon$ is defined in (3.1).*

# INT-CTXT



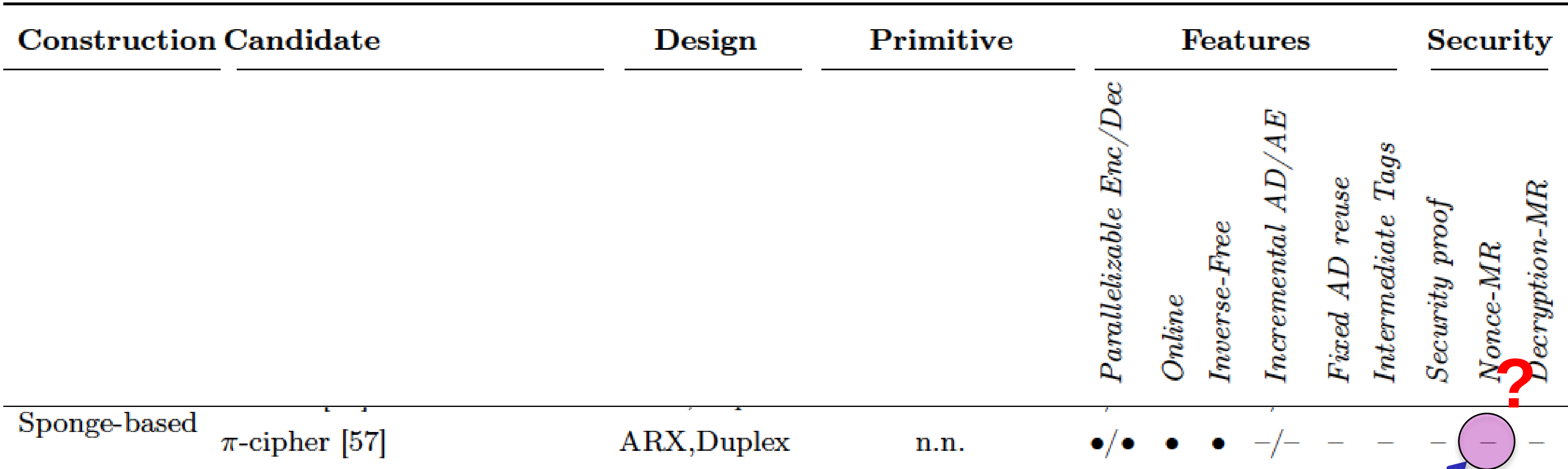
### 3.1.2 Authenticity of $\pi$-Cipher

**Theorem 3.** *Let $\Pi = (\mathcal{E}, \mathcal{D})$ be the proposed authenticated encryption scheme with an ideal permutation $\pi$ which operates on $b$ bits. Then,*

$$\boldsymbol{Adv}_{\Pi}^{auth}(q_p, q_\varepsilon, \lambda_\varepsilon, q_\mathcal{D}, \lambda_\mathcal{D}) \leqslant \frac{(q_p + \sigma_\varepsilon + \sigma_\mathcal{D})^2}{2^b} + \frac{q_\mathcal{D}}{2^\tau} + \frac{q_p + \sigma_\varepsilon + \sigma_\mathcal{D}}{2^k} + \frac{q_p r}{2^c} + \frac{q_\varepsilon a + q_\mathcal{D} a}{2^r} + \sqrt{\frac{8e\sigma_\varepsilon q_p}{2^b}} + \frac{\sigma_\mathcal{D}(q_p + \sigma_\varepsilon + \sigma_\mathcal{D}/2)}{2^c},$$

*where $\sigma_\varepsilon$ and $\sigma_\mathcal{D}$ are defined in (3.1).*

# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

?

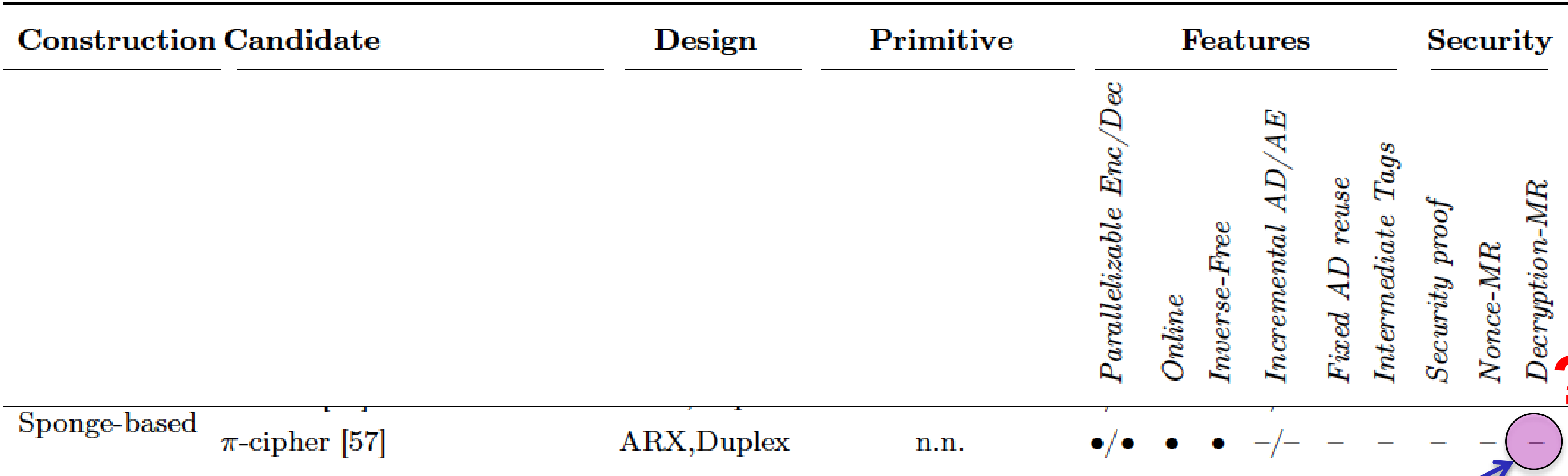
Yes for authenticity,
Yes (conditional) for privacy
(when SMN is not repeated)

# Nonce Misuse Resistance

- Nonce = PMN (27 candidates)
- Nonce = (PMN, SMN) (2 candidates: $\pi$ -Cipher and ICEPOLE-128)

- An intermediate level of nonce-misuse resistance is manifested when legitimate key holder reuses K, PMN and AD, but SMN is different

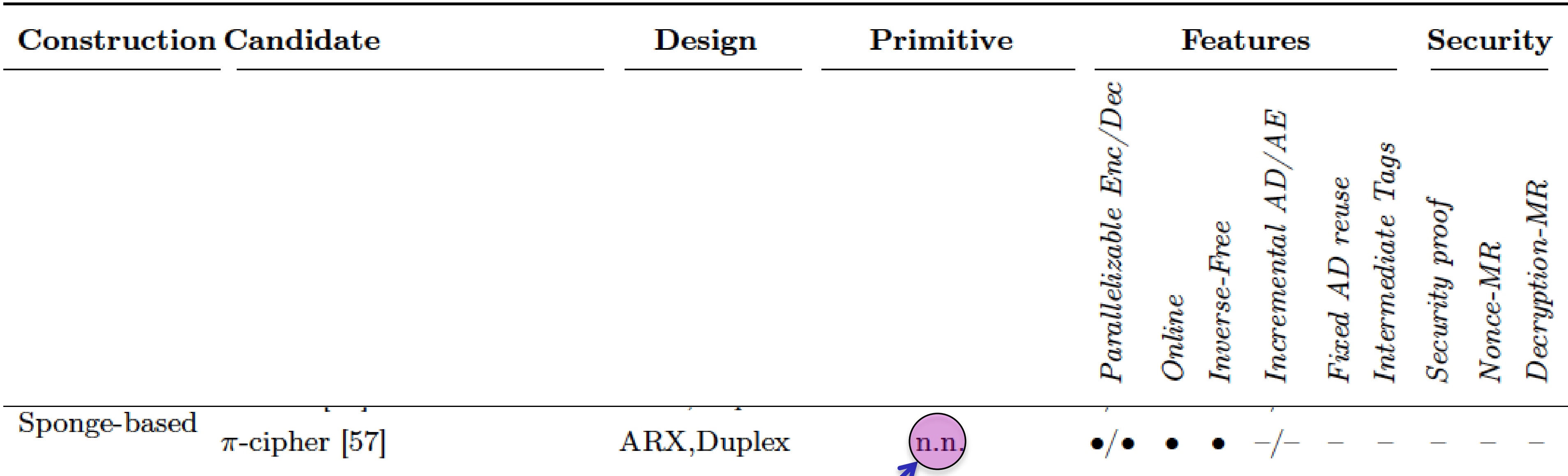
# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features |  |  |  |  |  | Security |  |  |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

Yes, it is automatically achieved if it is implemented with intermediate tags, but still we need security proof (work in progress)

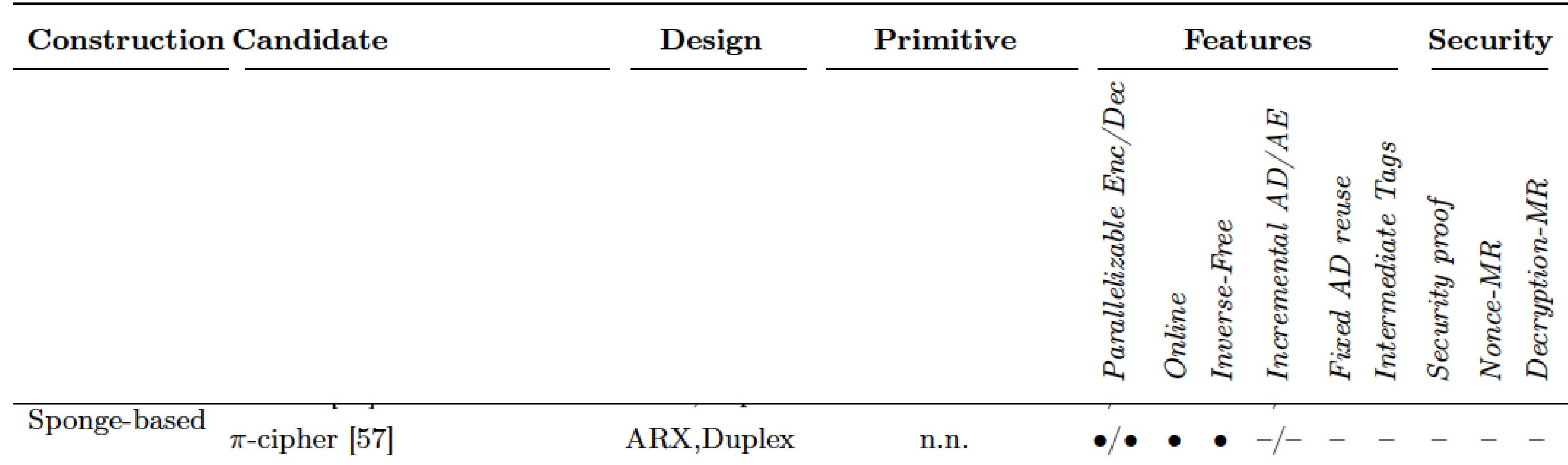
# How $\pi$ - Cipher is perceived and what are its actual properties



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

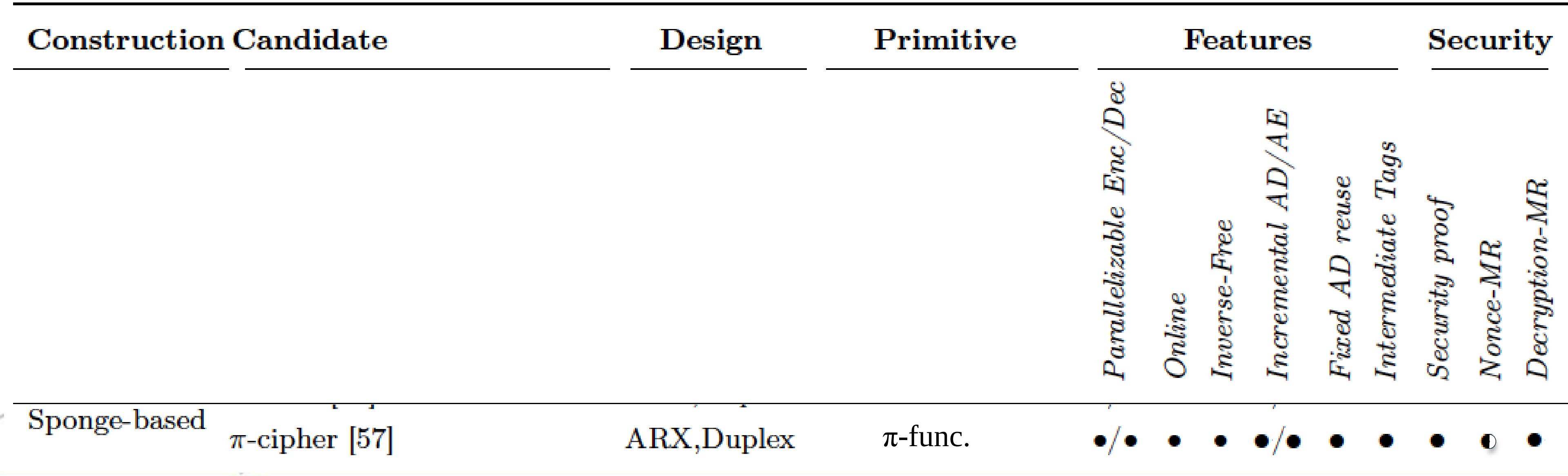
**Hint: Permutation function is called π-function**

| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

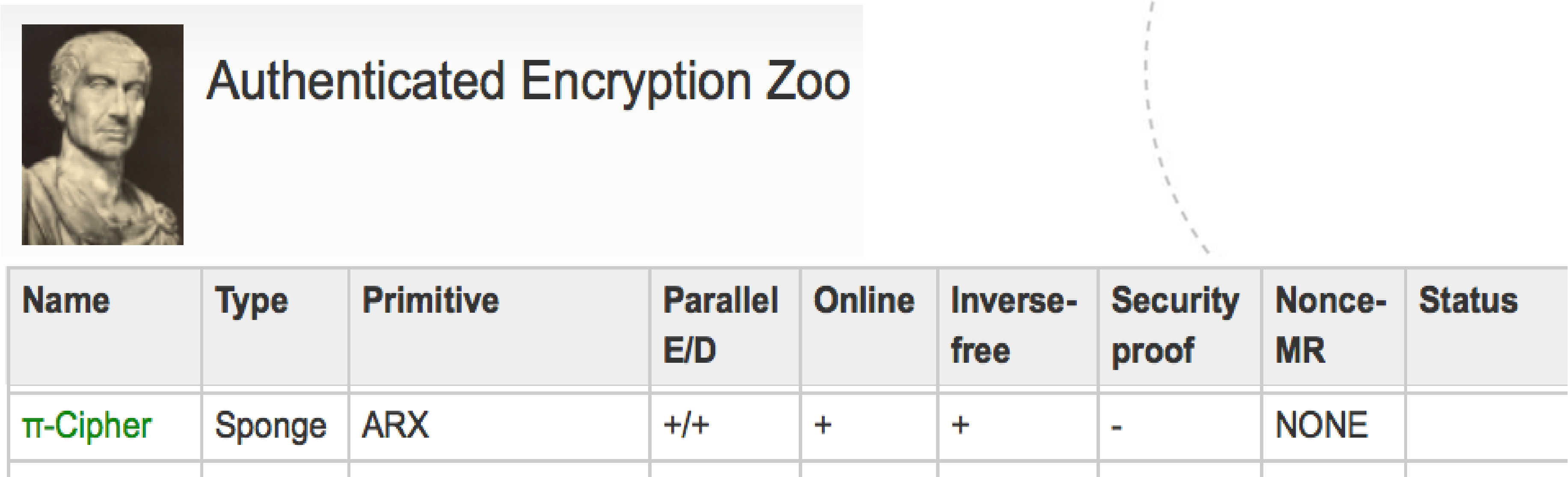


| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | –/– | – | – | – | – | – |

Replace with

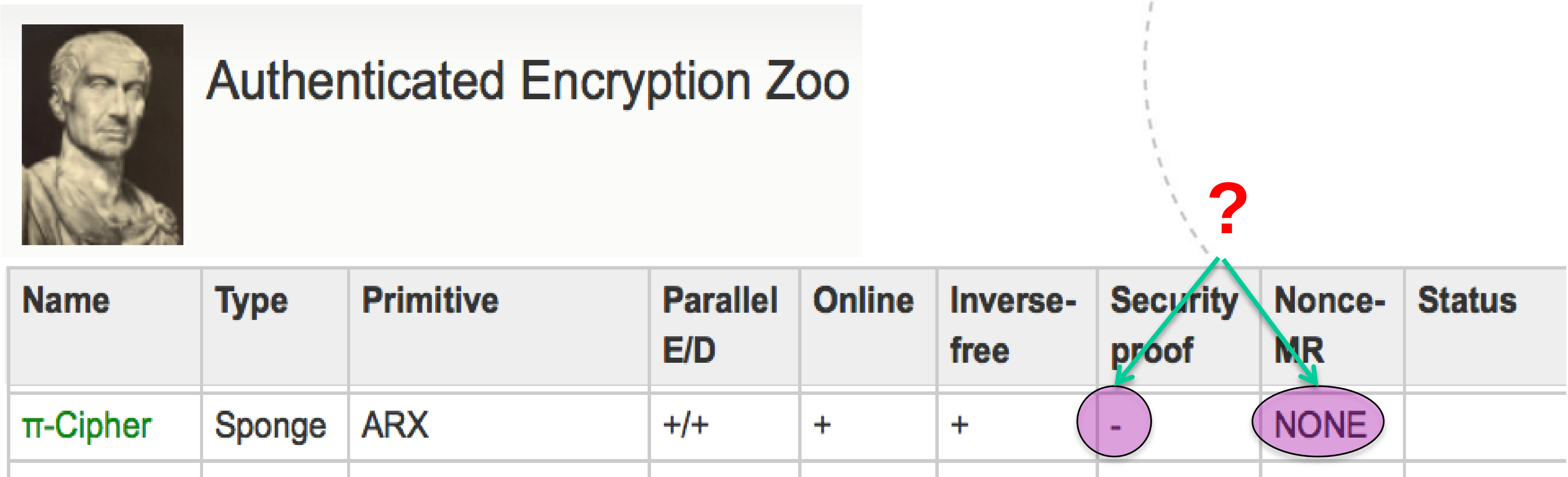


| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | π-func. | ●/● | ● | ● | ●/● | ● | ● | ● | ◐ | ● |



Authenticated Encryption Zoo

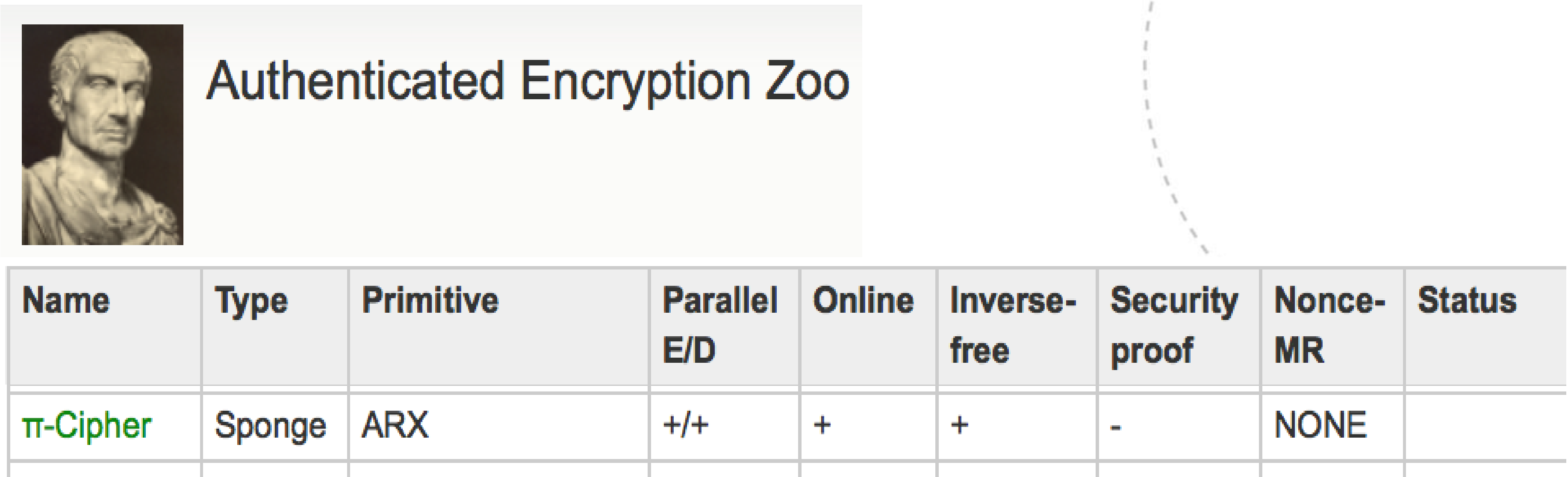
| Name | Type | Primitive | Parallel E/D | Online | Inverse-free | Security proof | Nonce-MR | Status |
|---|---|---|---|---|---|---|---|---|
| π-Cipher | Sponge | ARX | +/+ | + | + | - | NONE | |



# Authenticated Encryption Zoo

?

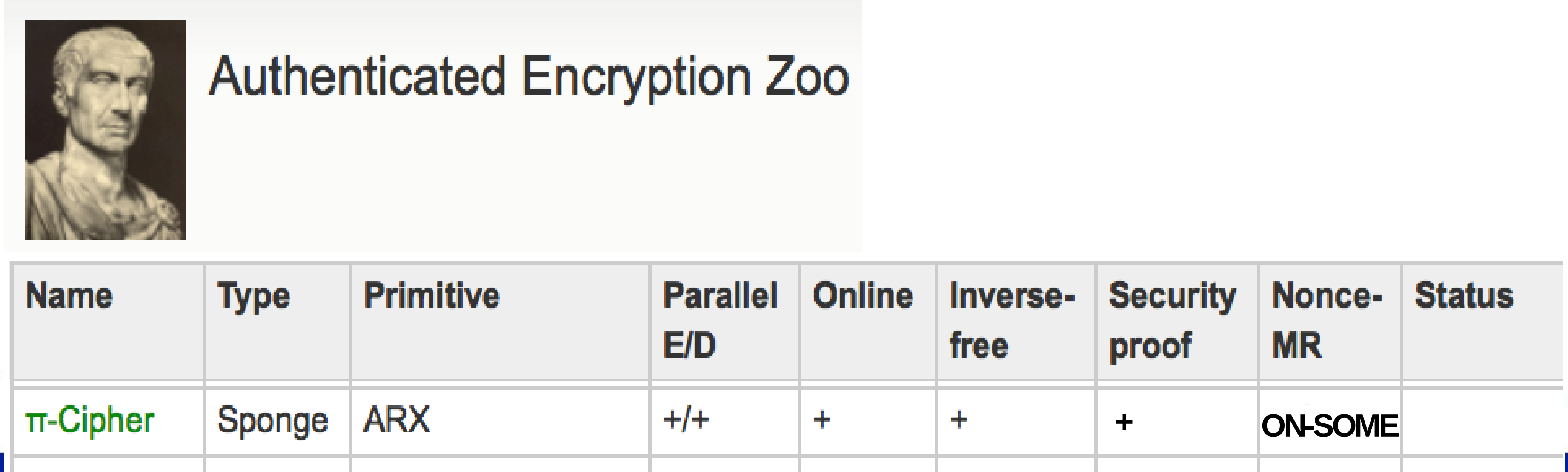
| Name | Type | Primitive | Parallel E/D | Online | Inverse-free | Security proof | Nonce-MR | Status |
|---|---|---|---|---|---|---|---|---|
| π-Cipher | Sponge | ARX | +/+ | + | + | - | NONE | |



## Authenticated Encryption Zoo

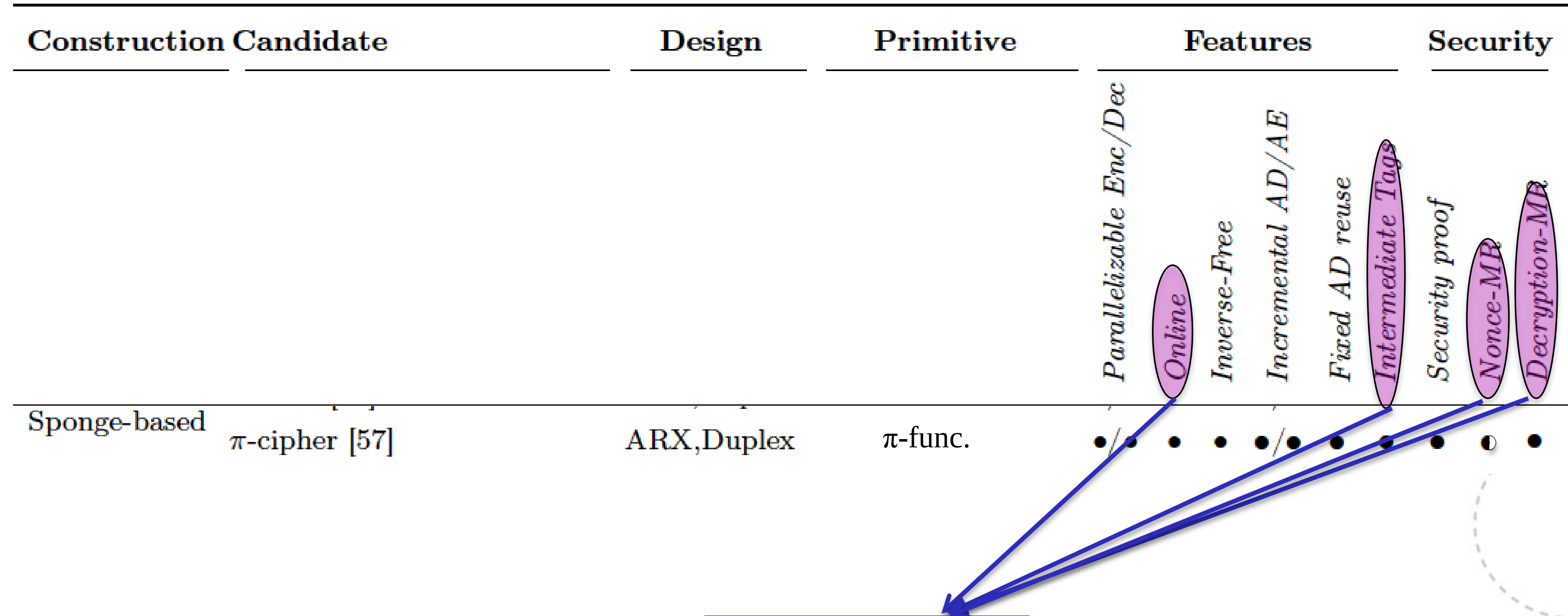
| Name | Type | Primitive | Parallel E/D | Online | Inverse-free | Security proof | Nonce-MR | Status |
|---|---|---|---|---|---|---|---|---|
| π-Cipher | Sponge | ARX | +/+ | + | + | - | NONE | |

**Replace with**



## Authenticated Encryption Zoo

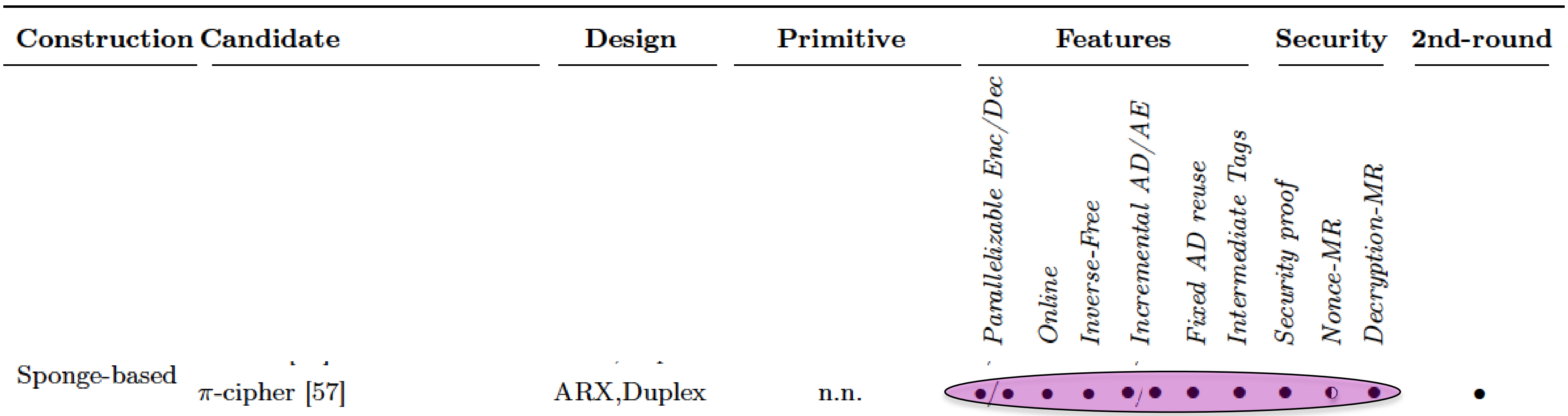
| Name | Type | Primitive | Parallel E/D | Online | Inverse-free | Security proof | Nonce-MR | Status |
|---|---|---|---|---|---|---|---|---|
| π-Cipher | Sponge | ARX | +/+ | + | + | + | ON-SOME | |



| Construction | Candidate | Design | Primitive | Features | | | | | | Security | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* |
| Sponge-based | π-cipher [57] | ARX,Duplex | π-func. | ●/● | ● | ● | ●/● | ● | ● | ● | ◐ | ● |

OAE2 Scheme

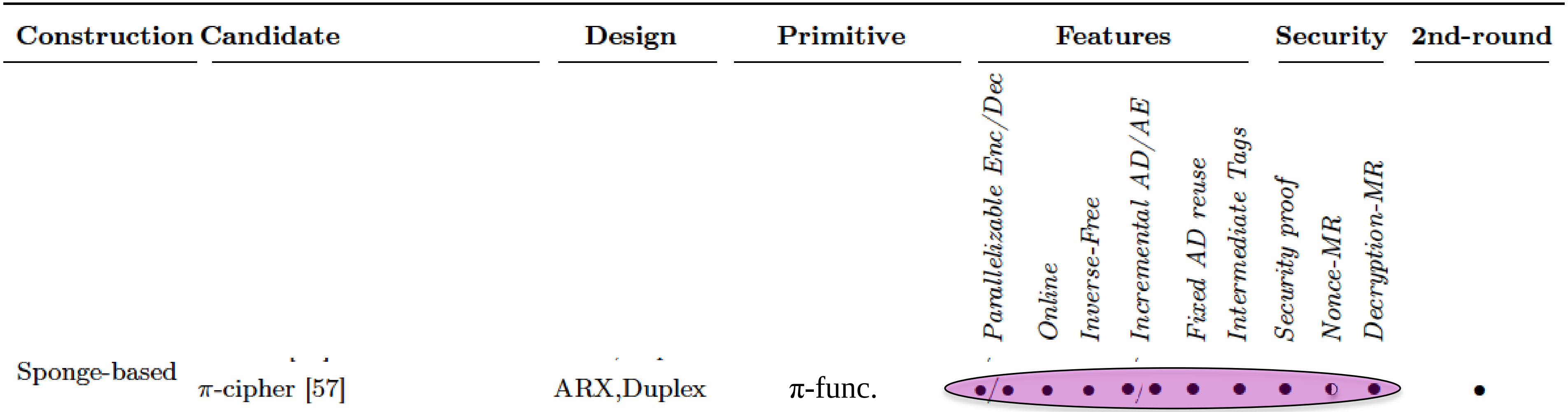
V. T. Hoang, R. Reyhanitabar, P. Rogaway, and D. Vizr. "*Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance*", CRYPTO 2015. There, thay say: "Sponge duplex construction of Bertoni et al., resembles OAE2."



| Construction | Candidate | Design | Primitive | Features | | | | | | | Security | | 2nd-round |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* | |
| Sponge-based | $\pi$-cipher [57] | ARX,Duplex | n.n. | ●/● | ● | ● | ●/● | ● | ● | ● | ◐ | ● | ● |

$\pi$ - Cipher is based on sponge duplex construction of Bertoni et al., with additional cryptographic mechanisms that strengthen its robustness such as the features:

- tag second preimage resistance
- wide block tweakability
- incrementability
- use of SMN that guarantees confidentiality and integrity even when the K, AD and PMN are reused



| Construction | Candidate | Design | Primitive | Features | | | | | | | | | 2nd-round |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | *Parallelizable Enc/Dec* | *Online* | *Inverse-Free* | *Incremental AD/AE* | *Fixed AD reuse* | *Intermediate Tags* | *Security proof* | *Nonce-MR* | *Decryption-MR* | |
| Sponge-based | π-cipher [57] | ARX,Duplex | π-func. | ●/● | ● | ● | ●/● | ● | ● | ● | ◐ | ● | ● |

(The "Security" header is printed above the last three feature columns: Security proof, Nonce-MR, Decryption-MR.)

*π* - Cipher is based on sponge duplex construction of Bertoni et al., with additional cryptographic mechanisms that strengthen its robustness su

- tag second
- wide block
- incrementa
- use of SMN that guarantees confidentiality and integrity even when the K, AD and PMN are reused

*π* - Cipher is STREAM OAE2+ cipher

# Efficiency

- Software speed of non SSE implementation of π64-Cipher in v1.0 was around 11 cpb on Sandy Bridge. We expect v2.0 to be faster.

- Still we want to emphasize the incrementality feature of π-cipher by which it can outperform the speed of any non-incremental cipher even with 0.01 cpb

# Efficiency

- Recent lightweight hardware implementation of π16-Cipher on Xilinx Virtex-7 platform XC7VX485T-2FFG1761 is:
  - 266 slices for the pi-function
  - 1114 slices for encryption engine without AD and SMN

  running at 347MHz
- Another lightweight implementation of π16-Cipher for AVR 8-bit MCU
  - 1.9 KB code size for encryption-authentication/decryption-verification part

# Acknowledgements

- Gäetan Leurent and Thomas Fuhr
  - thanks for your detaild observation on the π-Cipher and pointing out the problem with padding

- Bart Mennink
  - thanks for your valuable and excellent advices in the process of proving the security of π-Cipher

# Thank you for listening!

?