Forgery attacks on TinyJAMBU-256 and TinyJAMBU-192

Orr Dunkelman[1] Shibam Ghosh[1] **Eran Lambooij**[2]

[1]University of Haifa, [2]Bar-Ilan University

FSE 2024, Leuven

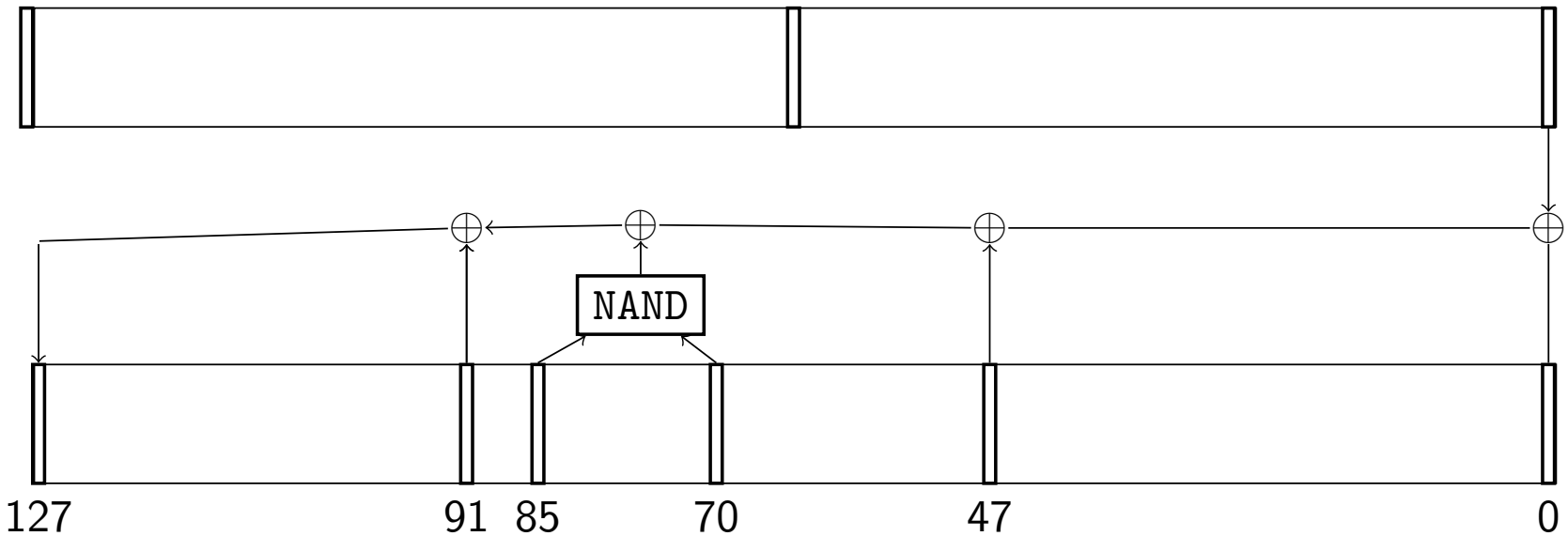
TinyJAMBU

- TinyJAMBU [WH19, WH21] was one of the finalists of the NIST Lightweight Competition.
- TinyJAMBU is a Duplex like construction with a 128-bit state and 32-bit rate
- The permutation is based on a keyed NLFSR
- Supports 128, 192, and 256-bit keys
- 64-bit authentication security in nonce respecting setting
- At most 2^{50} bytes of message (2^{48} encryptions)

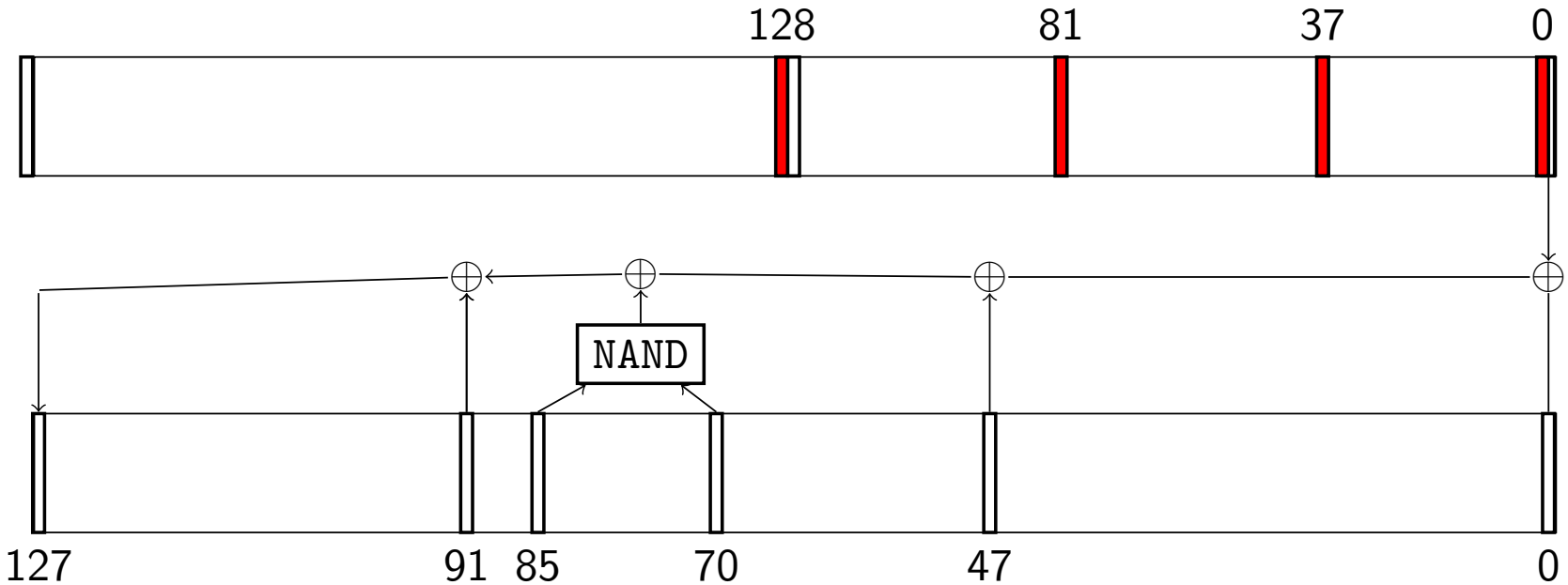
Results

- Related-key differential from initialisation to the first output with probability:
  - 2^{-32} for TinyJAMBU-256
  - 2^{-40} for TinyJAMBU-192
- Practical forgery with data complexity in RK setting:
  - $2^{32} + 2^{24}$ data using 2^{10} related key pairs for TinyJAMBU-256
  - $2^{40} + 2^{30}$ data using 2^{12} related key pairs for TinyJAMBU-192
- This result shows that TinyJAMBU is not key-committing

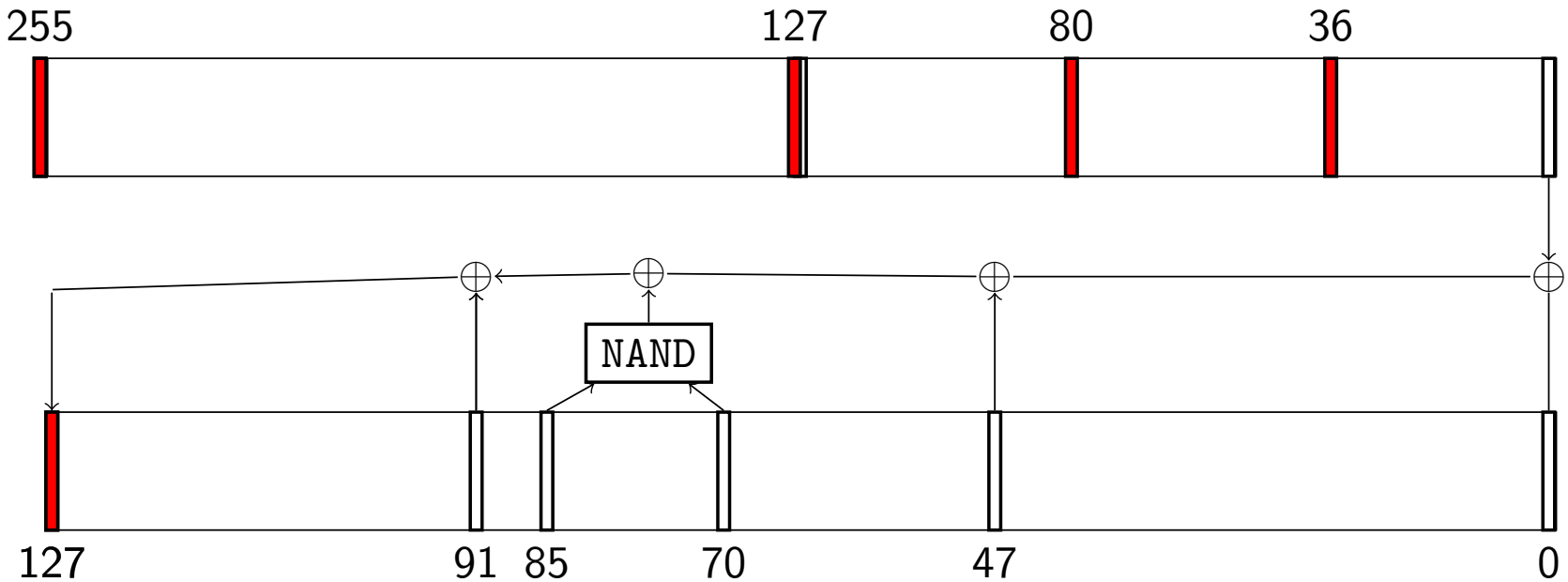
TinyJAMBU-256 Keyed Permutation



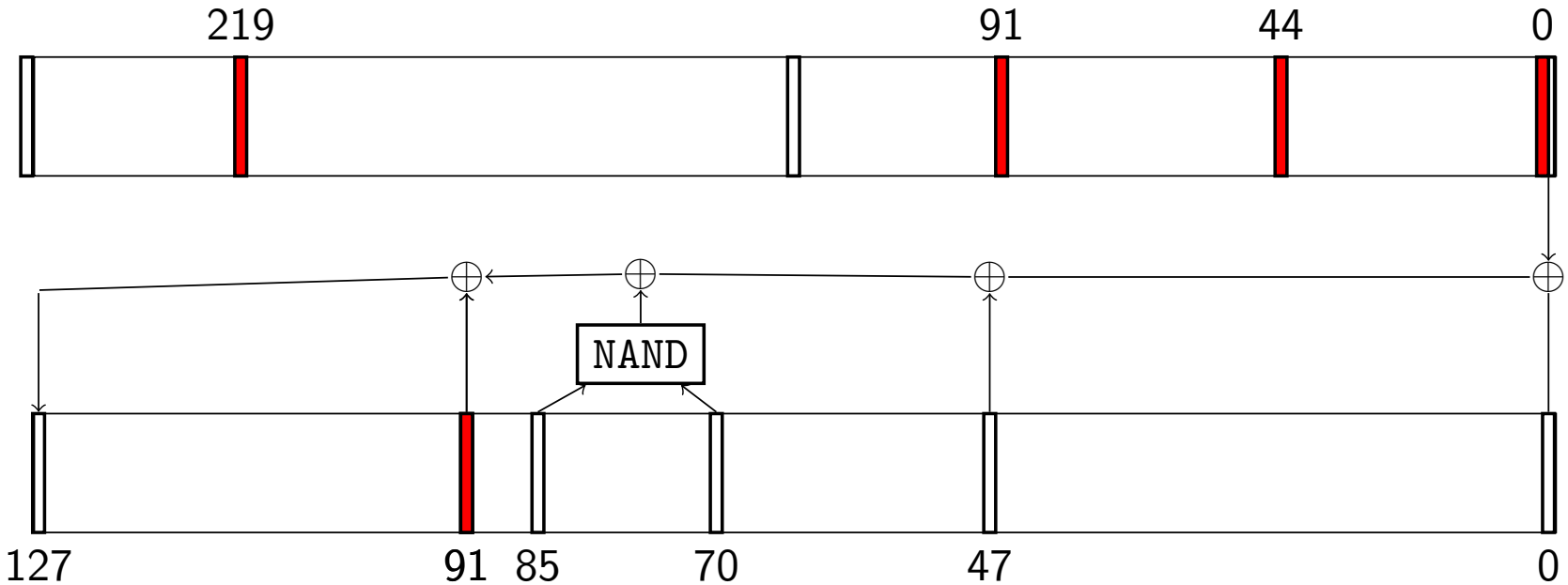
Related Key Differential ($r = 0$)



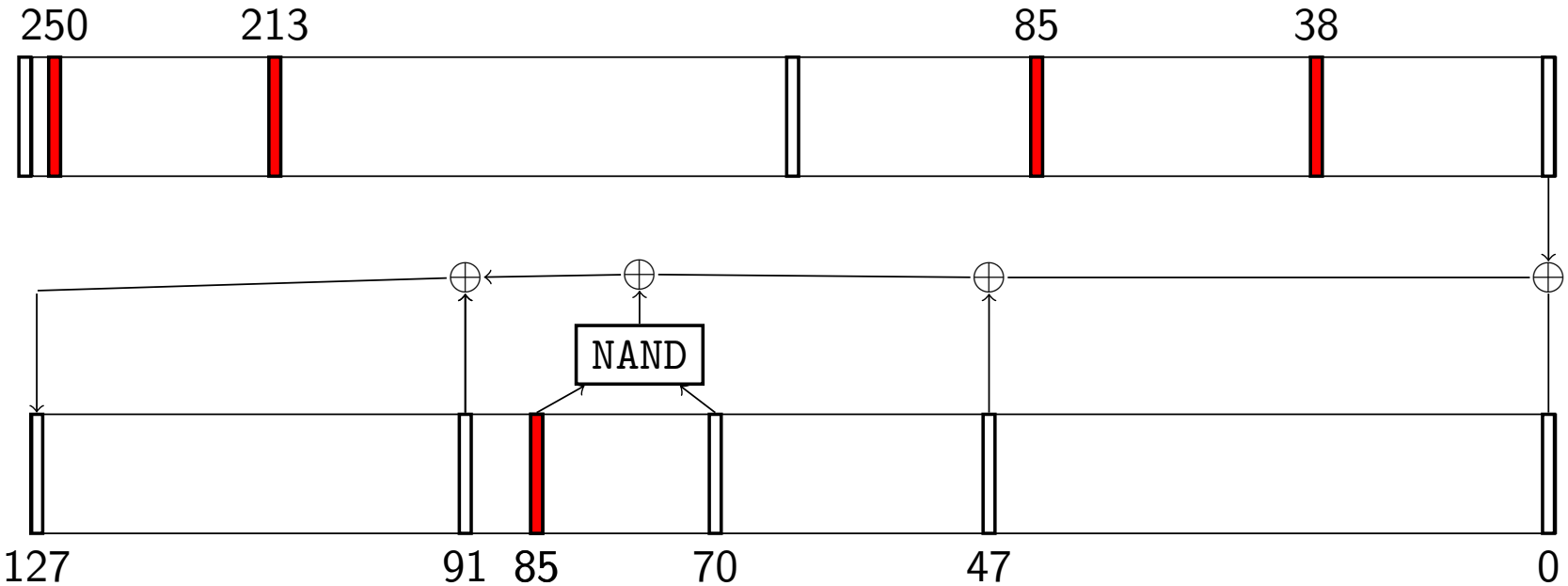
Related Key Differential ($r = 1$)



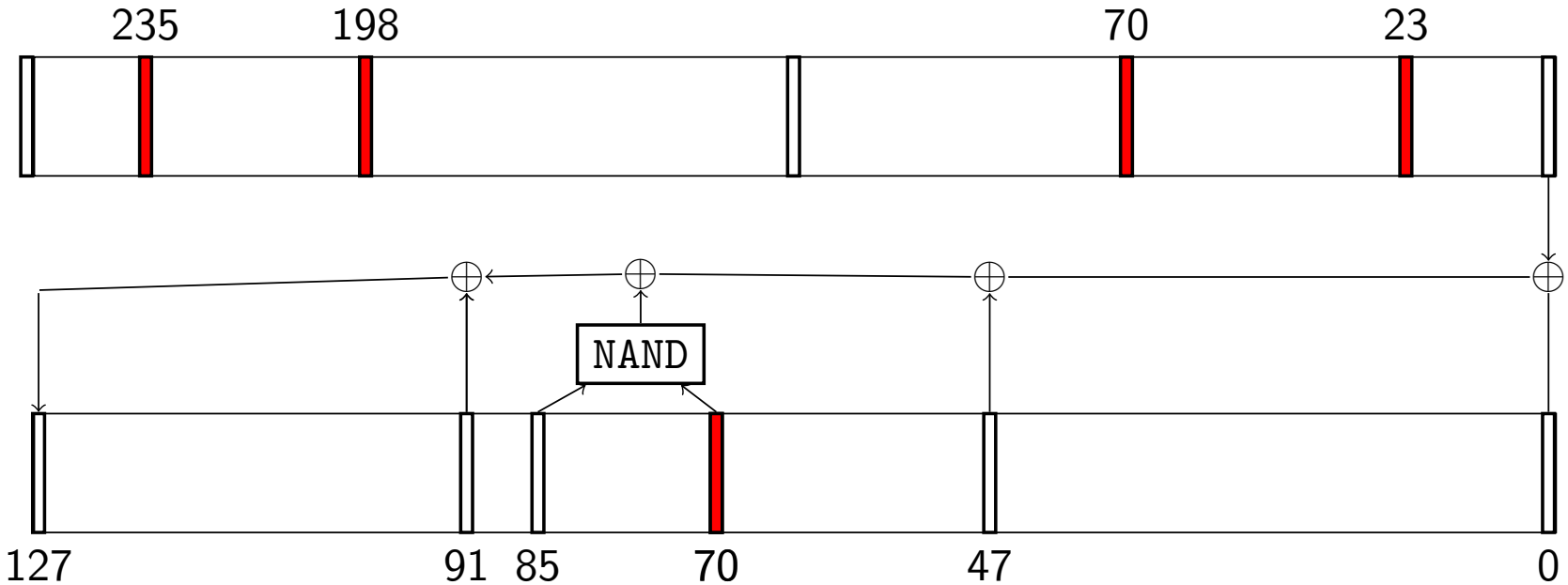
Related Key Differential ($r = 37$)



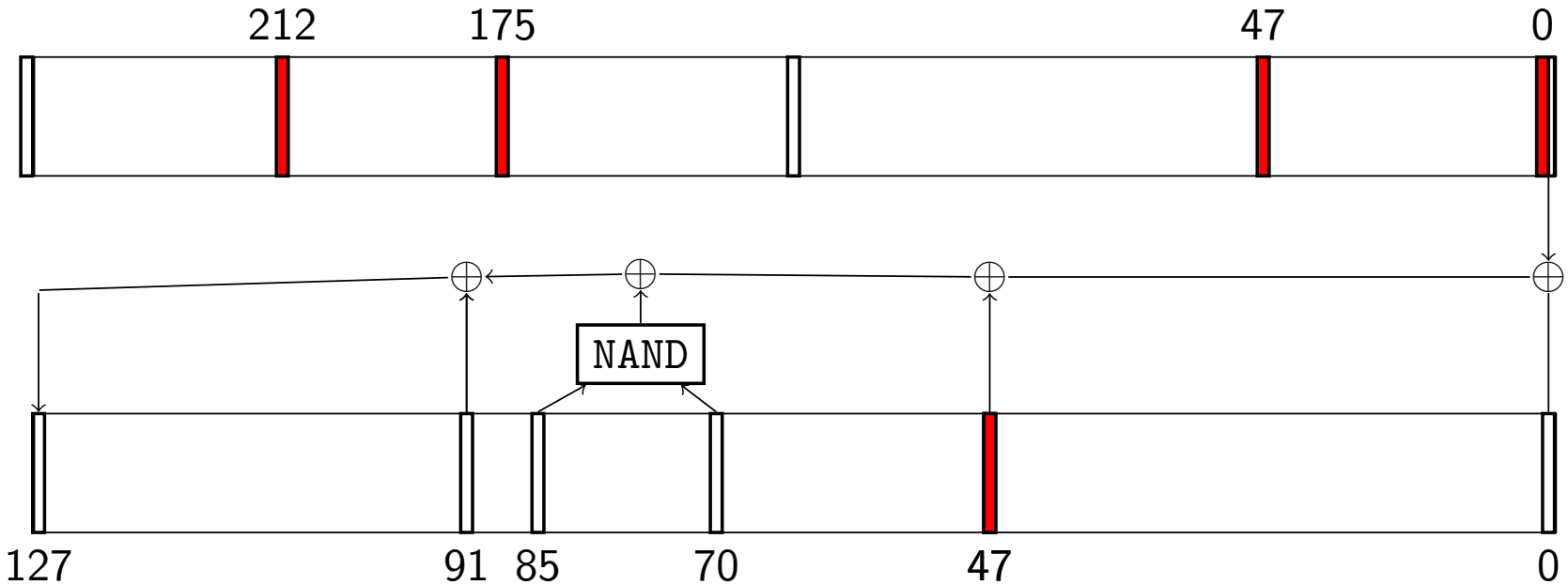
Related Key Differential ($r = 43$)



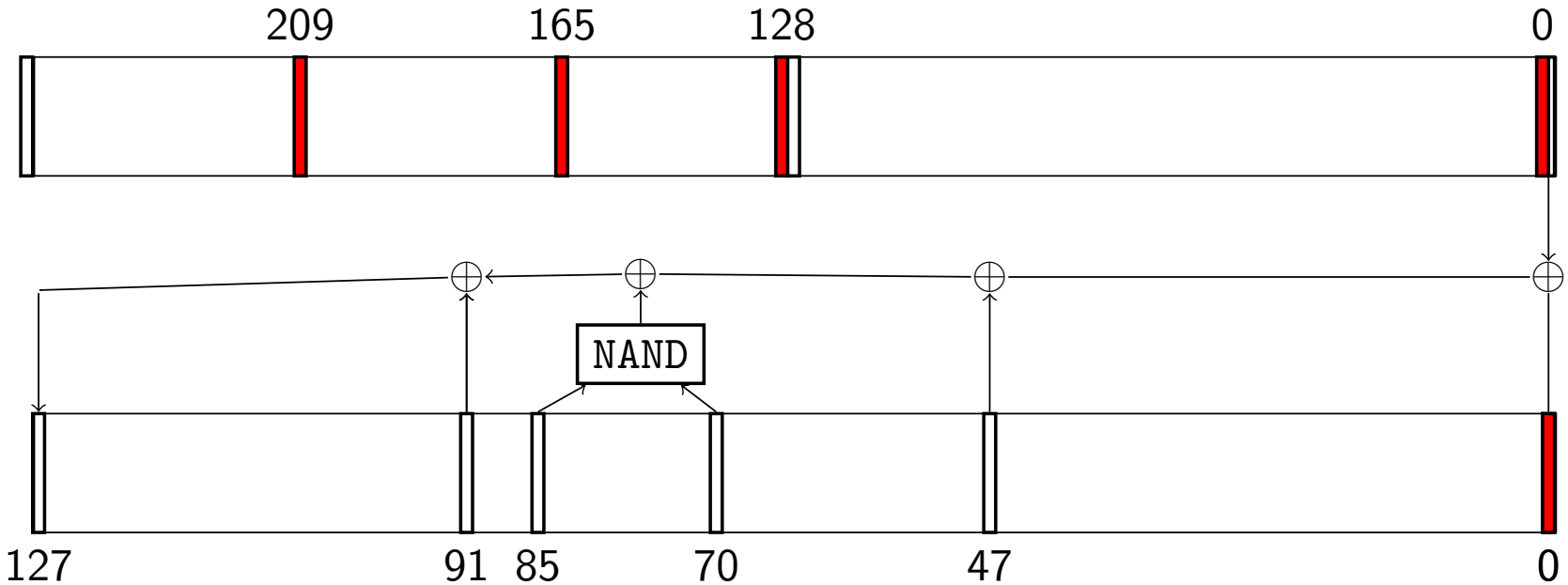
Related Key Differential ($r = 58$)



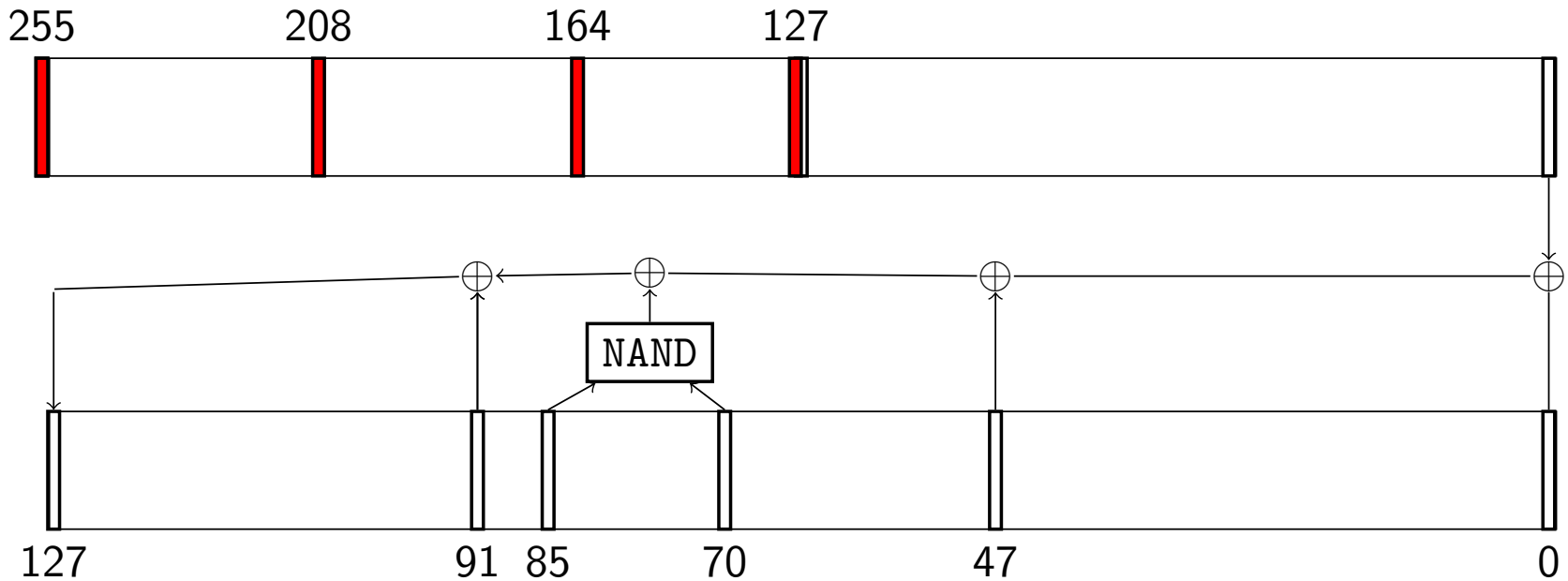
Related Key Differential ($r = 81$)



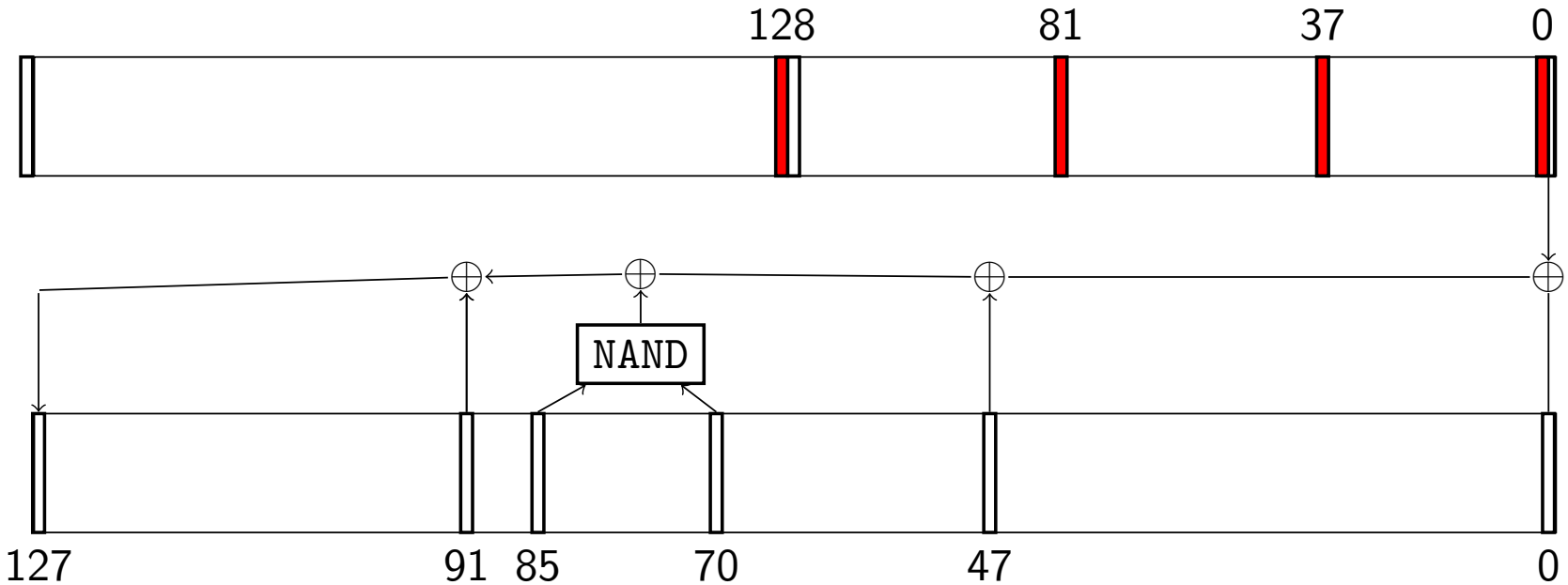
Related Key Differential ($r = 127$)



Related Key Differential ($r = 128$)



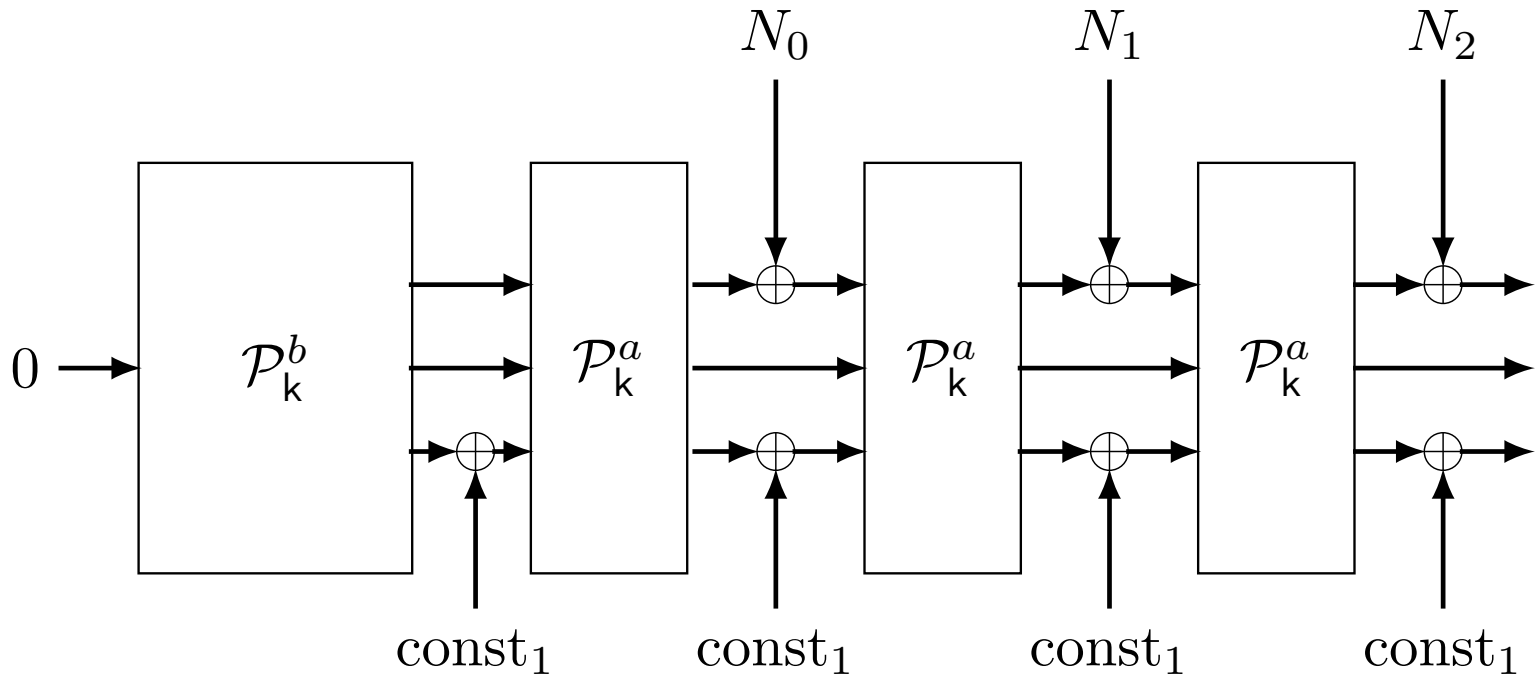
Related Key Differential ($r = 255$)



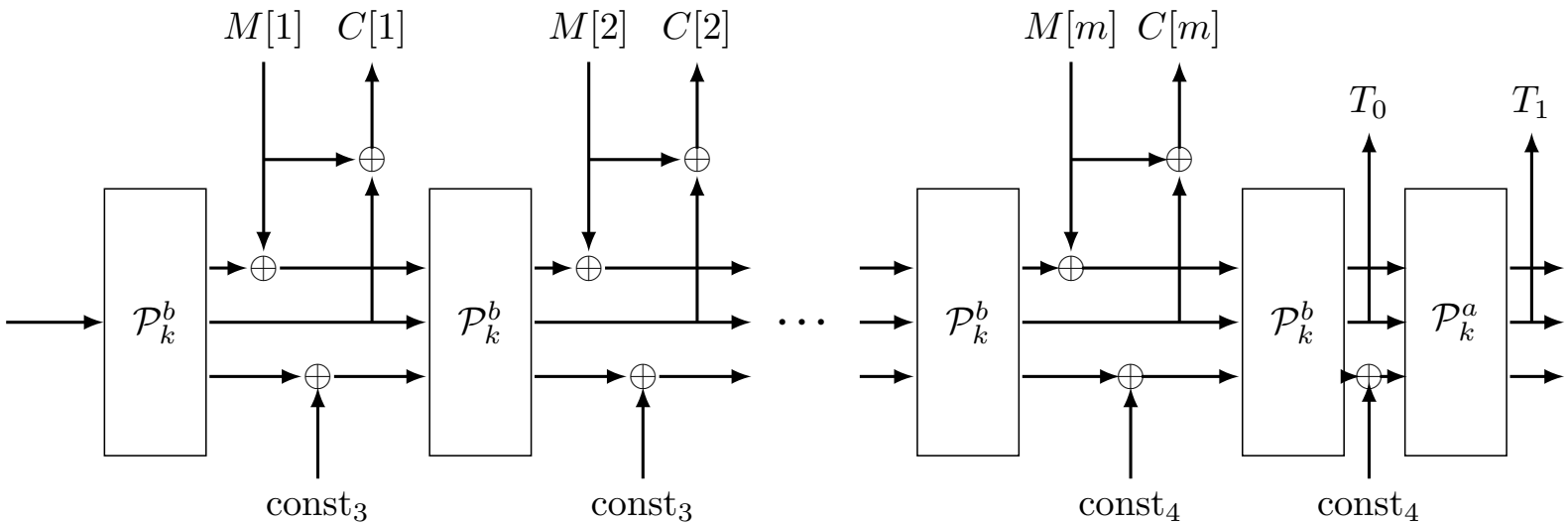
Related Key Differentials

Keysize	a	b	Prob. $\mathcal{P}^a$	Prob. $\mathcal{P}^b$
256	1280	640	2^{-10}	2^{-4}
192	1152	640	2^{-12}	2^{-6}

TinyJAMBU Mode of Operation: Initialization



TinyJAMBU Mode of Operation: Message + Tag



Forgery

1. Find K, K' and N, N' s.t. we have a 0 difference after the initialisation
   - Uses $2^{10+4+4+4+10} = 2^{32}$ data.
2. Change N, N', and M, M', s.t. there is no difference in the tag
   - Uses 2^{10+4} data in the **nonce misuse** setting.
   - Uses $2^{10+10+4}$ data in the **nonce respecting** setting.

A technicality

- The first time we can change the state is after one $\mathcal{P}^a$ and one $\mathcal{P}^b$.
- Probability 2^{-14} for the characteristic to hold for each key pair.
- We need at least 2^{14} related key pairs.
- Since each key has 32 keys it can be a related key pair with, we need a set of 2^{10} related keys.

Practical Results

Key size	Key	Nonce	Message	Ciphertext	Tag
192	9AE19248 8B102E07 AB0F2C02 9EDB377D 090EF19C 66F4AAEB	19A2492E DF81AB70 923635DC	11129DA1	C9211BA2	1734A489 1229B9F6
	9AE19248 8B102E87 AB0F2C02 8EDB377D 090EF09C 66F4AA6B	19A249AE DF81ABF0 9236355C	11129DA1	C9211BA2	1734A489 1229B9F6
256	B429DBD1 14F8B269 7D83ABD0 3893F974 79626DF1 B3A3D867 A415E2BB D5A2A68A	BF8A51BD B71DC3C6 8443C018	29594AD7	E015A04A	1E8CA308 95CBD1F7
	B429DBD1 14F8B269 7D83ABD0 3893F9F4 79626DF1 A3A3D867 A415E3BB D5A2A60A	BF8A513D B71DC346 8443C098	29594AD7	E015A04A	1E8CA308 95CBD1F7

Thank you for your attention!

Questions?

eprint 2022/1122

References


Hongjun Wu and Tao Huang, *TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms: Submission to NIST LwC*, 2019, https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf.


———, *TinyJAMBU : A family of lightweight authenticated encryption algorithms (version 2)*, 2021, https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/tinyjambu-spec-final.pdf.