PRIMATEs

Elena Andreeva
Atul Luykx
Nicky Mouha
Begül Bilgin
Florian Mendel
Qingju Wang
Andrey Bogdanov
Bart Mennink
Kan Yasuda

PRIMATEs

PRIMATEs

APE

misuse
resistance

PRIMATEs

APE

misuse
resistance

HANUMAN

security with
ideal
permutation

PRIMATEs

APE

misuse resistance

HANUMAN

security with ideal permutation

GIBBON

trade-off speed/security

PRIMATEs



- Sponge inspired (9)

PRIMATEs

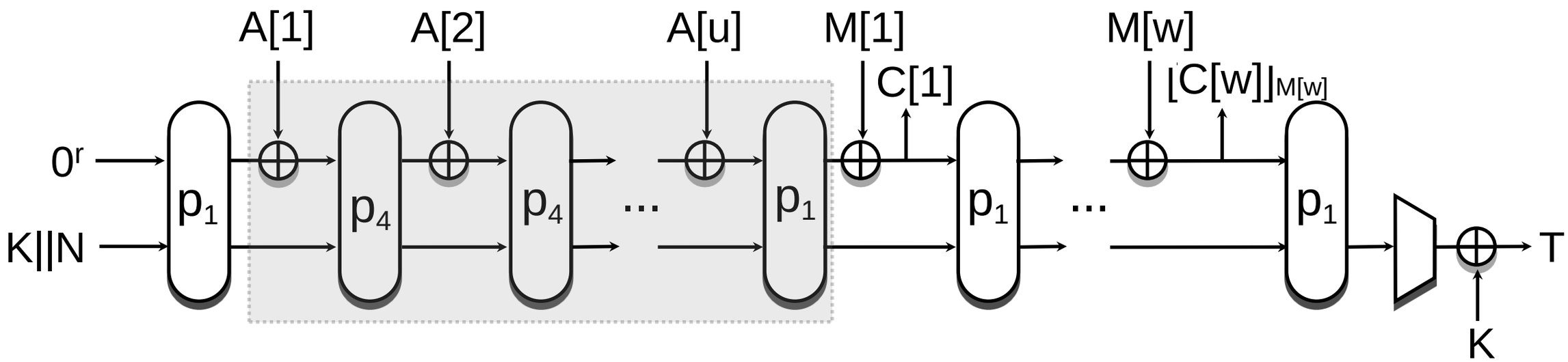


- Sponge inspired

permutation	PRIMATE–80	PRIMATE–120
security	80 bits	120 bits
b (state size)	200 bits	280 bits
c (capacity size)	160 bits	240 bits
r (rate size)	40 bits	40 bits

- Lightweight
- Substitution-Permutation-Network (SPN)
- Efficient threshold implementation
- Ideal permutation proof

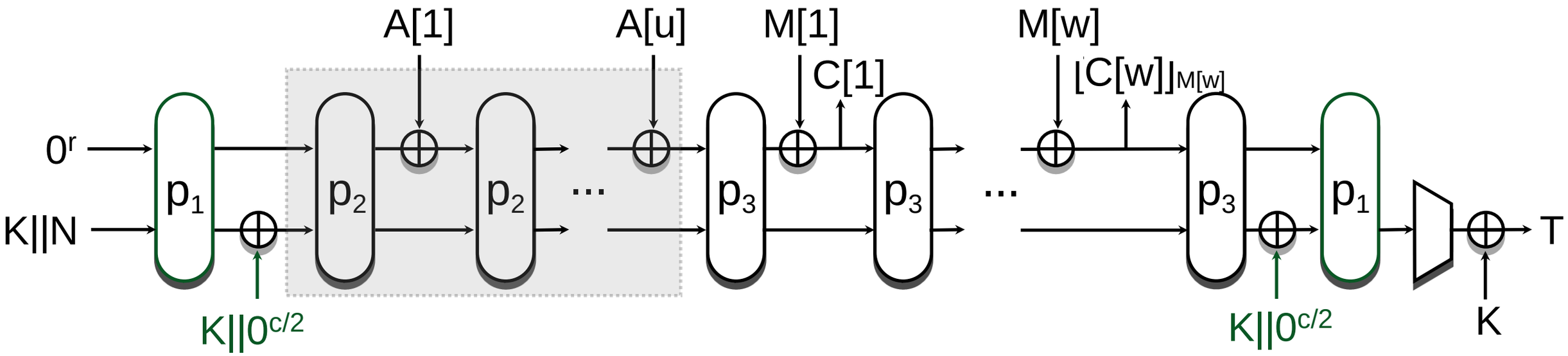
HANUMAN



K, N and T are 80 (resp. 120) bits

- Nonce-based
- Online encryption
- Domain separation: p_1, p_4
- No ciphertext expansion

GIBBON

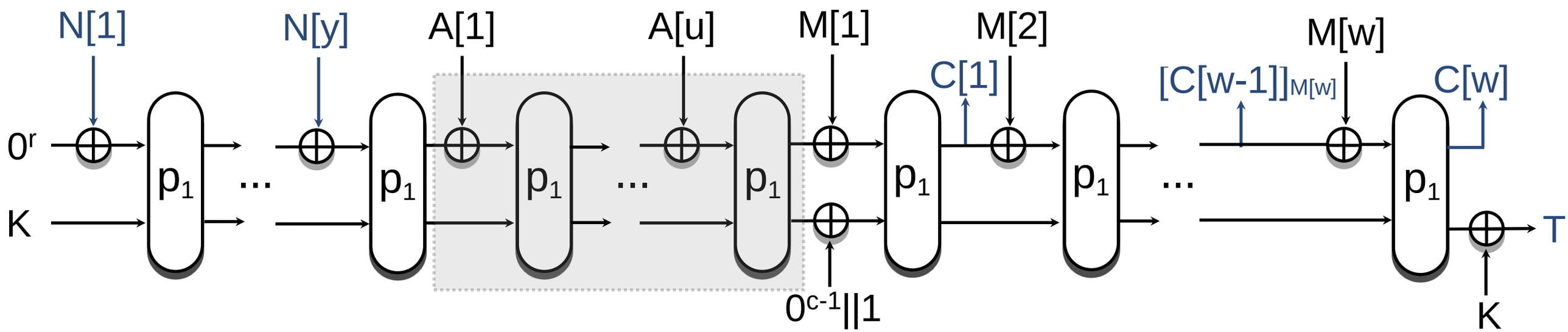


K, N and T are 80 (resp. 120) bits

Differences with HANUMAN:

- Key addition: state recovery → no key recovery
- Three permutations: p_1, p_2, p_3
- Reduced round permutations (p_2&p_3: 6 rounds) → faster

APE



N is 80 (resp. 120) bits
K and T are 160 (resp. 240) bits

Differences with HANUMAN:

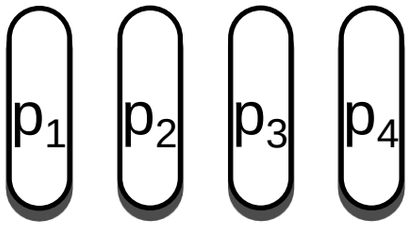
- Nonce misuse resistant (common prefix)
- Secure in Releasing Unverified Plaintext (RUP) setting
- Inverse permutation needed

Also using APE: PRØST

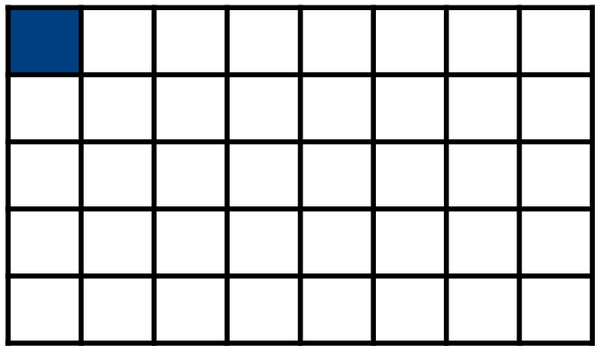
PRIMATEs Permutation

PRIMATEs

Structure



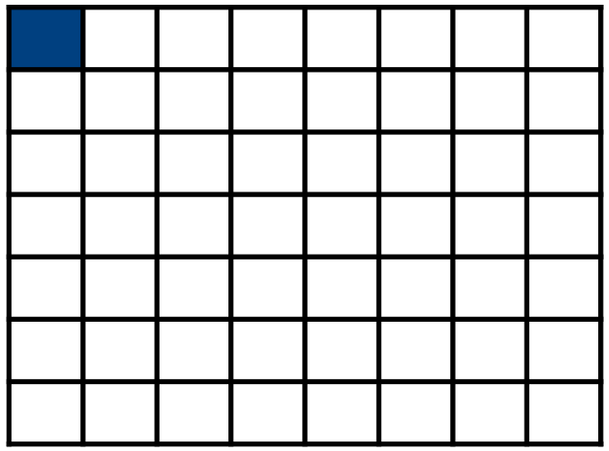
Primate–80



5x8

200-bit state

Primate–120

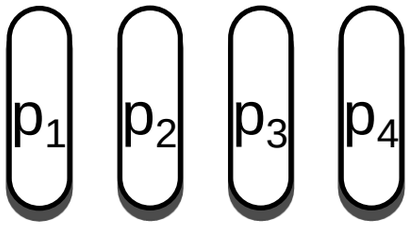


7x8

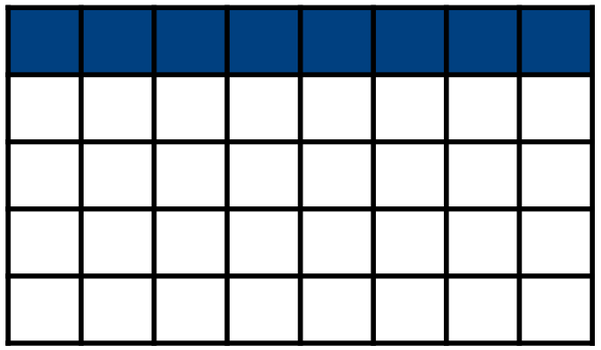
280-bit state

PRIMATEs

Structure



Primate–80



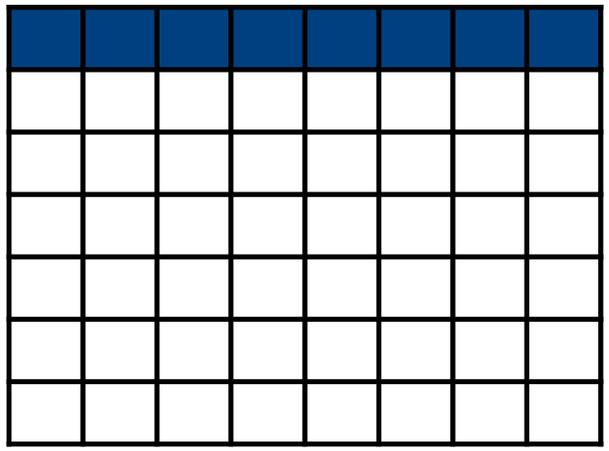
5x8

200-bit state

5-bit elements

40-bit rate

Primate–120



7x8

280-bit state

5-bit elements

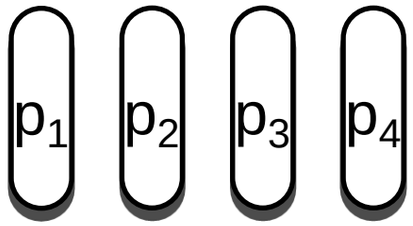
40-bit rate

Round Update: CA o MC o SR o SE

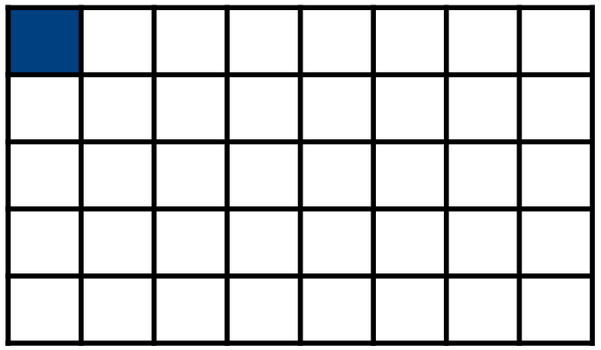
p_1, p_2, p_3 and p_4 differ in # of rounds and constants

PRIMATEs

SubElements (S-box)

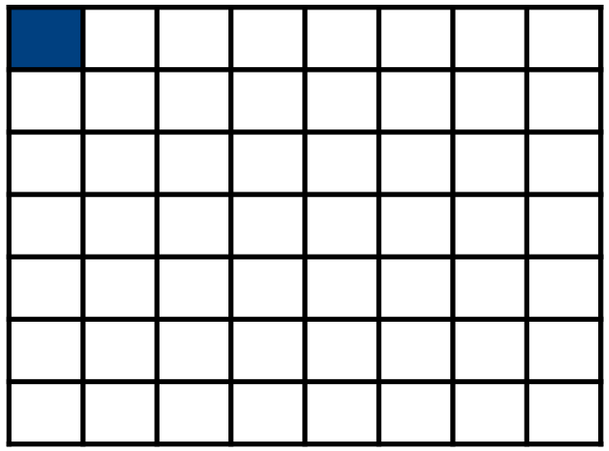


Primate–80



5x8

Primate–120

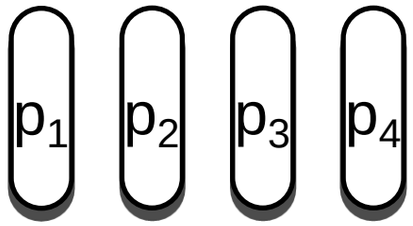


7x8

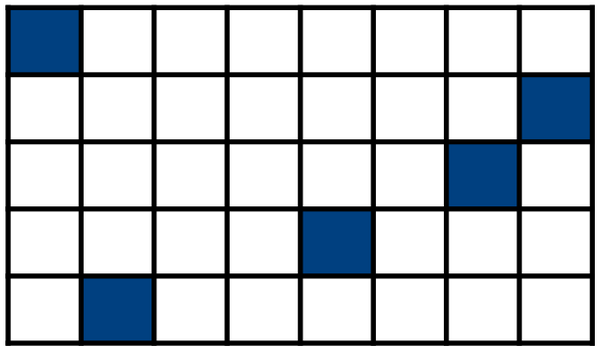
- Almost bent permutation
- Optimal linear/differential probabilities
- Small area for both plain and DPA-secure implementation

PRIMATEs

ShiftRows



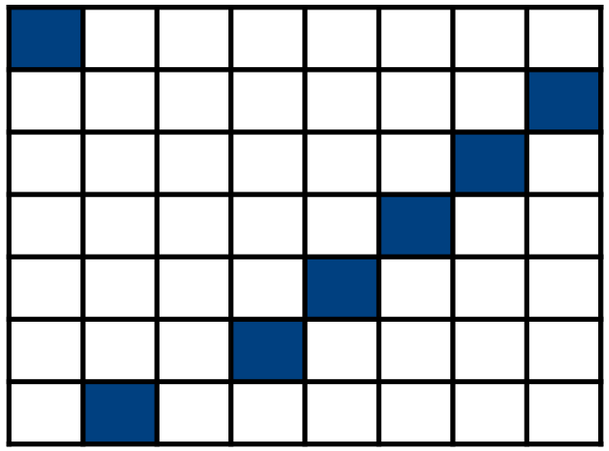
Primate–80



5x8

<< 0
<< 1
<< 2
<< 4
<< 7

Primate–120

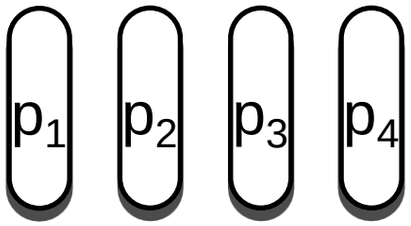


7x8

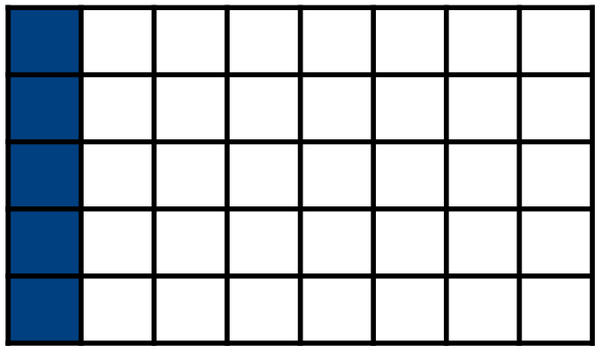
<< 0
<< 1
<< 2
<< 3
<< 4
<< 5
<< 7

PRIMATEs

MixColumns

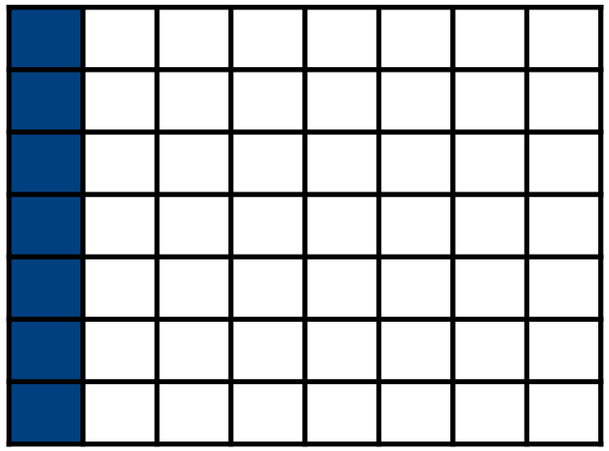


Primate–80



5x8

Primate–120



7x8

Recursive MDS matrix

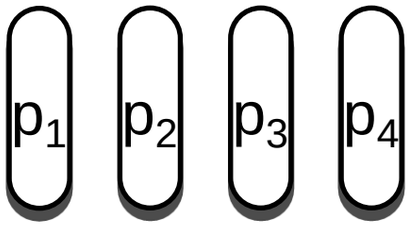
$$\otimes \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 18 & 2 & 2 & 18 \end{bmatrix}^5$$

$$\otimes \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 2 & 15 & 9 & 9 & 15 & 2 \end{bmatrix}^7$$

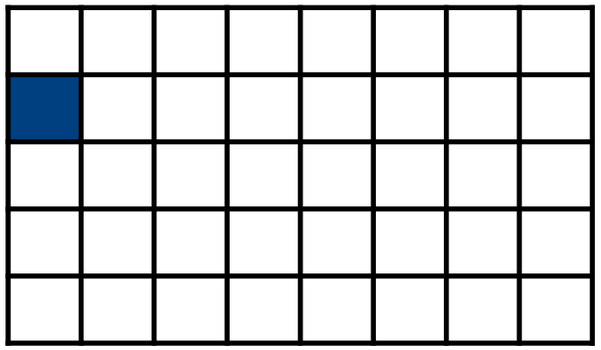
Lightweight implementation

PRIMATEs

ConstantAddition

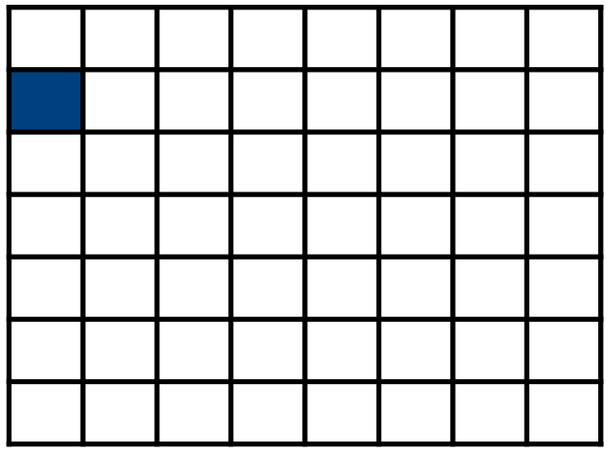


Primate–80



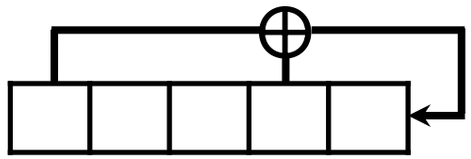
5x8

Primate–120



7x8

- 5-bit Fibonacci LFSR



- Break symmetry between rounds
- Generate different permutations

	p_1	p_2	p_3	p_4
Number of rounds	12	6	6	12
Initial value of the LFSR	1	24	30	24

PRIMATEs

Security of PRIMATEs–80/120

- Differential/linear trails for 12 rounds: max. $2^{-100}/2^{-196}$
- Impossible differentials: 5/6 rounds
- Collision trails
  - 6 rounds: 84/128 active S-boxes
  - 12 rounds: 162/224 active S-boxes

PRIMATEs vs. Other AE

PRIMATEs

- ~1300 GE (resp. ~1900 GE)
- 55 cpr (resp. 61 cpr)

AES-GCM

- AES alone is 2600 GE (21 cpr)
- Not all nonce lengths handled in same way

PRIMATEs vs. Ketje

- Ketje Jr.: ~1270 GE reg.
- Ketje Sr.: ~2500 GE reg.

PRIMATEs

General Info

http://primates.ae

PRIMATEs

Authenticated Encryption with Associated Data

Home Design Implementation Literature About Us

PRIMATEs: HANUMAN, GIBBON and APE

PRIMATEs are a family of **permutation-based authenticated encryption** algorithms for **lightweight applications**. They are currently under submission to the CAESAR competition.

There are **three PRIMATEs**: the basic SpongeWrap-variant **HANUMAN**, **GIBBON** for speed-critical applications, and **APE** for additional security when nonces are reused or unverified plaintext is released.

When resistance against **hardware side-channel attacks** is required, the PRIMATEs permutation has been designed to offer an **efficient threshold implementation** to counter first-order DPA attacks, based on glitch-free secret-sharing-based masking.

primates May 7, 2014 Uncategorized

Search

Up to date specifications

Recent Posts

- Specification v1.01
- PRIMATEs: HANUMAN, GIBBON and APE
- Drunken Monkey Competition
- Software implementation v1
- Specification v1

Contact Us

primates@esat.kuleuven.be

Drunken Monkey Competition

For the **most interesting cryptanalysis** of PRIMATEs as submitted to first round of the CAESAR competition, we give away an **entire crate** (24 bottles of 33 cl) of the **best beer in the world**: the Westvleteren XII Trappist beer.

Entries must be sent to the crypto-competitions mailing list before the start of DIAC 2014. The choice of the winner is at the discretion of the

PRIMATEs

General Info

http://primates.ae

PRIMATEs

Authenticated Encryption with Associated Data

Home Design Implementation Literature About Us

PRIMATEs: HANUMAN, GIBBON and APE

PRIMATEs are a family of **permutation-based authenticated encryption** algorithms for **lightweight applications**. They are currently under submission to the CAESAR competition.

There are **three PRIMATEs**: the basic SpongeWrap-variant **HANUMAN**, **GIBBON** for speed-critical applications, and **APE** for additional security when nonces are reused or unverified plaintext is released.

When resistance against **hardware side-channel attacks** is required, the PRIMATEs permutation has been designed to offer an **efficient threshold implementation** to counter first-order DPA attacks, based on glitch-free secret-sharing-based masking.

primates May 7, 2014 Uncategorized

Search

Recent Posts

Specification v1.01

PRIMATEs: HANUMAN, GIBBON and APE

Drunken Monkey Competition

Software implementation v1

Specification v1

Contact Us

primates@esat.kuleuven.be

Up to date specifications

SW implementation

Drunken Monkey Competition

For the **most interesting cryptanalysis** of PRIMATEs as submitted to first round of the CAESAR competition, we give away an **entire crate** (24 bottles of 33 cl) of the **best beer in the world**: the Westvleteren XII Trappist beer.

Entries must be sent to the crypto-competitions mailing list before the start of DIAC 2014. The choice of the winner is at the discretion of the

PRIMATEs

General Info

http://primates.ae

PRIMATEs

Authenticated Encryption with Associated Data

Home Design Implementation Literature About Us

PRIMATEs: HANUMAN, GIBBON and APE

PRIMATEs are a family of **permutation-based authenticated encryption** algorithms for **lightweight applications**. They are currently under submission to the CAESAR competition.

There are **three PRIMATEs**: the basic SpongeWrap-variant **HANUMAN**, **GIBBON** for speed-critical applications, and **APE** for additional security when nonces are reused or unverified plaintext is released.

When resistance against **hardware side-channel attacks** is required, the PRI permutation has been designed to offer an **efficient threshold** first-order DPA attacks, based on glitch-free secret

primates May 7, 20

Coming soon: HW implementation

Monkey Competition

For the **most interesting cryptanalysis** of PRIMATEs as submitted to first round of the CAESAR competition, we give away an **entire crate** (24 bottles of 33 cl) of the **best beer in the world**: the Westvleteren XII Trappist beer.

Entries must be sent to the crypto-competitions mailing list before the start of DIAC 2014. The choice of the winner is at the discretion of the

Westvleteren

Search

Recent Posts

Specification v1.01

PRIMATEs: HANUMAN and APE

Specification v1

Contact Us

primates@esat.kuleuven.be

Up to date specifications

SW implementation

Drunken Monkey Competition

For the most interesting cryptanalysis of PRIMATEs

Deadline: DIAC 2014

Runner-up

In a Nutshell

PRIMATEs

- Permutation-based AE
- Lightweight

Three designs

- APE: misuse resistance
- HANUMAN: ideal permutation
- GIBBON: trade-off speed/security

Efficient threshold implementation

Thank You!

Supporting Slides

PRIMATEs

Ranking w.r.t security



- APE–120
- HANUMAN–120
- GIBBON–120
- APE–80
- HANUMAN–80
- GIBBON–80