Security and IoT Applications of the Cryptosystem TinyJambu

A. FÚSTER-SABATER and M. E. PAZO-ROBLES

Institute of Physical and Information Technologies
Spanish National Research Council **(CSIC)**
Madrid, SPAIN
amparo.fuster@csic.es eugepazorobles@gmail.com

Amparo Fúster-Sabater

- Amparo Fúster-Sabater received the M.S. and Ph. D. in Physics from the University of Madrid (Spain) in 1992 and 1996, respectively.
- She is currently a Scientific Researcher at the Institute of Physical and Information Technologies (Spanish National Research Council) in Madrid.
- Her current research interests are: symmetric cryptography, cryptanalysis, cellular automata, discrete systems, linearization of complex systems.

NIST call for lightweight cryptography

- **IoT Technology:** deployed to connect devices of daily use

  all these connections need security!!!!

- The National Institute of Standards and Technology (NIST)

  "*initiated a process to solicit, evaluate, and standardize lightweight cryptographic algorithms …*" (2018)

  https://csrc.nist.gov/Projects/lightweight-cryptography

- **Lightweight** does not means **less secure**

- **Cryptosystem TinyJambu:**

  one of the 10 finalists

Connecting the world

The Cryptosystem TinyJambu

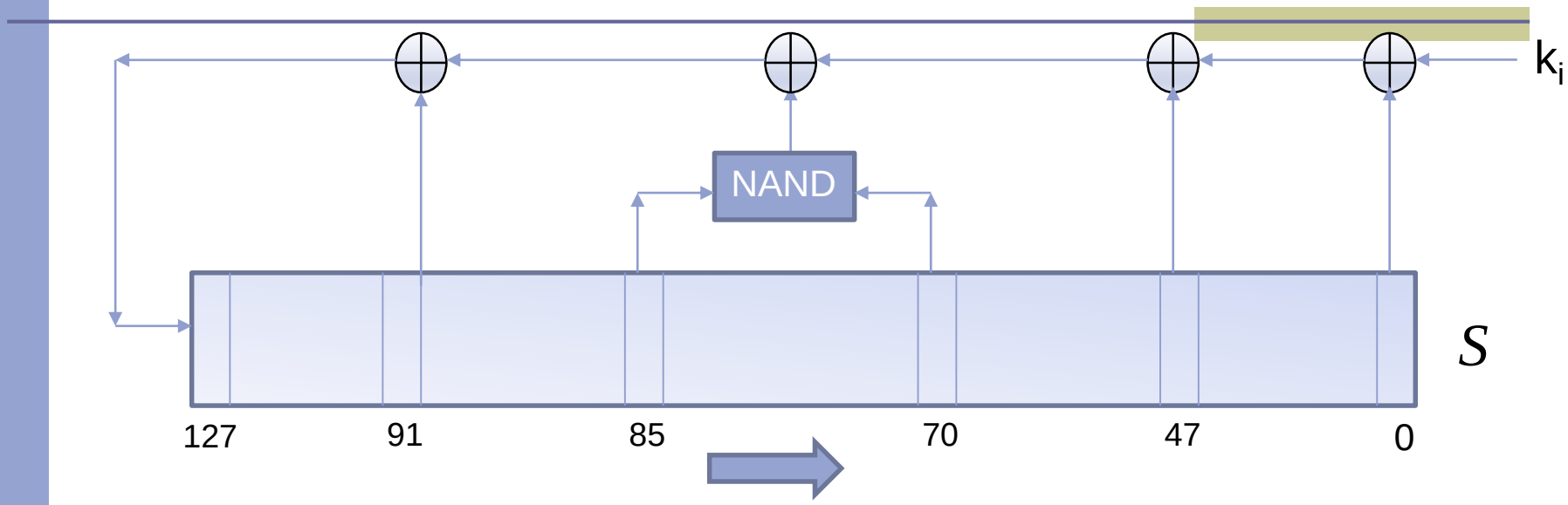
- **TinyJambu**: **the fastest** among the 10 finalists
- Authors: Hongjun Wu and Tao Huang (Division of Mathematical Sciences, Nanyang Technological University, China)

  https://csrc.nist.gov/Projects/lightweight-cryptography/round-2-candidates

- Different versions of TinyJambu:

Name	Key	Nonce	Tag	State
TinyJambu-128	128 bits	96 bits	64 bits	128 bits
TinyJambu-192	192 bits	96 bits	64 bits	128 bits
TinyJambu-256	256 bits	96 bits	64 bits	128 bits

The cryptosystem TinyJambu: structure



$$feedback = s_0 \oplus s_{47} \oplus (\overline{s_{70} s_{85}}) \oplus s_{91} \oplus k_i$$

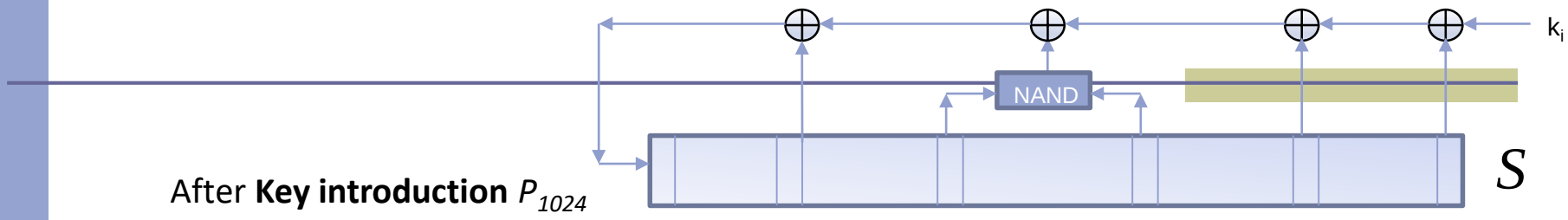
$$for\ \ j = 0\ \ to\ \ 126$$

$$s_j = s_{j+1}$$

$$s_{127} = feedback$$

- NAND: the only nonlinear component
- Update: by means of permutation (n shifts or rounds) P_n
- The scenario is just the NLFSR
- Weakness: Nonce introduction ($n = 384$ shifts or rounds) P_{384}

The Cryptosystem TinyJambu: Operation mode



After **Key introduction** P_{1024}

NONCE introduction

for *i* from 0 to 2
  Update the state using P_{384}
  $s_{\{96 \dots 127\}} = s_{\{96 \dots 127\}} + \mathbf{nonce}_{\{32i \dots 32i+31\}}$
end *for*

ENCRYPTION

for *i* from 0 to [*mlen/32*]
  Update the state using P_{1024}
  $\mathbf{ciphered}_{\{32i \dots 32i+31\}} = s_{\{96 \dots 127\}} + \mathbf{message}_{\{32i \dots 32i+31\}}$
end *for*

AD introduction

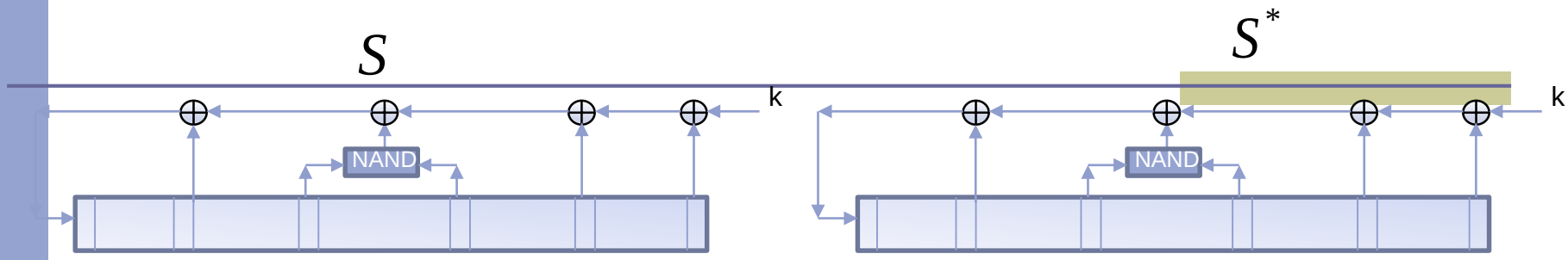
for *i* from 0 to [*adlen/32*]
  Update the state using P_{384}
  $s_{\{96 \dots 127\}} = s_{\{96 \dots 127\}} + \mathbf{ad}_{\{32i \dots 32i+31\}}$
end *for*

TAG construction

Update the state using P_{1024}
  $\mathbf{tag}_{\{0 \dots 31\}} = s_{\{64 \dots 95\}}$

Update the state using P_{384}
  $\mathbf{tag}_{\{32 \dots 63\}} = s_{\{64 \dots 95\}}$

Security margin in TinyJambu (I)



- **Differential Cryptanalysis:** evolution of the nonlinear part

- **Active AND gate** is a differential with

$$\Delta(S_{70+j}S_{85+j}) = 1 \qquad (j = 1, \cdots, 384)$$

- **Probability of success** for a differential attack is related with the number of active AND gates

  X **= No. active AND gates**

$$P_{success} \approx 2^{-X} = \frac{1}{2^X}$$

- **IDEA:** find differential trails that minimize the number of AND gates

Security margin in TinyJambu (II)

- **Designers:** $X = 80$ ⇒ $P_{designers} \approx 2^{-80}$

- **Saha et al. :** Saha, D., Sasaki, Y., Danping, S., Sibleyras, F., and Sun, S. ,"On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis". *IACR Transactions on Symmetric Cryptology* 2020(3), 152–174 (2020).

  - **Correlation conditions:**

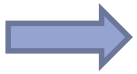
    - **If** $(\Delta S_{70+j}, \Delta S_{85+j}, \Delta S_{100+j}) = (1,0,1) \quad and \quad S_{85+j} = 1$

    - **then** $\Delta(S_{70+j} S_{85+j}) = \Delta(S_{85+j} S_{100+j}) = 1$ After 15 rounds

  - They count "correlated active gates" as a single active AND gates, thus the number of active gates is **reduced**

$$X = X_{AND} - X_{corr} = 88 - 14 = 74 \Rightarrow P_{Saha} \approx 2^{-74}$$

Our contribution

- A more refined search of differential trails based on the Saha *et al.* Model (correlated AND gates)
- We identify multiple trails for 384 rounds
- **We find differential trails with a number of active gates less than the number previously computed**
- $X = X_{AND} - X_{corr} = 84 - 13 = 71$  $P_{our} \approx 2^{-71}$
- **Gurobi Optimizer** (11.0.0) + **programmes in Python** language 3.11 64-bit + a **desktop PC** (13th Gen Intel® Core™ i9-13900K with 3.00GHz, RAM 128 GB, 24 cores) Microsoft Windows 11 Pro Operating System

Comparison among probabilities

- **For 384 rounds**

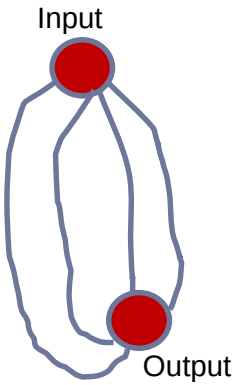


TABLE 1. SAHA et al. differential probabilities

Probability	2^{-74}	2^{-75}	2^{-76}	2^{-77}	2^{-78}	2^{-79}
# Trails	1	5	9	14	20	24

TABLE 2. OUR differential probabilities

Probability	2^{-71}	2^{-72}	2^{-73}	2^{-74}	2^{-75}	2^{-76}
# Trails	9	24	27	28	18	14

$$P_{success} \approx \frac{1}{2^{71}} > \frac{1}{2^{74}} > \frac{1}{2^{80}}$$

OURS SAHA DESIGNERS

$$P_{diff} \approx \frac{1}{2^{65.94}} > \frac{1}{2^{70.68}} > \frac{1}{2^{80}}$$

OURS SAHA DESIGNERS

Improving the security level

- For 384 rounds: TinyJambu is **not SECURE**
- Increasing the number of rounds up to 640 rounds:
  - The number of active gates increases too
  - TinyJambu seems to be immune to this kind of differential attack
- TinyJambu exhibits **good performances: (simplicity + speed)**
  - Good relationship throughput/area
  - Speed in encryption/decryption process
  - Low energy consumption
- The 640-version of TinyJambu is recommended for IoT Applications non equipped with security mechanisms

IoT Applications

- **The 640 round-version TinyJambu is recommended for:**
  - **Any sort of wearable devices** (fitness tracker, smartwatches, wearable blood pressure, etc)
  - **Environmental Sensors:** humidity, temperature, smart agriculture (Good environmental conditions)
  - **Smart cities:** air quality, parking planification, garbage collection, home automation, …
  - **In general, in any kind of application with**
    - **A non very demanding level of security**

- **The 640 round-version TinyJambu is not recommended for:**
  - **Any sort of critical infrastructures** (power plants, protection of classified information, Defence sector, emergency services, …)

Conclusions and Future Work

- TinyJambu with 384 rounds exhibits security flows
- The updated version with 640 rounds increases the level of security
- This updated version can be recommended for IoT applications with no high level of security
- This updated version must not be recommended for applications with a very demanding level of security.

- **Future work:**
  - Incorporation of TinyJambu in protocols operating in sensors Networks (e.g. MQTT protocol)
  - Study the relation between number of rounds and minimum number of active AND gates

Acknowledgements

- Thanks to

Project P2QProMeTe
PID2020-112586RBI00
funded by MCIN/ AEI
/10.14039/501100011033

Project *PID2020-112586RBI00* funded by

MINISTERIO DE CIENCIA E INNOVACIÓN

AGENCIA ESTATAL DE INVESTIGACIÓN

P^2QProMeTe