On the Security Margin of TinyJAMBU with Refined Differential and Linear Cryptanalysis

Dhiman Saha[1] Yu Sasaki[2] Danping Shi[3,4] Ferdinand Sibleyras[5], Siwei Sun[3,4] Yingjie Zhang[3,4]

[1]de.ci.phe.red Lab, Department of Electrical Engineering and Computer Science, IIT Bhilai

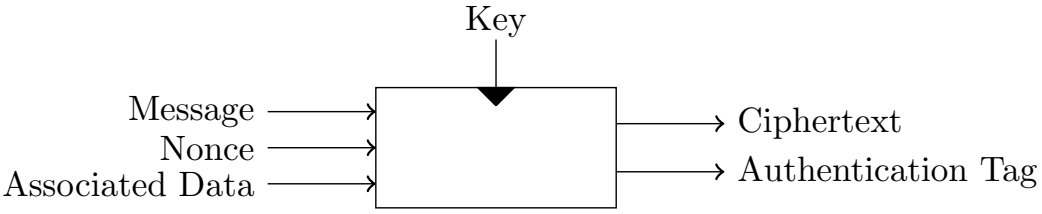
[2]NTT Secure Platform Laboratories

[3]State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences

[4]University of Chinese Academy of Sciences

[5]Inria

NIST Lightweight Cryptography Workshop 2020


Key
Message
Nonce
Associated Data
Ciphertext
Authentication Tag

- Designed by Hongjun Wu and Tao Huang
- A small variant of JAMBU [WH15]
- A family of AEAD schemes
- Currently a Round-2 candidate in NIST LWC

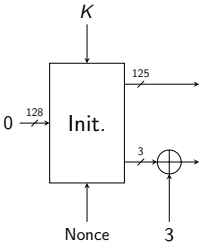
Table: Security goals of TinyJAMBU with unique nonce

Version	Encryption	Authentication
TinyJAMBU-128	112-bit	64-bit
TinyJAMBU-192	168-bit	64-bit
TinyJAMBU-256	224-bit	64-bit

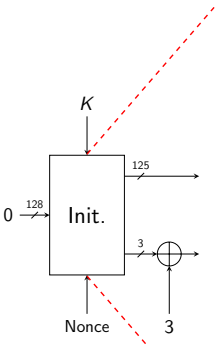
Reference:

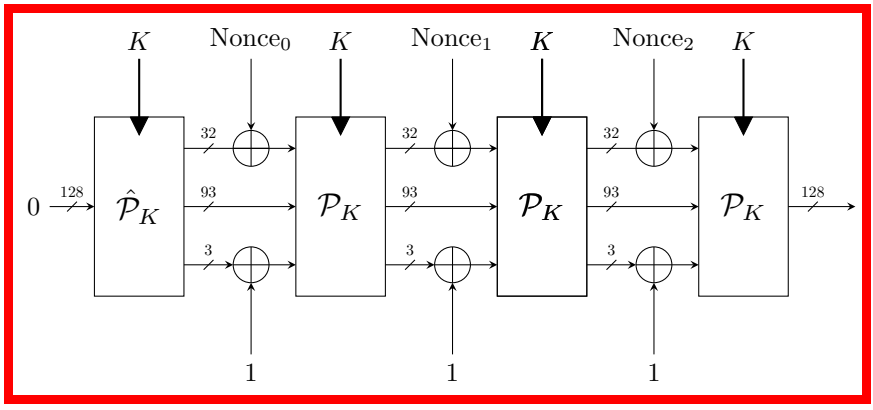
- WH15 - JAMBU Lightweight Authenticated Encryption Mode and AES-JAMBU. Submission to CAESAR, 2015

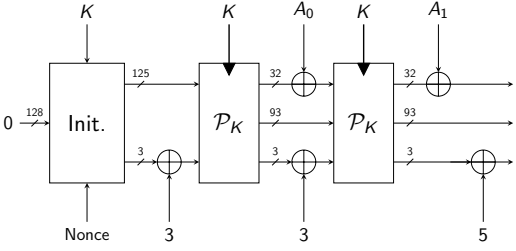
Step 1: Initialization



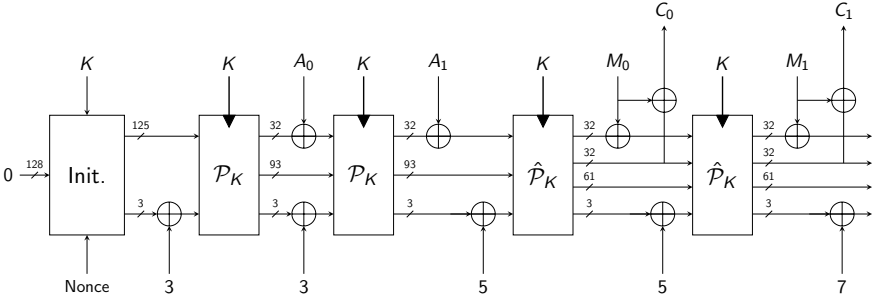
Inside Init. (Key Setup + Nonce Setup)



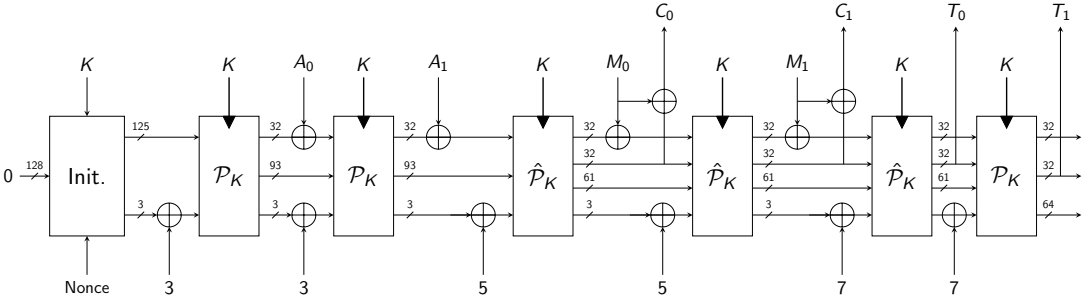


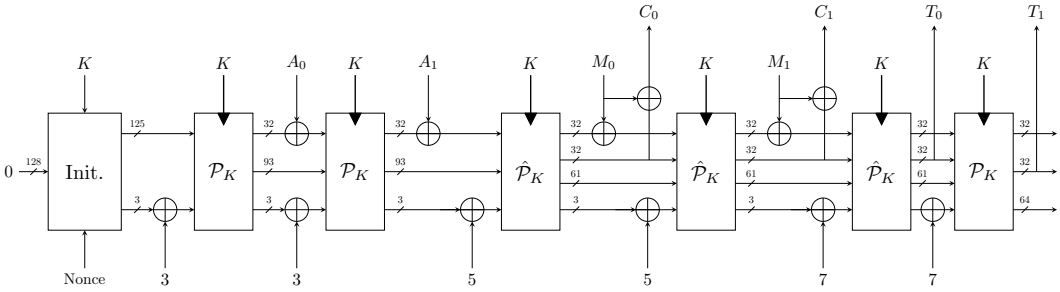

K
K
A_0
K
A_1
0
128
Init.
125
3
$\mathcal{P}_K$
32
93
3
$\mathcal{P}_K$
32
93
3
Nonce
3
3
5

Step 3: Encryption



Step 4: Finalization

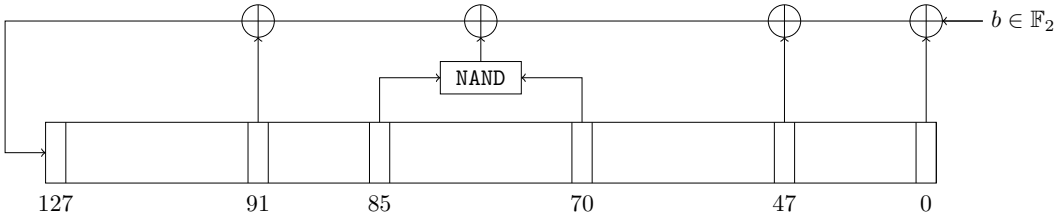




AEAD	Sizes in bits				# of rounds	
	State	Key	Nonce	Tag	$\mathcal{P}_K$	$\hat{\mathcal{P}}_K$
TinyJAMBU-128	128	128	96	64	384	1024
TinyJAMBU-192	128	192	96	64	384	1152
TinyJAMBU-256	128	256	96	64	384	1280

- Note: The number of rounds of $\hat{\mathcal{P}}_K$ is much **larger** than that of $\mathcal{P}_K$
- Used in Key Setup and Encryption

- NLFSR based keyed-permutation
- Computes only a single NAND gate as a non-linear component per round



Previous Cryptanalysis and Research Challenges

Strategy

Counts the number of **active AND** gates to find differential and linear trails with the minimum of such active gates by MILP

Why is this insufficient? → **Fast but inaccurate**

- Ignores the correlation between multiple AND gates which can impact probabilities of the differential or linear trails [KLT15, AEL+18]
- Designers have ignored effect of differentials which can amplify the probabilities of the trails [AK18]
- For linear cryptanalysis designer only analyzed internal permutation assuming access to all input bits

- KLT15 - Kölbl et al. Observations on the SIMON block cipher family. CRYPTO 2015
- AEL+18 - Ashur et al. Cryptanalysis of MORUS ASIACRYPT 2018
- AK18 - Ankele and Kölbl. Mind the Gap - A Closer Look at the Security of Block Ciphers against Differential Cryptanalysis. SAC 2018

A Note on Existing Literature on MILP Modeling

- Techniques exists to evaluate the exact probability by limiting the search space to only valid trails [SHW+15a, SHW+15b]

What is the issue? → **Accurate but too slow**

- Such models involve too many variables and constraints
- Cannot be solved in practical time
- Good for verifying the validity of a given trail
- Not so efficient to find optimal ones [SHW+15a]

- SHW+15a - Sun et al. Constructing mixed-integer programming models whose feasible region is exactly the set of all valid differential characteristics of SIMON. ePrint 2015
- SHW+15b - Sun et al. Extending the applicability of the mixed- integer programming technique in automatic differential cryptanalysis. ISC 2015

A Note on Existing Literature on MILP Modeling

- Techniques exists to evaluate the exact probability by limiting the search space to only valid trails [SHW+15a, SHW+15b]

What is the issue? → **Accurate but too slow**

- Such models involve too many variables and constraints
- Cannot be solved in practical time
- Good for verifying the validity of a given trail
- Not so efficient to find optimal ones [SHW+15a]

Our Motivation: Strike a good balance of efficiency and accuracy while modeling

---

- SHW+15a - Sun et al. Constructing mixed-integer programming models whose feasible region is exactly the set of all valid differential characteristics of SIMON. ePrint 2015
- SHW+15b - Sun et al. Extending the applicability of the mixed- integer programming technique in automatic differential cryptanalysis. ISC 2015

Our Contributions

What happens in the simple model?

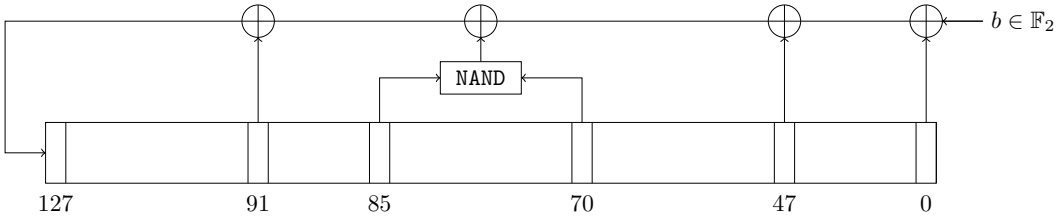
If there is a difference on at least one of the two input bits, the output of the AND gates has a difference with probability 2^{-1} or does not with probability 2^{-1}

- It considers independently every AND gate and
- Treats every AND gate in the same way

Table: Restrictions on the values of a and b in $a \cdot b = z$ when $\Delta z = 1$.

Δa	Δb	$\Delta z = 1$ iff
0	0	Never
0	1	$a = 1$
1	0	$b = 1$
1	1	$a = b$

Simple model fails to capture these restrictions

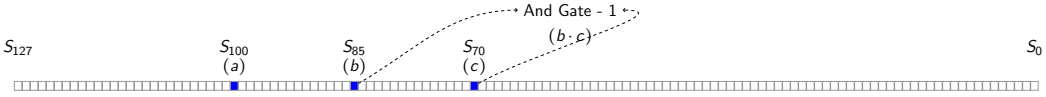


Main Observation

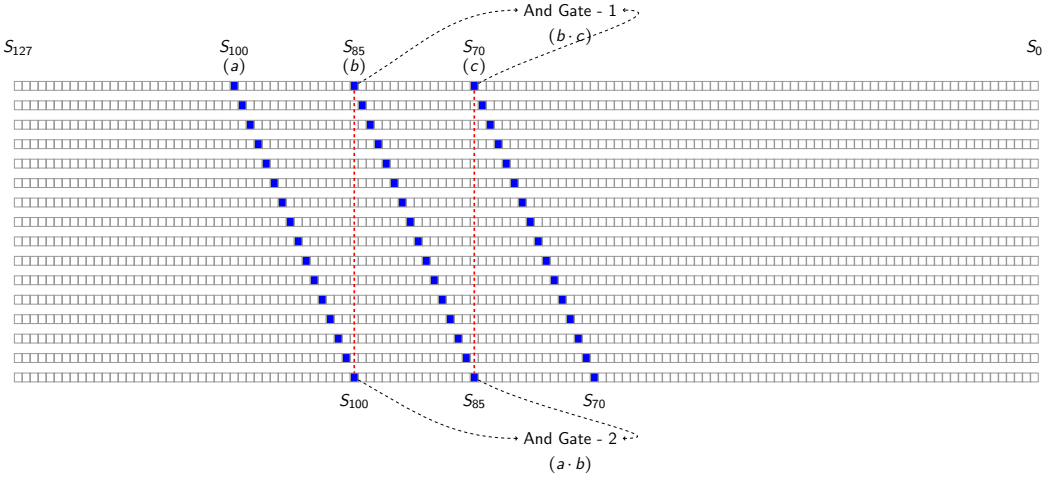
The same value, as it is shifted, will enter twice in two different AND gates.

The Internal State ($S_{127}, \cdots S_0$)

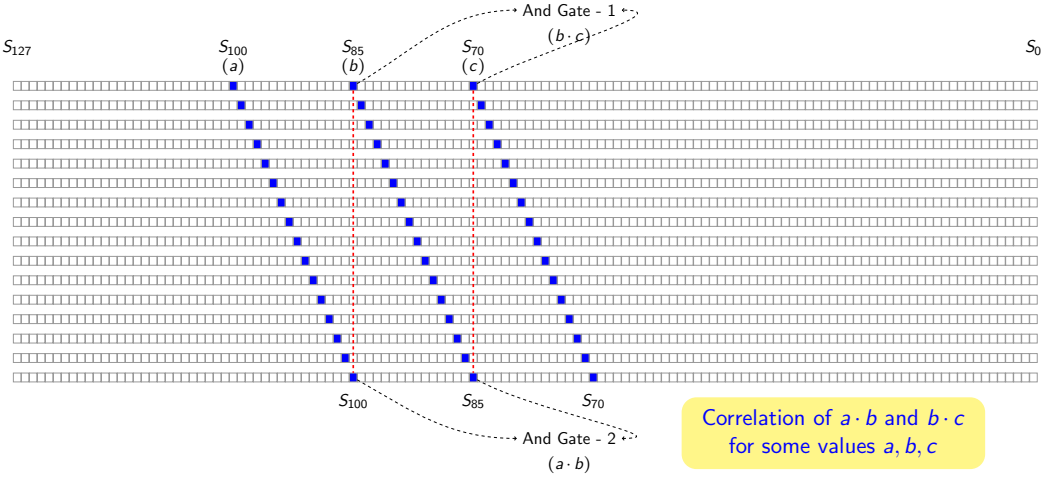
S_{85} Enters AND gate Twice (First: $b \cdot c$)



After 15 rounds (Second: $a \cdot b$)

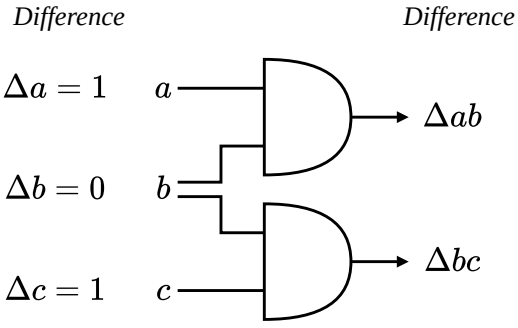


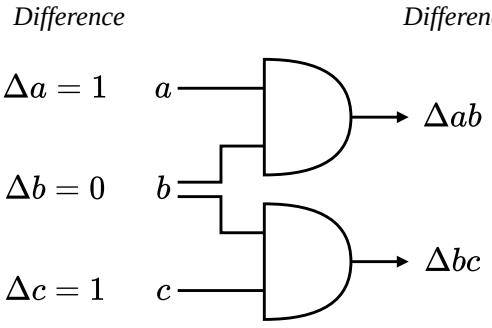
First Order Correlations



Correlation of $a \cdot b$ and $b \cdot c$ for some values a, b, c

Dependency of two AND gates

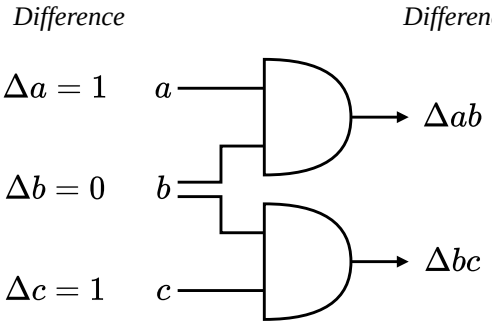




Case-1: $b = 0$

$\Delta ab = \Delta bc = 0$

$\text{Probability} = 2^{-1}$



Case-1: $b = 0$

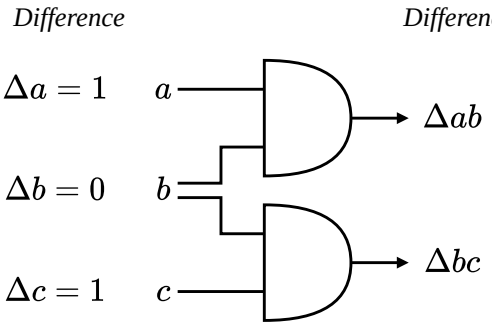
$\Delta ab = \Delta bc = 0$

$\text{Probability} = 2^{-1}$

Case-2: $b = 1$

$\Delta ab = \Delta bc = 1$

$\text{Probability} = 2^{-1}$



Case-1: $b = 0$

$\Delta ab = \Delta bc = 0$

$\text{Probability} = 2^{-1}$

Case-2: $b = 1$

$\Delta ab = \Delta bc = 1$

$\text{Probability} = 2^{-1}$

In this scenario **Refined model**

- Forces that both differences jointly propagate, or not, and
- Only counts this as a **single** active gate.

MILP model variables:

- d_a modelizes Δa
- d_{ab} modelizes Δab
- γ_{abc} indicates if there's a correlation between the two AND gates ab and bc.

Finally

Subtract all values γ_{abc} in the objective function to only count this **once**, whereas the simple model would count two active gates.

- It adds **additional** constraints on top of the simple model
- All chained AND gates are recorded

Example Recorded Chains - $\{(d_{ab}, d_a, d_b), (d_{bc}, d_b, d_c), \dots\}$

Then for all consecutive couples $\big((d_{ab}, d_a, d_b), (d_{bc}, d_b, d_c)\big)$ the following constraint is added:

$$\begin{aligned} \gamma_{abc} &= d_a \overline{d_b} d_c \\ d_{ab} - d_{bc} &\leq 1 - \gamma_{abc} \\ d_{bc} - d_{ab} &\leq 1 - \gamma_{abc} \end{aligned}$$

Differential Cryptanalysis

- Designers searched for the differential trail that has the minimum number of active AND gates in the **simple** model

  Type 1: Input differences only exist in the 32 MSBs. No constraint on the output.

  Type 2: No constraint on the input. Output differences only exist in the 32 MSBs.

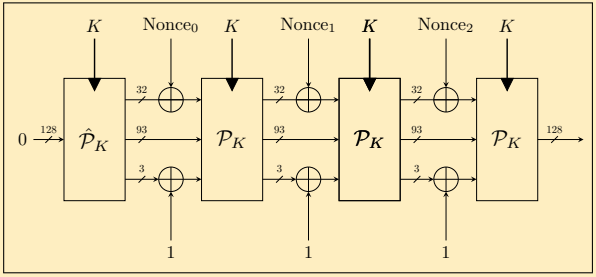
  Type 3: Both of the input and output differences only exist in the 32 MSBs.

  Type 4: No constraint.

Designers Claim	Proven **Wrong** in Refined Model

- Max. probability of the 384-round trail of Type 3 is 2^{-80}
- Max. probability of the 320-round characteristic of Type 4 is 2^{-13}

Forgery for TinyJAMBU Mode



Exploiting $(\Delta_i \| 0^{96}) \xrightarrow{\mathcal{P}_K} (\Delta_{i+1} \| 0^{96})$ with probability p

- Attack the nonce setup or
- The associated data processing
- Recall $\mathcal{P}_K \rightarrow$ 384 Rounds
- Use Type 3 trails

- Also makes the case for MAC reforgeability [BC09]
- We also look at cluster of multiple trails **unlike** designers

- BC09 - Black and Cochran. MAC reforgeability. FSE 2009

Observations on Full 384 Rounds

- Found contradiction for simple model
- Refined model reports 88 active AND gates
- 14 couples are correlated
- Prob. $= 2^{-(88-14)} = 2^{-74}$

Input:	$\Delta S_{127..0}$	01004800	00000000	00000000	00000000
	$\Delta S_{255..128}$	81044c80	24080304	d9200000	22090000
	$\Delta S_{383..256}$	81004082	00010200	83000010	26090240
Output:	$\Delta S_{511..384}$	81004082	00000000	00000000	00000000

103 distinct differential trails — **Overall Differential Prob.** $= 2^{-70.68}$

Probability	2^{-74}	2^{-75}	2^{-76}	2^{-77}	2^{-78}	2^{-79}	2^{-80}
# Trails	1	5	9	14	20	24	30

Differential Cryptanalysis of 338 Rounds

- Find largest number of rounds with security less than 64 bits
- Trail found with 76 active AND gates
- Correlation of two AND gates occurs 12 times
- Prob. $= 2^{-(76-12)} = 2^{-64}$

Input:	$\Delta S_{127..0}$	80104912	00000000	00000000	00000000
	$\Delta S_{255..128}$	00104c12	24800628	91000810	40092240
	$\Delta S_{383..256}$	00000000	00000200	81040000	04010200
Output:	$\Delta S_{465..338}$	00802041	00000000	00000000	00000000

24 distinct differential trails — **Overall Differential Prob.** $= 2^{-62.68}$

Probability	2^{-64}	2^{-66}	2^{-67}	2^{-68}	2^{-69}	2^{-70}	2^{-71}	2^{-72}
# Trails	1	2	4	4	4	5	4	4

Unrestricted Differentials

- No restriction on the input or output
- Type 4 as per `TinyJAMBU` submission document

Rounds	192	320	384
Designers (Simple)	4	13	-
Ours (Refined)	4	12	19

Type 4 Found with refined model

Prob. $= 2^{-19}$

Input:	$\Delta S_{127..0}$	80000000	20010000	00000092	00000000
	$\Delta S_{255..128}$	00000000	20000000	00004000	00000004
	$\Delta S_{383..256}$	00000000	20000000	00000000	00000000
Output:	$\Delta S_{511..384}$	81020000	20001000	00004080	00000004

- Trails experimentally **verified**[1] with conforming pairs

[1] `https://github.com/c-i-p-h-e-r/refinedTrailsTinyJambu`

Partly Restricted Differentials

- Type 1 (Input restricted)

Rounds	256	320	384	448	512
Designers (Simple)	22	33	45	55	68
Ours (Refined)	20	29	41	51	64?

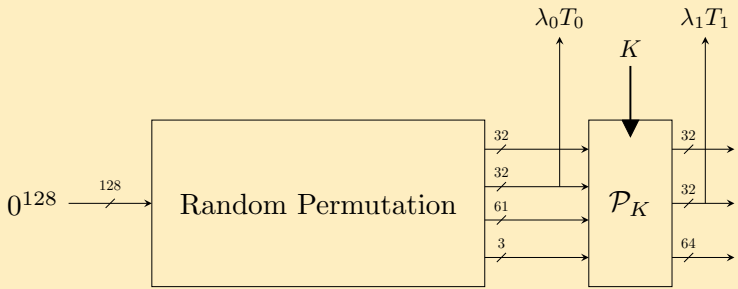
- Type 2 (Output restricted)

Rounds	384	512
Designers (Simple)	28	47
Ours (Refined)	28	47

- Note Type 1 Score is improved for all rounds
- Combining Type 1 and 2 for forgery (384 Rounds) as suggested in submission document
  - Designers $\rightarrow 2^{-73}$
  - Ours $\rightarrow 2^{-69}$

Linear Cryptanalysis

Linear trails of TinyJAMBU carrying the correlation of the tag



- We can adapt the **same idea** of correlated AND gates to refine our model to look for better linear approximations

- The best linear trails were consistently having **no** correlated gates
- Score of the best linear trail with unrestricted input, restricted output:

Rounds	256	320	384	448	512
Designers	12	16	22	26	29
Ours (Refined)	10	15	22	27?	46?

- Bias 2^{-41} optimal linear trail for 384 rounds found with the refined model
- Does not contradict the authors' claims

Input:	$mS_{127..0}$	00000000	41100081	00000000	00000000
	$mS_{255..128}$	00408000	41120491	02008024	08000088
	$mS_{383..256}$	30c80024	41804890	00449144	80000089
Output:	$mS_{511..384}$	00000000	00022890	00000000	00000000

Summary

- First 3rd-Part Cryptanalysis of `TinyJAMBU`
- Refined model efficiently finds highly accurate differential and linear trails
- With the refined model, we found
  - A forgery attack with complexity $2^{62.68}$ on 338 rounds
  - A differential trail with probability $2^{-70.68}$ for the full 384 rounds
- Security margin of `TinyJAMBU` is smaller than originally expected
  - 12% with respect to the number of unattacked rounds
  - Less than 8 bits in the data complexity for the full rounds.
- Refined model for the linear cryptanalysis found the better bias for some number of rounds.
- One simple solution would be to increase the number of rounds of the small version, $\mathcal{P}_K$ from 384 to 512 rounds.
- Using the refined model may lead to a better choice of tap positions with respect to DC/LC

Thank You

Image Source: Google

Work **initiated** during group discussion sessions of ASK 2019, Japan
Accepted at IACR Trans. on Symmetric Cryptology Volume 2020, Issue 3.

The source code for finding conforming pairs and the MILP trails search can be found here
`https://github.com/c-i-p-h-e-r/refinedTrailsTinyJambu`