Revisiting the Extension of Matsui's Algorithm 1 to Linear Hulls: Application to TinyJAMBU

Muzhou Li[1,2] Nicky Mouha[3] Ling Sun[1,2] Meiqin Wang[1,2,4,✉]

[1]Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

[2]School of Cyber Science and Technology, Shandong University, Qingdao, China

[3]Strativia, Largo, MD, USA

[4]Quan Cheng Shandong Laboratory, Jinan, China

March 24, 2023 @ Beijing

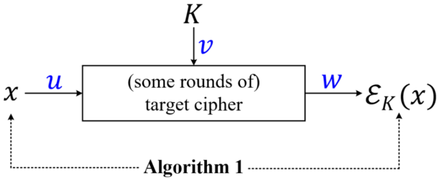
Outline

Outline

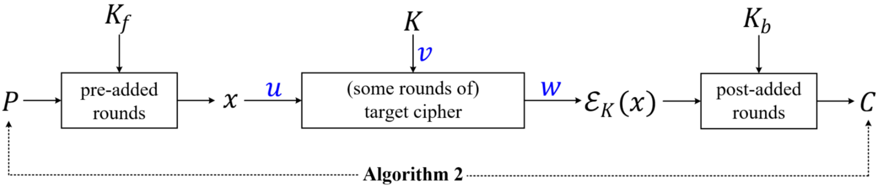
Motivation

Linear Cryptanalysis [Matsui @ EUROCRYPT 1993]

$$u \cdot x \oplus w \cdot \mathcal{E}_K(x) = v \cdot K \text{ (high correlation Cor)}$$



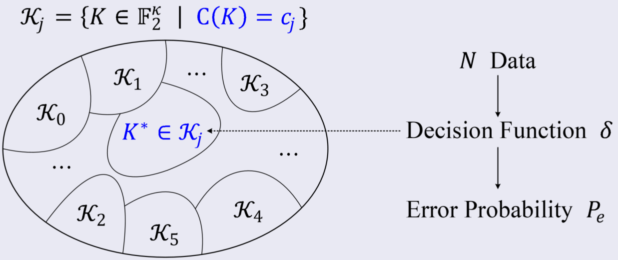
sign of Cor $\Rightarrow v \cdot K$



absolute value of Cor $\Rightarrow K_f, K_b, v \cdot K$

Motivation

Linear Hull Version of Algorithm 1 [Röck & Nyberg @ DCC]



Relation between N and P_e is not accurately described (Experiments)

▲ Inaccuracy comes from the methodology of deducing this relation.

▲ Algorithm 1 is more suitable than Algorithm 2: for ciphers where only part of the state can be obtained.

Contribution

New Statistical Models

Absolute Error $\max|P_e^{theory} - P_e^{expr.}| =$

1. Previous Methodology $\Rightarrow$ 93.75% (MLE)
2. Our Methodology $\Rightarrow$ 1.9% $\searrow$ (MLE), 2.19% $\searrow$ (Threshold)

Key Recovery Attacks on TinyJAMBU [Wu & Huang]

	Method	Attack Phase	Attacked/ Total	Key Len. Supported	Key Bits Rec.	Reference
v1	Cube	Ini. & Enc.	2604/3200	128	1-bit	Teng et al. @ ePrint2021/1164
	Linear Hull	**Tag Gen.**	**384/384**	**all**	**$\geq$ 7-bit**	**Our**
v2	**Linear Hull**	**Tag Gen.**	**387/640**	**all**	**$\geq$ 7-bit**	**Our**

First cryptanalysis results in the nonce-respecting setting on the full TinyJAMBU v1 and the round-reduced TinyJAMBU v2.

Contribution

New Statistical Models

Absolute Error $\max|\mathrm{P}_e^{\text{theory}} - \mathrm{P}_e^{\text{expr.}}| =$

1. Previous Methodology $\Rightarrow$ 93.75% (MLE)
2. Our Methodology $\Rightarrow$ 1.9% $\searrow$ (MLE), 2.19% $\searrow$ (Threshold)

Key Recovery Attacks on TinyJAMBU [Wu & Huang]

	Method	Attack Phase	Attacked/ Total	Key Len. Supported	Key Bits Rec.	Reference
v1	Cube	Ini. & Enc.	2604/3200	128	1-bit	Teng et al. @ ePrint2021/1164
	Linear Hull	**Tag Gen.**	**384/384**	**all**	$\geq$ **7-bit**	**Our**
v2	**Linear Hull**	**Tag Gen.**	**387/640**	**all**	$\geq$ **7-bit**	**Our**

First cryptanalysis results in the nonce-respecting setting on the full TinyJAMBU v1 and the round-reduced TinyJAMBU v2.

Outline

Previous Extension: Key Recovery Framework

$$\mathcal{K}_j = \{K \in \mathbb{F}_2^\kappa \mid \mathtt{C}(K) = c_j\}, \qquad \pi_j = \frac{|\mathcal{K}_j|}{2^\kappa}$$

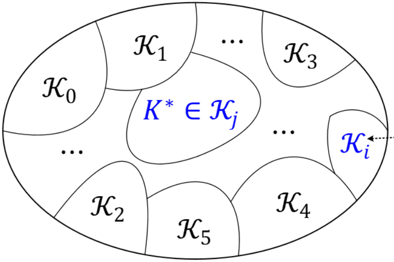
N Data

$\downarrow$

Statistic T

$\downarrow$

Decision Function $\delta(T)$



P_{ij}

$$P_j^e = \sum_{i \neq j} P_{ij}$$

$$P_e = \sum_j \pi_j \, P_j^e \quad \text{(average over all keys)}$$

- Relation between N and P_e should be depicted accurately.

Previous Extension: Methodology

Given desired P_e:

- $P_{ij} = \frac{P_e}{m-1}$ (assumption) *with m being the number of all key classes*
- N_{ij}: data needed in making decision between $\mathcal{K}_i$ and $\mathcal{K}_j$
- Construct the relation between P_{ij} and N_{ij} with statistical models
- $N = \max N_{ij}$ (upper bound)

Such methodology causes the inaccuracy.

Previous Extension: Three Attack Settings

Direct Attack:

$$\mathcal{K}_i = \{K \in \mathbb{F}_2^\kappa \mid C(K) = c_i\}$$

Basic RK: *fixed key difference* α

$$\mathcal{K}_i^\alpha = \{K \in \mathbb{F}_2^\kappa \mid C(K) - C(K \oplus \alpha) = c_i\}$$

Multiple RK: t *differences* $\alpha_0, \alpha_1, \cdots, \alpha_{t-1}$ *(form a basis)*

- Proceed basic rk attack under each α_j, and obtain guessed $\mathcal{K}_{\eta_j}^{\alpha_j}$
- If all these attacks succeed, K^* must belong to $\bigcap_{0 \le j \le t-1} \mathcal{K}_{\eta_j}^{\alpha_j}$

Key Information Obtained

Direct Attack < Basic RK < Multiple RK

Outline

Threshold-Based Statistical Model (Direct Attack)

New Methodology

For each j:

- Depict clearly the distribution $\mathcal{D}_j$ of T related to N when $K^* \in \mathcal{K}_j$
- Compute P_{ij} with the CDF of $\mathcal{D}_j$ and $\delta(T) = i$

Get $P_e = \sum_j \pi_j \sum_{i \neq j} P_{ij}$

Statistic & Distribution

Let N_0^K records how many x fulfill the linear hull given N known data x.

$$T = 2\frac{N_0^K}{N} - 1 \sim \mathcal{D}_j = \mathcal{N}\left(c_j, \sigma^2 = \frac{1 - c_j^2}{N} B\right)$$

when $K^* \in \mathcal{K}_j$, where $B = 1$ (KP sampling) or $\frac{2^n - N}{2^n - 1}$ (DKP sampling).

Threshold-Based Statistical Model (Direct Attack)

New Methodology

For each j:

- Depict clearly the distribution $\mathcal{D}_j$ of T related to N when $K^* \in \mathcal{K}_j$
- Compute P_{ij} with the CDF of $\mathcal{D}_j$ and $\delta(T) = i$

Get $P_e = \sum_j \pi_j \sum_{i \neq j} P_{ij}$

Statistic & Distribution

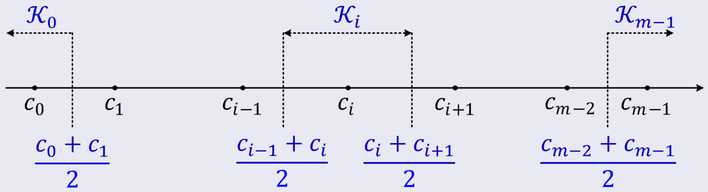
Let N_0^K records how many x fulfill the linear hull given N known data x.

$$T = 2\frac{N_0^K}{N} - 1 \sim \mathcal{D}_j = \mathcal{N}\left(c_j, \sigma^2 = \frac{1 - c_j^2}{N} B\right)$$

when $K^* \in \mathcal{K}_j$, where $B = 1$ (KP sampling) or $\frac{2^n - N}{2^n - 1}$ (DKP sampling).

Threshold-Based Statistical Model (Direct Attack)

Threshold-Based Decision Function $\delta(T)$

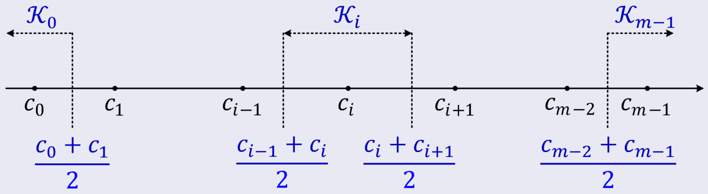


$$
\begin{aligned}
P_{ij} &= \Pr[\,\delta(T) = i \,|\, T \sim D_j\,] \\
&= \Pr\left[\frac{c_{i-1}+c_i}{2} < T \le \frac{c_i+c_{i+1}}{2} \,\middle|\, T \sim \mathcal{N}\left(c_j, \sigma^2\right)\right] \\
&= \Phi\left(\frac{\frac{c_i+c_{i+1}}{2} - c_j}{\sigma}\right) - \Phi\left(\frac{\frac{c_{i-1}+c_i}{2} - c_j}{\sigma}\right)
\end{aligned}
$$

where $\Phi(\cdot)$ denotes the CDF of $\mathcal{N}(0,1)$.

Threshold-Based Statistical Model (Direct Attack)

Threshold-Based Decision Function $\delta(T)$



$$
\begin{aligned}
P_{ij} &= \Pr[\,\delta(T) = i \,|\, T \sim D_j\,] \\
&= \Pr\left[\frac{c_{i-1} + c_i}{2} < T \leq \frac{c_i + c_{i+1}}{2} \,|\, T \sim \mathcal{N}\left(c_j, \sigma^2\right)\right] \\
&= \Phi\left(\frac{\frac{c_i + c_{i+1}}{2} - c_j}{\sigma}\right) - \Phi\left(\frac{\frac{c_{i-1} + c_i}{2} - c_j}{\sigma}\right)
\end{aligned}
$$

where $\Phi(\cdot)$ denotes the CDF of $\mathcal{N}(0, 1)$.

Experimental Verification on Threshold-Based Models

Use 256-round keyed permutation of TinyJAMBU

Linear Hull: $\{7, 30, 37, 44, 54, 64, 77, 81, 84, 91, 98, 118, 121\} \to \{64\}$

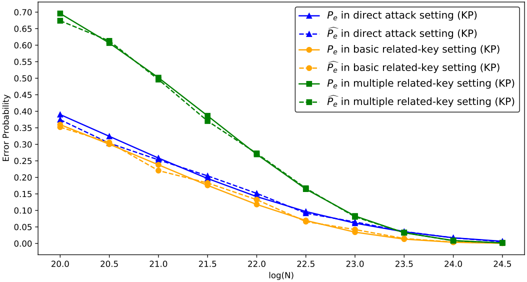
- Trail 1: $7, 27, 30, 37, 44, 81, 111, 118$ ($\mathrm{Cor} = +2^{-10}$)
- Trail 2: $6, 7, 27, 30, 37, 44, 81, 111, 118$ ($\mathrm{Cor} = -2^{-11}$)
- Trail 3: $7, 21, 27, 30, 37, 44, 81, 111, 118$ ($\mathrm{Cor} = -2^{-11}$)
- Trail 4: $6, 7, 21, 27, 30, 37, 44, 81, 111, 118$ ($\mathrm{Cor} = +2^{-11}$)

Let $ek = k_7 \oplus k_{27} \oplus k_{30} \oplus k_{37} \oplus k_{44} \oplus k_{81} \oplus k_{111} \oplus k_{118}$. The whole key space $k_{21} \| ek \| k_6 \in \mathbb{F}_2^3$ is divided into four disjoint classes:

$$\mathcal{K}(c_0 = -2.5 \cdot 2^{-10}) = \{7\}, \mathcal{K}(c_1 = -0.5 \cdot 2^{-10}) = \{2, 3, 6\},$$
$$\mathcal{K}(c_2 = +0.5 \cdot 2^{-10}) = \{0, 1, 4\}, \mathcal{K}(c_3 = +2.5 \cdot 2^{-10}) = \{5\}.$$

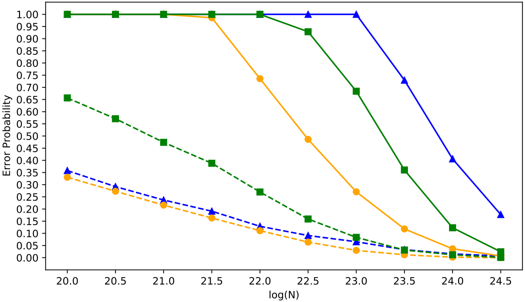
Key information can be recovered using our statistical models.

Experimental Verification on Threshold-Based Models



Our Threshold-Based

2.19%



Previous MLE-Based

93.45%

MLE-Based Statistical Models

Direct Attack (KP Sampling)

- $\delta(T) = i \iff \mathrm{ML}(T, i) > \mathrm{ML}(T, t)$ for $\forall\, t \neq i$
- For each t:
  - When $p_i > p_t$,

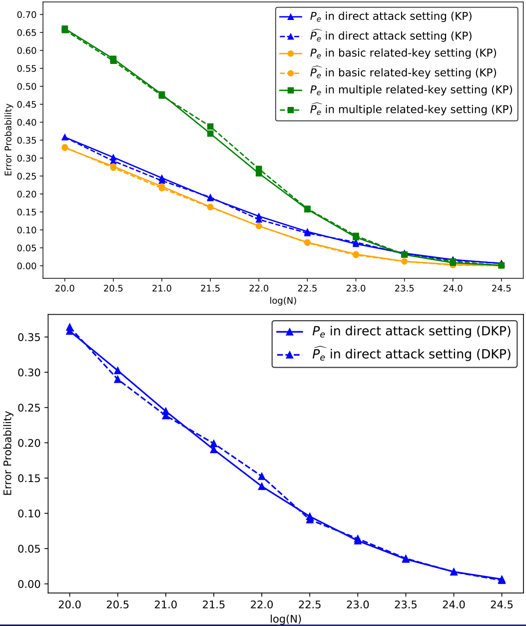
$$\frac{\log_2 \pi_t - \log_2 \pi_i + N \log_2(1 - p_t) - N \log_2(1 - p_i)}{\log_2 p_i - \log_2(1 - p_i) - \log_2 p_t + \log_2(1 - p_t)} < T < N$$

  - When $p_i < p_t$,

$$0 < T < \frac{\log_2 \pi_t - \log_2 \pi_i + N \log_2(1 - p_t) - N \log_2(1 - p_i)}{\log_2 p_i - \log_2(1 - p_i) - \log_2 p_t + \log_2(1 - p_t)}$$

- Intersection of above $(m - 1)$ intervals: $N^i_{\min} < T < N^i_{\max}$
- $P_{ij} = \Phi^b_{N,p_j}\left(N^i_{\max}\right) - \Phi^b_{N,p_j}\left(N^i_{\min}\right)$. Φ^b_{N,p_j} is the CDF of T.

Experimental Verification on MLE-Based Models



Our MLE-Based

1.9%

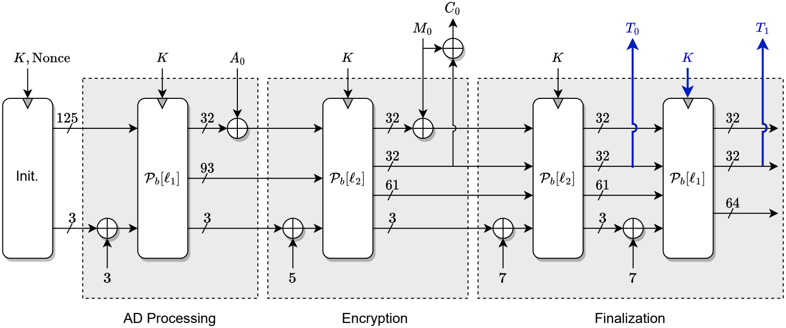
slightly more precise
but
much slower to compute

Outline

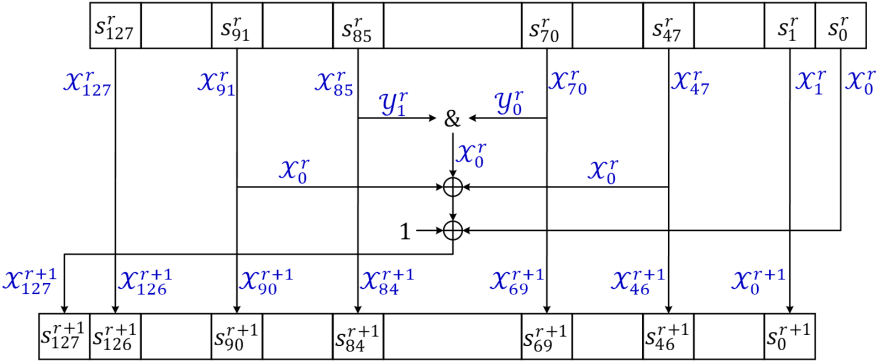
Brief Introduction to TinyJAMBU

TinyJAMBU [Wu & Huang]:

- Key: 128-, 192-, 256-bit
- $\mathcal{P}_b : (s_{127}, s_{126}, \cdots, s_0) \rightarrow (z, s_{127}, \cdots, s_1)$
  $$z = s_0 \oplus s_{47} \oplus (\sim (s_{70} \& s_{85})) \oplus s_{91} \oplus k_i$$
- $l_1 = 384$ (v1); $l_1 = 640$ (v2)



Correlation Evaluation of Linear Trail



For R-round trail:

$$\lambda_0 \cdot T_0 \oplus \lambda_1 \cdot T_1 = \mathcal{X}^0 \cdot x^0 \oplus \mathcal{X}^R \cdot x^R = \bigoplus_{r=0}^{R-1} (\mathcal{X}^r \cdot x^r \oplus \mathcal{X}^{r+1} \cdot x^{r+1}) = \bigoplus_{s=0}^{14} f_s$$

Correlation Evaluation of Linear Trail

$$
\begin{aligned}
f_s = & \mathcal{X}_0^s(x_{70}^s \& x_{85}^s) \oplus \mathcal{X}_0^{s+15}(x_{85}^s \& x_{85}^{s+15}) \oplus \mathcal{X}_0^{s+30}(x_{85}^{s+15} \& x_{85}^{s+30}) \\
& \oplus \cdots \oplus \mathcal{X}_0^{s+15t_s}(x_{85}^{s+15(t_s-1)} \& x_{85}^{s+15t_s}) \\
& \oplus \mathcal{X}_0^s \mathcal{Y}_0^s x_{70}^s \\
& \oplus \left[\mathcal{X}_0^s \mathcal{Y}_1^s \oplus \mathcal{X}_0^{s+15} \mathcal{Y}_0^{s+15}\right] x_{85}^s \\
& \oplus \left[\mathcal{X}_0^{s+15} \mathcal{Y}_1^{s+15} \oplus \mathcal{X}_0^{s+30} \mathcal{Y}_0^{s+30}\right] x_{85}^{s+15} \oplus \cdots \\
& \oplus \left[\mathcal{X}_0^{s+15(t_s-1)} \mathcal{Y}_1^{s+15(t_s-1)} \oplus \mathcal{X}_0^{s+15t_s} \mathcal{Y}_0^{s+15t_s}\right] x_{85}^{s+15(t_s-1)} \\
& \oplus \mathcal{X}_0^{s+15t_s} \mathcal{Y}_1^{s+15t_s} x_{85}^{s+15t_s} \\
& \oplus \bigoplus_{j=0}^{t_s} \mathcal{X}_0^{s+15j}(1 \oplus k_{s+15j \bmod \kappa})
\end{aligned}
$$

f_s contains several Boolean functions with chained AND gates.

Correlation evaluation of the linear trail $\iff$ evaluate these f_s

Correlation Evaluation of Linear Trail

$$f(x_0, \ldots, x_n) = x_0 \& x_1 \oplus x_1 \& x_2 \oplus \cdots \oplus x_{n-1} \& x_n \oplus a_0 x_0 \oplus \cdots \oplus a_n x_n$$

Absolute Correlation [Song et al.]

1. n Odd: $|\mathrm{Cor}(f)| = 2^{-(n+1)/2}$.
2. n Even: $|\mathrm{Cor}(f)| = 2^{-n/2}$ if $\bigoplus_{j=0}^{n/2} a_{2j} = 0$; otherwise, $|\mathrm{Cor}(f)| = 0$.

$$\mathrm{Sign}(f) = \prod_{i=0}^{t-1} (-1)^{\left(\bigoplus_{j=0}^{i} a_{2j}\right) a_{2i+1}}, t = \begin{cases} \frac{n+1}{2}, & n \text{ Odd} \\ \frac{n}{2}, & n \text{ Even and } \bigoplus_{j=0}^{t} a_{2j} = 0 \end{cases}$$

Key Bits Involved

$$\lambda_0 \cdot T_0 \oplus \lambda_1 \cdot T_1 \approx \bigoplus_{r=0}^{R-1} \mathcal{X}_0^r (1 \oplus k_{r \bmod \kappa})$$

k_j is involved in the trail if $\bigoplus_{r \in \mathcal{J}} \mathcal{X}_0^r = 1$, $\mathcal{J} = \{r \mid j = r \bmod k\}$

Correlation Evaluation of Linear Trail

$$f(x_0, \ldots, x_n) = x_0 \& x_1 \oplus x_1 \& x_2 \oplus \cdots \oplus x_{n-1} \& x_n \oplus a_0 x_0 \oplus \cdots \oplus a_n x_n$$

Absolute Correlation [Song et al.]

1. n Odd: $|\mathrm{Cor}(f)| = 2^{-(n+1)/2}$.
2. n Even: $|\mathrm{Cor}(f)| = 2^{-n/2}$ if $\bigoplus_{j=0}^{n/2} a_{2j} = 0$; otherwise, $|\mathrm{Cor}(f)| = 0$.

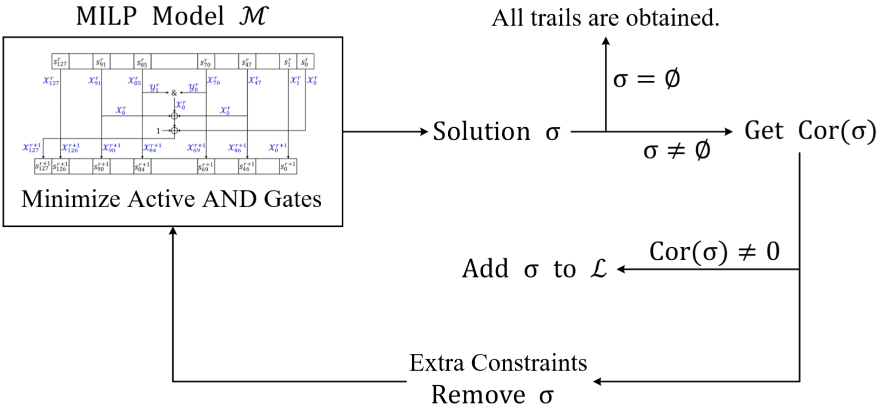
$$\mathrm{Sign}(f) = \prod_{i=0}^{t-1} (-1)^{\left(\bigoplus_{j=0}^{i} a_{2j}\right) a_{2i+1}}, t = \begin{cases} \frac{n+1}{2}, & n \text{ Odd} \\ \frac{n}{2}, & n \text{ Even and } \bigoplus_{j=0}^{t} a_{2j} = 0 \end{cases}$$

Key Bits Involved

$$\lambda_0 \cdot T_0 \oplus \lambda_1 \cdot T_1 \approx \bigoplus_{r=0}^{R-1} \mathcal{X}_0^r (1 \oplus k_{r \bmod \kappa})$$

k_j is involved in the trail if $\bigoplus_{r \in \mathcal{J}} \mathcal{X}_0^r = 1$, $\mathcal{J} = \{r \mid j = r \bmod k\}$

Searching All Linear Tails in a Given Hull for TinyJAMBU



Linear Hull used in Attacking V1

384-Round Linear Hull ($\lambda_0 = \texttt{0x8024C000}, \lambda_1 = \texttt{0x00220808}$):

Cor.	$+2^{-42}$	$+2^{-43}$	$+2^{-44}$	$+2^{-45}$	$+2^{-46}$	$+2^{-47}$	$+2^{-48}$
Trail	1	10	39	92	120	81	82
Cor.	-2^{-42}	-2^{-43}	-2^{-44}	-2^{-45}	-2^{-46}	-2^{-47}	-2^{-48}
Trail	2	11	36	93	117	82	84

850 trails are composed in this hull.

Key Recovery Attacks on Full V1 (Threshold-Based)

Setting	Type	N	Users	Key Info. Rec.	$Pr_{success}$	$\kappa = 128$	$\kappa \in \{192, 256\}$
Direct Attack	weak-key multi-user	$2^{96.8}$	2^{50}	7.639	$82.35\,\%$		✓
	single-user	$2^{96.8}$	1	7.639	$82.35\,\%$	✓	✓
Basic RK	weak-key multi-user	$2^{97.1}$	2^{50}	8.033	$86.16\,\%$		✓
	single-user	$2^{97.1}$	1	8.033	$86.16\,\%$	✓	✓
Multiple RK	weak-key multi-user	$2^{102.31}$	2^{56}	14.063	$84.85\,\%$		✓
	single-user	$2^{102.31}$	1	14.063	$84.85\,\%$	✓	✓

Data limits: the number of tags collected per key should $\leq 2^{47}$.

Weak-key multi-user: each user has their own key but with some bits in common.

Outline

Conclusion and Future Work

Conclusion: New Statistical Models

Absolute Error $\max|\mathrm{P}_e^{\text{theory}} - \mathrm{P}_e^{\text{expr.}}|$:

- Threshold-based: 2.19% & MLE-based: 1.9%
- Röck and Nyberg: 93.45%

Improvements on accuracy are due to our new methodology.

Conclusion: Cryptanalysis of TinyJAMBU

- Full v1 & Round-Reduced v2

Partial key bits are recovered in the nonce-respecting setting.

Future Work

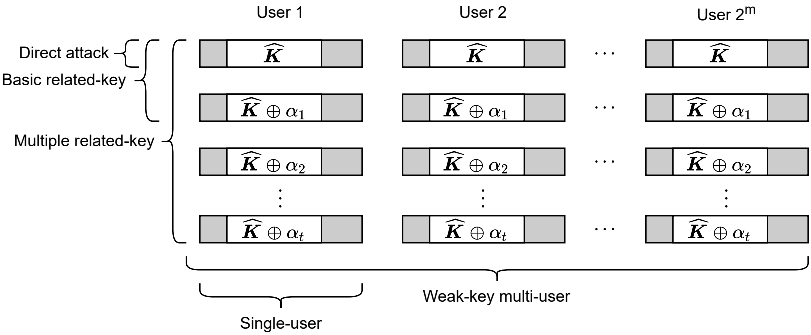
- Further applications of our models
- Investigate whether different masks can recover more key bits

Thanks for Your Attention!

Any Questions?

Backup Slides

Attack Settings



Security margin of TinyJAMBU in the multi-user setting will drop from 2^{d} to $2^{\mathrm{d}-\mathrm{m}}$ when 2^{m} different values of keys are used.