Security Analysis of KNOT-AEAD and KNOT-Hash

Wentao Zhang, Tianyou Ding, Chunning Zhou, Fulei Ji

Institute of Information Engineering, Chinese Academy of Sciences

{zhangwentao, dingtianyou, zhouchunning, jifulei}@iie.ac.cn

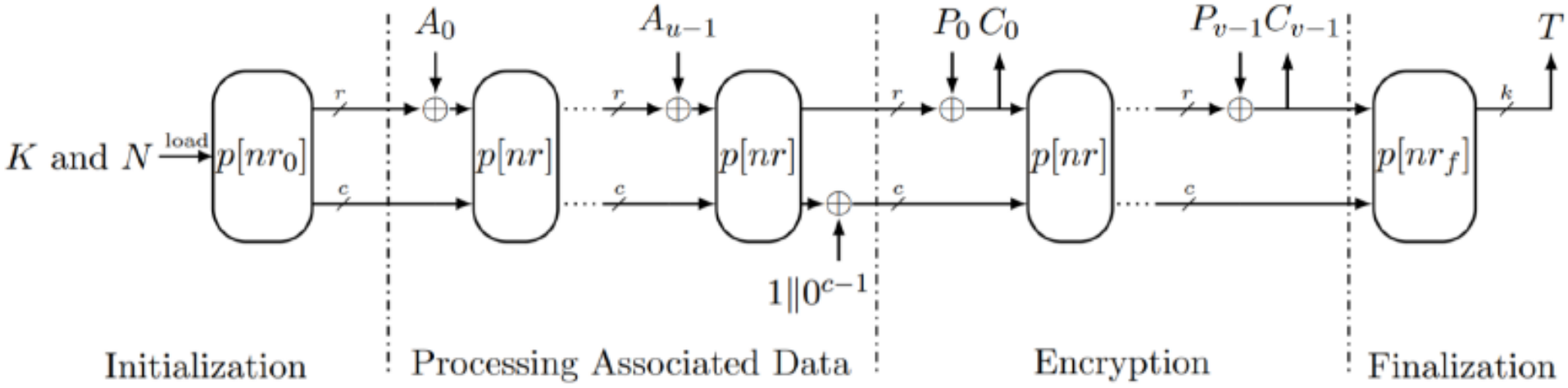
Outline

1. The KNOT Family
2. Motivation
3. Our New Method
4. Attack Models
5. Experimental Results for KNOT
6. Validity of Our New Method
7. Summary and Discussion

1.The KNOT Family

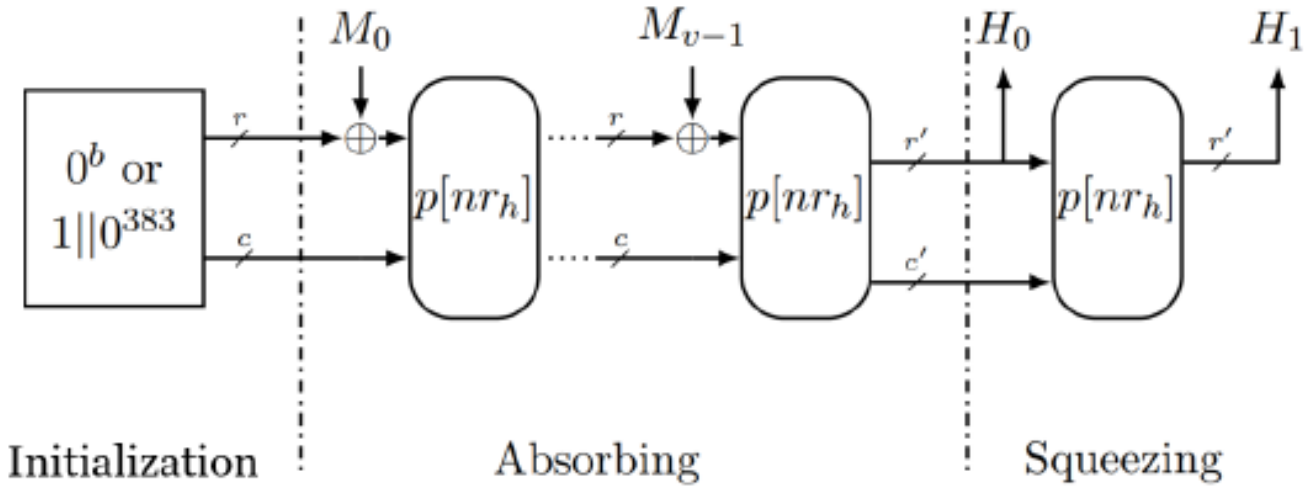
- KNOT is a family of bit-slice lightweight AEAD and hashing algorithms:
  - **KNOT-AEAD**
  - **KNOT-Hash**

- KNOT uses permutation-based modes.



Encryption of KNOT-AEAD

- KNOT-AEAD: **MonkeyDuplex,** with a reduced number of rounds in the data processing and finalization phases



KNOT-Hash

- KNOT-Hash: **an extended Sponge**, with a different bit rate in the squeezing phase

- **KNOT-AEAD has 4 members**. They are different in state size, bit rate and key size.

- Accordingly, **KNOT-Hash also has 4 members.**

- For **each KNOT-pair**, the corresponding KNOT-AEAD and KNOT-Hash have **the same state size** and use **an identical round transformation**:
  - the primary pair, 256-bit state

The KNOT permutations

- **State width b**: 256/384/512 bits

$$\begin{bmatrix} a_{0,\frac{b}{4}-1} & \cdots & a_{0,1} & a_{0,0} \\ a_{1,\frac{b}{4}-1} & \cdots & a_{1,1} & a_{1,0} \\ a_{2,\frac{b}{4}-1} & \cdots & a_{2,1} & a_{2,0} \\ a_{3,\frac{b}{4}-1} & \cdots & a_{3,1} & a_{3,0} \end{bmatrix}$$

A b-bit state

The KNOT permutations

- **Structure:** SP-network, each of the rounds has 3 steps

$$
\begin{aligned}
\{ \quad & AddRoundConstant_b(STATE, RC) \\
& SubColumn_b(STATE) \\
& ShiftRow_b(STATE) \\
\}
\end{aligned}
$$

where RC denotes a round constant.

SubColumn: parallel application of sboxes to the 4 bits in the same column, $S : \mathrm{F}_2{}^4 \longrightarrow \mathrm{F}_2{}^4$

$$\begin{pmatrix} a_{0,\frac{b}{4}-1} \\ a_{1,\frac{b}{4}-1} \\ a_{2,\frac{b}{4}-1} \\ a_{3,\frac{b}{4}-1} \end{pmatrix} \cdots \begin{pmatrix} a_{0,1} \\ a_{1,1} \\ a_{2,1} \\ a_{3,1} \end{pmatrix} \begin{pmatrix} a_{0,0} \\ a_{1,0} \\ a_{2,0} \\ a_{3,0} \end{pmatrix}$$

$$\downarrow S \qquad \cdots \qquad \downarrow S \qquad \downarrow S$$

$$\begin{pmatrix} b_{0,\frac{b}{4}-1} \\ b_{1,\frac{b}{4}-1} \\ b_{2,\frac{b}{4}-1} \\ b_{3,\frac{b}{4}-1} \end{pmatrix} \cdots \begin{pmatrix} b_{0,1} \\ b_{1,1} \\ b_{2,1} \\ b_{3,1} \end{pmatrix} \begin{pmatrix} b_{0,0} \\ b_{1,0} \\ b_{2,0} \\ b_{3,0} \end{pmatrix}$$

ShiftRow: a left rotation to each row over different offsets

$$
\begin{aligned}
&\left(a_{0,\frac{b}{4}-1} \quad \cdots \quad a_{0,1} \quad a_{0,0}\right) \xrightarrow{\lll 0} \left(a_{0,\frac{b}{4}-1} \quad \cdots \quad a_{0,1} \quad a_{0,0}\right) \\
&\left(a_{1,\frac{b}{4}-1} \quad \cdots \quad a_{1,1} \quad a_{1,0}\right) \xrightarrow{\lll c_1} \left(a_{1,\frac{b}{4}-c_1-1} \quad \cdots \quad a_{1,\frac{b}{4}-c_1+1} \quad a_{1,\frac{b}{4}-c_1}\right) \\
&\left(a_{2,\frac{b}{4}-1} \quad \cdots \quad a_{2,1} \quad a_{2,0}\right) \xrightarrow{\lll c_2} \left(a_{2,\frac{b}{4}-c_2-1} \quad \cdots \quad a_{2,\frac{b}{4}-c_2+1} \quad a_{2,\frac{b}{4}-c_2}\right) \\
&\left(a_{3,\frac{b}{4}-1} \quad \cdots \quad a_{3,1} \quad a_{3,0}\right) \xrightarrow{\lll c_3} \left(a_{3,\frac{b}{4}-c_3-1} \quad \cdots \quad a_{3,\frac{b}{4}-c_3+1} \quad a_{3,\frac{b}{4}-c_3}\right)
\end{aligned}
$$

2. Motivation

- In the KNOT design document, the **designers evaluated in detail the security of the underlying permutations** against various cryptanalytic approaches:
  - among which DC and LC are the most powerful approaches

- Although **distinguishers of the permutations** can give insights in the resistance of the AEAD and hash primitives against various cryptanalytic attacks, they **usually can not be directly used in an attack.**

- To have a better understanding of the security of KNOT, we furthermore study **the best differential/linear distinguishers with constraints**, which can be **directly used to mount attacks on KNOT-AEAD and KNOT-Hash**.

- The evaluation of the KNOT permutations against DC and LC is achieved by using **Matsui's search algorithm and its improvements**. However, **when constraints are added, the efficiency is not satisfied,** e.g., the 256-bit KNOT permutation, the best linear trail:
  - constraints: all active bits of both the input and output mask are only allowed in the rate part.
  - search time: 98 hours for 11 rounds; additional 49 hours for 12 rounds.

- The design of the KNOT permutations inherits the design of RECTANGLE.

- **An observation on RECTANGLE** is that **the best long-round differential and linear trail always contains iterative sub-trails**, which motivates us to study differential/linear distinguishers containing iterative sub-trails for KNOT.

3. Our Method

- Main idea:
  1). By using the algorithm of finding elementary circuits (a circuit is elementary if no vertex but the first and last appears twice), we can **find all elementary iterative differential/linear trails** for each of the KNOT permutations.
  2). Then, by checking all the differential/linear iterative trails within the scope of consideration and **connecting them repeatedly**, we can efficiently derive the difference/linear propagations for a given number of rounds and given input/output difference (or input/output mask).
  3). Finally, by using Matsui's search algorithm, we can **extend** the difference (or linear) propagations obtained in the previous step **both forward and backward** for several rounds.

- The **accuracy of our calculation** on differential probability (linear correlation) is closely related with **the number of trails collected:**
  - The more trails we collect, the more accurate the estimation is, yet the more time and memory the program costs.
  - In our experiments **for each KNOT member**, we try to make an **appropriate tradeoff between the accuracy and efficiency.**

- For more details, please refer to our paper:

  Ding Tianyou, Zhang Wentao, Ji Fulei, Zhou Chunning: *An Automatic Search Tool for Iterative Trails and its Application to KNOT, PRESENT, GIFT-64 and RECTANGLE*, https://eprint.iacr.org/2020/1152.

4.Attack Models

- KNOT-AEAD: 6 attack models
- KNOT-Hash: 2 attack models

6 attack models for KNOT-AEAD

Note: all the attacks are in the nonce-respecting setting; for forgery attacks , nonce can be reused in decryption oracle.

	Target phase	Distinguisher Type	Constraints	Attack Goal
Diff-Init-D	Initialization	truncated difference propagation	**input difference:** active bits only allowed in nonce part **output difference**: the rate part is some fixed value	distinguishing
Linear-Ini-KR		linear propagation	**input mask**: the key part is active **output mask**: active bits only allowed in rate part	key recovery
Linear-Ini-D		linear propagation	**input mask**: the key part is zero **output mask:** active bits only allowed in rate part	distinguishing
Diff-Enc-F	Encryption	difference propagation	**both input and output difference**: active bits only allowed in rate part	forgery
Linear-Enc-D		linear propagation	**both input and output mask**: active bits only allowed in rate part	distinguishing
Diff-Final-F	Finalization	truncated difference propagation	**input difference**: active bits only allowed in rate part **output difference**: the tag part is some fixed value	Forgery

2 attack models for KNOT-Hash

	Distinguisher Type	Constraints	Attack Goal
Diff-Col-I	difference propagation	**both input and output difference**: active bits only allowed in rate part	collsion
Diff-Col-II	truncated difference Propagation	**input difference**: active bits only allowed in rate part **output difference**: the hash-value part is zero	near collision

5.Experimental Results for KNOT

- According to the claimed security strength and data limit of KNOT, we study:
  - the security margin of **each KNOT-AEAD** member **against the 6 attack models** in the **single-key scenario**
  - the security margin of **each KNOT-Hash** member against **the 2 attack models**.

	Plaintext Confidentiality	Ciphertext Integrity	Data Limit
KNOT-AEAD(128, 256, 64)	125	125	2^{64}
KNOT-AEAD(128, 384, 192)	128	128	2^{64}
KNOT-AEAD(192, 384, 96)	189	189	2^{96}
KNOT-AEAD(256, 512, 128)	253	253	2^{128}

KNOT-AEAD: claimed security strength and data limit

Name	Security (bit)			Data limit
	pre.	2nd pre.	col.	
KNOT-Hash(256, 256, 32, 128)	128	112	112	2^{64}
KNOT-Hash(256, 384, 128, 128)	128	128	128	2^{64}
KNOT-Hash(384, 384, 48, 192)	192	168	168	2^{96}
KNOT-Hash(512, 512, 64, 256)	256	224	224	2^{128}

KNOT-Hash: claimed security strength and data limit

- **data complexity** of a **differential/linear attack**:
  - For a difference propagation, *P*: the **probability**, $-\log_2 p$: **weight.**
    The **data complexity** is proportional to p^{-1}
  - For a linear propagation, *cor*: the **correlation,** $-\log_2 cor$: **weight.**
    The **data complexity** is proportional to cor^{-2}.

- The following 5 tables present our experimental results for KNOT:
  - **the numbers in red color** denote **the highest weight of an effective distinguisher** considering **the data limit**, and the corresponding number of rounds is **the highest number of rounds of an effective distinguisher**

KNOT-AEAD v1 (primary version): weights of the best r-round distinguisher

r	Diff-Init-D	Linear-Init-KR	Linear-Init-D	Diff-Enc-F	Linear-Enc-D	Diff-Final-F
10	43	25	26	52.4	27	47.1
11	47.9	28	28	57.4	30	51.8
12	52.6	30	31	62.4	32	56.6
13	57.4	33	33	67.7	35	61.4
14	62.2	35	36	72.4	37	66.2
15	67	38	38	77.1	40	71.0

- For the primary version of KNOT-AEAD, **the highest number of rounds** of an effective distinguisher are **14, 12, and 13 rounds** respectively for the **initialization, encryption** and **finalization phase** :
  - note that the full number of rounds are 52 , 28 and 32 rounds respectively, the highest number of rounds of an effective distinguisher is less than 43% of the full number of rounds.

KNOT-AEAD v2: weights of the best r-round distinguisher

r	Diff-Init-D	Linear-Init-KR	Linear-Init-D	Diff-Enc-F	Linear-Enc-D	Diff-Final-F
10	46.4	25	26	51.4	25.4	44.0
11	51.2	28	29	56.7	28	48.6
12	56	30	31	61.4	30.4	53.2
13	60.8	33	34	66.1	33	57.9
14	65.6	35	36	71.1	35.4	62.6
15	70.4	38	39	76.1	38	67.4

KNOT-AEAD v3: weights of the best r-round distinguisher

r	Diff-Init-D	Linear-Init-KR	Linear-Init-D	Diff-Enc-F	Linear-Enc-D	Diff-Final-F
10	43	25	26	52.4	27	47.1
11	47.9	28	28	57.4	30	51.8
12	52.6	30	31	62.4	32	56.6
13	57.4	33	33	67.7	35	61.4
14	62.2	35	36	72.4	37	66.2
15	67	38	38	77.1	40	71.0
16	71.8	40	41	82.1	42	75.8
17	76.6	43	43	87.1	45	80.6
18	81.4	45	46	92.1	47	85.4
19	86.2	48	48	96.8	50	90.1
20	91	50	51	101.5	52	94.9
21	95.8	53	53	106.5	55	99.7
22	100.5	55	56	111.5	57	104.5

KNOT-AEAD v4: weights of the best r-round distinguisher

r	Diff-Init-D	Linear-Init-KR	Linear-Init-D	Diff-Enc-F	Linear-Enc-D	Diff-Final-F
10	43	25	26	52.4	27	47.1
11	47.9	28	28	57.4	30	51.8
12	52.6	30	31	62.4	32	56.6
13	57.4	33	33	67.7	35	61.4
14	62.2	35	36	72.4	37	66.2
15	67	38	38	77.1	40	71.0
16	71.8	40	41	82.1	42	75.8
17	76.6	43	43	87.1	45	80.6
18	81.4	45	46	92.1	47	85.4
19	86.2	48	48	96.8	50	90.1
20	91	50	51	101.5	52	94.9
21	95.8	53	53	106.5	55	99.7
22	100.6	55	56	111.5	57	104.5
23	105.3	58	58	116.3	60	109.3
24	110.1	60	61	121.1	62	114.1
25	114.9	63	63	125.9	65	118.9
26	119.7	65	66	130.9	67	123.7
27	124.5	68	68	135.8	70	128.5
28	129.3	70	71	140.5	72	133.3

KNOT hash: weights of the best r-round distinguisher

	KNOT-Hash v1		KNOT-Hash v2		KNOT-Hash v3		KNOT-Hash v4	
r	Diff-Col-I	Diff-Col-II	Diff-Col-I	Diff-Col-II	Diff-Col-I	Diff-Col-II	Diff-Col-I	Diff-Col-II
10	53.7	47.1	51.4	44.1	54.0	47.1	53.7	47.1
11	59.4	51.8	56.7	48.7	57.4	51.8	57.4	51.8
12	62.7	56.6	61.4	53.4	62.4	56.6	62.4	56.6
13	67.7	61.4	66.1	58.1	67.8	61.4	67.7	61.4
14	72.7	66.2	71.1	62.8	72.4	66.2	72.4	66.2
15	-	-	76.1	67.5	77.4	71.0	77.1	71.0
16	-	-	-	-	82.7	75.8	82.1	75.8
17	-	-	-	-	88.7	80.6	87.1	80.6
18	-	-	-	-	95.2	85.4	92.1	85.4
19	-	-	-	-	100.8	90.1	96.8	90.1
20	-	-	-	-	106.5	94.9	101.5	94.9
21	-	-	-	-	112.2	99.7	106.5	99.7
22	-	-	-	-	-	-	111.5	104.5
23	-	-	-	-	-	-	116.3	109.3
24	-	-	-	-	-	-	121.1	114.1
25	-	-	-	-	-	-	126.1	118.9
26	-	-	-	-	-	-	131.2	123.7
27	-	-	-	-	-	-	136.2	128.5

To sum up

- The **security margin** of **KNOT-AEAD** against **the 6 attack models**:
  - for all the 4 members, the highest number of rounds of an effective distinguisher is less than 50% of the full number of rounds, which means a **50% security margin**; especially, for **initialization phase**, the security margin **is higher than 72%.**

- The **security margin** of **KNOT-Hash** against **the 2 attack models**:
  - for all the 4 members, the highest number of rounds of an effective distinguisher is less than 20% of the full number of rounds, which means a **80% security margin**.

6.Validity of Our New Method

- we investigate **the accuracy of our new method** in **two different ways**:
  - Firstly, we apply our new method to RECTANGLE, which is an ancestor of the KNOT permutations, and **compare the results obtained by our new method with those in the specification document of RECTANGLE**.
  - Secondly, **we use MILP method** to compute the **differential and linear clustering effect** of the **256-bit KNOT permutation** and **compare the results** obtained by MILP method with those obtained by our new method.

- **Differential clustering of 14-round RECTANGLE:**
  - The designers of RECTANGLE claim that: *" For 14-round RECTANGLE, the probability of the best differential trail is 2^{-61} . We have searched for all 14-round differential trails with probability between 2^{-61} and 2^{-71}, and examined all the difference propagations made up of these investigated trails."* Then they present a 14-round difference propagation with probability $2^{-60.66}$.
  - Fixing the input and output difference and **applying our method**, we obtain **the same probability $2^{-60.66}$**.

- **Linear clustering of 14-round RECTANGLE:**
  - The designers of RECTANGLE claim that: **"For 14-round RECTANGLE, we have searched for all the linear trails with a correlation (absolute value) between 2^{-34} and 2^{-37} and examined all the linear propagations made up of the investigated trails."** Then they present a linear propagation with correlation $2^{-31.61}$.
  - Fixing the input and output mask and **applying our method**, we obtain a correlation $2^{-32.32}$, which is very close to the designers' result $2^{-31.61}$.

- **10-round difference propagation of 256-bit KNOT permutation:**
  - for Diff-Col-I type distinguishers, a 10-round difference propagation is given by

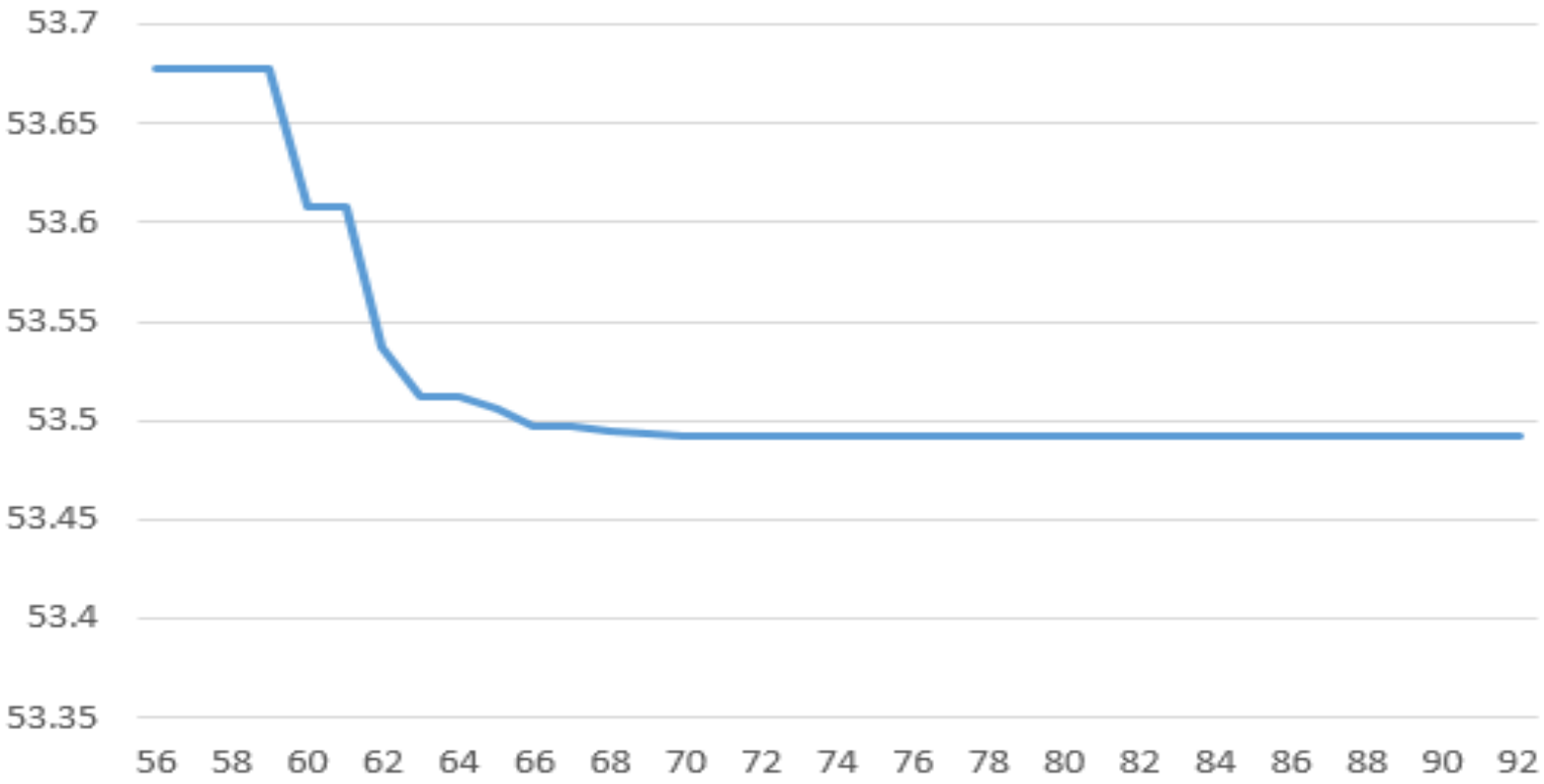
0000000000000000000000000000100000000000000010000000000000

↓

0000000000000000000000000000100000000000000000000000000001

with probability $2^{-53.7}$.

  - Fixing the input and output difference and **using MILP method**, we have searched for all the differential trails with probability between 2^{-56} and 2^{-92}, and get **a total probability $2^{-53.5}$**.



For the 10-round difference propagation, y = f(x) is the accumulated weight by considering all the differential trails with weight less than or equal to x.

- **10-round linear propagation of the 256-bit KNOT permutation:**
  - for Linear-Enc-D type distinguisher, a 10-round linear propagation is given by

1000000000000000000000010000000000000000000000000000000000000000

↓

0000000000000000000000010000000000000000100000000000000000000000

with correlation amplitude 2^{-27}.

  - Fixing the input and output mask and **using MILP method**, we have searched for all the linear trails with probability between 2^{-30} and 2^{-40}, and get **a correlation amplitude $2^{-25.4}$**.

- we use an **11-round linear propagation** (Linear-Enc-D type) for further verification

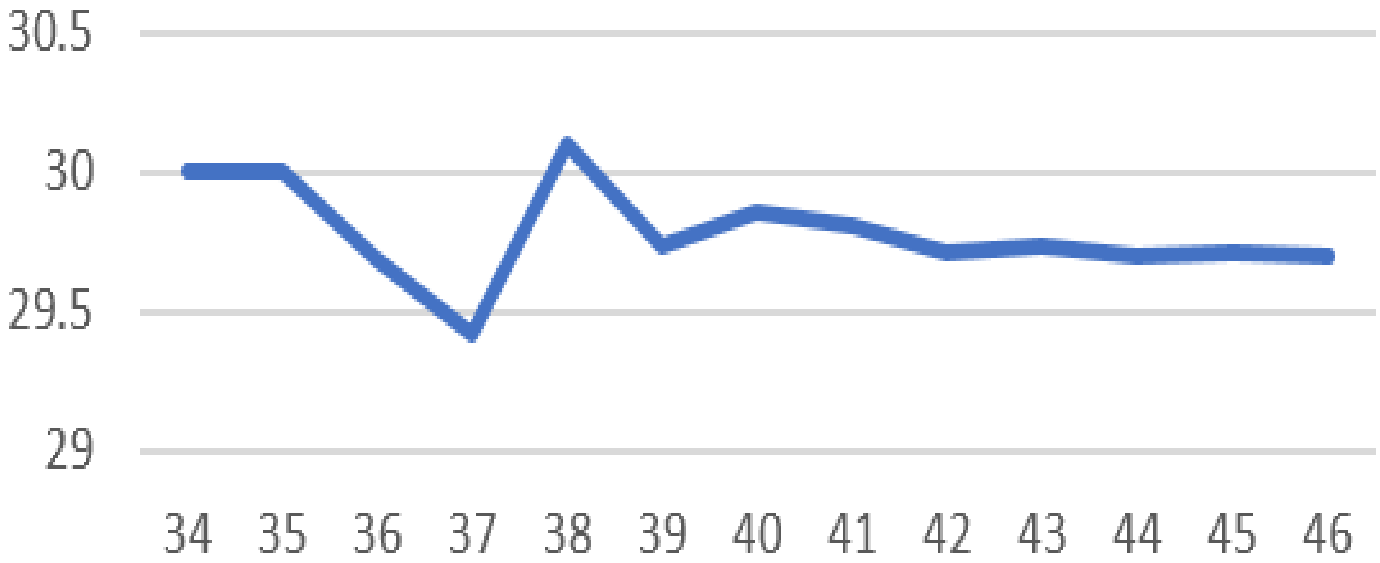
  1000000000000000000000010000000000000000000000000000000000

  ↓

  0000000000000000000000010000000000000010000000000000000000

  with correlation amplitude 2^{-30} using our method.

  - Fixing the input and output mask and **using MILP method**, we have searched for all the linear trails with a probability between 2^{-34} and 2^{-46}, and get **a correlation amplitude $2^{-29.7}$**, which is very close to the value 2^{-30}.



For the 11-round linear propagation, $y = f(x)$ is the accumulated weight by considering all the linear trails with weight less than or equal to x.

7.Summary and Discussion

- By studying **the class of differential/linear trails which contain iterative sub-trails**, we have **efficiently obtained effective differential/linear distinguishers** for each KNOT-AEAD member w.r.t. 6 attack models and for each KNOT-Hash member w.r.t. 2 attack models.

- Furthermore, we investigated the accuracy of our new method in two different ways. Based on these comparative results, we can reasonably infer that the results using our new approach provide **a quite accurate security evaluation** of KNOT-AEAD and KNOT-Hash:
  - **each KNOT-AEAD member** has **at least 50% security margin** against the 6 attack models. Especially, **72% security margin of the initialization phase**, *possibility of reducing the number of rounds in initialization phase.*
  - **each KNOT-Hash member** has **at least 80% security margin** against the 2 attack models, *possibility of reducing the number of rounds.*

- Security decreases in a multi-key scenario:
  - If taking multi-key attacks into account, the number of rounds of KNOT need to be increased.

- However, in practice, the data limit 2^{64} is sufficient for lightweight applications.

Thanks for your attention!

Questions?