Improved Linear Key Recovery Attacks on PRESENT

Wenhui Wu[1,3], Muzhou Li[1,3,✉] and Meiqin Wang[1,2,3]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, China
[2] Quan Cheng Shandong Laboratory, Jinan, China
[3] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China
wenhuiwu@mail.sdu.edu.cn, muzhouli@mail.sdu.edu.cn, mqwang@sdu.edu.cn

Abstract. PRESENT is an ultra-lightweight block cipher designed by Bogdanov *et al.*, and has been widely studied since its proposal. It supports 80-bit and 128-bit keys, which are referred as PRESENT-80 and PRESENT-128, respectively. Up to now, linear cryptanalysis is the most effective method on attacking this cipher, especially when accelerated with the pruned Walsh transform. Combing pruned Walsh transform with multiple linear attacks, one can recover the right key for 28-round PRESENT-80 and -128. Later, this method is further improved with affine pruned Walsh transform by adding more zeros in the Walsh spectrum through rejecting some data. This leads to the 29-round attack on PRESENT-128 with full codebook.

In this paper, we follow the affine pruned Walsh transform accelerated linear method, and propose 29-round attacks on both PRESENT-80 and PRESENT-128 without using full codebook. Both attacks rely on a statistical model depicting distributions of the experimental correlation when some data are artificially rejected in its computation. Besides, detailed analysis of complexity reduction for each linear hull used in attacking PRESENT is also provided and supported by an automatic tool. Our 29-round attack on PRESENT-80 mainly benefits from this tool. According to our knowledge, both attacks are the best ones on PRESENT so far.

Keywords: PRESENT · Affine Pruned Walsh Transform · Linear Cryptanalysis

1 Introduction

Lightweight cryptography is a widely discussed topic in recent years, especially its design and cryptanalytic results. PRESENT [BKL+07] is one of the typical lightweight ciphers announced by Bogdanov *et al.* in CHES'07, and has been an ISO standard since 2012. This cipher operates on the 64-bit state with the 80-bit or 128-bit master key, which are named as PRESENT-80 and PRESENT-128, respectively. Both variants adopt the same round function that is based on the substitution-permutation network. Given the 64-bit plaintext, they proceed 31 times of the round function and then the last whitening key is XORed with the state before outputs the ciphertext.

Since its proposal, many cryptanalytic results have been provided, such as integral attack [ZRHD08], differential attacks [Wan08, AC09, ÖVTK09], statistical saturation [CS09], and various variants of linear attacks [Ohk09, JSZW09, Cho10, ZZ15, BTV18, FN20, Fló22]. Among all of them, the most effective attacks are given by variants of linear cryptanalysis, especially those using (affine) pruned Walsh transform accelerated [FN20, Fló22].

Linear cryptanalysis [Mat93] was proposed by Matsui in EUROCRYPT'93, and has become one of the most important methods in designing and analysing ciphers. It exploits a linear approximation connecting some plaintext and ciphertext bits, as well as key bits. Matsui proposed two types of key recovery attacks based on this linear approximation, which are named as Matsui's Algorithm 1 and Matsui's Algorithm 2 in the literature. In Matsui's Algorithm 1, one can deduce 1-bit key after gathering enough plaintext-ciphertext pairs. When using Matsui's Algorithm 2, one will put the linear approximation in the middle part of the target (round-reduced) cipher, and try to recover key bits involved in rounds in both sides. Statistical behavior of this method is accurately constructed by Blondeau and Nyberg [BN17].

Multiple linear cryptanalysis is a variant of linear attacks, which was firstly proposed by Kaliski and Robshaw [JR94], and then extended by Biryukov *et al.* [BCQ04]. In this variant, one will adopt multiple independent linear approximations and can gain lower data complexities. Its statistical behavior is also refined in [BN17]. Meanwhile, there also exist other type of linear attacks that use multiple approximations, such as the multidimensional linear attack [BJV04, HCN08, HCN09, HVLN15] and multivariate linear attack [BTV18].

The idea of using Walsh transform to accelerate linear key recovery attacks was provided by Collard *et al.* [CSQ07], where only the last-round key can be recovered efficiently with fast Walsh transform (FWT). In EUROCRYPT'20, Flórez-Gutiérrez *et al.* [FN20] provided a framework to deal with the general case when key recovery is considered on both the plaintext and ciphertext sides. In their framework, the experimental correlation is evaluated step-by-step, and thus can be accelerated in many steps with FWT. Meanwhile, they also used the pruned Walsh transform whenever possible, which avoid wasting time costs to some extent. With this framework, they proposed 28-round key recovery attacks on both PRESENT-80 and PRESENT-128 with multiple independent approximations. Later, in ASIACRYPT'22, Flórez-Gutiérrez [Fló22] introduced the affine pruned Walsh transform technique, which further improves this framework. When evaluating the experimental correlation for some linear hulls, more zeros are added in the Walsh spectrum through rejecting some data, thus leading to reduced time complexity. With this improved framework, 29-round attack on PRESENT-128 using full codebook is proposed. However, it's unclear how the success probability of this attack is estimated. From [Fló22], we only found one sentence: "the statistical model from [BN17] is used with careful consideration that the number of available plaintexts depends on the approximation". Taking the number of remaining data into consideration will change the form of the statistic constructed in [BN17]. In other words, previous model cannot be directly used. Meanwhile, whether this improved framework can lead to 29-round key recovery attack on PRESENT-80 is uncertain. Hence, we are motivated to check if we can gain better key recovery attacks on these two ciphers with the affine pruned Walsh transform technique, and provide a better understanding of the statistical behavior behind this new technique. Our contributions are listed as follows.

Statistical Behavior behind the Affine Pruned Walsh Transform Technique. In this new method, some data are rejected during the evaluation of the experimental correlation, with the aim of reducing its time costs. However, such artificially filtering of data will lead to deviation from expected distributions given in [BN17]. Similar questions also exist when multiple independent linear hulls are used. In Sect. 3, we introduce the statistical behavior behind this new technique, where distributions of the experimental correlation when some data are rejected during its evaluation are provided. Based on the statistical behavior for a single linear hull, we also construct a statistical model to deal with the case when multiple independent hulls are utilized. All our statistical models are proposed under strictly proofs and have been experimentally verified using `SmallPRESENT-[4]`. Such newly constructed models provide the accurate relation between success probability and data complexity for the improved framework proposed by [Fló22].

Non Full-Codebook Key Recovery Attack on 29-Round PRESENT-128. Following the affine pruned Walsh transform framework, we introduce the improved 29-round multiple linear attack on PRESENT-128 in Sect. 4. We adopt the same linear hulls used in [Fló22] but with more detailed analysis of complexity reduction for each linear hull. Such analysis is efficiently proceeded by an automatic tool we constructed. Meanwhile, benefiting from our statistical models, this attack can be mounted without adopting the full-codebook.

First Key Recovery Attack on 29-Round PRESENT-80. In Sect. 5, we adopt a similar key recovery process as used in attacking 29-round PRESENT-128. However, we subtly choose some 24-round linear hulls from those given by [FN20]. A linear hull is included only if it can enlarge the distance between variances of right and wrong key guesses, and in the same time, the extra time complexity caused by this hull cannot increase the final complexity too fast. Such trade-offs can be effectively found using our constructed automatic tool, which provides detailed analysis of complexity reduction for each hull.

Comparison between our attacks and previous linear-like attacks is depicted in Table 1.

Table 1: Comparison of linear attacks on round-reduced PRESENT. KP denotes the known-plaintext setting, while DKP is the distinct known-plaintext setting. Time complexities are evaluated in encryption units, and memory costs are evaluated in memory registers.

Key	Rds.	Non Full		Complexity		Success	Ref.
		Codebook	Data	Time	Memory	Pr.	
128	28†		$2^{64.0}$ DKP	2^{122}	$2^{84.6}$	95%	[FN20]
	29		$2^{64.0}$ DKP	$2^{124.06}$	$2^{99.2}$	40.11%‡	[Fló22]
		✓	**$2^{62.88}$ DKP**	**$2^{126.33}$**	**$2^{97.91}$**	**62.83%**	**Sect. 4**
80	26	✓	$2^{63.8}$ KP	$2^{72.0}$	$2^{32.0}$	51%	[BN16, Cho10]
		✓	$2^{63.0}$ KP	$2^{68.6}$	$2^{48.0}$	95%	[BTV18]
		✓	$2^{61.1}$ KP	$2^{68.2}$	$2^{44.0}$	95%	[FN20]
		✓	$2^{60.8}$ KP	$2^{71.8}$	$2^{44.0}$	95%	[FN20]
	27		$2^{64.0}$ KP	$2^{74.0}$	$2^{67.0}$	95%	[ZZ15]
		✓	$2^{63.8}$ DKP	$2^{77.3}$	$2^{48.0}$	95%	[BTV18]
		✓	$2^{63.4}$ DKP	$2^{72.0}$	$2^{44.0}$	95%	[FN20]
	28†		$2^{64.0}$ DKP	$2^{77.4}$	$2^{51.0}$	95%	[FN20]
	29	✓	**$2^{63.93}$ DKP**	**$2^{78.87}$**	**2^{71}**	**51.23%**	**Sect. 5**

†Trade-offs between data and time complexities can be made in these two attacks [FN20].

‡Success probability is re-evaluated with our statistical model constructed in Sect. 3, since previous estimation in [Fló22] is not accurate as shown in Appendix D.

2 Preliminaries

2.1 Brief Introduction of PRESENT

PRESENT [BKL+07] is an ultra-lightweight block cipher proposed by Bogdanov *et al.*. It adopts the substitution-permutation network with 64-bit block length. Its key length can be 80 and 128 bits, which are often referred as PRESENT-80 and PRESENT-128 in the literature, respectively.

Both variants of PRESENT iterates the same round function 31 times, and then a whitening key is XORed to the state at the end. Round function of PRESENT is composed of three consecutive operations: `addRoundKey`, `sBoxLayer` and `pLayer`. Denote the i-th rightmost bit of X starting from 0 as $X[i]$. In `addRoundKey`, a 64-bit round key K_i is XORed to the 64-bit state. The `sBoxLayer` consists of 16 parallel 4-bit Sboxes $S(x)$, which is shown in Table 2. `pLayer` is a bit-wise permutation that moves the j-th bit to the $P(j)$-th bit, where $P(j) = 16j \mod 63$ for $j \neq 63$, and $P(63) = 63$. Given the 80-bit or 128-bit master key K, one can generate all K_i as well as the last whitening key with key schedules depicted in Algorithm 1 and 2 given in Appendix A.

Table 2: 4-bit Sbox used in PRESENT (in hex form).

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

2.2 (Affine) Pruned Walsh Transform Accelerated Linear Attacks

Linear Cryptanalysis. This method was originally proposed by Matsui [Mat93], where a linear approximation is utilized to distinguish between the right and wrong key guesses. To mount key recovery attacks, Matsui gave two different algorithms. Matsui's Algorithm 1 directly use this linear approximation and can deduce 1-bit key information after obtaining enough plaintext-ciphertext pairs $(\tilde{x}, \tilde{y})$. While in Matsui's Algorithm 2, the linear approximation is placed in the middle of the block cipher. Denote E_K as the target cipher with block length n, which is divided into three parts $E_2 \circ E'_K \circ E_1$. E'_K is the part covered by the linear approximation, while E_1 and E_2 are rounds covered in the key recovery process. Let $\hat{x} = E_1(\tilde{x})$ and $\hat{y} = E_2^{-1}(\tilde{y})$. The linear approximation can then be represented as $\langle u, \hat{x}\rangle \oplus \langle v, \hat{y}\rangle = 0$, where $\langle u, \hat{x}\rangle$ denotes the inner product of u and $\hat{x}$. The mask pair (u, v) is also referred as the linear hull in the literature. Given N plaintext-ciphertext pairs $(\tilde{x}, \tilde{y})$, one computes the experimental correlation

$$\widehat{cor} = \frac{1}{N} \sum_{(\tilde{x},\tilde{y})} (-1)^{\langle u, E_1(\tilde{x})\rangle \oplus \left\langle v, E_2^{-1}(\tilde{y})\right\rangle}$$

for each key guess. According to [BN17], this statistic follows different distributions under the right and wrong key guess, thus one can recover the right key with some success probability $\Pr_s$. Correlation of (u, v) is determined by all linear trails comprising it, and varies from the right key K. Denote $C(u, v)(K)$ as its correlation under K. To determine the relation between N and $\Pr_s$, Nyberg [Nyb94] introduced the definition of expected linear potential $ELP = 2^{-|K|} \sum_K |C(u, v)(K)|^2$. Detailed relation is constructed in [BN17] with its ELP as a vital parameter. When multiple independent linear hulls are available, Blondeau and Nyberg also constructed the above relation in [BN17] by summing these squared experimental correlations $\widehat{cor}^2$ of each hull together.

Linear Cryptanalysis with (Affine) Pruned Walsh Transform. The idea of using Walsh transform to accelerate linear cryptanalysis was introduced by Collard *et al.* [CSQ07]. However, this framework is restricted to the case where only the last-round key in the key recovery process can be recovered. In EUROCRYPT'20, Flórez-Gutiérrez *et al.* [FN20] generalized their technique into the case when key recovery is considered on both the plaintext and ciphertext sides. They also considered pruned Walsh transform whenever possible, which can save time costs to some extent. Last year, Flórez-Gutiérrez [Fló22] improved this framework using the affine pruned Walsh transform technique, by adding more zeros in the Walsh spectrum through rejecting some data.

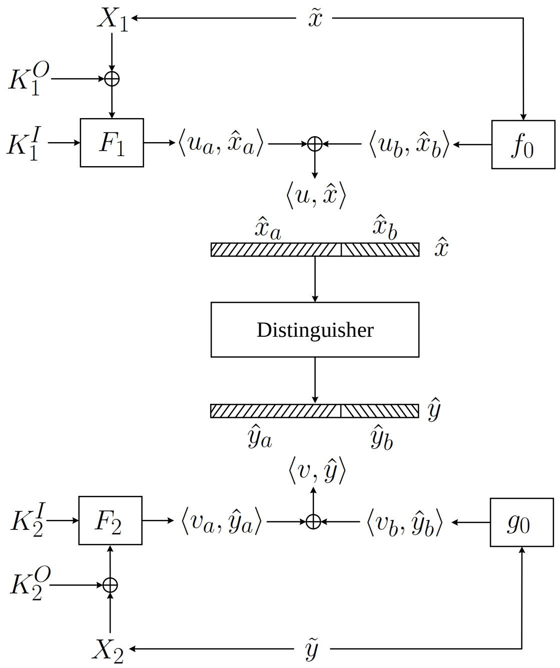

X_1
$\tilde{x}$
K_1^O
K_1^I
F_1
$\langle u_a, \hat{x}_a \rangle$
$\langle u_b, \hat{x}_b \rangle$
f_0
$\langle u, \hat{x} \rangle$
$\hat{x}_a$
$\hat{x}_b$
$\hat{x}$
Distinguisher
$\hat{y}$
$\hat{y}_a$
$\hat{y}_b$
$\langle v, \hat{y} \rangle$
K_2^I
F_2
$\langle v_a, \hat{y}_a \rangle$
$\langle v_b, \hat{y}_b \rangle$
g_0
K_2^O
X_2
$\tilde{y}$

Figure 1: Framework of (affine) pruned Walsh transform accelerated linear attacks.

Here, we briefly recall the core idea of [FN20] and [Fló22] following notations in Fig. 1. In the linear key recovery attack, one aims to evaluate the experimental correlation through the linear approximation $\langle u, \hat{x} \rangle \oplus \langle v, \hat{y} \rangle = 0$ given N plaintext-ciphertext pairs $(\tilde{x}, \tilde{y})$. In [FN20] and [Fló22], the above evaluation is performed under several Walsh Transforms. When computing $\langle u, \hat{x} \rangle$, some bits of $\hat{x}$ may be obtained without any key material, *i.e.* forward-slash part in Fig. 1, while the value of those backslash part can only be achieved after guessing corresponding key bits. In this case, $\langle u, \hat{x} \rangle = f_0(\tilde{x}) \oplus F_1(X_1 \oplus K_1^O, K_1^I)$, where X_1 represents some bits of $\tilde{x}$ and we denote as $\tilde{x} \to X_1$. Similarly, $\langle v, \hat{y} \rangle = g_0(\tilde{y}) \oplus F_2(X_2 \oplus K_2^O, K_2^I)$ with X_2 being some bits of $\tilde{y} = E_K(\tilde{x})$ and denoted as $E_K(\tilde{x}) \to X_2$. Therefore, as shown in [Fló22], the experimental correlation $\widehat{cor}$ under $(K_1^O, K_2^O, K_1^I, K_2^I)$ can be computed as

$$
\begin{aligned}
N \cdot \widehat{cor} &= \sum_{\substack{\tilde{x} \in D, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{F_1(X_1 \oplus K_1^O, K_1^I) \oplus F_2(X_2 \oplus K_2^O, K_2^I) \oplus f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x}))} \\
&= \sum_{X_1, X_2} (-1)^{F_1(X_1 \oplus K_1^O, K_1^I) \oplus F_2(X_2 \oplus K_2^O, K_2^I)} \underbrace{\sum_{\substack{\tilde{x} \in D, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x}))}}_{A[X_1, X_2]} \\
&= \frac{1}{2^{|Y_1| + |Y_2|}} \sum_{Y_1, Y_2} (-1)^{\langle Y_1, K_1^O \rangle \oplus \langle Y_2, K_2^O \rangle} S_{Y_1}^{K_1^I} S_{Y_2}^{K_2^I} \widehat{A}[Y_1, Y_2],
\end{aligned}
$$

where $S_{Y_j}^{K_j^I} = \sum_{Z_j} (-1)^{\langle Y_j, Z_j \rangle \oplus F_j(Z_j, K_j^I)}$ with $j \in \{1, 2\}$, and

$$
\widehat{A}[Y_1, Y_2] = \sum_{X_1, X_2} (-1)^{\langle Y_1, X_1 \rangle \oplus \langle Y_2, X_2 \rangle} A[X_1, X_2].
$$

Note that $\widehat{A}[Y_1, Y_2]$ is the Walsh transform of $A[X_1, X_2]$, and thus can be evaluated within

$L2^L$ additions with $L = |Y_1| + |Y_2|$. When evaluating $S_{Y_j}^{K_j^I}$, one can separate $F_1(Z_1, K_1^I)$ and $F_2(Z_2, K_2^I)$ into the XORed value of several small Boolean functions $f_{1,i}(z_{1,i}, k_{1,i}^I)$ and $f_{2,i}(z_{2,i}, k_{2,i}^I)$, as shown in [Fló22]. Hence, for each $j \in \{1, 2\}$,

$$S_{Y_j}^{K_j^I} = \prod_i \sum_{z_{j,i}} (-1)^{\langle y_{j,i}, z_{j,i}\rangle \oplus f_{j,i}(z_{j,i}, k_{j,i}^I)} = \prod_i (-2)\widehat{f_{j,i}},$$

which can then be effectively obtained with the pruned Walsh transform algorithm.

To further reduce the cost of above computations, Flórez-Gutiérrez [Fló22] utilized the following idea. When computing $S_{Y_1}^{K_1^I}$ and $S_{Y_2}^{K_2^I}$, if Z_1 or Z_2 are restricted in specific subsets of $\mathbb{F}_2^n$, some $\widehat{f_{j,i}}$ will become zeros. In this case, one can achieve much faster computations of $S_{Y_1}^{K_1^I}$ and $S_{Y_2}^{K_2^I}$ using the affine pruned Walsh transform algorithm proposed in [Fló22]. However, one should be aware that $\widehat{cor}$ no longer follows the distributions proposed in [BN17] in this case. Detailed discussions are given in Appendix D. Therefore, the statistic behavior of $\widehat{cor}$ when Z_1 or Z_2 are limited in a subset should be reconstructed.

3 Statistical Models for Linear Attacks with Affine Pruned Walsh Transform

In traditional linear key recovery attacks, the adversary will utilize all obtained N plaintext-ciphertext pairs to compute the experimental correlation. Thus, statistical models proposed by Blondeau and Nyberg in [BN17] are utilized to deduce the relation between N and success probability. However, in the affine pruned Walsh transform accelerated linear attacks [Fló22], we may not use all these N known plaintext-ciphertext pairs, with the aim of reducing time cost.

In this section, we will show the statistic behavior of the experimental correlation under the right and wrong key guesses when some data are rejected in its computation. We also provide the accurate relation between data complexity N and success probability. Dedicated statistical models are given for the general case when $l \geq 1$ independent linear hulls are utilized. Experimental verifications on these statistical models using `SmallPRESENT-[4]` are shown in Sect. 3.3. Notations in this section are borrowed from Sect. 2.

3.1 Classical Setting using One Linear Hull

Before starting this subsection, we give Lemma 1, which is used in the following theorems. Proof of this Lemma is given in Appendix B.

Lemma 1. *The $2^{|Y_1|+|Y_2|}$-dimensional statistic vector $(\widehat{A}[0,0], \cdots, \widehat{A}[2^{|Y_1|}-1, 2^{|Y_2|}-1])$ follows the multivariate normal distribution. Each $\widehat{A}[Y_1, Y_2]$ has expectation $NC_{[Y_1,Y_2]}$. Covariance between $\widehat{A}[Y_1^a, Y_2^a]$ and $\widehat{A}[Y_1^b, Y_2^b]$ is $NB\delta_{[Y_1^a \oplus Y_1^b, Y_2^a \oplus Y_2^b]} - NBC_{[Y_1^a, Y_2^a]}C_{[Y_1^b, Y_2^b]}$, where*

$$C_{[Y_1,Y_2]} = \frac{1}{2^n} \sum_{\substack{\tilde{x} \in \mathbb{F}_2^n, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{\langle Y_1, X_1\rangle \oplus \langle Y_2, X_2\rangle \oplus f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x}))},$$

$$\delta_{[Y_1^a \oplus Y_1^b, Y_2^a \oplus Y_2^b]} = \frac{1}{2^n} \sum_{\substack{\tilde{x} \in \mathbb{F}_2^n, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{\left\langle Y_1^a \oplus Y_1^b, X_1\right\rangle \oplus \left\langle Y_2^a \oplus Y_2^b, X_2\right\rangle},$$

and B equals to 1 (KP Sampling) or $\frac{2^n - N}{2^n - 1}$ (DKP Sampling).

Right Key Guess. Given the linear hull (u, v), we denote $C(u, v)(K)$ as the correlation of the approximation $\langle u, \hat{x}\rangle \oplus \langle v, \hat{y}\rangle = 0$ evaluated using the full codebook, where $\hat{y} = E'_K(\hat{x})$. According to [BN17], when all possible Z_1 and Z_2 are used, $\widehat{cor}$ will follow the normal distribution with expectation $C(u, v)(K)$ and variance $\frac{B}{N}\left(1 - [C(u, v)(K)]^2\right)$ under the right key guess. Note that the above distribution of $\widehat{cor}$ cannot be directly used in mounting key recovery attacks, since $C(u, v)(K)$ is unknown to the adversary and related to the right key. Blondeau and Nyberg [BN17] took a step further by assuming that $C(u, v)(K)$ follows a normal distribution. Denote its expectation as c, and the expected linear potential $ELP = 2^{-|K|}\sum_K [C(u, v)(K)]^2$. Thus, its variance is $ELP - c^2$ according to its definition. In this case, one can conclude that $\widehat{cor}$ approximately follows the normal distribution with expectation c and variance $\frac{B}{N} + ELP - c^2$.

When Z_1 or Z_2 are limited in a subset, we show that $\widehat{cor}$ is also a normal variable, but with different expectation and variance. To avoid confusion, we use variables with subscript $_{(s)}$ to denote the case when not all possible Z_1 or Z_2 are used, such as $\widehat{cor}_{(s)}$, $S^{K_j^I}_{Y_j,(s)}$ and $C(u, v)(K)_{(s)}$. Theorem 1 shows the distribution of $\widehat{cor}_{(s)}$ when K is fixed, which is related to $C(u, v)(K)_{(s)}$. Next, we investigate the relation between $C(u, v)(K)_{(s)}$ and $C(u, v)(K)$ in Theorem 2. Thus, one can obtain the final distribution of $\widehat{cor}_{(s)}$ (Theorem 3). Note that restricted Z_1 or Z_2 will lead to restricted values of $(\hat{x}, \hat{y})$ under fixed K. Denote Q_K as the set recording all these left $(\hat{x}, \hat{y})$. All Q_K have the same size $\#Q_K$ since E_K is a fixed-key permutation, which can be obtained once the linear hull, Q_1 and Q_2 are fixed.

Theorem 1. *Experimental correlation evaluated under right key guess* $(K_1^O, K_2^O, K_1^I, K_2^I)$ *with restricted* Z_1 *or* Z_2 *is*

$$\widehat{cor}_{(s)} = \frac{1}{N}\frac{1}{2^{|Y_1|+|Y_2|}}\sum_{Y_1,Y_2}(-1)^{\langle Y_1,K_1^O\rangle\oplus\langle Y_2,K_2^O\rangle} S^{K_1^I}_{Y_1,(s)} S^{K_2^I}_{Y_2,(s)} \widehat{A}[Y_1, Y_2].$$

For fixed right key guess K*, it follows the normal distribution with expectation*

$$C(u, v)(K)_{(s)} = \frac{1}{2^n}\sum_{(\hat{x},\hat{y})\in Q_K}(-1)^{\langle u,\hat{x}\rangle\oplus\langle v,\hat{y}\rangle}$$

and variance $\frac{B}{N}\left(\#Q_K \cdot 2^{-n} - [C(u, v)(K)_{(s)}]^2\right)$*, where* $\#Q_K$ *denotes the size of* Q_K*.*

Proof. According to Lemma 1, statistic vector $(\widehat{A}[0, 0], \cdots, \widehat{A}[2^{|Y_1|} - 1, 2^{|Y_2|} - 1])$ follows the multivariate normal distribution. Hence, $\widehat{cor}_{(s)}$ follows the normal distribution [KH11]. Without loss of generality, we assume $Z_1 \in Q_1$ and $Z_2 \in Q_2$ under the fixed K_1^I and K_2^I. Thus, according to Lemma 1, expectation of $\widehat{cor}_{(s)}$ is

$$\begin{aligned}
E(\widehat{cor}_{(s)}) =& \frac{1}{N}\frac{1}{2^{|Y_1|+|Y_2|}}\sum_{Y_1,Y_2}(-1)^{\langle Y_1,K_1^O\rangle\oplus\langle Y_2,K_2^O\rangle} S^{K_1^I}_{Y_1,(s)} S^{K_2^I}_{Y_2,(s)} E(\widehat{A}[Y_1, Y_2])\\
=& \frac{1}{2^{|Y_1|+|Y_2|}}\sum_{Y_1,Y_2}(-1)^{\langle Y_1,K_1^O\rangle\oplus\langle Y_2,K_2^O\rangle} S^{K_1^I}_{Y_1,(s)} S^{K_2^I}_{Y_2,(s)} C_{[Y_1,Y_2]}\\
=& \frac{1}{2^{|Y_1|+|Y_2|}}\frac{1}{2^n}\sum_{\substack{\tilde{x}\in\mathbb{F}_2^n,\\ \tilde{x}\to X_1, E_K(\tilde{x})\to X_2}}(-1)^{f_0(\tilde{x})\oplus g_0(E_K(\tilde{x}))} R_1 R_2,
\end{aligned}$$

where

$$\begin{aligned}
R_1 &= \sum_{Z_1\in Q_1}(-1)^{F_1(Z_1,K_1^I)}\sum_{Y_1}(-1)^{\langle Y_1,K_1^O\oplus X_1\oplus Z_1\rangle},\\
R_2 &= \sum_{Z_2\in Q_2}(-1)^{F_2(Z_2,K_2^I)}\sum_{Y_2}(-1)^{\langle Y_2,K_2^O\oplus X_2\oplus Z_2\rangle},
\end{aligned}$$

and the last equality comes directly from the definition of $C_{[Y_1,Y_2]}$ given in Lemma 1. For each $\tilde{x} \in \mathbb{F}_2^n$, if $\exists Z_1 \in Q_1$ and $\exists Z_2 \in Q_2$ s.t. $X_1 \oplus K_1^O = Z_1$ and $X_2 \oplus K_2^O = Z_2$, we have $R_1 = (-1)^{F_1(X_1 \oplus K_1^O, K_1^I)} 2^{|Y_1|}$ and $R_2 = (-1)^{F_2(X_2 \oplus K_2^O, K_2^I)} 2^{|Y_2|}$. However, if $\forall Z_1 \in Q_1$ s.t. $X_1 \oplus K_1^O \neq Z_1$ or $\forall Z_2 \in Q_2$ s.t. $X_2 \oplus K_2^O \neq Z_2$, we have $R_1 R_2 = 0$. Therefore,

$$\begin{aligned} E(\widehat{cor}_{(s)}) =& \frac{1}{2^{|Y_1|+|Y_2|}} \frac{1}{2^n} \sum_{\substack{\tilde{x} \in \mathbb{F}_2^n, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2, \\ \exists Z_1 \in Q_1, \text{ s.t. } X_1 \oplus K_1^O = Z_1, \\ \exists Z_2 \in Q_2, \text{ s.t. } X_2 \oplus K_2^O = Z_2}} (-1)^{f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x}))} R_1 R_2 \\ =& \frac{1}{2^n} \sum_{\substack{\tilde{x} \in \mathbb{F}_2^n, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2, \\ \exists Z_1 \in Q_1, \text{ s.t. } X_1 \oplus K_1^O = Z_1, \\ \exists Z_2 \in Q_2, \text{ s.t. } X_2 \oplus K_2^O = Z_2}} (-1)^{f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x})) \oplus F_1(X_1 \oplus K_1^O, K_1^I) \oplus F_2(X_2 \oplus K_2^O, K_2^I)} \end{aligned}$$

For the fixed $\tilde{x}$, we know that there is only one $\hat{x}$, X_1 and Z_1 under K. Similarly, if $\tilde{y}$ is fixed, $\hat{y}$, X_2 and Z_2 are all fixed values. Hence, restricted Z_1 or Z_2 will leads to restricted value set Q_K of $(\hat{x}, \hat{y})$. Recall that $\langle u, \hat{x} \rangle \oplus \langle v, \hat{y} \rangle = f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x})) \oplus F_1(X_1 \oplus K_1^O, K_1^I) \oplus F_2(X_2 \oplus K_2^O, K_2^I)$, we can obtain

$$E(\widehat{cor}_{(s)}) = \frac{1}{2^n} \sum_{(\hat{x}, \hat{y}) \in Q_K} (-1)^{\langle u, \hat{x} \rangle \oplus \langle v, \hat{y} \rangle} = C(u,v)(K)_{(s)}.$$

According to Lemma 1, $(\widehat{A}[0,0], \cdots, \widehat{A}[2^{|Y_1|}-1, 2^{|Y_2|}-1])$ follows the multivariate normal distribution. Note that variance of any linear combination $\sum_{Y_1,Y_2} a_{[Y_1,Y_2]} \widehat{A}[Y_1, Y_2]$ is

$$\sum_{Y_1^a, Y_2^a} a_{[Y_1^a, Y_2^a]} \sum_{Y_1^b, Y_2^b} a_{[Y_1^b, Y_2^b]} \mathbf{Cov}(\widehat{A}[Y_1^a, Y_2^a], \widehat{A}[Y_1^b, Y_2^b]).$$

Therefore, according to Lemma 1, we can obtain $Var\left(\widehat{cor}_{(s)}\right)$, which equals to

$$\begin{aligned} &\left(\frac{1}{N} \frac{1}{2^{|Y_1|+|Y_2|}} \right)^2 \sum_{Y_1^a, Y_2^a} \sum_{Y_1^b, Y_2^b} (-1)^{\left\langle Y_1^a \oplus Y_1^b, K_1^O \right\rangle \oplus \left\langle Y_2^a \oplus Y_2^b, K_2^O \right\rangle} \\ &\qquad S_{Y_1^a,(s)}^{K_1^I} S_{Y_2^a,(s)}^{K_2^I} S_{Y_1^b,(s)}^{K_1^I} S_{Y_2^b,(s)}^{K_2^I} \left(NB\delta_{[Y_1^a \oplus Y_1^b, Y_2^a \oplus Y_2^b]} - NBC_{[Y_1^a, Y_2^a]} C_{[Y_1^b, Y_2^b]} \right). \end{aligned}$$

Denote W as the first part of the above formula ignoring its coefficient, which is

$$\sum_{Y_1^a, Y_2^a} \sum_{Y_1^b, Y_2^b} (-1)^{\left\langle Y_1^a \oplus Y_1^b, K_1^O \right\rangle \oplus \left\langle Y_2^a \oplus Y_2^b, K_2^O \right\rangle} S_{Y_1^a,(s)}^{K_1^I} S_{Y_2^a,(s)}^{K_2^I} S_{Y_1^b,(s)}^{K_1^I} S_{Y_2^b,(s)}^{K_2^I} \delta_{[Y_1^a \oplus Y_1^b, Y_2^a \oplus Y_2^b]},$$

one can represent $Var\left(\widehat{cor}_{(s)}\right)$ as

$$\begin{aligned} &\frac{B}{N} \left(\frac{1}{2^{|Y_1|+|Y_2|}} \right)^2 W - \frac{B}{N} \left(\frac{1}{2^{|Y_1|+|Y_2|}} \sum_{Y_1^a, Y_2^a} (-1)^{\left\langle Y_1^a, K_1^O \right\rangle \oplus \left\langle Y_2^a, K_2^O \right\rangle} S_{Y_1^a,(s)}^{K_1^I} S_{Y_2^a,(s)}^{K_2^I} C_{[Y_1^a, Y_2^a]} \right) \\ &\qquad \left(\frac{1}{2^{|Y_1|+|Y_2|}} \sum_{Y_1^b, Y_2^b} (-1)^{\left\langle Y_1^b, K_1^O \right\rangle \oplus \left\langle Y_2^b, K_2^O \right\rangle} S_{Y_1^b,(s)}^{K_1^I} S_{Y_2^b,(s)}^{K_2^I} C_{[Y_1^b, Y_2^b]} \right) \\ =& \frac{B}{N} \left(\frac{1}{2^{|Y_1|+|Y_2|}} \right)^2 W - \frac{B}{N} \left(\frac{1}{2^{|Y_1|+|Y_2|}} \sum_{Y_1, Y_2} (-1)^{\left\langle Y_1, K_1^O \right\rangle \oplus \left\langle Y_2, K_2^O \right\rangle} S_{Y_1,(s)}^{K_1^I} S_{Y_2,(s)}^{K_2^I} C_{[Y_1, Y_2]} \right)^2. \end{aligned}$$

From Lemma 1, recall that $E(\widehat{A}[Y_1, Y_2]) = NC_{[Y_1,Y_2]}$. Hence, $Var\left(\widehat{cor}_{(s)}\right)$ equals to

$$\frac{B}{N}\left(\frac{1}{2^{|Y_1|+|Y_2|}}\right)^2 W - \frac{B}{N}\left(E(\widehat{cor}_{(s)})\right)^2 = \frac{B}{N}\left(\frac{1}{2^{|Y_1|+|Y_2|}}\right)^2 W - \frac{B}{N}\left[C(u,v)(K)_{(s)}\right]^2.$$

Now let's focus on W. Let $T_1 = Y_1^a \oplus Y_1^b$ and $T_2 = Y_2^a \oplus Y_2^b$, we have

$$\begin{aligned} W =& \sum_{T_1,T_2}\sum_{Y_1^b,Y_2^b} (-1)^{\langle T_1,K_1^O\rangle\oplus\langle T_2,K_2^O\rangle} S^{K_1^I}_{Y_1^b,(s)} S^{K_2^I}_{Y_2^b,(s)} S^{K_1^I}_{Y_1^b\oplus T_1,(s)} S^{K_2^I}_{Y_2^b\oplus T_2,(s)} \delta_{[T_1,T_2]} \\ =& \sum_{T_1,T_2} (-1)^{\langle T_1,K_1^O\rangle\oplus\langle T_2,K_2^O\rangle} \delta_{[T_1,T_2]} \left(\sum_{Y_1^b} S^{K_1^I}_{Y_1^b,(s)} S^{K_1^I}_{Y_1^b\oplus T_1,(s)}\right)\left(\sum_{Y_2^b} S^{K_2^I}_{Y_2^b,(s)} S^{K_2^I}_{Y_2^b\oplus T_2,(s)}\right). \end{aligned}$$

Since $S^{K_1^I}_{Y_1^b,(s)} = \sum_{Z_1\in Q_1}(-1)^{\langle Y_1^b,Z_1\rangle\oplus F_1(Z_1,K_1^I)}$, we have

$$\begin{aligned} &\sum_{Y_1^b} S^{K_1^I}_{Y_1^b,(s)} S^{K_1^I}_{Y_1^b\oplus T_1,(s)} \\ =&\sum_{Y_1^b}\left(\sum_{Z_1\in Q_1}(-1)^{\langle Y_1^b,Z_1\rangle\oplus F_1(Z_1,K_1^I)}\right)\left(\sum_{Z_1'\in Q_1}(-1)^{\langle Y_1^b\oplus T_1,Z_1'\rangle\oplus F_1(Z_1',K_1^I)}\right) \\ =&\sum_{Z_1\in Q_1}\sum_{Z_1'\in Q_1}\left((-1)^{\langle T_1,Z_1'\rangle\oplus F_1(Z_1,K_1^I)\oplus F_1(Z_1',K_1^I)}\sum_{Y_1^b}(-1)^{\langle Y_1^b,Z_1\oplus Z_1'\rangle}\right) \\ =&\sum_{Z_1\in Q_1}(-1)^{\langle T_1,Z_1\rangle}2^{|Y|}. \end{aligned}$$

The last equality comes from the fact that when $Z_1 = Z_1'$, the sum $\sum_{Y_1^b}(-1)^{\langle Y_1^b,Z_1\oplus Z_1'\rangle}$ equals to $2^{|Y|}$; while it equals to 0 when $Z_1 \neq Z_1'$. In this case, with the definition of $\delta_{[T_1,T_2]}$ shown in Lemma 1,

$$\begin{aligned} W =& \sum_{T_1,T_2}(-1)^{\langle T_1,K_1^O\rangle\oplus\langle T_2,K_2^O\rangle}\delta_{[T_1,T_2]}\left(2^{|Y_1|}\sum_{Z_1\in Q_1}(-1)^{\langle T_1,Z_1\rangle}\right)\left(2^{|Y_2|}\sum_{Z_2\in Q_2}(-1)^{\langle T_2,Z_2\rangle}\right) \\ =&\frac{2^{|Y_1|+|Y_2|}}{2^n}\sum_{\substack{\tilde{x}\in\mathbb{F}_2^n,\\ \tilde{x}\to X_1, E_K(\tilde{x})\to X_2}}\prod_{j=1}^{2}\left(\sum_{T_j}\sum_{Z_j\in Q_j}(-1)^{\langle T_j,K_j^O\oplus X_j\oplus Z_j\rangle}\right). \end{aligned}$$

As discussed before, for each $\tilde{x} \in \mathbb{F}_2^n$, the above product is $2^{|T_1|+|T_2|}$ or 0 depending on whether corresponding Z_1 and Z_2 exist. In this case, we can deduce that

$$W = \frac{1}{2^n}2^{|Y_1|+|Y_2|}2^{|T_1|+|T_2|}\sum_{\substack{\tilde{x}\in\mathbb{F}_2^n,\\ \tilde{x}\to X_1,E_K(\tilde{x})\to X_2,\\ \exists Z_1\in Q_1,\text{ s.t. } X_1\oplus K_1^O=Z_1,\\ \exists Z_2\in Q_2,\text{ s.t. } X_2\oplus K_2^O=Z_2}} 1 = \left(2^{|Y_1|+|Y_2|}\right)^2\#Q_K\cdot 2^{-n},$$

which leads to $Var(\widehat{cor}_{(s)}) = \frac{B}{N}(\#Q_K\cdot 2^{-n} - [C(u,v)(K)_{(s)}]^2)$. □

When K is fixed, $C(u,v)(K)_{(s)} = 2^{-n}\sum_{(\hat{x},\hat{y})\in Q_K}(-1)^{\langle u,\hat{x}\rangle\oplus\langle v,\hat{y}\rangle}$ is a fixed value. However, one cannot obtain it unless K is known since Q_K has to be obtained at first. Hence, we have to consider the effect of different K, as Blondeau and Nyberg did in [BN17].

Theorem 2. *$C(u,v)(K)_{(s)}$ approximately follows the normal distribution with expectation $\#Q_K 2^{-n}c$ and variance $\#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2)$.*

Proof. Denote $p_{K,(s)}$ as the probability that $\langle u, \hat{x}\rangle \oplus \langle v, \hat{y}\rangle = 0$ when $(\hat{x}, \hat{y}) \in Q_K$. Thus,

$$p_{K,(s)} = \frac{2^n C(u,v)(K)_{(s)} + \#Q_K}{2\#Q_K}.$$

When the above approximation is evaluated under all 2^n possible values of $(\hat{x}, \hat{y})$, we denote corresponding probability as p_K, which equals to $2^{-1}(1 + C(u,v)(K))$.

Note that $p_{K,(s)}$ can be regarded as the sample proportion when $\#Q_K$ samples are considered. According to the central limit theorem for sample proportions [Wei82], we know that $p_{K,(s)}$ approximately follows the normal distribution with expectation p_K and variance $\frac{1}{\#Q_K} p_K(1 - p_K)$. Hence, $C(u,v)(K)_{(s)} = \#Q_K 2^{-n}(2p_{K,(s)} - 1)$ also approximately follows the normal distribution with expectation $\#Q_K 2^{-n} C(u,v)(K)$ and variance $\#Q_K 2^{-2n}(1 - [C(u,v)(K)]^2)$. As Blondeau and Nyberg did in [BN17], one can replace this variance by its close upper bound that is $\#Q_K 2^{-2n}$.

Given $C(u,v)(K) \sim \mathbf{N}\left(c, ELP - c^2\right)$, one can obtain the distribution of $C(u,v)(K)_{(s)}$ by exploiting characteristic functions of normal distributions, which are

$$\mathcal{CF}_{C(u,v)(K)_{(s)}|C(u,v)(K)}(it) = \exp\left\{it\#Q_K 2^{-n} C(u,v)(K) - \frac{t^2}{2}\#Q_K 2^{-2n}\right\},$$

$$\mathcal{CF}_{C(u,v)(K)}(it) = \exp\left\{itc - \frac{t^2}{2}(ELP - c^2)\right\}.$$

Thus,

$$\begin{aligned}
&\mathcal{CF}_{C(u,v)(K)_{(s)}}(it)\\
=&\exp\left\{-\frac{t^2}{2}\#Q_K 2^{-2n}\right\} \cdot \mathcal{CF}_{C(u,v)(K)}(it\#Q_K 2^{-n})\\
=&\exp\left\{-\frac{t^2}{2}\#Q_K 2^{-2n}\} \exp\{it\#Q_K 2^{-n}c - \frac{t^2(\#Q_K 2^{-n})^2}{2}(ELP - c^2)\right\}\\
=&\exp\left\{it\#Q_K 2^{-n}c - \frac{t^2}{2}\left(\#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2)\right)\right\}.
\end{aligned}$$

Hence, $C(u,v)(K)_{(s)}$ is a normal variable with claimed expectation and variance. □

Theorem 3. *When guessed key is right, $\widehat{cor}_{(s)}$ approximately follows the normal distribution with expectation $\#Q_K 2^{-n}c$ and variance*

$$\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2),$$

where $B = 1$ (KP Sampling) or $B = \frac{2^n - N}{2^n - 1}$ (DKP Sampling).

Proof. As did in [BN17], we replace the variance of $\widehat{cor}_{(s)}$ when K is fixed by its close upper bound. Therefore, with Theorem 1 and 2, we have

$$\widehat{cor}_{(s)} \sim \mathbf{N}\left(C(u,v)(K)_{(s)}, \frac{B}{N}\#Q_K \cdot 2^{-n}\right),$$

$$C(u,v)(K)_{(s)} \sim \mathbf{N}\left(\#Q_K 2^{-n}c, \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2)\right).$$

Characteristic function of the first distribution is

$$\mathcal{CF}_{\widehat{cor}_{(s)}|C(u,v)(K)_{(s)}}(it) = \exp\left\{itC(u,v)(K)_{(s)} - \frac{t^2}{2}\frac{B}{N}\#Q_K \cdot 2^{-n}\right\}.$$

It follows that

$$\begin{aligned}&\mathcal{CF}_{\widehat{cor}_{(s)}}(it)\\ =&\exp\left\{-\frac{t^2}{2}\frac{B}{N}\#Q_K\cdot 2^{-n}\right\}\cdot\mathcal{CF}_{C(u,v)(K)_{(s)}}(it)\\ =&\exp\left\{it\#Q_K 2^{-n}c-\frac{t^2}{2}\left(\frac{B}{N}\#Q_K 2^{-n}+\#Q_K 2^{-2n}+(\#Q_K 2^{-n})^2(ELP-c^2)\right)\right\}.\end{aligned}$$

In other words, $\widehat{cor}_{(s)}$ is a normal variate with claimed expectation and variance. □

Wrong Key Guess. Denote $\hat{x}'=\tilde{E_1}(\tilde{x})$ and $\hat{y}'=\tilde{E_2}(\tilde{y})$ as values encrypted or decrypted under wrong key K_w, respectively. $C(K_w)$ represents the correlation of $\langle u,\hat{x}'\rangle\oplus\langle v,\hat{y}'\rangle=0$ evaluated using the full codebook, where $\hat{y}'=\tilde{E_2}\circ E_K\circ\tilde{E_1}^{-1}(\hat{x}')$. When all possible Z_1 and Z_2 are used, $\widehat{cor}$ follows the normal distribution with expectation $C(K_w)$ and variance $\frac{B}{N}\left(1-[C(K_w)]^2\right)$ when K_w is fixed [BN17]. By regarding $\tilde{E_2}\circ E_K\circ\tilde{E_1}^{-1}$ as a random vectorial Boolean function, $C(K_w)$ follows the normal distribution with expectation 0 and variance 2^{-n}. Combing above two distributions, one can obtain that $\widehat{cor}$ follows the normal distribution with expectation 0 and variance $\frac{B}{N}+2^{-n}$. When Z_1 or Z_2 are limited in a subset, we can achieve that $\widehat{cor}_{(s)}$ also follows a normal distribution with the same expectation but different variance following Theorem 4, 5 and 6.

Theorem 4. *Experimental correlation evaluated under wrong key guess $(K_1^O,K_2^O,K_1^I,K_2^I)$ with restricted Z_1 or Z_2 is*

$$\widehat{cor}_{(s)}=\frac{1}{N}\frac{1}{2^{|Y_1|+|Y_2|}}\sum_{Y_1,Y_2}(-1)^{\langle Y_1,K_1^O\rangle\oplus\langle Y_2,K_2^O\rangle}S_{Y_1,(s)}^{K_1^I}S_{Y_2,(s)}^{K_2^I}\widehat{A}[Y_1,Y_2].$$

For fixed wrong key guess K_w, it follows the normal distribution with expectation

$$C(K_w)_{(s)}=\frac{1}{2^n}\sum_{(\hat{x}',\hat{y}')\in Q_K}(-1)^{\langle u,\hat{x}'\rangle\oplus\langle v,\hat{y}'\rangle}$$

and variance $\frac{B}{N}\left(\#Q_K\cdot 2^{-n}-[C(K_w)_{(s)}]^2\right)$, where $\#Q_K$ denotes the size of Q_K.

Proof. This proof follows directly from the one of Theorem 1. Difference between them is shown as follows. From the former proof, we have learned that

$$E(\widehat{cor}_{(s)})=\frac{1}{2^n}\sum_{\substack{\tilde{x}\in\mathbb{F}_2^n,\\ \tilde{x}\to X_1,E_K(\tilde{x})\to X_2,\\ \exists Z_1\in Q_1,\text{ s.t. }X_1\oplus K_1^O=Z_1,\\ \exists Z_2\in Q_2,\text{ s.t. }X_2\oplus K_2^O=Z_2}}(-1)^{f_0(\tilde{x})\oplus g_0(E_K(\tilde{x}))\oplus F_1(X_1\oplus K_1^O,K_1^I)\oplus F_2(X_2\oplus K_2^O,K_2^I)}.$$

When guessed key K_w is wrong, $E(\widehat{cor}_{(s)})$ represents the correlation of $\langle u,\hat{x}'\rangle\oplus\langle v,\hat{y}'\rangle=0$ where $(\hat{x}',\hat{y}')$ is obtained from $(\tilde{x},\tilde{y})$ under K_w and restricted in a subset Q_{K_w}. Hence, $E(\widehat{cor}_{(s)})=C(K_w)_{(s)}$. Since $\tilde{E_2}\circ E_K\circ\tilde{E_1}^{-1}$ is a fixed-key permutation, Q_{K_w} will have the same size for any K_w due to the same subsets Q_1 and Q_2. Similarly, $\#Q_{K_w}$ equals to previous mentioned $\#Q_K$ since both $\tilde{E_2}\circ E_K\circ\tilde{E_1}^{-1}$ and E_K' are fixed-key permutations. Meanwhile, its variance is

$$\frac{B}{N}\left(\frac{1}{2^{|Y_1|+|Y_2|}}\right)^2W-\frac{B}{N}\left(E(\widehat{cor}_{(s)})\right)^2=\frac{B}{N}\left(\frac{1}{2^{|Y_1|+|Y_2|}}\right)^2W-\frac{B}{N}\left(C(K_w)_{(s)}\right)^2,$$

where $W=\left(2^{|Y_1|+|Y_2|}\right)^2\#Q_K\cdot 2^{-n}$ as shown in the former proof. □

Theorem 5. *$C(K_w)_{(s)}$ approximately follows the normal distribution with expectation 0 and variance $\#Q_K 2^{-2n}$.*

Proof. Similar with [BN17], $\tilde{E_2} \circ E_K \circ \tilde{E_1}^{-1}$ can be regarded as a random vectorial Boolean function for each wrong key guess K_w. Hence, the probability that $\langle u, \hat{x}' \rangle \oplus \langle v, \hat{y}' \rangle = 0$ is always 2^{-1}. Note that $2^{-1}(2^n C(K_w)_{(s)} + \#Q_K)$ is the number of $(\hat{x}', \hat{y}') \in Q_K$ fulfilling this approximation. Thus, it approximately follows the normal distribution with expectation $\#Q_K 2^{-1}$ and variance $\#Q_K 2^{-2}$. It follows that $C(K_w)_{(s)}$ is a normal variable with claimed expectation and variance. □

Theorem 6. *When guessed key is wrong, $\widehat{cor}_{(s)}$ approximately follows the normal distribution with expectation 0 and variance*

$$\frac{B}{N} \#Q_K 2^{-n} + \#Q_K 2^{-2n},$$

where $B = 1$ (KP Sampling) or $B = \frac{2^n - N}{2^n - 1}$ (DKP Sampling).

Proof. Replacing the variance of $\widehat{cor}_{(s)}$ when the guessed key K_w is fixed by its close upper bound, we obtain

$$\widehat{cor}_{(s)} \sim \mathbf{N}\left(C(K_w)_{(s)}, \frac{B}{N} \#Q_K \cdot 2^{-n} \right)$$

from Theorem 4. With Theorem 5, $C(K_w)_{(s)} \sim \mathbf{N}\left(0, \#Q_K 2^{-2n}\right)$. Hence, using characteristic functions of above two normal distributions, we can obtain the claimed distribution. □

Data Complexity and Error Probabilities. With Theorem 3 and 6, we can deduce the relation between N and two types of error probabilities α_0 and α_1. When the expectation of $C(u,c)(K)$, which is denoted as c, equals to zero, Corollary 1 shows the above relation, while Corollary 3 given in Appendix C describes the above relation when $c \neq 0$. In our applications on PRESENT, $c = 0$ as shown in [BN17]. Note that c is often hard to be estimated in practical applications unless all dominant linear trails in the hull can be obtained [BN17].

To deduce the above relation, we have to perform a statistic test which can decide whether the obtained statistic $\widehat{cor}_{(s)}$ is computed under the right key or a wrong key guess. When $c = 0$, it's impossible to distinguish two normal distributions with the same expectation with a single value of $\widehat{cor}_{(s)}$. However, we can still construct the relation between N, α_0 and α_1 if we use $[\widehat{cor}_{(s)}]^2$ as our statistic. Note that

$$[\widehat{cor}_{(s)}]^2 \sim \begin{cases} \left(\frac{B}{N} \#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2 ELP \right) \chi^2(1), \text{ right key guess,} \\ \left(\frac{B}{N} \#Q_K 2^{-n} + \#Q_K 2^{-2n} \right) \chi^2(1), \text{ wrong key guess.} \end{cases}$$

according to Theorem 3 and 6, where $\chi^2(1)$ denotes the chi-square distribution with the degree of freedom 1. In this case, we use the threshold-based decision function, where we regard the guessed key is possibly right if $[\widehat{cor}_{(s)}]^2 > \tau$, otherwise, it's a wrong key guess. Detailed relation is depicted in Corollary 1.

Corollary 1. *Denote α_0 as the probability of rejecting the right key, and α_1 as the probability of accepting a wrong key. When $c = 0$, the number of plaintexts needed is*

$$N = \begin{cases} M_2(\alpha_0, \alpha_1), & \textit{KP Sampling,} \\ 2^n \dfrac{M_2(\alpha_0, \alpha_1)}{2^n - 1 + M_2(\alpha_0, \alpha_1)}, & \textit{DKP Sampling,} \end{cases}$$

and the threshold value is

$$\tau = \left(\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2 ELP\right) q_{\alpha_0},$$

where

$$M_2(\alpha_0, \alpha_1) = 2^n \frac{q_{\alpha_0} - q_{1-\alpha_1}}{q_{1-\alpha_1} - q_{\alpha_0} - \#Q_K q_{\alpha_0} ELP}$$

with q_{α_0} and $q_{1-\alpha_1}$ as lower quantiles of $\chi^2(1)$.

Proof. By the definition of α_0 and our statistic test, we have $\Pr\{[\widehat{cor}_{(s)}]^2 < \tau\} = \alpha_0$ when $[\widehat{cor}_{(s)}]^2$ follows the distribution under the right key guess. Then,

$$\Pr\left\{\frac{[\widehat{cor}_{(s)}]^2}{E_R} < \frac{\tau}{E_R}\right\} = \alpha_0$$

where $E_R = \left(\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2 ELP\right)$. By the definition of a quantile, $\frac{\tau}{E_R} = q_{\alpha_0}$. In other words, $\tau = E_R q_{\alpha_0}$. Similarly, we can obtain $\tau = E_w q_{1-\alpha_1}$ due to $\Pr\{[\widehat{cor}_{(s)}]^2 < \tau\} = 1-\alpha_1$ when $[\widehat{cor}_{(s)}]^2$ follows the distribution under a wrong key guess, where $E_w = \left(\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n}\right)$. Hence, we see that $E_R q_{\alpha_0} = E_w q_{1-\alpha_1}$ by eliminating τ from the above two equations. In this case, N can be obtained as claimed. □

3.2 Multiple Linear Setting with l Linear Hulls

Linear key recovery attack using multiple independent linear hulls was proposed in [JR94, BCQ04], and its statistical model is then refined in [BN17]. Here, we show how to construct the statistic model for l hulls when Z_1 or Z_2 are restricted in a subset. Note that for different hull, one may add different restrictions on Z_1 and Z_2, or even no restrictions are made. However, our statistical model here can deal with all possible cases together.

For the i-th hull, we represent its expected linear potential as ELP_i. Expectation of $C(u,v)(K)$ of this hull is c_i. Besides, $\#Q_K$ for this hull equals to $2^n p_i$. Denote $\mathcal{C}_i$ as the experimental correlation evaluated for the i-th hull. Hence, we adopt

$$\mathcal{C} = \sum_{i=1}^{l} \frac{[\mathcal{C}_i]^2}{p_i}$$

as the final statistic. According to Theorem 3 and 6, we know that

$$\frac{\mathcal{C}_i}{\sqrt{p_i}} \sim \begin{cases} \mathbf{N}\left(\sqrt{p_i}c_i, \frac{B}{N} + 2^{-n} + p_i(ELP_i - c_i^2)\right), \text{ right key guess,} \\ \mathbf{N}\left(0, \frac{B}{N} + 2^{-n}\right), \text{ wrong key guess.} \end{cases}$$

Hence, for the wrong key guess, C follows $\left(\frac{B}{N} + 2^{-n}\right)\chi^2(l)$ since all $\frac{\mathcal{C}_i}{\sqrt{p_i}}$ follow the same normal distribution. While for the right key guess, each $\frac{\mathcal{C}_i}{\sqrt{p_i}}$ follows the normal distribution with different variances. According to [Coe20], there is no finite form of the density function of $\mathcal{C}$. However, one can approximate its density function by approximating each variance with $\frac{B}{N} + 2^{-n} + \bar{\sigma}$. There are many different ways to determine $\bar{\sigma}$, such as the arithmetic mean of $p_i(ELP_i - c_i^2)$ adopted by [BN17]. Thus, for the right key guess,

$$\mathcal{C} \sim \left(\frac{B}{N} + 2^{-n} + \bar{\sigma}\right)\chi^2(l, \gamma)$$

with the non-central parameter $\gamma = \sum_{i=1}^{l} p_i c_i^2$. In practical applications, c_i is always hard to be obtained since one cannot traverse all possible K. Similar question also exist in [BN17], where $\sum_{i=1}^{l} c_i^2$ is assumed to be zero. Here, we also adopt this assumption in our applications, which leads to $\gamma = 0$. We summarize above results in Theorem 7.

Theorem 7. *Let $\mathcal{C}_i$ be the experimental correlation evaluated for the i-th hull. Then*

$$\mathcal{C} = \sum_{i=1}^{l} \frac{[\mathcal{C}_i]^2}{p_i} \sim \begin{cases} \left(\frac{B}{N} + 2^{-n} + \bar{\sigma}\right)\chi^2(l), & \textit{right key guess,} \\ \left(\frac{B}{N} + 2^{-n}\right)\chi^2(l), & \textit{wrong key guess.} \end{cases}$$

$\bar{\sigma}$ is the arithmetic mean of these $p_i ELP_i$, where $p_i = \#Q_K 2^{-n}$ is the filtering ratio, and ELP_i is the expected linear potential of the i-th hull.

Relation between N and two types of error probabilities α_0 and α_1 can then be obtained by Theorem 7, which is depicted in Corollary 2. To deduce the relation, we adopt a similar decision function where we regard the guessed key is right if $\mathcal{C} > \tau$. Proof of this corollary is similar with that of Corollary 1. Hence, we omit it here.

Corollary 2. *Denote α_0 as the probability of rejecting the right key, and α_1 as the probability of accepting a wrong key. Assuming that $\gamma = 0$, the number of plaintexts is*

$$N = \begin{cases} M_3(\alpha_0, \alpha_1), & \textit{KP Sampling,} \\ 2^n \frac{M_3(\alpha_0, \alpha_1)}{2^n - 1 + M_3(\alpha_0, \alpha_1)}, & \textit{DKP Sampling,} \end{cases}$$

and the threshold value is

$$\tau = \left(\frac{B}{N} + 2^{-n} + \bar{\sigma}\right) q_{\alpha_0},$$

where

$$M_3(\alpha_0, \alpha_1) = 2^n \frac{q_{\alpha_0} - q_{1-\alpha_1}}{q_{1-\alpha_1} - q_{\alpha_0} - 2^n q_{\alpha_0}\bar{\sigma}}$$

with q_{α_0} and $q_{1-\alpha_1}$ as lower quantiles of $\chi^2(l)$.

3.3 Experimental Verifications

To verify our statistical models, we mount linear key recovery attacks on `SmallPRESENT-[4]` with a single linear hull and 6 linear hulls, respectively.

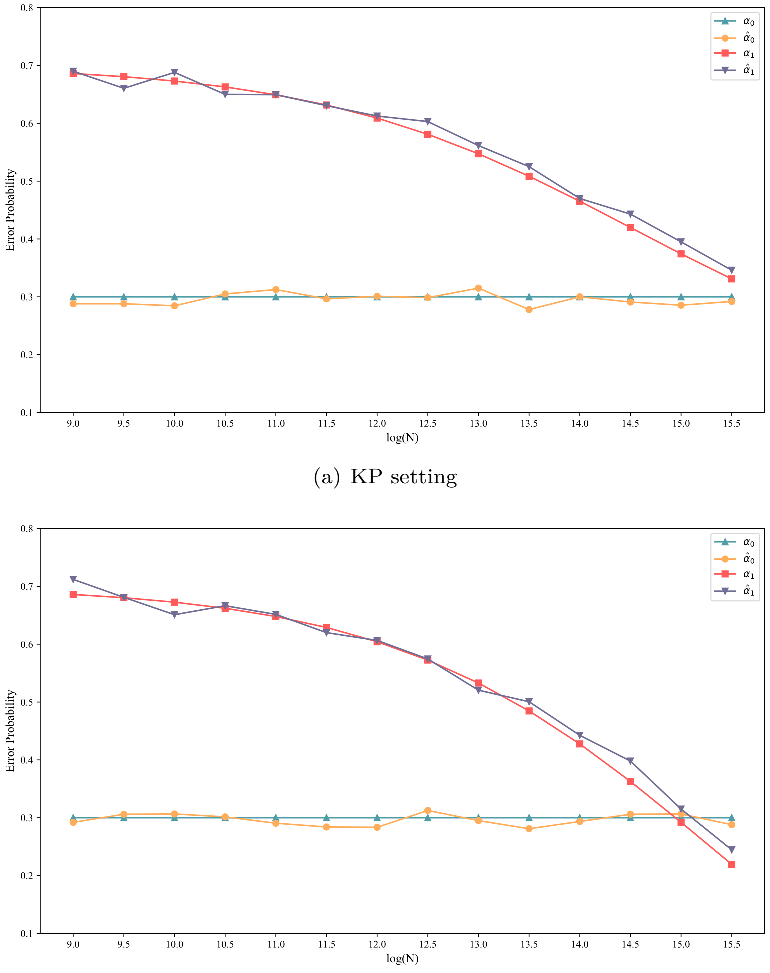
`SmallPRESENT-[4]` is a 16-bit scale variant of PRESENT proposed by Leander [Lea10]. To simplify the key recovery process, we assumed that all round keys are chosen independently. We use 4-round hulls to mount 6-round attacks by appending two rounds after. All linear hulls used are depicted in Table 3.

Table 3: 4-Round linear hulls used in attacking 6-Round `SmallPRESENT`.

	Input Mask	Output Mask	ELP	Filtering Ratio p	Value Rejected
1	00a0	0020	$2^{-11.89}$	0.75	$\{3, 5, B, D\}$
2	00a0	0040	$2^{-11.84}$	0.75	$\{1, 3, D, F\}$
3	00a0	0080	$2^{-11.61}$	0.5	$\{0, 1, 2, 4, 5, 7, 9, C\}$
4	0020	0020	$2^{-12.35}$	1	$\emptyset$
5	0020	0040	$2^{-13.05}$	1	$\emptyset$
6	0020	0080	$2^{-12.35}$	1	$\emptyset$

The first hull shown in Table 3 is used in the case where only one linear hull is adopted. Corresponding experiment is denoted as Type-I experiment in this subsection. All 6 hulls in Table 3 are used in the multiple linear setting, and we refer corresponding experiment as Type-II experiment hereafter.

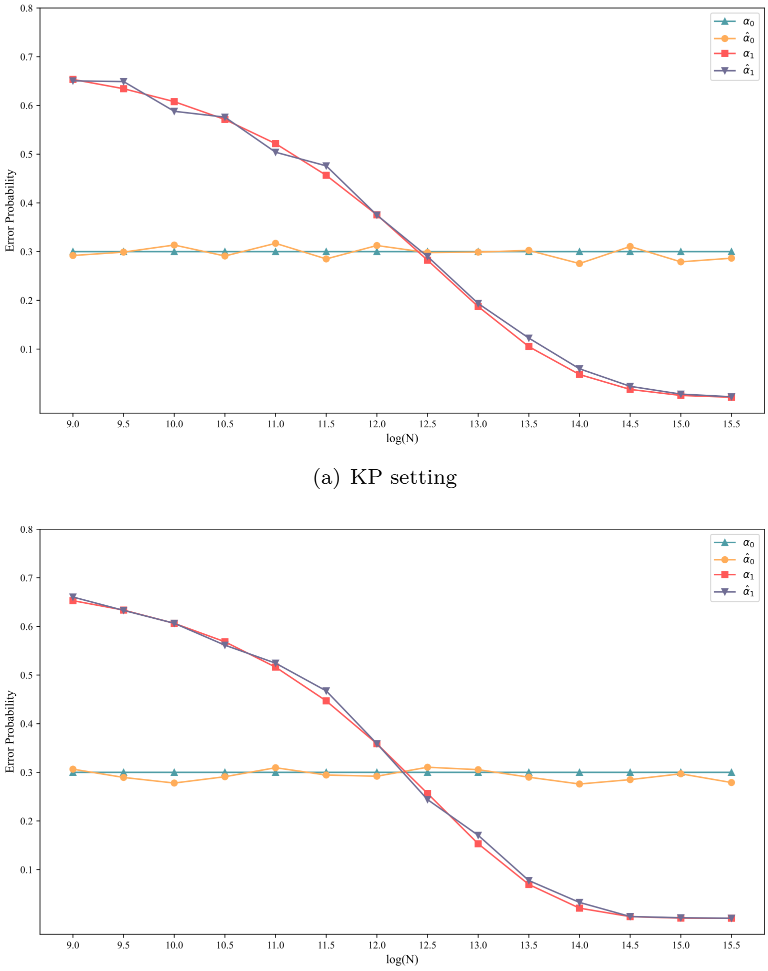
Both experiments follow a similar process, although they adopt different statistics. Let's take Type-I experiment as an example. Setting $\alpha_0 = 0.3$ and choosing different values for N, we can obtain α_1 and τ according to Corollary 1 due to $c = 0$. In each test, we independently choose N (distinct) plaintexts and query for their corresponding ciphertexts under the same randomly chosen right key. Next, we follow the framework proposed by Flórez-Gutiérrez [Fló22] to compute $\widehat{cor}_{(s)}$ under each key guess, where the output of the active Sbox in the fifth round (*i.e.* the first key recovery round) is restricted to take values not included in $\{\mathtt{3}, \mathtt{5}, \mathtt{B}, \mathtt{D}\}$. After obtaining $\widehat{cor}_{(s)}$ and comparing it with τ, we can decide whether the guessed key is right. By launching this test 2000 times, we can obtain experimental error probabilities $\hat{\alpha_0}$ and $\hat{\alpha_1}$. Therefore, we can compare them with theoretical ones α_0 and α_1, which is shown in Fig. 2. Similarly, for Type-II experiment, we show their comparisons in Fig. 3, where $\bar{\sigma}$ in Corollary 2 is set to be the arithmetic mean of $p_i(ELP_i - c_i^2)$. From these two figures, one can see that the test results for error probabilities are in good accordance with those for the theoretical model. Thus, our statistical models are constructed accurately.



(a) KP setting

(b) DKP setting

Figure 2: Experimental results of the statistical model in Sect. 3.1 with `SmallPRESENT-[4]`.



(a) KP setting

(b) DKP setting

Figure 3: Experimental results of the statistical model in Sect. 3.2 with `SmallPRESENT-[4]`.

4 Non Full-Codebook Attack on 29-Round PRESENT-128

In this section, we follow the affine pruned Walsh transform technique [Fló22] to mount a 29-round multiple linear key recovery attack on PRESENT-128 without using the full-codebook. This attack is based on our newly constructed statistical models depicted in Sect. 3, as well as detailed complexity analysis when using each linear hull. Note that this is the best key recovery attack on PRESENT-128.

4.1 Linear Hulls Used in the Attack

We adopt one of the three sets of the 24-round linear hulls introduced in [FN20], which is Set II. All these linear hulls are listed in Table 4. Different with previous notations, the output masks and S-Boxes here are those after the last `pLayer`, *i.e.* the actual outputs of the 24-round distinguisher. Hereafter, we also use the four-tuple $[u, v, S_u, S_v]$ to represent a specific linear hull, whose input mask is u, input S-Box is S_u, output mask is v, and output S-Box is S_v.

According to the Hamming weight of input masks, all these linear hulls can be divided

Table 4: The 24-round linear hulls used in attacking 29-round PRESENT-128 belonging to Set II of [FN20]. Here, output masks and S-Boxes are those after the last `pLayer`.

Group	Input Mask	Input S-Box	Output Mask	Output S-Box	Qty.	Filtering Ratio	24R ELP
A	A	5,6,9,10	2	5,7,13,15	16	3/4	$2^{-65.1}$
	A	5,6,9,10	8	5,7,13,15	16	1/2	
B	C	5,6,9,10	2	5,7,13,15	16	3/4	$2^{-65.6}$
	C	5,6,9,10	8	5,7,13,15	16	1/2	
C	A	5,6,9,10	4	5,7,13,15	16	3/4	$2^{-65.8}$
	A	13,14	2	5,7,13,15	8	3/4	
	A	13,14	8	5,7,13,15	8	1/2	
D	2,4	5,6,9,10	2	5,7,13,15	32	1	2^{-66}
	2,4	5,6,9,10	8	5,7,13,15	32	1	
E	C	5,6,9,10	4	5,7,13,15	16	3/4	$2^{-66.3}$
	C	13,14	2	5,7,13,15	8	3/4	
	C	13,14	8	5,7,13,15	8	1/2	
F	A	13,14	4	5,7,13,15	8	3/4	$2^{-66.5}$
G	2,4	5,6,9,10	4	5,7,13,15	32	1	$2^{-66.7}$
	8	5,6,9,10	2	5,7,13,15	16	1	
	8	5,6,9,10	8	5,7,13,15	16	1	
	2,4	13,14	2	5,7,13,15	16	1	
	2,4	13,14	8	5,7,13,15	16	1	
				Total	296		$2^{-57.8}$

into two types: *Type I*, including 160 linear hulls with input masks of Hamming weight 1 and *Type II*, including 136 linear hulls with input masks of Hamming weight 2. In other words, *Type I* is composed of Group D and G, while the other groups constitute *Type II*.

To mount the 29-round attack, we add two rounds before these 24-round linear hulls, and appending three rounds after. Therefore, this key recovery procedure involves some bits in round keys K_1, K_2, K_{28}, K_{29} and K_{30}. For linear hulls in *Type I*, there are 16 bits in K_1, 4 bits in K_2, 4 bits in K_{28}, 16 bits in K_{29} and 64 bits in K_{30}; while for those in *Type II*, they are 32, 8, 4, 16, 64, respectively. For better understanding, we show two examples in Fig. 4.

4.2 Detailed Key Recovery Procedure

For the purpose of reducing time complexity, we will apply the affine pruning technique to linear hulls in *Type II*. That is, we will reject some data when evaluating experimental correlations using these hulls. Detailed rejection rules follow those used in [Fló22, Table 4], and filtering ratios p_i of each hull have been shown in Table 4. According to Sect. 3.2, one has to compute the statistic $\mathcal{C} = \sum_i \frac{\mathcal{C}_i^2}{p_i}$ where $\mathcal{C}_i$ denotes the statistic evaluated for the i-th linear hull.

For a single linear hull, we use $(k_1, k_2, k_{28}, k_{29}, k_{30})$ to denote specific key bits needed to be guessed in each key recovery rounds. Note that different hulls may share the same key guess bits. For linear hulls in *Type I*, they can be separated into 24 groups; while for those in *Type II*, they are divided into 16 groups. In each group, one need to guess the same key bits. Considering the key schedule, if we know the 64-bit k_{30}, we can deduce some key bits in k_1, k_2, k_{28} and k_{29}. In our attack, we will construct a table Tk for the k-th group, which is indexed by these involved key bits and used to record intermediate values in evaluating $\mathcal{C}_i$. Namely, we denote $T0$, $T1$, $\cdots$, $T23$ as tables related to linear hulls in *Type I*; while $T24$, $T25$, $\cdots$, $T39$ are those for hulls in *Type II*. Denote that n_k bits

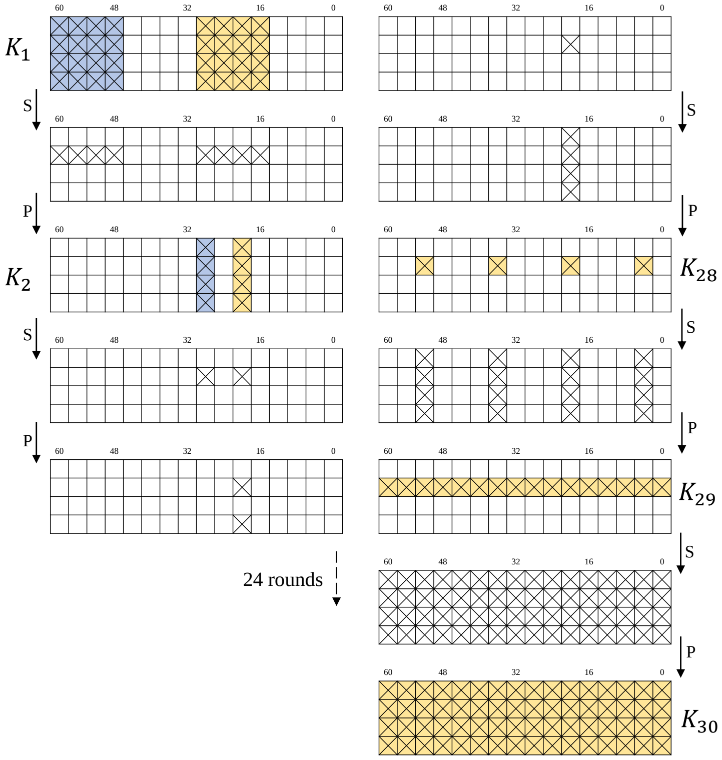


Figure 4: Key Bits involved in two different hulls. Bits in yellow color represent key bits needed to be guessed for the hull [2,2,5,5], while both blue and yellow ones indicate those for the hull [A,2,5,5].

can be deduced from k_{30}. Size of each table Tk is 2^{104-n_k} for $k \in \{0, 1, \cdots, 23\}$ or 2^{124-n_k} for $k \in \{24, 25, \cdots, 39\}$. Detailed information of these tables are shown in Appendix E. In our attack, we have to store these 40 tables, which costs $2^{97.91}$ registers in total.

When evaluating $\mathcal{C}_i$ for the i-th linear hull, (k_1, k_{30}) are outer key bits, (k_2, k_{28}, k_{29}) are inner key bits, and $(k_1, k_{30}, k_2, (k_{28}, k_{29}))$ corresponds to $(K_1^O, K_2^O, K_1^I, K_2^I)$. Assuming that we have known $K_1^I||K_2^I$, some bits of $K_1^O||K_2^O$ may be deduced according to the key schedule. Here, we denote m_i bits of $K_1^O||K_2^O$ can be deduced for the i-th hull. As shown in [Fló22], we can divide $Y_1||Y_2$ into two subspaces with size $2^{32+64-16} = 2^{80}$ when dealing with *Type-II* linear hulls whose output mask is 2 or 4, while only one subspace with size 2^{80} exits for those in *Type-II* with output mask 8. For *Type-I* hulls, the size of $Y_1||Y_2$ is $2^{16+64} = 2^{80}$. Hereafter, we use g_i to denote the number of subspaces for the i-th hull, where each subspace has size 2^{s_i}, *i.e.* 2^{80} here. During the above evaluation, we can firstly use a fixed $K_1^I||K_2^I$ to obtain necessary Walsh coefficients, and then one can obtain corresponding coefficients for arbitrary $K_1^I||K_2^I$ by changing its sign. This is ensured according to [Fló22, Corollary 14] relying on the fact that only after three rounds, PRESENT will get a full diffusion.

Given N plaintext-ciphertext pairs, we firstly update Tk tables for every linear hull, and then one can recover the master key with these Tk tables using our statistical models.

Update Tk table for the i-th linear hull. According to Appendix E, one can see which Tk table is related to this linear hull. Thus, we will use N data to update this Tk table with the i-th linear hull by following steps. To be more clear, we construct an automatic tool to generate all necessary parameters of each hull, and list them in Appendix F.

S1. Compute $S_{Y_1}^{K_1^I}$ and $S_{Y_2}^{K_2^I}$ with FWT, where K_1^I and K_2^I can be fixed to be zero without loss of generality during **S1** to **S3**. This step costs $|Y_1|2^{|Y_1|} + |Y_2|2^{|Y_2|}$ additions, and $2^{|Y_1|} + 2^{|Y_2|}$ registers.

S2. For the j-th subspace of $Y_1||Y_2$, we can get array $\widehat{A}[Y_1, Y_2]$ using the fast Walsh transform pruned to affine subspaces algorithm [Fló22], which is depicted in Appendix I. However, to gain lower time costs and combining it with the next Walsh transform, we return g in Line 17 of the above algorithm as $\widehat{A}_j$. Thus, this step costs $g_iN + g_it_i2^{t_i}$ additions with $t_i = 80$ according to [Fló22, Proposition 7], and needs $g_i2^{t_i}$ registers.

S3. For the j-th subspace of $Y_1||Y_2$, we firstly determine whether $S_{Y_1}^{K_1^I} \neq 0$ and $S_{Y_2}^{K_2^I} \neq 0$. If so, after computing $\widehat{A}_jS_{Y_1}^{K_1^I}S_{Y_2}^{K_2^I}$, and proceeding Line 15 and 16, one can return g as H_j. The proportion of the condition is $Pr_{con} = (10/16)^{20}$ according to the Walsh spectrum of S-Box. Thus, this step costs $2g_i2^{s_i}(10/16)^{20}$ multiplications and $g_i2^{s_i}(10/16)^{20}$ additions. Note that for *Type I* hulls, we will directly compute H_j as $\widehat{A}_jS_{Y_1}^{K_1^I}S_{Y_2}^{K_2^I}$. Hence, for those hulls, this step costs $2g_i2^{s_i}$ multiplications.

S4. Under each guess of $K_1^I||K_2^I$, for the j-th subspace, we firstly change the sign of H_j according to $K_1^I||K_2^I$ and then use FWT to get $\widehat{H}_j$. This costs $2^{|K_1^I|+|K_2^I|}\sum_{j=1}^{g_i} r_i^j 2^{r_i^j}$ additions and uses $\sum_{j=1}^{g_i} 2^{r_i^j}$ registers, where r_i^j will be different for different subspaces. It can be deduced with Proposition 7 in [Fló22]. Next, we traverse the index of Tk, get corresponding bits of $K_1^I||K_2^I$ from this index, and check if these bits are the same as previous guessed ones. If so, for each subspace of $Y_1||Y_2$, we proceed Line 18 to 20, get $\widehat{h}_j$ and then add it to Cor_{tmp}. Finally, we update the value of Tk in this index by adding Cor_{tmp}^2/p_i. This step need $2^{n_i}g_i$ additions, and $2 \cdot 2^{n_i}$ multiplications.

Guess the master key. After updating Tk tables with all linear hulls, we can use them to compute the statistic $\mathcal{C}_{k_T}$ for every possible global key guess k_T. Here, we choose k_T as the 115-bit key colored with red in Fig. 6, which is composed of 113-bit in KS_{29}, 1-bit KS_1 and 1-bit KS_2. From k_T, one can deduce all key bits of $K_1^O||K_2^O||K_1^I||K_2^I$, which are needed in the key recovery procedure, using its key schedule. Next, we traverse all these 40 tables Tk, get corresponding values under this $K_1^O||K_2^O||K_1^I||K_2^I$, and then add them to $\mathcal{C}_{k_T}$. This costs $40 \cdot 2^{115} = 2^{120.32}$ additions. Once getting a $\mathcal{C}_{k_T}$ for a global key guess k_T, it is compared with τ to see whether it is a candidate key. Setting $\alpha_1 = 2^{-a}$, about $2^{115}\alpha_1 = 2^{115-a}$ $\mathcal{C}_{k_T}$ satisfies this condition, and will be kept as the right key candidates. After traversing the other 15-bit unknown key in KS_{29}, one can compute the 1-bit KS_1 and 1-bit KS_2, which costs $2^{115-a} \cdot 2^{15} \cdot (1/8) = 2^{127-a}$ times of 29-round encryptions. Averagely, there will be $2^{115-a+15-2}$ keys left and need to be further verified with new plaintext-ciphertext pair. This step needs 2^{128-a} times of 29-round encryptions.

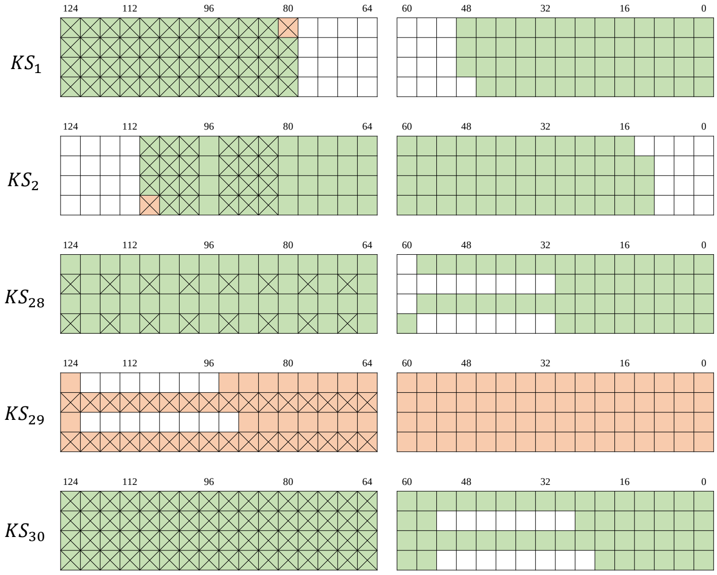


Figure 5: Determining involved key bits for all linear hulls (crossed out in the figure) with as fewer guesses as possible when attacking PRESENT-128. We can deduce the (light) green bits if we know the 115 key bits highlighted in (dark) red.

Analysis of attack complexities. Using the statistical model proposed in Sect. 3.2, 62.83% success probability could be achieved with $2^{62.88}$ DKP and $\alpha_1 = 2^{-a} = 2^{-2.26}$. For each hull, time complexity of updating its corresponding table Tk can be computed with information given in Appendix F. In total, the time complexity of the whole attack is composed of $2^{121.39}$ additions, $2^{102.07}$ multiplications and $2^{126.32}$ times of 29-round encryptions. A simple lower bound on the cost of a 29-round PRESENT encryption is $2 \cdot 64 \cdot 29 + 64 = 3776$ binary operations, while an addition is 128 and a multiplication is 2143 [FN20]. Therefore, the final time complexity is at most $2^{126.33}$ times of 29-round encryptions. The dominant memory cost comes from storing 40 tables Tk, which needs $2^{97.91}$ registers. Note that the same memory could be reused during the update process of table Tk for each hull. In this procedure, the highest memory complexity is 2^{81} registers, which can be ignored.

5 First Key Recovery Attack on 29-Round PRESENT-80

In this section, we provide the first 29-round attack on PRESENT-80, which benefits from subtly chosen 24-round linear hulls with detailed analysis of its complexity reduction, as well as our newly proposed statistical models.

To mount the 29-round attack, two and three rounds are added before and after the 24-round linear hulls, respectively. Linear hulls used in this attack are depicted in Table 5, which are chosen from those given in [FN20] in a trade-off manner. When picking each linear hull, we try to ensure that the arithmetic mean of $p_i ELP_i$ of all chosen hulls can be larger while extra time complexity caused by this hull should not increase the final complexity too fast. Such trade-off can be effectively obtained using our constructed automatic tool, which can provide detailed analysis of complexity reduction of each linear hull. Attack parameters for each linear hull are depicted in Appendix H.

Table 5: The 24-round linear hulls used in attacking 29-round PRESENT-80, which are chosen from those proposed by [FN20].

Linear Hull	ELP	p_i	**Linear Hull**	ELP	p_i
[4, 2, 5, 13]	$2^{-66.0}$	3/4	[4, 2, 5, 15]	$2^{-66.0}$	3/4
[4, 2, 9, 13]	$2^{-66.0}$	3/4	[4, 2, 9, 15]	$2^{-66.0}$	3/4
[4, 8, 5, 5]	$2^{-66.0}$	1/2	[4, 8, 5, 7]	$2^{-66.0}$	1/2
[4, 8, 9, 5]	$2^{-66.0}$	1/2	[4, 8, 9, 7]	$2^{-66.0}$	1/2
[4, 4, 5, 13]	$2^{-66.7}$	3/4	[4, 4, 5, 15]	$2^{-66.7}$	3/4
[4, 4, 9, 13]	$2^{-66.7}$	3/4	[4, 4, 9, 15]	$2^{-66.7}$	3/4
[4, 2, 13, 13]	$2^{-66.7}$	3/4	[4, 2, 13, 15]	$2^{-66.7}$	3/4
[4, 8, 13, 5]	$2^{-66.7}$	1/2	[4, 8, 13, 7]	$2^{-66.7}$	1/2

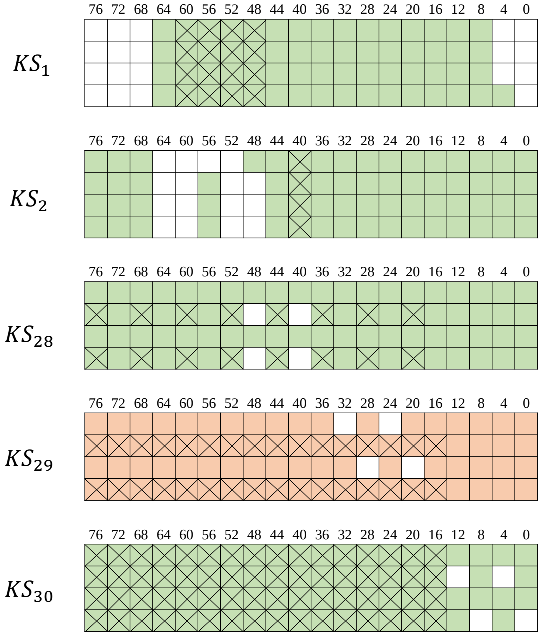


Figure 6: Determining involved key bits for all linear hulls (crossed out in the figure) with as fewer guesses as possible when attacking PRESENT-80. We can deduce the (light) green bits if we know the 76 key bits highlighted in (dark) red.

Similar with the 29-round attack on PRESENT-128, we also construct some Tk tables, whose index is involved key bits and stores intermediate values in evaluating the final statistic $\mathcal{C}$. Here, we adopt four tables $T0$, $T1$, $T2$ and $T3$. Detailed information of these tables are provided in Appendix G. During the attack, these four tables need to be stored and thus need $4 \cdot 2^{69} = 2^{71}$ registers in total. When updating these Tk tables, the probability Pr_{con} occurs in **S3** is changed to $(10/16)^{15}$. After obtaining these updated Tk tables, one can use them to recover the right key bits as follows. As shown in Fig. 6, we choose k_T as 76-bit KS_{29} to compute the statistic $\mathcal{C}$. Setting $\alpha_1 = 2^{-a} = 2^{-1.39}$ and $N = 2^{63.93}$ DKP, we can mount such attack with success probability 51.23%. Time complexity of the whole attack process is $2^{80.99}$ additions, 2^{74} multiplications and $2^{78.61}$ times of 29-round encryptions. In other words, the time complexity is at most $2^{78.87}$ times of 29-round encryptions. Memory cost is dominated by storing Tk, thus is 2^{71} registers.

6 Conclusion and Future Work

Following the affine pruned Walsh transform framework, we introduce improved linear key recovery attacks on both PRESENT-80 and PRESENT-128 based on two ideas. The first one is that we have made detailed analysis of complexity reduction for each linear hull, thus one can decide to use which linear hulls with the aim of obtaining better key recovery attacks. This procedure is proceeded automatically with an tool designed by us. Our 29-round attack on PRESENT-80 mainly benefits from this idea, where we subtly choose some 24-round linear hulls to get the balance between attack complexities and success probabilities. Without such detailed analysis, trade-offs may be not easy to efficiently achieve. The second idea is constructing a dedicated statistical model for such affine pruned Walsh transform technique, since there exist deviations from statistical models built for classical linear attacks when some data are artificially rejected. With this newly proposed statistical models, we can construct the accurate relation between data complexity and success probability, which gives the chance to make further trade-offs. Based on our statistical models, we can mount 29-round attacks on PRESENT-80 and PRESENT-128 without using full-codebook. Both attacks are the best ones so far. In future, there are plenty of interesting works. On the one hand, further applications on other ciphers using this technique with our statistical models are encouraged. On the other hand, statistical behaviors behind this technique when combing with other variants of linear attacks are worth to be discovered, such as for the multidimensional linear attacks or multivariate ones, or even for linear attacks using (multiple) zero-correlation linear hulls.

References

[AC09] Martin R. Albrecht and Carlos Cid. Algebraic techniques in differential cryptanalysis. In Orr Dunkelman, editor, *FSE 2009*, volume 5665 of *LNCS*, pages 193–208. Springer, 2009.

[BCQ04] Alex Biryukov, Christophe De Cannière, and Michaël Quisquater. On multiple linear approximations. In Matthew K. Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 1–22. Springer, 2004.

[BJV04] Thomas Baignères, Pascal Junod, and Serge Vaudenay. How far can we go beyond linear cryptanalysis? In Pil Joong Lee, editor, *ASIACRYPT 2004*, volume 3329 of *LNCS*, pages 432–450. Springer, 2004.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid

Verbauwhede, editors, *CHES 2007*, volume 4727 of *LNCS*, pages 450–466. Springer, 2007.

[BN16] Céline Blondeau and Kaisa Nyberg. Improved parameter estimates for correlation and capacity deviates in linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(2):162–191, 2016.

[BN17] Céline Blondeau and Kaisa Nyberg. Joint data and key distribution of simple, multiple, and multidimensional linear cryptanalysis test statistic and its impact to data complexity. *Des. Codes Cryptogr.*, 82(1-2):319–349, 2017.

[BTV18] Andrey Bogdanov, Elmar Tischhauser, and Philip S. Vejre. Multivariate profiling of hulls for linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2018(1):101–125, 2018.

[Cho10] Joo Yeon Cho. Linear cryptanalysis of reduced-round PRESENT. In Josef Pieprzyk, editor, *CT-RSA 2010*, volume 5985 of *LNCS*, pages 302–317. Springer, 2010.

[Coe20] Carlos A. Coelho. *On the Distribution of Linear Combinations of Chi-Square Random Variables*, pages 211–252. Springer International Publishing, Cham, 2020.

[CS09] Baudoin Collard and François-Xavier Standaert. A statistical saturation attack against the block cipher PRESENT. In Marc Fischlin, editor, *CT-RSA 2009*, volume 5473 of *LNCS*, pages 195–210. Springer, 2009.

[CSQ07] Baudoin Collard, François-Xavier Standaert, and Jean-Jacques Quisquater. Improving the time complexity of matsui's linear cryptanalysis. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *ICISC 2007*, volume 4817 of *LNCS*, pages 77–88. Springer, 2007.

[Fló22] Antonio Flórez-Gutiérrez. Optimising linear key recovery attacks with affine walsh transform pruning. In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022*, volume 13794 of *LNCS*, pages 447–476. Springer, 2022.

[FN20] Antonio Flórez-Gutiérrez and María Naya-Plasencia. Improving key-recovery in linear attacks: Application to 28-round PRESENT. In Anne Canteaut and Yuval Ishai, editors, *EUROCRYPT 2020*, volume 12105 of *LNCS*, pages 221–249. Springer, 2020.

[HCN08] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional linear cryptanalysis of reduced round serpent. In Yi Mu, Willy Susilo, and Jennifer Seberry, editors, *ACISP 2008*, volume 5107 of *LNCS*, pages 203–215. Springer, 2008.

[HCN09] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Multidimensional extension of Matsui's algorithm 2. In Orr Dunkelman, editor, *Fast Software Encryption, 16th International Workshop, FSE 2009, Leuven, Belgium, February 22-25, 2009, Revised Selected Papers*, volume 5665 of *LNCS*, pages 209–227. Springer, 2009.

[HVLN15] Jialin Huang, Serge Vaudenay, Xuejia Lai, and Kaisa Nyberg. Capacity and data complexity in multidimensional linear attack. In Rosario Gennaro and Matthew Robshaw, editors, *CRYPTO 2015*, volume 9215 of *LNCS*, pages 141–160. Springer, 2015.

[JR94] Burton S. Kaliski Jr. and Matthew J. B. Robshaw. Linear cryptanalysis using multiple approximations. In Yvo Desmedt, editor, *CRYPTO 1994*, volume 839 of *LNCS*, pages 26–39. Springer, 1994.

[JSZW09] Jorge Nakahara Jr., Pouyan Sepehrdad, Bingsheng Zhang, and Meiqin Wang. Linear (hull) and algebraic cryptanalysis of the block cipher PRESENT. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *CANS 2009*, volume 5888 of *LNCS*, pages 58–75. Springer, 2009.

[KH11] Damir Kalpić and Nikica Hlupić. *Multivariate Normal Distributions*, pages 907–910. Springer Berlin Heidelberg, Berlin, Heidelberg, 2011.

[Lea10] Gregor Leander. Small scale variants of the block cipher PRESENT. *IACR Cryptol. ePrint Arch.*, page 143, 2010.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT 1993*, volume 765 of *LNCS*, pages 386–397. Springer, 1993.

[Nyb94] Kaisa Nyberg. Linear approximation of block ciphers. In Alfredo De Santis, editor, *EUROCRYPT 1994*, volume 950 of *LNCS*, pages 439–444. Springer, 1994.

[Ohk09] Kenji Ohkuma. Weak keys of reduced-round PRESENT for linear cryptanalysis. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *SAC 2009*, volume 5867 of *LNCS*, pages 249–265. Springer, 2009.

[ÖVTK09] Onur Özen, Kerem Varici, Cihangir Tezcan, and Çelebi Kocair. Lightweight block ciphers revisited: Cryptanalysis of reduced round PRESENT and HIGHT. In Colin Boyd and Juan Manuel González Nieto, editors, *ACISP 2009*, volume 5594 of *LNCS*, pages 90–107. Springer, 2009.

[Wan08] Meiqin Wang. Differential cryptanalysis of reduced-round PRESENT. In Serge Vaudenay, editor, *AFRICACRYPT 2008*, volume 5023 of *LNCS*, pages 40–49. Springer, 2008.

[Wei82] Neil A. Weiss. Introductory statistics. 1982.

[ZRHD08] Muhammad Reza Z'aba, Håvard Raddum, Matthew Henricksen, and Ed Dawson. Bit-pattern based integral attack. In Kaisa Nyberg, editor, *FSE*, volume 5086 of *LNCS*, pages 363–381. Springer, 2008.

[ZZ15] Lei Zheng and Shao-Wu Zhang. FFT-based multidimensional linear attack on PRESENT using the 2-bit-fixed characteristic. *Secur. Commun. Networks*, 8(18):3535–3545, 2015.

A Key Schedules of PRESENT

B Proof of Lemma 1

Proof. Denote $h(\tilde{x}) : \mathbb{F}_2^n \to \mathbb{F}_2^{|X_1|+|X_2|+2}$ as the vectorial Boolean function. Let $X_{1,i}$ and $X_{2,i}$ denote the i-th bit of X_1 and X_2, respectively. Each component $h_i(\tilde{x})$ is

$$h_0(\tilde{x}) = X_{1,0},\ h_1(\tilde{x}) = X_{1,1},\ \cdots,\ h_{|X_1|-1}(\tilde{x}) = X_{1,|X_1|-1},$$

$$h_{|X_1|}(\tilde{x}) = X_{2,0},\ h_{|X_1|+1}(\tilde{x}) = X_{2,1},\ \cdots,\ h_{|X_1|+|X_2|-1}(\tilde{x}) = X_{2,|X_1|-1},$$

Algorithm 1: Key Schedule of PRESENT-80

```
for $i \to 1$ to 31 do
    $K_i \to K[79, 78, \cdots, 16]$;
    $K \to K \ggg 19$;
    $K[79, 78, 77, 76] \to S(K[79, 78, 77, 76])$;
    $K[19, \cdots, 15] \to K[19, \cdots, 15] \oplus RC_i$;
$K_{32} \to K[79, 78, \cdots, 16]$;
```

Algorithm 2: Key Schedule of PRESENT-128

```
for $i \to 1$ to 31 do
    $K_i \to K[127, 126, \cdots, 64]$;
    $K \to K \lll 61$;
    $K[127, 126, 125, 124] \to S(K[127, 126, 125, 124])$;
    $K[123, 122, 121, 120] \to S(K[123, 122, 121, 120])$;
    $K[66, \cdots, 62] \to K[66, \cdots, 62] \oplus RC_i$;
$K_{32} \to K[127, 126, \cdots, 64]$;
```

$$h_{|X_1|+|X_2|} = f_0(\tilde{x}),\ h_{|X_1|+|X_2|+1} = g_0(E_K(\tilde{x})).$$

Suppose the probability that $h(\tilde{x}) = \eta$ is $\hat{p}_\eta$ when $\tilde{x} \in D$, we can deduce that

$$\begin{aligned}
\widehat{A}[Y_1, Y_2] &= \sum_{X_1, X_2} (-1)^{\langle Y_1, X_1\rangle \oplus \langle Y_2, X_2\rangle} A[X_1, X_2] \\
&= \sum_{\substack{\tilde{x} \in D, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{\langle Y_1, X_1\rangle \oplus \langle Y_2, X_2\rangle \oplus f_0(\tilde{x}) \oplus g_0(E_K(\tilde{x}))} \\
&= \sum_{\substack{\tilde{x} \in D, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{\langle Y_1 || Y_2 || 11, h(\tilde{x})\rangle} \\
&= \sum_{\eta \in \mathbb{F}_2^{|X_1|+|X_2|+2}} (-1)^{\langle Y_1 || Y_2 || 11, \eta\rangle} N \hat{p}_\eta.
\end{aligned}$$

The last equality comes from [HCN08, Lemma 1].

Denote $\hat{T}_\eta = N\hat{p}_\eta$, which is the number of $\tilde{x} \in D$ that fulfills $h(\tilde{x}) = \eta$. Besides, we have $\sum_\eta \hat{T}_\eta = N$. Thus, when $\tilde{x} \in D$ are chosen with known-plaintext (KP) sampling, statistic vector $(\hat{T}_0, \hat{T}_1, \cdots, \hat{T}_{2^{|X_1|+|X_2|+2}-1})$ will follow the multinomial distribution; while in the distinct known-plaintext (DKP) sampling, it follows the multivariate hypergeometric distribution. Both distributions can then be approximated as multivariate normal ones. Denote q_η as the probability that $h(\tilde{x}) = \eta$ when $\tilde{x} \in \mathbb{F}_2^n$. Expectation and variance of each $\hat{T}_\eta$ are Nq_η and $NBq_\eta(1-q_\eta)$, respectively. Covariance between $\hat{T}_{\eta_1}$ and $\hat{T}_{\eta_2}$ is $-NBq_{\eta_1}q_{\eta_2}$. Since all $\widehat{A}[Y_1, Y_2]$ are linear combinations of $\hat{T}_\eta$, $(\widehat{A}[0, 0], \cdots, \widehat{A}[2^{|Y_1|} - 1, 2^{|Y_2|} - 1])$ also follows the multivariate normal distribution [KH11]. Meanwhile, its expectation is

$$\begin{aligned}
E(\widehat{A}[Y_1, Y_2]) = &\sum_{\eta \in \mathbb{F}_2^{|X_1|+|X_2|+2}} (-1)^{\langle Y_1 || Y_2 || 11, \eta\rangle} \cdot E(\hat{T}_\eta) = N \sum_{\eta \in \mathbb{F}_2^{|X_1|+|X_2|+2}} (-1)^{\langle Y_1 || Y_2 || 11, \eta\rangle} q_\eta \\
=&N \frac{1}{2^n} \sum_{\substack{\tilde{x} \in \mathbb{F}_2^n, \\ \tilde{x} \to X_1, E_K(\tilde{x}) \to X_2}} (-1)^{\langle Y_1 || Y_2 || 11, h(\tilde{x})\rangle} = NC_{[Y_1, Y_2]},
\end{aligned}$$

while the third equality also comes from [HCN08, Lemma 1]. Covariance between $\widehat{A}[Y_1^a, Y_2^a]$ and $\widehat{A}[Y_1^b, Y_2^b]$ is

$$
\begin{aligned}
&Cov(\widehat{A}[Y_1^a, Y_2^a], \widehat{A}[Y_1^b, Y_2^b]) = \sum_{\eta_a}\sum_{\eta_b}(-1)^{\langle Y_1^a||Y_2^a||11,\eta_a\rangle \oplus \left\langle Y_1^b||Y_2^b||11,\eta_b\right\rangle} Cov(\hat{T}_{\eta_a}, \hat{T}_{\eta_b})\\
=&\sum_{\eta}(-1)^{\left\langle Y_1^a||Y_2^a||11 \oplus Y_1^b||Y_2^b||11,\eta\right\rangle} NBq_\eta - \sum_{\eta_a}\sum_{\eta_b}(-1)^{\langle Y_1^a||Y_2^a||11,\eta_a\rangle \oplus \left\langle Y_1^b||Y_2^b||11,\eta_b\right\rangle} NBq_{\eta_a}q_{\eta_b}\\
=&NB\frac{1}{2^n}\sum_{\substack{\tilde{x}\in\mathbb{F}_2^n,\\ \tilde{x}\rightarrow X_1, E_K(\tilde{x})\rightarrow X_2}}(-1)^{\left\langle (Y_1^a\oplus Y_1^b)||(Y_2^a\oplus Y_2^b)||00, h(\tilde{x})\right\rangle} - NBC_{[Y_1^a,Y_2^a]}C_{[Y_1^b,Y_2^b]}\\
=&NB\delta_{[Y_1^a\oplus Y_1^b, Y_2^a\oplus Y_2^b]} - NBC_{[Y_1^a,Y_2^a]}C_{[Y_1^b,Y_2^b]}.
\end{aligned}
$$

Note that the third equality can be obtained from [HCN08, Lemma 1]. □

C Relation between Data Complexity and Error Probabilities when $c \neq 0$ in the Classical Setting

To deduce this relation, we have to perform a statistic test which can decide whether the obtained statistic $\widehat{cor}_{(s)}$ is computed under the right key or a wrong key guess. In this test, we compare $\widehat{cor}_{(s)}$ to a threshold value τ. When $c > 0$, we regard the guessed key is possibly right if $\widehat{cor}_{(s)} > \tau$, while it's a wrong key otherwise. When $c < 0$, the decision rule is a little different. In this case, we will regard it is possibly right if $\widehat{cor}_{(s)} < \tau$. Hence, one can obtain Corollary 3. Its proof is similar with Corollary 1, thus we omit it.

Corollary 3. *Denote α_0 as the probability of rejecting the right key, and α_1 as the probability of accepting a wrong key. When $c > 0$, the number of plaintexts needed is*

$$
N = \begin{cases} M_1(\alpha_0, \alpha_1), & \textit{KP Sampling,}\\ 2^n\dfrac{M_1(\alpha_0,\alpha_1)}{2^n - 1 + M_1(\alpha_0,\alpha_1)}, & \textit{DKP Sampling,}\end{cases}
$$

and the threshold value is

$$
\tau = \#Q_K 2^{-n}c + q_{\alpha_0}\sqrt{\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2)},
$$

where $M_1(\alpha_0, \alpha_1)$ equals to

$$
\frac{2^{2n}(q_{\alpha_0}^2 - q_{1-\alpha_1}^2) + 2c\#Q_K 2^n q_{\alpha_0}}{2^n(q_{1-\alpha_1}^2 - q_{\alpha_0}^2) - 2^n c^2\#Q_K - 2c\#Q_K q_{\alpha_0} - \#Q_K(ELP - c^2)(2^n q_{\alpha_0}^2 + 2c\#Q_K q_{\alpha_0})}
$$

with q_{α_0} and $q_{1-\alpha_1}$ as lower quantiles of $\mathbf{N}(0,1)$. When $c < 0$, N has the similar form except that it's $M_1(1-\alpha_0, 1-\alpha_1)$ rather than $M_1(\alpha_0, \alpha_1)$, while

$$
\tau = \#Q_K 2^{-n}c + q_{1-\alpha_0}\sqrt{\frac{B}{N}\#Q_K 2^{-n} + \#Q_K 2^{-2n} + (\#Q_K 2^{-n})^2(ELP - c^2)}.
$$

D Discussions on Statistical Models used in [Fló22]

In [Fló22], key recovery attacks on DES and 29-round PRESENT-128 are proposed. Both attacks use the statistical model from [BN17]. However, these two attacks belong to different cases. For the one mounted on DES, no data is artificially rejected during the evaluation of the experimental correlation. Hence, it still follows the model from [BN17]. While for 29-round PRESENT-128, different ratio of data is rejected when evaluating the experimental correlation under different linear hull. From [Fló22], the statistical model used is unclear. There is only one sentence: "the statistical model from [BN17] is used with careful consideration that the number of available plaintexts depends on the approximation". Note that [Fló22] takes the number of remaining data into consideration, which changes the form of the previous statistic constructed in [BN17]. Since no specific form of this statistic is given in [Fló22], one cannot check whether the claimed success probability 67% is correct or not. Meanwhile, with our statistical model constructed in Sect. 3, the success probability of this 29-round attack is only 40.11%, which is much lower than 67%. To be more clear, we also verified the applicability of the model from [BN17] in the classical linear setting where only one linear hull is used, when some data are rejected. We follow the same Type-I experiment proposed in Sect. 3.3 with the first linear hull shown in Table 3, where the experimental correlation is assumed to fulfill distributions from [BN17]. Fig. 7 shows the comparison between experimental error probabilities and theoretical ones. Hence, the statistical model from [BN17] cannot be directly used when some data are rejected even in the classical setting. This motivated us to study the statistical behavior behind this new technique. Compared with [Fló22], our newly constructed statistical model is clear and accurate (See Fig. 2 and 3). Since [Fló22] uses the models from [BN17], one can conclude that the estimation of data/time complexity and success probability is not accurate in [Fló22].

E Table Tk used in Attacking 29-round PRESENT-128

All Tk tables contains the 64-bit k_{30}. Bits colored in red are those can be deduced from the 64-bit k_{30}.

- Table $T0$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [20, 21, 22, 23]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [2, 2, 5, 5], [2, 4, 5, 5], [2, 8, 5, 5], [2, 2, 9, 5], [2, 4, 9, 5], [2, 8, 9, 5], [2, 2, 13, 5], [2, 8, 13, 5]
- Table $T1$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

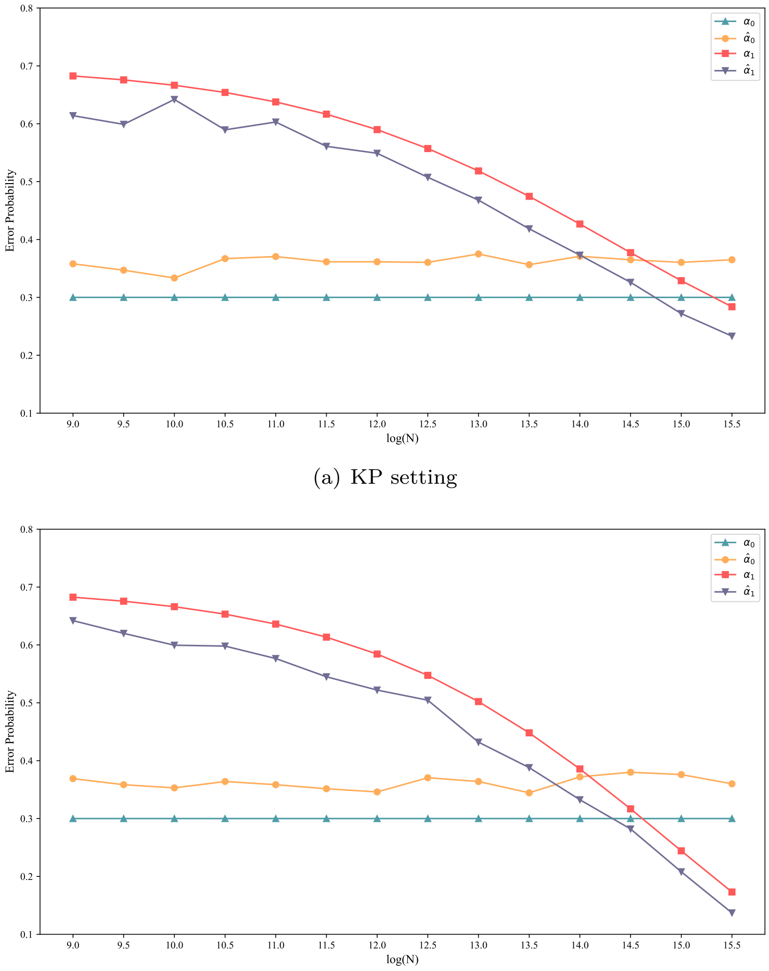
    k_2: [20, 21, 22, 23]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [2, 2, 5, 13], [2, 4, 5, 13], [2, 8, 5, 13], [2, 2, 9, 13], [2, 4, 9, 13], [2, 8, 9, 13], [2, 2, 13, 13], [2, 8, 13, 13]
- Table $T2$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]



(a) KP setting

(b) DKP setting

Figure 7: Experimental results of the statistical model (only one linear hull) from [BN17] with `SmallPRESENT-[4]` when some data are artificially rejected.

k_2: [20, 21, 22, 23]

k_{28}: [15, 31, 47, 63]

k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]

- Included Linear Hulls:

  [2, 2, 5, 15], [2, 4, 5, 15], [2, 8, 5, 15], [2, 2, 9, 15], [2, 4, 9, 15], [2, 8, 9, 15], [2, 2, 13, 15], [2, 8, 13, 15]

- Table $T3$ of size 2^{90}

  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [20, 21, 22, 23]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]

  - Included Linear Hulls:

    [2, 2, 5, 7], [2, 4, 5, 7], [2, 8, 5, 7], [2, 2, 9, 7], [2, 4, 9, 7], [2, 8, 9, 7], [2, 2, 13, 7], [2, 8, 13, 7]

- Table $T4$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [36, 37, 38, 39]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [2, 2, 6, 5], [2, 4, 6, 5], [2, 8, 6, 5], [2, 2, 10, 5], [2, 4, 10, 5], [2, 8, 10, 5], [2, 2, 14, 5], [2, 8, 14, 5]
- Table $T5$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [36, 37, 38, 39]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [2, 2, 6, 13], [2, 4, 6, 13], [2, 8, 6, 13], [2, 2, 10, 13], [2, 4, 10, 13], [2, 8, 10, 13], [2, 2, 14, 13], [2, 8, 14, 13]
- Table $T6$ of size 2^{91}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [36, 37, 38, 39]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [2, 2, 6, 15], [2, 4, 6, 15], [2, 8, 6, 15], [2, 2, 10, 15], [2, 4, 10, 15], [2, 8, 10, 15], [2, 2, 14, 15], [2, 8, 14, 15]
- Table $T7$ of size 2^{90}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31]

    k_2: [36, 37, 38, 39]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [2, 2, 6, 7], [2, 4, 6, 7], [2, 8, 6, 7], [2, 2, 10, 7], [2, 4, 10, 7], [2, 8, 10, 7], [2, 2, 14, 7], [2, 8, 14, 7]
- Table $T8$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]

    k_2: [24, 25, 26, 27]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [4, 2, 5, 5], [4, 4, 5, 5], [4, 8, 5, 5], [4, 2, 9, 5], [4, 4, 9, 5], [4, 8, 9, 5], [4, 2, 13, 5], [4, 8, 13, 5]

- Table $T9$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [13, 29, 45, 61]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [4, 2, 5, 13], [4, 4, 5, 13], [4, 8, 5, 13], [4, 2, 9, 13], [4, 4, 9, 13], [4, 8, 9, 13], [4, 2, 13, 13], [4, 8, 13, 13]
- Table $T10$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [15, 31, 47, 63]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [4, 2, 5, 15], [4, 4, 5, 15], [4, 8, 5, 15], [4, 2, 9, 15], [4, 4, 9, 15], [4, 8, 9, 15], [4, 2, 13, 15], [4, 8, 13, 15]
- Table $T11$ of size 2^{83}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [7, 23, 39, 55]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [4, 2, 5, 7], [4, 4, 5, 7], [4, 8, 5, 7], [4, 2, 9, 7], [4, 4, 9, 7], [4, 8, 9, 7], [4, 2, 13, 7], [4, 8, 13, 7]
- Table $T12$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [40, 41, 42, 43]
    k_{28}: [5, 21, 37, 53]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [4, 2, 6, 5], [4, 4, 6, 5], [4, 8, 6, 5], [4, 2, 10, 5], [4, 4, 10, 5], [4, 8, 10, 5], [4, 2, 14, 5], [4, 8, 14, 5]
- Table $T13$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [40, 41, 42, 43]
    k_{28}: [13, 29, 45, 61]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [4, 2, 6, 13], [4, 4, 6, 13], [4, 8, 6, 13], [4, 2, 10, 13], [4, 4, 10, 13], [4, 8, 10, 13], [4, 2, 14, 13], [4, 8, 14, 13]

- Table $T14$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]

    k_2: [40, 41, 42, 43]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [4, 2, 6, 15], [4, 4, 6, 15], [4, 8, 6, 15], [4, 2, 10, 15], [4, 4, 10, 15], [4, 8, 10, 15], [4, 2, 14, 15], [4, 8, 14, 15]
- Table $T15$ of size 2^{83}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]

    k_2: [40, 41, 42, 43]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [4, 2, 6, 7], [4, 4, 6, 7], [4, 8, 6, 7], [4, 2, 10, 7], [4, 4, 10, 7], [4, 8, 10, 7], [4, 2, 14, 7], [4, 8, 14, 7]
- Table $T16$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [28, 29, 30, 31]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [8, 2, 5, 5], [8, 8, 5, 5], [8, 2, 9, 5], [8, 8, 9, 5]
- Table $T17$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [28, 29, 30, 31]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [8, 2, 5, 13], [8, 8, 5, 13], [8, 2, 9, 13], [8, 8, 9, 13]
- Table $T18$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [28, 29, 30, 31]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [8, 2, 5, 15], [8, 8, 5, 15], [8, 2, 9, 15], [8, 8, 9, 15]
- Table $T19$ of size 2^{83}

  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [28, 29, 30, 31]
    k_{28}: [7, 23, 39, 55]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [8, 2, 5, 7], [8, 8, 5, 7], [8, 2, 9, 7], [8, 8, 9, 7]
- Table $T20$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [44, 45, 46, 47]
    k_{28}: [5, 21, 37, 53]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [8, 2, 6, 5], [8, 8, 6, 5], [8, 2, 10, 5], [8, 8, 10, 5]
- Table $T21$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [44, 45, 46, 47]
    k_{28}: [13, 29, 45, 61]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [8, 2, 6, 13], [8, 8, 6, 13], [8, 2, 10, 13], [8, 8, 10, 13]
- Table $T22$ of size 2^{84}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [44, 45, 46, 47]
    k_{28}: [15, 31, 47, 63]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [8, 2, 6, 15], [8, 8, 6, 15], [8, 2, 10, 15], [8, 8, 10, 15]
- Table $T23$ of size 2^{83}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [44, 45, 46, 47]
    k_{28}: [7, 23, 39, 55]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [8, 2, 6, 7], [8, 8, 6, 7], [8, 2, 10, 7], [8, 8, 10, 7]
- Table $T24$ of size 2^{95}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]
    k_2: [20, 21, 22, 23, 28, 29, 30, 31]
    k_{28}: [5, 21, 37, 53]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]

  - Included Linear Hulls:

    [a, 2, 5, 5], [a, 4, 5, 5], [a, 8, 5, 5], [a, 2, 9, 5], [a, 4, 9, 5], [a, 8, 9, 5], [a, 2, 13, 5], [a, 4, 13, 5], [a, 8, 13, 5]

- Table $T25$ of size 2^{95}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [20, 21, 22, 23, 28, 29, 30, 31]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [a, 2, 5, 13], [a, 4, 5, 13], [a, 8, 5, 13], [a, 2, 9, 13], [a, 4, 9, 13], [a, 8, 9, 13], [a, 2, 13, 13], [a, 4, 13, 13], [a, 8, 13, 13]

- Table $T26$ of size 2^{95}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [20, 21, 22, 23, 28, 29, 30, 31]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [a, 2, 5, 15], [a, 4, 5, 15], [a, 8, 5, 15], [a, 2, 9, 15], [a, 4, 9, 15], [a, 8, 9, 15], [a, 2, 13, 15], [a, 4, 13, 15], [a, 8, 13, 15]

- Table $T27$ of size 2^{94}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [20, 21, 22, 23, 28, 29, 30, 31]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [a, 2, 5, 7], [a, 4, 5, 7], [a, 8, 5, 7], [a, 2, 9, 7], [a, 4, 9, 7], [a, 8, 9, 7], [a, 2, 13, 7], [a, 4, 13, 7], [a, 8, 13, 7]

- Table $T28$ of size 2^{95}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [36, 37, 38, 39, 44, 45, 46, 47]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [a, 2, 6, 5], [a, 4, 6, 5], [a, 8, 6, 5], [a, 2, 10, 5], [a, 4, 10, 5], [a, 8, 10, 5], [a, 2, 14, 5], [a, 4, 14, 5], [a, 8, 14, 5]

- Table $T29$ of size 2^{95}

- Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
  k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

  k_2: [36, 37, 38, 39, 44, 45, 46, 47]

  k_{28}: [13, 29, 45, 61]

  k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
- Included Linear Hulls:
  [a, 2, 6, 13], [a, 4, 6, 13], [a, 8, 6, 13], [a, 2, 10, 13], [a, 4, 10, 13], [a, 8, 10, 13], [a, 2, 14, 13], [a, 4, 14, 13], [a, 8, 14, 13]

- Table $T30$ of size 2^{95}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [36, 37, 38, 39, 44, 45, 46, 47]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [a, 2, 6, 15], [a, 4, 6, 15], [a, 8, 6, 15], [a, 2, 10, 15], [a, 4, 10, 15], [a, 8, 10, 15], [a, 2, 14, 15], [a, 4, 14, 15], [a, 8, 14, 15]
- Table $T31$ of size 2^{94}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [36, 37, 38, 39, 44, 45, 46, 47]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [a, 2, 6, 7], [a, 4, 6, 7], [a, 8, 6, 7], [a, 2, 10, 7], [a, 4, 10, 7], [a, 8, 10, 7], [a, 2, 14, 7], [a, 4, 14, 7], [a, 8, 14, 7]
- Table $T32$ of size 2^{88}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [24, 25, 26, 27, 28, 29, 30, 31]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [c, 2, 5, 5], [c, 4, 5, 5], [c, 8, 5, 5], [c, 2, 9, 5], [c, 4, 9, 5], [c, 8, 9, 5], [c, 2, 13, 5], [c, 8, 13, 5]
- Table $T33$ of size 2^{88}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [24, 25, 26, 27, 28, 29, 30, 31]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]

  - Included Linear Hulls:

    [c, 2, 5, 13], [c, 4, 5, 13], [c, 8, 5, 13], [c, 2, 9, 13], [c, 4, 9, 13], [c, 8, 9, 13], [c, 2, 13, 13], [c, 8, 13, 13]

- Table $T34$ of size 2^{88}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [24, 25, 26, 27, 28, 29, 30, 31]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [c, 2, 5, 15], [c, 4, 5, 15], [c, 8, 5, 15], [c, 2, 9, 15], [c, 4, 9, 15], [c, 8, 9, 15], [c, 2, 13, 15], [c, 8, 13, 15]

- Table $T35$ of size 2^{87}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [24, 25, 26, 27, 28, 29, 30, 31]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [c, 2, 5, 7], [c, 4, 5, 7], [c, 8, 5, 7], [c, 2, 9, 7], [c, 4, 9, 7], [c, 8, 9, 7], [c, 2, 13, 7], [c, 8, 13, 7]

- Table $T36$ of size 2^{88}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [40, 41, 42, 43, 44, 45, 46, 47]

    k_{28}: [5, 21, 37, 53]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:

    [c, 2, 6, 5], [c, 4, 6, 5], [c, 8, 6, 5], [c, 2, 10, 5], [c, 4, 10, 5], [c, 8, 10, 5], [c, 2, 14, 5], [c, 8, 14, 5]

- Table $T37$ of size 2^{88}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [40, 41, 42, 43, 44, 45, 46, 47]

    k_{28}: [13, 29, 45, 61]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:

    [c, 2, 6, 13], [c, 4, 6, 13], [c, 8, 6, 13], [c, 2, 10, 13], [c, 4, 10, 13], [c, 8, 10, 13], [c, 2, 14, 13], [c, 8, 14, 13]

- Table $T38$ of size 2^{88}

  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [40, 41, 42, 43, 44, 45, 46, 47]

    k_{28}: [15, 31, 47, 63]

    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]

  - Included Linear Hulls:

    [c, 2, 6, 15], [c, 4, 6, 15], [c, 8, 6, 15], [c, 2, 10, 15], [c, 4, 10, 15], [c, 8, 10, 15], [c, 2, 14, 15], [c, 8, 14, 15]

- Table $T39$ of size 2^{87}

  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:

    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63]

    k_2: [40, 41, 42, 43, 44, 45, 46, 47]

    k_{28}: [7, 23, 39, 55]

    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]

  - Included Linear Hulls:

    [c, 2, 6, 7], [c, 4, 6, 7], [c, 8, 6, 7], [c, 2, 10, 7], [c, 4, 10, 7], [c, 8, 10, 7], [c, 2, 14, 7], [c, 8, 14, 7]

F Attack Parameters of Linear Hulls in the 29-Round Attack on PRESENT-128

- $L0$: [2, 2, 5, 5] , $g_0 = 1, s_0 = (80), t_0 = (80), r_0 = (80)$, belongs to $T0$.

  $m_0 = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L1$: [2, 2, 5, 7] , $g_1 = 1, s_1 = (80), t_1 = (80), r_1 = (80)$, belongs to $T3$.

  $m_1 = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L2$: [2, 2, 5, 13] , $g_2 = 1, s_2 = (80), t_2 = (80), r_2 = (80)$, belongs to $T1$.

  $m_2 = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L3$: [2, 2, 5, 15] , $g_3 = 1, s_3 = (80), t_3 = (80), r_3 = (80)$, belongs to $T2$.

  $m_3 = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L4$: [2, 4, 5, 5] , $g_4 = 1, s_4 = (80), t_4 = (80), r_4 = (80)$, belongs to $T0$.

  $m_4 = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L5$: [2, 4, 5, 7] , $g_5 = 1, s_5 = (80), t_5 = (80), r_5 = (80)$, belongs to $T3$.

  $m_5 = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L6$: [2, 4, 5, 13] , $g_6 = 1, s_6 = (80), t_6 = (80), r_6 = (80)$, belongs to $T1$.

  $m_6 = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L7$: [2, 4, 5, 15] , $g_7 = 1, s_7 = (80), t_7 = (80), r_7 = (80)$, belongs to $T2$.

  $m_7 = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L8$: [2, 8, 5, 5] , $g_8 = 1, s_8 = (80), t_8 = (80), r_8 = (80)$, belongs to $T0$.

  $m_8 = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L9$: [2, 8, 5, 7] , $g_9 = 1, s_9 = (80), t_9 = (80), r_9 = (80)$, belongs to $T3$. $m_9 = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L10$: [2, 8, 5, 13] , $g_{10} = 1, s_{10} = (80), t_{10} = (80), r_{10} = (80)$, belongs to $T1$. $m_{10} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L11$: [2, 8, 5, 15] , $g_{11} = 1, s_{11} = (80), t_{11} = (80), r_{11} = (80)$, belongs to $T2$. $m_{11} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L12$: [2, 2, 6, 5] , $g_{12} = 1, s_{12} = (80), t_{12} = (80), r_{12} = (80)$, belongs to $T4$. $m_{12} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L13$: [2, 2, 6, 7] , $g_{13} = 1, s_{13} = (80), t_{13} = (80), r_{13} = (80)$, belongs to $T7$. $m_{13} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L14$: [2, 2, 6, 13] , $g_{14} = 1, s_{14} = (80), t_{14} = (80), r_{14} = (80)$, belongs to $T5$. $m_{14} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L15$: [2, 2, 6, 15] , $g_{15} = 1, s_{15} = (80), t_{15} = (80), r_{15} = (80)$, belongs to $T6$. $m_{15} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L16$: [2, 4, 6, 5] , $g_{16} = 1, s_{16} = (80), t_{16} = (80), r_{16} = (80)$, belongs to $T4$. $m_{16} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L17$: [2, 4, 6, 7] , $g_{17} = 1, s_{17} = (80), t_{17} = (80), r_{17} = (80)$, belongs to $T7$. $m_{17} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L18$: [2, 4, 6, 13] , $g_{18} = 1, s_{18} = (80), t_{18} = (80), r_{18} = (80)$, belongs to $T5$. $m_{18} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L19$: [2, 4, 6, 15] , $g_{19} = 1, s_{19} = (80), t_{19} = (80), r_{19} = (80)$, belongs to $T6$. $m_{19} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L20$: [2, 8, 6, 5] , $g_{20} = 1, s_{20} = (80), t_{20} = (80), r_{20} = (80)$, belongs to $T4$. $m_{20} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L21$: [2, 8, 6, 7] , $g_{21} = 1, s_{21} = (80), t_{21} = (80), r_{21} = (80)$, belongs to $T7$. $m_{21} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L22$: [2, 8, 6, 13] , $g_{22} = 1, s_{22} = (80), t_{22} = (80), r_{22} = (80)$, belongs to $T5$. $m_{22} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L23$: [2, 8, 6, 15] , $g_{23} = 1, s_{23} = (80), t_{23} = (80), r_{23} = (80)$, belongs to $T6$. $m_{23} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L24$: [2, 2, 9, 5] , $g_{24} = 1, s_{24} = (80), t_{24} = (80), r_{24} = (80)$, belongs to $T0$. $m_{24} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L25$: [2, 2, 9, 7] , $g_{25} = 1, s_{25} = (80), t_{25} = (80), r_{25} = (80)$, belongs to $T3$. $m_{25} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L26$: [2, 2, 9, 13] , $g_{26} = 1, s_{26} = (80), t_{26} = (80), r_{26} = (80)$, belongs to $T1$. $m_{26} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L27$: [2, 2, 9, 15] , $g_{27} = 1, s_{27} = (80), t_{27} = (80), r_{27} = (80)$, belongs to $T2$. $m_{27} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L28$: [2, 4, 9, 5] , $g_{28} = 1, s_{28} = (80), t_{28} = (80), r_{28} = (80)$, belongs to $T0$. $m_{28} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L29$: [2, 4, 9, 7] , $g_{29} = 1, s_{29} = (80), t_{29} = (80), r_{29} = (80)$, belongs to $T3$. $m_{29} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L30$: [2, 4, 9, 13] , $g_{30} = 1, s_{30} = (80), t_{30} = (80), r_{30} = (80)$, belongs to $T1$. $m_{30} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L31$: [2, 4, 9, 15] , $g_{31} = 1, s_{31} = (80), t_{31} = (80), r_{31} = (80)$, belongs to $T2$. $m_{31} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L32$: [2, 8, 9, 5] , $g_{32} = 1, s_{32} = (80), t_{32} = (80), r_{32} = (80)$, belongs to $T0$. $m_{32} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L33$: [2, 8, 9, 7] , $g_{33} = 1, s_{33} = (80), t_{33} = (80), r_{33} = (80)$, belongs to $T3$. $m_{33} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L34$: [2, 8, 9, 13] , $g_{34} = 1, s_{34} = (80), t_{34} = (80), r_{34} = (80)$, belongs to $T1$. $m_{34} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L35$: [2, 8, 9, 15] , $g_{35} = 1, s_{35} = (80), t_{35} = (80), r_{35} = (80)$, belongs to $T2$. $m_{35} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L36$: [2, 2, 10, 5] , $g_{36} = 1, s_{36} = (80), t_{36} = (80), r_{36} = (80)$, belongs to $T4$. $m_{36} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L37$: [2, 2, 10, 7] , $g_{37} = 1, s_{37} = (80), t_{37} = (80), r_{37} = (80)$, belongs to $T7$. $m_{37} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L38$: [2, 2, 10, 13] , $g_{38} = 1, s_{38} = (80), t_{38} = (80), r_{38} = (80)$, belongs to $T5$. $m_{38} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L39$: [2, 2, 10, 15] , $g_{39} = 1, s_{39} = (80), t_{39} = (80), r_{39} = (80)$, belongs to $T6$. $m_{39} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L40$: [2, 4, 10, 5] , $g_{40} = 1, s_{40} = (80), t_{40} = (80), r_{40} = (80)$, belongs to $T4$. $m_{40} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L41$: [2, 4, 10, 7] , $g_{41} = 1, s_{41} = (80), t_{41} = (80), r_{41} = (80)$, belongs to $T7$. $m_{41} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L42$: [2, 4, 10, 13] , $g_{42} = 1, s_{42} = (80), t_{42} = (80), r_{42} = (80)$, belongs to $T5$. $m_{42} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L43$: [2, 4, 10, 15] , $g_{43} = 1, s_{43} = (80), t_{43} = (80), r_{43} = (80)$, belongs to $T6$. $m_{43} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L44$: [2, 8, 10, 5] , $g_{44} = 1, s_{44} = (80), t_{44} = (80), r_{44} = (80)$, belongs to $T4$. $m_{44} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L45$: [2, 8, 10, 7] , $g_{45} = 1, s_{45} = (80), t_{45} = (80), r_{45} = (80)$, belongs to $T7$. $m_{45} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L46$: [2, 8, 10, 13] , $g_{46} = 1, s_{46} = (80), t_{46} = (80), r_{46} = (80)$, belongs to $T5$. $m_{46} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L47$: [2, 8, 10, 15] , $g_{47} = 1, s_{47} = (80), t_{47} = (80), r_{47} = (80)$, belongs to $T6$. $m_{47} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L48$: [4, 2, 5, 5] , $g_{48} = 1, s_{48} = (80), t_{48} = (80), r_{48} = (80)$, belongs to $T8$. $m_{48} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L49$: [4, 2, 5, 7] , $g_{49} = 1, s_{49} = (80), t_{49} = (80), r_{49} = (80)$, belongs to $T11$. $m_{49} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L50$: [4, 2, 5, 13] , $g_{50} = 1, s_{50} = (80), t_{50} = (80), r_{50} = (80)$, belongs to $T9$. $m_{50} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L51$: [4, 2, 5, 15] , $g_{51} = 1, s_{51} = (80), t_{51} = (80), r_{51} = (80)$, belongs to $T10$. $m_{51} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L52$: [4, 4, 5, 5] , $g_{52} = 1, s_{52} = (80), t_{52} = (80), r_{52} = (80)$, belongs to $T8$. $m_{52} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L53$: [4, 4, 5, 7] , $g_{53} = 1, s_{53} = (80), t_{53} = (80), r_{53} = (80)$, belongs to $T11$. $m_{53} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L54$: [4, 4, 5, 13] , $g_{54} = 1, s_{54} = (80), t_{54} = (80), r_{54} = (80)$, belongs to $T9$. $m_{54} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L55$: [4, 4, 5, 15] , $g_{55} = 1, s_{55} = (80), t_{55} = (80), r_{55} = (80)$, belongs to $T10$. $m_{55} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L56$: [4, 8, 5, 5] , $g_{56} = 1, s_{56} = (80), t_{56} = (80), r_{56} = (80)$, belongs to $T8$. $m_{56} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L57$: [4, 8, 5, 7] , $g_{57} = 1, s_{57} = (80), t_{57} = (80), r_{57} = (80)$, belongs to $T11$. $m_{57} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L58$: [4, 8, 5, 13] , $g_{58} = 1, s_{58} = (80), t_{58} = (80), r_{58} = (80)$, belongs to $T9$. $m_{58} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L59$: [4, 8, 5, 15] , $g_{59} = 1, s_{59} = (80), t_{59} = (80), r_{59} = (80)$, belongs to $T10$. $m_{59} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L60$: [4, 2, 6, 5] , $g_{60} = 1, s_{60} = (80), t_{60} = (80), r_{60} = (80)$, belongs to $T12$. $m_{60} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L61$: [4, 2, 6, 7] , $g_{61} = 1, s_{61} = (80), t_{61} = (80), r_{61} = (80)$, belongs to $T15$. $m_{61} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L62$: [4, 2, 6, 13] , $g_{62} = 1, s_{62} = (80), t_{62} = (80), r_{62} = (80)$, belongs to $T13$. $m_{62} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L63$: [4, 2, 6, 15] , $g_{63} = 1, s_{63} = (80), t_{63} = (80), r_{63} = (80)$, belongs to $T14$. $m_{63} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L64$: [4, 4, 6, 5] , $g_{64} = 1, s_{64} = (80), t_{64} = (80), r_{64} = (80)$, belongs to $T12$. $m_{64} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L65$: [4, 4, 6, 7] , $g_{65} = 1, s_{65} = (80), t_{65} = (80), r_{65} = (80)$, belongs to $T15$. $m_{65} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L66$: [4, 4, 6, 13] , $g_{66} = 1, s_{66} = (80), t_{66} = (80), r_{66} = (80)$, belongs to $T13$. $m_{66} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L67$: [4, 4, 6, 15] , $g_{67} = 1, s_{67} = (80), t_{67} = (80), r_{67} = (80)$, belongs to $T14$. $m_{67} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L68$: [4, 8, 6, 5] , $g_{68} = 1, s_{68} = (80), t_{68} = (80), r_{68} = (80)$, belongs to $T12$. $m_{68} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L69$: [4, 8, 6, 7] , $g_{69} = 1, s_{69} = (80), t_{69} = (80), r_{69} = (80)$, belongs to $T15$. $m_{69} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L70$: [4, 8, 6, 13] , $g_{70} = 1, s_{70} = (80), t_{70} = (80), r_{70} = (80)$, belongs to $T13$. $m_{70} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L71$: [4, 8, 6, 15] , $g_{71} = 1, s_{71} = (80), t_{71} = (80), r_{71} = (80)$, belongs to $T14$. $m_{71} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L72$: [4, 2, 9, 5] , $g_{72} = 1, s_{72} = (80), t_{72} = (80), r_{72} = (80)$, belongs to $T8$. $m_{72} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L73$: [4, 2, 9, 7] , $g_{73} = 1, s_{73} = (80), t_{73} = (80), r_{73} = (80)$, belongs to $T11$. $m_{73} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L74$: [4, 2, 9, 13] , $g_{74} = 1, s_{74} = (80), t_{74} = (80), r_{74} = (80)$, belongs to $T9$. $m_{74} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L75$: [4, 2, 9, 15] , $g_{75} = 1, s_{75} = (80), t_{75} = (80), r_{75} = (80)$, belongs to $T10$. $m_{75} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L76$: [4, 4, 9, 5] , $g_{76} = 1, s_{76} = (80), t_{76} = (80), r_{76} = (80)$, belongs to $T8$. $m_{76} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L77$: [4, 4, 9, 7] , $g_{77} = 1, s_{77} = (80), t_{77} = (80), r_{77} = (80)$, belongs to $T11$. $m_{77} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L78$: [4, 4, 9, 13] , $g_{78} = 1, s_{78} = (80), t_{78} = (80), r_{78} = (80)$, belongs to $T9$. $m_{78} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L79$: [4, 4, 9, 15] , $g_{79} = 1, s_{79} = (80), t_{79} = (80), r_{79} = (80)$, belongs to $T10$. $m_{79} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L80$: [4, 8, 9, 5] , $g_{80} = 1, s_{80} = (80), t_{80} = (80), r_{80} = (80)$, belongs to $T8$. $m_{80} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L81$: [4, 8, 9, 7] , $g_{81} = 1, s_{81} = (80), t_{81} = (80), r_{81} = (80)$, belongs to $T11$. $m_{81} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L82$: [4, 8, 9, 13] , $g_{82} = 1, s_{82} = (80), t_{82} = (80), r_{82} = (80)$, belongs to $T9$. $m_{82} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L83$: [4, 8, 9, 15] , $g_{83} = 1, s_{83} = (80), t_{83} = (80), r_{83} = (80)$, belongs to $T10$. $m_{83} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L84$: [4, 2, 10, 5] , $g_{84} = 1, s_{84} = (80), t_{84} = (80), r_{84} = (80)$, belongs to $T12$. $m_{84} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L85$: [4, 2, 10, 7] , $g_{85} = 1, s_{85} = (80), t_{85} = (80), r_{85} = (80)$, belongs to $T15$. $m_{85} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L86$: [4, 2, 10, 13] , $g_{86} = 1, s_{86} = (80), t_{86} = (80), r_{86} = (80)$, belongs to $T13$. $m_{86} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L87$: [4, 2, 10, 15] , $g_{87} = 1, s_{87} = (80), t_{87} = (80), r_{87} = (80)$, belongs to $T14$. $m_{87} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L88$: [4, 4, 10, 5] , $g_{88} = 1, s_{88} = (80), t_{88} = (80), r_{88} = (80)$, belongs to $T12$. $m_{88} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L89$: [4, 4, 10, 7] , $g_{89} = 1, s_{89} = (80), t_{89} = (80), r_{89} = (80)$, belongs to $T15$. $m_{89} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L90$: [4, 4, 10, 13] , $g_{90} = 1, s_{90} = (80), t_{90} = (80), r_{90} = (80)$, belongs to $T13$. $m_{90} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L91$: [4, 4, 10, 15] , $g_{91} = 1, s_{91} = (80), t_{91} = (80), r_{91} = (80)$, belongs to $T14$. $m_{91} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L92$: [4, 8, 10, 5] , $g_{92} = 1, s_{92} = (80), t_{92} = (80), r_{92} = (80)$, belongs to $T12$. $m_{92} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L93$: [4, 8, 10, 7] , $g_{93} = 1, s_{93} = (80), t_{93} = (80), r_{93} = (80)$, belongs to $T15$. $m_{93} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L94$: [4, 8, 10, 13] , $g_{94} = 1, s_{94} = (80), t_{94} = (80), r_{94} = (80)$, belongs to $T13$. $m_{94} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L95$: [4, 8, 10, 15] , $g_{95} = 1, s_{95} = (80), t_{95} = (80), r_{95} = (80)$, belongs to $T14$. $m_{95} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L96$: [8, 2, 5, 5] , $g_{96} = 1, s_{96} = (80), t_{96} = (80), r_{96} = (80)$, belongs to $T16$. $m_{96} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L97$: [8, 2, 5, 7] , $g_{97} = 1, s_{97} = (80), t_{97} = (80), r_{97} = (80)$, belongs to $T19$. $m_{97} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L98$: [8, 2, 5, 13] , $g_{98} = 1, s_{98} = (80), t_{98} = (80), r_{98} = (80)$, belongs to $T17$. $m_{98} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L99$: [8, 2, 5, 15] , $g_{99} = 1, s_{99} = (80), t_{99} = (80), r_{99} = (80)$, belongs to $T18$. $m_{99} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L100$: [8, 8, 5, 5] , $g_{100} = 1, s_{100} = (80), t_{100} = (80), r_{100} = (80)$, belongs to $T16$. $m_{100} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L101$: [8, 8, 5, 7] , $g_{101} = 1, s_{101} = (80), t_{101} = (80), r_{101} = (80)$, belongs to $T19$. $m_{101} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L102$: [8, 8, 5, 13] , $g_{102} = 1, s_{102} = (80), t_{102} = (80), r_{102} = (80)$, belongs to $T17$. $m_{102} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L103$: [8, 8, 5, 15] , $g_{103} = 1, s_{103} = (80), t_{103} = (80), r_{103} = (80)$, belongs to $T18$. $m_{103} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L104$: [8, 2, 6, 5] , $g_{104} = 1, s_{104} = (80), t_{104} = (80), r_{104} = (80)$, belongs to $T20$. $m_{104} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L105$: [8, 2, 6, 7] , $g_{105} = 1, s_{105} = (80), t_{105} = (80), r_{105} = (80)$, belongs to $T23$. $m_{105} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L106$: [8, 2, 6, 13] , $g_{106} = 1, s_{106} = (80), t_{106} = (80), r_{106} = (80)$, belongs to $T21$. $m_{106} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L107$: [8, 2, 6, 15] , $g_{107} = 1, s_{107} = (80), t_{107} = (80), r_{107} = (80)$, belongs to $T22$. $m_{107} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L108$: [8, 8, 6, 5] , $g_{108} = 1, s_{108} = (80), t_{108} = (80), r_{108} = (80)$, belongs to $T20$. $m_{108} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L109$: [8, 8, 6, 7] , $g_{109} = 1, s_{109} = (80), t_{109} = (80), r_{109} = (80)$, belongs to $T23$. $m_{109} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L110$: [8, 8, 6, 13] , $g_{110} = 1, s_{110} = (80), t_{110} = (80), r_{110} = (80)$, belongs to $T21$. $m_{110} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L111$: [8, 8, 6, 15] , $g_{111} = 1, s_{111} = (80), t_{111} = (80), r_{111} = (80)$, belongs to $T22$. $m_{111} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L112$: [8, 2, 9, 5] , $g_{112} = 1, s_{112} = (80), t_{112} = (80), r_{112} = (80)$, belongs to $T16$. $m_{112} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L113$: [8, 2, 9, 7] , $g_{113} = 1, s_{113} = (80), t_{113} = (80), r_{113} = (80)$, belongs to $T19$. $m_{113} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L114$: [8, 2, 9, 13] , $g_{114} = 1, s_{114} = (80), t_{114} = (80), r_{114} = (80)$, belongs to $T17$. $m_{114} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L115$: [8, 2, 9, 15] , $g_{115} = 1, s_{115} = (80), t_{115} = (80), r_{115} = (80)$, belongs to $T18$. $m_{115} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L116$: [8, 8, 9, 5] , $g_{116} = 1, s_{116} = (80), t_{116} = (80), r_{116} = (80)$, belongs to $T16$. $m_{116} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L117$: [8, 8, 9, 7] , $g_{117} = 1, s_{117} = (80), t_{117} = (80), r_{117} = (80)$, belongs to $T19$. $m_{117} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L118$: [8, 8, 9, 13] , $g_{118} = 1, s_{118} = (80), t_{118} = (80), r_{118} = (80)$, belongs to $T17$. $m_{118} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L119$: [8, 8, 9, 15] , $g_{119} = 1, s_{119} = (80), t_{119} = (80), r_{119} = (80)$, belongs to $T18$. $m_{119} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L120$: [8, 2, 10, 5] , $g_{120} = 1, s_{120} = (80), t_{120} = (80), r_{120} = (80)$, belongs to $T20$. $m_{120} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L121$: [8, 2, 10, 7] , $g_{121} = 1, s_{121} = (80), t_{121} = (80), r_{121} = (80)$, belongs to $T23$. $m_{121} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L122$: [8, 2, 10, 13] , $g_{122} = 1, s_{122} = (80), t_{122} = (80), r_{122} = (80)$, belongs to $T21$. $m_{122} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L123$: [8, 2, 10, 15] , $g_{123} = 1, s_{123} = (80), t_{123} = (80), r_{123} = (80)$, belongs to $T22$. $m_{123} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L124$: [8, 8, 10, 5] , $g_{124} = 1, s_{124} = (80), t_{124} = (80), r_{124} = (80)$, belongs to $T20$. $m_{124} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L125$: [8, 8, 10, 7] , $g_{125} = 1, s_{125} = (80), t_{125} = (80), r_{125} = (80)$, belongs to $T23$. $m_{125} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L126$: [8, 8, 10, 13] , $g_{126} = 1, s_{126} = (80), t_{126} = (80), r_{126} = (80)$, belongs to $T21$. $m_{126} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L127$: [8, 8, 10, 15] , $g_{127} = 1, s_{127} = (80), t_{127} = (80), r_{127} = (80)$, belongs to $T22$. $m_{127} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L128$: [2, 2, 13, 5] , $g_{128} = 1, s_{128} = (80), t_{128} = (80), r_{128} = (80)$, belongs to $T0$. $m_{128} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L129$: [2, 2, 13, 7] , $g_{129} = 1, s_{129} = (80), t_{129} = (80), r_{129} = (80)$, belongs to $T3$. $m_{129} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L130$: [2, 2, 13, 13] , $g_{130} = 1, s_{130} = (80), t_{130} = (80), r_{130} = (80)$, belongs to $T1$. $m_{130} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L131$: [2, 2, 13, 15] , $g_{131} = 1, s_{131} = (80), t_{131} = (80), r_{131} = (80)$, belongs to $T2$. $m_{131} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L132$: [2, 8, 13, 5] , $g_{132} = 1, s_{132} = (80), t_{132} = (80), r_{132} = (80)$, belongs to $T0$. $m_{132} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L133$: [2, 8, 13, 7] , $g_{133} = 1, s_{133} = (80), t_{133} = (80), r_{133} = (80)$, belongs to $T3$. $m_{133} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L134$: [2, 8, 13, 13] , $g_{134} = 1, s_{134} = (80), t_{134} = (80), r_{134} = (80)$, belongs to $T1$. $m_{134} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L135$: [2, 8, 13, 15] , $g_{135} = 1, s_{135} = (80), t_{135} = (80), r_{135} = (80)$, belongs to $T2$. $m_{135} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L136$: [2, 2, 14, 5] , $g_{136} = 1, s_{136} = (80), t_{136} = (80), r_{136} = (80)$, belongs to $T4$. $m_{136} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L137$: [2, 2, 14, 7] , $g_{137} = 1, s_{137} = (80), t_{137} = (80), r_{137} = (80)$, belongs to $T7$. $m_{137} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L138$: [2, 2, 14, 13] , $g_{138} = 1, s_{138} = (80), t_{138} = (80), r_{138} = (80)$, belongs to $T5$. $m_{138} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L139$: [2, 2, 14, 15] , $g_{139} = 1, s_{139} = (80), t_{139} = (80), r_{139} = (80)$, belongs to $T6$. $m_{139} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L140$: [2, 8, 14, 5] , $g_{140} = 1, s_{140} = (80), t_{140} = (80), r_{140} = (80)$, belongs to $T4$. $m_{140} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L141$: [2, 8, 14, 7] , $g_{141} = 1, s_{141} = (80), t_{141} = (80), r_{141} = (80)$, belongs to $T7$. $m_{141} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L142$: [2, 8, 14, 13] , $g_{142} = 1, s_{142} = (80), t_{142} = (80), r_{142} = (80)$, belongs to $T5$. $m_{142} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L143$: [2, 8, 14, 15] , $g_{143} = 1, s_{143} = (80), t_{143} = (80), r_{143} = (80)$, belongs to $T6$. $m_{143} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L144$: [4, 2, 13, 5] , $g_{144} = 1, s_{144} = (80), t_{144} = (80), r_{144} = (80)$, belongs to $T8$. $m_{144} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L145$: [4, 2, 13, 7] , $g_{145} = 1, s_{145} = (80), t_{145} = (80), r_{145} = (80)$, belongs to $T11$. $m_{145} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L146$: [4, 2, 13, 13] , $g_{146} = 1, s_{146} = (80), t_{146} = (80), r_{146} = (80)$, belongs to $T9$. $m_{146} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L147$: [4, 2, 13, 15] , $g_{147} = 1, s_{147} = (80), t_{147} = (80), r_{147} = (80)$, belongs to $T10$. $m_{147} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L148$: [4, 8, 13, 5] , $g_{148} = 1, s_{148} = (80), t_{148} = (80), r_{148} = (80)$, belongs to $T8$. $m_{148} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L149$: [4, 8, 13, 7] , $g_{149} = 1, s_{149} = (80), t_{149} = (80), r_{149} = (80)$, belongs to $T11$. $m_{149} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L150$: [4, 8, 13, 13] , $g_{150} = 1, s_{150} = (80), t_{150} = (80), r_{150} = (80)$, belongs to $T9$. $m_{150} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L151$: [4, 8, 13, 15] , $g_{151} = 1, s_{151} = (80), t_{151} = (80), r_{151} = (80)$, belongs to $T10$. $m_{151} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L152$: [4, 2, 14, 5] , $g_{152} = 1, s_{152} = (80), t_{152} = (80), r_{152} = (80)$, belongs to $T12$. $m_{152} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L153$: [4, 2, 14, 7] , $g_{153} = 1, s_{153} = (80), t_{153} = (80), r_{153} = (80)$, belongs to $T15$.

  $m_{153} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L154$: [4, 2, 14, 13] , $g_{154} = 1, s_{154} = (80), t_{154} = (80), r_{154} = (80)$, belongs to $T13$.

  $m_{154} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L155$: [4, 2, 14, 15] , $g_{155} = 1, s_{155} = (80), t_{155} = (80), r_{155} = (80)$, belongs to $T14$.

  $m_{155} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L156$: [4, 8, 14, 5] , $g_{156} = 1, s_{156} = (80), t_{156} = (80), r_{156} = (80)$, belongs to $T12$.

  $m_{156} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L157$: [4, 8, 14, 7] , $g_{157} = 1, s_{157} = (80), t_{157} = (80), r_{157} = (80)$, belongs to $T15$.

  $m_{157} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L158$: [4, 8, 14, 13] , $g_{158} = 1, s_{158} = (80), t_{158} = (80), r_{158} = (80)$, belongs to $T13$.

  $m_{158} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L159$: [4, 8, 14, 15] , $g_{159} = 1, s_{159} = (80), t_{159} = (80), r_{159} = (80)$, belongs to $T14$.

  $m_{159} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L160$: [a, 2, 5, 5] , $g_{160} = 2, s_{160} = (80, 80), t_{160} = (80, 80), r_{160} = (77, 77)$, belongs to $T24$.

  $m_{160} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L161$: [a, 2, 5, 7] , $g_{161} = 2, s_{161} = (80, 80), t_{161} = (80, 80), r_{161} = (76, 80)$, belongs to $T27$.

  $m_{161} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L162$: [a, 2, 5, 13] , $g_{162} = 2, s_{162} = (80, 80), t_{162} = (80, 80), r_{162} = (76, 76)$, belongs to $T25$.

  $m_{162} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L163$: [a, 2, 5, 15] , $g_{163} = 2, s_{163} = (80, 80), t_{163} = (80, 80), r_{163} = (77, 80)$, belongs to $T26$.

  $m_{163} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L164$: [a, 4, 5, 5] , $g_{164} = 2, s_{164} = (80, 80), t_{164} = (80, 80), r_{164} = (80, 77)$, belongs to $T24$.

  $m_{164} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L165$: [a, 4, 5, 7] , $g_{165} = 2, s_{165} = (80, 80), t_{165} = (80, 80), r_{165} = (76, 76)$, belongs to $T27$.

  $m_{165} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L166$: [a, 4, 5, 13] , $g_{166} = 2, s_{166} = (80, 80), t_{166} = (80, 80), r_{166} = (80, 76)$, belongs to $T25$.

  $m_{166} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L167$: [a, 4, 5, 15] , $g_{167} = 2, s_{167} = (80, 80), t_{167} = (80, 80), r_{167} = (77, 77)$, belongs to $T26$.

  $m_{167} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L168$: [a, 8, 5, 5] , $g_{168} = 1, s_{168} = (80), t_{168} = (80), r_{168} = (77)$, belongs to $T24$.

  $m_{168} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L169$: [a, 8, 5, 7] , $g_{169} = 1, s_{169} = (80), t_{169} = (80), r_{169} = (76)$, belongs to $T27$.

  $m_{169} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L170$: [a, 8, 5, 13] , $g_{170} = 1, s_{170} = (80), t_{170} = (80), r_{170} = (76)$, belongs to $T25$.

  $m_{170} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L171$: [a, 8, 5, 15] , $g_{171} = 1, s_{171} = (80), t_{171} = (80), r_{171} = (77)$, belongs to $T26$.

  $m_{171} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L172$: [a, 2, 6, 5] , $g_{172} = 2, s_{172} = (80, 80), t_{172} = (80, 80), r_{172} = (77, 77)$, belongs to $T28$.

  $m_{172} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L173$: [a, 2, 6, 7] , $g_{173} = 2, s_{173} = (80, 80), t_{173} = (80, 80), r_{173} = (76, 80)$, belongs to $T31$.

  $m_{173} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L174$: [a, 2, 6, 13] , $g_{174} = 2, s_{174} = (80, 80), t_{174} = (80, 80), r_{174} = (76, 76)$, belongs to $T29$.

  $m_{174} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L175$: [a, 2, 6, 15] , $g_{175} = 2, s_{175} = (80, 80), t_{175} = (80, 80), r_{175} = (77, 80)$, belongs to $T30$.

  $m_{175} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L176$: [a, 4, 6, 5] , $g_{176} = 2, s_{176} = (80, 80), t_{176} = (80, 80), r_{176} = (80, 77)$, belongs to $T28$.

  $m_{176} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L177$: [a, 4, 6, 7] , $g_{177} = 2, s_{177} = (80, 80), t_{177} = (80, 80), r_{177} = (76, 76)$, belongs to $T31$.

  $m_{177} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L178$: [a, 4, 6, 13] , $g_{178} = 2, s_{178} = (80, 80), t_{178} = (80, 80), r_{178} = (80, 76)$, belongs to $T29$.

  $m_{178} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L179$: [a, 4, 6, 15] , $g_{179} = 2, s_{179} = (80, 80), t_{179} = (80, 80), r_{179} = (77, 77)$, belongs to $T30$.

  $m_{179} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L180$: [a, 8, 6, 5] , $g_{180} = 1, s_{180} = (80), t_{180} = (80), r_{180} = (77)$, belongs to $T28$.

  $m_{180} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L181$: [a, 8, 6, 7] , $g_{181} = 1, s_{181} = (80), t_{181} = (80), r_{181} = (76)$, belongs to $T31$.

  $m_{181} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L182$: [a, 8, 6, 13] , $g_{182} = 1, s_{182} = (80), t_{182} = (80), r_{182} = (76)$, belongs to $T29$.

  $m_{182} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L183$: [a, 8, 6, 15] , $g_{183} = 1, s_{183} = (80), t_{183} = (80), r_{183} = (77)$, belongs to $T30$.

  $m_{183} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L184$: [a, 2, 9, 5] , $g_{184} = 2, s_{184} = (80, 80), t_{184} = (80, 80), r_{184} = (77, 77)$, belongs to $T24$.

  $m_{184} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L185$: [a, 2, 9, 7] , $g_{185} = 2, s_{185} = (80, 80), t_{185} = (80, 80), r_{185} = (76, 80)$, belongs to $T27$.

  $m_{185} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L186$: [a, 2, 9, 13] , $g_{186} = 2, s_{186} = (80, 80), t_{186} = (80, 80), r_{186} = (76, 76)$, belongs to $T25$.

  $m_{186} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L187$: [a, 2, 9, 15] , $g_{187} = 2, s_{187} = (80, 80), t_{187} = (80, 80), r_{187} = (77, 80)$, belongs to $T26$.

  $m_{187} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L188$: [a, 4, 9, 5] , $g_{188} = 2, s_{188} = (80, 80), t_{188} = (80, 80), r_{188} = (80, 77)$, belongs to $T24$.

  $m_{188} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L189$: [a, 4, 9, 7] , $g_{189} = 2, s_{189} = (80, 80), t_{189} = (80, 80), r_{189} = (76, 76)$, belongs to $T27$.

  $m_{189} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L190$: [a, 4, 9, 13] , $g_{190} = 2, s_{190} = (80, 80), t_{190} = (80, 80), r_{190} = (80, 76)$, belongs to $T25$.

  $m_{190} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L191$: [a, 4, 9, 15] , $g_{191} = 2, s_{191} = (80, 80), t_{191} = (80, 80), r_{191} = (77, 77)$, belongs to $T26$.

  $m_{191} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L192$: [a, 8, 9, 5] , $g_{192} = 1, s_{192} = (80), t_{192} = (80), r_{192} = (77)$, belongs to $T24$.

  $m_{192} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L193$: [a, 8, 9, 7] , $g_{193} = 1, s_{193} = (80), t_{193} = (80), r_{193} = (76)$, belongs to $T27$.

  $m_{193} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L194$: [a, 8, 9, 13] , $g_{194} = 1, s_{194} = (80), t_{194} = (80), r_{194} = (76)$, belongs to $T25$.

  $m_{194} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L195$: [a, 8, 9, 15] , $g_{195} = 1, s_{195} = (80), t_{195} = (80), r_{195} = (77)$, belongs to $T26$.

  $m_{195} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L196$: [a, 2, 10, 5] , $g_{196} = 2, s_{196} = (80, 80), t_{196} = (80, 80), r_{196} = (77, 77)$, belongs to $T28$.

  $m_{196} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L197$: [a, 2, 10, 7] , $g_{197} = 2, s_{197} = (80, 80), t_{197} = (80, 80), r_{197} = (76, 80)$, belongs to $T31$.

  $m_{197} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L198$: [a, 2, 10, 13] , $g_{198} = 2, s_{198} = (80, 80), t_{198} = (80, 80), r_{198} = (76, 76)$, belongs to $T29$.

  $m_{198} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L199$: [a, 2, 10, 15] , $g_{199} = 2, s_{199} = (80, 80), t_{199} = (80, 80), r_{199} = (77, 80)$, belongs to $T30$.

  $m_{199} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L200$: [a, 4, 10, 5] , $g_{200} = 2, s_{200} = (80, 80), t_{200} = (80, 80), r_{200} = (80, 77)$, belongs to $T28$.

  $m_{200} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L201$: [a, 4, 10, 7] , $g_{201} = 2, s_{201} = (80, 80), t_{201} = (80, 80), r_{201} = (76, 76)$, belongs to $T31$.

  $m_{201} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L202$: [a, 4, 10, 13] , $g_{202} = 2, s_{202} = (80, 80), t_{202} = (80, 80), r_{202} = (80, 76)$, belongs to $T29$.

  $m_{202} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L203$: [a, 4, 10, 15] , $g_{203} = 2, s_{203} = (80, 80), t_{203} = (80, 80), r_{203} = (77, 77)$, belongs to $T30$.

  $m_{203} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L204$: [a, 8, 10, 5] , $g_{204} = 1, s_{204} = (80), t_{204} = (80), r_{204} = (77)$, belongs to $T28$.

  $m_{204} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L205$: [a, 8, 10, 7] , $g_{205} = 1, s_{205} = (80), t_{205} = (80), r_{205} = (76)$, belongs to $T31$.

  $m_{205} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L206$: [a, 8, 10, 13] , $g_{206} = 1, s_{206} = (80), t_{206} = (80), r_{206} = (76)$, belongs to $T29$.

  $m_{206} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L207$: [a, 8, 10, 15] , $g_{207} = 1, s_{207} = (80), t_{207} = (80), r_{207} = (77)$, belongs to $T30$.

  $m_{207} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L208$: [c, 2, 5, 5] , $g_{208} = 2, s_{208} = (80, 80), t_{208} = (80, 80), r_{208} = (77, 77)$, belongs to $T32$.

  $m_{208} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L209$: [c, 2, 5, 7] , $g_{209} = 2, s_{209} = (80, 80), t_{209} = (80, 80), r_{209} = (76, 80)$, belongs to $T35$.

  $m_{209} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L210$: [c, 2, 5, 13] , $g_{210} = 2, s_{210} = (80, 80), t_{210} = (80, 80), r_{210} = (76, 76)$, belongs to $T33$.

  $m_{210} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L211$: [c, 2, 5, 15] , $g_{211} = 2, s_{211} = (80, 80), t_{211} = (80, 80), r_{211} = (77, 80)$, belongs to $T34$.

  $m_{211} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L212$: [c, 4, 5, 5] , $g_{212} = 2, s_{212} = (80, 80), t_{212} = (80, 80), r_{212} = (80, 77)$, belongs to $T32$.

  $m_{212} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L213$: [c, 4, 5, 7] , $g_{213} = 2, s_{213} = (80, 80), t_{213} = (80, 80), r_{213} = (76, 76)$, belongs to $T35$.

  $m_{213} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L214$: [c, 4, 5, 13] , $g_{214} = 2, s_{214} = (80, 80), t_{214} = (80, 80), r_{214} = (80, 76)$, belongs to $T33$.

  $m_{214} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L215$: [c, 4, 5, 15] , $g_{215} = 2, s_{215} = (80, 80), t_{215} = (80, 80), r_{215} = (77, 77)$, belongs to $T34$.

  $m_{215} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L216$: [c, 8, 5, 5] , $g_{216} = 1, s_{216} = (80), t_{216} = (80), r_{216} = (77)$, belongs to $T32$.

  $m_{216} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L217$: [c, 8, 5, 7] , $g_{217} = 1, s_{217} = (80), t_{217} = (80), r_{217} = (76)$, belongs to $T35$.

  $m_{217} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L218$: [c, 8, 5, 13] , $g_{218} = 1, s_{218} = (80), t_{218} = (80), r_{218} = (76)$, belongs to $T33$.

  $m_{218} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L219$: [c, 8, 5, 15] , $g_{219} = 1, s_{219} = (80), t_{219} = (80), r_{219} = (77)$, belongs to $T34$.

  $m_{219} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L220$: [c, 2, 6, 5] , $g_{220} = 2, s_{220} = (80, 80), t_{220} = (80, 80), r_{220} = (77, 77)$, belongs to $T36$.

  $m_{220} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L221$: [c, 2, 6, 7] , $g_{221} = 2, s_{221} = (80, 80), t_{221} = (80, 80), r_{221} = (76, 80)$, belongs to $T39$.

  $m_{221} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L222$: [c, 2, 6, 13] , $g_{222} = 2, s_{222} = (80, 80), t_{222} = (80, 80), r_{222} = (76, 76)$, belongs to $T37$.

  $m_{222} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L223$: [c, 2, 6, 15] , $g_{223} = 2, s_{223} = (80, 80), t_{223} = (80, 80), r_{223} = (77, 80)$, belongs to $T38$.

  $m_{223} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L224$: [c, 4, 6, 5] , $g_{224} = 2, s_{224} = (80, 80), t_{224} = (80, 80), r_{224} = (80, 77)$, belongs to $T36$.

  $m_{224} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L225$: [c, 4, 6, 7] , $g_{225} = 2, s_{225} = (80, 80), t_{225} = (80, 80), r_{225} = (76, 76)$, belongs to $T39$.

  $m_{225} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L226$: [`c`, 4, 6, 13] , $g_{226} = 2, s_{226} = (80, 80), t_{226} = (80, 80), r_{226} = (80, 76)$, belongs to $T37$.

  $m_{226} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L227$: [`c`, 4, 6, 15] , $g_{227} = 2, s_{227} = (80, 80), t_{227} = (80, 80), r_{227} = (77, 77)$, belongs to $T38$.

  $m_{227} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L228$: [`c`, 8, 6, 5] , $g_{228} = 1, s_{228} = (80), t_{228} = (80), r_{228} = (77)$, belongs to $T36$.

  $m_{228} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L229$: [`c`, 8, 6, 7] , $g_{229} = 1, s_{229} = (80), t_{229} = (80), r_{229} = (76)$, belongs to $T39$.

  $m_{229} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L230$: [`c`, 8, 6, 13] , $g_{230} = 1, s_{230} = (80), t_{230} = (80), r_{230} = (76)$, belongs to $T37$.

  $m_{230} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L231$: [`c`, 8, 6, 15] , $g_{231} = 1, s_{231} = (80), t_{231} = (80), r_{231} = (77)$, belongs to $T38$.

  $m_{231} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L232$: [`c`, 2, 9, 5] , $g_{232} = 2, s_{232} = (80, 80), t_{232} = (80, 80), r_{232} = (77, 77)$, belongs to $T32$.

  $m_{232} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L233$: [`c`, 2, 9, 7] , $g_{233} = 2, s_{233} = (80, 80), t_{233} = (80, 80), r_{233} = (76, 80)$, belongs to $T35$.

  $m_{233} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L234$: [`c`, 2, 9, 13] , $g_{234} = 2, s_{234} = (80, 80), t_{234} = (80, 80), r_{234} = (76, 76)$, belongs to $T33$.

  $m_{234} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L235$: [`c`, 2, 9, 15] , $g_{235} = 2, s_{235} = (80, 80), t_{235} = (80, 80), r_{235} = (77, 80)$, belongs to $T34$.

  $m_{235} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L236$: [`c`, 4, 9, 5] , $g_{236} = 2, s_{236} = (80, 80), t_{236} = (80, 80), r_{236} = (80, 77)$, belongs to $T32$.

  $m_{236} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L237$: [`c`, 4, 9, 7] , $g_{237} = 2, s_{237} = (80, 80), t_{237} = (80, 80), r_{237} = (76, 76)$, belongs to $T35$.

  $m_{237} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L238$: [`c`, 4, 9, 13] , $g_{238} = 2, s_{238} = (80, 80), t_{238} = (80, 80), r_{238} = (80, 76)$, belongs to $T33$.

  $m_{238} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L239$: [`c`, 4, 9, 15] , $g_{239} = 2, s_{239} = (80, 80), t_{239} = (80, 80), r_{239} = (77, 77)$, belongs to $T34$.

  $m_{239} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L240$: [c, 8, 9, 5] , $g_{240} = 1, s_{240} = (80), t_{240} = (80), r_{240} = (77)$, belongs to $T32$.

  $m_{240} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L241$: [c, 8, 9, 7] , $g_{241} = 1, s_{241} = (80), t_{241} = (80), r_{241} = (76)$, belongs to $T35$.

  $m_{241} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L242$: [c, 8, 9, 13] , $g_{242} = 1, s_{242} = (80), t_{242} = (80), r_{242} = (76)$, belongs to $T33$.

  $m_{242} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L243$: [c, 8, 9, 15] , $g_{243} = 1, s_{243} = (80), t_{243} = (80), r_{243} = (77)$, belongs to $T34$.

  $m_{243} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L244$: [c, 2, 10, 5] , $g_{244} = 2, s_{244} = (80, 80), t_{244} = (80, 80), r_{244} = (77, 77)$, belongs to $T36$.

  $m_{244} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L245$: [c, 2, 10, 7] , $g_{245} = 2, s_{245} = (80, 80), t_{245} = (80, 80), r_{245} = (76, 80)$, belongs to $T39$.

  $m_{245} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L246$: [c, 2, 10, 13] , $g_{246} = 2, s_{246} = (80, 80), t_{246} = (80, 80), r_{246} = (76, 76)$, belongs to $T37$.

  $m_{246} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L247$: [c, 2, 10, 15] , $g_{247} = 2, s_{247} = (80, 80), t_{247} = (80, 80), r_{247} = (77, 80)$, belongs to $T38$.

  $m_{247} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L248$: [c, 4, 10, 5] , $g_{248} = 2, s_{248} = (80, 80), t_{248} = (80, 80), r_{248} = (80, 77)$, belongs to $T36$.

  $m_{248} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L249$: [c, 4, 10, 7] , $g_{249} = 2, s_{249} = (80, 80), t_{249} = (80, 80), r_{249} = (76, 76)$, belongs to $T39$.

  $m_{249} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L250$: [c, 4, 10, 13] , $g_{250} = 2, s_{250} = (80, 80), t_{250} = (80, 80), r_{250} = (80, 76)$, belongs to $T37$.

  $m_{250} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L251$: [c, 4, 10, 15] , $g_{251} = 2, s_{251} = (80, 80), t_{251} = (80, 80), r_{251} = (77, 77)$, belongs to $T38$.

  $m_{251} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L252$: [c, 8, 10, 5] , $g_{252} = 1, s_{252} = (80), t_{252} = (80), r_{252} = (77)$, belongs to $T36$.

  $m_{252} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L253$: [c, 8, 10, 7] , $g_{253} = 1, s_{253} = (80), t_{253} = (80), r_{253} = (76)$, belongs to $T39$.

  $m_{253} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L254$: [c, 8, 10, 13] , $g_{254} = 1, s_{254} = (80), t_{254} = (80), r_{254} = (76)$, belongs to $T37$.

  $m_{254} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L255$: [c, 8, 10, 15] , $g_{255} = 1, s_{255} = (80), t_{255} = (80), r_{255} = (77)$, belongs to $T38$.

  $m_{255} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L256$: [a, 2, 13, 5] , $g_{256} = 2, s_{256} = (80, 80), t_{256} = (80, 80), r_{256} = (77, 77)$, belongs to $T24$.

  $m_{256} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L257$: [a, 2, 13, 7] , $g_{257} = 2, s_{257} = (80, 80), t_{257} = (80, 80), r_{257} = (76, 80)$, belongs to $T27$.

  $m_{257} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L258$: [a, 2, 13, 13] , $g_{258} = 2, s_{258} = (80, 80), t_{258} = (80, 80), r_{258} = (76, 76)$, belongs to $T25$.

  $m_{258} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L259$: [a, 2, 13, 15] , $g_{259} = 2, s_{259} = (80, 80), t_{259} = (80, 80), r_{259} = (77, 80)$, belongs to $T26$.

  $m_{259} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L260$: [a, 4, 13, 5] , $g_{260} = 2, s_{260} = (80, 80), t_{260} = (80, 80), r_{260} = (80, 77)$, belongs to $T24$.

  $m_{260} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L261$: [a, 4, 13, 7] , $g_{261} = 2, s_{261} = (80, 80), t_{261} = (80, 80), r_{261} = (76, 76)$, belongs to $T27$.

  $m_{261} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L262$: [a, 4, 13, 13] , $g_{262} = 2, s_{262} = (80, 80), t_{262} = (80, 80), r_{262} = (80, 76)$, belongs to $T25$.

  $m_{262} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L263$: [a, 4, 13, 15] , $g_{263} = 2, s_{263} = (80, 80), t_{263} = (80, 80), r_{263} = (77, 77)$, belongs to $T26$.

  $m_{263} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L264$: [a, 8, 13, 5] , $g_{264} = 1, s_{264} = (80), t_{264} = (80), r_{264} = (77)$, belongs to $T24$.

  $m_{264} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L265$: [a, 8, 13, 7] , $g_{265} = 1, s_{265} = (80), t_{265} = (80), r_{265} = (76)$, belongs to $T27$.

  $m_{265} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L266$: [a, 8, 13, 13] , $g_{266} = 1, s_{266} = (80), t_{266} = (80), r_{266} = (76)$, belongs to $T25$.

  $m_{266} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L267$: [a, 8, 13, 15] , $g_{267} = 1, s_{267} = (80), t_{267} = (80), r_{267} = (77)$, belongs to $T26$.

  $m_{267} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L268$: [a, 2, 14, 5] , $g_{268} = 2, s_{268} = (80, 80), t_{268} = (80, 80), r_{268} = (77, 77)$, belongs to $T28$.

  $m_{268} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L269$: [a, 2, 14, 7] , $g_{269} = 2, s_{269} = (80, 80), t_{269} = (80, 80), r_{269} = (76, 80)$, belongs to $T31$.

  $m_{269} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L270$: [a, 2, 14, 13] , $g_{270} = 2, s_{270} = (80, 80), t_{270} = (80, 80), r_{270} = (76, 76)$, belongs to $T29$.

  $m_{270} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L271$: [a, 2, 14, 15] , $g_{271} = 2, s_{271} = (80, 80), t_{271} = (80, 80), r_{271} = (77, 80)$, belongs to $T30$.

  $m_{271} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L272$: [a, 4, 14, 5] , $g_{272} = 2, s_{272} = (80, 80), t_{272} = (80, 80), r_{272} = (80, 77)$, belongs to $T28$.

  $m_{272} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L273$: [a, 4, 14, 7] , $g_{273} = 2, s_{273} = (80, 80), t_{273} = (80, 80), r_{273} = (76, 76)$, belongs to $T31$.

  $m_{273} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L274$: [a, 4, 14, 13] , $g_{274} = 2, s_{274} = (80, 80), t_{274} = (80, 80), r_{274} = (80, 76)$, belongs to $T29$.

  $m_{274} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L275$: [a, 4, 14, 15] , $g_{275} = 2, s_{275} = (80, 80), t_{275} = (80, 80), r_{275} = (77, 77)$, belongs to $T30$.

  $m_{275} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L276$: [a, 8, 14, 5] , $g_{276} = 1, s_{276} = (80), t_{276} = (80), r_{276} = (77)$, belongs to $T28$.

  $m_{276} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L277$: [a, 8, 14, 7] , $g_{277} = 1, s_{277} = (80), t_{277} = (80), r_{277} = (76)$, belongs to $T31$.

  $m_{277} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L278$: [a, 8, 14, 13] , $g_{278} = 1, s_{278} = (80), t_{278} = (80), r_{278} = (76)$, belongs to $T29$.

  $m_{278} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L279$: [a, 8, 14, 15] , $g_{279} = 1, s_{279} = (80), t_{279} = (80), r_{279} = (77)$, belongs to $T30$.

  $m_{279} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L280$: [c, 2, 13, 5] , $g_{280} = 2, s_{280} = (80, 80), t_{280} = (80, 80), r_{280} = (77, 77)$, belongs to $T32$.

  $m_{280} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L281$: [c, 2, 13, 7] , $g_{281} = 2, s_{281} = (80, 80), t_{281} = (80, 80), r_{281} = (76, 80)$, belongs to $T35$.

  $m_{281} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L282$: [c, 2, 13, 13] , $g_{282} = 2, s_{282} = (80, 80), t_{282} = (80, 80), r_{282} = (76, 76)$, belongs to $T33$.

  $m_{282} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L283$: [c, 2, 13, 15] , $g_{283} = 2, s_{283} = (80, 80), t_{283} = (80, 80), r_{283} = (77, 80)$, belongs to $T34$.

  $m_{283} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

- $L284$: [c, 8, 13, 5] , $g_{284} = 1, s_{284} = (80), t_{284} = (80), r_{284} = (77)$, belongs to $T32$.
  $m_{284} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L285$: [c, 8, 13, 7] , $g_{285} = 1, s_{285} = (80), t_{285} = (80), r_{285} = (76)$, belongs to $T35$.
  $m_{285} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L286$: [c, 8, 13, 13] , $g_{286} = 1, s_{286} = (80), t_{286} = (80), r_{286} = (76)$, belongs to $T33$.
  $m_{286} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L287$: [c, 8, 13, 15] , $g_{287} = 1, s_{287} = (80), t_{287} = (80), r_{287} = (77)$, belongs to $T34$.
  $m_{287} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L288$: [c, 2, 14, 5] , $g_{288} = 2, s_{288} = (80, 80), t_{288} = (80, 80), r_{288} = (77, 77)$, belongs to $T36$.
  $m_{288} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L289$: [c, 2, 14, 7] , $g_{289} = 2, s_{289} = (80, 80), t_{289} = (80, 80), r_{289} = (76, 80)$, belongs to $T39$.
  $m_{289} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L290$: [c, 2, 14, 13] , $g_{290} = 2, s_{290} = (80, 80), t_{290} = (80, 80), r_{290} = (76, 76)$, belongs to $T37$.
  $m_{290} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L291$: [c, 2, 14, 15] , $g_{291} = 2, s_{291} = (80, 80), t_{291} = (80, 80), r_{291} = (77, 80)$, belongs to $T38$.
  $m_{291} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.
- $L292$: [c, 8, 14, 5] , $g_{292} = 1, s_{292} = (80), t_{292} = (80), r_{292} = (77)$, belongs to $T36$.
  $m_{292} = 3$ bits (k_{30}: [15, 31, 47]) could be deduced from k_2, k_{28}, k_{29}.
- $L293$: [c, 8, 14, 7] , $g_{293} = 1, s_{293} = (80), t_{293} = (80), r_{293} = (76)$, belongs to $T39$.
  $m_{293} = 4$ bits (k_{30}: [1, 17, 33, 49]) could be deduced from k_2, k_{28}, k_{29}.
- $L294$: [c, 8, 14, 13] , $g_{294} = 1, s_{294} = (80), t_{294} = (80), r_{294} = (76)$, belongs to $T37$.
  $m_{294} = 4$ bits (k_{30}: [7, 23, 39, 55]) could be deduced from k_2, k_{28}, k_{29}.
- $L295$: [c, 8, 14, 15] , $g_{295} = 1, s_{295} = (80), t_{295} = (80), r_{295} = (77)$, belongs to $T38$.
  $m_{295} = 3$ bits (k_{30}: [9, 25, 41]) could be deduced from k_2, k_{28}, k_{29}.

G Table Tk used in Attacking 29-round PRESENT-80

All Tk tables contains the 64-bit k_{30}. Bits colored in red are those can be deduced from the 64-bit k_{30}.

- Table $T0$ of size 2^{69}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [13, 29, 45, 61]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]

- Included Linear Hulls:
  [4, 2, 5, 13], [4, 2, 9, 13], [4, 4, 5, 13], [4, 4, 9, 13], [4, 2, 13, 13]

- Table $T1$ of size 2^{69}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [15, 31, 47, 63]
    k_{29}: [3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, 51, 55, 59, 63]
  - Included Linear Hulls:
    [4, 2, 5, 15], [4, 2, 9, 15], [4, 4, 5, 15], [4, 4, 9, 15], [4, 2, 13, 15]

- Table $T2$ of size 2^{69}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [5, 21, 37, 53]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [4, 8, 5, 5], [4, 8, 9, 5], [4, 8, 13, 5]

- Table $T3$ of size 2^{69}
  - Key Bits Need to Guess in K_1, K_2, K_{28}, K_{29}:
    k_1: [32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47]
    k_2: [24, 25, 26, 27]
    k_{28}: [7, 23, 39, 55]
    k_{29}: [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61]
  - Included Linear Hulls:
    [4, 8, 5, 7], [4, 8, 9, 7], [4, 8, 13, 7]

H Attack Parameters of Linear Hulls in the 29-Round Attack on PRESENT-80

- $L0$: [4, 2, 5, 13] , $g_0 = 2, s_0 = (64, 64), t_0 = (64, 64), r_0 = (45, 45)$, belongs to $T0$.

  $m_0 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 7, 8, 12, 16, 20, 23, 24, 28, 32, 36, 40, 44, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L1$: [4, 2, 5, 15] , $g_1 = 2, s_1 = (64, 64), t_1 = (64, 64), r_1 = (45, 48)$, belongs to $T1$.

  $m_1 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 8, 9, 12, 16, 20, 24, 25, 28, 32, 36, 40, 44, 57]) could be deduced from k_2, k_{28}, k_{29}.

- $L2$: [4, 2, 9, 13] , $g_2 = 2, s_2 = (64, 64), t_2 = (64, 64), r_2 = (45, 45)$, belongs to $T0$.

  $m_2 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 7, 8, 12, 16, 20, 23, 24, 28, 32, 36, 40, 44, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L3$: [4, 2, 9, 15] , $g_3 = 2, s_3 = (64, 64), t_3 = (64, 64), r_3 = (45, 48)$, belongs to $T1$.

  $m_3 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 8, 9, 12, 16, 20, 24, 25, 28, 32, 36, 40, 44, 57]) could be deduced from k_2, k_{28}, k_{29}.

- $L4$: [4, 8, 5, 5] , $g_4 = 1, s_4 = (64), t_4 = (64), r_4 = (47)$, belongs to $T2$.

  $m_4 = 17$ bits (k_1: [43, 44, 45, 46], k_{30}: [2, 6, 10, 14, 15, 18, 22, 26, 30, 34, 38, 42, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L5$: [4, 8, 5, 7] , $g_5 = 1, s_5 = (64), t_5 = (64), r_5 = (46)$, belongs to $T3$.

  $m_5 = 18$ bits (k_1: [43, 44, 45, 46], k_{30}: [1, 2, 6, 10, 14, 17, 18, 22, 26, 30, 34, 38, 42, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L6$: [4, 8, 9, 5] , $g_6 = 1, s_6 = (64), t_6 = (64), r_6 = (47)$, belongs to $T0$.

  $m_6 = 17$ bits (k_1: [43, 44, 45, 46], k_{30}: [2, 6, 10, 14, 15, 18, 22, 26, 30, 34, 38, 42, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L7$: [4, 8, 9, 7] , $g_7 = 1, s_7 = (64), t_7 = (64), r_7 = (46)$, belongs to $T1$.

  $m_7 = 18$ bits (k_1: [43, 44, 45, 46], k_{30}: [1, 2, 6, 10, 14, 17, 18, 22, 26, 30, 34, 38, 42, 49]) could be deduced from k_2, k_{28}, k_{29}.

- $L8$: [4, 4, 5, 13] , $g_8 = 2, s_8 = (64, 64), t_8 = (64, 64), r_8 = (48, 45)$, belongs to $T0$.

  $m_8 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 7, 8, 12, 16, 20, 23, 24, 28, 32, 36, 40, 44, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L9$: [4, 4, 5, 15] , $g_9 = 2, s_9 = (64, 64), t_9 = (64, 64), r_9 = (45, 45)$, belongs to $T1$.

  $m_9 = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 8, 9, 12, 16, 20, 24, 25, 28, 32, 36, 40, 44, 57]) could be deduced from k_2, k_{28}, k_{29}.

- $L10$: [4, 4, 9, 13] , $g_{10} = 2, s_{10} = (64, 64), t_{10} = (64, 64), r_{10} = (48, 45)$, belongs to $T2$.

  $m_{10} = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 7, 8, 12, 16, 20, 23, 24, 28, 32, 36, 40, 44, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L11$: [4, 4, 9, 15] , $g_{11} = 2, s_{11} = (64, 64), t_{11} = (64, 64), r_{11} = (45, 45)$, belongs to $T3$.

  $m_{11} = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 8, 9, 12, 16, 20, 24, 25, 28, 32, 36, 40, 44, 57]) could be deduced from k_2, k_{28}, k_{29}.

- $L12$: [4, 2, 13, 13] , $g_{12} = 2, s_{12} = (64, 64), t_{12} = (64, 64), r_{12} = (45, 45)$, belongs to $T0$.

  $m_{12} = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 7, 8, 12, 16, 20, 23, 24, 28, 32, 36, 40, 44, 55]) could be deduced from k_2, k_{28}, k_{29}.

- $L13$: [4, 2, 13, 15] , $g_{13} = 2, s_{13} = (64, 64), t_{13} = (64, 64), r_{13} = (45, 48)$, belongs to $T1$.

  $m_{13} = 19$ bits (k_1: [43, 44, 45, 46], k_{30}: [0, 4, 8, 9, 12, 16, 20, 24, 25, 28, 32, 36, 40, 44, 57]) could be deduced from k_2, k_{28}, k_{29}.

- $L14$: [4, 8, 13, 5] , $g_{14} = 1, s_{14} = (64), t_{14} = (64), r_{14} = (47)$, belongs to $T2$.

  $m_{14} = 17$ bits (k_1: [43, 44, 45, 46], k_{30}: [2, 6, 10, 14, 15, 18, 22, 26, 30, 34, 38, 42, 47]) could be deduced from k_2, k_{28}, k_{29}.

- $L15$: [4, 8, 13, 7] , $g_{15} = 1, s_{15} = (64), t_{15} = (64), r_{15} = (46)$, belongs to $T3$.

  $m_{15} = 18$ bits (k_1: [43, 44, 45, 46], k_{30}: [1, 2, 6, 10, 14, 17, 18, 22, 26, 30, 34, 38, 42, 49]) could be deduced from k_2, k_{28}, k_{29}.

I Fast Walsh Transform Pruned to Affine Subspaces [Fló22]

Algorithm 3: Fast Walsh Transform pruned to affine subspaces [Fló22]

```
**Parameters:** $L \subseteq x_0 + X \subseteq \mathbb{F}_2^n, M \subseteq u_0 + U \subseteq \mathbb{F}_2^n$, $(X, U$ subspaces) ;
**Input:** $\widehat{f} : L \to \mathbb{C}$ ;
**Output:** $\widehat{f} : M \to \mathbb{C}$ ;
$\mathcal{B}_X = \{y_1, \ldots, y_t\} \leftarrow$ GetBasis$(X/(X \cap U^{\perp}))$ ;
$\mathcal{B}_U = \{v_1, \ldots, v_t\} \leftarrow$ GetBasis$(U/(U \cap X^{\perp}))$ ;
for $k \leftarrow 1$ to $t-1$ do
    while $\langle y_k, v_k \rangle$ do
        $(v_k . v_{k+1}, \ldots, v_{t-1}, v_t) \leftarrow (v_{k+1}, \ldots, v_{t-1}, v_t, v_k)$;
    for $i \leftarrow k+1$ to $t$ do
        $y_i \leftarrow y_i + \langle y_i, v_k \rangle y_k$ ;
    for $j \leftarrow k+1$ to $t$ do
        $v_j \leftarrow v_j + \langle y_k, v_j \rangle v_k$ ;
let $g : \mathbb{F}_2^t \to \mathbb{C},\ g(y) = 0\ \forall y\ \in \mathbb{F}_2^t$;
for each $x \in L$ do
    $(i_1, \ldots, i_t) \leftarrow$ GetCoordinates$(\overline{x - x_0}, \mathcal{B}_X)$ ;
    $g(i_1, \ldots, i_t) \leftarrow g(i_1, \ldots, i_t) + (-1)^{\langle x - x_0, u_0 \rangle} f(x)$ ;
$g \leftarrow FWT(g)$;
for each $u \in M$ do
    $(j_1, \ldots, j_t) \leftarrow$ GetCoordinates$(\overline{u - u_0}, \mathcal{B}_U)$;
    $\widehat{f}(u) \leftarrow (-1)^{\langle x_0, u \rangle} g(j_1, \ldots, j_t)$ ;
return $\widehat{f}$
```