Des. Codes Cryptogr. (2017) 83:467–492
DOI 10.1007/s10623-016-0242-3

Truncated differential based known-key attacks on round-reduced SIMON

Yonglin Hao[1] · **Willi Meier**[2]

Received: 28 January 2016 / Revised: 13 June 2016 / Accepted: 16 June 2016 /
Published online: 28 June 2016

Abstract At Crypto 2015, Blondeau, Peyrin and Wang proposed a truncated-differential-based known-key attack on full PRESENT, a nibble oriented lightweight block cipher with an SPN structure. The truncated difference they used is derived from the existing multidimensional linear characteristics. An innovative technique of their work is the design of a MITM layer added before the characteristic that covers extra rounds with a complexity lower than that of a generic construction. We notice that there are good linear hulls for bit-oriented block cipher SIMON corresponding to highly qualified truncated differential characteristics. Based on these characteristics, we propose known-key distinguishers on round-reduced SIMON block cipher family, which is bit oriented and has a Feistel structure. Similar to the MITM layer, we design a specific start-from-the-middle method for pre-adding extra rounds with complexities lower than generic bounds. With these techniques, we launch basic known-key attacks on round-reduced SIMON. We also involve some key guessing technique and further extend the basic attacks to more rounds. Our known-key attacks can reach as many as 29/32/38/48/63-rounds of SIMON32/48/64/96/128, which comes quite close to the full number of rounds. To the best of our knowledge, these are the first known-key results on the block cipher SIMON.

Keywords Cryptanalysis · Truncated differential · Known-key attack · SIMON

Communicated by C. Mitchell.

✉ Yonglin Hao
haoyl12@mails.tsinghua.edu.cn

Willi Meier
willi.meier@fhnw.ch

[1] Department of Computer Science and Technology, Tsinghua Universtiy, Beijing 100084, China

[2] FHNW, Windisch, Switzerland

Mathematics Subject Classification 94A60 · 14G50 · 11T71

1 Introduction

Lightweight cryptographic primitives are designated for the implementation and protection in resource-constrained environments such as RFID tags. The wide use of smart cards and wireless sensor networks has largely stimulated the research on lightweight block ciphers. During the past decade or so, a large number of well designed lightweight block ciphers, such as PRESENT [11], mCrypton [29], LED [23], Prince [12], Piccolo [39], KLEIN [22], TWINE [42], KATAN & KTANTAN [13], HIGHT [24] etc., have been proposed providing reasonable trade-off between the performance and security.

In 2013, NSA proposed a new family of lightweight block ciphers named SIMON [5,6]. As a Feistel structure based, bit oriented primitive, SIMON eliminated the commonly used S-box substitutions and its round function only consists of bitwise AND, XOR and rotation, leading to an optimized performance in hardware. Ever since its proposal, SIMON has drawn the attention of many researchers and the security evaluation of SIMON has become a hot topic in the community of cryptology. Various cryptanalysis methods have been used to analyze SIMON [1–4,7,14,26,34,37,38,40,41,43,44]. These results focus on the security of SIMON under the classical secret single-key model. It is noticeable that block ciphers are often adapted to build cryptographic hash functions with methods such as the PGV schemes [8,33]. From this perspective, SIMON is a natural candidate to build lightweight compression functions and hash functions. Therefore, the resistance of SIMON against known-key attacks is in close relationship with the security of potential SIMON-based hash functions as is proved in [30].

Known-key attacks (also referred as known-key distinguishers) on block ciphers were introduced by Knudsen and Rijmen at Asiacrypt 2007 [25]. Unlike the setting of the conventional single-key model, the adversary in the known-key model knows the randomly drawn key that the cipher operates with. With the knowledge of the key, the adversary is supposed to find a non-random property that an ideal cipher (a randomly drawn permutation) should not have.

In the original [25], the authors used the integral property and successfully distinguished 7-round AES from a random permutation. This property works quite well on AES-like block ciphers so that many refinements and extensions emerged afterwards [20,31,36]. Recently at Asiacrypt 2014, Gilbert [21] eventually gives an integral-based known-key attack on full 10-round AES-128. Besides the integral, other non-random properties can be applied as well for constructing known-key attacks. There are known-key attacks using differential characteristics [27,32], linear hulls [28], collisions [18,19,35] and so on.

Very recently at Crypto 2015, Blondeau, Peyrin and Wang [10] proposed a truncated differential based known-key attack on full PRESENT, an SPN-based, nibble oriented block cipher. The truncated differential characteristic they used was first given in [9] and is derived from some multidimensional linear approximations. Their innovative technique is the application of a meet-in-the-middle (MITM) layer. The MITM layer can not only pre-add extra rounds, but also collect conforming plaintexts deterministically. With some gradual matching algorithm, the complexity of this deterministic data collection in the MITM layer is much lower than that of the generic probabilistic method.

Our Contributions In this paper, we give an evaluation to the security of SIMON under the known-key model. More specifically, we show that the procedure as developed for the known-key distinguisher on full PRESENT in [10] can be applied to SIMON, despite its quite different design. To achieve this goal, we develop several specific methods to reach almost the full number of rounds of SIMON.

We derive truncated differential characteristics from some available linear hulls used previously in secret single-key attacks using the methods of [9]. Secondly, although the gradual matching technique cannot work for the bit oriented cipher SIMON, we still manage to find a way to pre-add a MITM layer and deterministically collect data with a lower complexity than the probabilistic generic method.

With the characteristics and the MITM layer, we manage to launch our basic known-key attacks on round-reduced SIMON of all versions. These basic attacks can reach at least as many rounds as the secret single-key recoveries and can distinguish the cipher from a random permutation with significant success probabilities.

The combination of truncated differentials and MITM has already enabled Blondeau et al. to attack full PRESENT, but this is not the case for SIMON. In order to extend the basic attacks to more rounds, we lend the idea of Gilbert in [21]. By involving some subkey guesses in the checking phase, we extend our basic attacks by 5–7 rounds. As is thoroughly discussed in [21], these extended attacks are non-generic and meaningful since they are “efficiently checkable”. Furthermore, thanks to the property of SIMON, the extended attacks share exactly the same success probabilities with their basic counterparts.

We summarize our main results in Table 1. There are 8 attacks numbered as Attack 1–8 using different characteristics and targeting at different SIMON versions. To the best of our knowledge, these are the first known-key results on SIMON. We also implemented Attacks 1–2 that are targeting at SIMON32 and their complexities are practical. The results are in accordance with our deductions, indicating the effectiveness of our attacks.

Organization of the paper In Sect. 2, we introduce the theoretic basis and the general procedure of our attacks. It also involves a brief introduction to the SIMON block cipher. Then, we detail our basic truncated-differential based known-key attacks on SIMON in Sect. 3. We discuss the method of extending the basic attacks to more rounds in Sect. 4. The correctness of our attacks are practically verified in Sect. 5. Finally, we conclude the whole paper in Sect. 6.

2 Preliminary

In the first part of this section, we give an introduction to our theoretic basis, a combination of [10,21]. Then, we describe the general procedure of the truncated-differential-based known-key attacks. In the 3rd part, we briefly introduce SIMON.

Table 1 The truncated differential based known-key attacks on round-reduced SIMON

SIMON	Attack	Rounds			Complexity		Success prob. (%)	Chara.
version	no.	Basic	Extended	Total	Data	Time		source
32	1	23	28	32	2^{30}	2^{30}	66.94	[2][a]
	2	24	29		2^{30}	2^{30}	59.48	[2][a]
48	3	24	30	36	2^{46}	2^{46}	99.99	[1][a]
	4	25	31		2^{46}	2^{46}	99.86	[41][a]
	5	26	32		2^{46}	2^{46}	54.10	[2]
64	6	31	37	42/44	2^{62}	2^{62}	83.63	[1][a]
96	7	41	48	52/54	2^{94}	2^{94}	89.09	[1][a]
128	8	56	63	68/69/72	2^{126}	2^{126}	89.09	[1][a]

[a] These characteristics are also used by Chen et al. for key recoveries in [14]

2.1 Combining two different known-key attacks

The basic idea of our known-key attacks on SIMON originates from the method on full PRESENT in [10]. Our extended attacks are following the criteria given in [21] where the author extended the basic attack on 8-round AES to the full 10-round version. Like all the attacks under the the known-key model, the adversaries in [10,21] are given a white box access to an instance of the encryption function associated with a known random key and its inverse. But their purposes are slightly different.

The adversary in [21] aims at simultaneously controlling the inputs and the outputs of the block cipher to achieve a non-random property that cannot be acquired by replacing the block cipher with a random permutation within the same time complexity. As a formalization of the known-key model, [21] gives the concept of "T-Intractable Relation" which we cite as Definition 1.

Definition 1 (*T-Intractable Relation* [21]) Let $E : (K, X) \in \{0, 1\}^k \times \{0, 1\}^n \to E_K(X) \in \{0, 1\}^n$ denote a block cipher of block size n bits. Let $N \geq 1$ and $\mathcal{R}$ denote an integer and any relation over the set S of N-tuples of n-bit blocks. $\mathcal{R}$ is said to be T-intractable relatively to E if, given any algorithm $\mathcal{A}'$ that is given an oracle access to a perfect random permutation π of $\{0, 1\}^n$ and its inverse, it is impossible for $\mathcal{A}'$ to construct in time $T' \leq T$ two N-tuples $\mathcal{X}' = (X'_i)$ and $\mathcal{Y}' = (Y'_i)$ such that $Y'_i = \pi(X'_i)$, $i = 1 \ldots N$ and $\mathcal{X}'\mathcal{R}\mathcal{Y}'$ with a success probability $p' \geq 1/2$ over π and the random choices of $\mathcal{A}'$. The computing time T' of $\mathcal{A}'$ is measured as an equivalent number of computations of E, with the convention that the time needed for one oracle query to π or π^{-1} is equal to 1. Thus if q' denotes the number of queries of $\mathcal{A}'$ to π or π^{-1}, $q' \leq T'$.

Based on the T-Intractable Relation, [21] also gives a formal criterion for a non-generic and meaningful known-key attack and we cite it as Definition 2.

Definition 2 (*Known-Key Distinguisher*) Let $E : (K, X) \in \{0, 1\}^k \times \{0, 1\}^n \to E_K(X) \in \{0, 1\}^n$ denote a block cipher of block size n bits. A known-key distinguisher $(\mathcal{R}, \mathcal{A})$ of order $N \geq 1$ consists of (1) a relation $\mathcal{R}$ over the N-tuples of n-bit blocks; (2) An algorithm $\mathcal{A}$ that on input a k-bit key K produces in time $T_{\mathcal{A}}$, i.e. in time equivalent with $T_{\mathcal{A}}$ computations of E, an N-tuple $\mathcal{X} = (X_i)_{i=1,\ldots,N}$ of plaintext blocks and an N-tuple $Y = (Y_i)_{i=1,\ldots,N}$ of ciphertext blocks related by $Y_i = E_K(X_i)$, for which the following conditions must be met:

(i) The relation $\mathcal{R}$ must be $T_{\mathcal{A}}$-intractable relatively to E.

(ii) The validity of $\mathcal{R}$ must be efficiently checkable: this requirement is formalized by incorporating the time for checking whether two N-tuples are related by R in the computing time $T_{\mathcal{A}}$ of algorithm $\mathcal{A}$.

It is specifically claimed in [21] that the criterion (ii) is avoiding specifying an explicit upper bound on the time complexity for checking whether two N-tuples are related by $\mathcal{R}$. It is restricted that, in order to make the known-key attack non-generic, the time complexity for checking $\mathcal{R}$ should be no more than the N computations of E. The known-key attack on AES in [21] follows strictly the criteria in Definition 2. The integral-based property is suitable for the start-from-the-middle strategy, so that the adversary can construct the N-tuple input & output blocks with exactly N computations of E. Therefore, the relation chosen in [21] is definitely N-intractable. Besides, [21] stress that no information related to K should not provided when checking the relation $\mathcal{R}$, which is also necessary for making their extended attack on 10-round AES meaningful.

The scenario for the known-key attack on full PRESENT in [10] is quite straightforward. In [10], there is an oracle $\mathcal{O}$ that can be either a full PRESENT primitive E_K (the master key K is known) or a random permutation π. The adversary needs to distinguish whether $\mathcal{O} = E_K$ or $\mathcal{O} = \pi$ with N queries of $\mathcal{O}$ at a success probability $P_S > 50\,\%$. Although this known-key attack seems different from that of [21], we believe that they are not contradicting. The distinguisher of [10] is based on some truncated differential property. Following the interpretation of [21], the relation $\mathcal{R}$ of this attack can be described as:

Relation $\mathcal{R}$ in [10]: $(X_i)_{i=1,\ldots,N}\mathcal{R}(Y_i)_{i=1,\ldots,N}$ iff

- $X_1, \ldots, X_N$ share the same value at bits $[52, 55]$
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(Y_i, Y_j)_{1\le i<j\le N}$ colliding at bits $[52, 55]$

The τ parameter is based on the truncated differential characteristics of PRESENT and is affected by the selection of N. This relation $\mathcal{R}$ of PRESENT is not suitable for the start-from-the-middle strategy in [21] and there is no characteristic that can cover all 31 rounds of PRESENT. As a result, [10] has to add a 7-round MITM layer before a 24-round truncated differential characteristic to collect the N input blocks needed. The procedure of the known-key attack on full PRESENT can be summarized into three phases as follows:

Preparation: Collect the conforming N-tuple plaintexts $\mathcal{X} = (X_1, \ldots X_N)$

Construction: Construct the N-tuple ciphertexts $\mathcal{Y} = (Y_1, \ldots, Y_N)$ by querying $\mathcal{O}$ as $Y_i = \mathcal{O}(X_i)$ for $i = 1, \ldots, N$.

Checking: Check whether there is $\mathcal{X}\mathcal{R}\mathcal{Y}$. If there is $\mathcal{X}\mathcal{R}\mathcal{Y}$, make the judgment $\mathcal{O} = E_K$; otherwise, $\mathcal{O} = \pi$.

The probability of $\mathcal{X}\mathcal{R}\mathcal{Y}$ when $\mathcal{O} = E_K$ is denoted by p_0 and that when $\mathcal{O} = \pi$ is denoted by p_1. So the success probability of this known-key attack is $P_S = 2^{-1}[p_0 + (1 - p_1)]$. For full PRESENT, according to [10], there is $P_S = 50.5\%$, higher than that of the random guess $(50\,\%)$ so the attack is meaningful.

It might be doubtful that the preparation phase of this attack also involves the master key K and it requires some computations as well. But we insist that the $\mathcal{R}$-relation of [10] can still be regarded as N-intractable since the construction phase is still dominating the overall complexity and the N plaintext & ciphertext pairs are generated at the lowest possible complexity, which is exactly N queries to $\mathcal{O}$.

In our basic attacks on SIMON, we strictly follow the procedure in [10]. As to the extended attacks, the preparation and construction phases are typically unchanged while the checking phase will involve some key guesses making the complexity increase. But we can prove that this increment does not violate the criterion (ii) of Definition 2, so our extended attacks are still meaningful.

2.2 The truncated differential based known-key attack

We give a generalized description of the method derived in [10]. Some notations used throughout this paper are as follows:

E_K: The block cipher controlled by the master key K.
n: The block size of E_K.
π: A random permutation. $\pi : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$.
X: A n-bit state is denoted by a capital letter (and similarly, the n-bit intermediate state after r processed encryption rounds of E_K).
$X[i]$: The i-th bit of the state X, where $i = 0, 1, \ldots, n-1$, from the LSB (the leftmost bit of X) to MSB (the rightmost bit of X).
$\mathcal{I}$: A sequence of indices $\mathcal{I} = (i_s, \ldots, i_1)$ where $0 \leq i_1 < \ldots < i_s \leq n-1$. Specifically, we denote the bit sequence $X[\mathcal{I}] = (X[i_s], \ldots, X[i_1])$.
$\oplus \wedge \vee \lll$: Denote bitwise XOR by $\oplus$, AND by $\bigwedge$, OR by $\bigvee$, cyclic left rotation by $\lll$.

We consider that E_K starts from S_{r_0} (plaintext) and ends at S_{r_2} (ciphertext). As set out in (1), the intermediate state S_{r_1} divides E_K into two parts: the **TD** part and the **MITM** part.

$$E_K : S_{r_0} \xrightarrow[E_K^{(0)}]{MITM} S_{r_1} \xrightarrow[E_K^{(1)}]{TD} S_{r_2} \tag{1}$$

TD. A truncated differential characteristic is placed in the TD part. For two predefined sequences $\mathcal{I}_1, \mathcal{I}_2$,

$$\mathcal{I}_1 = (i_s, \ldots, i_1), \quad s \geq 1 \tag{2}$$

$$\mathcal{I}_2 = (j_q, \ldots, j_1), \quad q \geq 1, \tag{3}$$

the corresponding truncated differential characteristic can be described as Property 1.

Property 1 *For two n-bit intermediate states (S_{r_1}, S'_{r_1}) satisfying*

$$S_{r_1}[\mathcal{I}_1] = S'_{r_1}[\mathcal{I}_1], \tag{4}$$

the corresponding (S_{r_2}, S'_{r_2}) after $r_2 - r_1$ rounds of encryptions conform $S_{r_2}[\mathcal{I}_2] = S'_{r_2}[\mathcal{I}_2]$ with probability

$$P_{TD} = Pr\left\{S_{r_2}[\mathcal{I}_2] = S'_{r_2}[\mathcal{I}_2]\right\} = 2^{-q} \cdot (1 + C), \quad C > 0 \tag{5}$$

where C is a parameter decided by the block cipher and the truncated differential characteristic itself.

If (S_{r_2}, S'_{r_2}) are generated by a random permutation π, the probability $S_{r_2}[\mathcal{I}_2] = S'_{r_2}[\mathcal{I}_2]$ is apparently $2^{-q} < P_{TD}$. Therefore, if we can find sufficiently many pairs (S_{r_1}, S'_{r_1}) conforming (4), we can utilize Property 1 to distinguish E_K from a random permutation.

MITM. For a predefined $\mathcal{I}_0$ s.t. $|\mathcal{I}_0| = |\mathcal{I}_1| = s$, the MITM part aims at finding N plaintexts $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ satisfying

$$\begin{cases} S_{r_0}^{(i)}[\mathcal{I}_0] = Cst_0 \\ S_{r_1}^{(i)}[\mathcal{I}_1] = Cst_1 \end{cases} \quad i \in [1, N], \tag{6}$$

where Cst_0 and Cst_1 are constant values of $\mathbb{F}_2^s$. In this way, $\binom{N}{2} \approx N^2/2$ pairs conforming (4) are acquired. The trivial way to construct the structure (6) requires $2^s N$ trials of $S_{r_0} \rightarrow S_{r_1}$. This method is probabilistic rather than deterministic. Furthermore, the generic $2^s N$ computations of $S_{r_0} \rightarrow S_{r_1}$ are likely to exceed the N queries to $\mathcal{O}$, making our attacks unavailable. Therefore, the authors of [10] used the match in the middle strategy as shown in (7).

$$Cst_0 = S_{r_0}[\mathcal{I}_0] \xrightarrow{Encrypt} S_{r_m} \underset{Matching}{\overset{Sub-Nibble}{\longleftrightarrow}} X_{r_m} \xleftarrow{Decrypt} S_{r_1}[\mathcal{I}_1] = Cst_1 \tag{7}$$

They start from the $S_{r_0}[\mathcal{I}_0]$ and $S_{r_1}[\mathcal{I}_1]$, and match at the Sub-Nibble layer in the middle. For the SPN structure based, nibble-oriented PRESENT, the Sub-Nibble layer is only 16 parallelised 4-bit Sboxes. The intermediate state S_{r_m} $(r_0 < r_m < r_1)$ can be deduced nibble by nibble using the gradual matching technique [10]. After $S_{r_m}^{(1)}, \ldots, S_{r_m}^{(N)}$ are acquired, the corresponding plaintexts $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ can be deduced through partial decryptions. This method is deterministic. The complexity of the partial decryption is only about $0.5N$, and the computations of $S_{r_0} \rightarrow S_{r_1}$ and the complexity of the gradual matching are even lower. So the overall complexity of this deterministic method is lower than the generic $2^s N$.

With the predefined $\mathcal{I}_0, \mathcal{I}_1, \mathcal{I}_2$, the relation of the known-key attack can be defined as

Relation $\mathcal{R}$: $(S_{r_0}^{(i)})_{i=1,\ldots,N} \mathcal{R} (S_{r_2}^{(i)})_{i=1,\ldots,N}$ iff

- $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ share the same value Cst_0 at bits $\mathcal{I}_0$
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(S_{r_2}^{(i)}, S_{r_2}^{(j)})_{1 \le i < j \le N}$ colliding at bits $\mathcal{I}_2$

Following the description in Sect. 2.1, the 3 phases of the truncated-differential-based known-key attacks can be summarized as follows:

Preparation: Collect the N specific plaintexts:

1. Deduce the plaintexts $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ conforming (6).

Construction: Acquire the ciphertexts from the oracle:

2. Query the oracle for the ciphertexts $S_{r_2}^{(i)} = \mathcal{O}(S_{r_0}^{(i)})$ for $i = 1, \ldots, N$.

Checking: Check whether the plaintext & ciphertext pairs conform $\mathcal{R}$:

3. Count for ψ, the number of ciphertext pairs colliding on $S_{r_2}[\mathcal{I}_2]$:

$$\psi := \# \left\{ (S_{r_2}^{(i)}, S_{r_2}^{(j)}) : S_{r_2}^{(i)}[\mathcal{I}_2] = S_{r_2}^{(j)}[\mathcal{I}_2], 1 \le i < j \le N \right\}$$

4. If $\psi > \tau$, we conclude $\mathcal{O} = E_K$; otherwise, $\mathcal{O} = \pi$.

Let $N_S = \binom{N}{2} \approx N^2/2$ be the total number of ciphertext pairs. Apparently we have $\psi \le N_S$. We define the two probabilities Pr_0 and Pr_1 as

$$Pr_0 := Pr\{\psi > \tau | \mathcal{O} = E_K\} \tag{8}$$

$$Pr_1 := Pr\{\psi \le \tau | \mathcal{O} = \pi\}. \tag{9}$$

Since $\mathcal{O}$ can be either E_K or π with equal chances, the success probability of this known-key attack can be determined as

$$P_S = \frac{Pr_0 + Pr_1}{2}. \tag{10}$$

The known-key attack can only be regarded as "effective" when $P_S > 0.5$. This requires a proper assignment of the τ value.

Equation (10) is a precise evaluation to the success probability P_S. But the parameters Pr_0 and Pr_1 defined in (8) and (9) are hard to acquire other than running the experiments for many times, which is impractical. Therefore, based on some rational assumptions, [9,10] give a method to determine both τ and P_S simultaneously with N, C, q. They assume that: for $\mathcal{O} = E_K$, the variable ψ follows the normal distribution $Norm(\mu_R, \sigma_R^2)$; for $\mathcal{O} = \pi$, $\psi \sim Norm(\mu_W, \sigma_W^2)$ where

$$\begin{cases} \mu_R = N_S \cdot 2^{-q} \cdot (1 + C) \\ \mu_W = N_S \cdot 2^{-q} \end{cases} \quad \begin{cases} \sigma_R^2 = N_S \cdot 2^{-q} \cdot (1 + C) \cdot \left[1 - 2^{-q}(1 + C)\right] \\ \sigma_W^2 = N_S \cdot 2^{-q} \cdot \left(1 - 2^{-q}\right) \end{cases} \tag{11}$$

According to [10], the success probability of this attack (P_S) is

$$P_S = \Phi\left(\frac{\mu_R - \mu_W}{\sigma_R + \sigma_W}\right) \approx \Phi\left(\frac{\sqrt{2^{-q} \cdot N_S} \cdot C}{2}\right). \tag{12}$$

and the τ parameter in Step 4 can be decided accordingly as:

$$\tau = \mu_R - \sigma_R \cdot \Phi^{-1}(P_S) = \mu_W + \sigma_W \cdot \Phi^{-1}(P_S). \tag{13}$$

The computations in the checking phase are negligible, so the overall complexity is dominated by the N queries to the oracle in the construction phase.

Although the computation of P_S in (12) is only an approximation compared with (10), (12) is more suitable for theoretical deductions. Therefore, we use (12) to deduce the theoretic success probabilities in Table 1, as well as the τ value in (13). And, in Sect. 5, we use (10) to get the exact success probability with the experimentally acquired Pr_0 and Pr_1.

2.3 Brief introduction to SIMON

SIMON is a family of lightweight block ciphers with a Feistel structure. According to the block size n, we denote the 5 SIMON versions as SIMONn where $n = 32/48/64/96/128$. The intermediate state S_r consists of two $\frac{n}{2}$-bit words $x_{r+1}, x_r \in \mathbb{F}_2^{\frac{n}{2}}$ as $S_r = (x_{r+1}, x_r)$. Therefore we have $x_r = S_r[\frac{n}{2} - 1, \ldots, 0]$ and $x_{r+1} = S_r[n - 1, \ldots, \frac{n}{2}]$. The r-th ($r = 0, 1, \ldots$) round function of SIMONn is

$$S_r = (x_{r+1}, x_r) \xrightarrow{r\text{-th Round}} S_{r+1} = (x_{r+2}, x_{r+1}) = (F(x_{r+1}) \oplus x_r \oplus k_r, x_{r+1}) \tag{14}$$

where $F : \mathbb{F}_2^{\frac{n}{2}} \rightarrow \mathbb{F}_2^{\frac{n}{2}}$,

$$F(x) = ((x \lll 8) \wedge (x \lll 1)) \oplus (x \lll 2). \tag{15}$$

The k_r in (14) is the round key generated with the key schedule. The key schedule as well as other details of SIMON is not used in this paper and we refer interested readers to [5].

3 Basic known-key attacks on SIMON

The basic known-key attacks on SIMON follow the procedure summarized in Sect. 2.2. We first deduce the truncated differential for the TD part based on the existing linear approximations. Then, we introduce our deterministic method for constructing conforming plaintexts within the MITM part. In the third part, we describe the detailed procedure of our known-key attacks on different SIMON versions.

3.1 The truncated differential characteristics in the TD part

A large number of highly qualified linear characteristics for SIMON have been found in recent works. Based on these linear approximations, many (secret) single-key attacks are proposed.

We define the operation $\odot : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ as

$$X \odot Y := \bigoplus_{i=0}^{n-1} (X[i] \wedge Y[i])$$

A n-bit word X can also be determined with the set $\mathcal{B}(X)$ containing all the indices of the active bits of X:

$$\mathcal{B}(X) := \{i \in [0, n-1] : X[i] = 1\}.$$

and we have

$$X \odot Y = \bigoplus_{i \in \mathcal{B}(X)} Y[i]$$

For a linear hull (Γ_1, Γ_2) of $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, its correlation, denoted by $\mathbf{cor}(\Gamma_1, \Gamma_2)$, is defined as

$$\begin{aligned}\mathbf{cor}(\Gamma_1, \Gamma_2) := {} & Pr\left[(\Gamma_1 \odot X) \oplus (\Gamma_2 \odot F(X)) = 0\right] \\ & - Pr\left[(\Gamma_1 \odot X) \oplus (\Gamma_2 \odot F(X)) = 1\right]\end{aligned}$$

If we have s linearly independent Γ_1's, denoted by $\Gamma_1^1, \ldots, \Gamma_1^s$, and q linearly independent Γ_2's, denoted by $\Gamma_2^1, \ldots, \Gamma_2^q$, any of the 2^{s+q} linear combinations $(\Gamma_1^{(\nu_1,\ldots,\nu_s)}, \Gamma_2^{(\omega_1,\ldots,\omega_q)})$ defined as

$$\begin{aligned}\Gamma_1^{(\nu_1,\ldots,\nu_s)} &= \nu_1 \Gamma_1^1 \oplus \ldots \oplus \nu_s \Gamma_1^s, \\ \Gamma_2^{(\omega_1,\ldots,\omega_q)} &= \omega_1 \Gamma_2^1 \oplus \ldots \oplus \omega_q \Gamma_2^q\end{aligned}$$

where $\nu_i, \omega_j \in \{0, 1\}, i \in [1, s], j \in [1, q]$, can still be regarded as a linear approximation. Combining the 2^{s+q} linear approximations makes a multidimensional linear approximation which can be transformed to a truncated differential characteristic according to Theorem 1.

Theorem 1 [9] *Let* $\mathbb{F}_2^n = \mathbb{F}_2^s \times \mathbb{F}_2^t = \mathbb{F}_2^q \times \mathbb{F}_2^r$ *and*

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n, x = (x_s, x_t) \to (y_q, y_r)$$

Given a multidimensional approximation $\left[(a_s, 0), (b_q, 0)\right]_{a_s \in \mathbb{F}_2^s, b_q \in \mathbb{F}_2^q}$ *with capacity*

$$C = \sum_{(a_s, b_q) \neq (0,0)} \mathbf{cor}^2 \left[(a_s \odot x_s) \oplus (b_q \odot y_q)\right],$$

and a truncated differential composed of 2^t *input differences* $(0, \sigma_t) \in \{0\} \times \mathbb{F}_2^t$*, and* 2^r *output differences* $(0, \gamma_r) \in \{0\} \times \mathbb{F}_2^r$ *with probability*

$$P_{TD} = \frac{1}{2^q} \sum_{(\sigma_t, \gamma_r) \in \mathbb{F}_2^t \times \mathbb{F}_2^r} \mathbf{P}\left[(0, \sigma_t) \to (0, \gamma_r)\right]$$

where $\mathbf{P}\left[(0, \sigma_t) \to (0, \gamma_r)\right] = 2^{-n} \# \left\{x \in \mathbb{F}_2^n : F(x) \oplus F(x \oplus (0, \sigma_t)) = (0, \gamma_r)\right\}$. *We have*

$$P_{TD} = 2^{-q}(C + 1).$$

As to traditional linear hulls for SIMON, we have $s = q = 1$ and Theorem 1 is still applicable as has been proved in [9]. Suppose that a linear hull (Γ_1, Γ_2) is placed at the TD part of E_K in (1). Its correlation is $\mathbf{cor}(\Gamma_1, \Gamma_2)$ defined as

$$\begin{aligned}\mathbf{cor}(\Gamma_1, \Gamma_2) = Pr &\left[(\Gamma_1 \odot S_{r_1}) \oplus (\Gamma_2 \odot S_{r_2}) = 0\right] \\ -Pr &\left[(\Gamma_1 \odot S_{r_1}) \oplus (\Gamma_2 \odot S_{r_2}) = 1\right]\end{aligned}$$

and its capacity can also be acquired as $C = 2^{-1} \cdot \mathbf{cor}^2(\Gamma_1, \Gamma_2)$. Then, according to Theorem 1, we can derive a truncated differential characteristic having Property 2.

Property 2 *For a pair* (S_{r_1}, S'_{r_1}) *satisfying* $\Gamma_1 \odot S_{r_1} = \Gamma_1 \odot S'_{r_1}$*, their corresponding* (S_{r_2}, S_{r_2}) *will have the property*

$$Pr\left[\Gamma_2 \odot S_{r_2} = \Gamma_2 \odot S'_{r_2}\right] = P_{TD} = 2^{-1}(1 + C).$$

In this way, all existing linear hulls of SIMON can be transformed to truncated differential characteristics that can be used for our known-key attacks.

3.2 The data collections in the MITM part

The MITM part of SIMON also aims at constructing plaintexts $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ and their corresponding $S_{r_1}^{(1)}, \ldots, S_{r_1}^{(N)}$ satisfying

$$\begin{cases} S_{r_0}^{(i)}[\lambda] = 0 \\ \Gamma_1 \odot S_{r_1}^{(i)} = 0 \end{cases} \quad i \in [1, N] \tag{16}$$

where $\lambda \in [0, n-1]$ is a predefined index. Apparently, the probabilistic method for acquiring these plaintexts requires $2N$ queries of $S_{r_0} \to S_{r_1}$ and we are going to propose a deterministic method for data collections with lower complexity than the generic bound.

Unfortunately, there is no gradual matching for bit-oriented SIMON. Instead of matching in the middle, we use the start from the middle strategy as shown in (17),

$$S_{r_0}[\lambda] \xleftarrow{Decrypt} S_{r_m} \xrightarrow{Encrypt} \Gamma_1 \odot S_{r_1}. \tag{17}$$

Our method is based on Observation 1

Observation 1 *Let* $\mathbf{v} = (v_0, \ldots, v_n)$ *where* $v_0, \ldots, v_n$ *are boolean variables. Supposing that we have a boolean function* F *s.t.: for some* $i \in [0, n]$, *the algebraic normal form (ANF) of* F *can be regarded as:*

$$F(\mathbf{v}) = v_i + G \tag{18}$$

where $G \in \mathbb{F}_2[v_0, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n]$ *is irrelevant to the variable* v_i. *Then, we can nullify* F *by modifying* $\mathbf{v}$ *to* $\mathbf{v}'$ *defined as*

$$\mathbf{v}'[j] = \begin{cases} \mathbf{v}[j], & j \neq i \\ G, & j = i \end{cases} \tag{19}$$

With this modification, we have $F(\mathbf{v}') = 0$. *In this case, we refer* v_i *as a "linear variable" of* F.

Linear variables do widely occur in primitives with low-degree updating functions. Dinur and Shamir have already used linear variables to nullify the crucial bits and successfully launched dynamic cube key recovery attacks on the stream cipher Grain-128 [15,17].

Apparently, both of the two bits $S_{r_0}[\lambda]$ and $\Gamma_1 \odot S_{r_1}$ in (17) are boolean functions of the intermediate state S_{r_m}. The knowledge of the whole ANF in (18) is essential for the key recoveries in [15,17]. Even with very few rounds of iterations, the ANFs of SIMON's intermediate bits will become extremely complicated which barricades us from further extensions. But in fact, the explicit expressions of the ANFs are unnecessary for our known-key attacks. We only need to know two indices u and v such that: $S_{r_m}[u]$ is a linear variable of $\Gamma_2 \odot S_{r_1}$ and $S_{r_m}[v]$ is a linear variable of $S_{r_0}[\lambda]$. Therefore, instead of deducing ANFs, we identify available pairs (u, v) in a probabilistic manner:

1. We define a sufficiently large integer T as the test strength (for example $T = 2^{13}$).
2. For all of the (u, v) pairs, which is $n \cdot (n-1)$ in total, we do the following substeps:
   (a) We run Algorithm 1 with inputs $((u, v), T)$
   (b) If Algorithm 1 returns 1, (u, v) is available with a probability $1 - 2^{-T}$; otherwise, (u, v) is unavailable with probability 1.

As can be seen from (15), the updating function of SIMON is only of degree 2 and its linear diffusion is also weak, enabling us to find linear variables after several rounds. Therefore, our MITM part for SIMON can pre-add at least 9 rounds to the truncated differential characteristics.

The plaintexts we need should conform (16) which is a 2-bit filter, so there are only 2^{n-2} available. With (u, v) settled (supposing that $0 \leq u < v \leq n-1$), we claim that, for all $N \leq 2^{n-2}$, we can deterministically collect N available plaintexts with $MITM(\lambda, \Gamma_1, u, v)$ described as in Algorithm 2.

Algorithm 1: Identify whether a candidate (u, v) is available.

```
Input: Candidate pair $(u, v) \in \mathbb{Z}_n \times \mathbb{Z}_n$, $u \neq v$; the test strength $T \in \mathbb{Z}^+$.
Output: 1 (if $(u, v)$ is available) or 0 (if $(u, v)$ is unavailable).
Initialize $\gamma \leftarrow 1$.
for $i = 1, \ldots, T$ do
    Randomly pick a intermediate state $S_{r_m}$ and a masterkey $K$.
    Compute from $S_{r_m}$ and acquire the bit $\Gamma_2 \odot S_{r_1}$.
    Update the $v$-th bit of $S_{r_m}$ as $S_{r_m}[v] \leftarrow S_{r_m}[v] \oplus (\Gamma_2 \odot S_{r_1})$.
    Compute from $S_{r_m}$ and acquire the bit $S_{r_0}[\lambda]$.
    Update the $u$-th bit of $S_{r_m}$ as $S_{r_m}[u] \leftarrow S_{r_m}[v] \oplus S_{r_0}[\lambda]$.
    Compute from $S_{r_m}$ and acquire both $S_{r_0}[\lambda]$ and $\Gamma_2 \odot S_{r_1}$.
    if $S_{r_0}[\lambda] = \Gamma_2 \odot S_{r_1} = 0$ then
        Continue;
    else
        Assign $\gamma \leftarrow 0$ and break.
    end if
end for
Return $\gamma$.
```

Algorithm 2: Construct Available Plaintexts in the MITM Part $MITM(\lambda, \Gamma_1, u, v)$

```
Input: The targeted bit position $\lambda$. The number of plaintexts $N$. The input mask $\Gamma_1$. The available
    $(u, v) \in \mathbb{Z}_n \times \mathbb{Z}_n$ corresponding to $\Gamma_1$ and $\lambda$. The unknown oracle $\mathcal{O} \in \{E_K, \pi\}$
Output: The plaintexts $S_{r_0}^{(1)}, \ldots, S_{r_0}^{(N)}$ conforming (16).
1: Define the sequence $\mathcal{I}_m := \{x \in [0, n-1] : x \neq u, x \neq v\}$.
2: Select $N$ $S_{r_m}$'s, denoted as $S_{r_m}^{(1)}, \ldots, S_{r_m}^{(N)}$ that are mutually different in bits $S_{r_m}[\mathcal{I}_m]$.
3: for $i = 1, \ldots, N$ do
4:     Compute from $S_{r_m}^{(i)}$ to the bit $\Gamma_1 \odot S_{r_1}^{(i)}$ and update $S_{r_m}^{(i)}[u] \leftarrow S_{r_m}[u] \oplus (\Gamma_1 \odot S_{r_1}^{(i)})$.
5:     Compute backward from $S_{r_m}^{(i)}$ to the bit $S_{r_0}^{(i)}[\lambda]$ and update $S_{r_m}^{(i)}[v] \leftarrow S_{r_m}[v] \oplus S_{r_0}^{(i)}[\lambda]$.
6: end for
7: for $i = 1, \ldots, N$ do
8:     Compute from $S_{r_m}^{(i)}$ the plaintext $S_{r_0}^{(i)}$.
9: end for
```

The complexity of this data collection is no more than $1.5N$ computations of $S_{r_0} \rightarrow S_{r_1}$, lower than the generic bound $2N$. Furthermore, since the ratio $(r_1 - r_0)/(r_2 - r_0)$ of our attacks is much smaller than $(1.5)^{-1} = \frac{2}{3}$, this $1.5N$ computations of $S_{r_0} \rightarrow S_{r_1}$ is significantly lower than that of the N queries of $\mathcal{O}$ in the construction phase. Step 2 of Algorithm 2 makes sure that the plaintexts are distinct for all $N \leq 2^{n-2}$ and the procedure is deterministic.

3.3 The basic known-key attacks on SIMON

The truncated differential characteristics we used are derived from the existing linear hulls which have been verified by previous secret single-key attacks such as [2,14]. According to Sect. 2.2, a truncated differential characteristic can be determined by the parameters: Γ_1, Γ_2, C and $r_2 - r_1$. According to Sect. 3.2, the MITM part can be determined by the parameters: $\lambda, u, v, r_1 - r_m, r_m - r_0$. The relation $\mathcal{R}$ of the basic attacks are defined as

Relation $\mathcal{R}$: $(S_{r0}^{(i)})_{i=1,\ldots,N}\mathcal{R}(S_{r2}^{(i)})_{i=1,\ldots,N}$ iff

- $S_{r0}^{(1)},\ldots,S_{r0}^{(N)}$ share the same value 0 at bit λ;
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(S_{r2}^{(i)},S_{r2}^{(j)})_{1\le i<j\le N}$ satisfying $\Gamma_2\odot S_{r2}^{(i)}=\Gamma_2\odot S_{r2}^{(j)}$.

The attack procedure on SIMONn is as follows:

1. Collect N ($N\le 2^{n-2}$) plaintexts $S_{r0}^{(1)},\ldots,S_{r0}^{(N)}=MITM(\lambda,\Gamma_1,u,v)$ using Algorithm 2. (**Preparation**)
2. Query the oracle $\mathcal{O}$ for the ciphertexts $S_{r2}^{(i)}=\mathcal{O}(S_{r0}^{(i)})$ for $i=1,\ldots,N$. (**Construction**)
3. Assign a counter $m=0$. (**Checking**)
4. For $i=1,\ldots,N$, if $\Gamma_2\odot S_{r2}^{(i)}=0$, update $m\leftarrow m+1$. (**Checking**)
5. Assign $\psi\leftarrow\binom{m}{2}+\binom{N-m}{2}$. (**Checking**)
6. If $\psi>\tau$, make the judgment $\mathcal{O}=E_K$; otherwise, $\mathcal{O}=\pi$. (**Checking**)

The complexity of the construction phase is dominated by the N queries to the oracle $\mathcal{O}$ in Step 2, which is also the overall complexity of the whole known-key attack. The checking phase only involves the XOR operations of computing $\Gamma_2\odot S_{r2}^{(i)}=0$ for $i=1,\ldots,N$ whose complexity is much lower than that of the construction phase.

The success probability P_S and the τ parameter can be approximated with the method in Sect. 2.2.

Detailed parameters of our basic attacks are shown in Table 2. The attacks can mount to r_2-r_0 rounds, which is equal to the summation of the numbers in the 3rd, 4th and 11th column.

4 Further extension of the basic attacks

In [21], Gilbert extends the basic 8-round attack on AES to 10 rounds by involving some subkey guesses in the checking phase. He proved that: as long as the complexity of the checking phase is significantly lower than that of the construction phase, the known-key distinguishers can still be meaningful. This criterion is formally stated in (ii) of Definition 2. [21] also stress the necessity of key guesses considering that no information related to the key should be provided in the checking phase.

We can also apply the method in [21] to extend the basic distinguishers forward and backward. After the extension, the block cipher E_K in (1) is now transformed to (20)

$$E_K: S_{r_b}\xrightarrow[E_K^{(b)}]{BExt}S_{r_0}\xrightarrow[E_K^{(0)}]{MITM}S_{r_1}\xrightarrow[E_K^{(1)}]{TD}S_{r_2}\xrightarrow[E_K^{(f)}]{FExt}S_{r_f}\tag{20}$$

where $BExt$ is short for "Backward Extension" and $FExt$ for "Forward Extension".

In the extended attacks, we are still using the collision properties of the two bits $S_{r_0}[\lambda]$ and $\Gamma_2\odot S_{r_2}$. To acquire these two bits, some subkey bits, k_b and k_f, are to be guessed in the checking phase so that we can acquire $S_{r_0}[\lambda]$ and $\Gamma_2\odot S_{r_2}$ through partial encryptions & decryptions denoted as

$$S_{r_0}[\lambda]=P(k_b,S_{r_b}),\quad \Gamma_2\odot S_{r_2}=Q(k_f,S_{r_f}).\tag{21}$$

Table 2 Basic truncated differential based known-key attacks on SIMONn where n is the block size

n	No.	MITM					TD					P_S
		$r_m - r_0$	$r_1 - r_m$	λ	u	v	$\mathcal{B}(\Gamma_1)$	$\mathcal{B}(\Gamma_2)$	C	$r_2 - r_1$	Source	
32	1	5	5	31	14	7	22	14	$2^{-29.69}$	13	[2]*	66.94 %
	2	5	5	23	8	15	0	24, 6	$2^{-30.56}$	14	[2]*	59.48 %
48	3	6	3	29	7	29	43, 35, 31, 17, 9	29, 19, 11, 7, 3	$2^{-42.11}$	15	[1]*	100.00 %
	4	6	3	30	17	30	45, 29, 25, 23	29, 25, 23	$2^{-42.92}$	16	[41]*	99.86 %
	5	6	3	24	18	24	46, 38, 30, 26, 0	24, 22, 16, 14, 6, 2	$2^{-47.78}$	17	[2]	54.10 %
64	6	6	4	33	22	57	56, 52, 22	54, 24, 20	$2^{-60.52}$	21	[1]*	83.63 %
96	7	7	4	51	44	49	90, 86, 82, 50, 36	94, 90, 50, 40, 0	$2^{-92.2}$	30	[1]*	89.09 %
128	8	8	7	64	2	64	126, 122, 66, 60	124, 62, 58, 2, 0	$2^{-124.6}$	41	[1]*	89.09 %

The P_S can be acquired with the data complexity $N = 2^{n-2}$ for $n = 32/48/64/96/128$

* These characteristics are also used by Chen et al. for key recoveries in [14]

The ALH in [14] has $ALH = 2^{-2} \cdot C$

The selection of k_b makes sure that there is only one $\alpha \in \{0, 1\}^{|k_b|}$ conforming $P(\alpha, S_{r_b}^{(i)}) = 0$ for all $i = 1, \ldots, N$. The correct assignment of k_f should enable us to acquire the desired ψ parameter at the lowest cost. The determinations of k_b and k_f are to be detailed in Sect. 4.2. The computation of P requires no more than $\frac{r_0-r_b}{r_f-r_b}$ computations while Q requires $\frac{r_f-r_2}{r_f-r_b}$. Therefore, the relation $\mathcal{R}$ of this attack is now transformed as

Relation $\mathcal{R}$: $(S_{r_b}^{(i)})_{i=1,\ldots,N}\mathcal{R}(S_{r_f}^{(i)})_{i=1,\ldots,N}$ iff there are bit strings $\alpha \in \mathbb{F}_2^{|k_b|}$ and $\beta \in \mathbb{F}_2^{|k_f|}$ conforming to:

- $P(\alpha, S_{r_b}^{(i)}) = 0$ for all $i = 1, \ldots, N$;
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(S_{r_f}^{(i)}, S_{r_f}^{(j)})_{1\leq i<j\leq N}$ satisfying $Q(\beta, S_{r_f}^{(i)}) = Q(\beta, S_{r_f}^{(j)})$.

The procedure of this extended attack will be changed accordingly as follows:

1. Collect the N ($N \leq 2^{n-2}$) intermediate states satisfying (16) and compute backward for their plaintexts $S_{r_b}^{(1)}, \ldots, S_{r_b}^{(N)}$. (**Preparation**)
2. Query the oracle $\mathcal{O}$ for the ciphertexts $S_{r_f}^{(i)} = \mathcal{O}(S_{r_b}^{(i)})$ for $i = 1, \ldots, N$. (**Construction**)
3. Set a table $\mathcal{T}$ consisting of $2^{|k_f|}$ counters and initiate them to 0 ($\mathcal{T}[s] \leftarrow 0$ for all $s = 0, \ldots, 2^{|k_b|+|k_f|} - 1$). (**Checking**)
4. Initialize a flag $\mathfrak{f} \leftarrow 0$.
5. For the $\alpha = 0, \ldots, 2^{|k_b|} - 1$, we do the following substeps: (**Checking**)
   (a) For all $i = 1, \ldots, N$, if for any $P(\alpha, S_{r_b}^{(i)}) \neq 0$, then continue.
   (b) Assign $\mathfrak{f} \leftarrow 1$ and break;
6. For $\beta = 0, \ldots, 2^{|k_f|} - 1$, we do the following substeps: (**Checking**)
   (a) Initialize a $m \leftarrow 0$.
   (b) For all $i = 1, \ldots, N$, if $Q(\beta, S_{r_f}^{(i)}) = 0$, update $m \leftarrow m + 1$.
   (c) Update $\mathcal{T}[\beta] \leftarrow \binom{m}{2} + \binom{N-m}{2}$.
7. Assign $\psi \leftarrow \max \mathcal{T}$. (**Checking**)
8. If $\psi > \tau$ and $\mathfrak{f} = 1$, make the judgment $\mathcal{O} = E_K$; otherwise, $\mathcal{O} = \pi$. (**Checking**)

4.1 The complexity analysis of the extended attacks

The preparation and construction phases of the extended attack resemble that of the basic attack and the overall complexity is still dominated by the N times of $\mathcal{O}$ queries in the construction phase.

The complexity of the checking phase, denoted as θ, is somewhat complicated. With the subkey bits k_b and k_f involved, the complexity of the checking phase has largely increased. The more extension $r_0 - r_b$ ($r_f - r_2$) gets, the bigger the key length $|k_b|$ ($|k_f|$) will be and the complexity θ will grow accordingly. According to (ii) in Definition 2, the extended distinguishers can still be meaningful as long as the relation $\mathcal{R}$ is "efficiently checkable". This criterion restricts that the complexity of the checking phase should be lower than that of the construction phase. In other words, we should make sure $\theta < N$.

The checking phase complexity θ can be estimated step by step. For the inappropriate assignment of $\alpha \in \{0, 1\}^{|k_b|}$, Step 5.(a) will run averaging

$$2^{-N}N + \sum_{i=1}^{N}(i2^i) \approx \frac{1}{1-2^{-1}} = 2$$

computations P before continuing to $\alpha + 1$. Such an assignment of α can reach Step 5.(b) with a negligible probability 2^{-N}. So the complexity of Step 2 is bounded by

$$\left[2 \cdot (2^{|k_b|} - 1) + N\right] \cdot \frac{r_0 - r_b}{r_f - r_b}.$$

Step 6 requires $2^{|k_f|} \cdot N$ computations of $S_{r_f} \to S_{r_2}$. So the overall complexity of the attack can be approximated as

$$\begin{aligned}\theta &= (2^{|k_b|+1} - 2 + N) \cdot \frac{r_0 - r_b}{r_f - r_b} + 2^{|k_f|} \cdot N \cdot \frac{r_f - r_2}{r_f - r_b} \\ &\approx N \cdot \frac{2^{|k_f|} \cdot (r_f - r_2) + (r_0 - r_b)}{r_f - r_b} + 2^{|k_b|+1} \cdot \frac{r_0 - r_b}{r_f - r_b}\end{aligned} \tag{22}$$

The memory complexity of the extended attacks is bounded by the size of $\mathcal{T}$ which is $2^{|k_f|}$.

In order to keep $\theta < N$, we restrict k_b and k_f to conform (23).

$$\begin{cases} |k_b| < \log N \\ |k_f| < \log \frac{r_f - r_b}{r_f - r_2 + r_0 - r_b} \end{cases} \tag{23}$$

4.2 Determine k_b and k_f

For any extension r_b and r_f, we need to determine the corresponding key bits k_b and k_f required for the computation of the targeted $S_{r_0}[\lambda]$ and $\Gamma_2 \odot S_{r_2}$ respectively. This involves analyzing the ANFs of the targeted bits and is similar to the method used by Dinur et al. in [15] to determine the key guesses for full Grain-128.

For the backward extension, we need to compute the targeted state bit $S_{r_0}[\lambda]$ precisely and k_b should be the subkey bits sufficient and necessary for the computation. The sufficiency requires that the knowledge of k_b is well enough to acquire $S_{r_0}[\lambda]$. The necessity restricts that: for any wrong guess of k_b, denoted as α, it should be impossible for the N plaintexts to conform $P(\alpha, S_{r_b}^{(i)}) = 0$ for $i = 1, \ldots, N$. The computation of the whole state S_{r_0} involves the $\frac{n}{2}$-bit round keys, denoted as $K_{r_b}, \ldots, K_{r_0-1}$ and obviously k_b is only a part of them. We identify the k_b by analyzing the ANF of $S_{r_0}[\lambda]$ as follows.

For $i \in [r_b, r_0 - 1]$, we assign its j-th bit ($j \in [0, \frac{n}{2} - 1]$) with a symbolic boolean variable $x_{\frac{n}{2}\cdot i+j}$ such that $K_i[j] = x_{\frac{n}{2}\cdot i+j}$. The n plaintext bits of S_{r_0} are assigned to n boolean variables $v_0, \ldots, v_{n-1}$ such that $S_{r_b}[i] = v_i$ for $i = 0, \ldots, n-1$. With this S_{r_b} and round keys $K_{r_b}, \ldots, K_{r_0-1}$, we run the encryption procedure of the first $r_0 - r_b$ rounds and acquire the ANF of $S_{r_0}[\lambda]$ which, following the notations in [16], can be represented as

$$\begin{aligned}S_{r_0}[\lambda] &= P(k_b, S_{r_b}) = f(\mathbf{x}, \mathbf{v}) \\ &= \sum_{u=(u_0,\ldots,u_{n-1})\in\mathbb{F}_2^n} a_u M_u\end{aligned} \tag{24}$$

where $\mathbf{v} = (v_0, \ldots, v_{n-1})$, $\mathbf{x} = (x_0, \ldots, x_L)$ ($L = \frac{n}{2} \cdot (r_0 - r_b) - 1$), $M_u = \prod_{i=0}^{n-1} v_i^{u_i}$, $a_u = a_u(\mathbf{x}) \in \mathbb{F}_2[x_0, \ldots, x_L]$ and the function P is defined as (21). We also define $P^*(k_b, S_{r_b}) = f^*(\mathbf{x}, \mathbf{v})$ as

$$\hat{S}_{r_0}[\lambda] = P^*(k_b, S_{r_b}) = f^*(\mathbf{x}, \mathbf{v}) = f(\mathbf{x}, \mathbf{v}) + a_0 = \sum_{u \in \mathbb{F}_2^n \setminus \{0\}} a_u M_u.$$

By analyzing the ANF of $f(\mathbf{x}, \mathbf{v})$ and $f^*(\mathbf{x}, \mathbf{v})$, we have the following observation.

Observation 2 *For SIMON, we divide the set of indices $\{0, \ldots, L\}$ into three non-overlapping categories as follows:*

1. *Let $\mathcal{X}$ contain all the indices i s.t. the corresponding x_i's affect $f^*(\mathbf{x}, \mathbf{v})$. Therefore, $\mathcal{X}$ can be defined as*

$$\mathcal{X} := \left\{ i \in [0, L] : x_i \in f^*(\mathbf{x}, \mathbf{v}) \right\}$$

where $x_i \in f^*(\mathbf{x}, \mathbf{v})$ indicates that x_i appears in the ANF $f^*(\mathbf{x}, \mathbf{v})$.

2. *Let $\mathcal{L}_x$ be the set of indices l s.t. $l \notin \mathcal{X}$ and the key bits x_l are linear variables of $f(\mathbf{x}, \mathbf{v})$. More formally, we define $\mathcal{L}_x$ as:*

$$\mathcal{L}_x := \{ l \notin \mathcal{X} : f(\mathbf{x}, \mathbf{v}) = x_l + \eta, \text{ where } \eta \text{ is irrelevant to } x_l \}.$$

3. *The remaining indices j are all categorized as $\overline{\mathcal{X} \cup \mathcal{L}_x}$ and the corresponding key bits x_j have no effect on the targeted bit.*

We stress that such a categorization is suitable for all extended attacks on SIMON but we do not expect it to be available elsewhere. With Observation 2, we can define the set of index $\mathcal{P}$ as

$$\mathcal{P} := \mathcal{X} \cup \{l\}$$

where l is an arbitrary element of $\mathcal{L}$. Then, we can have

$$k_b := x_{\mathcal{P}}.$$

For the correct encryptions, we have $S_{r_0}^{(i)}[\lambda] = 0$ for all $i = 1, \ldots, N$. The correct guess of key bits $x_{\mathcal{X}}$ will ensure that $\hat{S}_{r_0}^{(i)}[\lambda] = \delta$ for some static $\delta \in \{0, 1\}$ and all of $i = 1, \ldots, N$. Since x_l is a linear variable of $f(\mathbf{x}, \mathbf{v})$ and $l \notin \mathcal{X}$, we know that x_l can only affect the value a_0. So there must be one assignment of x_l s.t. $a_0 = \delta$. Therefore, this assignment of x_l along with the correct guess of $x_{\mathcal{X}}$ will ensure that $S_{r_0}^{(i)}[\lambda] = 0$ for all $i = 1, \ldots, N$.

The determination of k_f is quite similar to that of k_b. We assign the ciphertext to $\mathbf{v}$ and the involved round keys $K_{r_b-1}, K_{r_b-2}, \ldots, K_{r_2}$ are assigned to $\mathbf{y} = (y_0, \ldots, y_{L'})$ where $L' = \frac{n}{2} \cdot (r_f - r_2) - 1$. Then, the ANF of the targeted $\Gamma_2 \odot S_{r_2}$ can be represented as

$$\begin{aligned} \Gamma_2 \odot S_{r_2} &= Q(k_f, S_{r_f}) = g(\mathbf{y}, \mathbf{v}) \\ &= \sum_{u \in \mathbb{F}_2^n} c_u M_u \end{aligned}$$

where $c_u = c_u(\mathbf{y}) \in \mathbb{F}_2[y_0, \ldots, y_{L'}]$. We also have

$$\widehat{\Gamma_2 \odot S_{r_2}} = Q^*(k_f, S_{r_f}) = g(\mathbf{y}, \mathbf{v}) + c_0 = \sum_{u \in \mathbb{F}_2^n \setminus \{0\}} c_u M_u. \tag{25}$$

We can also divide the indices $\{0, \ldots, L'\}$ into $\mathcal{Y}$, $\mathcal{L}_y$ corresponding to the $\mathcal{X}$ and $\mathcal{L}_x$ in Observation 2. However, instead of $y_l \| y_{\mathcal{Y}}$ $(l \in \mathcal{L}_y)$, we find that letting $k_f := y_{\mathcal{Y}}$ is well enough for us to acquire the final ψ parameter as is proved in Proposition 1.

Proposition 1 *Supposing that $k_f = y_l \| y_{\mathcal{Y}}$ where $l \in \mathcal{L}_y$, then for any $\zeta \in \mathbb{F}_2^{|k_f|-1}$, we have*

$$\mathcal{T}[y_l \| \zeta] = \mathcal{T}[(y_l + 1) \| \zeta] \tag{26}$$

and the final ψ cannot be affected by the correct guessing of y_l.

Proof As to $\mathcal{T}[y_l \| \zeta]$, we denote the set $\mathcal{W}(y_l, \zeta)$

$$\mathcal{W}(y_l, \zeta) = \left\{ i \in [1, N] : Q\left(y_l \| \zeta, S_{r_f}^{(i)}\right) = 0 \right\}$$

so we have

$$\mathcal{T}[y_l \| \zeta] = \binom{|\mathcal{W}(y_l, \zeta)|}{2} + \binom{N - |\mathcal{W}(y_l, \zeta)|}{2}.$$

According to the definition of y_l, we know that y_l is linear to the targeted bit $\Gamma_2 \odot S_{r_f}$ which means

$$Q\left(y_l \| \zeta, S_{r_f}^{(i)}\right) = Q\left((y_l + 1) \| \zeta, S_{r_f}^{(i)}\right) + 1$$

for all $i \in [1, N]$. Therefore, we know that

$$\begin{aligned} \mathcal{W}(y_l + 1, \zeta) &= \left\{ i \in [1, N] : Q\left((y_l + 1) \| \zeta, S_{r_f}^{(i)}\right) = 0 \right\} \\ &= \left\{ i \in [1, N] : Q\left(y_l \| \zeta, S_{r_f}^{(i)}\right) = 1 \right\} \\ &= \overline{\mathcal{W}(y_l, \zeta)} \end{aligned}$$

and $|\mathcal{W}(y_l + 1, \zeta)| = N - |\mathcal{W}(y_l, \zeta)|$. So the $\mathcal{T}[(y_l + 1) \| \zeta]$ satisfies

$$\begin{aligned} \mathcal{T}[(y_l + 1) \| \zeta] &= \binom{|\mathcal{W}(y_l + 1, \zeta)|}{2} + \binom{N - |\mathcal{W}(y_l + 1, \zeta)|}{2} \\ &= \binom{N - |\mathcal{W}(y_l, \zeta)|}{2} + \binom{|\mathcal{W}(y_l, \zeta)|}{2} \\ &= \mathcal{T}[y_l \| \zeta] \end{aligned}$$

which proves (26). Since $\psi = \max \mathcal{T}$, there is some $\delta \in \mathbb{F}_2$, $\zeta \in \mathcal{F}_2^{|k_f|-1}$ satisfying

$$\psi = \mathcal{T}[\delta \| \zeta] = \mathcal{T}[(\delta + 1) \| \zeta].$$

This indicate that the assignment of y_l cannot affect the final ψ value of the extended attacks. □

Proposition 1 make it safe for us to determine $k_f = y_{\mathcal{Y}}$. We show later that this property enables us to extend the basic attack forward by 1 round for free and the extended attacks share the same success probability P_S with their corresponding basic attacks.

4.3 The success probability of the extended attacks

When $|k_f| = 0$ (equivalently $r_f = r_2$), the only non-zero entry of $\mathcal{T}$ is $\mathcal{T}[k_b]$. In this situation, the P_S, as well as the parameter τ, of this extended attack is equal to that of its basic counterpart.

For $|k_f| > 0$ ($r_f > r_2$), the success probability is slightly complicated. We refer to the table $\mathcal{T}$ corresponding to $\mathcal{O} = E_K$ and $\mathcal{O} = \pi$ as $\mathcal{T}^{E_K}$, $\mathcal{T}^{\pi}$ respectively. According to [9], the maximum entries of $\mathcal{T}^{E_K}$ and $\mathcal{T}^{\pi}$, denoted by $\max \mathcal{T}^{E_K}$, $\max \mathcal{T}^{\pi}$, follows the normal distribution as (27).

$$\max \mathcal{T}^{E_K} \sim Norm(\mu_R, \sigma_R^2), \qquad \max \mathcal{T}^{\pi} \sim Norm(\mu_W, \sigma_W^2) \tag{27}$$

As long as we can figure out the parameters $\mu_R, \mu_W, \sigma_R, \sigma_W$, we can evaluate the success probability P_S of the extended known-key attacks using (12). The τ parameter can be acquired accordingly as (13).

We denote the density function of variable $X \sim Norm(\mu, \sigma^2)$ by $f_{\mu,\sigma}(x)$ and the cumulative function as $F_{\mu,\sigma}(x)$. There are $2^{|k_f|}$ non-zero entries in $\mathcal{T}$, namely $\mathcal{T}[0], \ldots, \mathcal{T}[k_f], \ldots, \mathcal{T}[(2^{|k_f|} - 1)]$. We have $\mathcal{T}^{E_K}[k_f] \sim Norm(\mu_0, \sigma_0^2)$ where

$$\mu_0 = N \cdot (2^{-1} + 2^{-1}C), \qquad \sigma_0^2 = N \cdot (2^{-2} - 2^{-2}C^2)$$

while the other $\beta \neq k_f$ satisfies $\mathcal{T}^{E_K}[\beta] \sim Norm(\mu_1, \sigma_1^2)$

$$\mu_1 = 2^{-1}N, \qquad \sigma_1^2 = 2^{-2}N.$$

As to the random permutation π, the entry $\mathcal{T}^{\pi}[\beta] \sim Norm(\mu_1, \sigma_1^2)$ for all $\beta \in [0, 2^{|k_f|} - 1]$. Then, our targeted parameters $\mu_R, \mu_W, \sigma_R, \sigma_W$ can be acquired precisely with Propositions 2 and 3.

Proposition 2 *The accumulative function of* $\max \mathcal{T}^{E_K}$ *satisfies*

$$F_{\mu_R,\sigma_R}(x) = Pr\left\{\max \mathcal{T}^{E_K} < x\right\} = F_{\mu_0,\sigma_0}(x) \cdot F_{\mu_1,\sigma_1}^{2^{|k_f|}-1}(x)$$

and the corresponding density function is

$$f_{\mu_R,\sigma_R}(x) = f_{\mu_0,\sigma_0}(x) \cdot F_{\mu_1,\sigma_1}^{2^{|k_f|}-1}(x) + (2^{|k_f|} - 1) \cdot f_{\mu_1,\sigma_1}(x) \cdot F_{\mu_0,\sigma_0}(x) \cdot F_{\mu_1,\sigma_1}^{2^{|k_f|}-2}(x).$$

The parameters μ_R and σ_R^2 can be computed as

$$\mu_R = \int_{-\infty}^{\infty} x \cdot f_{\mu_R,\sigma_R}(x)dx, \qquad \sigma_R^2 = \int_{-\infty}^{\infty} (x - \mu_R)^2 \cdot f_{\mu_R,\sigma_R}(x)dx.$$

Proposition 3 *The accumulative function of* $\max \mathcal{T}^{\pi}$ *satisfies*

$$F_{\mu_W,\sigma_W}(x) = Pr\left\{\max \mathcal{T}^{\pi} < x\right\} = F_{\mu_1,\sigma_1}^{2^{|k_f|}}(x)$$

and the corresponding density function is

$$f_{\mu_W,\sigma_W}(x) = 2^{|k_f|} f_{\mu_1,\sigma_1}(x) \cdot F_{\mu_1,\sigma_1}^{2^{|k_f|}-1}(x).$$

The parameters μ_W and σ_W^2 can be computed as

$$\mu_W = \int_{-\infty}^{\infty} x \cdot f_{\mu_W,\sigma_W}(x)dx, \qquad \sigma_W^2 = \int_{-\infty}^{\infty} (x - \mu_W)^2 \cdot f_{\mu_W,\sigma_W}(x)dx.$$

Table 3 Extended attacks on SIMONn where $n = 32/48/64/96/128$ and the data complexity is $N = 2^{n-2}$

n	No.	$r_f - r_b$	$r_2 - r_0$	$r_0 - r_b$	$\|k_b\|$	$r_f - r_2$	$\|k_f\|$	P_S (%)
32	1	28	23	4	17	1	0	66.94
	2	29	24	4	17	1	0	59.48
48	3	30	24	5	37	1	0	100.00
	4	31	25	5	37	1	0	99.86
	5	32	26	5	37	1	0	54.10
64	6	37	31	5	38	1	0	83.63
96	7	48	41	6	86	1	0	89.09
128	8	63	56	6	108	1	0	89.09

Although the deductions of these parameters are quite straightforward, the complicated integrations are not easy to compute when $|k_f| > 0$.

We increase the parameter $r_0 - r_b$ from 1 and determine the corresponding k_b with the method in Sect. 4.2. In this way, we can find the maximum $r_0 - r_b$ whose k_b does not violates the restriction in (23).

After $r_0 - r_b$ and k_b are settled, we start from $r_f - r_2 = 1$ to identify the corresponding k_f.

For SIMON, the situation of k_f is interesting. When we have $r_f - r_2 = 1$, using the method of Sect. 4.2, we have $\mathcal{Y} = \phi$ so the corresponding $k_f = y_{\mathcal{Y}}$ is an empty string so that $|k_f| = 0$ so the size of the table $\mathcal{T}$ is 1 and $\mathcal{T}[0]$ is its only entry. Instead of computing $\Gamma_2 \odot S_{r_f}$, we only need H defined

$$H^{(i)} := H(S_{r_f}^{(i)}) = \widehat{\Gamma_2 \odot S_{r_f}^{(i)}}, \quad i \in [1, N]$$

where $\widehat{\Gamma_2 \odot S_{r_f}^{(i)}}$ is defined as (25) and it can be acquired merely with the knowledge of the ciphertexts $S_{r_f}^{(i)}$. Let m be the number of i's satisfying $H^{(i)} = 0$. The corresponding ψ value is

$$\psi = \max \mathcal{T} = \mathcal{T}[0] = \binom{m}{2} + \binom{N-m}{2}.$$

In this situation of $r_f - r_2 = 1$ and $|k_f| = 0$, the extended attacks share the same P_S with their corresponding basic attacks. For $r_f - r_2 = 2$, the $|k_f|$ grows dramatically and violates the restriction of (23), indicating a strong diffusion of the SIMON round function. Therefore, all the 8 attacks can only extend forward by 1 round. After the forward extension, the success probabilities remain unchanged.

The parameters of the extended attacks are listed in Table 3.

4.4 A tradeoff in the checking phase

For the plaintexts generated in the construction phase, the appropriate assignment of k_b can ensure that $P(k_b, S_{r_b}^{(i)}) = 0$ for all $i = 1, \ldots, N$. For the inappropriate assignments, this can happen with a probability 2^{-N}. Since there are $2^{|k_b|}-1$ inappropriate assignments, the probability that one of them reaches Step 5.(b) of the extended attacks is $2^{|k_b|-N}$.

N is usually significantly larger than $|k_b|$ and it seems unnecessary for us to use all N plaintexts to filter out all the $2^{|k_b|}-1$ inappropriate assignments. Let $M = O(|k_b|)$ (for example $M = 2|k_b|, 3|k_b|, \dots$). Therefore, we can modify the relation $\mathcal{R}$ of the extended attack as

Relation $\mathcal{R}$: $(S_{r_b}^{(i)})_{i=1,\dots,N}\mathcal{R}(S_{r_f}^{(i)})_{i=1,\dots,N}$ iff there are bit strings $\alpha \in \mathbb{F}_2^{|k_b|}$ and $\beta \in \mathbb{F}_2^{|k_f|}$ conforming to:

- $P(\alpha, S_{r_b}^{(i)}) = 0$ for all $i = 1, \dots, M$;
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(S_{r_f}^{(i)}, S_{r_f}^{(j)})_{1\le i<j\le N}$ satisfying $Q(\beta, S_{r_f}^{(i)}) = Q(\beta, S_{r_f}^{(j)})$.

and the Step 5 of the extended attack should be changed accordingly as follows:

5. For the $\alpha = 0, \dots, 2^{|k_b|}-1$, we do the following substeps: (**Checking**)
   (a) For all $i = 1, \dots, M$, if for any $P(\alpha, S_{r_b}^{(i)}) \neq 0$, then continue.
   (b) Assign $\mathfrak{f} \leftarrow 1$ and break;

The probability that an inappropriate assignment to reach Step 5.(b) is only $2^{|k_b|-M}$ which is still sufficiently low. But the complexity of the online phase can be reduced significantly.

5 Practical verifications

The complexities of Attacks 1–2 (the extended versions) on SIMON32 are practical ($N = 2^{30}$). So we practically implement them to verify the correctness of our methods.

We first detail the procedure of Attack 2. For such a 29-round attack on SIMON32, we can assign

$$r_b = 0, r_0 = 4, r_1 = 14, r_2 = 28, r_f = 29.$$

We assign the plaintext S_0 with boolean variables $\mathbf{v} = (v_0, \dots, v_{31})$ and the subkeys $K_0, \dots, K_3$ with $\mathbf{x} = (x_0, \dots, x_{63})$. By running the partial encryption, we acquire the ANF of $S_4[23] = f(\mathbf{x}, \mathbf{v})$. By analyzing $f(\mathbf{x}, \mathbf{v})$, we can acquire the two sets

$$\mathcal{X} = \{2, 3, 4, 5, 6, 11, 12, 13, 15, 20, 21, 23, 29, 30, 38, 47\}$$
$$\mathcal{L}_x = \{1, 19, 37, 55\}$$

which are defined as Observation 2. We can define $\mathcal{P} = \mathcal{X} \cup \{1\}$ and $k_b = x_{\mathcal{P}}$ so we have $|k_b| = 17$.

For k_f, we first assign the ciphertext S_{29} with boolean variables $\mathbf{v} = (v_0, \dots, v_{31})$ and the subkey K_{28} with $\mathbf{y} = (y_0, \dots, y_{15})$. Then, the ANF of $\Gamma_2 \odot S_{29}$ is

$$\Gamma_2 \odot S_{29} = g(\mathbf{x}, \mathbf{v}) = y_6 + v_4 + v_5v_{14} + v_8 + v_{22}$$

so we have $\mathcal{Y} = \phi$ and $|k_f| = 0$. Therefore, for any ciphertext $S_{29}^{(i)}$ ($i = 1, \dots, N$), we only need to compute

$$H(S_{29}^{(i)}) = \bigoplus_{j\in\{4,8,22\}} (S_{29}^{(i)}[j]) \oplus (S_{29}^{(i)}[5] \wedge S_{29}^{(i)}[14]) \tag{28}$$

Table 4 The parameters for attack 1–2 when $N = 2^{30}$

No.	τ	Pr_0 (%)	Pr_1 (%)	Exp (%)	P_S (%)
1	288230376139236000	45.77	83.92	64.85	66.94
2	288230376027507000	29.56	78.66	54.11	59.48

The column "Exp" is the experimentally acquired success probability according to (10). The P_S column is the theoretic approximation following (12)

and compute the ψ parameter. The relation $\mathcal{R}$ of Attack 3 can be defined as
Relation $\mathcal{R}$: $(S_0^{(i)})_{i=1,\ldots,N}\mathcal{R}(S_{29}^{(i)})_{i=1,\ldots,N}$ iff there are bit strings $\alpha \in \mathbb{F}_2^{17}$ conforming to:

- $P(\alpha, S_0^{(i)}) = 0$ for all $i = 1, \ldots, N$;
- There are more than τ out of the $\binom{N}{2}$ ciphertext pairs $(S_{29}^{(i)}, S_{29}^{(j)})_{1\le i<j\le N}$ satisfying $H(S_{29}^{(i)}) = H(S_{29}^{(j)})$ where $H(\cdot)$ is defined as (28).

In order to acquire the highest P_S, we use the maximum data complexity $N = 2^{30}$ and the corresponding $\tau = 288230376027507000$ using (13). With all parameters settled, we run Attack 3. By modifying $S_9[15, 8]$, we can nullify the $S_4[23]$ and $\Gamma_1 \odot S_{14} = S_{14}[0]$, and collect the N plaintexts $S_0^{(1)}, \ldots, S_0^{(N)}$. For the appropriate assignment of k_b, we have $P(k_b, S_0^{(i)}) = 0$ for all $i = 1, \ldots, N$. For the inappropriate assignments $\alpha \in \mathbb{F}_2^{17}$, the event $P(\alpha, S_0^{(i)}) = 1$ appears within 20 different i attempts as has been verified by our experiments. Therefore, it is safe for us to set $M = 3|k_b| = 51$ and utilize the tradeoff in Sect. 4.4 for lowering the complexity of the checking phase. This tradeoff can only sacrifice the success probability by $2^{|k_b|-M} = 2^{-34}$ which is still negligible. But the running time of Step 5.(a) can lower from 2^{30} to only 51.

With thousands of experiments, we are able to acquire the averaging $Pr_0 \approx 29.56\,\%$ and $Pr_1 \approx 78.66\,\%$ where Pr_0 and Pr_1 are defined as (8) (9) respectively. Since $\mathcal{O}$ has equal possibility to be E_K or π, the experimentally acquired success probability of this known-key attack is 54.11 % according to (10), slightly lower than that of the theoretic 59.48 % but still significantly higher than 50 %. This indicates that our known-key attacks are effective.

The procedure of Attack 1 is the same so we just list the main parameters in Table 4. As can be seen, the experimentally acquired "Exp" is also close to the theoretic P_S.

To sum up, all our experiments are showing the significant success probabilities of Attack 1–2 and indicating the effectiveness of our methods.

6 Conclusion

In this paper, we develop and apply the latest known-key attacking techniques to round-reduced SIMON block cipher. Although our procedures follow a similar pattern as those by Blondeau, Peyrin and Wang, a number of specific methods have been elaborated to achieve known-key distinguishers for many rounds of SIMON. Our known-key attacks are able to mount up to 29/32/38/47/63 rounds for SIMON32/48/64/96/128 respectively, which comes relatively close to the full numbers of rounds. The security margin of SIMON under the known-key model is thus not as large as expected. Our findings do not affect the security of SIMON in a secret single-key scenario.

Acknowledgements The authors would like to thank the anonymous reviewers for their very helpful comments on the preliminary version of this paper. This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834205) and National Natural Science Foundation of China (Grant Nos. 61133013, 61373142).

References

1. Abdelraheem M.A., Alizadeh J., Alkhzaimi H.A., Aref M.R., Bagheri N., Gauravaram P., Lauridsen M.M.: Improved linear cryptanalysis of reduced-round SIMON. IACR Cryptology ePrint Archive 2014, 681 (2014).
2. Abdelraheem M.A., Alizadeh J., AlKhzaimi H.A., Aref M.R., Bagheri N., Gauravaram P.: Improved linear cryptanalysis of reduced-round SIMON-32 and SIMON-48. In: Biryukov, A., Goyal, V. (eds.) Progress in Cryptology—INDOCRYPT 2015. Proceedings of the 16th International Conference on Cryptology in India, Bangalore, India, 6–9 Dec 2015. Lecture Notes in Computer Science, vol. 9462, pp. 153–179. Springer, Berlin (2015).
3. Abed F., List E., Lucks S., Wenzel J.: Differential cryptanalysis of round-reduced Simon and Speck. In: Cid, C., Rechberger, C., (eds.) Fast Software Encryption—21st International Workshop, FSE 2014, London, UK, 3–5 Mar 2014. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8540, pp. 525–545. Springer, Berlin (2015).
4. Ashur T.: Improved linear trails for the block cipher Simon. IACR Cryptology ePrint Archive 2015, 285 (2015).
5. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L.: The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive 2013, 404 (2013).
6. Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L.: The SIMON and SPECK lightweight block ciphers. In: Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, 7–11 June 2015, pp. 175:1–175:6. ACM, New York (2015).
7. Biryukov A., Roy A., Velichkov V.: Differential analysis of block ciphers SIMON and SPECK. In: Cid, C., Rechberger, C., (eds.) Fast Software Encryption. 21st International Workshop, FSE 2014, London, UK, 3–5 Mar 2014. Revised Selected Papers. Lecture Notes in Computer Science, vol. 8540, pp. 546–570. Springer, Berlin (2015).
8. Black J., Rogaway P., Shrimpton T.: Black-box analysis of the block-cipher-based hash-function constructions from PGV. In: Yung, M. (ed.) Advances in Cryptology—CRYPTO 2002. Proceedings of 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, 18–22 Aug 2002. Lecture Notes in Computer Science, vol. 2442, pp. 320–335. Springer, Berlin (2002).
9. Blondeau C., Nyberg K.: Links between truncated differential and multidimensional linear properties of block ciphers and underlying attack complexities. In: Nguyen, P.Q., Oswald, E., (eds.) Advances in Cryptology—EUROCRYPT 2014. Proceedings of the 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014. Lecture Notes in Computer Science, vol. 8441, pp. 165–182. Springer, Berlin (2014).
10. Blondeau C., Peyrin T., Wang L.: Known-key distinguisher on full PRESENT. In: Gennaro, R., Robshaw, M. (eds.) Proceedings of the 35th Annual Cryptology Conference on Advances in Cryptology—CRYPTO 2015, Santa Barbara, CA, USA, 16–20 Aug 2015. Part I. Lecture Notes in Computer Science, vol. 9215, pp. 455–474. Springer, Berlin (2015).
11. Bogdanov A., Knudsen L.R., Leander G., Paar C., Poschmann A., Robshaw M.J.B., Seurin Y., Vikkelsoe C.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I., (eds.) Proceedings of the 9th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2007, Vienna, Austria, 10–13 Sept 2007. Lecture Notes in Computer Science, vol. 4727, pp. 450–466. Springer, Berlin (2007).
12. Borghoff J., Canteaut A., Güneysu T., Kavun E.B., Knezevic M., Knudsen L.R., Leander G., Nikov V., Paar C., Rechberger C., Rombouts P., Thomsen S.S., Yalçin T.: PRINCE—a low-latency block cipher

for pervasive computing applications—extended abstract. In: Wang, X., Sako, K. (eds.) Advances in Cryptology—ASIACRYPT 2012. Proceedings of the 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, 2–6 Dec 2012. Lecture Notes in Computer Science, vol. 7658, pp. 208–225. Springer, Berlin (2012).

13. Cannière C.D., Dunkelman O., Knezevic M.: KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers. In: Clavier, C., Gaj, K. (eds.) Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2009, Lausanne, Switzerland, 6–9 Sept 2009. Lecture Notes in Computer Science, vol. 5747, pp. 272–288. Springer, Berlin (2009).
14. Chen H., Wang X.: Improved linear hull attack on round-reduced Simon with dynamic key-guessing techniques. IACR Cryptology ePrint Archive 2015, 666 (2015).
15. Dinur I., Güneysu T., Paar C., Shamir A., Zimmermann R.: An experimentally verified attack on full Grain-128 using dedicated reconfigurable hardware. In: Lee, D.H., Wang, X., (eds.) Advances in Cryptology—ASIACRYPT 2011. Proceedings of the 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, 4–8 Dec 2011. Lecture Notes in Computer Science, vol. 7073, pp. 327–343. Springer, Berlin (2011).
16. Dinur I., Liu Y., Meier W., Wang Q.: Optimized interpolation attacks on LowMC. In: Iwata, T., Cheon, J.H., (eds.) Advances in Cryptology—ASIACRYPT 2015. Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015. Part II. Lecture Notes in Computer Science, vol. 9453, pp. 535–560. Springer, Berlin (2015).
17. Dinur I., Shamir A.: Breaking Grain-128 with dynamic cube attacks. In: Joux, A. (ed.) 18th International Workshopon ast Software Encryption, FSE 2011, Lyngby, Denmark, 13–16 Feb 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 6733, pp. 167–187. Springer, Berlin (2011).
18. Dong L., Wang Y., Wu W., Zou J.: Known-key distinguishers on 15-round 4-branch type-2 generalised Feistel networks with single substitution-permutation functions and near-collision attacks on its hashing modes. IET Inf. Secur. **9**(5), 277–283 (2015).
19. Dong L., Wu W., Wu S., Zou J.: Known-key distinguishers on type-1 Feistel scheme and near-collision attacks on its hashing modes. Front. Comput. Sci. **8**(3), 513–525 (2014).
20. Fouque P., Jean J., Peyrin T.: Structural evaluation of AES and chosen-key distinguisher of 9-round AES-128. In: Canetti, R., Garay, J.A. (eds.) Proceedings of the 33rd Annual Cryptology Conference on Advances in Cryptology—CRYPTO 2013, Santa Barbara, CA, USA, 18–22 Aug 2013. Part I. Lecture Notes in Computer Science vol. 8042, pp. 183–203. Springer, Berlin (2013).
21. Gilbert H.: A simplified representation of AES. In: Sarkar, P., Iwata, T., (eds.): Advances in Cryptology—ASIACRYPT 2014. Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., 7–11 Dec 2014. Part I. Lecture Notes in Computer Science, vol. 8873, pp. 200–222. Springer, Berlin (2014).
22. Gong Z., Nikova S., Law Y.W.: KLEIN: a new family of lightweight block ciphers. In: Juels, A., Paar, C., (eds.) RFID. Security and Privacy—7th International Workshop, RFIDSec 2011, Amherst, USA, 26–28 June 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 7055, pp. 1–18. Springer, Berlin (2011).
23. Guo J., Peyrin T., Poschmann A., Robshaw M.J.B.: The LED block cipher. In: Preneel, B., Takagi, T., (eds.) Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2011, Nara, Japan, 28 Sept–1 Oct 2011. Lecture Notes in Computer Science, vol. 6917, pp. 326–341. Springer, Berlin (2011).
24. Hong D., Sung J., Hong S., Lim J., Lee S., Koo B., Lee C., Chang D., Lee J., Jeong K., Kim H., Kim J., Chee S.: HIGHT: a new block cipher suitable for low-resource device. In: Goubin, L., Matsui, M., (eds.) Proceedings of the 8th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2006, Yokohama, Japan, 10–13 Oct 2006. Lecture Notes in Computer Science, vol. 4249, pp. 46–59. Springer, Berlin (2006).
25. Knudsen L.R., Rijmen V.: Known-key distinguishers for some block ciphers. In: Kurosawa, K. (ed.) Advances in Cryptology—ASIACRYPT 2007. Proceedings of the 13th International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 Dec 2007. Lecture Notes in Computer Science, vol. 4833, pp. 315–324. Springer, Berlin (2007).
26. Kölbl S., Leander G., Tiessen T.: Observations on the SIMON block cipher family. In: Gennaro, R., Robshaw, M., (eds.) Proceedings of the 35th Annual Cryptology Conference on Advances in Cryptology—

CRYPTO 2015, Santa Barbara, CA, USA, 16–20 Aug 2015. Part I. Lecture Notes in Computer Science, vol. 9215, pp. 161–185. Springer, Berlin (2015).

27. Koyama T., Sasaki Y., Kunihiro N.: Multi-differential cryptanalysis on reduced DM-PRESENT-80: collisions and other differential properties. In: Kwon, T., Lee, M., Kwon, D. (eds.) 15th International Conference on Information Security and Cryptology—ICISC 2012, Seoul, Korea, 28–30 Nov 2012, Revised Selected Papers. Lecture Notes in Computer Science, vol. 7839, pp. 352–367. Springer, Berlin (2012).
28. Lauridsen M.M., Rechberger C.: Linear distinguishers in the key-less setting: Application to PRESENT. In: Leander, G. (ed.) Fast Software Encryption—22nd International Workshop, FSE 2015, Istanbul, Turkey, 8–11 Mar 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9054, pp. 217–240. Springer, Berlin (2015).
29. Lim C.H., Korkishko T.: mCrypton—a lightweight block cipher for security of low-cost RFID tags and sensors. In: Song, J., Kwon, T., Yung, M. (eds.) Information Security Applications: 6th International Workshop, WISA 2005, Jeju Island, Korea, 22–24 Aug 2005, Revised Selected Papers. Lecture Notes in Computer Science, vol. 3786, pp. 243–258. Springer, Berlin (2005).
30. Mennink B., Preneel B.: On the impact of known-key attacks on hash functions. In: Iwata, T., Cheon, J.H., (eds.): Advances in Cryptology—ASIACRYPT 2015. Proceedings of the 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29–December 3 2015. Part II. Lecture Notes in Computer Science, vol. 9453, pp. 59–84. Springer, Berlin (2015).
31. Minier M., Phan R.C., Pousse B.: Distinguishers for ciphers and known key attack against Rijndael with large blocks. In: Preneel, B. (ed.) Progress in Cryptology—AFRICACRYPT 2009, Proceedings of the Second International Conference on Cryptology in Africa, Gammarth, Tunisia, 21–25 June 2009. Lecture Notes in Computer Science, vol. 5580, pp. 60–76. Springer, Berlin (2009).
32. Nikolic I., Pieprzyk J., Sokolowski P., Steinfeld R.: Known and chosen key differential distinguishers for block ciphers. In: Rhee, K.H., Nyang, D., (eds.) 13th International Conference on Information Security and Cryptology—ICISC 2010, Seoul, Korea, 1–3 Dec 2010, Revised Selected Papers. Lecture Notes in Computer Science vol. 6829, pp. 29–48. Springer, Berlin (2010).
33. Preneel B., Govaerts R., Vandewalle J.: Hash functions based on block ciphers: a synthetic approach. In: Stinson, D.R. (ed.) Advances in Cryptology—CRYPTO '93. Proceedings of the 13th Annual International Cryptology Conference, Santa Barbara, California, USA, 22–26 Aug 1993. Lecture Notes in Computer Science, vol. 773, pp. 368–378. Springer, Berlin (1993).
34. Raddum H.: Algebraic analysis of the Simon block cipher family. In: Lauter, K.E., Rodríguez-Henríquez, F. (eds.) Progress in Cryptology—LATINCRYPT 2015. Proceedings of the 4th International Conference on Cryptology and Information Security in Latin America, Guadalajara, Mexico, 23–26 Aug 2015. Lecture Notes in Computer Science, vol. 9230, pp. 157–169. Springer, Berlin (2015).
35. Sasaki Y., Yasuda K.: Known-key distinguishers on 11-round Feistel and collision attacks on its hashing modes. In: Joux, A. (ed.) Fast Software Encryption—18th International Workshop, FSE 2011, Lyngby, Denmark, 13–16 Feb 2011, Revised Selected Papers. Lecture Notes in Computer Science, vol. 6733, pp. 397–415. Springer, Berlin (2011).
36. Sasaki Y.: Known-key attacks on Rijndael with large blocks and strengthening *ShiftRow* parameter. In: Echizen, I., Kunihiro, N., Sasaki, R. (eds.) Advances in Information and Computer Security. Proceedings of the 5th International Workshop on Security, IWSEC 2010, Kobe, Japan, 22–24 Nov 2010. Lecture Notes in Computer Science vol. 6434, pp. 301–315. Springer, Berlin (2010).
37. Shanmugam D., Selvam R., Annadurai S.: Differential power analysis attack on SIMON and LED block ciphers. In: Chakraborty, R.S., Matyas, V., Schaumont, P. (eds.) Proceedings of the 4th International Conference on Security, Privacy, and Applied Cryptography Engineering, SPACE 2014, Pune, India, 18–22 Oct 2014. Lecture Notes in Computer Science, vol. 8804, pp. 110–125. Springer, Berlin (2014).
38. Shi D., Hu L., Sun S., Song L., Qiao K., Ma X.: Improved linear (hull) cryptanalysis of round-reduced versions of SIMON. IACR Cryptology ePrint Archive 2014, 973 (2014).
39. Shibutani K., Isobe T., Hiwatari H., Mitsuda A., Akishita T., Shirai T.: Piccolo: an ultra-lightweight blockcipher. In: Preneel, B., Takagi, T., (eds.) Proceedings of the 13th International Workshop on Cryptographic Hardware and Embedded Systems—CHES 2011, Nara, Japan, 28 Sept–1 Oct 2011. Lecture Notes in Computer Science, vol. 6917, pp. 342–357. Springer, Berlin (2011).

40. Song L., Hu L., Ma B., Shi D.: Match box meet-in-the-middle attacks on the SIMON family of block ciphers. In: Eisenbarth, T., Öztürk, E. (eds.) Lightweight Cryptography for Security and Privacy-Third International Workshop, LightSec 2014, Istanbul, Turkey, 1–2 Sept, 2014, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8898, pp. 140–151. Springer, Berlin (2014).
41. Sun S., Hu L., Wang P., Qiao K., Ma X., Song L.: Automatic security evaluation and (related-key) differential characteristic search: application to SIMON, PRESENT, LBlock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T., (eds.) Advances in Cryptology—ASIACRYPT 2014, Proceedings of the 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., 7–11 Dec 2014. Part I. Lecture Notes in Computer Science, vol. 8873, pp. 158–178. Springer, Berlin (2014).
42. Suzaki T., Minematsu K., Morioka S., Kobayashi E.: TWINE: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) Selected Areas in Cryptography: 19th International Conference, SAC 2012, Windsor, ON, Canada, 15–16 Aug 2012, Revised Selected Papers. Lecture Notes in Computer Science, vol. 7707, pp. 339–354. Springer, Berlin (2012).
43. Takahashi J., Fukunaga T.: Fault analysis on SIMON family of lightweight block ciphers. In: Lee, J., Kim, J. (eds.) 17th International Conference on Information Security and Cryptology—ICISC 2014, Seoul, Korea, 3–5 Dec 2014, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8949, pp. 175–189. Springer, Berlin (2014).
44. Wang N., Wang X., Jia K., Zhao J.: Improved differential attacks on reduced SIMON versions. IACR Cryptology ePrint Archive 2014, 448 (2014).