IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Final version of this paper is available for public access at the following link: https://ieeexplore.ieee.org/document/10323405 with the DOI number below.

Digital Object Identifier 10.1109/ACCESS.2023.3335271

New Security Proofs and Complexity Records for Advanced Encryption Standard

ORHUN KARA
IZTECH İzmir Institute of Technology, Faculty of Science, Department of Mathematics, 35430, Urla, Izmir, Turkey (e-mail:orhunkara@iyte.edu.tr)

This work is partially supported by TÜBİTAK 1001 Project under the grant number 121E228.

ABSTRACT Common block ciphers like AES specified by the NIST or KASUMI (A5/3) of GSM are extensively utilized by billions of individuals globally to protect their privacy and maintain confidentiality in daily communications. However, these ciphers lack comprehensive security proofs against the vast majority of known attacks. Currently, security proofs are limited to differential and linear attacks for both AES and KASUMI. For instance, the consensus on the security of AES is not based on formal mathematical proofs but on intensive cryptanalysis over its reduced rounds spanning several decades. In this work, we introduce new security proofs for AES against another attack method: impossible differential (ID) attacks. We classify ID attacks as reciprocal and nonreciprocal ID attacks. We show that sharp and generic lower bounds can be imposed on the data complexities of reciprocal ID attacks on substitution permutation networks. We prove that the minimum data required for a reciprocal ID attack on AES using a conventional ID characteristic is 2^{66} chosen plaintexts whereas a nonreciprocal ID attack involves at least 2^{88} computational steps. We mount a nonreciprocal ID attack on 6-round AES for 192-bit and 256-bit keys, which requires only 2^{18} chosen plaintexts and outperforms the data complexity of any attack. Given its marginal time complexity, this attack does not pose a substantial threat to the security of AES. However, we have made enhancements to the integral attack on 6-round AES, thereby surpassing the longstanding record for the most efficient attack after a period of 23 years.

INDEX TERMS Advanced Encryption Standard (AES), block cipher, confidentiality, cryptanalysis, impossible differential attack, integral attack, reciprocal attack, Substitution Permutation Network (SPN)

I. INTRODUCTION

Substitution permutation network (SPN) ciphers constitute a fundamental category of block ciphers that are widely used in modern cryptography. The Advanced Encryption Standard (AES) specified by the National Institute of Standards and Technology (NIST) [1] is an example of an SPN cipher that is extensively employed to provide confidentiality in various cryptographic protocols, such as Transport Layer Security (TLS), WiFi Protected Access (WPA), and the Signal protocol utilized in applications like WhatsApp. In this context, the cryptanalysis of SPN ciphers in generic settings plays a crucial role in comprehending the security of commonly utilized ciphers, and in evaluating their resilience against potential attacks.

In contrast to the majority of previous research on cryptanalysis, which has largely focused on specific ciphers, this study adopts a more abstract and theoretical approach by examining the data complexity of reciprocal impossible differential (ID) attacks and the time complexity of nonreciprocal ID attacks on SPN ciphers in generic settings. Reciprocal attacks are those that require the same amount of data complexity to prepare the necessary data for the attack, regardless of whether the attacker has access to the encryption oracle or the decryption oracle. To provide a precise description of reciprocal attacks, we present Definition 1, and we establish various results regarding the minimum data requirements for reciprocal ID attacks on generic SPN ciphers.

The data requirement of an attack can be considered the most vital and critical complexity among time and memory complexities. This is due to the fact that data collection may not always be feasible, and the attacker has no control over the throughput of the oracle producing the data. Conversely, ad-

vancements in time and memory complexities are achievable through the efficient utilization of high-speed, parallel supercomputer platforms. Therefore, low-data complexity attacks stand out as particularly noteworthy. For instance, Bouillaguet et al. explore the possibility of attacking AES with only one or two plaintext/ciphertext pairs [2]. Hence, in this work, we investigate the minimum data requirement of reciprocal ID attacks on AES.

We focus on establishing lower bounds for data and time complexities related to reciprocal and nonreciprocal ID attacks on AES respectively. Despite AES being a subject of extensive research, comprehensive security proofs are notably lacking for various attack methods. The designers of AES have provided security proofs against differential and linear attacks [3]. Subsequent efforts have aimed at refining and enhancing these security bounds [4]. However, it is important to emphasize the existing gap in security proofs against other potential attack methods. We address this gap specifically in the context of ID attacks in this work.

Cryptanalysis techniques on SPN ciphers, particularly AES, have made significant progress. One example is the class of impossible differential (ID) attacks which were introduced by Biham et al. [5] and Knudsen [6] independently. The distinguisher in an ID attack utilizes an input-output difference of an encryption function that is not generated by any key. We classify ID attacks on SPN ciphers into reciprocal and nonreciprocal attacks. Reciprocal ID attacks are identified as those that can be executed with the same data complexity in the chosen ciphertext (CC) scenario as in the chosen plaintext (CP) scenario. It is apparent that almost all ID attacks on well-known SPN ciphers are reciprocal, and as yet there is no nonreciprocal ID attack on AES. While it seems that reciprocal ID attacks are generally more efficient and faster than nonreciprocal ones, this study reveals that reciprocal ID attacks on SPN ciphers require a considerable amount of data.

A. RELATED WORK

The prevalent approach in security of AES often involves an ad-hoc paradigm, and intensively mounting attacks on reduced rounds as a heuristic measure. These attacks include Meet-in-The-Middle (MiTM) attacks (such as those proposed by Demirci and Selçuk [7], Dunkelman et al. [8], [9], Wang and Zhu, [10], Derbez et al. [11], Li et al. [12], Gilbert and Minier [13]), square attacks (such as those proposed by Ferguson et al. [14]), biclique attacks (such as those proposed by Bogdanov et al. [15], Tao and Wang [16]), yoyo attacks (such as those proposed by Saha et al. [17] and Rahman et al. [18]), truncated boomerang attacks (such as those proposed by Bariant and Leurent [19]), zero difference attacks (such as those proposed by Bardeh and Rijmen [20]), algebraic attacks (such as those proposed by Zhao et al. [21]), mixture differential attacks (such as those proposed by Grassi [22]), mixture integral attack (such as those proposed by Grassi and Schofnegger [23]) and the ID attacks. Even, its key schedule is cryptanalyzed intensively [9], [24].

Several ID attacks have been proposed for AES, all of which rely on exploiting the 4-round conventional ID characteristics as described in [25]. To date, no other ID characteristics for AES have been identified. In fact, Sun et al. have demonstrated that AES has no 5-round ID unless the specifics of the S-Box are disregarded [26]. Wang and Jin [27] have also verified this claim through the "dependent tree" method, although their conclusion is based on the assumption that all the round keys are independent and uniformly random. In addition, Boura and Coggia [28] have demonstrated that no 5-round ID with two active bytes exists for AES, using MILP solvers.

The distinguishing feature of ID attacks on AES is that they are all reciprocal and require extensive data. These attacks rely on an outrageous number of chosen plaintexts to identify all the incorrect keys in the initial and final rounds. Boura et al. have introduced bounds on data, time, and memory complexities for various generic types of block ciphers [29]. However, the bound for data complexity is notably loose. Several ID attacks on AES have different data requirements, ranging from $2^{117.5}$ CP in [30] to $2^{75.5}$ CP in [31], and 2^{92} CP in [32] and [33] when 4-round conventional ID characteristics are enclosed by initial and final rounds. Remark that the 6-round attack in [31] has the lowest data requirements among all the ID attacks on AES.

The category of practical attacks or attacks with low data on few rounds of AES, has gained popularity in the cryptanalysis of AES for understanding its security [2], [3], [17], [34]–[38]. The critical lower bound of the number of rounds for a dramatic jump in the required data complexity can be considered as six. This is supported by findings that while there exist attacks on 5-round AES that require only 8 CP [39], attacks on 6-round AES require at least 2^{26} CP [34].

The square attack introduced by Daemen et al. on 6-round AES in [40] held the record for more than two decades, requiring 2^{32} chosen plaintexts. Although some improved versions of the square attack, such as the partial sum technique [36] and improved meet-in-the-middle attacks [10], [11], have better time complexities, their data complexities could not surpass 2^{32} chosen plaintexts. Bar-On et al. improved the record to $2^{27.5}$ chosen plaintexts with the mixture meet-in-the-middle technique [35]. They further enhanced their analysis and achieved a data complexity of 2^{26} chosen plaintexts in [34].

B. OUR CONTRIBUTIONS

We present a set of parameters that can be used to identify an ID attack, and we investigate the data complexity of reciprocal ID attacks on SPN ciphers in a generic setting, using these parameters. Our analysis yields several theoretical and generic results concerning the minimum data requirement of such attacks. These results are presented in Theorem 2, Theorem 4, and Theorem 5. By offering a more extensive and rigorous comprehension of the minimum data requirements of reciprocal ID attacks, our results serve to augment the current understanding of this class of attacks.

Table 1. Attacks a 6- round AES with minimal data. Memory is in Byte. Data is CP. *: We make a minor amendment to rectify the complexity computation in [36]. See Section VIII

.

Variant	Data	Time	Memory	Source
All	$2^{27.5}$	2^{81}	$2^{27.5}$	[35]
All	2^{26}	2^{80}	2^{35}	[34]
All	$6 \cdot 2^{32}$	2^{46} *	$6 \cdot 2^{36}$	[36]
All	2^{32}	2^{72}	2^{36}	[3]
AES-128	2^{38}	2^{83}	2^{33}	[41]
All	2^{33}	2^{44}	2^{37}	Section VIII
AES-128	2^{32}	2^{43}	$3 \cdot 2^{36}$	Section VIII
AES-192	2^{18}	2^{180}	2^{78}	Section VII
AES-256	2^{18}	2^{186}	2^{43}	Section VII

Based on the parameters of the ID characteristic, we propose a generic formula for estimating the minimum data complexity of a reciprocal ID attack on an SPN cipher in Theorem 5. This formula is independent of the sieving method employed in the attack. Specifically, we demonstrate that a reciprocal ID attack that exploits at least one structure in the encryption and decryption directions necessitates at least the cube root of $2^{n+1}/p$ data by Theorem 3, where n represents the block length of the SPN cipher and p denotes the probability that an input/output difference pair leads to the ID characteristic. To illustrate, we find that the minimum amount of data required for such an attack is 2^{43} CP for a 128-bit block length.

In order to investigate if there are reciprocal ID attacks that attain the lower bound established by Theorem 5 with respect to data complexity, we propose Definition 2. These attacks are denoted as "reciprocal ID attacks with optimal data". It is worth noting that the most efficient ID attacks currently known do not fall under this category. Furthermore, there is a lack of literature on reported reciprocal ID attacks on AES with optimal data, leading to an open question regarding the precision of the lower bound presented in Theorem 5.

We provide comprehensive lower bounds on either data or time complexities for all types of ID attacks on AES. We prove that any reciprocal ID attack on AES exploiting a 4-round conventional ID characteristic and containing at least one initial and one final round uses at least 2^{66} chosen plaintexts (CP) in Theorem 7. We observe that all the ID attacks on AES utilize 4 active bytes either in the first or in the last round yielding only one active byte after the MC or MC^{-1} operations. We prove that the data complexity is bounded by 2^{62} for these attacks in Theorem 8 whatsoever the ID characteristic is. Moreover, we prove that any nonreciprocal ID attack on AES, which exploits a conventional ID characteristic, has a time complexity of at least 2^{88} computational steps in Theorem 9. Consequently, we introduce security bounds against a different type of attack for the first time since introducing the security bounds against differential and linear attacks for AES.

To assess the degree of sharpness of the bounds established in Theorem 7 and Theorem 2, we conduct a 6-round reciprocal ID attack with 2^{66} chosen plaintexts. While not the most effective attack, we present this attack to demonstrate that it reaches the bound described in Theorem 2 and represents the first instance of a reciprocal ID attack with optimal data. This means that it attains the bound in Theorem 5 as well, establishing the sharpness of these theorems.

We have successfully mounted a couple of nonreciprocal ID attacks on 6-round AES with a record low data requirement of only 2^{18} CP, to illustrate that ID attacks do not necessarily require a lot of data. This result is particularly surprising as ID attacks are known to typically require significantly larger amounts of data. The theoretical infrastructures we have developed for the data requirements of reciprocal ID attacks in this work have enabled us to establish the frameworks for our nonreciprocal attacks with minimal data. While our attacks may not be the most optimal with their marginal time complexities, it is notable for their remarkable efficiency in terms of data usage. To compensate it for having a practical application, we improve the integral attack through the partial sum technique in [36]. Our attack is the fastest attack on 6-round AES, surpassing the prior record established over a span of 23 years. A summary of low-data complexity attacks on 6-round AES is presented in Table 1.

Consequently, we contribute to the theoretical characterization of the data requirements of reciprocal ID attacks in this work. Our other crucial contribution is to provide security bounds of certain levels for AES against both reciprocal and nonreciprocal ID attacks by utilizing our generic statements on SPN ciphers. Moreover, we mount an attack of the minimum data on 6-round AES-192 and AES-256; and another attack of the best complexity on 6-round AES.

C. ORGANIZATION

The paper is structured as follows. In Section II, we provide a concise overview of SPN ciphers and AES. Subsequently, we present the framework of our work and investigate the data complexities of the reciprocal ID attacks on SPN ciphers in Section III. We establish a lower bound on the data of the reciprocal ID attacks and a lower bound on the time complexities of nonreciprocal ID attacks on AES in Section IV. Our reciprocal ID attack with optimal data and nonreciprocal ID attack on AES are detailed in Section V and Section VI, respectively. Section VII outlines our attack with minimum data. We introduce our improvement of the integral attack in Section VIII. Finally, we conclude the paper in Section IX with a conjecture.

II. PRELIMINARIES

We give a brief decryption of SPN (Substitution permutation network) ciphers and AES (Advanced Encryption Standard) along with the notation we comply with in this section.

A. SUBSTITUTION PERMUTATION NETWORKS

A substitution permutation network is a block cipher $E_K : GF(2)^n \rightarrow GF(2)^n$. For a fixed k-bit key K, E_K is an n-bit permutation. Its inverse, D_K, is the decryption function such that $D_K E_K(P) = E_K D_K(P) = P \ \ \forall P \in GF(2)^n$. E_K is

supposed to behave like a random permutation to be a secure cipher.

The round function of an SPN cipher consists of key addition, an S-box layer, and a linear transformation. The input is added to the round key. Then, each block is divided into n/s subblocks of s-bit in an SPN cipher. We call each subblock a *word*. Subsequently, S-boxes are executed to n/s words simultaneously. That is, each S-box is a nonlinear permutation from $GF(2)^s$ into $GF(2)^s$. The last operation of the round function is the linear transformation. It is a multiplication by an invertible matrix in the $n \times n$ general linear group over the field $GF(2)$. There is an extra round key addition at the end of the last round.

B. ADVANCED ENCRYPTION STANDARD

Advanced Encryption Standard (AES), is the most prominent SPN cipher, as being the FIPS 197 standard [1]. Its block length is 128-bit. The key lengths are $k = 128, 192$ or $k = 256$ bits, corresponding to $r = 10$ round, $r = 12$ round, or $r = 14$ round encryptions respectively. We give a brief description of AES. One can refer to [1], [3] for detailed information. It is convenient to demonstrate a round state of AES by a 4×4 matrix. There are four round functions of AES which are given as follows. These functions are depicted in Figure 1.

a: SubBytes (SB):

It is the layer of S-box operations. $s = 8$ for AES and we call a single S-box operation an AES S-box. It substitutes each byte by another byte according to the look-up table of the AES S-box bijectively without changing the byte position in the matrix. There are 16 identical S-boxes.

b: ShiftRows (SR):

Rotates the i-th row $i - 1$ byte to the left for $2 \leq i \leq 4$.

c: MixColumns (MC):

Multiplies each column of the input state by a fixed 4×4 MDS matrix.

d: AddRoundKey (ARK):

XORs the output state of the ith round with the i-th subkey.

At first, there is a whitening key addition with the plaintext. The MC operation is omitted in the last round. We call single matrix multiplication of one column as MC also for the sake of simplicity.

SB^{-1}, SR^{-1} and MC^{-1} are inverses of SB, SR and MC respectively. Let the i-th subkey be RK_i and let us denote the j-th column of RK_i by $RK_i\{j\} = RK\{j + 4i\}$. Let $N = 6$ and $N = 8$ for the key length to be 192 and 256-bit respectively. Any column $RK\{j\}$ of a subkey is computed as

$$\begin{cases} RK\{j-N\} \oplus f(RK\{j-1\}), & \text{if } j \bmod N = 0, \\ RK\{j-8\} \oplus g(RK\{j-1\}), & \text{if } j \bmod 8 = 4 \text{ and } N = 8, \\ RK\{j-N\} \oplus RK\{j-1\}, & \text{else;} \end{cases}$$

where f and g are functions on columns that consist of S-box, cyclic shift, and round constant addition operations.

C. NOTATION

The symbols P, C, and K denote a plaintext, ciphertext, and main key, respectively, in the context of AES (Advanced Encryption Standard). The notation ΔX represents the difference between a pair of elements X, where ΔP and ΔC refer to the plaintext and ciphertext differences, respectively. To specify both the output of an AES function and the round number for an arbitrary output, subscripts are employed. Specifically, SB_i and MC_i indicate the output of the data in the i-th round of the SubBytes and MixColumns operations, respectively. Likewise, ΔSB_i and ΔMC_i refer to the output difference of a pair of data in the i-th round of the SubBytes and MixColumns operations, respectively. Equivalent notations are employed for the inverse operations, SB_i^{-1}, MC_i^{-1}, ΔSB_i^{-1}, and ΔMC_i^{-1}. If it is necessary to specify a particular input or output of these functions, the standard notation $MC_i(X)$, $SB_i(X)$, or $MC_i^{-1}(X)$ is used.

The bytes of a state are denoted by $[\cdot]$ notation. Specifically, $X[i_1, i_2, \ldots, i_r]$ denotes the $(i_1 + 1), (i_2 + 1), \ldots, (i_r + 1)$-th bytes of the state X. For example, $\Delta SB_4^{-1}[0, 2]$ denotes the first and third bytes of an input difference for the SB operation in the fourth round. The index numbers of words in the 4×4 matrix are arranged as depicted in Figure 2. This matrix arranges words with indices $0, 1, 2, 3$ in the first row; words with indices $4, 5, 6, 7$ in the second row; words with indices $8, 9, 10, 11$ in the third row; and words with indices $12, 13, 14, 15$ in the last row.

III. RECIPROCAL ID ATTACKS ON SPN CIPHERS

Any attack on a block cipher E_K is an algorithm whose input is a particular set of plaintext/ciphertext pairs. The output is the secret key. In general, E_K is used as an oracle to produce the data that the attack makes use of. Alternatively, it is possible to produce the data through D_K. Yet, the number of calls generally changes. We introduce Definition 1 for a reciprocal attack if the attack has the same data complexity when it is mounted on D_K as when it is mounted on E_K.

Definition 1 *Let the data required in a non-adaptive attack algorithm $\mathcal{A}$ on a block cipher be produced by either α_e calls of the encryption oracle E_K or α_d calls of the decryption oracle D_K. If $O(\alpha_e) = O(\alpha_d)$ then $\mathcal{A}$ is said to be a reciprocal attack, where O is the big-O notation. Otherwise, it is a nonreciprocal attack.*

KP (known plaintext) attacks are clearly reciprocal. Because the same amount of data necessary for a known plaintext attack can be collected through the decryption oracle. Some of the CP (Chosen Plaintext) attacks are reciprocal. We show that ID attacks need not be reciprocal even though any ID characteristic is valid for the decryption function. To the best of our knowledge, all the prominent ID attacks on AES in the literature are reciprocal attacks. Therefore, these attacks can

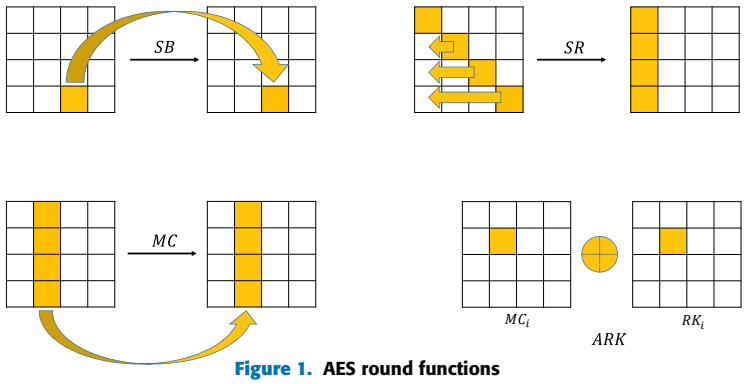

Figure 1. AES round functions

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

Figure 2. Word indices in a state.

be mounted as CC (Chosen Ciphertext) attacks with the same complexities.

The literature shows that the most efficient and fastest ID attacks are reciprocal ID attacks. However, we prove that reciprocal ID attacks require too much data. We introduce a lower bound for the data complexity of reciprocal ID attacks on SPN ciphers. For this, we use the following notation.

- k_i/k_f: # of independent key bits in the initial/final rounds involved in producing the input/output differences of the ID characteristic respectively.
- n_i/n_f: # of active input/output words in the plaintext/ciphertext differences respectively.
- P_i/P_f: The probability that a subkey in the initial/final rounds produces the input/output difference of the ID characteristic for a given input/output pair respectively.
- D_u: The average number of pairs used in the attack.
- U_i/U_f: # of structures in plaintexts/ciphertexts respectively.

a: Typical ID attack:

A *typical* ID attack on an n-bit SPN cipher is a successful ID attack (faster than exhaustive search) that exploits one truncated ID characteristic in the middle rounds. Some few rounds are added in the beginning which we call *initial* rounds and some few rounds are added at the end we call *final* rounds. Then, the attack searches for all the necessary subkey bits in the initial and final rounds in order to check if a given plaintext pair produces the input difference of the ID characteristic and its corresponding ciphertext pair produces the output difference of the ID characteristic as truncated differences. We call these subkey bits the involved bits. We assume these bits are independent. If some of them can be computed by means of the key schedule, we skip searching for them. We use enough data to sieve all the involved subkey bits in a typical ID attack. We adopt the big-O notation for data complexities in our statements but we ignore the use of the notation $O(\cdot)$ for the sake of simplicity.

Shakiba et al. introduce the definition of an ideal ID attack in terms of its complexity in [42]. They categorize an ID attack as an ideal ID attack if the dominant part of its time complexity is the number of memory accesses for sieving out the stored subkeys that are involved in producing the input/output differences of the ID characteristic. We also assume a typical ID attack is ideal.

Let an ID attack make use of the pairs $(\Delta P, \Delta C)$ where specific n_i words of ΔP and n_f words of ΔC are active. That is, we have nonzero differences only on these words. A structure for the inputs is a set of plaintexts whose n_i words take all the values and other words are constant. Similarly, a structure for the outputs is a set of ciphertexts whose n_f words take all the values and other words are constant. There are around $2^{sn_i-1}(2^{sn_i}-1)$ pairs in a structure of plaintexts. But we assume there are 2^{2sn_i-1} pairs for $n_i > 1$. This does not change the complexities in big-O notation. Similarly, we assume a structure for ciphertexts contains 2^{2sn_f-1} pairs.

For a CP attack, we construct U_i structures and check the ciphertext pair ΔC of each plaintext pair ΔP in a structure if ΔC has exactly n_f active words only on the specific positions. Then, this $(\Delta P, \Delta C)$ is used in the attack. If a subkey guess leads to the ID characteristic in the middle rounds from $(\Delta P, \Delta C)$, this subkey is eliminated.

A typical ID attack has the following parameters in CP scenario:

$$(U_i, D_u, n_i, n_f, k_i, k_f, P_i, P_f).$$

The parameters of this attack will be

$$(U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$$

in CC scenario. Let us note that we do not consider multiple ID attacks or an ID attack exploiting multiple ID characteristics simultaneously in a typical ID attack. A trivial lower bound for the time complexity is $\max\{2^{sn_i}, 2^{sn_f}\}$.

The numbers of structures are integers in general in practice. But, we do not impose U_i or U_j to be integers. If the number of structures is not an integer, then not all of the elements in one of the structures are used. Let $U_i = q_i + \epsilon_i$ with $0 \leq \epsilon_i < 1$, $q_i \in \mathbb{Z}$, $q_i \geq 0$, and $U_f = q_f + \epsilon_f$ with $0 \leq \epsilon_f < 1$, $q_f \in \mathbb{Z}$, $q_f \geq 0$.

Remark 1 *We assume* $O((q_i + \epsilon_i)2^{sn_i}) \neq O(q_i 2^{sn_i})$ *and* $O((q_f + \epsilon_f)2^{sn_f}) \neq O(q_f 2^{sn_f})$ *for nonzero* ϵ_i *and nonzero* ϵ_f *throughout the paper. Therefore, we simply assume* $\epsilon_i = \epsilon_f = 0$ *for* $q_i \geq 4$ *and* $q_f \geq 4$.

We need D_u pairs to eliminate all the wrong subkeys involved in either a CP attack or a CC attack. However, the number of calls of the oracle to get D_u pairs may change. We assume that enough number of pairs are used to eliminate all the wrong subkeys. We also assume that each subkey candidate (K_i, K_f) from the initial subkey K_i and the final subkey K_f is eliminated by the probability of $P_i P_f$ through an input/output pair and hence it survives with the probability of $(1 - P_i P_f)^{D_u}$ in all D_u pairs. Therefore, the minimum number of pairs in order to eliminate all the subkeys is

$$D_u \geq \frac{k_i + k_f}{\log_2(e) P_i P_f}$$

for a typical ID attack on an SPN cipher with parameters $(U_i, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$ where e is the Euler's number.

The elimination process may utilize several techniques such as guess and determine methods, hash tables, and early abort techniques to enhance the time complexity as proposed in [33], [43]. However, we study the reciprocal ID attacks in a generic setting. So, it is not possible to introduce statements about time complexities since they depend on the attack algorithms. Therefore, we do not consider time or memory complexities. But, we can introduce the trivial lower bound as $2^{k_i+k_f}$ memory accesses to eliminate all the wrong keys. In this work, we focus on data complexities.

Proposition 1 *Let a typical ID attack on an SPN cipher have the number of the structures,* $U_i = q_i + \epsilon_i$ *and* $U_f = q_f + \epsilon_f$. *Then, this ID attack is reciprocal if and only if*

$$2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f).$$

Proof A typical ID attack is reciprocal if and only if its data complexities are equal in both CP and CC scenarios by Definition 1. We use all the elements in q_i structures. So, we have $q_i 2^{2sn_i - 1}$ pairs of the plaintexts. On the other hand, we use $\epsilon_i 2^{sn_i}$ plaintexts of the last structure. So, we can produce $\epsilon_i^2 2^{2sn_i - 1}$ pairs from this structure. Together we have

$$q_i 2^{2sn_i - 1} + \epsilon_i^2 2^{2sn_i - 1}$$

pairs. We check if their ciphertext pairs have exactly n_f active words in the specific positions. So, the number of pairs used in the attack is

$$\frac{q_i 2^{2sn_i - 1} + \epsilon_i^2 2^{2sn_i - 1}}{2^{n - sn_f}} \tag{1}$$

which is also equal to

$$\frac{q_f 2^{2sn_f - 1} + \epsilon_f^2 2^{2sn_f - 1}}{2^{n - sn_i}} \tag{2}$$

since the same data pairs are used in both CP and CC scenarios. Organizing Equation 1 and Equation 2, we have

$$q_i 2^{sn_i} + \epsilon_i^2 2^{sn_i} = q_f 2^{sn_f} + \epsilon_f^2 2^{sn_f}. \tag{3}$$

On the other hand, the data complexity is $q_i 2^{sn_i} + \epsilon_i 2^{sn_i}$ in CP scenario and $q_f 2^{sn_f} + \epsilon_f 2^{sn_f}$ in CC scenario. We need them to be equal for the attack to be reciprocal. Substituting $q_i 2^{sn_i} - q_f 2^{sn_f}$ with $\epsilon_f 2^{sn_f} - \epsilon_i 2^{sn_i}$ in Equation 3, we obtain

$$-\epsilon_i 2^{sn_i} + \epsilon_i^2 2^{sn_i} = -\epsilon_f 2^{sn_f} + \epsilon_f^2 2^{sn_f}$$

which simply gives the equality

$$2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f).$$

Conversely if $2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f)$ then $2^{sn_i}\epsilon_i^2 - 2^{sn_f}\epsilon_f^2 = 2^{sn_i}\epsilon_i - 2^{sn_f}\epsilon_f$. Then, substituting in Equation 3, we have

$$q_i 2^{sn_i} + \epsilon_i 2^{sn_i} = q_f 2^{sn_f} + \epsilon_f 2^{sn_f} \tag{4}$$

which means that data complexities are equal in both CP and CC scenarios. Note that Equation 3 is always valid in any ID attack. □

Corollary 1 *In a typical reciprocal ID attack,* $\epsilon_i = 0$ *if and only if* $\epsilon_f = 0$.

Proof If an ID attack with the numbers of structures $U_i = q_i + \epsilon_i$ in the encryption direction and $U_f = q_f + \epsilon_f$ is reciprocal, then we have $2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f)$ by Proposition 1. If $\epsilon_i = 0$ then $2^{sn_f}(\epsilon_f^2 - \epsilon_f) = 0$. $2^{sn_f} \neq 0$ and hence $\epsilon_f = 0$ since it cannot be 1. Similarly $\epsilon_f = 0 \implies \epsilon_i = 0$. □

Corollary 2 below can be considered as a useful characterization of reciprocal ID attacks which can be used in practice to identify that the ID attacks on SPN ciphers in the literature are mostly reciprocal attacks.

Corollary 2 *If both* U_i *and* U_f *are integers in a typical ID attack then the attack is reciprocal.*

Proof Let the numbers of structures of a typical ID attack be integers in both CP and CC scenarios. Then $\epsilon_i = \epsilon_f = 0$. Hence, we have $2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f)$. This simply implies that the attack is reciprocal by Proposition 1. □

It is crucial to note that any attack with $U_i \geq 4$ and $U_f \geq 4$ is reciprocal by Corollary 2. For example, the numbers of structures used in all the well-known ID attacks on AES are much higher than 4 and are all integers [30]–[33], [43]–[49]. So, all the known ID attacks on AES are reciprocal by Corollary 2. We observe that the reciprocal attacks achieve good performance in terms of time complexity. However, they require a lot of data. We can give lower bounds for the data complexities of such attacks through our statements in Section IV.

The following theorem characterizes the reciprocal attacks when the numbers of structures are not integers.

Theorem 1 *Let a typical ID attack have $U_i = q_i + \epsilon_i$ and $U_f = q_f + \epsilon_f$ with $\epsilon_i \neq 0$ and $\epsilon_f \neq 0$. Then, the attack is reciprocal if and only if $n_i = n_f$, $q_i = q_f$, and $\epsilon_i = \epsilon_f$.*

Proof If we have $n_i = n_f$ and $\epsilon_i = \epsilon_f$ then it is clear that $2^{sn_i}(\epsilon_i^2 - \epsilon_i) = 2^{sn_f}(\epsilon_f^2 - \epsilon_f)$ and hence the attack is reciprocal by Proposition 1. On the other hand, assume that the attack is reciprocal. If $n_i = n_f$ then $q_i+\epsilon_i = q_f+\epsilon_f$ since $2^{sn_i}(q_i+\epsilon_i) = 2^{sn_f}(q_f+\epsilon_f)$. This implies that $q_i = q_f$ and $\epsilon_i = \epsilon_f$. Because q_i and q_f are integers and $0 \leq \epsilon_i < 1$, $0 \leq \epsilon_f < 1$. Assume on the contrary that $n_i \neq n_f$. Let $n_i < n_f$. If $q_i \neq 0$. We have $q_i + \epsilon_i = 2^{s(n_f-n_i)}(q_f + \epsilon_f)$ and $q_i + \epsilon_i^2 = 2^{s(n_f-n_i)}(q_f + \epsilon_f^2)$. But there is no nonzero solution for ϵ_f for these two equations since both $\epsilon_f \approx q_i 2^{s(n_i-n_f)} - q_f$ and $\epsilon_f^2 \approx q_i 2^{s(n_i-n_f)} - q_f$. If $q_i = 0$ then q_f must be zero. Otherwise $\epsilon_i > 1$. When $q_f = 0$ also, we have no nonzero solutions of ϵ_f and ϵ_i again since $2^{s(n_f-n_i)} \neq 1$. In summary, if $n_i \neq n_f$ then the attack cannot be reciprocal for nonzero ϵ_i and ϵ_f. □

We construct our lower bounds for the data complexities of typical ID attacks in general in Theorem 2. We introduce a precise lower bound for the data complexities of reciprocal ID attacks.

Theorem 2 *A typical reciprocal ID attack on an SPN cipher with its parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$ requires at least*

$$\left(\frac{2^{n+1}(k_i+k_f)}{\log_2(e)P_iP_f}\right)^{1/3}\left(\frac{U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6}$$

chosen plaintexts (or, equally, chosen ciphertexts) where $U_i = q_i + \epsilon_i$ and $U_f = q_f + \epsilon_f$; $0 \leq \epsilon_i < 1$; $0 \leq \epsilon_f < 1$, $q_i, q_f \in \mathbb{Z}$, $q_i \geq 0$, $q_f \geq 0$.

Proof The data complexity is $U_i 2^{sn_i}$ which is $U_f 2^{sn_f}$ at the same time since the attack is reciprocal. We have

$$D_u = (q_i + \epsilon_i^2)2^{2sn_i - 1 + sn_f - n} \geq \frac{k_i + k_f}{\log_2(e)P_iP_f}.$$

Taking the logarithm,

$$2sn_i + sn_f \geq \log_2\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right) + n + 1 - \log_2(q_i+\epsilon_i^2) \quad (5)$$

and similarly for the CC scenario

$$2sn_f + sn_i \geq \log_2\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right) + n + 1 - \log_2(q_f+\epsilon_f^2). \quad (6)$$

Summing Inequality 5 and Inequality 6 and then dividing by 3, we obtain a lower bound for $sn_f + sn_i$:

$$\log_2\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right)^{2/3} + \frac{2(n+1)}{3} - \frac{\log_2(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}{3}. \quad (7)$$

On the other hand, we have $U_i 2^{sn_i} = U_f 2^{sn_f}$ since the attack is reciprocal and hence

$$sn_i - sn_f = \log_2(U_f) - \log_2(U_i). \quad (8)$$

Adding Inequality 7 to Equation 8 and dividing by 2, we get a lower bound for sn_i:

$$\log_2\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right)^{1/3} + \frac{n+1}{3} + \frac{\log_2(U_f) - \log_2(U_i)}{2} - \frac{\log_2(q_i+\epsilon_i^2) + \log_2(q_f+\epsilon_f^2)}{6}. \quad (9)$$

Therefore, the logarithm of the data complexity is bounded by

$$\log_2(U_i 2^{sn_i}) \geq \log_2\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right)^{1/3} + \frac{n+1}{3} - \frac{\log_2(q_i+\epsilon_i^2) + \log_2(q_f+\epsilon_f^2)}{6} + \frac{\log_2(U_f) + \log_2(U_i)}{2}. \quad (10)$$

Taking the powers of the both sides of Inequality 10, we get

$$D \geq \left(\frac{2^{n+1}(k_i+k_f)}{\log_2(e)P_iP_f}\right)^{1/3}\left(\frac{U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6}. \quad (11)$$

□

One straightforward conclusion of Theorem 2 is introducing the following lower bound for reciprocal ID attacks. Even though it is the most generic bound, it is a loose bound.

Corollary 3 *A typical reciprocal ID attack on an SPN cipher with $U_i \geq 1$ has the data complexity of at least $2^{(n+1)/3}$ chosen plaintexts.*

Proof The data complexity is bounded below by

$$\left(\frac{2^{n+1}(k_i+k_f)}{\log_2(e)P_iP_f}\right)^{1/3}\left(\frac{U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6} \quad (12)$$

by Theorem 2. $U_i \geq 1 \Rightarrow U_f \geq 1$ by Theorem 1. On the other hand

$$\left(\frac{U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6} \geq 1$$

since $U_i \geq 1$, $U_f \geq 1$. Meanwhile, $(k_i + k_f) \geq 2$ and $P_iP_f < 1$. Hence, $\left(\frac{k_i+k_f}{\log_2(e)P_iP_f}\right)^{1/3} \geq 1$ which simply implies the result. □

We can directly use Corollary 3 for AES with $n = 128$.

Corollary 4 *Any typical reciprocal ID attack on AES with $U_i \geq 1$ has the data complexity of at least 2^{43} chosen plaintexts.*

The most dominant parameters in data complexity are P_i and P_f. So, we can simplify the lower bound as follows.

Theorem 3 *A typical reciprocal ID attack on an SPN cipher with $U_i \geq 1$ has the data complexity of at least $(2^{n+1}(P_iP_f)^{-1})^{1/3}$ chosen plaintexts.*

The probability $p = P_iP_f$ is 2^{-68} in [47]; 2^{-52} in [32] and [33] ; 2^{-74} in [30] and [31] (7-round attack); and 2^{-36} in [31] for the 6-round attack. So the data complexities are bounded by $2^{65.7}$, $2^{60.3}$, $2^{67.7}$ and 2^{55} respectively. The following bound is a sharp bound but specific to the parameters of an attack as in Theorem 2. But Theorem 4 is more simple than Theorem 2.

Theorem 4 *A typical reciprocal ID attack on an SPN cipher with (n_i, n_f, U_i, U_f) has the data complexity of at least $\sqrt{2^{sn_i+sn_f}U_iU_f}$ chosen plaintexts (or, equally, chosen ciphertexts).*

Proof The data complexity is at least

$$\left(\frac{2^{n+1}(k_i+k_f)}{\log_2(e)P_iP_f}\right)^{1/3}\left(\frac{U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6}$$

chosen plaintexts (or, equally, chosen ciphertexts) by Theorem 2. We can write this bound as

$$\left(\frac{2^{2sn_i+sn_f}2^{2sn_f+sn_i}(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)U_i^3U_f^3}{(q_i+\epsilon_i^2)(q_f+\epsilon_f^2)}\right)^{1/6}$$

which is equal to $\sqrt{2^{sn_i+sn_f}U_iU_f}$. □

Let us note that the bound in Theorem 4 is the geometric mean of the data complexities in CP and CC scenarios. So, if they are equal, they also equal their geometric mean. So, we have precise equality. In general, it is possible to bound the data complexity by using the number of active words in Lemma 1. This well-known result is valid for an arbitrary ID attack.

Lemma 1 ([29]) *A typical ID attack on an SPN cipher with the parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$ requires at least*

$$\frac{2^{n+1-s(n_i+n_f)}(k_i+k_f)}{\log_2(e)P_iP_f}$$

data in both the chosen plaintexts and the chosen ciphertext scenarios.

Indeed, the data attains the bound if the numbers of structures are integers. That is, we have $D = D_u2^{n+1-sn_i-sn_f}$ in CP if $O(U_i2^{sn_i}) = O(q_i2^{sn_i})$ and $D = D_u2^{n+1-sn_i-sn_f}$ in CC if $O(U_f2^{sn_f}) = O(q_f2^{sn_f})$. We have seen that $D = D_u2^{n+1-sn_i-sn_f}$ in almost all the ID attacks (e.g. [30]–[33], [47]) since the attacks make use of plenty of structures to optimize the overall complexity in both directions. As one exceptional example, the parameters of the attack on Camellia in [50] are $sn_i = 128$, $sn_f = 56$ and $D_u = 2^{168}$. So, $U_i = 2^{-7.5}$ and $U_f = 2^{57}$. Then, the attack requires $D_u2^{129-128-56} = 2^{57}2^{56} = 2^{113}$ CC in the decryption oracle, but $2^{121.5}$ CP in the encryption oracle.

The bound in Lemma 1 might be insufficient for a reciprocal attack if the quantity of the difference, $|n_i - n_f|$, is large enough or the number of structures is less than one in one direction. We treat all the cases to have complete security proofs of SPN ciphers in terms of data requirements of reciprocal ID attacks. It is possible to eliminate the pairs from the cancellations either in the ciphertexts or in the plaintexts. Therefore, if one of n_i or n_f is too small, the corresponding reciprocal attack requires so much data.

Theorem 5 *The data complexity of a typical reciprocal ID attack on an SPN cipher having the parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$ is bounded below by*

$$\sqrt{\frac{2^{n+1-s\cdot\min\{n_i,n_f\}}(k_i+k_f)}{\log_2(e)P_iP_f}}. \tag{13}$$

Proof We have

$$D = (q_i+\epsilon_i)2^{sn_i} \geq \sqrt{q_i+\epsilon_i^2}2^{sn_i} = \sqrt{2D_u2^{n-sn_f}}$$
$$\geq \sqrt{\frac{2^{n+1-sn_f}(k_i+k_f)}{\log_2(e)P_iP_f}}$$

in CP scenario. Similarly,

$$D = (q_f+\epsilon_f)2^{sn_f} \geq \sqrt{q_f+\epsilon_f^2}2^{sn_f} = \sqrt{2D_u2^{n-sn_i}}$$
$$\geq \sqrt{\frac{2^{n+1-sn_i}(k_i+k_f)}{\log_2(e)P_iP_f}}$$

in CC scenario. Hence, the data complexity is bounded below by

$$\sqrt{\frac{2^{n+1-s\cdot\min\{n_i,n_f\}}(k_i+k_f)}{\log_2(e)P_iP_f}}$$

which concludes the proof. □

Theorem 5 introduces an efficient bound. In fact, $\min\{n_i, n_f\} = 4$ in almost all the reciprocal attacks on AES, and the data complexities of some of them are depicted in Table 2 along with the lower bounds deduced through Theorem 5. The question is if the bound in Theorem 5 is sharp. We claim that it is a sharp bound and define the reciprocal attacks attaining this bound as the attacks with optimal data.

Remark 2 *Theorem 2 may be seen similar to the bound given in [29], which is stated as*

$$\sqrt{\frac{2^{n+1-s\cdot\max\{n_i,n_f\}}(k_i+k_f)}{\log_2(e)P_iP_f}} \tag{14}$$

It is plain that the maximum of n_i, n_f is taken in [29] and the bound in Theorem 2 is superior to the bound in Equation 14 which simply improves the lower bound significantly. The bound in Lemma 1 dominates the data if the number of structures is not small (more than four according to our assumption) in both directions and simply determines the data complexity in most of the attacks. However, we must develop

a generic bound valid for any reciprocal ID attack. We use Theorem 5 to provide minimum data required for an arbitrary *reciprocal ID attack. For example, we prove Theorem 7, Theorem 8 and Theorem 9 by using Inequality 13 in Theorem 5 for the security of AES.*

Definition 2 *We call a reciprocal ID attack with data complexity D as a* reciprocal ID attack with optimal data *if its data complexity is not more than twice the bound given in Theorem 5. That is,*

$$\left\lfloor \log_2 D - \log_2 \left(\sqrt{\frac{2^{n+1-s\cdot\min\{n_i,n_f\}}(k_i+k_f)}{\log_2(e)P_iP_f}} \right) \right\rfloor = 0$$

where $\lfloor\cdot\rfloor$ is the flooring function.

There is no reciprocal ID attack on AES with optimal data yet. For the first time, we introduce it in Section V. This example proves that the bound in Theorem 5 is a sharp bound.

Table 2. Some examples of reciprocal ID attacks on 7-round AES with $\min\{n_i, n_f\} = 4$. The data is given in CP. The lower bound in the last column is by Theorem 5.

Attack	(k_i, k_f, P_i, P_f)	Data	Bound
Phan [32],Lu et al. [33]	$(32, 104, 2^{-22}, 2^{-30})$	2^{91}	2^{78}
Bahrak and Aref [30]	$(32, 80, 2^{-22}, 2^{-52})$	2^{115}	2^{89}
Jiang et al. [45]	$(88, 32, 2^{-46}, 2^{-22})$	2^{106}	2^{86}
Zhang et al. [31]	$(32, 64, 2^{-22}, 2^{-54})$	2^{115}	2^{90}
Mala et al. [47]	$(80, 32, 2^{-32}, 2^{-22})$	2^{106}	2^{80}

We characterize the reciprocal ID attacks with data attaining the bound in Theorem 5 in the following statement.

Theorem 6 *Assume $n_i \leq n_f$. The data complexity D of a typical reciprocal ID attack on an SPN cipher having the parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$ attains the bound in Inequality 13 if and only if $D \leq 2^{sn_f}$, and if $D < 2^{sn_f}$ then $n_i = n_f$.*

Proof Let $n_i \leq n_f$ and $D_u = \frac{k_i+k_f}{\log eP_iP_f}$. Assume $D \leq 2^{sn_f}$. That is, $D = \epsilon 2^{sn_f}$ where $\epsilon \leq 1$. Then $D_u = \epsilon^2 2^{2sn_f+sn_i-n-1}$ in terms of the CC attack. So, $D = \epsilon 2^{sn_f} = \sqrt{2^{n+1-sn_i} D_u}$ which is simply equal to

$$\sqrt{\frac{2^{n+1-s\cdot\min\{n_i,n_f\}}(k_i+k_f)}{\log_2(e)P_iP_f}}.$$

For the other direction, assume D is equal to the bound in Inequality 13. The number of the structures is at least $\frac{D_u}{2^{2sn_i+sn_f-n-1}}$ and then

$$\frac{2^{sn_i}\cdot D_u}{2^{2sn_i+sn_f-n-1}} \leq D = \sqrt{2^{n+1-sn_i}\cdot D_u}\,.$$

Solving the inequality with respect to D_u, we have $D_u \leq 2^{2sn_f+sn_i-n-1}$. But, this is the number of the pairs in the CC scenario with only one structure or its subset. So, $D = \epsilon 2^{sn_f}$. If $\epsilon < 1$ then $n_i = n_f$ by Theorem 1 since the attack is reciprocal. □

Corollary 5 *Assume $D \leq 2^{\max\{sn_i,sn_f\}}$ of a typical reciprocal ID attack on an SPN cipher having the parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$. Then,*

$$D_u \leq 2^{\min\{sn_i,sn_f\}+2\max\{sn_i,sn_f\}-n-1}$$

and $n+1 \leq \min\{sn_i, sn_f\} + 2\max\{sn_i, sn_f\}$.

Proof Assume $D \leq 2^{sn_f}$ and $n_i \leq n_f$. Then $\sqrt{2^{n+1-sn_i}D_u} \geq 2^{n+1-sn_i-sn_f}D_u$ by Theorem 6. So, $D_u \leq 2^{sn_i+2sn_f-n-1}$. On the other hand, $1 \leq D_u$. So, $n+1 \leq sn_i + 2sn_f$. □

Corollary 5 can be utilized in developing a design criterion for an SPN cipher to provide security against ID attacks. The diffusion layer of a block cipher is supposed to satisfy the bound

$$P_iP_f \leq 2^{n+1-\min\{sn_i,sn_f\}-2\max\{sn_i,sn_f\}}$$

for any initial and final rounds and for any ID characteristic.

The straightforward conclusion of Corollary 5 is that if the number of structures is less than one, then the number of active words in both input and output cannot be arbitrarily small.

Corollary 6 *Assume $U_i < 1$ for a typical reciprocal ID attack on an SPN cipher having the parameters $(U_i, U_f, D_u, n_i, n_f, k_i, k_f, P_i, P_f)$. Then, $\frac{n+1}{3s} \leq n_i = n_f$*

IV. PROVABLE SECURITY OF AES AGAINST ID ATTACKS

Any ID attack on AES makes use of 4-round ID characteristics and all these characteristics are identified by Grassi et al. in [25]. We introduce the result of the minimum number of data used in a typical reciprocal ID attack on AES exploiting one of these characteristics.

Lemma 2 ([25]) *If the total numbers of the active input diagonal and the output inverse diagonal columns in any 4-round characteristic of AES is less than four then this characteristic is an ID characteristic.*

Definition 3 *We call any 4-round ID characteristic described in Lemma 2 as a 4-round conventional ID characteristic of AES.*

All the known ID attacks on AES are reciprocal ID attacks since their number of structures are integers in both encryption and decryption directions. Moreover, they all exploit 4-round conventional ID characteristics. Indeed, there are no known ID characteristics of AES other than conventional ones. We give a lower bound for the data complexity of a reciprocal ID attack on AES exploiting one of the 4-round conventional ID characteristics.

We introduce the following conjecture in Claim 1. Then, Theorem 7 below can be extended to all the ID attacks on AES when the conjecture is proven.

Claim 1 *All the truncated ID characteristics of r-round AES where $r \geq 4$ are conventional 4-round ID characteristics.*

There are powerful indicators in the literature about the correctness of Claim 1. Sun et al. reduce the problem of the existence of an ID for a given SPN (Substitution Permutation Network) to the problem of the existence of an ID whose input and output Hamming weights are both one. They conclude that AES has no 5-round ID unless the details of the S-Box are not taken into consideration [26]. Another proof is provided by Wang and Jin in [27], exploiting the properties of AES S-box by using the "dependent tree" method. However, their result is given under the assumption that all the round keys are uniformly random and independent. Boura and Coggia show that AES has no 5-round ID by using MILP solvers if the details of both the S-box and the key schedule are taken into account. Moreover, their result is valid only if the first and the last rounds of the characteristic contain two active S-boxes in total [28].

Theorem 7 gives a powerful lower bound for the data complexities of all the known reciprocal ID attacks on AES.

Theorem 7 *A typical reciprocal ID attack on AES exploiting a 4-round conventional ID characteristic has the data complexity of at least 2^{66} chosen plaintexts.*

Proof The number of active *MC* operations (whose input difference is nonzero) before and after any conventional ID characteristic is at least two (one in the initial rounds and one in the final rounds). The total number of passive bytes in one column of the input and in one column of the output of a 4-round conventional ID characteristic is at least 4 by Lemma 2. So, $P_iP_f \leq \binom{4}{2}^2 2^{-32}$. The number of the key bits involved is at least 48. Hence, we have $\frac{k_i+k_f}{\log_2(e)P_iP_f} \geq 2^{31}$. If $n_i + n_f < 12$ then the data $D \geq 2^{70}$ by Lemma 1. Let $n_i + n_f = 12$. Then, we have at least three active *MC* operations. If there are exactly 3 active MC operations then there is only one active MC operation either in the input or in the output. So, $n_i \leq 4$ or $n_f \leq 4$ and hence $2^{129-8\cdot\min\{n_i,n_f\}} \geq 2^{97}$. On the other hand, $P_iP_f \leq 2^{-24} \cdot 4^2 \cdot 2^{-16} = 2^{-36}$ and $k_i + k_f \geq 64$. Hence, $D \geq 2^{69}$ by Theorem 5. We need more data if $n_i \leq 4$ or $n_f \leq 4$ and there are more than 3 active *MC* operations, again by Theorem 5. So, assume $n_i > 4$ and $n_i > 4$ and hence there are at least two active *MC* operations in each direction. Then $P_iP_f \leq \binom{4}{2}^2 2^{-64} \leq 2^{-58}$. We have $k_i + k_f \geq 96$. So, $\frac{k_i+k_f}{\log_2(e)P_iP_f} \geq 2^{64}$. Then, we have $2^{129-8\cdot\min\{n_i,n_f\}} \geq 2^{81}$ since $\min\{n_i, n_f\} \leq 6$. Therefore, $D \geq 2^{71}$ by Theorem 5. So, let $n_i + n_f > 12$. In this case, the number of active *MC* operations is at least 4. Let the number of the active *MC* operations in the initial and final rounds be m_i and m_f respectively. If $(m_i, m_f) = (1, 3)$ then $P_iP_f \leq 2^{-22}2^{-22} = 2^{-44}$ and $k_i + k_f \geq 80$. Hence, $D_u \geq 2^{49}$. On the other hand, $n_i \leq 4$. So, $D \geq 2^{(49+96+1)/2} = 2^{71}$ in the CC scenario. The case $(m_i, m_f) = (3, 1)$ is similar. One can mount the attack in the CP scenario in this case. We need more data for $(m_i, m_f) = (1, \geq 3)$ since P_iP_f is getting less and $k_i + k_f$ increases and hence D_u increases. Assume $(m_i, m_f) = (2, 2)$. Then, $P_iP_f \leq \binom{4}{2}^2 2^{-64}$ and $k_i + k_f \geq 104$ for the minimum data. Hence, $D_u \geq 2^{65}$. So, we need at least 2^{129} pairs. One structure contains at most 2^{127} pairs and at least 2^{-64} of them will be discarded. That is, we need at least 2^2 structures and so $D \geq 2^{66}$ both in CP and in CC scenario. The $(m_i, m_f) = (2, \geq 2)$ case require more data in CC scenario and $(m_i, m_f) = (\geq 2, 2)$ case require more data in CP scenario. When $(m_i, m_f) = (3, 3)$, $P_iP_f \leq \binom{4}{2}^2 2^{-96}$ and $k_i + k_f \geq 128$ since 128 is the minimum key length of AES. So, $D_u \geq 2^{97}$. If $n_i = n_f = 12$ then the attack is slower than the exhaustive search for any key length. If $n_f \leq 11$ than we need at least $2^{97+40} = 2^{137}$ pairs which require at least $D \geq 2^{69}$ CP. Similarly, $D \geq 2^{69}$ CC if $n_i \leq 11$. The cases $(m_i, m_f) = (3, \geq 3)$ or $(m_i, m_f) = (\geq 3, 3)$ require more data. For the last case, let $(m_i, m_f) = (4, 4)$. Then, $P_iP_f \leq \binom{4}{2}^2 2^{-128}$ and $k_i + k_f \geq 128$ since 128 is the minimum key length of AES. So, $D_u \geq 2^{129}$. Again we need more than 2^{66} data for a successful attack. □

We prove in Theorem 7 that any reciprocal ID attack on AES exploiting a conventional 4-round ID characteristic requires at least 2^{66} data whatsoever its steps are. The question is if there are reciprocal ID attacks on AES with roughly this data complexity. We introduce an example in Section V. This attack is both a reciprocal ID attack with optimal data and its data complexity attains the bound in Theorem 7.

Almost all the ID attacks on AES in the literature make use of four active bytes in either the first or the last round which produces only one byte active after the MDS multiplication. Then, we can prove the following statement for these attacks even though they do not exploit conventional ID characteristics.

Theorem 8 *Let a reciprocal ID attack make use of only four active bytes in the plaintext pairs and the MC operation in the first round produces only one active byte. Then the minimum data to eliminate all the subkeys involved is bounded below by 2^{62}.*

Proof We have $n_i = 4$, $k_i = 32$ and $P_i = 2^{-22}$. Assume $n_f \geq 4$. Then $K_f \geq 32$. Hence, $\min\{n_i, n_f\} = 4$ and then $D \geq \sqrt{\frac{2^{129-32}(32+32)}{\log_2(e)2^{-22}}} \geq 2^{62}$ by Theorem 5. If $n_f < 4$ then $\min\{n_i, n_f\} \leq 3$ and hence $D \geq \sqrt{\frac{2^{129-24}\cdot 32}{\log_2(e)2^{-22}}} > 2^{62}$. Therefore the minimum data to eliminate all the subkeys involved is bounded below by 2^{62}. □

All the well-known ID attacks on AES in [30]–[33], [47] make use of one active column of the *MC* operation in the first round. This column results in only one active byte. Hence all these attacks require at least 2^{62} CP according to Theorem 8.

It seems it is not possible to introduce an eligible lower bound for the data complexity of a typical nonreciprocal ID attack on AES. But we can give a lower bound for the time complexity.

Theorem 9 *Any typical nonreciprocal ID attack on AES exploiting one of the 4-round conventional ID characteristics has the time complexity of at least 2^{88} trials.*

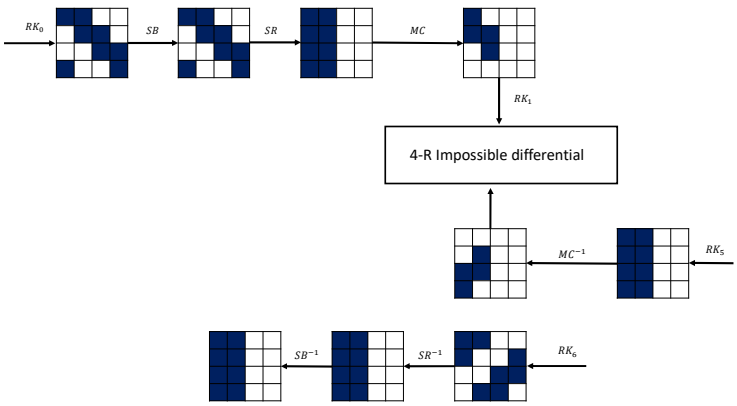

Figure 3. 6-Round reciprocal ID Attack on AES with optimal data

Proof Let us show that n_i or n_f of a nonreciprocal attack on AES is greater than 10. Assume $n_i \leq 9$. If $n_i = 9$ then one structure can produce 2^{143} pairs and there are at least 3 active *MC* operations in the first round. If there is only one active *MC* operation in the last round then at most 2^{47} of the pairs remain and $P_iP_f \leq 4^2 2^{-24} 2^{-24} = 2^{-44}$ with $D_u \geq 2^{50}$. So, we need at least 8 structures in CP attack and many more structures in CC attack. So, the attack will be reciprocal. Assume there are two active *MC* operations in the last round. Then, $P_iP_f \leq 6^2 2^{-48} 2^{-32}$ and $D_u \geq 2^{83}$. Again, the number of remaining pairs in a structure is at most 2^{79}. Hence we need at least 16 structures in CP attack and many more in CC attack. So, the attack cannot be reciprocal. Assume there are three active *MC* operations in the last round. Then, assume $n_f \leq 10$. This implies that $P_iP_f \leq 6^2 2^{-48} 2^{-48}$ and $D_u \geq 2^{91}$. So, again, there are at least 2^4 structures in both directions. Similarly, if all the *MC* operations are active and $n_f \leq 10$ then there is only one case: $n_f = 10$. The number of active bytes in the ciphertext pairs in each *MC* operation must be 2-2-3-3 or 2-2-2-4. So, $P_iP_f \leq 4^2 2^{-72} 2^{-32}$ and $D_u \geq 2^{115}$ and the attack will be obviously reciprocal. In conclusion, if $n_i = 9$ then $n_f \geq 11$. Similarly, if $n_i < 9$ then $n_f \geq 11$. So, there are at least 11 active bytes in the plaintext pairs or in the ciphertext pairs. That is, we need at least 2^{88} trials. □

Notice that Theorem 9 is valid for any key schedule. That is, if AES had no key schedule and all the round keys were equal then again any nonreciprocal ID attack would require at least 2^{88} trials. Each trial is almost one encryption or partial encryption, depending on the characteristic of the special attack.

V. A RECIPROCAL ID ATTACK WITH OPTIMAL DATA

We introduce an example of a 6-round reciprocal ID attack as depicted in Figure 3 on AES to show that our lower bound is almost sharp. In this attack $n_i = n_f = 8, P_i = P_f = 6 \cdot 2^{-32} \approx 2^{-29.5}, k_i = k_f = 64$. Hence $D_u \geq (2^{59} 2^7)/\log_2(e) \approx 2^{65.3}$. So, take $U_i = 5 \approx 2^{2.5}$. Then, the data complexity is $D = 2^{64} 2^{2.5} = 2^{66.5}$. Each pair among D_u pairs suggests around $(6 \cdot 2^{32})^2 \approx 2^{69}$ subkeys and we can determine all these keys by guessing four bytes from RK_0 and four bytes from RK_6. Then, we detect the wrong keys to be eliminated for each guess and for each pair. So, the time complexity is around $2^{65.5} 2^{69} = 2^{134.5}$ memory accesses which is roughly 2^{131} encryptions. We can recover 64 bits of RK_6 which are $RK_6[0, 1, 4, 7, 10, 11, 13, 14]$. Then, we can recover the remaining 16 bytes of RK_6 and RK_5 by exhaustive search for AES-192 or we mount the attack with the same data, this time to recover the other round key bytes of RK_6 by switching the active and passive bytes in the ciphertext pairs. Therefore, this attack works on AES-192 and AES-256.

If we have only 2^{66} CP, then the number of pairs D_u will be 2^{65}. We have around $2^{35.5}$ pairs which suggest the output of the 4-round ID characteristic for a fixed value of $RK_6[0, 1, 4, 7, 10, 11, 13, 14]$. Then, the probability that a candidate for the 64-bit whitening key bytes $RK_0[0, 1, 5, 6, 10, 11, 12, 15]$ is not eliminated is $(1 - 2^{-29.5})^{2^{35.5}} \approx e^{-64} \approx 2^{-92.3}$. Hence the probability that all the 64-bit whitening keys are eliminated is $(1 - 2^{-92.3})^{2^{64}} > 1 - 2^{-28}$. That is, we expect more than $(2^{64} - 2^{36})$ of the candidates for the round key $RK_6[0, 1, 4, 7, 10, 11, 13, 14]$ to be eliminated. That is, we get its 28-bit information about RK_6 and the attack with 2^{66} CP data will be faster than the exhaustive search. Therefore our attack is an ID attack with optimal data by Definition 2.

VI. A NONRECIPROCAL ID ATTACK ON AES

We show that the reciprocal ID attacks require many data. Particularly, any reciprocal ID attack on AES exploiting a 4-round conventional ID characteristic requires at least 2^{66} data by Theorem 7. We examine if a high data complexity requirement is necessary for any ID attack in this section. So, we introduce a nonreciprocal ID attack on AES which requires only 2^{30} CP to show that Theorem 7 is not true for nonreciprocal ID attacks even though the characteristic

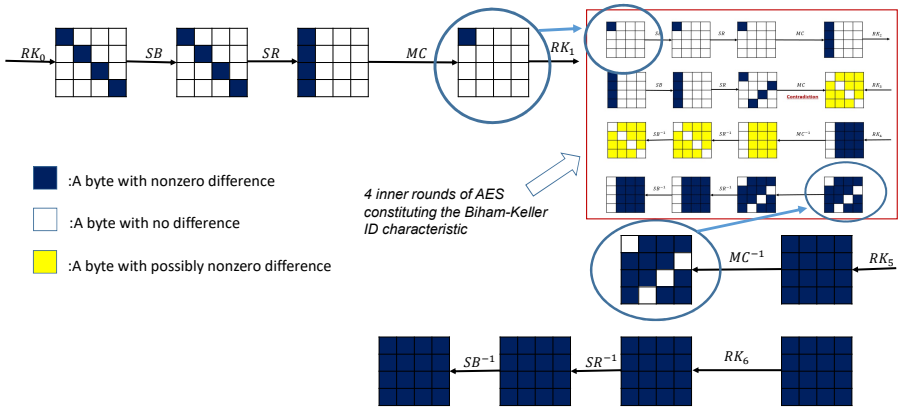

Figure 4. 6-Round nonreciprocal ID Attack on AES exploiting Biham-Keller characteristic

exploited is a 4-round conventional ID characteristic given in Lemma 2.

For the illustration of how to mount an ID attack on AES with small data complexity, we exploit the well-known ID characteristic introduced by Biham and Keller [43]. The Biham-Keller characteristic is exploited in several ID attacks such as [31]–[33], [43]. We use this characteristic to mount a typical ID attack on 6-round AES which is depicted in Figure 4. The parameters of the attack are as follows: $n_i = 4, k_i = 32, U_i = 2^{-2}, P_i = 2^{-22}$; $n_f = 16, k_f = 128, U_f = 2^{-50}, P_f = 2^{-30}$. Then, the data complexity for the CP attack is $U_i 2^{8n_i} = 2^{-2}2^{32} = 2^{30}$ whereas it is $U_f 2^{8n_f} = 2^{-50}2^{128} = 2^{78}$ chosen ciphertexts. Clearly, it is not reciprocal. Indeed, $2^{32}(2^{-4}-2^{-2}) \neq 2^{128}(2^{-100}-2^{-50})$ and hence the attack is nonreciprocal by Proposition 1. As easily observed, Theorem 2, Theorem 4, and Theorem 5 do not work for this attack since it is a nonreciprocal attack. Indeed, the lower bounds are $2^{136/3}$, 2^{54}, and 2^{46} respectively, which are even higher than $D = 2^{30}$.

VII. A NEW ATTACK WITH MINIMUM DATA

We introduce a nonreciprocal ID attack on 6-round AES which requires only 2^{18} CP. This is a record in terms of the minimum data complexity.

We derive a 3-round Impossible Differential (ID) characteristic by loosening the Biham-Keller ID characteristic. This expansion entails the activeness of all bytes in the output difference (see Figure 5). We can exploit it by utilizing the property that all the bytes after the *SR* operation in the third round of the ID characteristic are active. So, if we add one round at the beginning and one more round at the end, we expect all the bytes of an input pair of *MC* in the fourth round to be active for a whiting key producing only one active byte at the end of the first round, as depicted in Figure 5. We exploit this property as our distinguisher for our ID attack. We can examine the distinguisher since the whole round key is searched in the last round.

We mount our ID attack on 6-round AES-192 and AES-256 and we exploit their key schedules to use the minimum data in our attack on 6-round AES. First of all, we extend the idea of the key bridge of the key schedule of AES-256 introduced by Dunkelman et al. [9].

Proposition 2 *$RK_0[15]$ can be computed through RK_6 for AES-256.*

Proof Let us assume the last round key RK_6 is known. The key schedule of AES-256 gives us

$$RK_0[15] = RK_2[14] \oplus RK_2[15] = RK_4[13] \oplus RK_4[15]$$

which equals

$$RK_6[12] \oplus RK_6[13] \oplus RK_6[14] \oplus RK_6[15].$$

□

a: AES-256 Case:

Let us take 2^{18} chosen plaintexts which give us 2^{35} pairs. Guess 128-bit RK_6. Then, we can compute $RK_0[15]$ through the key schedule by Proposition 2 for AES-256 and determine the remaining 24 bits, $RK_0[0, 5, 10]$ for each pair through the linear equations $\Delta MC_1[4, 8, 12] = 0$, $\Delta MC_1[0, 8, 12] = 0$, $\Delta MC_1[0, 4, 12] = 0$, and $\Delta MC_1[0, 4, 8] = 0$. Obtain the ciphertexts of around 2^{13} pairs which produce only one active byte at the end of the first round for a fixed 32-bit RK_0 in the four active input bytes, since the probability of producing one active byte through MC_1 is 2^{-22}.

Let us consider the equivalent key $MC^{-1}(RK_5)$ which is executed before the *MC* operation and choose one of its inverse diagonals to eliminate. Each inverse diagonal enables us to compute the corresponding column of the output of the fourth round. If we consider the first inverse diagonal then we can eliminate the round key bytes $MC^{-1}(RK_5)[0, 7, 10, 13]$ by computing the first row of the output difference of the fourth round and checking if MC_4^{-1} produces less than four active bytes in the first column. This will give us a contradiction since we expect all the bytes of an input pair of *MC* to

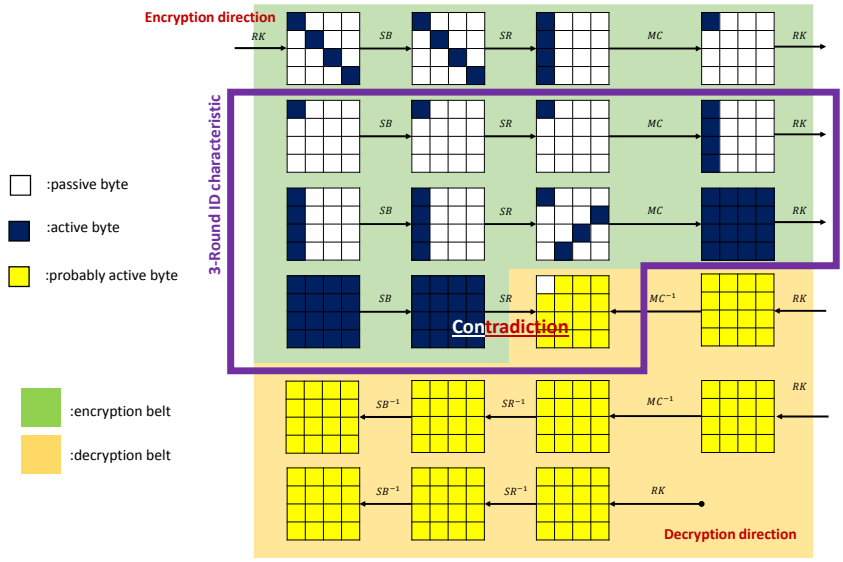

Figure 5. 6-Round nonreciprocal ID Attack on AES with minimum data

be active in the fourth round. The probability of this contradiction is slightly larger than 2^{-6}. Therefore, the probability of eliminating each candidate for $MC^{-1}(RK_5)[0,7,10,13]$ is $(1-2^{-6})^{2^{13}} \approx e^{-128} \approx 2^{-184.5}$. Hence we expect all the guessed keys to be eliminated. If there are some key candidates left, we repeat the attack for the second, third, and last columns of MC_4^{-1} to eliminate the keys left.

We guess 128 bits of RK_6 and determine 8 bits of RK_0 through the key schedule and 24 bits of RK_0 from data. So, we have 152 bits and each guess is eliminated by about 2^{11} pairs on average. Hence the time complexity is $2^{152}2^{11}2^{26} = 2^{189}$ memory accesses which is around 2^{186} encryptions. The memory complexity is $2^{24}2^{13} = 2^{37}$ units which is roughly 2^{43} bytes. The data complexity is 2^{18} CP.

b: ***AES-192 Case:***

We need a hash table for $RK_0[0,5,10,15]$ which can be prepared during offline (see [43]). The table contains about 2^{10} keys for each plaintext pair $(P[0,5,10,15], P'[0,5,10,15]$ leading to only one active byte after MC_1, and is sorted with respect to the plaintext pairs.

First, let us guess RK_6. Then, compute $MC^{-1}(RK_5)[0,13]$ through the key schedule for AES-192 since we can compute the first two columns of RK_5 from RK_6. Furthermore, guess one byte from $MC^{-1}(RK_5)[10,7]$ and determine the other byte through each ciphertext pair. Then, for each 144-bit secret information, determine the ciphertext pairs among 2^{35} pairs leading to the impossible differential in the output. That is, check if $\Delta MC_4^{-1}[0,4,8,12]$ has at least one passive byte. The probability is about 2^{-6}. So, there will be around 2^{29} ciphertext pairs for each 144-bit guess of RK_6 and $MC^{-1}(RK_5)[10,7]$, which is loaded in a memory for key. This memory can be reused for different 144-bit guesses.

Each 144-bit candidate is tested with the plaintext pairs of the corresponding ciphertext pairs. We have around 2^{29} plaintext pairs and each pair eliminates around 2^{10} keys $RK_0[0,5,10,15]$ from the hash table. If all the candidates for $RK_0[0,5,10,15]$ are eliminated, then the 144-bit guess is eliminated. So, the time complexity is $2^{144}2^{29}2^{10} = 2^{183}$ memory accesses which is around 2^{180} encryptions for AES-192. The memory complexity is $12 \cdot 2^{32}2^{32}2^{10} \approx 2^{78}$ bytes. The data complexity is 2^{18} CP.

VIII. ENHANCING INTEGRAL ATTACK

We have introduced an attack on 6-round AES with the minimum data in the previous section. Its time complexity is marginal. In this section, we study the improvements over the best attack on 6-round AES in terms of data, time, and memory complexities.

The integral attack using the partial sum technique in [36] has been the best attack on 6-round AES with respect to the total complexity given in [36] as 2^{44} encryptions since 2000. In this section, we examine the practical security of 6-round AES and improve the best attack further. We utilize the partial sum technique but we refrain from an extensive elaboration on this technique. One can see [36] for the details. In summary, we prove better complexities in data, time, and memory.

First of all, we introduce here a small correction in the attack in [36]. It is given only for recovering the four bytes of one of the reverse diagonals of the round key RK_6 in the sixth round with a complexity of 2^{44} encryptions. However, the attack should be repeated four times to recover the whole round key in the last round. The fifth round key can be recovered much faster in the cases of 192-bit and 256-bit key lengths. So, the overall complexity should be 2^{46} rather than 2^{44}. We correct this minor fault and amend the complexity in

Table 1 accordingly.

The attack uses $6 \cdot 2^{32}$ CP in [36]. In this section, we improve the attack by using only 2^{32} CP for AES-128 and it is 8 times faster. The attack is 4 times faster for the other key lengths and utilizes 2^{33} CP.

Let an oracle encrypt 2^{32} CP where the first diagonal $(P[0,5,10,15])$ takes all the values and the other bytes are constant, and it publishes the corresponding ciphertexts.

We evaluate the S-box operations as 8×32-bit given as

$$S(x) = 0e{\cdot}SB^{-1}(x)||0b{\cdot}SB^{-1}(x)||0d{\cdot}SB^{-1}(x)||09{\cdot}SB^{-1}(x)$$

to deal with the Galois field multiplication, and obtain the four bytes of the inverse MixColumn operation in one S-Box call, where $||$ is the concatenation.

For each inverse diagonal, guess the 32-bit key in the sixth round and one byte of $MC^{-1}(RK_5)$ from the column where this 32-bit key affects after the SR^{-1} operation. So, we can compute the corresponding byte at the end of the fourth round and then check if the sum is zero for all the 2^{32} ciphertexts.

We exploit the zero-sum distinguisher as in [36] by using the partial sum technique. As one improvement, we utilize the zero-sum property not for only one byte in each column in MC_4, but for all the bytes since all the 16 bytes of MC_4 are balanced. Hence, our distinguisher has the false alarm probability of 2^{-128} instead of 2^{-32} for each structure, which enables us to reduce the data up to a factor of six for AES-128.

Guessing one key for the reverse diagonal $RK_6[0,7,10,13]$, around one candidate for $MC^{-1}(RK_5)[0]$ will pass the zero-sum test given as

$$\bigoplus_{i=0}^{2^{32}-1} MC_4[0] = 0.$$

Similarly, one candidate for $MC^{-1}(RK_5)[4]$ passes the zero-sum test given as

$$\bigoplus_{i=0}^{2^{32}-1} MC_4[4] = 0;$$

one candidate for $MC^{-1}(RK_5)[8]$ passes the zero-sum test given as

$$\bigoplus_{i=0}^{2^{32}-1} MC_4[8] = 0;$$

and one candidate for $MC^{-1}(RK_5)[12]$ passes the zero-sum test given as

$$\bigoplus_{i=0}^{2^{32}-1} MC_4[12] = 0.$$

After determining $MC^{-1}(RK_5)[0,4,8,12]$ for each guess of the reverse diagonal $RK_6[0,7,10,13]$, we can compute $RK_5[0,4,8,12]$ by applying MC. We have four zero-sum tests in one column and the probability that all the tests produce nonempty solution sets for a 32-bit guess for $RK_6[0,7,10,13]$ is $(1-\frac{255}{256}^{256})^4 \approx 2^{-2.6}$. So, we expect less than 2^{30} candidates for $RK_6[0,7,10,13]$, and around 2^{32} candidates for $(RK_6[0,7,10,13], RK_5[0,4,8,12])$.

Let us store them in a memory, say $\mathcal{A}_1$. Similarly, compute and store the candidates for

$$(RK_6[1,4,11,14], RK_5[1,5,9,13]), \quad (15)$$
$$(RK_6[2,5,8,15], RK_5[2,6,10,14]), \quad (16)$$
$$(RK_6[3,6,9,12], RK_5[3,7,11,15]) \quad (17)$$

in $\mathcal{A}_2$, $\mathcal{A}_3$, and $\mathcal{A}_4$ respectively. If we repeat the attack for the elements in the sets $\mathcal{A}_i$, $i = 1,\ldots,4$, by using another structure of 2^{32} CP, we have around one element in each set. So, we recover RK_5 and RK_6 by using two structures, without exploiting the key schedule.

The attack utilizes 2^{33} CP instead of $6 \cdot 2^{32}$ CP. Preparing each set $\mathcal{A}_i$, $i = 1,2,3,4$, costs around 2^{49} S-box operations through the partial sum. We have 2^{32} vectors for each reverse diagonal. Remove the vectors that appeared an even number of times and hence around 2^{31} will be left. The first step of the partial sum costs $2^{31}2^{16} \cdot 2 = 2^{48}$ S-box operations where we search only 2 bytes of the last round key in any reverse diagonal with 2 S-box operations. Then, there are around 2^{23} vectors left. The second step costs $2^{23}2^{24} \cdot 1 = 2^{47}$ S-box operations and the number of vectors left is around 2^{15}. The third step costs $2^{15}2^{32} \cdot 1 = 2^{47}$ S-box operations again. The last step is run with only 2^7 vectors and hence it costs also $2^7 2^{40} \cdot 1 = 2^{47}$ S-box operations. We use directly SB^{-1} in this last step. Then we can check the zero-sum condition. The total complexity is around $2^{48} + 3 \cdot 2^{47} \approx 2^{49}$ S-box operations.

We repeat this partial sum technique for 3 other reverse diagonals. So, the overall complexity is around 2^{51} S-box operations which is around 2^{43} encryptions if we assume 2^8 S-box operations is roughly one encryption, as in [36]. We mount the attack once more for the other structure to eliminate almost all the elements in the sets. Hence, the time complexity is 2^{44} encryptions. The memory complexity is $2^3 2^{32} = 2^{35}$ bytes for loading one set among $\mathcal{A}_i$, $i = 1,2,3,4$; and 2^{37} bytes for loading the ciphertexts. So, we need around 2^{37} bytes. Note that the memory for each set $\mathcal{A}_i$ can be reused if we construct one set and then eliminate its elements by utilizing the ciphertexts of the second structure before constructing the other sets.

We can further improve the attack for AES-128 by exploiting the key schedule. Only one structure is enough for this case. Sort $\mathcal{A}_1$ by $RK_5[12], RK_6[7], RK_5[0] \oplus RK_6[0]$. Because we can deduce these values from $\mathcal{A}_4$ through the key schedule for AES-128.

$$RK_5[12] = SB(RK_5[3]) \oplus RK_6[12], \quad (18)$$
$$RK_6[7] = RK_6[6] \oplus RK_5[7], \quad (19)$$
$$RK_5[0] \oplus RK_6[0] = SB(RK_5[7]). \quad (20)$$

Note that we ignore the round constants in the key schedule. The parameters on the left of the equations are unknown and the parameters on the right of the equations are known. So, if we choose one element from $\mathcal{A}_4$ then we can determine $RK_5[12], RK_6[7], RK_5[0] \oplus RK_6[0]$ through the key schedule

and hence there will be around 2^8 elements in $\mathcal{A}_1$. Similarly, sort $\mathcal{A}_3$ by $RK_6[8], RK_5[10], RK_6[2], RK_6[15], RK_5[6] \oplus RK_6[5]$ since we have

$$\begin{aligned} RK_6[8] &= SB(RK_5[12]) \oplus RK_5[8], && (21)\\ RK_5[10] &= RK_6[10] \oplus RK_6[9], && (22)\\ RK_6[2] &= RK_5[3] \oplus RK_6[3], && (23)\\ RK_5[6] \oplus RK_6[5] &= RK_6[6]. && (24) \end{aligned}$$

Then, we have only one element in $\mathcal{A}_3$ on average for each element in $\mathcal{A}_1$ and in $\mathcal{A}_4$. Hence, there are around 2^8 elements left in $\mathcal{A}_1$ and $\mathcal{A}_3$ for one chosen element in $\mathcal{A}_4$.

Similarly, we have nine byte equations for $\mathcal{A}_2$ with a condition of 2^{-72}. We can use four equations for sorting and 5 equations for checking. For instance, sort $\mathcal{A}_2$ by $(RK_6[1], RK_6[4], RK_6[11], RK_6[14])$ and for each candidate compute

$$\begin{aligned} RK_6[1] &= RK_6[2] \oplus RK_5[2], && (25)\\ RK_6[4] &= SB(RK_5[11]) \oplus RK_5[4], && (26)\\ RK_6[11] &= RK_5[11] \oplus RK_6[10], && (27)\\ RK_6[14] &= RK_5[15] \oplus RK_6[15]. && (28) \end{aligned}$$

These equations give one element on average for each element in $\mathcal{A}_1$, in $\mathcal{A}_3$, and in $\mathcal{A}_4$. Then, it is possible to check the candidate with the following 5 equations.

$$\begin{aligned} RK_5[9] &= RK_6[8] \oplus RK_6[9], && (29)\\ RK_5[13] &= RK_6[12] \oplus RK_6[13], && (30)\\ RK_6[4] \oplus RK_5[5] &= RK_6[5], && (31)\\ RK_6[1] \oplus RK_5[1] &= RK_6[0], && (32)\\ RK_6[14] &= RK_6[13] \oplus RK_5[14]. && (33) \end{aligned}$$

with a probability of 2^{-40}. We have 2^8 candidates for each element in $\mathcal{A}_4$ in the other sets. So, all together, we expect only one element to be left in the last five equations since we have 2^{40} candidates in all the sets and the probability that one candidate satisfies the five equations is 2^{-40}. That is, there are around two candidates passing both the zero-sum check and the equations of the key schedule. One of them is the correct key and it can be deduced by a quick search.

The complexity of constructing the sets $\mathcal{A}_i$ is around 2^{51} S-box operations which is around 2^{43} encryptions. The key schedule utilization phase is much faster. Because we test five equations in $\mathcal{A}_i$ for each of 2^{40} candidates. However, most of them are eliminated in Equation 29. So, the key schedule utilization phase consists of 2^{40} tests of equations like Equation 29, which is around 2^{40} byte-wise XOR operations. Similarly, eliminating vectors costs 2^{33} S-box and $3 \cdot 2^{32}$ XOR operations, 2^{40} S-box and 2^{42} XOR operations, and 2^{40} S-box and 2^{42} XOR operations in $\mathcal{A}_1$, $\mathcal{A}_3$, and $\mathcal{A}_2$ respectively. It is clear that the key schedule utilization phase is much less than 2^{40} encryptions.

The memory complexity is $4 \cdot 2^3 2^{32} = 2^{37}$ bytes for loading the sets $\mathcal{A}_i$, $i = 1, 2, 3, 4$; and 2^{36} bytes for loading the ciphertexts.

In total, we improve the best attack on 6-round AES-128 by a factor of 6 in data usage, by a factor of 8 in time complexity, and by a factor of 2 in memory complexity.

IX. CONCLUSION AND DISCUSSION

Our study has taken a distinct and generic approach to the security analysis of SPN ciphers against ID attacks compared to typical cryptanalysis works, which simply aim to find the best attack on a specific cipher. We have categorized ID attacks on SPN ciphers into two distinct types: reciprocal ID attacks and nonreciprocal ID attacks. Moreover, we have proved lower bounds on the data complexity of a reciprocal ID attack on an SPN cipher. We have introduced a vast theoretical framework for a comprehensive understanding of the data requirements of ID attacks on SPN ciphers.

As an illustrative application of our theoretical insights on SPN ciphers, we have made use of our generic statements to prove the security bounds for a widely recognized cipher, namely AES, against ID attacks. Particularly, we have shown that a reciprocal ID attack on AES exploiting a 4-round conventional ID characteristic requires at minimum 2^{66} CP. Our conjecture is that all 4-round ID characteristics for AES are conventional, resulting in a requirement of 2^{66} chosen plaintexts for any reciprocal ID attack on six or more rounds of AES. We have introduced also a reciprocal ID attack on 6-round AES with 2^{66} data to show that the lower bound is almost sharp. On the other hand, we have demonstrated a counterexample that this security bound is not valid for nonreciprocal ID attacks by mounting a nonreciprocal ID attack on 6-round AES-192 and AES-256 that requires only 2^{18} chosen plaintexts. However, its time complexity is marginal. Indeed, this is not a coincidence; we have proven that any nonreciprocal ID attack on AES exploiting a 4-round conventional ID characteristic has a time complexity of at least 2^{88} trials. Then, as a practical application, we improve the integral attack through the partial sum technique in [36], thereby enhancing the existing record after a duration of 23 years. Our attack is the fastest against 6-round AES. The time, data, and memory complexities are improved by factors of 4, 3, and 3 times (or 8, 6, and 2 times for AES-128), respectively.

We think that applying the theoretical foundation established in this study could lead to the discovery of several new results regarding ID attacks on other SPN ciphers. So, similar to proving the security bounds for AES, investigating the minimal data required for reciprocal ID attacks on other noteworthy SPN ciphers by utilizing Theorem 2, Theorem 4, and Theorem 5 is a prospect for future research. Additionally, similar findings can be obtained for Feistel networks.

ACKNOWLEDGMENT

We thank F. Karakoç, M.S. Kiraz, A.A. Selçuk, and B. Ustaoğlu, for their invaluable comments. We utilized ChatGPT for proofreading and rewording the abstract and the introduction.

References

[1] Morris Dworkin, Elaine Barker, James Nechvatal, James Foti, Lawrence Bassham, E. Roback, and James Dray. Advanced encryption standard (AES), 2001-11-26 2001.

[2] Charles Bouillaguet, Patrick Derbez, Orr Dunkelman, Pierre-Alain Fouque, Nathan Keller, and Vincent Rijmen. Low-data complexity attacks on AES. *IEEE Trans. Inf. Theory*, 58(11):7002–7017, 2012.

[3] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[4] Liam Keliher and Jiayuan Sui. Exact maximum expected differential and linear probability for two-round advanced encryption standard. *IET Inf. Secur.*, 1(2):53–57, 2007.

[5] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. *J. Cryptol.*, 18(4):291–311, 2005.

[6] Lars Knudsen. DEAL a 128-bit block cipher. *Complexity*, 258(2):216, 1998.

[7] Hüseyin Demirci and Ali Aydin Selçuk. A meet-in-the-middle attack on 8-round AES. In Kaisa Nyberg, editor, *Fast Software Encryption, 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, volume 5086 of *Lecture Notes in Computer Science*, pages 116–126. Springer, 2008.

[8] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. *J. Cryptol.*, 28(3):397–422, 2015.

[9] Orr Dunkelman, Nathan Keller, and Adi Shamir. Improved single-key attacks on 8-round AES-192 and AES-256. In Masayuki Abe, editor, *Advances in Cryptology - ASIACRYPT 2010 - 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings*, volume 6477 of *Lecture Notes in Computer Science*, pages 158–176. Springer, 2010.

[10] Gaoli Wang and Chunbo Zhu. Single key recovery attacks on reduced AES-192 and Kalyna-128/256. *Sci. China Inf. Sci.*, 60(9):99101, 2017.

[11] Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved key recovery attacks on reduced-round AES in the single-key setting. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2013.

[12] Leibo Li, Keting Jia, and Xiaoyun Wang. Improved single-key attacks on 9-round AES-192/256. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014. Revised Selected Papers*, volume 8540 of *Lecture Notes in Computer Science*, pages 127–146. Springer, 2014.

[13] Henri Gilbert and Marine Minier. A collision attack on 7 rounds of Rijndael. In *The Third Advanced Encryption Standard Candidate Conference, April 13-14, 2000, New York, New York, USA*, pages 230–241. National Institute of Standards and Technology,, 2000.

[14] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.

[15] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer, 2011.

[16] Biaoshuai Tao and Hongjun Wu. Improving the biclique cryptanalysis of AES. In Ernest Foo and Douglas Stebila, editors, *Information Security and Privacy - 20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, June 29 - July 1, 2015, Proceedings*, volume 9144 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2015.

[17] Dhiman Saha, Mostafizar Rahman, and Goutam Paul. New yoyo tricks with AES-based permutations. *IACR Trans. Symmetric Cryptol.*, 2018(4):102–127, 2018.

[18] Mostafizar Rahman, Dhiman Saha, and Goutam Paul. Boomeyong: Embedding yoyo within boomerang and its applications to key recovery attacks on AES and pholkos. *IACR Trans. Symmetric Cryptol.*, 2021(3):137–169, 2021.

[19] Augustin Bariant and Gaëtan Leurent. Truncated boomerang attacks and application to AES-based ciphers. In Carmit Hazay and Martijn Stam, editors, *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part IV*, volume 14007 of *Lecture Notes in Computer Science*, pages 3–35. Springer, 2023.

[20] Navid Ghaedi Bardeh and Vincent Rijmen. New key-recovery attack on reduced-round AES. *IACR Trans. Symmetric Cryptol.*, 2022(2):43–62, 2022.

[21] Kaixin Zhao, Jie Cui, and Zhiqiang Xie. Algebraic cryptanalysis scheme of AES-256 using Gröbner basis. *J. Electr. Comput. Eng.*, 2017:9828967:1–9828967:9, 2017.

[22] Lorenzo Grassi. Probabilistic mixture differential cryptanalysis on round-reduced AES. In Kenneth G. Paterson and Douglas Stebila, editors, *Selected Areas in Cryptography - SAC 2019 - 26th International Conference, Waterloo, ON, Canada, August 12-16, 2019, Revised Selected Papers*, volume 11959 of *Lecture Notes in Computer Science*, pages 53–84. Springer, 2019.

[23] Lorenzo Grassi and Markus Schofnegger. Mixture integral attacks on reduced-round AES with a known/secret s-box. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 312–331. Springer, 2020.

[24] Gaëtan Leurent and Clara Pernot. New representations of the AES key schedule. In Anne Canteaut and François-Xavier Standaert, editors, *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part I*, volume 12696 of *Lecture Notes in Computer Science*, pages 54–84. Springer, 2021.

[25] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. Subspace trail cryptanalysis and its applications to AES. *IACR Transactions on Symmetric Cryptology*, 2016(2):192–225, Feb. 2017.

[26] Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I*, volume 9665 of *Lecture Notes in Computer Science*, pages 196–213. Springer, 2016.

[27] Qian Wang and Chenhui Jin. More accurate results on the provable security of AES against impossible differential cryptanalysis. *Des. Codes Cryptogr.*, 87(12):3001–3018, 2019.

[28] Christina Boura and Daniel Coggia. Efficient MILP modelings for Sboxes and linear layers of SPN ciphers. *IACR Trans. Symmetric Cryptol.*, 2020(3):327–361, 2020.

[29] Christina Boura, María Naya-Plasencia, and Valentin Suder. Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon. In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer, 2014.

[30] Behnam Bahrak and Mohammad Reza Aref. Impossible differential attack on seven-round AES-128. *IET Inf. Secur.*, 2(2):28–32, 2008.

[31] Wentao Zhang, Wenling Wu, and Dengguo Feng. New results on impossible differential cryptanalysis of reduced AES. In Kil-Hyun Nam and Gwangsoo Rhee, editors, *Information Security and Cryptology - ICISC 2007, 10th International Conference, Seoul, Korea, November 29-30, 2007, Proceedings*, volume 4817 of *Lecture Notes in Computer Science*, pages 239–250. Springer, 2007.

[32] Raphael Chung-Wei Phan. Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES). *Inf. Process. Lett.*, 91(1):33–38, 2004.

[33] Jiqiang Lu, Orr Dunkelman, Nathan Keller, and Jongsung Kim. New impossible differential attacks on AES. In Dipanwita Roy Chowdhury, Vincent Rijmen, and Abhijit Das, editors, *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India,*

Kharagpur, India, December 14-17, 2008. Proceedings, volume 5365 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2008.

[34] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. *J. Cryptol.*, 33(3):1003–1043, 2020.

[35] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir. Improved key recovery attacks on reduced-round AES with practical data and memory complexities. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II*, volume 10992 of *Lecture Notes in Computer Science*, pages 185–212. Springer, 2018.

[36] Niels Ferguson, John Kelsey, Stefan Lucks, Bruce Schneier, Michael Stay, David A. Wagner, and Doug Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000, New York, NY, USA, April 10-12, 2000, Proceedings*, volume 1978 of *Lecture Notes in Computer Science*, pages 213–230. Springer, 2000.

[37] Navid Ghaedi Bardeh and Sondre Rønjom. Practical attacks on reduced-round AES. In Johannes Buchmann, Abderrahmane Nitaj, and Tajje-eddine Rachidi, editors, *Progress in Cryptology - AFRICACRYPT 2019 - 11th International Conference on Cryptology in Africa, Rabat, Morocco, July 9-11, 2019, Proceedings*, volume 11627 of *Lecture Notes in Computer Science*, pages 297–310. Springer, 2019.

[38] Debranjan Pal, Md Rasid Ali, Abhijit Das, and Dipanwita Roy Chowdhury. A cluster-based practical key recovery attack on reduced-round AES using impossible-differential cryptanalysis. *J. Supercomput.*, 79(6):6252–6289, 2023.

[39] Patrick Derbez. *Meet-in-the-Middle Attacks on AES*. Theses, Ecole Normale Supérieure de Paris - ENS Paris, December 2013.

[40] Joan Daemen, Lars R. Knudsen, and Vincent Rijmen. The block cipher Square. In Eli Biham, editor, *Fast Software Encryption, 4th International Workshop, FSE '97, Haifa, Israel, January 20-22, 1997, Proceedings*, volume 1267 of *Lecture Notes in Computer Science*, pages 149–165. Springer, 1997.

[41] Kexin Qiao, Junjie Cheng, and Changhai Ou. A new mixture differential cryptanalysis on round-reduced AES. *Mathematics*, 10(24):4736, 2022.

[42] Mohsen Shakiba, Mohammad Dakhilalian, and Hamid Mala. On computational complexity of impossible differential cryptanalysis. *Inf. Process. Lett.*, 114(5):252–255, 2014.

[43] Eli Biham and Nathan Keller. Cryptanalysis of reduced variants of Rijndael. *unpublished manuscript, 1999*, 1999.

[44] Christina Boura, Virginie Lallemand, María Naya-Plasencia, and Valentin Suder. Making the impossible possible. *J. Cryptol.*, 31(1):101–133, 2018.

[45] Zilong Jiang, Chenhui Jin, and Zebin Wang. Multiple impossible differentials attack on AES-192. *IEEE Access*, 7:138011–138017, 2019.

[46] Yiyuan Luo and Xuejia Lai. Improvements for finding impossible differentials of block cipher structures. *Secur. Commun. Networks*, 2017:5980251:1–5980251:9, 2017.

[47] Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi. Improved impossible differential cryptanalysis of 7-round AES-128. In Guang Gong and Kishan Chand Gupta, editors, *Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings*, volume 6498 of *Lecture Notes in Computer Science*, pages 282–291. Springer, 2010.

[48] Meiling Zhang, Weiguo Zhang, Jingmei Liu, and Xinmei Wang. General impossible differential attack on 7-round AES. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 93-A(1):327–330, 2010.

[49] Lorenzo Grassi, Christian Rechberger, and Sondre Rønjom. A new structural-differential property of 5-round AES. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, volume 10211 of *Lecture Notes in Computer Science*, pages 289–317, 2017.

[50] Hamid Mala, Mohsen Shakiba, Mohammad Dakhilalian, and Ghadamali Bagherikaram. New results on impossible differential cryptanalysis of reduced-round camellia-128. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography, 16th Annual International Workshop, SAC 2009, Calgary, Alberta, Canada, August 13-14, 2009, Revised Selected Papers*, volume 5867 of *Lecture Notes in Computer Science*, pages 281–294. Springer, 2009.

ORHUN KARA received the M.S. and the Ph.D. degrees in Mathematics from Bilkent University Ankara in 1998 and 2003 respectively. His thesis is about code construction on modular curves. His research interests include the design and analysis of symmetric ciphers.

He was a Visiting Researcher with the CNRS (Centre National de la Recherche Scientifique) in Luminy/Marseille, France from 2001 to 20002 and was a Researcher with the National Research Institute of Electronics and Cryptology (UEKAE) of TÜBİTAK BİLGEM from 2002 to 2020. He has been an Associative Professor with the Department of Mathematics in Izmir Institute of Technology (IZTECH) since 2020. In addition, he maintains an affiliation with TÜBİTAK BİLGEM UEKAE.