MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

# "AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

# TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

1-SON 1(5)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

# O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

## MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI FARG‘ONA FILIALI

**Muassis:** Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
**Chop etish tili:** O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

**Учредитель:** Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
**Язык издания:** узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

**Founder:** Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
**Language of publication:** Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

**2024 yil, Tom 1, №1**
**Vol.1, Iss.1, 2024 y**

**ELEKTRON ILMIY JURNALI** **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz



**FARG’ONA - 2024 YIL**

**Jurnal quyidagi bazalarda indekslanadi:**

Google Scholar · zenodo · ORCID · CYBERLENINKA · WORLD of JOURNALS · Directory of Research Journals Indexing

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

## MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

# Linear cryptanalysis of the SM4 block cipher algorithm

**Liu Lingyun,**
**Ph.D. student of the National University of Uzbekistan,**
**Jining Normal University,**
**Shenyu International Community, Jining District,**
**Ulanqab, Inner Mongolia, China**

**Abstract:** In this paper, the Chinese block cipher algorithm SM4 is evaluated as a linear cryptanalysis method. As a result of the analysis, it was found that $2^{126.4}$ plaintext and ciphertext pairs and $2^{121.7}$ time complexity are required for 23 rounds of the SM4 algorithm for linear cryptanalysis. And to implement the round 23 attack by the multidimensional linear cryptanalysis required $N = 2^{122.3}$ plaintext and ciphertext pairs. The time complexity is equivalent to $2^{122.5}$

**Keywords:** cryptographic, linear attack, differential attack, multidimensional linear attack, approximations, XOR, Branching operation, linear transformation, S-box

**Introduction.** SM4 has garnered significant attention within the cryptographic community, leading to the production of various cryptanalytic findings. In [2], rectangle and boomerang attacks on 18-round SM4, as well as linear and differential attacks on 22-round SM4, were presented. Etrog and Robshaw introduced an attack on 23-round SM4 utilizing multiple linear attacks in [5]. Additionally, [4, 7] introduced the concept of differential attacks and multiple linear attacks on 22-round SM4. Up to the present, the most effective differential attack for 23-round SM4 is outlined in [6]. Cho and Nyberg proposed a multidimensional linear attack on 23-round SM4 in [9]. The optimal linear attack on 23-round SM4 is detailed by Liu and Chen in [8]. Bai and Wu put forth a novel lookup-table-based white-box implementation for SM4, designed to safeguard large linear encodings from cancellation, as described in [11]. Furthermore, [10] provides insights into related-key differential attacks on SM4, while [13] analyzes the lower bound of the number of linearly active S-boxes for SMS4-like ciphers.

Linear cryptanalysis [12] stands out as a crucial technique in the examination of symmetric-key cryptographic primitives. This method primarily focuses on establishing linear approximations among plaintext, ciphertext, and the key. When a cipher exhibits non-random permutation behavior under linear cryptanalysis, it becomes possible to construct a distinguisher or even initiate a key recovery attack by incorporating additional rounds. The process involves making educated guesses for the subkeys of appended rounds, decrypting ciphertexts and/or encrypting plaintexts using these subkeys to calculate the intermediate state at the ends of the distinguisher. If the subkeys are accurately guessed, the distinguisher should be valid; otherwise, it will fail. Linear cryptanalysis has been employed in the analysis of various ciphers, including those detailed in [14–17].

**Main part.** Regarding the efficacy across all previous SM4 attacks in terms of the number of rounds, the most effective key recovery methods are linear cryptanalysis and differential cryptanalysis. Both approaches rely on 19-round distinguishers. Our primary motivation is to enhance the attacks on SM4 by seeking a superior distinguisher. Consequently, our focus centers on exploring linear approximations for SM4. The contributions of this paper can be outlined as follows.

The most effective previous linear attacks have focused on 19-round linear approximations. In response, we introduce a novel search algorithm specifically designed for iterative linear approximations over a small number of rounds in SM4. This involves systematically expanding the partial linear approximation table of the S-box. Initially, it is demonstrated that there are no one-round or two-round iterative linear approximations for SM4. Subsequently,

certain properties are derived for the iterative linear approximations of 3-round SM4. Leveraging these properties, our search algorithm is applied to obtain a 19-round linear approximation with a bias of $2^{-57,3}$ and a 20-round linear approximation with a bias of $2^{-60,5}$. A comparison of our identified linear approximations with previous ones is presented in Table 1. Notably, our linear approximations emerge as the most effective to date.

*Table 1. Overview of Linear Approximations for SM4.*

| **Reference** | **Bias (probability)** | **Rounds** |
|---|---|---|
| [8] | $2^{-62,27}$ | 19 |
| [27] | $2^{-58}$ | 19 |
| [27] | $2^{-61}$ | 20 |
| this work | $2^{-57,3}$ | 19 |
| this work | $2^{-60,5}$ | 20 |

The most effective prior attacks have demonstrated efficacy up to 23 rounds for SM4. Leveraging our identified 20-round linear approximation for SM4, we introduce a key recovery attack targeting 24-round SM4, which currently stands as the most potent attack based on the number of rounds for SM4. Additionally, we employ the newly established 19-round linear approximation to launch an attack on 23-round SM4, thereby enhancing the effectiveness of the best previous linear attack on 23-round SM4. An overview of our attacks and those previously conducted on SM4 is provided in Table 2.

*Table 2. Overview of Attacks on SMS4*

| **Type of cryptanalysis methods** | **Number of rounds** | **Time (T)** | **Data (D)** | **Reference** |
|---|---|---|---|---|
| Rectangle | *16* | $2^{116}$ | $2^{125}$ | *[26]* |
| Rectangle | *14* | $2^{87.69}$ | $2^{107.89}$ | *[13]* |
| Rectangle | *18* | $2^{112.83}$ | $2^{124}$ | *[2]* |
| Integral | *13* | $2^{114}$ | $2^{16}$ | *[7]* |
| Impossible Differential | *16* | $2^{96.07}$ | $2^{117.06}$ | *[13]* |
| Boomerang | *18* | $2^{116.83}$ | $2^{120}$ | *[2]* |
| Differential | *21* | $2^{126.6}$ | $2^{118}$ | *[26]* |
| Differential | *23* | $2^{126.7}$ | $2^{118}$ | *[6]* |
| Differential | *22* | $2^{125.71}$ | $2^{118}$ | *[2]* |
| Differential | *22* | $2^{112.3}$ | $2^{117}$ | *[4]* |
| Linear | *22* | $2^{117}$ | $2^{118.4}$ | *[5]* |
| Linear | *22* | $2^{109.86}$ | $2^{117}$ | *[2]* |
| Linear | *23* | $2^{122}$ | $2^{126.54}$ | *[8]* |
| Multiple Linear | *22* | $2^{119.75}$ | $2^{112}$ | *[18]* |
| Multidimensional Linear | *23* | $2^{127.4}$ | $2^{126.6}$ | *[9]* |
| Multidimensional Linear | *23* | $2^{122.7}$ | $2^{122.6}$ | *[8]* |
| Linear | *23* | $2^{121.7}$ | $2^{126.4}$ | *this work* |
| Multidimensional Linear | *23* | $2^{122.5}$ | $2^{122.3}$ | *this work* |

*Approximations of SM4*

All the previous attacks on SM4 are effective in terms of the number of rounds. Among the top key recovery attacks for SM4 are linear and differential cryptanalysis, both relying on 19-round distinguishers. Our primary motivation for enhancing SM4 attacks is to explore the possibility of obtaining a superior distinguisher. Therefore, the critical aspect is the search for the linear approximation of SM4. Various methods for finding linear approximations of SM4 have been explored in existing literature, including references [2, 5, 8, 18].

The approach outlined in [2] involves creating linear approximations for a reduced-round SM4. This is achieved by identifying a one-round linear approximation with identical input and output masks for the $T$ function. This minimizes the number of active $T$ functions. Consequently, an 18-round linear approximation with a bias of $2^{-57.28}$ for SM4 has been successfully identified.

In [5], Etrog and Robshaw developed a 5-round iterative linear approximation, with only the last two rounds exhibiting activity. Subsequently, they combined three of these five-round iterative linear approximations to formulate an 18-round linear approximation with a bias of $2^{-56.2}$.

In [18], Liu et al. applied the branch-and-bound algorithm from [20] to acquire a set of 5-round iterative linear approximations. These approximations were then employed to build an 18-round linear approximation with a bias of $2^{-56.14}$.

To enhance the linear approximation for SM4, Liu and Chen introduced a more specialized search algorithm in [8]. Initially, they employed a Mixed Integer Linear Programming (MILP)-based method to identify the configuration for the linear approximation with the minimum number of active S-boxes in reduced-round SM4. Subsequently, using the identified configuration, they derived a 19-round linear approximation with a bias of $2^{-62.27}$.

Clearly, minimizing the number of active S-boxes in a linear approximation doesn't guarantee that its bias will be maximized. Therefore, our emphasis is on searching for superior linear approximations, even if they involve a slightly higher number of active S-boxes.

During CT-RSA 2014, Biryukov and Velichkov expanded the branch-and-bound algorithm to explore the differential characteristics of ARX ciphers, incorporating the use of a partial differential distribution table for modular addition to enhance search efficiency [20]. Drawing inspiration from this concept, we intend to leverage the partial linear approximation table in our quest to discover linear approximations for SM4.

**Methodology.** Initially, we will introduce some properties related to fundamental operations like the XOR operation, the three-forked branching operation, and the linear map.

Biham highlighted that, akin to differential cryptanalysis [28], it is possible to define characteristics in linear cryptanalysis [23]. Subsequently, one can derive the linear approximations of a cipher by combining characteristics from each round. However, there are crucial distinctions in the concatenation rule:

Operation XOR: If $x = y \oplus z$, $\Gamma_x$, $\Gamma_y$ and $\Gamma_z$ are the masks of $x$, $y$ and $z$, respectively. Then $\Gamma_x = \Gamma_y = \Gamma_z$.

Branching operation: If $x = y = z$, $\Gamma_x$, $\Gamma_y$ and $\Gamma_z$ are the masks of $x$, $y$ and $z$, respectively. Then $\Gamma_x = \Gamma_y \oplus \Gamma_z$.

$L$ linear transformation: If $y = L(x)$, $\Gamma_x$ and $\Gamma_y$ are the masks of $x$ and $y$, respectively. Then $\Gamma_x = L^t(\Gamma_y)$ where $L^t$ is the transpose of $L$.

Using these guidelines, discovering a linear approximation is akin to finding a differential trail. The remaining challenge is to devise a strategy for finding the longest possible linear approximation. In this subsection, we introduce a novel approach to explore the linear approximations of SMS4. Our method aims to identify linear approximations with minimal active S-boxes, resulting in non-iterative ones that differ from those presented in [4, 11, 16, 18]. A representation of the 3-round linear approximation for the SM4 algorithm is shown in Figure 1. We employ a two-step procedure to accomplish this objective.

In the first step, our objective is to establish the minimum number of active S-boxes in the linear approximation and determine the positions of the active rounds. Following the approach suggested by Mouha et al. in [23], this can be accomplished using Mixed-Integer Linear Programming (MILP). In the context of linear cryptanalysis, Mouha et al. initially formulated equations that incorporated additional binary dummy variables for all branching operations and linear transformations in the cipher. Subsequently, they inputted these equations into a MILP solver for resolution. For instance, if the masks of a branching operation are represented by $\Gamma_x$, $\Gamma_y$, $\Gamma_z$and the binary dummy variable is denoted as $D_1$, the equations for this particular branching operation are as follows:

$$\xi(\Gamma_x) + \xi(\Gamma_y) + \xi(\Gamma_z) \geq 2D_1, \qquad D_1 \geq \xi(\Gamma_x), D_1 \geq \xi(\Gamma_y), D_1 \geq \xi(\Gamma_z)$$

Likewise, if the input and output byte-masks of a linear transformation are denoted as $\Gamma_{in1}, \Gamma_{in2}, \Gamma_{in3}, \Gamma_{in4}, \Gamma_{out1}, \Gamma_{out2}, \Gamma_{out3}, \Gamma_{out4}$ and the binary dummy variable is $D_2$, the equations are as follows:

$$\xi(\Gamma_{in1}) \oplus \xi(\Gamma_{in2}) \oplus \xi(\Gamma_{in3}) \oplus \xi(\Gamma_{in4}) \oplus \xi(\Gamma_{out1}) \oplus \xi(\Gamma_{out2}) \oplus \xi(\Gamma_{out3}) \oplus \xi(\Gamma_{out4}) \geq \boldsymbol{q} * D_2$$

$$D_2 \geq \xi(\Gamma_{in1})$$
$$D_2 \geq \xi(\Gamma_{in2})$$
$$D_2 \geq \xi(\Gamma_{in3})$$
$$D_2 \geq \xi(\Gamma_{in4})$$
$$D_2 \geq \xi(\Gamma_{out1})$$
$$D_2 \geq \xi(\Gamma_{out2})$$
$$D_2 \geq \xi(\Gamma_{out3})$$
$$D_2 \geq \xi(\Gamma_{out4})$$

Here, **q** represents the linear branch number, and for SMS4, **q** is equal to **5**.

Utilizing this approach, we formulate the MILP for SMS4 and apply it to the solver implemented in SAGE. Given that the best previous linear approximation involves 18 rounds, we aim to discover a linear approximation extending to 19 rounds. The solver provides a 19-round linear approximation with one active S-box in the 1st, 4th, 5th, 8th, 9th, 12th, 13th, 16th, and 17th rounds, respectively. It's important to note that what we obtain is solely a lower bound for the number of S-boxes, and it might be impossible to find such a linear approximation due to the limitations of degrees of freedom.

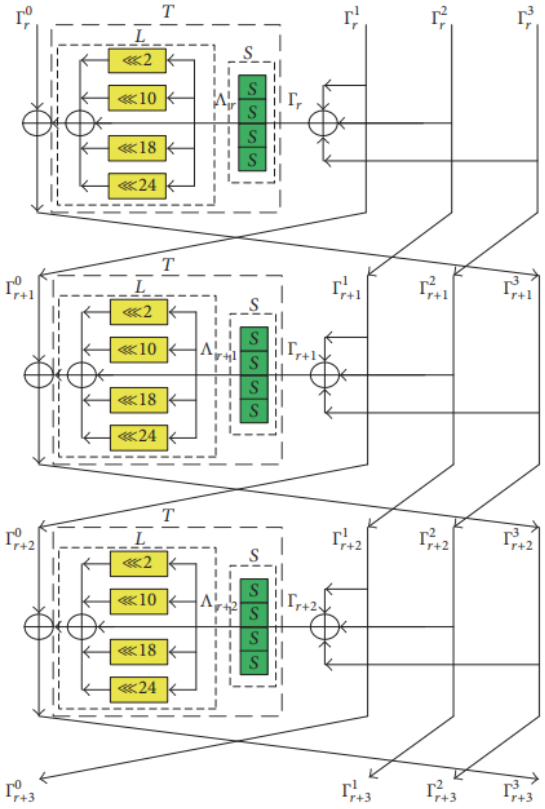


Fig. 1. Linear approximation of 3-round SM4.

To address this, we opt to fix the positions of the active rounds and increment the number of active S-boxes until a valid linear approximation is identified. Our observation suggests that a linear approximation is likely valid when the number of active S-boxes in each active round is two. In other words, the linear approximation we are attempting to discover has the following form:

$$2-0-0-2-2-0-0-2-2-0$$
$$-0-2-2-0-0-2-2$$
$$-0-0$$

*Theorem 1*. To construct the aforementioned 19-round linear approximation, it is necessary for the input masks of the T functions in two consecutive active rounds to be identical.

*Proof*. Let $\Gamma_{in}^{i}$and $\Gamma_{in}^{i}$ $(i = 1,\cdots,6)$ represent the input and output masks of the $T$ functions in the six-round linear approximation with the pattern $0-0-2-2-0-0$. Then $\Gamma_{in}^{3} \oplus \Gamma_{out}^{1} \oplus \Gamma_{in}^{2} = \Gamma_{in}^{4} \oplus \Gamma_{out}^{5}, \Gamma_{in}^{4} \oplus \Gamma_{out}^{6} \oplus \Gamma_{in}^{5} = \Gamma_{in}^{3} \oplus \Gamma_{out}^{2}$. Since $\Gamma_{in}^{j} = \Gamma_{out}^{j} = 0$ for $j = 1,2,5,6$. As a result $\Gamma_{in}^{3} = \Gamma_{in}^{4}$. *Theorem 1 is proved.*

**Results.** When extending backward to 19 rounds, it is established that the number of active S-boxes in the first round is 2. Given that for each S-box, there are 5 linear masks resulting in the highest bias, a total of 200 19-round linear approximations with the same bias can be identified. One such linear approximation is presented in Table 2. In this table, the fourth and fifth columns represent the output and input masks of the S-box layer, respectively, while the sixth column indicates the bias of the round. The remaining columns provide the masks of the intermediate values. Referring to [11], it is observed that the piling-up lemma [20] works effectively for SM4, resulting in a bias of approximately $2^{-57,3}$ for 19-round and $2^{-60,5}$ for 20-round for the linear approximation in Table 3.

Table 3. One of the 20-round Linear Approximations

| Round | $i$ | $X_i$ | $S_{out}$ | $S_{in}$ | Bias ($p$) | $X_{i+1}$ | $X_{i+2}$ | $X_{i+3}$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0x88086828 | 0x00008200 | 0x0000$CA$00 | $2^{-4}$ | 0x8808$A$228 | 0x88086828 | 0x8808$A$228 |
| 2 | 1 | 0 | 0 | 0 | - | 0 | 0x00006000 | 0x0000$AA$00 |
| 3 | 2 | 0 | 0 | 0 | - | 0x0000$AA$00 | 0x00006000 | 0 |
| 4 | 3 | 0x8808$A$228 | 0x0000$AA$00 | 0x00006000 | $2^{-4}$ | 0x8808$C$228 | 0 | 0 |
| 5 | 4 | 0x88080828 | 0x0000$A$A00 | 0x00008000 | $2^{-4}$ | 0x8808$A$228 | 0x88086828 | 0x88080828 |
| ... | | | | | | | | |
| 19 | 18 | 0x8808$A$228 | 0x0000$AA$00 | 0x0000$CA$00 | $2^{-4}$ | 0x 88086828 | 0x8808$C$228 | 0x8808$A$228 |
| 20 | 19 | 8808$A$228 | 0x00008200 | 0x0000$AA$00 | $2^{-4}$ | 0x 88080828 | 0x88086828 | 0x8808$A$228 |

To carry out the attack using these approximations, we need $N = 2^{126.4}$ plaintext and ciphertext pairs.

**Conclusion.** The time complexity of Step 3 is approximately $2^{126.4}$, which is equivalent to $2^{121.7}$, 23-round encryptions and is also the dominating complexity of the attack. The time complexity of Step 5 is about $2^{112}$, 4-round encryptions. In Step 6, e is calculated using the technique from [7], requiring the execution of 3 Fast Fourier Transformations; the complexity is $3 \times 2^{112} \times 2^{112} \approx 2^{120.4}$ arithmetic operations. The time complexity of Step 7 is $2^{120}$ encryptions. The memory complexity is approximately $(126.4 \times 2^{112} \times 2^{112})/8 \approx 2^{116}$ bytes, which is necessary to store t and the first column of M.

And to implement the round 23 attack by the multidimensional extension as presented in [27], we need $N = 2^{122.3}$ plaintext and ciphertext pairs. The time complexity is equivalent to $2^{122.5}$

## References

1. W. Diffie and G. Ledin, “SMS4 Encryption Algorithm for Wireless Networks,” Cryptology ePrint Archive 2008/329, 2014, http://eprint.iacr.org/2008/329.pdf.

2. T. Kim, J. Kim, S. Hong, and J. Sung, “Linear and Differential Cryptanalysis of Reduced SMS4 Block Cipher,” IACR Cryptology ePrint Archive 2008/281, 2008, https://eprint.iacr.org/2008/2811.pdf.

3. “Office of State Commercial Cryptography Administration: Specification of SMS4, block cipher for WLAN products-SMS4” (Chinese), http://www.oscca.gov.cn/UpFile/200621016423197990.pdf.

4. W. Zhang, W. Wu, D. Feng, and B. Su, “Some New Observations on the SMS4 Block Cipher in the Chinese WAPI Standard,” in Information Security Practice and Experience, vol. 5451 of Lecture Notes in Computer Science, pp. 324–335, Springer, Berlin, Germany, 2009.

5. J. Etrog and M. J. B. Robshaw, “The Cryptanalysis of ReducedRound SMS4,” in Selected Areas in Cryptography, vol. 5381 of Lecture Notes in Computer Science, pp. 51–65, Springer, Berlin, Germany, 2008.

6. B.-Z. Su, W.-L. Wu, and W.-T. Zhang, “Security of the SMS4 block cipher against differential cryptanalysis,” Journal of Computer Science and Technology, vol. 26, no. 1, pp. 130–138, 2011.

7. F. Liu, W. Ji, L. Hu et al., “Analysis of the SMS4 Block Cipher,” in Information Security and Privacy, vol. 4586 of Lecture Notes in Computer Science, pp. 158–170, Springer, Berlin, Germany, 2007.

8. M.-J. Liu and J.-Z. Chen, “Improved linear attacks on the Chinese block cipher standard,” Journal of Computer Science and Technology, vol. 29, no. 6, pp. 1123–1133, 2014.

9. J. Cho and K. Nyberg, “Improved Linear Cryptanalysis of SMS4 Block Cipher,” Symmetric Key Encryption Workshop, pp. 1–14, 2011.

10. J. Zhang, W. Wu, and Y. Zheng, “Security of SM4 Against (Related-Key) Differential Cryptanalysis,” in Proceedings of the International Conference on Information Security Practice and Experience, vol. 10060 of Lecture Notes in Computer Science, pp. 65–78, Springer, Berlin, Germany, November 2016.K.

11. Bai and C. Wu, “A secure white-box SM4 implementation,” Security and Communication Networks, vol. 9, no. 10, pp. 996– 1006, 2016.

12. T. Helleseth, “Linear cryptanalysis method for des cipher,” in Advances in Cryptology—EUROCRYPT, vol. 765 of Lecture Notes in Computer Science, pp. 386–397, Springer, Berlin, Germany, 1993.

13. B. Zhang and C. Jin, “Practical security against linear cryptanalysis for SMS4-like ciphers with

SP round function,” Science China Information Sciences, vol. 55, no. 9, pp. 2161–2170, 2012.

14. G. Jakimoski and L. Kocarev, “Differential and linear probabilities of a block-encryption cipher,” IEEE Transactions on Circuits and Systems. I. Fundamental Theory and Applications, vol. 50, no. 1, pp. 121–123, 2003. 10 Security and Communication Networks

15. F. Sano, K. Ohkuma, H. Shimizu, and S. Kawamura, “On the security of nested SPN cipher against the differential and linear cryptanalysis,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E86- A, no. 1, pp. 37–46, 2003.

16. Y. Liu, K. Fu, W. Wang, L. Sun, and M. Wang, “Linear cryptanalysis of reduced-round SPECK,” Information Processing Letters, vol. 116, no. 3, pp. 259–266, 2016.

17. Y. Sun, “Linear Cryptanalysis of Light-Weight Block Cipher ICEBERG,” in Advances in Electronic Commerce, Web Application and Communication, vol. 149, pp. 529–532, Springer Berlin Heidelberg, Berlin, Germany, 2012.

18. Z. Liu, D. Gu, and J. Zhang, “Multiple linear cryptanalysis of reduced-round SMS4 block cipher,” Chinese Journal of Electronics, vol. 19, no. 3, pp. 389–393, 2010.

19. D. Toz and O. Dunkelman, “Analysis of two attacks on reducedround versions of the SMS4,” in Information and Communications Security, vol. 5308 of Lecture Notes in Computer Science, pp. 141–156, Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

20. Biryukov and V. Velichkov, “Automatic search for differential trails in ARX ciphers,” in Topics in Cryptology—CT-RSA 2014, vol. 8366 of Lecture Notes in Comput. Sci., pp. 227–250, Springer, Berlin, Germany, 2014.

21. M. Matsui, “On correlation between the order of *S*-boxes and the strength of DES,” in Advances in cryptology—EUROCRYPT, vol. 950 of Lecture Notes in Comput. Sci., pp. 366–375, Springer, Berlin, Germany, 1994.

22. J. Daemen, R. Govaerts, and J. Vandewalle, “Correlation matrices,” in Fast Software Encryption, vol. 1008 of Lecture Notes in Computer Science, pp. 275–285, Springer, Berlin, Germany, 1994.

23. E. Biham, “On Matsui’s linear cryptanalysis,” in Advances in Cryptology, vol. 950 of Lecture Notes in Comput. Sci., pp. 341– 355, Springer, Berlin, Germany, 1994.

24. Bogdanov and E. Tischhauser, “On theWrong Key Randomisation and Key Equivalence Hypotheses in Matsui’s Algorithm 2,” in Fast Software Encryption, vol. 8424 of Lecture Notes in Computer Science, pp. 19–38, Springer, Berlin, Germany, 2013.

25. N. Ferguson, J. Kelsey, S. Lucks et al., “Improved Cryptanalysis of Rijndael,” in Fast Software Encryption, vol. 1978 of Lecture Notes in Computer Science, pp. 213–230, Springer, Berlin, Germany, 2000.

26. Zhang, L., Zhang, W., Wu, W.: Cryptanalysis of Reduced-Round SMS4 Block Cipher. In: Mu, Y., Susilo, W., Seberry, J. (eds.) ACISP 2008. Lecture Notes in Computer Science, vol. 5107, pp. 216–229. Springer (2008)

27. Liu, Yu et al. “New Linear Cryptanalysis of Chinese Commercial Block Cipher Standard SM4.” Secur. Commun. Networks 2017 (2017): 1461520:1-1461520:10.

28. Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) Advances in Cryptology - CRYPTO ’90. Lecture Notes in Computer Science, vol. 537, pp. 2–21. Springer (1991)