MILP-aided Cryptanalysis of Round Reduced ChaCha

Najwa Aaraj, Florian Caullery and Marc Manzano

DarkMatter, UAE

Abstract

The inclusion of ChaCha20 and Poly1305 into the list of supported ciphers in TLS 1.3 necessitates a security evaluation of those ciphers with all the state-of-the-art tools and innovative cryptanalysis methodologies. Mixed Integer Linear Programming (MILP) has been successfully applied to find more accurate characteristics of several ciphers such as SIMON and SPECK. In our research, we use MILP-aided cryptanalysis to search for differential characteristics, linear approximations and integral properties of ChaCha. We are able to find differential trails up to 2 rounds and linear trails up to 1 round. However, no integral distinguisher has been found, even for 1 round.

1 Introduction

Salsa [1] is a 256-bit stream cipher introduced by Bernstein in 2005. Salsa was proposed with the aim of being considerably faster than AES and easier to be securely implemented. It was designed as a chain of three simple operations on 32-bit words: modular addition, exclusive-or (XOR) and rotation. These operations constitute the well-known term ARX (i.e., Addition, Rotation and XOR). Salsa came in 3 flavors: Salsa20, Salsa12 and Salsa8, of 20, 12 and 8 rounds respectively.

Later on, Bernstein introduced ChaCha [2], a 256-bit stream cipher based on Salsa, which was specifically designed to improve the amount of diffusion per round, thus increasing resistance to cryptanalysis, while preserving and even improving the performance of Salsa. RFC 1654 provides further details regarding implementation and security considerations [3].

Recently, ChaCha has received renewed attention as the standardization process for inclusion of cipher suites based on ChaCha20-Poly1305 AEAD (i.e., ChaCha20 for symmetric encryption and Poly1305 for authentication) in TLS 1.3 has nearly concluded [4].

ChaCha has withstand several thorough security analysis. However, to the best of our knowledge, there is no attack on ChaCha searching for differential and linear trails. Similarly, there is no attack focusing on finding integral distinguishers either. Therefore, this work focuses on filling this gap of the literature and providing the scientific community with a broader knowledge of the security properties of ChaCha.

To carry out our study, we use MILP techniques which have gained popularity among the cryptology collective due to the fact that:

{najwa.aaraj,florian.caullery,marcos.manzano}@darkmatter.ae

This paper was presented at the NIK-2017 conference; see http://www.nik.no/.

a) it reduces the workload of designers as well as cryptanalysts because the task involves writing out equation systems over the reals representing Boolean equation systems, formulating an MILP optimization problem and finally providing it as an input into an MILP solver.

b) not much programming is required thus decreasing the time spent on cryptanalysis and reducing the possibility of human errors.

c) provides a higher performance than traditional methods when the problem has been properly formulated.

Organization of the paper

We give an overview of the previous attacks on ChaCha in Section 2. In Section 3, we describe what MILP is and present preceding studies which have used such techniques as a cryptanalysis tool. Then, the attacks searching for differential characteristics, linear approximations and integral properties are presented in Sections 4, 5 and 6, respectively. Finally, we conclude this paper in Section 7 stating our future directions.

2 Related Work

The most important cryptanalysis work focusing on ChaCha was proposed by Aumasson et al. at FSE 2008 [5] with the introduction of probabilistic neutral bits. It allowed him to break up to 7 rounds with an attack complexity of 2^{248}.

Then, several years later, Maitra improved the attack from Aumasson by exploiting addition probabilistic neural bits, decreasing the complexity down to 2^{243} [6]. In addition, he described how to properly chose IVs to even further decrease the complexity of the attack to 2^{239}.

Choudhuri et al. [7] considered multi-bit differentials as extension of suitable single-bit differentials with linear approximations, which is a differential-linear attack, to show how to theoretically choose a combination of output bits to obtain significantly improved biases. Then, they used the theoretical results to do a limited search over the input differences, and they obtained the best possible biases known so far for 4, 4.5 and 5 rounds of ChaCha. Finally, the work from Choudhuri concluded that 12 rounds of ChaCha should be considered sufficient for 256-bit keys under the current best known attack models [8].

3 Mixed Integer Linear Programming

A programming problem is a mathematical optimization which aims to achieve the minimal or maximal value of an objective function under certain constraints. In an integer programming problem the variables involved are restricted to be integers. Moreover, in a linear programming problem the objective function and constraints are linear. Mixed integer linear programming (i.e., MILP) covers problems in which only some of the variables are restricted to be integers while the rest are allowed to be non-integers. It has found a wide range of applications in industry as well as in academia, but its application to cryptography has been kept rather limited. Next, we show an example of a MILP problem:

$$
\begin{aligned}
\text{minimize} \quad & 8x + y \\
\text{subject to} \quad & x + 2y \geq -14 \\
& -4x - y \leq -33 \\
& 2x + y \leq 20 \\
& x \in \mathbb{R} \\
& y \in \mathbb{Z}
\end{aligned}
$$

where the optimal solution would be $(x, y) = (6.5, 7)$.

There exists a broad variety of optimization tools such as CPLEX [9] or Gurobi [10]. In this paper we use Gurobi to carry out our study. The above example, in Gurobi syntax would be as follows:

```
Minimize
8 x + y

Subject To
x + 2 y \>= - 14
- 4 x - y \<= - 33
2 x + y \<= 20
INTEGER
y
END
```

MILP and Cryptanalysis

Table 1: MILP-aided cryptanalysis previous studies

Reference	Cryptanalysis Property	Primitives under study
[11]	Algebraic	Bivium
[12]	Differential and linear	Unbalanced Feistel networks
[13]	Differential	SIMD
[14]	Differential and linear	Enocoro-128v2 and AES
[15]	Differential and linear	SIMON, PRESENT, Serpent, LBlock, and DESL
[16]	Integral	HIGHT, LEA, TEA, XTEA, KATAN and KTANTAN
[17]	Differential and linear	Speck
[18]	Integral	Midori64, LED, Joltik-BC, AES, Serpent, Noekeon, SPONGENT and PHOTON
[19]	Integral	SIMON, SIMECK, PRESENT, RECTANGLE, LBlock and TWINE

In recent years, MILP has attracted the attention of the cryptographic community as a cryptanalysis technique. In [11], Borghoff et al. transformed the quadratic equations describing the stream cipher Bivium into a MILP problem. Bogdanov calculated the minimum number of active S-boxes of unbalanced Feistel networks focusing on linear

and differential properties [12]. Later on, Bouillaguet et al. used MILP to find differential characeristics of the SIMD hash function [13]. Mouha et al. proposed new security bounds for the stream cipher Enocoro-128v2 carrying out differential and linear cryptanalysis using MILP [14].

In [15] Sun et al. used MILP to propose an automatic method for finding high probability differential and linear characteristics of block ciphers. Furthermore, ARX ciphers have also been analyzed focusing on integral properties [16] as well as on differential and linear trails [17]. Several word-oriented block ciphers were analyzed in [18] with the particularity that they had non-bit-permutation linear layers.

Finally the authors of [19] searched for integral distinguishers of 6 lightweight block ciphers. Moreover, they proposed a technique to check if a given cipher, at a given round has an integral distinguisher.

Table 1 summarizes the aforementioned previous works.

4 Differential Attack

The differential attack was introduced by Biham and Shamir in [20] and is now one of the most classical attacks on modern block ciphers. Resistance to this attack is the first requirement during the design of new cryptographic primitives. We refer to [21] for an introduction to differential cryptanalysis. Note that by differentials, we mean *XOR Difference* which is equivalent to flipping one or several bits of the state. In this work we do not consider the *Additive Difference* which consists in performing the modular addition of a word and a given difference.

Using the equations describing the differential properties of the XOR and modular addition given by Kai et al. in [17], we construct a model for the propagation of differentials in ChaCha at bit-level. Every modular addition of 2 32-bit words is modeled by 408 equations and every XOR by 160 equations for a total of 2272 equations per quarter-round and 18176 equations per round. As a consequence, the significant amount of variables and equations involved in the model makes it poorly scalable when focusing on bit-level. In our case, with this model we can only find trails for 1 round in a reasonable time.

To bypass the aforementioned problem, we remark that one can first model the differential properties of ChaCha at word level. Every quarter-round of ChaCha is acting on 4 32-bit words, then the words are mixed with a linear transformation. Hence, we see the first 4 quarter-rounds of ChaCha as 4 independent S-Boxes followed by a linear layer as presented in Fig. 1.

The next step of the strategy is to translate the S-Boxes into a system of linear inequalities suitable for MILP. We employ the method of [22] hereunder:

1. Find the possible and impossible differential patterns of the S-Boxes / quarter-rounds.
2. Use Sage (see [23]) to obtain the inequalities describing the convex hull of all possible differentials.
3. Use Algorithm 1 of [22] to reduce the number of inequalities needed to describe the convex hull.

We say that a differential word is active if at least one of its 32 bits is active. The first step of the strategy requires us to find all the differential patterns of the S-Boxes. This is

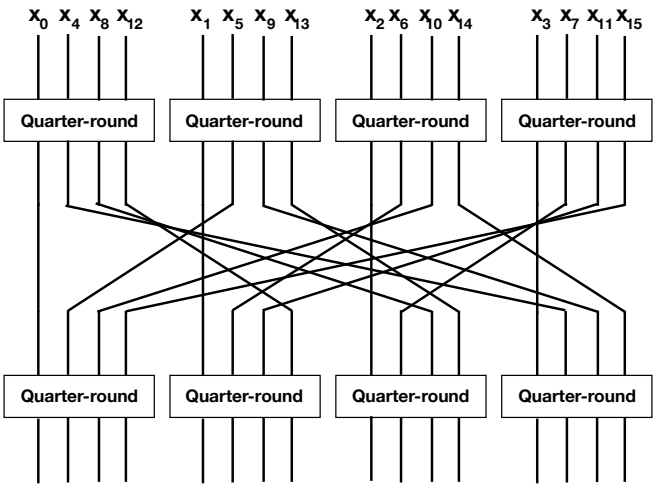

Figure 1: ChaCha's permutation represented as 4 independent S-Boxes followed by a linear layer.

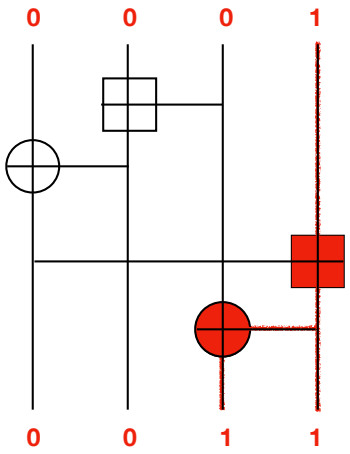

Figure 2: Half-quarter round of ChaCha with a possible trail.

tricky and error prone as there is no way to automatize it. Now, observe that the rotation operates within a word. If a word is active, then its rotation too. Hence, the rotations are not affecting the differentials at word level. Consequently, we can split a quarter-round into two equal parts as in Fig. 2, which contains one example of possible trail.

It is easy to describe all the possible trails of the above transformation. Then, as a quarter-round is just the series application of two of them, we can easily deduce all the possible differential trails of a quarter-round. Note that we have not taken into account the likelihood of the trails. We leave this as a future work. For our model, we get 16 inequalities describing a quarter-round.

We obtained differential trails at word level for up to 6 rounds of ChaCha. The next stage is to use those trails to force the values of certain variables in our model at bit-level and enable our MILP solver to handle more rounds. Indeed, a differential word taking the value 0 means that the differential for all its bits is equal to 0. On the other hand, a

differential word taking the value 1 has at least one of its bit set to 1. Plugging that into the solver enabled us to find differential trails at bit-level for up to 2 rounds of ChaCha with a probability of 2^{-24} where we could only solve our model for 1 round before this optimization. At the time of the submission, we are still running experiments and hope to solve the problem for more rounds.

5 Linear Attack

Another classical attack against modern ciphers is the linear attack introduced by Matsui in [24]. We again refer to [21] for an introduction to linear cryptanalysis. Our goal here is to find linear masks propagating through several rounds with high probability. We cannot use the method introduced in the previous section (i.e. describing the cipher at word level) because the modular addition has a linear component. Hence, the linear masks are always propagating at word level and the model would be irrelevant. Therefore, we use the equations for the linear propagation through modular addition given in [17] and the equations for the three forked branches given in [14] to construct the system of linear inequalities of ChaCha. Our model has 6672 equations per round and a total of 8705 auxiliary variables. We have been able to find a linear mask propagating through 1 round with probability 2^{-3} and we are still running experiments for higher number of rounds.

6 Integral Attack

Integral cryptanalysis was first proposed by Daemen et al. to evaluate the security of SQUARE [25], and then it was formalized by Knudsen and Wagner [26]. This technique uses a set of chosen plaintexts that contain all possible values for some bits, and has a constant value for other bits. The corresponding ciphertexts are calculated by using the cipher under study. If the XOR of the corresponding ciphertexts always becomes 0, it can be asserted that the cipher has an integral distinguisher.

Several years later, a new technique to find integral distinguishers was proposed at Eurocrypt 2015: the division property [27], a generalization of the integral property. It can effectively construct the integral distinguisher even if the block cipher has non-bijective functions, bit-oriented structures, and low-degree functions. From the point of view of the attackable number of rounds (or chosen plaintexts), the division property can construct better distinguishers than previous methods. For instance, it can reduce the required number of chosen plaintexts for the 10-round distinguisher on Keccak-f from 2^{1025} to 2^{515}. Recently, the cube attack using the division property has been successfully applied to several ciphers in order to perform key-recovery attacks [28].

To solve the scalability issue of [27], the authors of [19] modeled the division property propagations through rounds by linear inequalities, based on which they were able to construct a system of linear inequalities which could accurately describe the division propagation property of a block cipher, given an initial division property. Then, by choosing an appropriate objective function they converted the search algorithm in Todo's framework into an MILP problem.

The division property that focuses at bit-level is called bit-based division property, and was proposed by Todo [29]. In this work, we focus on the feasibility of the bit-based division property.

MILP-aided search of bit-based division property

To search for integral distinguishers based on bit-based division property by using MILP method we need to look for *division trails*. The term division trail is used to illustrate a division property propagation through a given number of rounds. Let f_r denote the round function of a cipher. Assume that the input of n-bits to a given cipher has an initial division property $\mathcal{D}_0^{1^n}$, and denote the division property after i-round propagations through f_r by $\mathcal{D}_i^{1^n}$. Thus, we have the following chain of division property propagations (i.e., a division trail) after r rounds:

$$\mathcal{D}_0^{1^n} \xrightarrow{f_r} \mathcal{D}_1^{1^n} \xrightarrow{f_r} \dots \mathcal{D}_r^{1^n} \tag{1}$$

According to [19], it is sufficient to check the last vectors of all division trails up to round r to estimate whether a distinguisher exists. Therefore, we construct a system of linear inequalities such that all feasible solutions of this system are exactly all the division trails. As a consequence, the constructed system of linear inequalities is sufficient to describe the division property propagations. For a division property propagation, if the resulting vectors for the first time contain all the vectors of Hamming weight one after propagating $r + 1$ rounds, the propagation procedure should terminate and an r-round distinguisher can be obtained.

Using the equations modeling the bit-based division properties of XOR, copy and modular addition given in [16, 19] we are able to construct a system of linear inequalities describing a ChaCha quarter-round. The total number of operations carried out per quarter-round are: 8 copy operations, 4 modular additions and 4 XORs.

It is important to highlight that the rotation operation embedded within the ChaCha quarter-round does not have to be converted into inequalities. It is enough to rotate the variables representing the rotated 32-bit word.

ChaCha's state is composed of 512 bits (i.e., 16 32-bit words). Our system consists of $512 \times ((r \times 2) + 1)$ variables representing the division property propagation, where r is the number of rounds to model. Note that for each round, we need an extra of 512 variables to model the division property propagation after half-quarter-round. Thus, for 1 round we need 1536 variables. In addition, the model necessitates of auxiliary variables required to carry out copy and modular addition operations. For 1 round we need 16800 auxiliary variables. Finally, for 1 round the system of linear inequalities is composed of 15328 inequalities.

To carry out the search for distinguishers, we have to initialize $\mathcal{D}_0^{1^n}$, where n is 512, with a given number of active bits. Therefore, the search consists of finding the appropriate combination of active bits in $\mathcal{D}_0^{1^n}$ that lead to an integral distinguisher at round r.

At the time of writing this work, we have not been able to find an integral distinguisher even for a single round of ChaCha. We have explored the most common strategies found in the literature to initialize $\mathcal{D}_0^{1^n}$, which represents a total of 2^{36} combinations of active bits out of the 2^{512} space. These results, although not being completed, pose hope on the fact that ChaCha is a secure candidate to be used in TLS 1.3.

7 Conclusions and Future Work

In this paper we focus on studying differential characteristics, linear approximations and integral properties of ChaCha. To conduct our research we use MILP techniques, which have recently gained popularity among the cryptology community. Firstly, we present the

study searching for differential trails. We show that we are able to find differential trails for 2 rounds of ChaCha at bit-level, and 6 rounds at word level. Secondly, we present the experiments checking for linear trails. We unveil that we found a linear trail for 1 round of ChaCha. Finally, we describe the analysis carried out searching for integral distinguishers, using the bit-based division property, and we point out that we have not been able to find a distinguisher for even just 1 round of ChaCha. It is important to note that this work is part of an ongoing study, and that therefore, the presented results are the best results found so far, but not definitive. In any case, ChaCha seems to resist the three attacks performed in this paper up to now.

As future work, we would like to carry out the differential attack but focusing on the additive difference, instead that in the XOR difference. Moreover, we would include the probabilities for the differential trails found at word level.

References

[1] Daniel J. Bernstein. "The Salsa20 Family of Stream Ciphers". In: *New Stream Cipher Designs: The eSTREAM Finalists*. 2008, pp. 84–97. URL: http://cr.yp.to/snuffle.

[2] Daniel J. Bernstein. *ChaCha, a variant of Salsa20*. 2008. URL: http://cr.yp.to/chacha.html.

[3] Yoav Nir and Adam Langley. *ChaCha20 and Poly1305 for IETF Protocols*. RFC 7539. 2015. URL: https://tools.ietf.org/html/rfc7539.

[4] Eric Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.3 draft-ietf-tls-tls13-21*. RFC. 2017. URL: https://tools.ietf.org/html/draft-ietf-tls-tls13-21.

[5] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, et al. "New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba". In: *Fast Software Encryption: 15th International Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*. 2008, pp. 470–488.

[6] Subhamoy Maitra. "Chosen IV Cryptanalysis on Reduced Round ChaCha and Salsa". In: *IACR Cryptology ePrint Archive* 2015 (2015), p. 698.

[7] Arka Rai Choudhuri and Subhamoy Maitra. "Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha". In: *IACR Trans. Symmetric Cryptol.* 2016 (2016), pp. 261–287.

[8] Arka Rai Choudhuri and Subhamoy Maitra. "Differential Cryptanalysis of Salsa and ChaCha - An Evaluation with a Hybrid Model". In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 377.

[9] CPLEX. https://www.ibm.com/us-en/marketplace/ibm-ilog-cplex. [Online; accessed 24-August-2017].

[10] Gurobi. http://www.gurobi.com. [Online; accessed 24-August-2017].

[11] Julia Borghoff, Lars R. Knudsen, and Mathias Stolpe. "Bivium as a Mixed-Integer Linear Programming Problem". In: *Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15-17, 2009. Proceedings*. 2009, pp. 133–152.

[12] Andrey Bogdanov. *Analysis and Design of Block Cipher Constructions*. Thesis (Ph.D.) – Ruhr University Bochum. 2009.

[13] Charles Bouillaguet, Pierre-Alain Fouque, and Gaëtan Leurent. "Security Analysis of SIMD". In: *Selected Areas in Cryptography - 17th International Workshop, SAC 2010, Waterloo, Ontario, Canada, August 12-13, 2010, Revised Selected Papers*. 2010, pp. 351–368.

[14] Nicky Mouha, Qingju Wang, Dawu Gu, et al. "Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming". In: *Information Security and Cryptology: 7th International Conference, Inscrypt 2011, Beijing, China, November 30 – December 3, 2011. Revised Selected Papers*. 2012, pp. 57–76.

[15] Siwei Sun, Lei Hu, Meiqin Wang, et al. "Towards Finding the Best Characteristics of Some Bit-oriented Block Ciphers and Automatic Enumeration of (Related-key) Differential and Linear Characteristics with Predefined Properties". In: *IACR Cryptology ePrint Archive* (2014), p. 747.

[16] Ling Sun, Wei Wang, Ru Liu, et al. "MILP-Aided Bit-Based Division Property for ARX-Based Block Cipher". In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 1101.

[17] Kai Fu, Meiqin Wang, Yinghua Guo, et al. "MILP-Based Automatic Search Algorithms for Differential and Linear Trails for Speck". In: *Revised Selected Papers of the 23rd International Conference on Fast Software Encryption - Volume 9783*. FSE 2016. 2016, pp. 268–288.

[18] Ling Sun, Wei Wang, and Meiqin Wang. "MILP-Aided Bit-Based Division Property for Primitives with Non-Bit-Permutation Linear Layers". In: *IACR Cryptology ePrint Archive* 2016 (2016), p. 811.

[19] Zejun Xiang, Wentao Zhang, Zhenzhen Bao, et al. "Applying MILP Method to Searching Integral Distinguishers Based on Division Property for 6 Lightweight Block Ciphers". In: *Advances in Cryptology – ASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*. Ed. by Jung Hee Cheon and Tsuyoshi Takagi. 2016, pp. 648–678.

[20] Eli Biham and Adi Shamir. "Differential Cryptanalysis of DES-like Cryptosystems". In: *Advances in Cryptology-CRYPT0' 90: Proceedings*. 1991, pp. 2–21.

[21] Howard M. Heys. "A Tutorial on Linear and Differential Cryptanalysis". In: *Cryptologia* 26.3 (July 2002), pp. 189–221. ISSN: 0161-1194. DOI: 10.1080/0161-110291890885. URL: http://dx.doi.org/10.1080/0161-110291890885.

[22] Siwei Sun, Lei Hu, Peng Wang, et al. "Automatic Security Evaluation and (Related-key) Differential Characteristic Search: Application to SIMON, PRESENT, LBlock, DES(L) and Other Bit-Oriented Block Ciphers". In: *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*. 2014, pp. 158–178.

[23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.0)*. http://www.sagemath.org. 2017.

[24] Mitsuru Matsui. “Linear cryptanalysis method for DES cipher”. In: *Workshop on the Theory and Application of of Cryptographic Techniques*. 1993, pp. 386–397.

[25] Joan Daemen, Lars Knudsen, and Vincent Rijmen. “The block cipher Square”. In: *Fast Software Encryption: 4th International Workshop, FSE’97 Haifa, Israel, January 20–22 1997 Proceedings*. Ed. by Eli Biham. 1997, pp. 149–165.

[26] Lars Knudsen and David Wagner. “Integral Cryptanalysis”. In: *Fast Software Encryption: 9th International Workshop, FSE 2002 Leuven, Belgium, February 4–6, 2002 Revised Papers*. Ed. by Joan Daemen and Vincent Rijmen. 2002, pp. 112–127.

[27] Yosuke Todo. “Structural Evaluation by Generalized Integral Property”. In: *Advances in Cryptology – EUROCRYPT 2015: 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*. Ed. by Elisabeth Oswald and Marc Fischlin. 2015, pp. 287–314.

[28] Yosuke Todo, Takanori Isobe, Yonglin Hao, et al. “Cube Attacks on Non-Blackbox Polynomials Based on Division Property”. In: *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*. 2017, pp. 250–279.

[29] Yosuke Todo and Masakatu Morii. “Bit-Based Division Property and Application to Simon Family”. In: *Fast Software Encryption: 23rd International Conference, FSE 2016, Bochum, Germany, March 20-23, 2016, Revised Selected Papers*. Ed. by Thomas Peyrin. 2016, pp. 357–377.