International Journal of Cryptology Research 11(1): 13 - 27 (2021)

AKSA MySEAL Block Ciphers: Four Years On

Muhammad Reza Z'aba

Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, 50603 Kuala Lumpur, Malaysia

E-mail: reza.zaba@um.edu.my

ABSTRACT

MySEAL was a project spearheaded by CyberSecurity Malaysia to develop a suite of national trusted cryptographic algorithms. The project began in 2016 and was concluded in 2020. At the end of 2017, the project published the AKSA MySEAL list which contains vetted cryptographic algorithms originally published in international standards or cryptographic listing projects. As the list now about to enter its fifth year, we review the current security status of the five block ciphers included in AKSA MySEAL.

Keywords: symmetric cryptography, block ciphers, stream ciphers

1 INTRODUCTION

The Advanced Encryption Standard (AES) project, which ran from 1997 until 2001, was organised by the US National Institute of Standards and Technology (NIST). The main goal of the project was to develop a Federal Information

Processing Standard (FIPS) specifying an encryption algorithm for use by the US federal government. Rijndael (Daemen and Rijmen, 1998) was later announced as FIPS 197 on November 2001. The AES project has sparked similar other projects such as NESSIE (which ran from 2000 until 2003), CRYPTREC (which stated in 2000 and continues until today) and eSTREAM (2004–2008). The gist of all these projects is to provide a list of safe cryptographic primitives for government and public use.

In Malaysia, such effort was initiated by CyberSecurity Malaysia with the MySEAL project[1]. The project began in 2016 and was concluded in 2020. There were two major outputs of this project: the AKSA MySEAL list and the AKBA MySEAL list. The former list comprises vetted cryptographic algorithms originally published in international standards and the latter list was supposed to contain secure cryptographic algorithms that were not previously included in any standard. This article focuses on the AKSA MySEAL list.

The inaugural AKSA MySEAL list, published in 2017, contains various cryptographic algorithms including block ciphers, stream ciphers, hash functions, asymmetric encryption schemes, digital signature schemes, key agreement schemes and prime number generators. At the time of writing (2021), the AKSA MySEAL list is in its fourth year and is about to enter its fifth year in a couple of months. It is therefore a good time for a review of the algorithms in the AKSA MySEAL.

Such a review is important in order to ensure that the algorithms are still secure for use. An ISO standard, for instance, is reviewed at least once every five years[2]. The NIST has also just embarked on a project to review its cryptographic standards every five years[3]. Although the AKSA MySEAL list is currently not a standard, it is still a good practice to review the listed algorithms periodically. In this article, we combed the literature in order to review the latest analysis done on the symmetric cryptographic algorithms listed in AKSA MySEAL.

The symmetric cryptographic algorithms in AKSA MySEAL contains five

[1] See https://myseal.cybersecurity.my.

[2] See https://www.iso.org/sites/ConsumersStandards/1_standards.html.

[3] See https://csrc.nist.gov/projects/crypto-publication-review-project.

block ciphers and three stream ciphers. The block ciphers are the AES (Daemen and Rijmen, 2001), Camellia (Aoki et al., 2001), CLEFIA (Shirai et al., 2007), PRESENT (Bogdanov et al., 2007) and HIGHT (Hong et al., 2006). The stream ciphers included in AKSA MySEAL are KCipher-2 (Kiyomoto et al., 2007) Rabbit (Boesgaard et al., 2003) and ChaCha20 (Bernstein, 2008). Since block ciphers seem to be more prominently in use, we focus our attention to block ciphers.

This article is organised as follows. Section 2 contains brief descriptions of all symmetric algorithms in AKSA MySEAL. Section 3 presents the current security analysis on these algorithms. Suggestions on the way forward for the symmetric cryptographic algorithms in the AKSA MySEAL list are given in Section 4. A summary is given in Section 5.

2 BRIEF DESCRIPTION OF THE ALGORITHMS

This section presents a brief description of all symmetric cryptographic algorithms in AKSA MySEAL. In AKSA MySEAL, the block ciphers are divided into general-purpose and lightweight. AES, Camellia and CLEFIA are grouped into the former category while HIGHT and PRESENT are in the latter category.

2.1 AES

The Advanced Encryption Standard (AES) (Daemen and Rijmen, 2002) is a block cipher published by the NIST as FIPS 197 (National Institute of Standards and Technology, 2001) in 2001. The cipher is a subset of the Rijndael block cipher submitted to the AES project in 1997 by Daemen and Rijmen (1998). The AES accepts as input a 128-bit plaintext block and a secret key of either 128, 192 or 256 bits. The cipher has 10, 12 or 14 rounds, depending on the length of the secret key.

2.2 Camellia

Camellia is a 128-bit block cipher proposed by Aoki et al. (2001) in 2000. It accepts key lengths of 128, 192 and 256 bits. The cipher consists of 18 rounds for 128-bit key, and 24 for both 192- and 256-bit keys. Two functions called FL and FL^{-1} are placed after every 6 rounds of the Feistel-based cipher.

2.3 CLEFIA

CLEFIA is a 128-bit block cipher proposed by Shirai et al. (2007) in 2007. The specification of the cipher is also available at Sony Corporation's website (Sony Corporation, 2007). The cipher supports key lengths of 128, 192 and 256 bits. The number of rounds are 18, 22 and 26 for the different key lengths. CLEFIA employs the so-called Type-II generalized Feistel network (GFN) (Zheng et al., 1990) and two different F functions.

2.4 HIGHT

HIGHT is a 64-bit block cipher proposed by Hong et al. (2006) in 2006. The cipher supports a key length of 128 bits and has 32 rounds. Similar to CLEFIA, the cipher employs the Type-II GFN (Zheng et al., 1990).

2.5 PRESENT

PRESENT is a 64-bit block cipher designed by Bogdanov et al. (2007) in 2007. It supports key lengths of 80 and 128 bits and the number of rounds is 31 for both key lengths. In 2017, Banik et al. (2017) proposed GIFT, which is based on PRESENT but improves over it with a much smaller footprint.

3 SECURITY OF THE ALGORITHMS

This section presents a review of the security of the algorithms from the literature. We searched for the best attacks applicable to each cipher in the year 2017 and then looked for any progress in the security of the cipher from 2018 until now. We consider an attack that can break the most number of rounds as the best attack. As block ciphers consist of a specific number of rounds, we use the security margin parameter to gauge the attack against the full rounds of the cipher. If an attack is able to penetrate n rounds of the full r-round cipher, then the security margin of the cipher is $(r-n)/r$. Note that we only focus on single-key attacks and exclude attacks based on related-keys and post-quantum security (such as by Bonnetain et al. (2019)).

Tables 1 and 2 list the best single-key attacks on AKSA MySEAL general-purpose and lightweight block ciphers, respectively. For each cipher, the table includes the number of attacked rounds, the attack complexities, the cipher's current security margin and the type of attack. Attacks published on or before 2017 are considered as the best attacks in 2017. Attacks published after 2017 are considered as the latest best attacks.

3.1 The General-Purpose Block Ciphers

On July 2021[4], the NIST published a review on the AES (Mouha, 2021). Their review concludes that the best non-biclique attacks managed to penetrate 7 (out of 10), 9 (out of 12) and 10 (out of 14) rounds of AES-128, AES-192 and AES-256, respectively. All these attacks (including bicliques) were published prior to 2018. We did a search on the literature for the best attacks and confirms NIST's findings. Although no improvements in the number of attacked rounds were reported since 2017, there are works that enhance the complexity of existing attacks such as the one by Bar-On et al. (2020). They managed to reduce the data, memory and time complexities to $2^{21.5}$ chosen plaintexts, memory and encryption operations to attack 5-round AES, which is very practical. The authors also obtain improved attack complexities for 7-round AES.

[4] This article was prepared in October 2021.

Table 1: Summary of the best single-key attacks on AKSA MySEAL general-purpose block ciphers

Algorithm	# of	Security	Complexity			Attack
	Rounds	Margin	Data	Time	Memory	
128-bit Key						
AES	7/10	0.30	2^{105}	$2^{106.9}$	2^{74}	Imp. Diff. (Boura et al., 2017)
	10/10	0	2^{88}	$2^{126.1}$	2^{8}	Biclique (Bogdanov et al., 2011)
	10/10	0	2^{72}	$2^{125.87}$	2^{60}	Biclique (Tao and Wu, 2015)
CLEFIA	14/18	0.22	2^{100}	2^{108}	$2^{101.3}$	Tr. Diff. (Li et al., 2015b)
	18/18	0	2^{64}	$2^{127.70}$	small	Biclique (Bogdanov, 2012)
Camellia	11/18	0.39	$2^{118.40}$	$2^{118.43}$	$2^{92.40}$	Imp. Diff. (Boura et al., 2014)
	18/18	0	2^{128}	$2^{127.60}$	small	Biclique (Bogdanov, 2012)
192-bit Key						
AES	9/12	0.25	2^{121}	$2^{186.50}$	$2^{177.5}$	MitM (Li et al., 2015a)
	12/12	0	2^{80}	$2^{189.7}$	2^{8}	Biclique (Bogdanov et al., 2011)
	12/12	0	2^{48}	$2^{189.76}$	2^{60}	Biclique (Tao and Wu, 2015)
Camellia	13/24	0.54	$2^{118.59}$	$2^{182.10}$	2^{124}	Imp. Diff. (Blondeau, 2015)
	24/24	0	2^{128}	$2^{191.70}$	small	Biclique (Bogdanov, 2012)
CLEFIA	14/22	0.36	2^{100}	2^{135}	2^{131}	Tr. Diff. (Li et al., 2015b)
	22/22	0	2	$2^{191.50}$	small	Biclique (Bogdanov, 2012)
256-bit Key						
AES	10/14	0.29	2^{111}	2^{253}	$2^{211.2}$	MitM (Li and Jin, 2016)
	14/14	0	2^{40}	$2^{254.40}$	2^{8}	Biclique (Bogdanov et al., 2011)
	14/14	0	2^{40}	$2^{254.18}$	2^{60}	Biclique (Tao and Wu, 2015)
Camellia	14/24	0.54	$2^{118.72}$	$2^{222.4}$	$2^{123.94}$	Imp. Diff. (Blondeau, 2015)
	24/24	0	2^{128}	$2^{255.7}$	small	Biclique (Bogdanov, 2012)
CLEFIA	15/26	0.42	2^{100}	2^{203}	2^{139}	Tr. Diff. (Li et al., 2015b)
	26/26	0	2^{64}	$2^{255.50}$	small	Biclique (Bogdanov, 2012)

Similarly, for both CLEFIA and Camellia, we did not find attacks that improve upon the number of attacked rounds for each cipher since 2017. As stated in Table 1, biclique attacks are able to bring down the security margins of the ciphers to zero. However, the time complexities are still close to performing a brute force of the key. Therefore, such attacks do not present a practical threat to the ciphers.

3.2 The Lightweight Block Ciphers

As stated in Table 2, there exists attacks that managed to penetrate more rounds than attacks published prior to 2018. Flórez-Gutiérrez and Naya-Plasencia (2020) are able to break 28 out of 31 rounds of PRESENT-80, which is one more round than the attack by Bogdanov et al. (2016). The same authors also did the same for PRESENT-128 (i.e. breaking 28 rounds), which improves the work of Zheng and Zhang (2015) by one more round. For HIGHT, the number of attacked rounds remain unchanged since 2017. However, Funabiki et al. (2019) are able to half the data complexity of the attack by Funabiki et al. (2017) on 29-round HIGHT.

3.3 On the Time Complexity of the Attacks

In Section 5.4.1 of the AKSA MySEAL guidelines (CyberSecurity Malaysia, 2020), a hypothetical crypto supercomputer was mentioned that is able to perform 2^{60} encryptions per second. A comparison was made to the fastest supercomputer at that time, named Summit, which was able to compute 2^{57} FLOPS (floating-point operations per second). The fastest mining hardware at that time (in 2019) was capable of performing 2^{43} hashes per second.

At the time of writing, the fastest supercomputer is the Fujitsu Fugaku. It is able to perform $2^{58.62}$ FLOPS, which is about two times faster than Summit. On the other hand, the fastest mining hardware to date is the MicroBT Whatsminer M30S++. This particular machine is able to execute 2^{47} hashes per second, which is about 16 times faster than the fastest mining machine in 2019.

Table 2: Summary of the best single-key attacks on AKSA MySEAL lightweight block ciphers

Algorithm	# of	Security		Complexity		Attack
	Rounds	Margin	Data	Time	Memory	
80-bit Key						
PRESENT	27/31	0.13	$2^{63.8}$	$2^{77.0}$	$2^{52.0}$	Mul. Lin. (Bogdanov et al., 2016)
	28/31	0.10	2^{64}	$2^{77.4}$	2^{51}	Lin. (Flórez-Gutiérrez and Naya-Plasencia, 2020)
	31/31	0	2^{22}	$2^{79.34}$	n/a	Biclique (Faghihi Sereshgi et al., 2016)
128-bit Key						
HIGHT	29/32	0.09	2^{64}	2^{126}	n/a	Integral (Funabiki et al., 2017)
	29/32	0.09	2^{63}	$2^{126.07}$	2^{118}	Integral (Funabiki et al., 2019)
	32/32	0	2^{42}	$2^{125.67}$	2^{10}	Biclique (Ahmadi et al., 2014)
PRESENT	27/31	0.13	2^{64}	$2^{125.67}$	2^{10}	Lin. (Zheng and Zhang, 2015)
	28/31	0.10	2^{64}	2^{122}	$2^{84.6}$	Lin. (Flórez-Gutiérrez and Naya-Plasencia, 2020)
	31/31	0	2^{23}	$2^{127.32}$	$2^{34.6}$	Biclique (Abed et al., 2013)

As cryptographic operations (such as encryption) are more complex than a floating-point operation, we can reasonably assume that the fastest machine at this point of time is able to do 2^{47} encryptions per second. This is the same as the fastest mining hardware to date and still much slower than the hypothetical 2^{60} crypto supercomputer mentioned in the AKSA MySEAL guidelines. The lowest time complexity reported for AKSA MySEAL symmetric ciphers is $2^{79.34}$, which is a biclique attack on PRESENT-80. If we run this attack on this particular machine[5], then it will take about 172 years to complete. If, however, we run the same operation on the hypothetical 2^{60} crypto machine mentioned in the AKSA MySEAL guidelines, then the operation should complete within 8 days.

Note that the hypothetical machine does not currently exist and is 8192 times more powerful than the fastest mining machine to date. Despite this, the use of PRESENT-80 should be restricted to protecting messages where their secrecy needs to be maintained for a very short period of time. This has already been mentioned in Section 5.2 of the AKSA MySEAL guidelines. In general, a minimum of 128-bit key should be use for all applications as the hypothetical 2^{60} crypto machine is expected to take 36.5 billion years to perform a brute force attack.

4 WAY FORWARD

Block ciphers and stream ciphers only protects the confidentiality of data. These algorithms, on their own, are unable to provide integrity and data-origin authentication protections which are important in secure communications. The straightforward solutions for these problems are to use the block cipher in an authenticated encryption (AE) mode of operation, pair the ciphers with a message authentication code (MAC) scheme or use a dedicated AE scheme. Furthermore, the latest version of the Transport Layer Security (TLS), which is 1.3, only provides support for AE modes. Currently, in the symmetric cryptography category, AKSA MySEAL only lists block cipher and stream cipher algorithms.

[5] The one that is able to perform 2^{47} encryptions per second.

Moving forward, there may be a need to consider including the block cipher modes of operation in the AKSA MySEAL list itself. The NIST specifies the confidentiality-only modes of operation in the Special Publication (SP) 800-38A. AE modes are defined in SP 800-38C and SP 800-38D. The Japanese CRYPTREC project explicitly mentions the block cipher modes operation (including AE modes) in the list of e-Government Recommended Ciphers[6]. In international standards, confidentiality-only modes of operation are standardised in ISO/IEC 10116 while modes that additionally provide integrity and data-origin authentication protections are standardised in ISO/IEC 19772.

At the moment, the block cipher modes of operation are stated in the AKSA MySEAL guidelines published in July 2020 (CyberSecurity Malaysia, 2020). We think that these modes of operation should be make more explicit in order for users of the AKSA MySEAL list to be more aware of them. Apart from these generic modes of operation, there are dedicated AE schemes that do not strictly follow the structure of these modes. Prominent examples include schemes that were submitted to the NIST Lightweight Cryptography project[7]. At the time of writing, the project is in its final stage. There are ten finalists shortlisted for standardisation. Once the final scheme or schemes have been selected, there may be a need to revise the AKSA MySEAL list to include these dedicated AE schemes.

Other schemes that are worth including in the AKSA MySEAL list are MAC and tweakable block ciphers. MAC schemes provide integrity and data-origin authentication protections. They are used when these protections need to be applied to plaintexts sent in the clear, or when paired with a confidentiality-only mode of operation. Tweakable block ciphers, on the other hand, include an additional public parameter that is useful to provide randomness at the primitive level. At the moment, these type of block ciphers are currently being considered for standardisation in ISO/IEC 18033-7. An example of a tweakable block cipher is SKINNY (Beierle et al., 2016).

[6] See `https://www.cryptrec.go.jp/list/cryptrec-ls-0001-2012r6.pdf`.

[7] See `https://csrc.nist.gov/Projects/lightweight-cryptography/finalists`.

5 SUMMARY

In this article, we have reviewed the security of the block cipher algorithms listed in AKSA MySEAL. We found that, for general-purpose block ciphers, the security margin of the ciphers with respect to non-biclique attacks remain the same since the AKSA MySEAL list was first published in 2017. For lightweight block ciphers, the security margin for PRESENT is slightly reduced from 0.13 as of 2017 to 0.10 as of now. Biclique attacks manage to decrease the security margin of all AKSA MySEAL block ciphers to zero. However, due to the extremely high complexity of the attacks, they do not pose a practical threat to the security of the ciphers.

REFERENCES

Abed, F., Forler, C., List, E., Lucks, S., and Wenzel, J. (2013). Biclique Cryptanalysis of PRESENT, LED, and KLEIN: Revision 2013-05-20. Cryptology ePrint Archive, Report 2012/591. `http://ia.cr/2012/591`.

Ahmadi, S., Ahmadian, Z., Mohajeri, J., and Aref, M. R. (2014). Low-Data Complexity Biclique Cryptanalysis of Block Ciphers with Application to Piccolo and HIGHT. *IEEE Transactions on Information Forensics and Security*, 9(10):1641–1652.

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T. (2001). Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms – Design and Analysis. In Stinson, D. R. and Tavares, S., editors, *Selected Areas in Cryptography, SAC 2000*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer-Verlag.

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M., and Todo, Y. (2017). `GIFT`: A Small Present. In Fischer, W. and Homma, N., editors, *Cryptographic Hardware and Embedded Systems – CHES 2017*, volume 10529 of *Lecture Notes in Computer Science*, pages 321–345. Springer-Verlag.

Bar-On, A., Dunkelman, O., Keller, N., Ronen, E., and Shamir, A. (2020). Improved Key Recovery Attacks on Reduced-Round AES with Practical Data and Memory Complexities. *Journal of Cryptology*, 33:1003–1043.

Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., and Sim, S. M. (2016). The `SKINNY` Family of Block Ciphers and Its Low Latency Variant `MANTIS`. In Robshaw, M. and Katz, J., editors, *Advances in Cryptology — CRYPTO 2016, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer-Verlag.

Bernstein, D. J. (2008). ChaCha, a Variant of Salsa20. `https://cr.yp.to/chacha.html`.

Blondeau, C. (2015). Impossible Differential Attack on 13-round Camellia-192. *Information Processing Letters*, 115(9):660–666.

Boesgaard, M., Vesterager, M., Pedersen, T., Christiansen, J., and Scavenius, O. (2003). Rabbit: A new high-performance stream cipher. In Johansson, T., editor, *Fast Software Encryption, FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 307–329. Springer-Verlag.

Bogdanov, A. (2012). Security Evaluation of Block Ciphers AES, Camellia, CLEFIA and SC2000 using Two New Techniques – Biclique Attacks and Zero-Correlation Linear Attacks. CRYPTREC Technical Report 2204. `http://bit.ly/2eNx9Aw+`.

Bogdanov, A., Khovratovich, D., and Rechberger, C. (2011). Biclique Cryptanalysis of the Full AES. In Lee, D. H. and Wang, X., editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 344–371. Springer-Verlag.

Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C. (2007). PRESENT: An Ultra-Lightweight Block Cipher. In Paillier, P. and Verbauwhede, I., editors, *Cryptographic Hardware and Embedded Systems – CHES 2007*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer-Verlag.

Bogdanov, A., Tischhauser, E., and Vejre, P. S. (2016). Multivariate Linear Cryptanalysis: The Past and Future of PRESENT. Cryptology ePrint Archive, Report 2016/667. `http://ia.cr/2016/667`.

Bonnetain, X., Naya-Plasencia, M., and Schrottenloher, A. (2019). Quantum Security Analysis of AES. *IACR Transactions on Symmetric Cryptology*, 2019(2):55–93.

Boura, C., Lallemand, V., Naya-Plasencia, M., and Suder, V. (2017). Making the Impossible Possible. *Journal of Cryptology*, pages 1–33. doi:10.1007/s00145-016-9251-7.

Boura, C., Naya-Plasencia, M., and Suder, V. (2014). Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and Simon. In Sarkar, P. and Iwata, T., editors, *Advances in Cryptology - ASIACRYPT 2014, Part I*, volume 8873 of *Lecture Notes in Computer Science*, pages 179–199. Springer-Verlag.

CyberSecurity Malaysia (2020). Guideline on the Usage of AKSA MySEAL Recommended Cryptographic Algorithms. MySEAL. `https://myseal.cybersecurity.my`.

Daemen, J. and Rijmen, V. (1998). AES proposal: Rijndael. NIST AES Proposal.

Daemen, J. and Rijmen, V. (2001). The Wide Trail Design Strategy. In Honary, B., editor, *IMA International Conference on Cryptography and Coding*, volume 2260 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag.

Daemen, J. and Rijmen, V. (2002). *The Design of Rijndael, AES – The Advanced Encryption Standard.* Springer-Verlag.

Faghihi Sereshgi, M. H., Dakhilalian, M., and Shakiba, M. (2016). Biclique Cryptanalysis of MIBS-80 and PRESENT-80 Block Ciphers. *Security and Communication Networks*, 9(1):27–33.

Flórez-Gutiérrez, A. and Naya-Plasencia, M. (2020). Improving Key-Recovery in Linear Attacks: Application to 28-Round PRESENT. In Coron, J.-S. and Nielsen, J. B., editors, *Advances in Cryptology — EUROCRYPT 2020, Part I*, volume 12105 of *Lecture Notes in Computer Science*, pages 221–249. Springer-Verlag.

Funabiki, Y., Todo, Y., Isobe, T., and Morii, M. (2017). Improved Integral Attack on HIGHT. In Pieprzyk, J. and Suriadi, S., editors, *Information*

Security and Privacy, ACISP 2017, Part I, volume 10342 of *Lecture Notes in Computer Science*, pages 363–383. Springer-Verlag.

Funabiki, Y., Todo, Y., Isobe, T., and Morii, M. (2019). Improved Integral Attack on HIGHT. *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, E102.A(9):1259–1271.

Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., and Chee, S. (2006). HIGHT: A New Block Cipher Suitable for Low-Resource Device. In Goubin, L. and Matsui, M., editors, *Cryptographic Hardware and Embedded Systems – CHES 2006*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59. Springer-Verlag.

Kiyomoto, S., Tanaka, T., and Sakurai, K. (2007). K2 Stream Cipher. In Filipe, J. and Obaidat, M. S., editors, *E-business and Telecommunications*, volume 23 of *Communications in Computer and Information Science*, pages 214–226. Springer-Verlag.

Li, L., Jia, K., and Wang, X. (2015a). Improved Single-Key Attacks on 9-Round AES-192/256. In Cid, C. and Rechberger, C., editors, *Fast Software Encryption, FSE 2014*, volume 8540 of *Lecture Notes in Computer Science*, pages 127–146. Springer-Verlag.

Li, L., Jia, K., Wang, X., and Dong, X. (2015b). Meet-in-the-Middle Technique for Truncated Differential and Its Applications to CLEFIA and Camellia. In Leander, G., editor, *Fast Software Encryption, FSE 2015*, volume 9054 of *Lecture Notes in Computer Science*, pages 48–70. Springer-Verlag.

Li, R. and Jin, C. (2016). Meet-in-the-Middle Attacks on 10-round AES-256. *Designs, Codes and Cryptography*, 80(3):459–471.

Mouha, N. (2021). Review of the Advanced Encryption Standard. NISTIR 8319. National Institute of Standards and Technology.

National Institute of Standards and Technology (2001). Advanced Encryption Standard. Federal Information Processing Standard (FIPS) 197. Available at `http://csrc.nist.gov/publications/fips/`.

Shirai, T., Shibutani, K., Akishita, T., Moriai, S., and Iwata, T. (2007). The 128-bit Blockcipher CLEFIA. In Biryukov, A., editor, *Fast Software Encryption: 14th International Workshop, FSE 2007*, volume 4593 of *Lecture Notes in Computer Science*, pages 181–195. Springer-Verlag.

Sony Corporation (2007). The 128-bit Blockcipher CLEFIA Algorithm Specification. `http://bit.ly/2fSx0sM+`.

Tao, B. and Wu, H. (2015). Improving the Biclique Cryptanalysis of AES. In Foo, E. and Stebila, D., editors, *Information Security and Privacy, ACISP 2015*, volume 9144 of *Lecture Notes in Computer Science*, pages 39–56. Springer-Verlag.

Zheng, L. and Zhang, S. (2015). FFT-Based Multidimensional Linear Attack on PRESENT using the 2-Bit-Fxed Characteristic. *Security and Communication Networks*, 8(18):3535–3545.

Zheng, Y., Matsumoto, T., and Imai, H. (1990). On the Construction of Block Ciphers Provably Secure and Not Relying on Any Unproved Hypotheses. In Brassard, G., editor, *Advances in Cryptology – CRYPTO ’89*, volume 435 of *Lecture Notes in Computer Science*, pages 461–480. Springer-Verlag.