μ^2 : A Lightweight Block Cipher

Wei-Zhu Yeoh, Je Sen Teh*, and Mohd Ilyas Sobirin Bin Mohd Sazali

Universiti Sains Malaysia, Penang, Malaysia
*jesen_teh@usm.my

Abstract. This paper presents a 64-bit lightweight block cipher, μ^2 with a key size of 80-bit. μ^2 is designed based on well-established design paradigms, achieving comparable performance and security when compared against existing state-of-the-art lightweight block ciphers. μ^2 is based on the Type-II generalized Feistel structure with a round function, F that is a 16-bit ultra-lightweight block cipher based on the substitution-permutation network. Security evaluation indicates that μ^2 offers a large security margin against known attacks such as differential cryptanalysis, linear cryptanalysis, algebraic attack and others.

Keywords: Cryptanalysis, Feistel, IoT, lightweight block cipher, SPN

1 Introduction

In recent years, the rise of Internet-of-Things (IoT) devices with constrained computing capability has been prominent. These devices have not only widely used in everyday life but are also interconnected to form a network to provide unobtrusive services to the consumers. However, this interconnectivity poses a range of security risks. Thus, lightweight block ciphers have been proposed in response to those concerns, such as PRESENT [9], LED[14] and CHAM [18]. These lightweight block ciphers have been meticulously designed to have simple structures and high throughput for their implementation. PRESENT is the currently the ISO/IEC standard [16] for 64-bit lightweight block ciphers. Despite its simple design based on the substitution-permutation network (SPN), it has been shown to resist various cryptanalytic attacks over the years. Although there exists recently proposed lightweight block ciphers [14,4,18], they have yet to undergo sufficient cryptanalysis to be considered state-of-the-art.

In this paper, we propose μ^2, a new 64-bit block cipher based on the Type-II generalized Feistel structure (GFS). Unlike regular ciphers, its round function F is in itself a 4-round ultra-lightweight cipher (ULC) is based on SPN. Embedding another block cipher within the design still maintains design simplicity and ease of analysis. The inspiration of the cipher's name μ^2 comes from the metric multiplicative prefix micro, μ which often associated with a very tiny value whereas the power of 2 implies the use of a two ciphers. μ^2 has shown to be more efficient than PRESENT, with comparable security margins. Therefore, it serves as a suitable lightweight block cipher candidate for resource-constrained devices. In addition, this work is in line with Malaysia's National Cryptography

R. Alfred et al. (eds.), *Computational Science and Technology*,
Lecture Notes in Electrical Engineering 603,
https://doi.org/10.1007/978-981-15-0058-9_27

Policy (NCP) [1] and National Cyber Security Policy (NCSP) [2], which supports cryptographic research and development towards self-reliance.

2 Specification of μ^2

2.1 Main Structure of μ^2

μ^2 is a lightweight block cipher with 15 rounds. It has a block length of 64 bits and a key length of 80 bits. The design of μ^2 is based on a Type-II GFS as shown in Figure 1. μ^2 uses a new ULC with a block size of 16 bits, which is based the SPN and Even-Mansour construction [11]. This ULC is detailed in Section 2.2. Four rounds of the ULC will be used for each F-function. μ^2 uses PRESENT's 4-bit s-box for encryption and key generation as shown in Table 1.

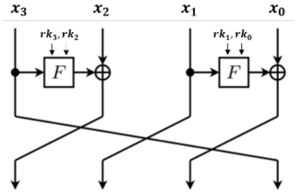


Fig. 1: μ^2 Structure

Table 1: Substitution Box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

The design of the key schedule (key generation algorithm) of μ^2 is based on PRESENT which can be summarized as

1. Initialize an 80-bit register with the 80-bit secret key.
2. Left rotate the register by 61 bits.
3. Substitute the four most significant bits (MSBs) and 64^{th} to 67^{th} bits using the substitution box (s-box).
4. XOR the 15^{th} to the 18^{th} bits with a round counter.
5. Extract the 64 MSBs as the round key, RK

or mathematically defined as

1. $[k_{79}k_{78}...k_1k_0] = [k_{18}k_{17}...k_{20}k_{19}]$

2. $[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$
3. $[k_{67}k_{66}k_{65}k_{64}] = S[k_{67}k_{66}k_{65}k_{64}]$
4. $[k_{18}k_{17}k_{16}k_{15}] = [k_{18}k_{17}k_{16}k_{15}] \oplus round\_counter$

Unlike PRESENT, the *round_counter* is only 4 bits because μ^2 only has 15 rounds, and is initialized to 0 at the beginning. Another change made is to feed 4 more distinct bits of value through the same s-box in due to the reduced rounds of the key schedule compared to PRESENT. The round key, RK is divided into four sub-round keys, $RK = \{rk_3, rk_2, rk_1, rk_0\}$. rk_3 and rk_2 are used in the left F-function whereas rk_1 and rk_0 are used in the right F-function as shown in Figure 1. New round keys are generated by repeating the same key generation algorithm. This is performed once after each round of μ^2. Note that the very first round key is directly extracted from the secret key prior to transformation.

2.2 Ultra-lightweight Cipher (*F*-function)

As previously mentioned, the F-function of μ^2 is a 16-bit block cipher based on the SPN and Even-Mansour construction. The sub-round keys are XOR-ed with the 16-bit input before and after the completing four rounds of the SPN. To break symmetry between each round, round constants are introduced, $con_i = \{0x1000, 0x2000, 0x3000, 0x4000\}$. To break the symmetry between each instance of the F-function, the ULC also includes a counter, F_{count} which is incremented after computing each F-function. Thus, each round of μ^2 will increment F_{count} by 2. F_{count} is initialized to 0 at the beginning.

The substitution layer consists of four 4-bit s-boxes defined in Table 1. This is followed by a bitwise permutation, π designed to maximize the number of active s-boxes (AS) defined as

$$\pi[b_{15}b_{14}...b_1b_0] = [b_3b_6b_9b_{12}b_7b_{10}b_{13}b_0b_{11}b_{14}b_1b_4b_{15}b_2b_5b_8], \tag{1}$$

where b_i is the i^{th} bit of the 16-bit data block. The effect of π on the number of AS is described in Section 4.1. A visual depiction of the entire SPN is as shown in Figure 2 whereas the block diagram of the F-function is as shown in Figure 3.

3 Design Choices

3.1 Intended Uses and Goals

The goal is to construct a new robust lightweight block cipher that is suitable for adoption and deployment by highly-constrained computing devices while maintaining the efficiency on 16/32/64-bit processors. This newly proposed cipher should not only be comparable with various existing proposals of similar intent but also outperforms the previous proposal in some aspect while maintaining the design and implementation simplicity.

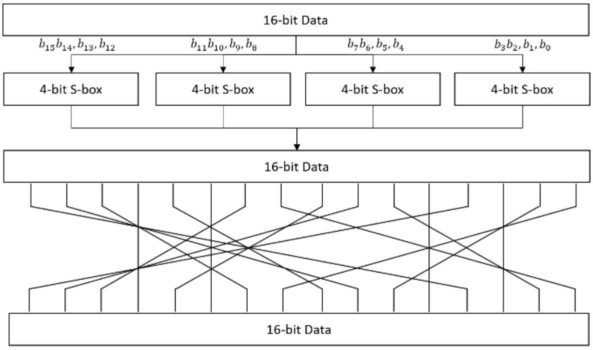
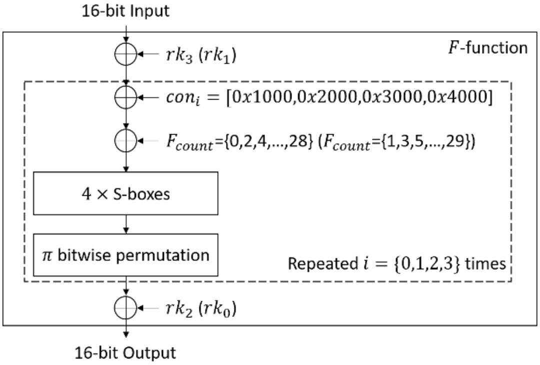


Fig. 2: Substitution-Permutation Network


16-bit Input
rk_3 (rk_1)
F-function
con_i = [0x1000,0x2000,0x3000,0x4000]
F_{count}={0,2,4,...,28} (F_{count}={1,3,5,...,29})
4 × S-boxes
π bitwise permutation
Repeated i = {0,1,2,3} times
rk_2 (rk_0)
16-bit Output

Notes:
Values in the bracket (*) are for the right F-function.
F_{count} is incremented after computing each F-function.

Fig. 3: F-function

3.2 Structure of the μ^2

The Type-II GFS structure of μ^2 and the choice of a more elaborate F-function is quite similar to that of the 4-branch version of the Simpira V2 permutation [13]. Unlike Simpira which uses AES [20] as its F-function, we proposed a new 16-bit ULC as the replacement that is suitable for constrained devices. We have also chosen the same number of rounds as Simpira to ensure sufficient bit diffusion.

The ULC constituting the F-function can be seen as a mini-PRESENT variant with 16-bit block size due to the fact that it uses the s-box from PRESENT and also adopts a similar bitwise approach to its permutation albeit with a different pattern. The choice of resemblance is explained in the following section.

3.3 Substitution Layer (S-box) and Permutation Layer (P-layer)

In order to maximize the efficiency of the algorithm, a single strong 4-bit to 4-bit S-box, $S : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$ is chosen as the non-linear substitution layer. Compared with larger size 8-bit s-box featured prominently in U.S. encryption standard AES [20], a 4-bit s-box is much more compact and advantageous when implemented in resource-constrained devices. μ^2 cipher adopted the s-box defined in the PRESENT which is well-studied and thoroughly investigated and thus is able to provide reasonably strong resistance against well-established attack due to its excellent nonlinearity, differential probability and algebraic order.

The permutation layer is chosen to maximize efficiency while providing adequate security. As such, a simple bitwise permutation layer was selected because of its simplicity and efficiency when implemented. Due to the simple nature of the bit permutation, it also allows clear and precise security analysis to be made in the later section.

3.4 Key Schedule and Even-Mansour Scheme

The key schedule of the cipher is a straightforward modification of the PRESENT key schedule. The robust yet simple key schedule defined by PRESENT has a minimal impact on the overall performance while providing some increased security against various type of cryptanalysis attack. There is some study on the strength of the PRESENT key schedule [15] but the investigation indicates that the 80-bit key schedule shows no significant exploitable weakness. The modification of the round counter bit and the inclusion of an extra non-linear s-box per round is in direct respond to the lower number of round of the proposed cipher.

The double-key Even-Mansour scheme [11] is used to introduce secret key information. Although there is a notable security proof [10] that shows single-key Even-Mansour scheme has the same security lower bound as the double-key scheme. The use of the double-key variant allows direct utilization of the modified PRESENT key schedule with minimal modification. The key schedule produces a 64-bit round key for each round which can be divided equally into two pairs of 16-bit keys to be used for tne two F-functions respectively.

4 Security Analysis

4.1 Differential and Linear Cryptanalysis

For differential and linear cryptanalysis, the minimum number of AS, AS_{min} determines the cipher's security margin. For μ^2 the following observations that can be made by examining the permutation layer in conjunction with the s-boxes of F-function:

1. The input to an s-box comes from four distinct s-boxes and the output of an s-box goes into four different s-boxes.
2. An input with a one-bit difference will always lead to an output difference of two bits or higher.

3. S-box activation patterns of $1-1-1$ and $1-2-1$ cannot occur.
4. When there is a non-zero difference entering the 4-round ULC, the $1-2-2-1$ pattern will have the least number of AS because any other patterns with fewer AS will violate observations 3 and 4.
5. If there are any other cases whereby any one of the rounds contains three or four AS, there will be at least six or more AS in total.

As stated above, $AS_{min} = 6$. The GFS structure has a minimum of 14 differentially activated F-function in 15 rounds. Thus, 15 rounds of μ^2 will have a minimum of $14 \times 6 = 84$ AS. The maximum differential probability of the s-box is 2^{-2}. Based on these criteria, the probability of a single path differential is upper-bounded by 2^{-168}. A successful attack would have a data complexity of 2^{168} which exceeds the available message space of 2^{-64}. Hence, μ^2 has a large security margin against differential cryptanalysis [7].

Next, we analyze μ^2's security against linear cryptanalysis. The maximum bias of the s-box is 2^{-2} and based on the previous analysis, each round of μ^2 has $AS_{min} = 6$. By applying the piling-up lemma [19],

$$\epsilon = 2^{(14\times6)-1} \times (2^{-2})^{14\times6} = 2^{-85}.$$

The data complexity of the linear attack can be calculated as

$$N_L = \frac{1}{\epsilon^2} \ .$$

Hence for 15 rounds of μ^2, the data complexity of a linear attack is estimated to be 2^{170} which exceeds the message space of 2^{64}.

4.2 Integral Attacks

Integral attacks [17] are known to be more applicable to the analysis of ciphers with word-like structures. However, there have been some attempts to use integral attack to analyze bit-based cipher [22,23] but the attack is not particularly detrimental to the overall strength of the cipher security. Any word-like structure of μ^2 will be disrupted by bit-wise operation of ULC. Hence, it is believed that integral attack poses no threat to μ^2.

4.3 Algebraic Attacks

Extending from the work by PRESENT, the s-box of the PRESENT can be described by 21 quadratic equations in eight input/output-bit variables over binary field, $GF(2)$. Each round of the cipher consist of 34 s-boxes (encryption and key generation). Therefore, the entire proposed system can be expressed by $34 \times 15 \times 21 = 10710$ quadratic equations in 4080 variables. These numbers tend to indicate that μ^2 exhibits a high level of immunity against algebraic attack.

4.4 Key Schedule Attacks

The most successful attacks on the key scheduling are the slide attack [8] and related-key attack [6]. These attacks rely on the relationship between each subsequent rounds. Since the key schedule of the mu^2 cipher is nearly identical to that of the PRESENT, some of the existing analysis can be easily extended. The relationship and symmetry of each round are broken up by the introduction of the round-dependent counter. Furthermore, the key is further scrambled using nonlinear s-box. The presence of F-function counter and ULC round counter also contribute towards the overall strength against these types of attacks as well. The combined efforts should thwart the attacker from mounting a successful slide or related-key attack on the key schedule.

4.5 Statistical Analysis

The NIST statistical test suite [21] was used to test the number sequences generated from the cipher to ensure that they resemble pseudorandom sequences with no statistical defects. A 1000-Mbit sample of number sequences was tested whereby the number sequences were generated by encrypting plaintext that was incremented by 1 for each block starting at 0 while the key is fixed at 0. The number sequences are considered to be random when the test results have a P-value of ≥ 0.01 and passing ratio ≥ 9.8056. Based on the acquired results illustrated at Table 2, the μ^2 cipher indeed approximates a pseudorandom function which is one of the desirable traits of a block cipher.

Table 2: NIST Test Result

Test	P-value	Passing Ratio	Result
Frequency	0.073	0.989	Pass
Block frequency	0.372	0.987	Pass
Cumulative sums	0.391	0.990	Pass
Runs	0.055	0.987	Pass
Longest run	0.365	0.992	Pass
Rank	0.514	0.989	Pass
FFT	0.575	0.989	Pass
Nonoverlapping templates	0.056	0.992	Pass
Overlapping templates	0.036	0.991	Pass
Universal	0.587	0.997	Pass
Approximate entropy	0.637	0.990	Pass
Random excursions	0.713	0.987	Pass
Random excursions variant	0.454	0.990	Pass
Serial	0.321	0.983	Pass
Linear complexity	0.997	0.988	Pass

5 Performance and Comparision

To illustrate that the performance of μ^2's software implementation is comparable to existing proposals, performance measurements from various lightweight ciphers including μ^2 were measured using the same computing device. Their performance were benchmarked using the Intel Skylake I5-6600K @ 3.5GHz CPU. The implementations for existing lightweight ciphers, PRESENT and SKINNY [3] were taken from existing resources made available by other researchers who have optimized the algorithm with respect to the target platform [24,12,5]. The acquired results are shown in Table 3. It can be seen that μ^2 achieved a comparable throughput when compared to other well-known lightweight block ciphers.

Table 3: Software implementation throughput of μ^2, PRESENT and SKINNY

Cipher	Throughput Mb/s^{-1}	Reference
$\mu^2 - 80^*$	148.28	This
PRESENT-80*	133.77	[9][24]
SKINNY-64*	121.23	[5][3]

* The implementations used do not represent the best possible optimized version.

6 Conclusion

In this paper, we presented a new lightweight block cipher μ^2 which has a block length of 64-bit and an 80-bit key. It is specifically designed to provide high security margins while maintaining good performance for constrained devices. A variant of Type-II GFS is used as the design foundation for the cipher with a SP-network based ULC as its 16-bit round function. The use of a single 4-bit s-box and bit permutation layer contribution towards the overall efficiency of the cipher which exceeds well-known lightweight ciphers such as PRESENT and SKINNY. Based on the security evaluation and the preliminary cryptanalytic results of μ^2, it is shown that μ^2 achieved sufficient security margin against well-known attacks. However, more security analysis still needs to be conducted to verify the security of the proposed cipher even further.

Acknowledgements

This work has been partially supported by Universiti Sains Malaysia under Grant No. 304/PKOMP/6315190.

References

1. Malaysia National Cryptography Policy. http://www.parlimen.gov.my/files/hindex/pdf/DN-09122013.pdf, https://cnii.cybersecurity.my/main/ncsp/policy_thrusts.html
2. Malaysia National Cyber Security Policy. https://cnii.cybersecurity.my/main/ncsp/policy_thrusts.html, https://cnii.cybersecurity.my/main/ncsp/policy_thrusts.html
3. SKINNY family of block ciphers. https://sites.google.com/site/skinnycipher/home
4. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A Small Present. In: Fischer, W., Homma, N. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2017, vol. 10529, pp. 321–345. Springer International Publishing, Cham (2017). https://doi.org/10.1007/978-3-319-66787-4_16
5. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016, vol. 9815, pp. 123–153. Springer Berlin Heidelberg, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5
6. Biham, E.: New types of cryptanalytic attacks using related keys. Journal of Cryptology **7**(4) (1994). https://doi.org/10.1007/BF00203965
7. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology **4**(1), 3–72 (1991). https://doi.org/10.1007/BF00630563
8. Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Goos, G., Hartmanis, J., van Leeuwen, J., Preneel, B. (eds.) Advances in Cryptology — EUROCRYPT 2000, vol. 1807, pp. 589–606. Springer Berlin Heidelberg, Berlin, Heidelberg (2000). https://doi.org/10.1007/3-540-45539-6_41
9. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2007, vol. 4727, pp. 450–466. Springer Berlin Heidelberg, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
10. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012, vol. 7237, pp. 336–354. Springer Berlin Heidelberg, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_21
11. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology **10**(3), 151–161 (Jun 1997). https://doi.org/10.1007/s001459900025
12. Gong, Z., Hartel, P., Nikova, S., Zhu, B.: Towards Secure and Practical MACs for Body Sensor Networks. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Roy, B., Sendrier, N. (eds.) Progress in Cryptology - INDOCRYPT 2009, vol. 5922, pp. 182–198. Springer Berlin Heidelberg, Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-10628-6_13
13. Gueron, S., Mouha, N.: Simpira v2: A Family of Efficient Permutations Using the AES Round Function. In: Cheon, J.H., Takagi, T. (eds.) Advances in Cryptology

– ASIACRYPT 2016, vol. 10031, pp. 95–125. Springer Berlin Heidelberg, Berlin, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_4

14. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED Block Cipher. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Preneel, B., Takagi, T. (eds.) Cryptographic Hardware and Embedded Systems – CHES 2011, vol. 6917, pp. 326–341. Springer Berlin Heidelberg, Berlin, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23951-9_22
15. Hernandez-Castro, J.C., Peris-Lopez, P., Aumasson, J.P.: On the Key Schedule Strength of PRESENT. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Garcia-Alfaro, J., Navarro-Arribas, G., Cuppens-Boulahia, N., de Capitani di Vimercati, S. (eds.) Data Privacy Management and Autonomous Spontaneus Security, vol. 7122, pp. 253–263. Springer Berlin Heidelberg, Berlin, Heidelberg (2012). https://doi.org/10.1007/978-3-642-28879-1_17
16. International Organization for Standardization: ISO/IEC 29192-2:2012 Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers (2019)
17. Knudsen, L., Wagner, D.: Integral Cryptanalysis. In: Goos, G., Hartmanis, J., van Leeuwen, J., Daemen, J., Rijmen, V. (eds.) Fast Software Encryption, vol. 2365, pp. 112–127. Springer Berlin Heidelberg, Berlin, Heidelberg (2002). https://doi.org/10.1007/3-540-45661-9_9
18. Koo, B., Roh, D., Kim, H., Jung, Y., Lee, D.G., Kwon, D.: CHAM: A Family of Lightweight Block Ciphers for Resource-Constrained Devices. In: Kim, H., Kim, D.C. (eds.) Information Security and Cryptology – ICISC 2017, vol. 10779, pp. 3–25. Springer International Publishing, Cham (2018). https://doi.org/10.1007/978-3-319-78556-1_1
19. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) Advances in Cryptology — EUROCRYPT '93, vol. 765, pp. 386–397. Springer Berlin Heidelberg, Berlin, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_33
20. National Institute of Standards and Technology: Advanced encryption standard (AES). Tech. Rep. NIST FIPS 197, National Institute of Standards and Technology, Gaithersburg, MD (Nov 2001). https://doi.org/10.6028/NIST.FIPS.197
21. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E.: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Tech. rep., BOOZ-ALLEN AND HAMILTON INC MCLEAN VA (May 2001)
22. Wu, S., Wang, M.: Integral Attacks on Reduced-Round PRESENT. In: Hutchison, D., Kanade, T., Kittler, J., Kleinberg, J.M., Mattern, F., Mitchell, J.C., Naor, M., Nierstrasz, O., Pandu Rangan, C., Steffen, B., Sudan, M., Terzopoulos, D., Tygar, D., Vardi, M.Y., Weikum, G., Qing, S., Zhou, J., Liu, D. (eds.) Information and Communications Security, vol. 8233, pp. 331–345. Springer International Publishing, Cham (2013). https://doi.org/10.1007/978-3-319-02726-5_24
23. Z'aba, M.R., Raddum, H., Henricksen, M., Dawson, E.: Bit-Pattern Based Integral Attack. In: Nyberg, K. (ed.) Fast Software Encryption, vol. 5086, pp. 363–381. Springer Berlin Heidelberg, Berlin, Heidelberg (2008). https://doi.org/10.1007/978-3-540-71039-4_23
24. Zhu, B.: An efficient software implementation of the block cipher PRESENT for 8-bit platforms: Bozhu/PRESENT-C (Feb 2019)