Avalanche effect and bit independence criterion of perfectly secure Shannon cipher based on matrix power

Matas Levinskas[1], **Aleksejus Mihalkovich**[2]
Department of Applied Mathematics, Kaunas University of Technology, Kaunas, Lithuania
[2]Corresponding author
E-mail: [1]*matas.levinskas@ktu.edu*, [2]*aleksejus.michalkovic@ktu.lt*

Received 4 August 2021; received in revised form 14 September 2021; accepted 28 September 2021
DOI https://doi.org/10.21595/mme.2021.22234

Abstract. In 2020 E. Sakalauskas with coauthors published a paper defining perfectly secure Shannon cipher based on matrix power function, proposing effective parallelization, and ensuring no need for multiple rounds encrypting one data block [1]. In this paper we present computational results with the avalanche effect and bit independence criterion (BIC). These criteria are important when describing the rate of confusion of bits in the ciphertext. It was observed that increasing matrix order and group size enhance BIC and avalanche effect results converging to the desired values. Based on the outputs it is possible to pick appropriate parameters satisfying security needs and available memory in a device where appropriate keys are going to be stored.

Keywords: symmetric cipher, perfect secrecy, block cipher, matrix power function, avalanche effect, bit independence criterion.

1. Introduction

1.1. Avalanche effect and BIC

Cryptography security analysis methods such as avalanche effect and BIC allow us to evaluate block cipher secrecy by computing elements confusion after changing just one bit [2], determine elements confusion and dependance from other elements [3, 4]. The values of these criteria are commonly calculated by considering the avalanche vector A^{e_i}, which describes ciphertext bits change after flipping one bit in the plaintext:

$$A^{e_i} = Enc(k,\mu) \oplus Enc(k,\mu \oplus e_i) = \left[a_1^{e_i} a_2^{e_i} \dots a_n^{e_i}\right], \tag{1}$$

where vector has all entries equal to 0 except for the i-th one which is equal to 1, entry $a_1^{e_i} \in \{0,1\}$ and function $Enc(k,\mu)$ is encryption function mapping shared key k and plaintext μ to the ciphertext generally denoted by c.

Using expression defined in Eq. (1), we compute the i-th bit avalanche $k_{AVAL}(i)$ effect as follows:

$$\begin{aligned} k_{AVAL}(i) &= \frac{1}{n \cdot 2^n} \sum_{j=1}^{n} W\left(a_j^{e_i}\right), \\ W\left(a_j^{e_i}\right) &= \sum_{X \in \{0,1\}^n} a_j^{e_i}, \end{aligned} \tag{2}$$

where $k_{AVAL}(i)$ indicates the number of bits changes after flipping i-th bit. The desired value of the avalanche effect is 0.5 for all the bits, meaning that it is infeasible to distinguish which bit changes occur after flipping a random bit of the original message.

The bit independence of the two entries is being calculated by the maximal absolute correlation coefficient between avalanche vector j and k components. According to [2], BIC can be calculated by the formula:

$$BIC(a_j, a_k) = \max_{1 \le i \le n} |\mathrm{corr}(a_j^{e_i}, a_k^{e_i})|. \tag{3}$$

Furthermore, relying on Eq. (3) we can define the overall BIC for the whole ciphertext block $Enc(k, m)$ as the maximal correlation by checking all available pairs:

$$BIC(Enc) = \max_{\substack{1 \le k, k \le n \\ k \ne j}} BIC(a_j, a_k). \tag{4}$$

Ideally, the value of BIC should be close to 0 hence ensuring that all the bit changes occur statistically independently.

1.2. Perfectly secure Shannon cipher based on matrix power function

The matrix power function (MPF) was introduced in [5], as the following mapping acting on the Cartesian product of the space of square matrices of order m with itself:

$$Mat_m(\mathbb{R}) \times Mat_m(\mathbb{S}) \times Mat_m(\mathbb{R}) \mapsto Mat_m(\mathbb{S}).$$

The general notation for this mapping is as follows:

$${}^{X}W^{Y} = E, \tag{5}$$

where $W, E \in Mat_m(\mathbb{S})$ are matrices with entries from semigroup $\mathbb{S}$ and $X, Y \in Mat_m(\mathbb{R})$ are matrices with entries from a finite ring of integers $\mathbb{R}$. This mapping allows us to raise the base matrix W to the so-called power matrices X and Y.

E. Sakalauskas with co-authors used the MPF in 2020 to propose a perfectly secure Shannon cipher defined over $\mathbb{Z}_3$ [1]. This cipher uses a plaintext matrix M, private keys X and Y along with a function $f: \mathbb{Z}_3 \mapsto \mathbb{G}_3$, which maps elements of $\mathbb{Z}_3$ to elements of the multiplicative Sylow group $\mathbb{G}_3 = \{1,2,4\}$, which is a subgroup of $\mathbb{Z}_7^*$. Note, that actions in $\mathbb{G}_3$ are performed modulo 7. A key feature of this mapping is that it does not carry over the addition in $\mathbb{Z}_3$ to the multiplication in $\mathbb{G}_3$ and hence is not an isomorphism. The encryption function can be expressed in a following way:

$$C = Enc(\{X, Y\}, M) = F^{-1}(F(X) \odot {}^{X}F(X + M)^{Y}) + X, \tag{6}$$

where $F: Mat_m(\mathbb{Z}_3) \mapsto Mat_m(\mathbb{G}_3)$ is an entry-wise matrix analogue of the mapping f and F^{-1} is its inverse. Note that since F is not an isomorphism no cancelations in Eq. (6) are possible. We also use $\odot$ to denote Hadamard product of two matrices.

It is worthy noting that the shared key $\{X, Y\}$ consists of $2m^2$ entries and hence is at least twice the length of the original plaintext given that extra bits may be added at the end message to make it appropriate length. However, the plaintext and ciphertext are roughly the same size.

To decipher the ciphertext, we denote by T^H the inverse of matrix T in Hadamard sense i.e., a matrix satisfying the following relation:

$$T^H \odot T = \mathbf{1},$$

where every entry in the matrix is the unit of the group $\mathbb{G}_3$.

Upon receiving the ciphertext its decryption is performed in the reverse order and can be summarized by the following expression:

$$Dec(\{X, Y\}, C) = F^{-1}\left({}^{Y^{-1}}[(F(X))^H \odot F(C - X)]^{Y^{(-1)}}\right) - X.$$

Perfect secrecy of the presented block cipher and the statistical independency of the ciphertext C from the plaintext M is proven in [1].

In this paper we investigate the avalanche effect and BIC for the presented block cipher in a more general form i.e., we expand the cardinalities of the algebraic structures considered. In other words, we consider the Sylow group $\mathbb{G}_q$ of the multiplicative group $\mathbb{Z}_p^*$ and an additive group $\mathbb{Z}_q$. Hence in Eq. (4) we have $W, E \in Mat_m(\mathbb{G}_q)$ and $X, Y \in Mat(\mathbb{Z}_q)$. Actions in $\mathbb{G}_q$ are performed modulo a prime $p = 2q + 1$.

2. Computational results

The avalanche effect of perfectly secure Shannon cipher defined in Eq. (6) is calculated using Eq. (2). For each fixed pair of parameters $\{p, q\}$ we investigate the relation between avalanche effect and the matrix order m. We executed 1000 experiments and the results averaged for each value of m given the fixed pair $\{p, q\}$. In Table 1 we present the results of our experiments.

Table 1. Avalanche effect with different parameters

	$p = 7$, $q = 3$	$p = 23$, $q = 11$	$p = 107$, $q = 53$	$p = 4079$, $q = 2039$	$p = 33553799$, $q = 16776899$
$m = 5$	0.4446	0.4615	0.4922	0.5007	0.5001
$m = 8$	0.4447	0.4638	0.4919	0.5002	0.5004
$m = 10$	0.4451	0.4626	0.4910	0.4997	0.4999
$m = 15$	0.4450	0.4627	0.4911	0.4996	0.4998
$m = 16$	0.4448	0.4625	0.4921	0.5002	0.4995
$m = 32$	0.4442	0.4628	0.4921	0.4999	0.5000

Analyzing the obtained results, we see that as the parameter q gets larger the avalanche effect increases to 0.5 whereas the matrix order does not have such big of an impact.

We perform the investigation of the BIC in a way similar to the one presented above. As above we performed experiments for each triplet $\{p, q, m\}$ and using Eq. (4) obtained the BIC values presented in Table 2.

Table 2. BIC with the different parameters

	$p = 7$, $q = 3$	$p = 23$, $q = 11$	$p = 107$, $q = 53$	$p = 4079$, $q = 2039$	$p = 33553799$, $q = 16776899$
$m = 5$	1	0.7391	0.4717	0.2508	0.1731
$m = 8$	1	0.5746	0.4074	0.2035	0.1264
$m = 10$	1	0.5798	0.3738	0.1555	0.1099
$m = 15$	1	0.5678	0.3539	0.1214	0.0785
$m = 16$	1	0.5704	0.3436	0.1171	0.0667
$m = 32$	1	0.5530	0.3367	0.0782	0.0376

Note that increasing group size reduces BIC value. However, more importantly we see that small values of the parameter p are clearly not suitable for implementation since the value of BIC approaches the worst possible case. Furthermore, we can see that increasing matrix order has some impact as well and it is more noticeable compared to an analogous result of the analysis of the avalanche effect.

3. Conclusions

In this paper we investigated the previously proposed Shannon block cipher which does not require multiple rounds to encrypt a message. Furthermore, we expanded our research of the initial scheme by introducing a pair of parameters $\{p, q\}$ which makes our cipher more flexible as compared to the original. The obtained results show that even though no information about the plaintext is revealed by the encryption algorithm itself, small values of parameters q cannot be used in practice since the BIC fails even for the largest value of matrix order we considered. However, the avalanche criterion is mostly satisfied and is quite near perfection even for small values of q. Hence, relying on the results presented in Table 1 and Table 2, a good recommendation to choose the system parameters $\{p, q, m\}$ is to find a balance between q and m keeping them reasonably small while also ensuring that BIC is satisfied. Keeping this in mind a triplet $\{4079, 2039, 15\}$ can be considered a suitable choice for practical implementation.

References

[1] E. Sakalauskas, L. Dindienė, A. Kilčiauskas, and K. Lukšys, "Perfectly secure Shannon cipher construction based on the matrix power function," *Symmetry*, Vol. 12, No. 5, p. 860, May 2020, https://doi.org/10.3390/sym12050860

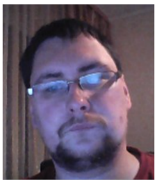
[2] Işıl Vergili, "Avalanche and bit independence properties for the ensembles of randomly chosen n × n S-Boxes," *Turkish Journal of Electrical Engineering Computer Sciences*, Vol. 9, No. 2, pp. 137–145, 2001.

[3] M. Salman, R. Yugitama, A., and R. F. Sari, "KAMIES: Security optimization of KASUMI algorithm by increasing diffusion level," *International Journal of Security and Its Applications*, Vol. 12, No. 3, pp. 29–46, May 2018, https://doi.org/10.14257/ijsia.2018.12.3.04

[4] L. Liu, "Designing a random S-box with the mixed spatiotemporal chaos," in *Conference series*, Vol. 1983, No. 1, 2021, https://doi.org/10.1088/1742-6596/1983/1/012040

[5] Sakalauskas Eligijus and Lukšys Kęstutis, "The matrix power function and its application to block cipher S-box construction," *International Journal of Innovative Computing, Information and Control*, Vol. 8, No. 4, pp. 2655–2663, 2012.

Matas Levinskas pursuing Master's degree of Applied Mathematics in Kaunas University of Technology. A member of Cryptography and Blockchain Technology research group.



Aleksejus Mihalkovich received Ph.D. degree in Kaunas University of Technology, in 2015. Since 2019 he is an Assist. Professor in the Department of Applied Mathematics and a member of Cryptography and Blockchain Technology research group. His current research interests include the cryptanalysis of symmetric and asymmetric cryptographic primitives.