Diffusion Analysis of F-function on KASUMI Algorithm

Rizki Yugitama, Bety Hayat Susanti, Magfirawaty
Crypto Engineering, Sekolah Tinggi Sandi Negara

Keywords:

KASUMI
F-function
Strict Avalanche Criterion (SAC)
Bit Independence Criterion (BIC)

ABSTRACT

There are several aspects and criteria that should be considered for designing Feistel block cipher, including: block size, key size, number of rounds, subkey generation algorithm, round function, fast software encryption/decryption, and ease of analysis. The function F is the heart of Feistel block ciphers. It provides confusion property that makes the relationship between ciphertext and encryption key as statistically complex as possible. One obvious property is that F must be nonlinear. The more non linear F, the more difficult any type of cryptanalysis be. KASUMI is the Feistel block cipher that used in UMTS, GSM, and GPRS mobile communication systems. F-function component of KASUMI composed of FI, FL, and FO functions.
In this paper, we analyzed the diffusion of F-function of KASUMI to determine its cryptographic strength using Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC). The SAC test result showed that FI-subfunction has smallest relative error. Whilst, the BIC test results show that FL-subfunction has a zero value.

Corresponding Author:

Bety Hayat Susanti
Sekolah Tinggi Sandi Negara,
Jalan H.Usa Putat Nutug, Ciseeng, Bogor, 16330.
Email: bety.hayat@lemsaneg.go.id

1. INTRODUCTION

KASUMI is a variation of the MISTY1 block cipher algorithm developed by the Security Algorithms Group of Experts (SAGE) as the basis of the A5/3 algorithm, which is used for GSM-based communication encryption algorithm. KASUMI operates on 64-bit input, using 128-bit key and produces 64-bit output. This algorithm will produce the output after eight times iteration. Operations that are used include: XOR, AND, OR, and bits rotation [1].

KASUMI algorithm has F-function with nonlinear property that makes it more strength. F-function of KASUMI decomposes into a number of subfunctions, namely FI, FO, and FL. FI is a left sub function of the FO. FI has a 16-bit input that divided into two parts: 9-bit to the left and 7-bit to the right. FO has a 32-bit input that divided to the left and the right side with the same size. FL subfunction has a 32-bit input that divided to the left and the right with the same size [1].

KASUMI become the standard algorithm for third generation of GSM communication [2]. Several attacks have succesfully conducted on KASUMI such as Boomerang and Sandwich attack performed by [3], but there is no detail description about the point of weaknesses. Since there is no detail description of KASUMI F-function testing from any literatures, we conducted research on the influence of diffusion level of F-function of KASUMI.

2. THEORETICAL BACKROUND

2.1. KASUMI Algorithm

KASUMI operates on 64-bit input, using a 128-bit key and a 64-bit output [1]. The input is divided into two 32-bit halves, left (L_0) and right (R_0). This operation will generate output after eight times iteration. The structure of KASUMI algorithm and its F-functions can be seen in [1].

2.2. F-functions of KASUMI

a. FI subfunction

Function FI is a sub function on the left side of FO [1]. The 16-bit input of FI is divided into two halves (L_0 and R_0), which L_0 is 9 bits wide and R_0 is 7 bits wide. FI used two S-boxes, i.e. S_7 that maps 7-bit

input to 7-bit output, and S_9 that maps 9-bit input. This function uses two additional functions, they are Zero Extend (ZE) function and Truncate (TR). ZE (x) take 7-bit input from x to turn it into a 9-bit by adding two bits of 0 (zero) in the MSB, while TR (x) took a 9-bit input of x, turn it into 7-bit by removing two bits on the MSB. It is operated as follows:

1) $L_1 = R_0$
2) $R_1 = S_9[L_0] \oplus ZE(R_0)$
3) $L_2 = R_1 \oplus KI_{i,j,}$
4) $R_2 = S_7[L_1] \oplus TR(R_1) \oplus KI_{i,j,1}$
5) $L_3 = R_2$
6) $R_3 = S_9[L_2] \oplus ZE(R_2)$
7) $L_4 = S_7[L_3] \oplus TR(R_3)$
8) $R_4 = R_3$

The results of this function are (L_4 || R_4) for 16-bit. FI structure can be seen in [1]. The decimal value of each element of S_7 and S_9 can be seen on [1].

b. FO and FL subfunction

FO subfunction

The 32-bit input I of FO is divided into two 16-bit halves [1].
$I = L_0 \,||\, R_0$
Two sets of subkeys, KO_i and KI_i, each measuring 48 bits is divided into three of the 16-bit subkey.
$KO_i = KO_{i,1} \,||\, KO_{i,2} \,||\, KO_{i,3}$
$KI_i = KI_{i,1} \,||\, KI_{i,2} \,||\, KI_{i,3}$
Every integer j with $1 \leq j \leq 3$ is defined :
$R_j = FI(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$
$L_j = R_{j-1}$
The function generate 32-bit output L_3 || R_3. FO structure can be seen in [1].

FL subfunction

The 32-bit input of I is divided into two 16-bit halves [1].
$I = L \,||\, R$
Subkey KL_i is divided into two parts.
$KL_i = KL_{i,1} \,||\, KL_{i,2}$
Then operated
$R' = R \oplus ROL(L \cap KL_{i,1})$
$L' = L \oplus ROL(R' \cup KL_{i,2})$
The function generate 32-bit output *L'* || *R'*. FL structure can be seen in [1].

2.3. Strict Avalanche Criterion (SAC)

Strict Avalanche Criterion (SAC) was introduced by Webster and Tavares in 1985 [4]. They said that $f : Z_2^n \rightarrow Z_2^m$ will satisfy the SAC if, whenever a single input bit is complemented, each of the output bits changes with a 50% probability. In other words, $f : Z_2^n \rightarrow Z_2^m$ will satisfy the SAC criterion if $\forall$ *i*, $1 \leq i \leq n$ satisfy the following equation :

$$\sum_{x \in Z_2^n} f(x) \oplus f(x \oplus c_i^n) = (2^{n-1}, 2^{n-1}, \dots, 2^{n-1}) \quad \text{..... (1)}$$

We can modify equation (1) to determine the parameter of SAC, K_{SAC}, as follows :

$$K_{SAC}(i,j) = \frac{1}{2} \omega t\left(f(x) \oplus f(x \oplus c_i^n)\right) = \frac{1}{2} \quad \text{..... (2)}$$

$K_{SAC}(i,j)$ in the *range* of [0,1] and can be interpreted as probability of a change in the j-th bit output when the i-th bit input change. If $K_{SAC}(i,j)$ is not equal to ½ for every pair of (*i*,*j*), then it is not satisfying SAC.

Relative error of SAC results can be obtained by the formula:

$$\in = \max_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} |2K_{SAC}(i,j) - 1)| \quad \text{.....(3)}$$

2.4. Bit Independence Criterion (BIC)

Bit Independence Criterion (BIC) was introduced by Webster and Tavares. A function $f : \{0,1\}^n \rightarrow \{0,1\}^m$ is to satisfy BIC if $\forall i, j, k \in \{1,2, \dots, n\}$, with $j \neq k$, inverting input bit i causes output bits j and k to change independently [5].

To measure the bit independence concept, one needs the correlation coefficient between the j'th and k'th components of the output difference string, which is called the avalanche vector a_i^{ei}. Bit independence parameter corresponding to the effect of the i'th input bit change on the j'th and k'th bits of a_i^{ei} is defined as:

$$BIC(a_j, a_k) = max_{1 \leq i \leq n} |corr\left(a_j^{ei}, a_k^{ei}\right)| \quad \text{..... (4)}$$

BIC parameter for function *f*or S-box is defined as

$$BIC(f) = \max_{\substack{1 \le j \le n \\ j=k}} BIC(a_j, a_k) \quad \text{..... (5)}$$

2.5. XOR Table

The XOR table of a *n* x *m* is a 2^n x 2^m matrix [4]. The rows of the matrix represent the change in the output of the S-box. An entry in the XOR table of an S-box indexed by (δ, *b*) indicates the number of input vectors P which, when changed from, result in the output difference of b. XOR value of an S-box is the highest value of the XOR table entries are defined by

$$b = f(P) \oplus f(P \oplus \delta)$$

The XOR table formula is given by : $XOR\ f(\delta, b) = \#\{P | f(P) \oplus f(P \oplus \delta) = b\}$ (6)
where $\delta \in Z_2^n$ and. $b \in Z_2^m$

2.6. Linear Approximation Table (LAT)

The robustness check of an S-box of a linear cryptanalysis can be seen from the value of LAT-distribution S-box or $f(x)$: $\{0,1\}^n \rightarrow \{0,1\}$. It can be done by making a linear function of S-box, each output or any combination of linear output can be formed with a linear function.

LAT distribution of an S-box function is defined as the sum of all variations of the input $X \in Z_2^n$ that caused value of the input bits are XOR-operated, α, equal to the value of the output bits are XOR-operated β [7]. Connor [7] explains the theory of LAT that if there is an S-box function $: Z_2^n \rightarrow Z_2^n$, that bijective with n-bit mapping, and if that bijective with n-bit mapping, and if S_{2^n} is the set of all mappings called group symmetrical.

Parameter testing criteria based on the results of LAT value [7] where:

$$LAT_\pi^{-}(\alpha, \beta) = | LAT_\pi(\alpha, \beta) - 2^{n-1} | \quad \text{..... (7)}$$

If the value of the LAT is far from ideal, 128, the S-box is increasingly vulnerable to linear cryptanalysis. On the table value of the LAT, will be counted as a linear approximation probability. The probability of less or more than half can be said there is a correlation between input and output so that it will be easy to cryptanalysis. Based on this, it can be concluded that the complexity of linear cryptanalysis depends on the values of entries in the LAT table [8].

2.7. Nonlinearity

According to [9], the nonlinearity of the function $f = (f_1 f_2 \dots f_n): Z_2^n \rightarrow Z_2^m$ where $f_i: Z_2^n \rightarrow Z_2$; *i* =1, 2, …, *m* is defined as the minimum Hamming distance between the set of Affine functions and every nonzero linear combination of the output coordinates of *f*, i.e.

$$\mathcal{NL}_f = \min_{b,c,w} \#\{x \in Z_2^n | c.f(x) \neq w.x \oplus b\} \quad \text{..... (8)}$$

where $w \in Z_2^n$, $c \in Z_2^m \backslash \{0\}$, $b \in Z_2$, and $w \cdot x$ denotes the dot product between *w* and *x* over Z_2,

$$c.f(x) = \bigoplus_{i=1}^{m} c_i f_i(x), \quad \text{..... (9)}$$

where $c = \{c_1, c_2, \dots, c_m\} \in Z_2^m$.

For a cryptosystem not to be susceptible to linear cryptanalysis, $\mathbf{NLM}_f$ is required to be as close as possible to its maximum value (perfect nonlinearity). The maximum nonlinearity value (perfect nonlinearity) of the Boolean function given by $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$ [6]. The minimum value of NLM_f is close to 0, indicating that the f function is approaching Affine function and vulnerable to linear cryptanalysis [10].

3. RESEARCH METHOD

This research will test the F-function of KASUMI using SAC and BIC. There are S-boxes on the FI subfunction, so we also do the S-box testing using SAC, BIC, XOR Table, LAT, and Nonlinearity. The research variables of S-box and F-function can be seen in Table 1. Due to limited time and computing resources, this research uses a sample to represent the population. We use probability sampling to determine simple random sample, where each population has an equal chance to be selected become the sample.

As seen in Table 2, the number of samples used in each F-function is 2^{12}. We determine the number of samples refer to the AES algorithm testing in [11]. The test results will be compared to each other to find out which one of the F-subfunctions that has a better diffusion rate.

Table 1. Research Variables

No	Testing	Object	Variable		
			Input		Output
			Independent	Control	Dependent
1.	SAC	$S_7$and S_9	S_7 and S_9 input	-	S_7 and S_9 output
		F-Function	F-Function input	Subkey	F-Function output
2	BIC	S_7 and S_9	S_7 and S_9 input	-	S_7 and S_9 output
		F-Function	F-Function input	Subkey	F-Function output
3	XOR Table	S_7 and S_9	S_7 and S_9 input	-	S_7 and S_9 output
4	LAT	S_7 and S_9	S_7 and S_9 input	-	S_7 and S_9 output
5	*Nonlinearity*	S_7 and S_9	S_7 and S_9 input	-	S_7 and S_9 output

Table 2. Number of samples on F-Function (*FL*, *FO* and*FI*)

No.	F-subfunction	Variable	Population (*N*)	Sample (*n*)
1.	*FL*	*FL* input	2^{32}	2^{12}
2.	*FO*	*FO* input	2^{32}	2^{12}
3.	*FI*	*FI* input	2^{16}	2^{12}

The F-function testing in this research is performed in two phases. The first phase is the sample generating in accordance with the population number of the independent variables specified for each F-subfunction. The margin of maximum relative error is 4%. When the input of F-function is treated as an independent variable then the key as the control variables are held constant with a value of zero. We use a constant zero value as a control variable in order to eliminate the influence of the control variables. The second phase is the sample test by conducting SAC and BIC. The results of SAC testing were presented in a matrix of percentage frequency of bit distribution as well as BIC testing results presented in the matrix of percentage distribution of the correlation coefficient of bits. After that, we analyze the matrix.

In this study, we also tested the S_7 and S_9 S-boxes which is one component of the FI subfunction in detail. Furthermore, we would do the S-box analysis based on S-box testing criteria. The Sbox testing criteria that will be evaluated including the SAC, BIC, XOR-Table, LAT, and Nonlinearity.

4. RESULTS AND ANALYSIS

4.1. S-box Testing

We can see in Table 3 that the minimum value of K_{SAC} of S_7 KASUMI is 0,5 and the maximum value is 0,5625. From Table 4, we can see that the maximum relative error value is 0,125, so the interval value ranging between $0{,}4375 \leq K_{SAC} \leq 0{,}5625$. Based on the result from Table 3 and Table 4, it can be concluded that the S_7 KASUMI does not satisfy the SAC criterion.

Table 3. SAC Value of S_7 KASUMI

ei	Bit position						
	1	2	3	4	5	6	7
1	0.5625	0.5	0.5	0.5	0.5	0.5	0.5
2	0.5	0.5	0.5	0.5625	0.5	0.5	0.5
3	0.5	0.5	0.5	0.5	0.5	0.5625	0.5
4	0.5	0.5	0.5	0.5	0.5	0.5	0.5625
5	0.5	0.5	0.5625	0.5	0.5	0.5	0.5
6	0.5	0.5	0.5	0.5	0.5625	0.5	0.5
7	0.5	0.5625	0.5	0.5	0.5	0.5	0.5

Table 4. SAC *Relative Error* Value of S_7 KASUMI

ei	Bit position						
	1	2	3	4	5	6	7
1	0.125	0	0	0	0	0	0
2	0	0	0	0.125	0	0	0
3	0	0	0	0	0	0.125	0
4	0	0	0	0	0	0	0.125
5	0	0	0.125	0	0	0	0
6	0	0	0	0	0.125	0	0
7	0	0.125	0	0	0	0	0

We can see from Table 5, that the minimum value of K_{SAC} of S_9 KASUMI is 0,5 and the maximum value is 1. From Table 6, we obtained that the maximum relative error value is 1, so the interval value of K_{SAC} ranging between $0 \leq K_{SAC} \leq 1$. Based on the results in Table 5 and Table 6, it can be concluded that S_9 KASUMI does not satisfy SAC criterion.

Table 5. SAC S_9 KASUMI Value

ei	Bit position								
	1	2	3	4	5	6	7	8	9
1	0,5	0,5	0,5	0,5	0,5	0,5	1	0,5	0,5
2	0,5	0,5	1	0,5	0,5	0,5	0,5	0,5	0,5
3	0,5	0,5	0,5	0,5	0,5	1	0,5	0,5	0,5
4	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5
5	0,5	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5
6	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5	0,5
7	0,5	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5
8	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1
9	0,5	0,5	0,5	0,5	0,5	0,5	0,5	1	0,5

Table 6. Relative Error Value SAC S_9 KASUMI Testing

ei	Bit position								
	1	2	3	4	5	6	7	8	9
1	0	0	0	0	0	0	1	0	0
2	0	0	1	0	0	0	0	0	0
3	0	0	0	0	0	1	0	0	0
4	1	0	0	0	0	0	0	0	0
5	0	0	0	0	1	0	0	0	0
6	0	0	0	1	0	0	0	0	0
7	0	1	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	1	0

Table 7. XOR Table Test Results of S_7 and S_9 KASUMI

S-box	**Total of entry**			
	0	**2**	**128**	**512**
S_7 KASUMI	8255	8128	1	0
S_9 KASUMI	131327	130816	0	1

At the XOR-Table test (see Table 7), it can be seen that the maximum entries generated by S_7 and S_9 KASUMI is 2. On S_7 KASUMI, this value indicates that there is 2 specific output difference value of 128 possibilities. The maximum probability of the S-box is $\frac{2}{128}$. For example in Table 7, S_7 KASUMI has the maximum value is 2 and the number of entries is 8128. It means there are 8128 input and output difference pairs that produces maximum output difference as much as 2 of the 128 possibilities and so on. The amount of the entry in the XOR Table shows the amount of possible input and output difference in S-box. The lower or minimum of the number of entries, it is easier to get the differential equation. So, it can be concluded that the differential cryptanalysis is not applicable to S_7 and S_9 KASUMI.

Table 8. LAT test results of S_7 and S_9 KASUMI

S-box	LAT value							
	56	**64**	**72**	**128**	**240**	**256**	**272**	**512**
S_7 KASUMI	4068	8255	4060	1	0	0	0	0
S_9 KASUMI	0	0	0	0	65416	131327	65400	1

Table 9. Minimum and Maximum LAT Value of S_7 and S_9 KASUMI

S-box	**Min**	**Max**	**LAT -64**	**LAT-64**	**LAT-256**	**LAT-256**
S_7 KASUMI	56	72	-8	8	0	0
S_9 KASUMI	240	272	0	0	-16	16

Based on Table 8 and Table 9, the extreme bias value obtained by S7 KASUMI is ranging between $-\frac{8}{128}$ to $\frac{8}{128}$. Then, it can be inferred that the S7 KASUMI has a value that is close to ideal LAT ranged from 56 to 72 and the bias value is $\pm\frac{8}{128}$ close to zero. While the bias value of S_9 KASUMI is ranging between $-\frac{16}{512}$ to $\frac{16}{512}$. Then it can be inferred that the S_9 KASUMI has a value that is close to ideal LAT ranged from 240 to 272 and the bias value is $\pm\frac{16}{512}$ close to zero. Therefore, S_7 and S_9 KASUMI are not susceptible to linear cryptanalysis.

Table 10. Nonlinearity Test Result of S_7 and S_9 KASUMI

S-box	***Nonlinearity Value***					
	56	**64**	**72**	**240**	**256**	**272**
S_7 KASUMI	8128	16256	8128	0	0	0
S_9 KASUMI	0	0	0	130816	261632	130816

Table 11. Nonlinearity Minimum Value of S_7 and S_9 KASUMI

S-box	**NLM(min)**	**Probability**
S_7 KASUMI	56	72/128
S_9 KASUMI	240	272/512

Based on the results of Table 11, it can be concluded that the minimum nonlinearity value of S_7 KASUMI is 56. The minimum value of the $\mathcal{NL}_f$ close to perfect nonlinearity value, i.e. $2^{n-1} - 2^{\frac{n}{2}-1} = 2^8 - 2^{\frac{7}{2}-1} = 58{,}3431$. Besides, the number of vectors in the minimum value of $\mathcal{NL}_f$ are 8128 vectors. Then, the number of inputs which satisfy the equation $c.f(x) = w.x \oplus b$ is 72. So, the probability result close to $\frac{1}{2}$, i.e. $\frac{72}{128}$.

4.2. Analysis of F-function

We can see from Table 12, that SAC test results of FL, FI and FO subfunctions with input as independent variable shows that FL, FI and FO are not satisfy SAC with the maximum relative error of FL value is 1. The minimum relative error is 0,0380 which is found in FI. FL, FI and FO subfunctions did not have a good diffusion properties as indicated by the largest error value that excess of 4%.

Table 11. SAC Test Results of F-function with Input as Independent Variable

F-Function	SAC Value	SAC Value (%)	Relative Error	Interval SAC Value	Description
FL	Min	0	1	$0 \leq k_{SAC}(i,j) \leq 100$	Failed
	Max	100	1		Failed
FI	Min	43,1396	0,1372	$43{,}13 \leq k_{SAC}(i,j) \leq 56{,}86$	Failed
	Max	51.9042	0,0380		Failed
FO	Min	43,0175	0,1396	$43{,}01 \leq k_{SAC}(i,j) \leq 56{,}98$	Failed
	Max	52.4902	0,0498		Failed

Based on Table 13, BIC test results of FL, FI and FO subfunctions with input as independent variable shows that FL is satisfy BIC, whilst FI and FO are not satisfy BIC with maximum value is 0,133 in FO. BIC minimum value is 0 in FL. So it can be stated that the avalanche variables of FL subfunction are independent. While the avalanche variables of FI and FO subfunctions are dependent.

Table 12. BIC Test results of F-Function with input as independent variable

F-Function	BIC Value	BIC Value (%)	Description
FL	Max	0	Passed
FI	Max	0,068	Failed
FO	Max	0,133	Failed

5. CONCLUSION

In this study, we conduct the KASUMI F-function testing using SAC and BIC in order to determine the level of diffusion, respectively. The result of SAC testing shows that FI-subfunction has smallest relative error. So, it can be stated that the FI-subfunction has a better rate of diffusion compared with FL and FO subfunctions. Whilst, the result of BIC testing shows that FL-subfunction has a zero value. Hence, it can be stated that the avalanche variable of FL-subfunction is independent. In future, further research needs to be done on the level of confusion in the KASUMI algorithm. It also needs to do more research on the implementation of algebraic attacks to determine the strength of the structure of KASUMI's F-function related to the level of diffusion and confusion.

REFERENCES

[1] ETSI/SAGE, "Specification of the 3GPP Confidentiality and Integrity Algorithms", Document 2: KASUMI Specification, 1999.
[2] S. Akleylek, "On The Avalanche Properties of MISTY1, KASUMI and KASUMI-R", Thesis, 2008.
[3] M.G. Mahmudhi, "Analisis Boomerang Attack, Sandwich Attack untuk Memecahkan Enkripsi Pengamanan Jaringan GSM 3G", Institut Teknologi Bandung, 2011.
[4] K. Kwangjo, "A Study on the Construction and Analysis of Substitution Boxes for Symmetric Cryptosystems", Yokohama: Division of Electrical and Computer Engineering, Yokohama National University, 1990.
[5] A.F. Webster and S.E. Tavares,"On the design of S-boxes", Department of Electrical Engineering, Queen's University, 1989.
[6] M.D.Yucel and I. Vergili, "Avalanche and Bit Independence Properties for the Ensembles of Randomly Chosen nxn S-boxes", EE Department of METU, Turkey,Turk J. Elec. Engin. Vol. 9 No. 2, 2001.
[7] L. O'Connor, "On Linear Approximation Tables and Cipher secure against Linear Cryptanalysis", ISRC-QUT Gardens Point, 1995.
[8] M. Matsui, "The First Experimental Cryptanalysis of the Data Encryption Standard", Advances in Cryptology - CRYPTO, 1994.
[9] A.M. Youssef, "Analysis and Design of Block Cipher", PhD Thesis, Queen's University, Canada, 1997.
[10] W. Meier and Othmar Staffelbach, "Nonlinearity Criteria for Cryptographic Function", Springer-Verlag Berlin Heidelberg, 1989.
[11] Deniz Toz, et.al., "Statistical Analysis of Block Cipher", 2006.

BIBLIOGRAPHY OF AUTHORS

	Rizki Yugitama is a student at Sekolah Tinggi Sandi Negara, Bogor. His interests are in mathematics, cryptography, and its related.
	Bety Hayat Susanti is a lecturer at Sekolah Tinggi Sandi Negara, Bogor. She obtained an undergraduate degree in Math and master's degree in Planning and Public Policy at University of Indonesia. Her interests are in mathematics, cryptography, and its related.
	Magfirawaty is a lecturer at Sekolah Tinggi Sandi Negara, Bogor. She obtained both undergraduate and master's degree in Physics at University of Indonesia. Her interests are in physics, cryptography, and its related.