Constructing an optimum 4×4 S-Box with quasigroup

G B Pambekti¹ and S Rosdiana²

¹Badan Siber dan Sandi Negara
²Politeknik Siber dan Sandi Negara

gigih.bagus@bssn.go.id, sri.rosdiana@poltekssn.ac.id

Abstract. The efficiency of cryptographic algorithms is a problem that is often encountered. One solution of this problem is the use of lightweight cryptography. S-Box is one of the basic nonlinear components in a cryptographic algorithm. Among all, 4×4 S-Box quasigroup is one kind of S-Box which can be used in lightweight cryptography, that formed by applying quasigroup transformation. The research described in this paper is the construction of the 4×4 S-Box using e-transformation of quasigroup as well as to know which leader pattern produces the highest number of optimum S-Box and mostly has higher Robustness value. The construction resulted in 6912 4×4 S-Boxes quasigroup by applying for each six leader patterns in four e-transformation rounds of 432 nonlinear quasigroups. The results of 4×4 S-Box quasigroup is calculated based on criteria of optimum 4×4 S-Box that has higher Robustness value. From all results of the 4×4 S-Box quasigroup, it is known that the leader pattern producing S-Box which meet the criteria and all S-Boxes have highest Robustness value are $l_1 l_2 l_1 l_2$ and $l_2 l_1 l_2 l_1$. The number of S-Box which meet the criteria is 18.75% of the total 5376 different 4×4 S-Boxes quasigroup and the highest Robustness value is 0.75.

1. Introduction

Issues and problems considering Big Data are increasing significantly in few decades earlier. As what defined by SAS in 2012, “Big Data” is a relative term describing a situation where the volume, velocity and variety of data exceed an organization’s storage or compute capacity for accurate and timely decision making [1]. The same year, [2] also defined Big Data as a term encompassing the use of techniques to capture, process, analyze and visualize potentially large datasets in a reasonable timeframe not accessible to standard IT technologies [2]. Facing both definitions, we know the “Big Data Dimension” ranges from Volume, Variety, Velocity, Variability, Value, and Complexity dimension of the data itself [1], [2].

Conditions and developments experienced by almost all organizations in the world [1]. The upcoming issues of Big Data are caused by none other than the rapidly developing technology, ranging from the number of transactions due to the density of online activities, social media activities, even the rise of smart phone usage which resulted in huge data production that occurs in minutes [1], [2]. That’s a lot of data, but it is the reality for many organizations. By some estimates, organizations in all sectors have at least 100 terabytes of data, many with more than a petabyte [1]. Speaking at a SAS webinar in
2011, Thornton May also said that many experts predict this number to double every six months going forward [1].

Like it or not, Big Data will also intensify the need for data quality and governance, for embedding analytics into operational systems, and for issues of security, privacy and regulatory compliance [1]. Everything that was problematic before will just grow even larger. Security is one of the most crucial success factors for all factors as the major challenge for a broader system using Big Data [2], [3].

Talking about security issues on Big Data, Intel in the year of 2014 stated that Security is essential to the deployment of Big Data application to protect sensitive data [4]. Yet knowing the needs of security on Big Data, cryptographic algorithm, which is one way to provide sensitive data protection, place heavy loads on the server and significantly slow application response times, especially in a new Big Data deployment [4]. Thus, we are facing the cryptographic algorithm efficiency problems.

One solution of this problem is the use of Lightweight Cryptography due its advantages in the efficiency of end-to-end communications and its applicability to lower resource devices[5]. Speaking of the use of Cryptography, one of the basic nonlinear components in cryptographic algorithm is S-Box [6].

In Lightweight Cryptography 4 × 4 S-Box is used rather than 8x8 S-Box used in AES as 4 × 4 S-Box proved to be more efficient [7]. S-Box that can withstand various attacks can be categorized as good S-Box. S-Box that can either be constructed with due regard to the method used when performing the construction. One method that can be used is to utilize a mathematical approach, such as quasigroup.

Quasigroup is one part of abstract algebra which can be applied in the world of cryptography. Quasigroup characteristics application considered to have advantages due its influence to give more efficient and safer impact [8]. Based on the transformation, quasigroup has four basic types of transformation. Those transformations are e-transformation, d-transformation, e' -transformation, and d' -transformation. Those transformations are widely known as basic quasigroup transformation. The basic transformation capable of providing an output string of n-length with n-length inputs. From those four types of transformation, e-transformation assessed to be able to show a good cryptographic property. This is because the e-transformation can increase the algebraic complexity and increase the Boolean functions degree, and simultaneously also provide value which is bijective to the generated values [9]. Thus the e-transformation can be applied iteratively or repeatedly in constructing the S-Box.

This research will discuss the implementation of e-transformation to form 4 × 4 S-Box quasigroup by including every possible input leader of order 4 with 2 leader values, namely l1 and l2, in six variants of the leader pattern. The e-transformation will be processed in four rounds.

Next, we checked the optimum S-Box criteria. Those criteria are, bijective, \( \text{Lin}(S) = \frac{1}{4} \), and \( \text{Diff}(S) = \frac{1}{4} \) [6]. Which is to calculate the linearity and differential of each S-Box in every pattern and determine which pattern produces the most S-Box that meet this criterion.

In this paper, there are several sections. Section II describes briefly the mathematical basis description associated with this research. Section III describes briefly the stages of research as a whole. Section IV contains the results of the research, and section V includes the conclusions of research undertaken.

2. Preliminaries Quasigroups, e-transformation, Bijective, Linearity, Differential and Robustness.

Assume \((Q, \cdot)\) as groupoid with a binary operation \( \cdot \) on a non-empty set \( Q \) and \( a, b \in Q \).

Definition 1 [8]. Groupoid is a finite set \( Q \) that has a binary operation \( \cdot \). Then for all \( a, b \in Q \), \( a \cdot b \in Q \). In other words, the value of the \( Q \) only has the properties covered in binary operation \( \cdot \).

Definition 2[10]. Quasigroup \((Q, \cdot)\) is a groupoid \( Q \) with binary operation \( \cdot \) which fulfills this condition: \((\forall u, v \in Q) (\exists! x, y \in Q)(x \cdot u = v \text{ and } u \cdot y = v)\).

In other word, \( x \cdot u = v \) and \( u \cdot y = v \) for all \( u, v \in Q \) has the unique solution \( x, y \) and \( Q \) is not an empty set. The unique solution can be denoted as \( x = v/u \) and \( y = u/v \). Two operations “/” (right division) and “\(\backslash\)" (left division) are defined on the set \( Q \) thus for \((Q,/)(Q,\backslash)\) are quasigroups [11].
From the uniqueness of the solution obtained, cancellation laws are applicable which is \( x \ast u = x \ast v \Rightarrow u = v, u \ast x = v \ast x \Rightarrow u = v \) which satisfy \((Q, \ast)\) and vice versa. Quasigroup formed can be represented in the Cayley table form.

Quasigroup can be associated with a Latin square. By eliminating quasigroup of order \( n \) the Cayley table border, which is the leftmost column and the topmost row, will result in a Latin square matrix of order \( n \). In other words the contents of the quasigroup Cayley table is a Latin square. So did the opposite when a Latin square of order \( n \) will be formed into a quasigroup, simply by adding a border to the Latin square to form a quasigroup of order \( n \).

The size of the quasigroup order \((Q, \ast)\) is the cardinal of \( Q \), which is denoted as \(|Q|\), from non-empty set \( Q \). A quasigroup \((Q, \ast)\) is said to be finite if it has a finite order as well. Thus, finite quasigroup can be defined as a finite groupoid for each element in the set \( Q \), certainly to be found exactly once or single in each row and each column in the Cayley table[9].

Example 1. Let \( Q = \{0, 1, 2, 3\} \), then one quasigroup formed in Cayley table is shown on Table 1.

| \* | 0   | 1   | 2   | 3   |
|----|-----|-----|-----|-----|
| 0  | 1   | 0   | 2   | 3   |
| 1  | 3   | 2   | 1   | 0   |
| 2  | 2   | 3   | 0   | 1   |
| 3  | 0   | 1   | 3   | 2   |

Table 1. Quasigroup with Order 4

Suppose that \( Q^r = \{a_1, a_2, \ldots, a_r \mid a_i \in Q, r \geq 2\} \) is the set of all finite strings with elements of \( Q \). Let \((Q, \ast)\) is a quasigroup, the fixed element \( l \in Q \) is the leader, then the e-transformation is expressed as follows:

\[
e_l(a_1, \ldots, a_r) = (b_1, \ldots, b_r)
\]

\[
\Leftrightarrow \begin{cases} 
  b_1 = l \ast a_1 \\
  b_i = b_{i-1} \ast a_i, 2 \leq i \leq r
\end{cases}
\]  

(1)

The graphical representation of an equation (1) is shown in Figure 1.

![Figure 1. e-transformation scheme [9].](image)

If there are several series of initial leader \( l_1, l_2, \ldots, l_k \) the implementation of e-transformation can be carried in a row. The composition of the e-transformation called combined quasigroup transformation. The combined transformation is obtained only from the composition of the e-transformation which is denoted as \( E \). We defined a joint transformation of e-transformation as follows:

\[
E = E_{l_k \ldots l_1}(k) = e_{l_k} \circ e_{l_{k-1}} \circ \ldots \circ e_{l_1}
\]  

(2)

Quasigroup with order \( 2^n \) can be represented as a Boolean function vector value \( f: \mathbb{F}_2^{2^n} \rightarrow \mathbb{F}_2^n \). This representation can be used to classify the finite quasigroup based on the polynomial degree and determine which quasigroup is linear or nonlinear. Let \( \mathbb{F}_2 = \{0, 1\} \) is a two-element field. Defined \( n \) variable Boolean function is \( f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \).

A Boolean function vector value is a mapping \( f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m \), with \( m \geq 2 \)[12]. Every Boolean function can be uniquely assigned to Algebraic Normal Form (ANF), which is a polynomial in \( n \) variables of the field \( \mathbb{F}_2 \) who has a degree \( \leq 1 \) in every single variable as follows:
\[ f(x_1, x_2, ..., x_n) = \sum_{i \subseteq \{1, ..., n\}} a_i x^i, \]  
(3)

with binomial \( x^i \) is the result of \( x^i = \prod_{t \in i} x_t \), \( x^\emptyset = 1 \), and \( a_i \in \mathbb{F}_2 \).

Every quasigroup \((Q, \ast)\) with order \( 2^n \) can be represented in Boolean function with the Boolean function value vector \( f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \). \( x \) and \( y \) variable is an element of quasigroup expressed as a binary vector \( x = (x_1, x_2, ..., x_n) \in \mathbb{F}_2^n \) and \( y = (y_1, y_2, ..., y_n) \in \mathbb{F}_2^n \). Then for every \( x, y \in Q \) expressed as follows:

\[
x \ast y \equiv f(x_1, x_2, ..., x_n)
= \left( f_1(x_1, x_2, ..., x_n), f_2(x_1, x_2, ..., x_n), f_3(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n) \right), \quad (4)
\]

with \( f_i = \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) is a component corresponding to \( f_i \). Let \((Q, \ast)\) is a quasigroup of order \( 2^n \) and

\[
f(x_1, x_2, ..., x_n) = (f_1(x_1, x_2, ..., x_n), ..., f_n(x_1, x_2, ..., x_n))
\]

is represented \((Q, \ast)\) which corresponds to a Boolean functions vector value. If the entire function of \( f_i \) for \( i = 1, 2, ..., n \) is a linear polynomial, then the quasigroup is also called a linear quasigroup.

Meanwhile, if there are \( f_i \) nonlinear functions for some \( i = 1, 2, ..., n \), then that quasigroup is referred to a nonlinear quasigroup [12].

Example 2. From Example 1, then the quasigroup with mapping function \( f: \mathbb{F}_2^3 \rightarrow \mathbb{F}_2^2 \) can be represented as \( f(x_1, x_2, x_3, x_4) = (x_1 + x_2 + x_3, 1 + x_1 + x_3 + x_1x_3 + x_2x_3) \). So, it is known that the quasigroup is nonlinear.

Definition 3. Function \( f \) is said to be one-one or injective if and only if \( f(x) = f(y) \), then \( x = y \) for \( x \) and \( y \) in the domain of \( f \).

Definition 4. Function \( f \) is said to be onto or surjective if and only if all elements \( y \in B \) with one element \( x \in A \), then \( f(x) = y \).

Definition 5. Function \( f \) is said to be bijective if the function satisfies one-one and onto mapping.

A Boolean function of \( n \) variables is a function \( f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \) and a boolean map is a map \( f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \). Suppose \( a = (a_0, a_1, ..., a_{n-1}) \) and \( b = (b_0, b_1, ..., b_{n-1}) \) with \( a, b \in \mathbb{F}_2^n \). The inner product of vectors \( a \) and \( b \) is defined by

\[
a \cdot b = \sum_{i=1}^{n} a_i b_i. \quad (6)
\]

To determine the linearity of a function, we need a tool which is able to calculate the linear. Walsh transformation is a tool that can be used to handle this case. Walsh transformation of \( 4 \times 4 \) S-Box can be calculated by the following equation [9].

\[
S^W(a, b) = \sum_{x \in \mathbb{F}_2^4} (-1)^{a \cdot x + b \cdot S(x)}, \quad (7)
\]

where \( a \in \mathbb{F}_2^4 \) and \( b \in \mathbb{F}_2^4 \). \( 4 \times 4 \) S-Box can be represented in Boolean mapping \( S: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4 \). The linearity of \( 4 \times 4 \) S-Box which is denoted by \( \text{Lin}(S) \), can be calculated as follows:

\[
\text{Lin}(S) = \max \left\{ \frac{1}{2^{2n}} \cdot |S^W(a, b)|^2 \big| (a, b) \in \mathbb{F}_2^4, (a, b) = 0 \right\}, \quad (8)
\]

with \( S^W \) is a Walsh transformation of the linear relation of the \( (a, b) \) pair, \( a \) is a part of the input value and \( b \) is a part of the output value of the S-Box.

Another approach for linearity is through a linear structure. It can be found by calculating the calculus difference. In cryptography, calculus difference is known as avalanche effect. Avalanche effect can be used to calculate the differential value of a S-Box.
Definition 6. Let \( f : \mathbb{F}_2^n \to \mathbb{F}_2^m \) be a Boolean mapping and \( u \in \mathbb{F}_2^n \). Then the differential mapping \( \Delta_u f : \mathbb{F}_2^n \to \mathbb{F}_2^m \) is:
\[
\Delta_u f(x) = f(x + u) - f(x), \text{ for all } x \in \mathbb{F}_2^n.
\] (9)

Definition 7[13]. Let \( f : \mathbb{F}_2^n \to \mathbb{F}_2^m \) be a Boolean mapping, the quantity \( \Omega_f \) is potential differential of \( f \), with \( \delta_f(u,v) \) defined as follow:
\[
\Omega_f = \max\{ \delta_f(u,v) | u \in \mathbb{F}_2^n, v \in \mathbb{F}_2^m \text{ and } (u,v) \neq 0 \}.
\] (10)

\[
\delta_f(u,v) = \frac{1}{2^n} \{\# \{x \in \mathbb{F}_2^n | \Delta_u f(x) = v\}\}.
\] (11)

In measuring the resistance against differential cryptanalysis to any S-Box, the differential of \( S \) can be defined as stated in Definition 8.

Definition 8. Let \( S \) be a S-Box with \( n \times m \) size and \( 2^n \) input value. Let \( \Delta_i \) as input difference, \( \Delta_o \) as output difference and \( \delta_s \) as
\[
\delta_s = \max \{\# \{x \in \mathbb{F}_2^n | S(x \oplus \Delta_i) - S(x) = \Delta_o, (\Delta_i, \Delta_o) \neq 0\}\},
\] (12)

\# is cardinal, thus the differential of \( S \) is \( \text{Diff}(S) = \frac{\delta_s}{2^n} \).

Based on Definition 8, then the equation for the \( 4 \times 4 \) S-Box is
\[
\delta_s = \max \{\# \{x \in \mathbb{F}_2^4 | S(x \oplus \Delta_i) - S(x) = \Delta_o, (\Delta_i, \Delta_o) \neq 0\}\},
\] (13)

then the differential of \( S \) is \( \text{Diff}(S) = \frac{\delta_s}{16} \).

Based on [14], we use the equations that used to calculate robustness values as follows:

Definition 9. A function \( f \) on \( V_n \) is said to be bent if
\[
2^{-\frac{n}{2}} \sum_{x \in V_n} (-1)^{f(x) \oplus \beta, x} = \pm 1,
\] (14)

for every \( \beta \in V_n \). Here \( x = (x_1, ... , x_n) \) and \( f(x) \oplus (\beta, x) \) is considered as a real valued function.

An \( n \times s \) S-Box is mapping from \( V_n \) to \( V_s \), where \( n \geq s \). Now we consider a nonlinearity criterion that measures the strength of a S-Box against differential cryptanalysis.

Definition 10. Let \( F = (f_1, ... , f_s) \) be an \( n \times s \) S-Box, where \( f_s \) is a function on \( V_n \), \( i = 1, ... , s \), and \( n \geq s \). Denote by \( L \) the largest value in the difference distribution table of \( F \), and by \( N \), the number of nonzero entries in the first column of the table. In either case the value \( 2^n \) in the first row is not counted. Then we say that \( F \) is \( R \)-robust against differential cryptanalysis, where \( R \) is defined by
\[
R = (1 - \frac{N}{2^n}) (1 - \frac{L}{2^n}),
\] (15)

Robustness gives more accurate information about the strength of a S-Box against the differential attack than differential uniformity does. The values of \( R \) in the range \([0,1]\), the higher Robustness value is, the more difficult differential cryptanalysis is to perform.

3. Research Stages
In achieving the objectives of this research, several steps are carried out as outlined below[15]:

- Forming quasigroup of order 4 and determine quasigroup of order 4 which are nonlinear.
- Constructing \( 4 \times 4 \) S-Box quasigroup uses e-transformation with six leader patterns and all possible values of the order four leaders.
- Checking the bijective of the entire S-Box generated in each leader pattern.
Calculating the linearity of the entire S-Box generated in each leader pattern.
Calculating the differential of the entire S-Box generated in each leader pattern.
Calculating the amount of the distribution of S-Box, which meet the criteria of optimum S-Box linearity and differential of each leader pattern.
Checking the number of different $4 \times 4$ S-Box quasigroup in each leader pattern.
Determining leader pattern which produce the highest number S-Box that meets the criteria of optimum $4 \times 4$ S-Box.
Calculating the amount of S-Box, which has the highest Robustness value of each leader pattern.

4. Result of Research
4.1. Constructing The S-Box
This study was to construct a quasigroup of order 4 in the form of $4 \times 4$ Latin square matrix as many as 576 pieces. From 576 pieces, there are 432 nonlinear quasigroup and 144 linear quasigroup as calculated using the ANF. Due to the S-Box is a nonlinear element, the construction process of the S-Box is only using nonlinear quasigroup. In experiments conducted for each leader pattern, there are 6912 $4 \times 4$ S-Box quasigroup generated from 432 nonlinear quasigroup used in e-transformation. Each of these nonlinear quasigroup is processed in the e-transformation with two leader values, namely $l_1$ and $l_2$, as many as 16 leader values which is a set of $\{0,1,2,3\}$. In the process of construction of a S-Box, e-transformation is performed by four rounds. For example, the construction of a S-Box can be seen in Example 3.

| Table 2. Quasigroup with Order 4 |
|----------------------------------|
| *  | 0 | 1 | 2 | 3 |
| 0  | 2 | 1 | 3 |   |
| 1  | 2 | 0 | 3 | 1 |
| 2  | 3 | 1 | 0 | 2 |
| 3  | 1 | 3 | 2 | 0 |

Example 3. Suppose we used two leader values, namely $l_1 = 1 = 01$ and $l_2 = 3 = 11$, with leader pattern $l_1^{-1}l_2^{-1}l_1l_2$. The used quasigroup is shown in Table 2. 1111 which is the binary representation of 0.1, ..., F. By applying the equation (1), then for each input can be done:

\[
\begin{align*}
  e_{01}(00,00) &= (10,11) \iff \begin{cases} 
    10 &= 01 \cdot 00 \\
    11 &= 10 \cdot 00 \\
    00 &= 11 \cdot 11 \\
    01 &= 00 \cdot 10 \\
  \end{cases} \\
  e_{11}(11,10) &= (00,01) \iff \begin{cases} 
    00 &= 01 \cdot 01 \\
    01 &= 00 \cdot 10 \\
  \end{cases} \\
  e_{01}(01,00) &= (00,00) \iff \begin{cases} 
    00 &= 00 \cdot 00 \\
    01 &= 11 \cdot 00 \\
    10 &= 01 \cdot 00 \\
  \end{cases} \\
  e_{11}(00,00) &= (01,10) \iff \begin{cases} 
    10 &= 01 \cdot 00 \\
    01 &= 00 \cdot 10 \\
    00 &= 11 \cdot 00 \\
  \end{cases} 
\end{align*}
\]

where swap is carried out in each end of the e-transformation process. The swap result is output to a round which was then used as input to the next round. After four rounds, the output= 1001 = 9. Thus the results of the e-transformation of the input = 0000 = 0 is 9. The process can be represented in graphical form as shown in Figure 2, and so on is done for other inputs in order to obtain the results of S-Box just as shown in Table 3.
Table 3. S-Box Construction Results

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S(x)$ | 9 | 5 | 1 | D | C | 8 | 0 | 4 | 2 | 6 | A | E | 7 | B | 3 | F |

Figure 2. The graphical representation of e-transformation

4.2. Analysis
Considering the impact of e-transformation is bijective, then bijective checking is carried out against the entire 4 × 4 S-Box quasigroup generated in each leader pattern. This research has shown that the entire S-Box in each leader pattern is bijective.

Table 4. Results of Linearity

| Pattern | $\text{Lin}(S)$ | Total |
|---------|-----------------|-------|
| $l_1l_1l_2l_2$ | 1158 3072 2682 6912 |
| $l_1l_2l_2l_1$ | 1152 3072 2682 6912 |
| $l_2l_1l_1l_2$ | 1152 3072 2682 6912 |
| $l_2l_1l_2l_1$ | 1156 3072 2682 6912 |
| $l_2l_2l_2l_1$ | 1158 3072 2682 6912 |

This research is checking linearity and differential calculations of the entire S-Box for each leader pattern. But before that, this research also does linearity and differential calculations separately. It aims to find out how many S-Box distribution in every leader pattern that meet the conditions of the optimum 4 × 4 S-Box linearity and how many S-Boxes which meet the conditions of optimum 4 × 4 S-Box differential.

Table 5. Differential Result of Each Leader Pattern

| Pattern | $\text{Lin}(S)$ | Total |
|---------|-----------------|-------|
| $l_1l_1l_2l_2$ | 80 2072 408 2560 1280 512 6912 |
| $l_1l_2l_1l_2$ | 80 2176 432 2304 1536 384 6912 |
| $l_1l_2l_2l_1$ | 80 2184 616 2496 1024 512 6912 |
| $l_2l_1l_1l_2$ | 80 2184 616 2496 1024 512 6912 |
The linearity criteria is still the same, namely 1158 units. The highest producer of the S-Box which meets the optimum linearity criteria is the $l_1 l_2 l_2 l_1$ pattern and $l_2 l_2 l_1 l_1$ as many as 1158 of the total 6912 S-Boxes.

### Table 6. Number of S-Box, which is Different for Every Leader Pattern

| Pattern       | Total Different S-Boxes |
|---------------|--------------------------|
| $l_1 l_2 l_2 l_2$ | 6096                     |
| $l_1 l_2 l_2 l_1$ | 5376                     |
| $l_1 l_2 l_1 l_1$ | 6048                     |
| $l_2 l_1 l_1 l_2$ | 6048                     |
| $l_2 l_1 l_1 l_1$ | 5376                     |
| $l_2 l_2 l_1 l_1$ | 6096                     |

In the calculation of the differential criteria, the calculation is performed using equation (8) so that differential values distribution for each leader pattern is obtained as shown in Table 4. Table 4 shows that the highest producer of the S-Box which meets the optimum differential criteria is the $l_1 l_2 l_2 l_1$ pattern and $l_2 l_2 l_1 l_1$ as many as 2184 of the total 6912 S-Boxes.

### Table 7. Different S-Box Linearity Results

| Pattern       | $\text{Lin}(S)$ |
|---------------|-----------------|
| $l_1 l_2 l_2 l_2$ | 1158 3072 1866 6096 |
| $l_1 l_2 l_2 l_1$ | 1156 2304 1916 5376 |
| $l_1 l_2 l_1 l_1$ | 1152 3072 1824 6048 |
| $l_2 l_1 l_2 l_2$ | 1152 3072 1824 6048 |
| $l_2 l_1 l_1 l_1$ | 1156 2304 1916 5376 |
| $l_2 l_2 l_1 l_1$ | 1158 3072 1866 6096 |

### Table 8. Differential of Different S-Box on Every Leader Pattern

| Pattern       | $\text{Lin}(S)$ |
|---------------|-----------------|
| $l_1 l_1 l_1 l_2$ | 80 2072 408 2560 736 240 6096 |
| $l_1 l_2 l_1 l_2$ | 80 1944 408 1024 1024 128 5376 |
| $l_1 l_2 l_1 l_1$ | 80 2184 616 2496 448 224 6048 |
| $l_2 l_1 l_1 l_2$ | 80 2184 616 2496 448 224 6048 |
| $l_2 l_1 l_1 l_1$ | 80 1944 408 1792 1024 128 5376 |
| $l_2 l_2 l_1 l_1$ | 80 2072 408 2560 736 240 6096 |

This research does not stop here. Furthermore, to make sure the leader pattern is the real expected pattern, then an examination of the 6912 generated S-Box is conducted on each pattern. The fact found that from 6912 the produced S-Box, it turns out not all of them are different S-Box. There are several S-Boxes which are the same in each leader pattern. The number of different S-Box can be seen in Table 6. By knowing the incident, this research re-calculate the linearity distribution from a number of different S-Box. Thus the result is shown in Table 7. It is seen that the number of S-Box which meets the linearity criteria is still the same, namely 1158 units. But if we look at Table 6 it is stated that the number of different S-Box is not 6912, then the resulting percentage will be likely different. Therefore,
the percentage calculation is carried out. Based on the calculations performed, the percentage obtained as follows: \( l_1l_2l_3l_4 \) and \( l_2l_1l_3l_4 \) pattern as much as 18,99606%, \( l_1l_2l_1l_2 \) and \( l_2l_1l_2l_1 \) pattern as much as 21,50297%, and \( l_1l_2l_1l_4 \) and \( l_2l_1l_1l_2 \) pattern as much as 19,04761%. Thus, the expected pattern leader is \( l_1l_2l_1l_2 \) and \( l_2l_1l_2l_1 \) because it produces the highest number of S-Box which meets the linearity criteria.

**Table 9. Number of Different S-Box, which Satisfy S-Box Optimum Criteria**

| Leader Pattern | Total Optimum S-Boxes | Total S-Boxes | Percentage   |
|----------------|-----------------------|---------------|--------------|
| \( l_1l_1l_2l_2 \) | 976                   | 6096          | 16,01049 %  |
| \( l_1l_2l_1l_2 \) | 1008                  | 5376          | 18,75 %     |
| \( l_1l_2l_2l_1 \) | 1008                  | 6048          | 16,66667 % |
| \( l_2l_1l_1l_2 \) | 1008                  | 6048          | 16,66667 % |
| \( l_2l_1l_2l_1 \) | 1008                  | 5376          | 18,75 %     |
| \( l_2l_2l_1l_1 \) | 976                   | 6096          | 16,01049 %  |

In the same way, the calculation of the differential criteria is also carried out with the results in Table 8. The percentage obtained as follows: \( l_1l_2l_1l_2 \) and \( l_2l_2l_1l_1 \) pattern as much as 33,989501%, \( l_1l_2l_1l_2 \) and \( l_2l_2l_1l_1 \) pattern as much as 36,160714%, and \( l_1l_2l_1l_2 \) and \( l_2l_1l_1l_2 \) pattern as much as 36,111111%. So, the expected pattern leader is \( l_1l_2l_1l_2 \) and \( l_2l_1l_1l_2 \) because it produces the highest number of S-Box which meets the differential criteria.

This research is looking for a leader pattern that produces \( 4 \times 4 \) S-Box that meet the optimum criteria. A S-Box meets the optimum condition when bijective, the linearity value is \( Lin(S) = \frac{1}{4} \), and the differential value is \( Diff(S) = \frac{1}{4} \). Therefore, in Table 9, we calculate all of its aspects. It was obtained that percentage obtained as follows: \( l_1l_1l_2l_2 \) and \( l_2l_2l_1l_1 \) pattern as much as 16,01049%, \( l_1l_2l_1l_2 \) and \( l_2l_1l_1l_2 \) pattern as much as 18,75%, and \( l_1l_1l_2l_2 \) and \( l_2l_1l_1l_2 \) pattern as much as 16,66667%. We can conclude that \( l_1l_2l_1l_2 \) and \( l_2l_1l_1l_2 \) is the most pattern which produce the highest optimum \( 4 \times 4 \) S-Box quasigroup.

In the calculation of Robustness value. The calculation is performed using equation (15) so that Robustness values for each leader pattern is obtained as shown in Table 10. Here is the number of S-Boxes that meet the optimum conditions for each leader pattern.

**Table 10. Number of Different S-Box, Based on Highest Robustness Value (0.75)**

| Leader Pattern | Total Optimum S-Boxes | The Highest Robustness Value (0.75) | Percentage   |
|----------------|-----------------------|-------------------------------------|--------------|
| \( l_1l_1l_2l_2 \) | 976                   | 624                                 | 63,9344 %    |
| \( l_1l_2l_1l_2 \) | 1008                  | 1008                                | 100 %        |
| \( l_1l_2l_1l_1 \) | 1008                  | 624                                 | 61,9048 %    |
| \( l_2l_1l_1l_2 \) | 1008                  | 624                                 | 61,9048 %    |
| \( l_2l_1l_2l_1 \) | 1008                  | 1008                                | 100 %        |
| \( l_2l_2l_1l_1 \) | 976                   | 624                                 | 63,9344 %    |

5. Conclusion

Based on the results obtained, the research produces the \( 4 \times 4 \) S-Box quasigroup in total as many as 6912 S-Boxes for each leader pattern. From the six applied leader patterns, it is obtained leader pattern which is able to produce the \( 4 \times 4 \) S-Box quasigroup that meet the criteria of the optimum S-Box. Those leader patterns are \( l_1l_2l_1l_2 \) and \( l_2l_1l_1l_2 \), which is as many as 1008 from 5376 S-Box or 18,75% from different \( 4 \times 4 \) S-Box quasigroup. Then calculate the Robustness value of each leader pattern, and we get leader patterns are \( l_1l_2l_1l_2 \) and \( l_2l_1l_2l_1 \) with each value is 0.75. From six leader patterns this value
is the highest. So, the application of quasigroup in constructing the $4 \times 4$ S-Box is proven able to produce optimum and robust $4 \times 4$ S-Box, especially by using $l_1l_2l_2l_1$ and $l_2l_1l_2l_1$ patterns.

References
[1] SAS 2012 Big data meets big data analytics Sas February 2016.
[2] NESSI 2012 Big data a new world of opportunities NESSI-Big Data White Paper.
[3] Labrinidis A and Jagadish H V 2012 Challenges and opportunities with big data Proc. VLDB Endow. 5 2032–2033.
[4] Intel 2014 Strong security with high performance for real-time, Big Data Deployments.
[5] Katagi M 2011 Lightweight cryptography for the internet of things.
[6] Mihajloska H and Gligoroski D 2012 Construction of optimal 4-bit S-boxes by quasigroups of order 4 in SECURWARE 2012 - 6th International Conference on Emerging Security Information, Systems and Technologies.
[7] Wu W and Zhang L 2011 LBlock: A lightweight block cipher in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6715 LNCS.
[8] Shcherbacov V A 2003 Elements of quasigroup theory and some its applications in code theory and cryptography.
[9] Mihajloska H D 2011 Analysis and construction of optimal 4-Bit S-Boxes for Block Ciphers with Quasigroups-Master Thesis-Skopje.
[10] Blass A Burris S and Sankappanavar H P 1984 A course in Universal Algebra. The American Mathematical Monthly 91, 1.
[11] Markovski S and Bakeva V 2017 Quasigroup string processing: Part 4 Contributions, Section of Natural, Mathematical and Biotechnical Sciences 27, 1–2.
[12] Gligoroski D Dimitrova V and Markovski S 2009 Quasigroups as Boolean Functions, Their Equation Systems and Gröbner Bases, in Gröbner Bases, Coding, and Cryptography, (Berlin, Heidelberg: Springer Berlin Heidelberg).
[13] Nyberg K 1994 Differentially uniform mappings for cryptography in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 765 LNCS.
[14] Seberry J Zhang X M and Zheng Y 1994 Pitfalls in designing substitution boxes in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 839 LNCS.
[15] Pambekti G B 2015 Penerapan Quasigroup dalam mengonstruksi S-Box $4 \times 4$, Bogor.