Research Journal of Applied Sciences 11 (11): 1324-1327, 2016
ISSN: 1815-932X

Comparative TOPSIS of Speed Analysis of the Crypto Algorithm Establishment

Cheng Hsiung Liu and Chun Wei R. Lin
Department of Business Administration, Asia University Taichung, Taichung, Taiwan

Abstract: In 2014, Sundar and Narayan study quantum cryptography to simulate the voting in C++ language written DES, 3DES, AES, BF, TF, SERP, RSA1, RSA2, to process the speed analysis through input size. They find that RSAl was the fastest but they did not clearly explain. This study helps explain the part that Sundar and Narayana didn't clearly explain by TOPSIS of speed analysis quantitative data analysis. Therefore, the paper is to aim at Sundar and Narayana speed analysis of cryptographic algorithms input size data with comparative TOPSIS of speed analysis by building the model of comparative TOPSIS of speed analysis. This study, comparative TOPSIS of speed analysis by quantization and description in data interpretation, found that DES is the fastest, followed by the sequential order of RSA1, AES, TF, BF, RSA2, SERP, 3DES, etc. which highlights the importance, value and contribution of this study.

Key words: TOPSIS, crypto algorithm, speed analysis, quantum cryptography, DES

INTRODUCTION

In 2014, Sundar and Narayan provided quantum cryptography to simulate voting, using C++ language along with the Crypto++ library in the simulation speed analysis of DES, 3DES, AES, BF, TF, SERP, RSA1, RSA2 cryptographic algorithms, by quantum key input size be simulation analysis for the implementation of the encryption algorithm (encryption and decryption jointly) substantial data transfer destination (Sundar and Narayan, 2014). They find that RSA1 (2046 bit key) was among the fastest but they did not clearly explain. Therefore, this study processes comparative TOPSIS of speed analysis quantitative data analysis and explanation by building the model of comparative TOPSIS of speed analysis which highlights the importance and value and contribution of this study.

Literature review

Cryptographic algorithms speed analysis: In 2014, Sundar and Narayan study quantum cryptography to simulate voting, using C++ language along with the Crypto++ library for the implementation to transfer the encryption algorithm data to destination, simulates the original vote Input size (Sundar and Narayan, 2014). Although, it's not stored in the voting machine, it won't pose a risk of info leaking in actually sending to the specified location which safely carries out speed analysis.

Topsis: In 1980, Yoon and Hwang University provided a multi-method assessment quasi decision-making in Kansas State, called TOPSIS "Technique for Order Preference by Similarity to Ideal Solution" which was designed to help policy makers deal with multi-selection program, when standard of each criterion and each program performance assessment was known. As the following explained: ideal solution: alternative scenarios based on input size guidelines by sec max value. Negative ideal Solution: alternative scenarios based on input size guidelines by sec min value. In this study, the smallest data of guidelines for the interest's face value alternatives is "the shortest distance from the ideal solution" and "the farthest from the negative ideal solution". Assumed that every criterion has a standard of decreasing effects (Kittur, 2015; Mokhtar *et al*., 2015; Li *et al*., 2015; Yan *et al*., 2014).

MATERIALS AND METHODS

Comparative TOPSIS of speed analysis model and case study: This case study is based on the Sundar and Narayan voting scheme using C++ language along with the Crypto++ library in the Input size (bytes) and speed analysis of DES, 3DES, AES, BF, TF, SERP, RSA1, RSA2 cryptographic algorithms (Sundar and Narayan, 2014).

Assumed that this research program was known as the following described (Kittur, 2015; Mokhtar *et al*., 2015; Li *et al*., 2015; Yan *et al*., 2014): Decision matrix establishment Rn×m (Table 1):

$$R = \left[r_{ij} \right]_{m \times n} \quad (1)$$

Corresponding Aouther: Cheng Hsiung Liu, Department of Business Administration Asia University Taichung, Taichung, Taiwan

Table 1: Cryptographic algorithms speed analysis (Sundar and Narayan, 2014)

Titles	Years	Algorithm	Full name	Definition
DES	1976	IBM	Data encryption algorithm	This symmetric key algorithm is to be most widely used by early DES
3DES	1998	ANS X9.52	Triple data encryption algorithm	To use algorithms, in accordance with encryption-decryption-encryption in 3 DES
AES by	2001	NIST	Advanced encryption standard	AES, encryption algorithms, was adopted the US federal government. It has been widely used globally now a days
BF	1993	Bruce schneider	Blowfish	Blowfish is a symmetric encryption algorithm, which has been applied in variety products
TF			Trans flash	Trans flash, also called secure digital (Secure Digital memory card) is a Memory card
RSA RSA 1 RSA2	1977	Ron Rivesti Adi Shamir Leonard Adleman		RSA encryption algorithm is an asymmetric encryption algorithm

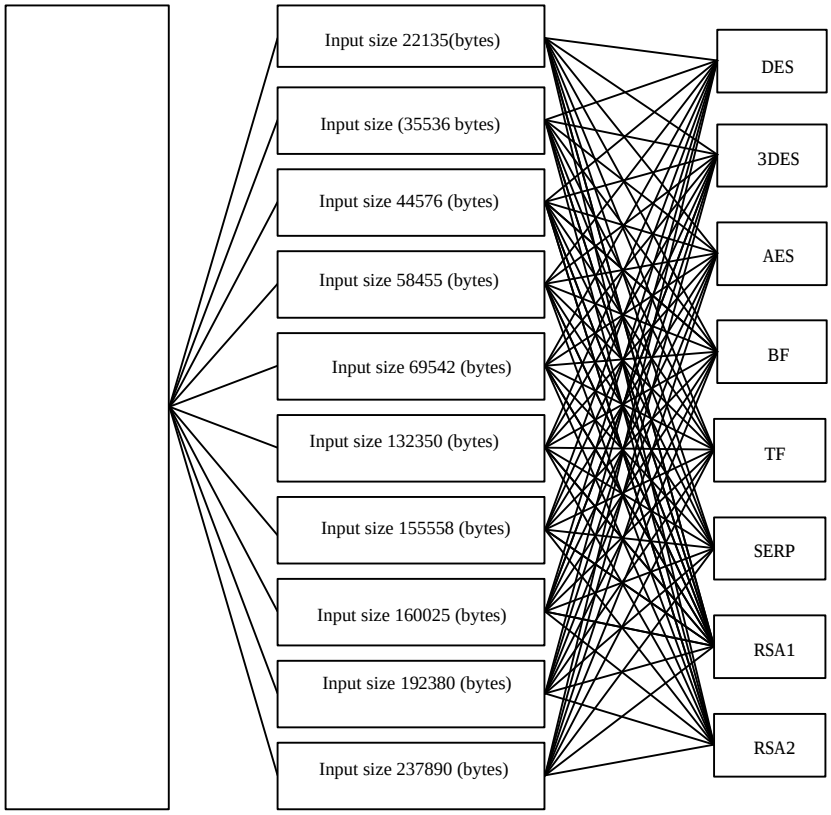

Fig. 1: Decision matrix establishment

There's a best solution to multi-objective problem. In the process, there are evaluation targets as n×m matrix (Fig. 1):

$$R = \begin{bmatrix} x_{11} & \cdots & x_{1j} & \cdots & x_{1jn} \\ \vdots & & \vdots & & \vdots \\ x_{i1} & \cdots & x_{ij} & \cdots & x_{in} \\ \vdots & & \vdots & & \vdots \\ x_{m1} & \cdots & x_{mj} & \cdots & x_{mn} \end{bmatrix} = \begin{bmatrix} R_1(x_1) \\ \vdots \\ R_i(X_j) \\ \vdots \\ R_m(X_n) \end{bmatrix} \quad (2)$$

$$= \left[X_1(x_1), \cdots, X_j(x_i), \cdots, X_n(x_m) \right]$$

the calculation of weight matrix (Table 2):

$$W_1 = \frac{x_1}{\sum x_{ij}} \quad (3)$$

$$\sum w_i = 1 \quad (4)$$

The calculation of normalized evaluation value calculation:

Table 2: W weight

Input size (bytes)	W (%)
22135 (132350)	1.9900 (11.930)
35536 (155558)	3.2000 (14.030)
44576 (160025)	4.0200 (14.430)
58455 (192380)	5.2700 (17.400)
69542 (237890)	6.2800 (21.450)

Table 3: The Z_{ij} values (Time, sec)

Input size (bytes)	DES	3DES	AES	BF	TF	SERP	RSA1	RSA2
22135	0.0034	0.0099	0.0058	0.007	0.0060	0.0086	0.0048	0.0084
35536	0.0035	0.0099	0.0059	0.007	0.0060	0.0086	0.0047	0.0084
44576	0.0035	0.0099	0.0059	0.007	0.0061	0.0086	0.0047	0.0084
58455	0.0035	0.0100	0.0059	0.007	0.0060	0.0086	0.0047	0.0083
69542	0.0035	0.0099	0.0059	0.007	0.0060	0.0085	0.0049	0.0083
132350	0.0035	0.0100	0.0059	0.007	0.0060	0.0086	0.0047	0.0083
155558	0.0035	0.0100	0.0059	0.007	0.0060	0.0086	0.0047	0.0083
160025	0.0035	0.0100	0.0059	0.007	0.0060	0.0086	0.0047	0.0083
192380	0.0035	0.0100	0.0060	0.007	0.0060	0.0086	0.0047	0.0083
237890	0.0035	0.0100	0.0059	0.007	0.0060	0.0086	0.0047	0.0083

Table 4: Positive ideal solution I* value

Input size (bytes)	I*
22135 (132350)	0.0034 (0.0035)
35536 (155558)	0.0035 (0.0035)
44576 (160025)	0.0035 (0.0035)
58455 (192380)	0.0035 (0.0035)
69542 (237890)	0.0035 (0.0035)

Table 5: Negative ideal solution I- value

Input size (bytes)	I-
22135 (132350)	0.0099 (0.0100)
35536 (155558)	0.0099 (0.0100)
44576 (160025)	0.0099 (0.0100)
58455 (192380)	0.0100 (0.0100)
69542 (237890)	0.0099 (0.0100)

Table 6: Positive ideal solution Y* value of Euclidean distance

DES Y*	3DES	AES	BF	TF	SERP	RSA1	RSA2
0.0000	0.0204	0.0075	0.0110	0.0080	0.0161	0.0039	0.0153

Table 7: Ideal solution Y-value of Euclidean distance

Y-DES	3DES	AES	BF	TF	SERP	RSA1	RSA2
0.0204	0.0000	0.0129	0.0094	0.0124	0.0043	0.0165	0.0051

$$r_{ij} = x_{ij} \Big/ \sqrt{\sum_{i=1}^{m} x_{ij}^2} \tag{5}$$

The calculation of evaluate normalized weighted value (Table 3):

$$z_{ij} = w_{ij} \times r_{ij_z} \tag{6}$$

The decision of positive ideal solution I* and negative ideal solution I- (Table 4and 5):

$$I^* = \{z1^*, z2^*, zn^*\} \tag{7}$$

$$I^- = \{z1^-, z2^-, zn^-\} \tag{8}$$

To calculate positive ideal solution Y* and negative ideal solution Y- of Euclidean distance (Table 6and 7).

$$Y^* = \sqrt{\sum_{j=1}^{n} (z_{ij} - z_{ij}^*)^2} \tag{9}$$

$$Y^- = \sqrt{\sum_{j=1}^{n} (z_{ij} - z_{ij}^-)^2} \tag{10}$$

To calculate every alternative scheme for the relative similarity of ideal solution (Table 8):

$$K_i^* = \frac{Y^*}{Y^* + Y^-}; \quad 0 \times K_i^* 1 \tag{11}$$

To rank K_i^* values according to the formula of $0 \times K_i^* 1$ The study found that TOPSIS calculus Ki* values from the min-max order:

- (1) DES is 0.00, (2) RSA1 is 0.10, (3) AES is 0.37, (4) TF is 0.39, (5) BF is 0.54, (6) RSA2 is 0.75, (7) SERP is 0.79, (8) 3DES is 1
- The difference between the maximum and minimum of K_i^* values is 1
- Among all, the difference between AES and TF is 0.02 and the other two, the difference between RSA2 and SERP is 0.02
- The study found K_i^* values plotted radar chart (Table 8 and Fig. 2)

The study found that the K value, ranking from min to max, is our best solution. DES is the fastest, following by RSA1, AES, TF, BF, RSA2, SERP, 3DES. The result is't also matches the study by Sundar and Narayan which highlights the importance and value and contribution of this study as Table 7 and 8.

Table 8: K_i^* value

Ki*DES	3DES	AES	BF	TF	SERP	RSA1	RSA2
0.00	1.00	0.37	0.54	0.39	0.79	0.19	0.75

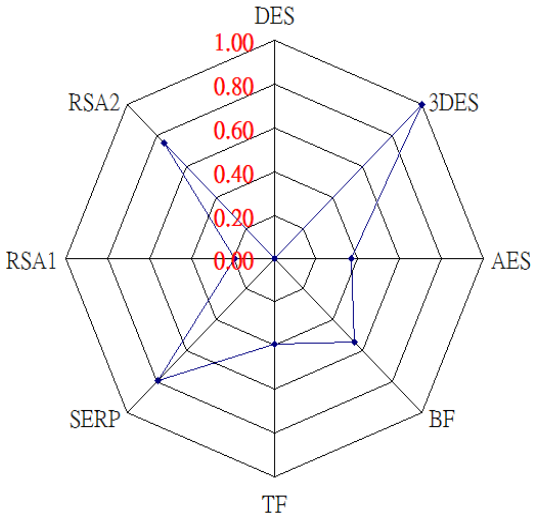

Fig. 2: K_i^* plotted radar chart

CONCLUSION

The summary of this study is as following:

- The study built the model of comparative TOPSIS of speed analysis
- (1) DES is 0.00, (2) RSA1 is 0.10, (3) AES is 0.37, (4) TF is 0.39, (5) BF is 0.54, (6) RSA2 is 0.75, (7) SERP is 0.79, (8) 3DES is 1
- The study found K_i^* values plotted radar chart that DES is 0.00 the fastest and 3DES is the 1 the slowest
- Assumed that it takes longer because 3DES encryption requires three calculations which use algorithms, in accordance with encryption decryption encryption in 3 DES
- The study found that DES is the fastest, following by RSA1, AES, TF, BF, RSA2, SERP, 3DES. The result isn't also matches the study by Sundar and Narayanwhich highlights the importance and value and contribution of this study
- This study helps explain the part that Sundar and Narayana didn't clearly explain by TOPSIS of speed analysis quantitative data analysis

This study highlights the importance and value and contribution of this study.

REFERENCES

Kittur, J., 2015. Using the promethee and topsis multi-criteria decision making methods to evaluate optimal generation. Proceeding of the 2015 International Conference on Power and Advanced Control Engineering (ICPACE), August 12-14, 2015, IEEE, Hubli, India, ISBN:978-1-4799-8371-1, pp: 80-85.

Li, X.Z., Y.L. Gao and H.L. Zhao, 2015. Comparative research on the IOT industry competitiveness of eastern, central and western China-a comprehensive evaluation based on TOPSIS and GRA. Proceeding of the 2015 IEEE International Conference on Grey Systems and Intelligent Services, August 18-20, 2015, IEEE, Beijing, China, ISBN:978-1-4799-8375-9, pp: 187-193.

Mokhtar, M.R., M.P. Abdullah, M.Y. Hassan and F. Hussin, 2015. Combination of AHP-PROMETHEE and TOPSIS for selecting the best Demand Side Management (DSM) options. Proceeding of the 2015 IEEE Student Conference on Research and Development (SCOReD), December 13-14, 2015, IEEE, Johor Bahru, Malaysia, ISBN:978-1-4673-9572-4, pp: 367-372.

Sundar, D.S. and N. Narayan, 2014. A novel voting scheme using quantum cryptography. Proceeding of the IEEE Conference on Open Systems (ICOS), October 26-28, 2014, IEEE, Chennai, India, ISBN:978-1-4799-6367-6, pp: 66-7.

Yan, Z., Z. Weige, X.S. Bing, Z. Fangdan and Z. Man, 2014. The application of TOPSIS in the study of the comprehensive performance of lithium-ion power battery. Proceeding of the IEEE Conference on Expo Transportation Electrification Asia-Pacific (ITEC Asia-Pacific), August 31-3 September, 2014, IEEE, Beijing, China, ISBN: 978-1-4799-4239-8, pp: 1-4.