Universiti Malaysia PAHANG
Engineering • Technology • Creativity

SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Doctor of Philosophy.

(Supervisor's Signature)

Full Name : DR. MOHAMAD FADLI ZOLKIPLI

Position : SENIOR LECTURER

Date : 27 FEB 2019

Universiti Malaysia PAHANG
Engineering • Technology • Creativity

STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

(Student's Signature)

Full Name : HUSSAM ALDDIN SHIHAB AHMED

ID Number : PCC13005

Date : 27 FEB 2019

DESIGNING SUBSTITUTION BOXES BASED ON CHAOTIC MAP AND GLOBALIZED FIREFLY ALGORITHM

HUSSAM ALDDIN SHIHAB AHMED

Thesis submitted in fulfillment of the requirements
for the award of the degree of
Doctor of Philosophy

Faculty of Computer Systems & Software Engineering

UNIVERSITI MALAYSIA PAHANG

FEBRUARY 2019

PERPUSTAKAAN
UNIVERSITI MALAYSIA PAHANG

No. Perolehan	No. Panggilan
127391	TS KKP .1487 2019 T THESIS
Tarikh 17 APR 2019	

Dedicated to

My

Parents;

Brothers and sisters

My fiancé

ACKNOWLEDGEMENTS

The road to my doctoral degree has been a long but rewarding journey. I would like to thank the following people and organisations. Without their help and support, this thesis would not have been possible.

I am deeply grateful to my parents: my mother Elham Salim and my father Shihab Ahmad for your prayers and unlimited support. I certainly would not be where I am today without their nurture, guidance, love and care throughout my life. Words would never be enough to express my gratitude. Whatever I do, I will not be able to return the love, bestowal and support. I pray Allah for your perfect health and prolong age and may Allah reward you richly. Love you both. To my fiancé Ayah, thank you for your assistance and encouragement.

I would like to take this opportunity to deeply thank my supervisor Dr. Mohamad Fadli Zolkipli for his wealthy advice. Special appreciation goes to him for his mentorship and constant support throughout this research.

Finally, I would like to acknowledge and thank Universiti Malaysia Pahang for allowing me to conduct my research and providing the required assistance. It is also my pleasure to thank all members of the Faculty of Computer Systems & Software Engineering, both academic and non-academic, who helped and supported me during my research.

ABSTRAK

Kegunaan dan aplikasi *chiphers* yang sesuai adalah asas kepada keselamatan sistem maklumat dan komunikasi elektronik kerana kemampuan *ciphers* ini menahan serangan kriptanitik secara langsung mempengaruhi kekuatan keseluruhan sistem. Kekuatan *cipher* bergantung kepada strukturnya yang mantap dan rekaan interaksi yang baik antara komponen-komponen di dalam rangka kerja. Komponen penting di dalam sistem *cipher* yang mmpengaruhi kekuatan sistem *cipher* ialah kotak penggantian atau *S-box*. *S-box* adalah komponen terpenting di dalam sistem *cipher* kerana ia menyediakan sistem yang mempunyai rintangan terhadap serangan kriptanitik tertentu yang diketahui dan berpotensi. Oleh itu, telah banyak usaha penyelidikan dikhaskan kepada pembangunan beberapa strategi reka bentuk *S-box* yang dapat mencapai ciri-ciri kriptografi optimum yang dikehendaki. *Nonlinearity, bijectivity, strict avalanche criteria, bit independence criteria, differential probability,* dan *linear probability* adalah ciri-ciri kriptografi utama yang dikaitkan S-box yang kuat. Sistem kriptografi yang berbeza memerlukan ciri-ciri keselamatan ini pada tahap tertentu. Untuk menjadi *S-box* yang mempamerkan gabungan ciri-ciri kriptografi tertentu pada kadar yang berbeza, reka bentuk kriptografi *S-box* yang kuat selalunya memerlukan pertukaran antara sifat-sifat ini untuk mencapai ciri-ciri optimum. Sehingga kini, banyak reka bentuk S-box telah dicadangkan dalam kesusasteraan, para penyelidik telah menganjurkan penggunaan reka bentuk S-box berasaskan meta-heuristik. Walaupun membantu, tiada dominasi tuntutan meta-heuristik terhadap penolakan yang lain. Atas sebab ini, penyelidikan untuk generasi baru S-box meta-heuristik masih merupakan usaha yang berguna. Tesis ini menggunakan pendekatan metaheuristik berdasarkan pengoptimuman algoritma kelip-kelip (FA) untuk menghasilkan konfigurasi yang sesuai untuk kotak 8 × 8 S-box. FA boleh membina S-box kuat yang memenuhi kriteria yang ditetapkan dengan pantas mencari subset ciri optimum atau hampir optimal yang meminimumkan fungsi kecergasan yang diberikan. FA adalah teknik pengiraan baru yang diilhamkan oleh kunang-kunang dan proses pencahayaan kilat mereka. Walau bagaimanapun, FA mungkin mengalami konvergensi awal apabila menyelesaikan masalah pengoptimuman. Tesis ini mencadangkan pengubahsuaian FA baru, iaitu algoritma kelaparan global (GFA), yang menggunakan pergerakan rawak berdasarkan firefly terbaik menggunakan peta huru-hara. Kelip-kelip yang terbaik tidak melakukan pencarian dalam algoritma firefly standard (SFA). Algoritma yang dicadangkan menggunakan reka bentuk baru untuk mendapatkan S-box kuat berdasarkan SFA, algoritma kelam kabut (CFA), GFA dan GFA dengan kekacauan. Hasil yang diperoleh dibandingkan dengan kaedah generasi sebelumnya S-box. Secara keseluruhannya, hasil eksperimen menunjukkan bahawa reka bentuk kotak S yang dicadangkan mempunyai ciri-ciri kriptografi yang memuaskan.

ABSTRACT

Cipher strength mainly depends on the robust structure and a well-designed interaction of the components in its framework. A significant component of a cipher system, which has a significant influence on the strength of the cipher system, is the substitution box or S-box. An S-box is a vital and most essential component of the cipher system due to its direct involvement in providing the system with resistance against certain known and potential cryptanalytic attacks. Hence, research in this area has increased since the late 1980s, but there are still several issues in the design and analysis of the S-boxes for cryptography purposes. Therefore, it is not surprising that the design of suitable S-boxes attracts a lot of attention in the cryptography community. Nonlinearity, bijectivity, strict avalanche criteria, bit independence criteria, differential probability, and linear probability are the major required cryptographic characteristics associated with a strong S-box. Different cryptographic systems requiring certain levels of these security properties. Being that S- boxes can exhibit a certain combination of cryptographic properties at differing rates, the design of a cryptographically strong S-box often requires the establishment of a trade-off between these properties when optimizing the property values. To date, many S-boxes designs have been proposed in the literature, researchers have advocated the adoption of metaheuristic based S-boxes design. Although helpful, no single metaheuristic claim dominance over their other countermeasure. For this reason, the research for a new metaheuristic based S-boxes generation is still a useful endeavour. This thesis aim to provide a new design for 8×8 S-boxes based on firefly algorithm (FA) optimization. The FA is a newly developed metaheuristic algorithm inspired by fireflies and their flash lighting process. In this context, the proposed algorithm utilizes a new design for retrieving strong S- boxes based on standard firefly algorithm (SFA). Three variations of FA have been proposed with an aim of improving the generated S-boxes based on the SFA. The first variation of FA is called chaotic firefly algorithm (CFA), which was initialized using discrete chaotic map to enhance the algorithm to start the search from good positions. The second variation is called globalized firefly algorithm (GFA), which employs random movement based on the best firefly using chaotic maps. If a firefly is brighter than its other counterparts, it will not conduct any search. The third variation is called globalized firefly algorithm with chaos (CGFA), which was designed as a combination of CFA initialization and GFA. The obtained result was compared with a previous S-boxes based on optimization algorithms. Overall, the experimental outcome and analysis of the generated S-boxes based on nonlinearity, bit independence criteria, strict avalanche criteria, and differential probability indicate that the proposed method has satisfied most of the required criteria for a robust S-box without compromising any of the required measure of a secure S-box.

TABLE OF CONTENT

DECLARATION

TITLE PAGE

ACKNOWLEDGEMENTS ii

ABSTRAK iii

ABSTRACT iv

TABLE OF CONTENT v

LIST OF TABLES iix

LIST OF FIGURES xi

LIST OF ABBREVIATIONS xiii

CHAPTER 1 INTRODUCTION 1

1.1 Problem Statements 4

1.2 Research Questions 7

1.3 Research Aims and Objectives 7

1.4 Research Hypothesis 7

1.5 Research Scope 8

1.6 Thesis Organization 8

CHAPTER 2 LITERATURE REVIEW 10

2.1 Computer Security Concept 10

2.1.1 Cryptology 11

2.1.2 The Cryptography 12

2.2 Symmetric Block Cipher 13

2.2.1 Confusion 14

2.2.2 Diffusion 14

2.3 Cryptanalysis Attacks 15

2.3.1 Linear Cryptanalysis 15

2.3.2 Differential Cryptanalysis 18

2.4 Boolean Function Theory 21

2.4.1 Substitution Boxes Theory 25

2.4.2 S-Box Definitions and Types 25

2.4.3 Performance Criteria of S-boxes 26

2.5 Methods of S-box Construction 30

2.5.1 Algebraic Constructions 30

2.5.2 Random Methods 31

2.5.3 Metaheuristic Methods 32

2.5.4 Existing S-boxes Designs Based Metaheuristics Methods 33

2.5.5 Analysis of the Previous Work 38

2.6 Review on Firefly Algorithm 39

2.6.1 Firefly Behavior 40

2.6.2 Artificial Firefly Algorithm 41

2.6.3 Firefly Algorithm Variants 43

2.6.4 Fireflies Movement Modification 46

2.6.5 The Justification of the Adoption of FA 51

2.7 Summary 52

CHAPTER 3 RESEARCH METHODOLOGY 54

3.1 Introduction 54

3.2 Problem Understanding and Literature Review Phase 55

3.3 Design Approach Phase 55

3.4 Implementation Phase 56

3.5 Testing and Evaluation Phase 56

3.6 Algorithm Performance Evaluation 57

3.7 S-boxes Performance Evaluation 58

3.7.1 Bijectivity 59

3.7.2 Nonlinearity 59

3.7.3 Strict Avalanche Criteria 59

3.7.4 Bit Independence Criteria 59

3.7.5 Differential Approximation Probability 59

3.7.6 Linear Approximation Probability 60

3.8 Improvement Phase 60

3.9 Summary 60

CHAPTER 4 STANDARD FIREFLY ALGORITHM 61

4.1 Introduction 61

4.2 Standard Firefly Algorithm Based S-box Design 61

4.3 Chaotic Firefly Algorithm 66

4.3.1 Discrete Chaotic Map 67

4.4 Globalized Firefly Algorithm 69

4.4.1 Attractiveness Calculation based GFA 72

4.4.2 Firefly Movement in GFA 73

4.5 Globalized Firefly Algorithm with Chaos based S-box Design 74

4.6 Tuning of FA Parameters 76

4.7 Summary 79

CHAPTER 5 RESULTS AND DISCUSSION 80

5.1 Experimental Evaluations 80

5.2 Experimental Settings 81

5.3 Experimental Results 83

5.3.1 Characterizing CFA 83

5.3.2 Characterizing GFA 86

5.3.3 Characterizing CGFA 87

5.4 Statistical Analysis for the Experimental Results 91

5.4.1 Experimental Results and Statistical Analysis 92

5.5 Benchmarking with Other Strategies 95

5.5.1 Bijectivity Property 96

5.5.2 Nonlinearity 96

5.5.3 Strict Avalanche Criterion 98

5.5.4 Bits Independence Criterion 101

5.5.5 Differential Probability 105

5.5.6 Linear Approximation Probability 108

5.6 Summary 109

CHAPTER 6 CONCLUSION AND FUTURE WORK 110

6.1 Research Achievement 110

6.2 Contribution 112

6.3 Threats to Validity 112

6.4 Future Work 113

REFERENCES 115

APPENDIXA Empirical Experimental Results 129

APPENDIX B Empirical Experimental Results 131

APPENDIX C List of Publications 137

LIST OF TABLES

Table 2.1	Example of a truth table. $n = 3$	22
Table 2.2	Advantages and disadvantages of the previous work	40
Table 2.3	Modified firefly algorithm	47
Table 2.4	The analysis of existing S-boxes methods	51
Table 5.1	Parameter settings	82
Table 5.2	Comparison result between SFA, CFA	84
Table 5.3	Comparison result between SFA, and GFA	86
Table 5.4	Comparison result between SFA and CGFA	89
Table 5.5	Friedman test for 250 iteration 40 swarm size	91
Table 5.6	Friedman test for 500 iteration 40 swarm size	91
Table 5.7	Friedman test for 1000 iteration 40 swarm size	91
Table 5.8	Wilcoxon signed test	92
Table 5.9	Nonlinearity analysis of S-boxes	97
Table 5.10	SAC values of the S-box based SFA	99
Table 5.11	SAC values of the S-box based CFA	99
Table 5.12	SAC values of the S-box based GFA	99
Table 5.13	SAC values of the S-box based CGFA	100
Table 5.14	SAC results comparison	100
Table 5.15	BIC-SAC of generated S-box based SFA	101
Table 5.16	BIC-SAC of generated S-box based CFA	101
Table 5.17	BIC-SAC of generated S-box based GFA	101
Table 5.18	BIC-SAC of generated S-box based CGFA	102
Table 5.19	BIC-SAC comparison of S-boxes	102
Table 5.20	BIC-nonlinearity of the S-box based SFA	103
Table 5.21	BIC-nonlinearity of the S-box based CFA	103
Table 5.22	BIC-nonlinearity of the S-box based GFA	103
Table 5.23	BIC-nonlinearity of the S-box based CGFA	104
Table 5.24	BIC-nonlinearity comparison of S-boxes	104
Table 5.25	DP of the S-box based SFA	106
Table 5.26	DP of the S-box based CFA	106
Table 5.27	DP of the S-box based GFA	107
Table 5.28	DP of the S-box based CGFA	107
Table 5.29	DP comparison of S-boxes	108

Table 5.30 LP comparison of S-boxes 109

LIST OF FIGURES

Figure 2.1	Overview of the computer security properties of cryptography	11
Figure 2.2	Overview of the cryptology	12
Figure 2.3	Diagram of symmetric block cipher	14
Figure 2.4	General linear cryptanalysis	18
Figure 2.5	General differential cryptanalysis	20
Figure 2.6	S-box construction methods	30
Figure 2.7	Pseudo code of firefly algorithm (FA) (Yang, 2010d).	43
Figure 2.8	Classification of firefly algorithm (Yang & He, 2013)	44
Figure 2.9	Uses FA in optimization (Pant, 2018)	44
Figure 2.10	Application of firefly algorithm (Fister et al., 2013a)	45
Figure 2.11	Modified algorithm (Verma et al., 2016)	48
Figure 3.1	Research methodology	55
Figure 3.2	Firefly flowchart (Yang, 2009a)	57
Figure 3.3	Experiment evaluation process	58
Figure 4.1	Flowchart of S-box generation process based SFA	64
Figure 4.2	Pseudocode of standard firefly algorithm (SFA)	65
Figure 4.3	S-box generation diagram	66
Figure 4.4	Pseudocode of chaotic firefly algorithm (CFA)	70
Figure 4.5	Flowchart of globalised firefly algorithm for S-box design	71
Figure 4.6	Pseudocode of globalized firefly algorithm (GFA)	72
Figure 4.7	Pseudocode of globalized firefly algorithm with chaos (CGFA)	75
Figure 4.8	The illustration of average nonlinearity score.	77
Figure 4.9	The illustration of best nonlinearity score	78
Figure 5.1	Convergence of SFA and CFA for 40 swarm size	85
Figure 5.2	Convergence of SFA and GFA for 40 swarm size	88
Figure 5.3	Convergence of SFA and CGFA for 40 swarm size	91
Figure 5.4	Box plot for 250 iteration	93
Figure 5.5	Box plot for 500 iteration	94
Figure 5.6	Box plot for 1000 iteration	95
Figure 5.7	Average nonlinearity scores of generated S-boxes	98
Figure 5.8	Average SAC values of generated S-boxes	100
Figure 5.9	Average BIC-SAC values of generated S-boxes	103
Figure 5.10	BIC-nonlinearity values of generated S-boxes	105

Figure 5.11 Maximum DP values of generated S-boxes 108
Figure 5.12 Comparison of linear approximation of proposed S-boxes 109

LIST OF ABBREVIATIONS

ABC	Ant bee colony
ACO	Ant colony optimization
AES	Advanced encryption standard
AP	Algorithm Portfolios
BFO	Bacterial foraging optimization
BIC	Bit independence criteria
BWD	Bee waggle dance
CA	Cellular automata
CGFA	Globalized firefly algorithm with chaos
DE	Differential evolution algorithm
DES	Data encryption standard
DP	Differential probability
FA	Firefly algorithm
GA	Genetic algorithm
GD	Gradient descent
GFA	Globalized firefly algorithm
HC	Hill climbing
HD	Hamming distance
HW	Hamming weight
LP	Linear probability
OSI	Open system interconnection
PSO	Particle swarm optimization
RRA	Redundancy removal algorithm
SA	Simulated annealing
SAC	Strict avalanche criteria
S-Boxes	Substitution boxes
SFA	Standard firefly algorithm
SPN	Substitution permutation network
SpImmAlg	Specific artificial immune algorithm
TLBO	Teaching learning based optimization
WHT	Walsh hadamard transform

REFERENCES

Abdullah, A., Deris, S., Mohamad, M. S., and Hashim, S. Z. M. 2012. A new hybrid firefly algorithm for complex and nonlinear problem. *In the Distributed Computing and Artificial Intelligence*, 673-680.

Adams, C., and Tavares, S. 1990. The structured design of cryptographically good S-boxes. *Journal of Cryptology.* **3**(1), 27-41.

Adaniya, M. H., Lima, M. F., Rodrigues, J. J., Abrao, T., and Proença, M. L. 2012. Anomaly detection using dsns and firefly harmonic clustering algorithm. *In the International Conference on Communications (ICC)* (pp.1183-1187). IEEE

Ahmad, M., Alauddin, M., and AlSharari, H. D. 2018. Heuristic approach for nonlinear $n\times n$ ($3\leq n\leq 7$) substitution-boxes. *In Data Engineering and Intelligent Computing* (pp. 347-355): Springer.

Ahmad, M., Bhatia, D., and Hassan, Y. 2015. A novel ant colony optimization based scheme for substitution box design. *Procedia Computer Science.* **57**, 572-580.

Ahmad, M., Doja, M., and Beg, M. S. 2018. ABC optimization based construction of strong substitution-boxes. *Wireless Personal Communications.* **101**(3), 1715-1729.

Ahmad, M., Seeru, F., Siddiqi, A. M., and Masood, S. 2018. Dynamic 9×9 substitution-boxes using chaos-based heuristic search. *Soft Computing: Theories and Applications* (pp. 839-851): Springer.

Alb, M., Alotto, P., Magele, C., Renhart, W., Preis, K., and Trapp, B. 2016. Firefly algorithm for finding optimal shapes of electromagnetic devices. *IEEE Transactions on Magnetics.* **52**(3), 1-4.

Altaleb, A., Saeed, M. S., Hussain, I., and Aslam, M. 2017. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances.* 7(3), 035116.

Anderson, R. 1994. On fibonacci keystream generators. *In the International Workshop on Fast Software Encryption*, (pp. 346-352): Springer.

Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., and Tokita, T. 2000. Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis. *In the Selected Areas in Cryptography.* (pp. 39-56). Springer.

Balachennaiah, P., Suryakalavathi, M., and Nagendra, P. 2016. Optimizing real power loss and voltage stability limit of a large transmission network using firefly algorithm. *Engineering Science and Technology, an International Journal.* **19**(2), 800-810.

Bard, G. 2009. *Algebraic cryptanalysis*. Springer Science & Business Media.

Bartz-Beielstein, T., Lasarczyk, C., and Preuss, M. 2010. The sequential parameter optimization toolbox. *In Experimental Methods for Analysis of Optimization Algorithms* (pp. 337-362): Springer.

Basu, B., and Mahanti, G. K. 2011. Firefly and artificial bees colony algorithm for synthesis of scanned and broadside linear array antenna. *Progress in Electromagnetics Research.* **32**, 169-190.

Biham, E. 2002. Observations on the relations between the bit-functions of many S-boxes. *In Presentation at the 3rd NESSIE Conference.*

Biham, E., and Shamir, A. 1991. Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology,* **4**(1), 3-72.

Boehm, B. W., Gray, T. E., and Seewaldt, T. 1984. Prototyping versus specifying: a multiproject experiment. *IEEE Transactions on Software Engineering.* (3), 290-303.

Burnett, L., Carter, G., Dawson, E., and Millan, W. 2000. Efficient methods for generating MARS-like S-boxes. *In the International Workshop on Fast Software Encryption*, (pp. 300-313). Springer.

Burnett, L. D. 2005. *Heuristic optimization of Boolean functions and substitution boxes for cryptography.* Doctoral dissertation, Queensland University of Technology.

Carlet, C. 2005. On highly nonlinear S-boxes and their inability to thwart DPA attacks. *In International Conference on Cryptology*, (pp. 49-62). Springer.

Carlet, C. 2010. Boolean functions for cryptography and error correcting codes. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* **2**, 257-397.

Carlet, C. 2010. Vectorial boolean functions for cryptography. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering.* **134**, 398-469.

Chandrasekaran, K., and Simon, S. P. 2012. Network and reliability constrained unit commitment problem using binary real coded firefly algorithm. *International Journal of Electrical Power & Energy Systems.* **43**(1), 921-932.

Chandrasekaran, K., Simon, S. P., and Padhy, N. P. 2013. Binary real coded firefly algorithm for solving unit commitment problem. *Information Sciences.* **249**, 67-84.

Chatterjee, A., Mahanti, G. K., and Chatterjee, A. 2012. Design of a fully digital controlled reconfigurable switched beam concentric ring array antenna using firefly and particle swarm optimization algorithm. *Progress in Electromagnetics Research.* **36**, 113-131.

Chen, G. 2008. A novel heuristic method for obtaining S-boxes. *Chaos, Solitons & Fractals.* **36**(4), 1028-1036.

Chen, H., and Feng, D.-g. 2004. An effective evolutionary strategy for bijective S-boxes. *In the Congress on Evolutionary Computation, (IEEE Cat. No. 04TH8753)*. (pp. 2120-2123. *IEEE*

Chen, H., and Feng, D. 2007. An effective genetic algorithm for self-inverse S-boxes. *In the International Conference on Computational Intelligence and Security*. (pp. 618-622). IEEE

Clark, J. A., Jacob, J. L., and Stepney, S. 2005. The design of S-boxes by simulated annealing. *New Generation Computing*. **23**(3), 219-231.

Cobas, J., and Brugos, J. 2005. Complexity-theoretical approaches to the design and analysis of cryptographical boolean functions. *In the International Conference on Computer Aided Systems Theory*. (pp. 337-345). Springer.

Courtois, N., and Pieprzyk, J. 2002. Cryptanalysis of block ciphers with overdefined systems of equations. *In the International Conference on the Theory and Application of Cryptology and Information Security*. (pp. 267-287). Springer.

Cui, L., and Cao, Y. 2007. A new S-box structure named Affine-Power-Affine. *International Journal of Innovative Computing, Information and Control*. **3**(3), 751-759.

Cusick, T. W., and Stanica, P. 2017. *Cryptographic boolean functions and applications*. Academic Press.

Daemen, J., Knudsen, L. R., and Rijmen, V. 1997. The block cipher Square. *In the International Workshop on Fast Software Encryption*. (pp. 149-165). Springer.

Daemen, J., and Rijmen, V. 2001. Advanced encryption standard (AES)(FIPS 197). *Technical Report, Katholijke Universiteit Leuven/ESAT*.

Daemen, J., and Rijmen, V. 2001. AES proposal: Rijndael.

Daemen, J., and Rijmen, V. 2001. Rijndael, the advanced encryption standard. *Dr. Dobb's Journal*. **26**(3), 137-139.

Daemen, J., and Rijmen, V. 2013. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media.

Daniel, W. W. 1990. Friedman two-way analysis of variance by ranks. *Applied Nonparametric Statistics*.pp.262-274.

Dawson, M., and Tavares, S. E. 1991. An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. *In the Workshop on the Theory and Application of Cryptographic Techniques*. (pp. 352-367). Springer.

Diffie, W., and Hellman, M. 1976. New directions in cryptography. *IEEE Transactions on Information Theory*. **22**(6), 644-654.

dos Santos Coelho, L., de Andrade Bernert, D. L., and Mariani, V. C. 2011. A chaotic firefly algorithm applied to reliability-redundancy optimization. *In IEEE Congress of Evolutionary Computation (CEC),* (pp. 517-521). IEEE.

dos Santos Coelho, L., and Mariani, V. C. 2008. Use of chaotic sequences in a biologically inspired algorithm for engineering design optimization. *Expert Systems with Applications.* **34**(3), 1905-1913.

Eastlake 3rd, D., and Jones, P. 2001. US secure hash algorithm 1 (SHA1). No. RFC 3174.

Eiben, A. E., and Smit, S. K. 2011. Parameter tuning for configuring and analyzing evolutionary algorithms. *Swarm and Evolutionary Computation.* **1**(1), 19-31.

Elbirt, A. J. 2009. Understanding and applying cryptography and data security. *Auerbach Publications.*

Falcon, R., Almeida, M., and Nayak, A. 2011. Fault identification with binary adaptive fireflies in parallel and distributed systems. *In the Congress on Evolutionary Computation (CEC)* (pp. 1359-1366). IEEE.

Farah, T., Rhouma, R., and Belghith, S. 2017. A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. *Nonlinear Dynamics.* **88**(2), 1059-1074.

Farahani, S. M., Abshouri, A., Nasiri, B., and Meybodi, M. 2011. A Gaussian firefly algorithm. *International Journal of Machine Learning and Computing.* **1**(5), 448.

Farahani, S. M., Abshouri, A. A., Nasiri, B., and Meybodi, M. 2012. Some hybrid models to improve firefly algorithm performance. *International Journal of Artificial Intelligence.* **8**(12), 97-117.

Fateen, S.-E. K., Bonilla-Petriciolet, A., and Rangaiah, G. P. 2012. Evaluation of covariance matrix adaptation evolution strategy, shuffled complex evolution and firefly algorithms for phase stability, phase equilibrium and chemical equilibrium problems. *Chemical Engineering Research and Design.* **90**(12), 2051-2071.

Fister, I., Fister Jr, I., Yang, X.-S., and Brest, J. 2013. A comprehensive review of firefly algorithms. *Swarm and Evolutionary Computation.* **13**, 34-46.

Fister, I., Yang, X.-S., Brest, J., and Fister Jr, I. 2013. Modified firefly algorithm using quaternion representation. *Expert Systems with Applications.* **40**(18), 7220-7230.

Fu, Q., Liu, Z., Tong, N., Wang, M., and Zhao, Y. 2015. A novel firefly algorithm based on improved learning mechanism. *In the International Conference on Logistics Engineering, Management and Computer Science (LEMCS); Atlantis Press.*

Fuller, J. E. 2003. *Analysis of affine equivalent Boolean functions for cryptography.* Doctoral dissertation, Queensland University of Technology.

Gandomi, A. H., Yang, X.-S., and Alavi, A. H. 2011. Mixed variable structural optimization using firefly algorithm. *Computers & Structures.* **89**(23), 2325-2336.

Gandomi, A. H., Yang, X.-S., Talatahari, S., and Alavi, A. H. 2013. Firefly algorithm with chaos. *Communications in Nonlinear Science and Numerical Simulation.* **18**(1), 89-98.

Gao, S., Ma, W., Feng, J., Guo, N., and Yan, Y. 2010. Improved hill-climbing methods in the design of bijective S-boxes. *In the Sixth International Conference on the Natural Computation (ICNC).* **5**, (pp. 2378-2380). IEEE.

Gérard, B., Grosso, V., Naya-Plasencia, M., and Standaert, F.-X. 2013. Block ciphers that are easier to mask: How far can we go? *In the International Workshop on Cryptographic Hardware and Embedded Systems.* (pp. 383-399). Springer.

Gholizadeh, S., and Barati, H. 2012. A comprative study of three metaheuristics for optimum design of trusses. 423-441.

Goering, R. 2004. Matlab edges closer to electronic design automation world. *Electronic Engineering Times.* (1341), 4-5.

Gonzalez, R., Woods, R., and Eddins, S. 2004. Digital image processing using MATLAB: Pearson Education. Second Indian Reprint.

Goodrich, M., and Tamassia, R. 2011. *Introduction to computer security.* Pearson.

Gope, S., Goswami, A. K., Tiwari, P. K., and Deb, S. 2016. Rescheduling of real power for congestion management with integration of pumped storage hydro unit using firefly algorithm. *International Journal of Electrical Power & Energy Systems.* **83**, 434-442.

Guesmi, R., Farah, M. A. B., Kachouri, A., and Samet, M. 2014. A novel design of chaos based S-Boxes using genetic algorithm techniques. *In the 11th International Conference on Computer Systems and Applications (AICCSA)* (pp. 678-684). IEEE.

Hassanzadeh, T., and Meybodi, M. R. 2012. A new hybrid approach for data clustering using firefly algorithm and K-means. *In the 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP)* (pp. 007-011). IEEE.

He, L., and Huang, S. 2017. Modified firefly algorithm based multilevel thresholding for color image segmentation. *Neurocomputing.* **240**, 152-174.

Horng, M.-H. 2012. Vector quantization using the firefly algorithm for image compression. *Expert Systems with Applications.* **39**(1), 1078-1091.

Horng, M.-H., and Jiang, T.-W. 2010. The codebook design of image vector quantization based on the firefly algorithm. *In the International Conference on Computational Collective Intelligence*, (pp. 438-447). Springer.

Horng, M.-H., Lee, Y.-X., Lee, M.-C., and Liou, R.-J. 2012. Firefly meta-heuristic algorithm for training the radial basis function network for data classification and disease diagnosis. *In the Theory and new applications of swarm intelligence*: InTechOpen.

Hussain, I., and Gondal, M. A. 2014. An algorithm to generating inverse S-box for Rijndael Encryption standard. *3D Research.* **5**(4), 30.

Hussain, I., Shah, T., Gondal, M. A., and Khan, W. A. 2011. Construction of cryptographically strong 8× 8 S-boxes. *World Applied Sciences Journal.* **13**(11), 2389-2395.

Husselmann, A. V., and Hawick, K. 2012. Parallel parametric optimisation with firefly algorithms on graphical processing units. *In the International Conference on Genetic and Evolutionary Methods (GEM)* (pp. 77-83).

Imanirad, R., Yang, X.-S., and Yeomans, J. S. 2016. Stochastic decision-making in waste management using a firefly algorithm-driven simulation-optimization approach for generating alternatives. *In Simulation-Driven Modeling and Optimization.* (pp. 299-323). Springer.

Isa, H., Jamil, N., and Z'aba, M. R. 2013. S-box construction from non-permutation power functions. *In the 6th International Conference on Security of Information and Networks*, (pp. 46-53). ACM.

Isa, H., Jamil, N., and Z'aba, M. R. 2016. Construction of cryptographically strong S-boxes inspired by bee waggle dance. *New Generation Computing.* **34**(3), 221-238.

Isa, H., Jamil, N., and Z'aba, M. R. 2016. Hybrid heuristic methods in constructing cryptograpgically strong S-Boxes. *International Journal of Cryptology Research.* **6**(1), 1-15.

Ivanov, G., Nikolov, N., and Nikova, S. 2015. Cryptographically strong S-boxes generated by modified immune algorithm. *In the International Conference on Cryptography and Information Security*. (pp. 31-42). Springer.

Ivanov, G., Nikolov, N., and Nikova, S. 2016. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. *Cryptography and Communications.* **8**(2), 247-276.

Izbenko, Y., Kovtun, V., and Kuznetsov, A. 2009. The design of boolean functions by modified hill climbing method. *In the Sixth International Conference on Information Technology: New Generations.* (pp. 356-361). IEEE.

Jakimoski, G., and Kocarev, L. 2001. Chaos and cryptography: block encryption ciphers based on chaotic maps. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications.* **48**(2), 163-169.

Jeklene, O. 2011. Optimization of the quality of continuously cast steel slabs using the firefly algorithm. *Materiali in tehnologije.* **45**(4), 347-350.

Kaminsky, A., Kurdziel, M., and Radziszowski, S. 2010. An overview of cryptanalysis research for the advanced encryption standard. *In the Military Communications Conference (MILCOM)*. (pp. 1310-1316). IEEE.

Kazem, A., Sharifi, E., Hussain, F. K., Saberi, M., and Hussain, O. K. 2013. Support vector regression with chaos-based firefly algorithm for stock market price forecasting. *Applied Soft Computing.* **13**(2), 947-958.

Kazemzadeh-Parsi, M. 2014. A modified firefly algorithm for engineering design optimization problems. *Iranian Journal of Science and Technology. Transactions of Mechanical Engineering.* **38**(M2), 403.

Kazemzadeh-Parsi, M. J. 2015. Optimal shape design for heat conduction using smoothed fixed grid finite element method and modified firefly algorithm. *Iranian Journal of Science and Technology. Transactions of Mechanical Engineering.* **39**(M2), 367.

Kazemzadeh-Parsi, M. J., Daneshmand, F., Ahmadfard, M. A., Adamowski, J., and Martel, R. 2015. Optimal groundwater remediation design of pump and treat systems via a simulation–optimization approach and firefly algorithm. *Engineering Optimization.* **47**(1), 1-17.

Kazlauskas, K., and Kazlauskas, J. 2009. Key-dependent S-box generation in AES block cipher system. *Informatica.* **20**(1), 23-34.

Kazymyrov, O., Kazymyrova, V., and Oliynykov, R. 2013. A method for generation of high-nonlinear S-boxes based on gradient descent. *IACR Cryptology ePrint Archive.*, 578.

Kocarev, L., and Lian, S. 2011. *Chaos-based cryptography: Theory, algorithms and applications.* **Vol. 354**. Springer Science & Business Media.

Lambić, D. 2014. A novel method of S-box design based on chaotic map and composition method. *Chaos, Solitons & Fractals.* **58**, 16-21.

Lambić, D. 2015. A new discrete chaotic map based on the composition of permutations. *Chaos, Solitons & Fractals.* **78**, 245-248.

Lambić, D., and Nikolić, M. 2017. Pseudo-random number generator based on discrete-space chaotic map. *Nonlinear Dynamics.* **90**(1), 223-232.

Laskari, E. C., Meletiou, G. C., and Vrahatis, M. N. 2006. Utilizing evolutionary computation methods for the design of S-boxes. *In the International Conference on Computational Intelligence and Security.* **2,** (pp. 1299-1302). IEEE.

Lehmer, D. H. 1960. Teaching combinatorial tricks to a computer. *Sympos. Appl. Math. Combinatorial Analysis.* (Vol. **10**, pp.179-193).

Lewis, S. M., and Cratsley, C. K. 2008. Flash signal evolution, mate choice, and predation in fireflies. *Annu. Rev. Entomol.* **53**, 293-321.

Li, Y., and Wang, M. 2014. Constructing differentially 4-uniform permutations over GF (2 2m) from quadratic APN permutations over GF (2 2m+ 1). *Designs, Codes and Cryptography.* 1-16.

Lihong, G., Gaige, W., and Heqi, W. 2013. An effective hybrid firefly algorithm with harmony search for global numerical optimization. *The Scientific World Journal.*

Liu, H., Kadir, A., and Niu, Y. 2014. Chaos-based color image block encryption scheme using S-box. *AEU-international Journal of Electronics and Communications.* **68**(7), 676-686.

Liu, H., Kadir, A., Sun, X., and Li, Y. 2017. Chaos based adaptive double-image encryption scheme using hash function and S-boxes. *Multimedia Tools and Applications.* 1-17.

Long, N. C., and Meesad, P. 2014. An optimal design for type–2 fuzzy logic system using hybrid of chaos firefly algorithm and genetic algorithm and its application to sea level prediction. *Journal of Intelligent & Fuzzy Systems.* **27**(3), 1335-1346.

Lukasik, S., and Zak, S. 2009. Firefly algorithm for continuous constrained optimization tasks. *In the International Conference on Computational Collective Intelligence* (pp. 97-106). Springer.

Marichelvam, M. K., Prabaharan, T., and Yang, X. S. 2014. A discrete firefly algorithm for the multi-objective hybrid flowshop scheduling problems. *IEEE Transactions on Evolutionary Computation.* **18**(2), 301-305.

Picek, S., Mariot, L., Leporati, A., and Jakobovic, D. 2017. Evolving S-boxes based on cellular automata with genetic programming. *In the Genetic and Evolutionary Computation Conference Companion.* (pp. 251-252). ACM.

Matsui, M. 1993. Linear cryptanalysis method for DES cipher. *In the Workshop on the Theory and Application of Cryptographic Techniques.* (pp. 386-397). Springer.

Matt, B. 2006. *Introduction to computer security.* Pearson Education India.

McLaughlin, J., and Clark, J. A. 2013. Using evolutionary computation to create vectorial Boolean functions with low differential uniformity and high nonlinearity. *arXiv preprint arXiv:1301.6972.*

Meier, W., and Staffelbach, O. 1989. Nonlinearity criteria for cryptographic functions. *In the Workshop on the Theory and Application of Cryptographic Techniques.* (pp. 549-562). Springer.

Katz, J., Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. Handbook of applied cryptography. CRC Press.

Millan, W. 1998. How to improve the nonlinearity of bijective S-boxes. *In the Australasian Conference on Information Security and Privacy.* (pp. 181-192). Springer.

Millan, W., Burnett, L., Carter, G., Clark, A., and Dawson, E. 1999. Evolutionary heuristics for finding cryptographically strong S-boxes. *In the International Conference on Information and Communications Security.* (pp. 263-274). Springer.

Millan, W., Clark, A., and Dawson, E. 1997. Smart hill climbing finds better boolean functions. *In the Workshop on Selected Areas in Cryptology*. (pp. 50-63).

Millan, W., Clark, A., and Dawson, E. 1999. Boolean function design using hill climbing methods. *In the 4th Australasian Conference on Information Security and Privacy* (pp. 1-11). Springer.

Mishra, M., Chaturvedi, U., and Pal, S. K. 2014. A multithreaded bound varying chaotic firefly algorithm for prime factorization. *In the International Advance Computing Conference (IACC)* (pp. 1322-1325). IEEE.

Nyberg, K. 1993. Differentially uniform mappings for cryptography. *In the Workshop on the Theory and Application of Cryptographic Techniques*. (pp. 55-64). Springer.

Osaba, E., Yang, X.-S., Diaz, F., Onieva, E., Masegosa, A. D., and Perallos, A. 2017. A discrete firefly algorithm to solve a rich vehicle routing problem modelling a newspaper distribution system with recycling policy. *Soft Computing*. **21**(18), 5295-5308.

Othman, M., El-Khattam, W., Hegazy, Y., and Abdelaziz, A. Y. 2016. Optimal placement and sizing of voltage controlled distributed generators in unbalanced distribution networks using supervised firefly algorithm. *International Journal of Electrical Power & Energy Systems*. **82**, 105-113.

Özkaynak, F. 2015. A novel method to improve the performance of chaos based evolutionary algorithms. *Optik*. **126**(24), 5434-5438.

Özkaynak, F. 2017. Construction of robust substitution boxes based on chaotic systems. *Neural Computing and Applications*, 1-10.

Özkaynak, F., and Özer, A. B. 2010. A method for designing strong S-Boxes based on chaotic Lorenz system. *Physics Letters A*. **374**(36), 3733-3738.

Palit, S., Sinha, S. N., Molla, M. A., Khanra, A., and Kule, M. 2011. A cryptanalytic attack on the knapsack cryptosystem using binary firefly algorithm. *In the 2nd International Conference on Computer and Communication Technology*. (pp. 428-432). IEEE.

Pan, F., Ye, C., Wang, K., and Cao, J. 2013. Research on the vehicle routing problem with time windows using firefly algorithm. *Journal of Computers*. **8**(9), 2256-2261.

Pant, M. 2018. A Brief Overview of Firefly Algorithm. *In Soft Computing: Theories and Applications*. (pp. 727-738). Springer.

Partheeban, P., and Kavitha, V. 2018. Dynamic key dependent AES S-box generation with optimized quality analysis. *Cluster Computing*. 1-11.

Picek, S., Cupic, M., and Rotim, L. 2016. A new cost function for evolution of s-boxes. *Evolutionary Computation*. **24**(4), 695-718.

Picek, S., Marchiori, E., Batina, L., and Jakobovic, D. 2014. Combining evolutionary computation and algebraic constructions to find cryptography-relevant boolean functions. *In the International Conference on Parallel Problem Solving from Nature*, (PP. 822-831). Springer.

Pop, C. B., Rozina Chifu, V., Salomie, I., Baico, R. B., Dinsoreanu, M., and Copil, G. 2011. A hybrid firefly-inspired approach for optimal semantic web service composition. *Scalable Computing: Practice and Experience.* **12**(3), 363-370.

Preneel, B. 1993. *Analysis and design of cryptographic hash functions.* Doctoral dissertation, Katholieke Universiteit te Leuven.

Rao, R. V., Savsani, V. J., and Vakharia, D. 2011. Teaching–learning-based optimization: a novel method for constrained mechanical design optimization problems. *Computer-Aided Design.* **43**(3), 303-315.

Rastgou, A., and Moshtagh, J. 2016. Application of firefly algorithm for multi-stage transmission expansion planning with adequacy-security considerations in deregulated environments. *Applied Soft Computing.* **41**, 373-389.

Rijmen, V., Daemen, J., Preneel, B., Bosselaers, A., and De Win, E. 1996. The cipher SHARK. *In the International Workshop on Fast Software Encryption.* (pp. 99-111). Springer.

Santos, A. F. d., Campos Velho, H. F. d., Luz, E. F., Freitas, S. R., Grell, G., and Gan, M. A. 2013. Firefly optimization to determine the precipitation field on South America. *Inverse Problems in Science and Engineering.* **21**(3), 451-466.

Sayadi, M. K., Hafezalkotob, A., and Naini, S. G. J. 2013. Firefly-inspired algorithm for discrete optimization problems: an application to manufacturing cell formation. *Journal of Manufacturing Systems.* **32**(1), 78-84.

Schneier, B. 1994. The Blowfish encryption algorithm. *Dr Dobb's Journal-Software Tools for the Professional Programmer.* **19**(4), 38-43.

Schneier, B. 2007. *Applied cryptography: protocols, algorithms, and source code in C.* John Wiley & Sons.

Schneier, B. 2011. *Secrets and lies: digital security in a networked world.* John Wiley & Sons.

Senthilnath, J., Omkar, S., and Mani, V. 2011. Clustering using firefly algorithm: performance study. *Swarm and Evolutionary Computation.* **1**(3), 164-171.

Severin, S., and Rossmann, J. 2012. A comparison of different metaheuristic algorithms for optimizing blended PTP movements for industrial robots. *In the International Conference on Intelligent Robotics and Applications.* (pp. 321-330). Springer

Shannon, C. E. 1949. Communication theory of secrecy systems. *Bell Labs Technical Journal.* **28**(4), 656-715.

Sisalem, D., Floroiu, J., Kuthan, J., Abend, U., and Schulzrinne, H. 2009. *SIP security*. John Wiley & Sons.

Souravlias, D., Parsopoulos, K. E., and Meletiou, G. C. 2017. Designing bijective S-boxes using Algorithm Portfolios with limited time budgets. *Applied Soft Computing*. **59**, 475-486.

Srivatsava, P. R., Mallikarjun, B., and Yang, X.-S. 2013. Optimal test sequence generation using firefly algorithm. *Swarm and Evolutionary Computation*. **8**, 44-53.

Stallings, W. 2006. *Cryptography and network security: principles and practices*. Pearson Education India.

Standard, D. E. 1977. Federal information processing standards publication 46. *National Bureau of Standards, US Department of Commerce, 4*.

Stinson, D. R. 2005. *Cryptography: theory and practice*. CRC Press.

Subramanian, R., and Thanushkodi, K. 2013. An efficient firefly algorithm to solve economic dispatch problems. *International Journal of Soft Computing and Engineering*. **2**(1), 52-55.

Subutic, M., Tuba, M., and Stanarevic, N. 2012. Parallelization of the firefly algorithm for unconstrained optimization problems. *Latest Advances in Information Science and Applications*. **22**(3), 264-269.

Szaban, M., and Seredynski, F. 2008. Application of cellular automata to create S-box functions. *In the International Symposium on Parallel and Distributed Processing*. (pp. 1-7). IEEE.

Szaban, M., and Seredynski, F. 2008. Cryptographically strong S-boxes based on cellular automata. *In the International Conference on Cellular Automata*, (pp. 478-485). Springer.

Szaban, M., and Seredynski, F. 2008. Designing cryptographically strong S-boxes with the use of cellular automata. *In the Annales Universitatis Mariae Curie-Sklodowska, sectio AI–Informatica*, **8** (2), 27.

Talbi, E.-G. 2009. *Metaheuristics: from design to implementation*. **Vol. 74**. John Wiley & Sons.

Tang, G., Liao, X., and Chen, Y. 2005. A novel method for designing S-boxes based on chaotic maps. *Chaos, Solitons & Fractals*. **23**(2), 413-419.

Tian, Y., and Lu, Z. 2016. S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*. **27**(1), 232-241.

Tian, Y., and Lu, Z. 2017. Chaotic S-Box: Intertwining logistic map and bacterial foraging optimization. *Mathematical Problems in Engineering*. **2017**.

Tilahun, S. L., and Ngnotchouye, J. M. T. 2017. Firefly algorithm for discrete optimization problems: a survey. *KSCE Journal of Civil Engineering.* **21**(2), 535-545.

Tilahun, S. L., Ngnotchouye, J. M. T., and Hamadneh, N. N. 2017. Continuous versions of firefly algorithm: a review. *Artificial Intelligence Review.* 1-48.

Tilahun, S. L., and Ong, H. C. 2012. Modified Firefly Algorithm. *Journal of Applied Mathematics.* **2012**.

Tilahun, S. L., and Ong, H. C. 2012. Modified firefly algorithm. *Journal of Applied Mathematics* 1-12.

Verma, O. P., Aggarwal, D., and Patodi, T. 2016. Opposition and dimensional based modified firefly algorithm. *Expert Systems with Applications.* **44**, 168-176.

Verma, S., and Mukherjee, V. 2016. Firefly algorithm for congestion management in deregulated environment. *Engineering Science and Technology, an International Journal.* **19**(3), 1254-1265.

Wagan, A. I., Shaikh, M. M., and Abro, R. 2015. Wind turbine micrositing by using the firefly algorithm. *Applied Soft Computing.* **27**, 450-456.

Wahid, F., Ghazali, R., and Shah, H. 2018. An improved hybrid firefly algorithm for solving optimization problems. *In the International Conference on Soft Computing and Data Mining.*(pp. 14-23). Springer.

Wang, G., Guo, L., Duan, H., Liu, L., and Wang, H. 2012. A modified firefly algorithm for UCAV path planning. *International Journal of Hybrid Information Technology.* **5**(3), 123-144.

Wang, H., Cui, Z., Sun, H., Rahnamayan, S., and Yang, X.-S. 2017. Randomly attracted firefly algorithm with neighborhood search and dynamic parameter adjustment mechanism. *Soft Computing.* **21**(18), 5325-5339.

Wang, H., Wang, W., and Sun, H. 2015. Firefly algorithm with generalised opposition-based learning. *International Journal of Wireless and Mobile Computing.* **9**(4), 370-376.

Wang, H., Wang, W., Sun, H., and Rahnamayan, S. 2016. Firefly algorithm with random attraction. *International Journal of Bio-Inspired Computation.* **8**(1), 33-41.

Wang, H., Wang, W., Zhou, X., Sun, H., Zhao, J., Yu, X., and Cui, Z. 2017. Firefly algorithm with neighborhood attraction. *Information Sciences.* **382**, 374-387.

Wang, Y., Lei, P., and Wong, K.-W. 2015. A method for constructing bijective S-Box with high nonlinearity based on chaos and optimization. *International Journal of Bifurcation and Chaos.* **25**(10), 1550127.

Wang, Y., Wong, K.-W., Li, C., and Li, Y. 2012. A novel method to design S-box based on chaotic map and genetic algorithm. *Physics Letters A.* **376**(6), 827-833.

Wang, Y., Xie, Q., Wu, Y., and Du, B. 2009. A software for S-box performance analysis and test. *In the International Conference on Electronic commerce and business intelligence*. (pp. 125-128). IEEE.

Webster, A., and Tavares, S. E. 1985. On the design of S-boxes. *In the Conference on the Theory and Application of Cryptographic Techniques*. (pp. 523-534). Springer.

Wilcoxon, F. 1945. Individual comparisons by ranking methods. *Biometrics bulletin.* **1**(6), 80-83.

Xu, M., and Liu, G. 2013. A multipopulation firefly algorithm for correlated data routing in underwater wireless sensor networks. *International Journal of Distributed Sensor Networks.* **9**(3), 865154.

Xu, X. 2010. A new genetic algorithm and tabu search for S-box optimization. *In the International Conference on Computer Design and Applications (ICCDA)*, (pp. 492- 495). IEEE

Yang, X.-S. 2008. *Nature-inspired metaheuristic algorithms*. Luniver press.

Yang, X.-S. 2009. Firefly algorithms for multimodal optimization. *In the International Symposium on Stochastic Algorithms.* (pp. 169-178). Springer.

Yang, X.-S. 2010. *Engineering optimization: an introduction with metaheuristic applications*. John Wiley & Sons.

Yang, X.-S. 2010. Firefly algorithm, Levy flights and global optimization. *In the Research and Development in Intelligent Systems XXVI* (pp. 209-218). Springer.

Yang, X.-S. 2010. Firefly algorithm, stochastic test functions and design optimisation. *International Journal of Bio-Inspired Computation.* **2**(2), 78-84.

Yang, X.-S. 2010. *Nature-inspired metaheuristic algorithms*. Luniver press.

Yang, X.-S. 2011. Metaheuristic optimization: algorithm analysis and open problems. *In the International Symposium on Experimental Algorithms*. (pp. 21-32). Springer.

Yang, X.-S. 2012. Efficiency analysis of swarm intelligence and randomization techniques. *Journal of Computational and Theoretical Nanoscience.* **9**(2), 189-198.

Yang, X.-S., Deb, S., and Fong, S. 2011. Accelerated particle swarm optimization and support vector machine for business optimization and applications. *In the International Conference on Networked Digital Technologies*. (pp. 53-66). Springer.

Yang, X.-S., and He, X. 2013. Firefly algorithm: recent advances and applications. *arXiv preprint arXiv:1308.3898.*

Yang, X.-S., Hosseini, S. S. S., and Gandomi, A. H. 2012. Firefly algorithm for solving non-convex economic dispatch problems with valve loading effect. *Applied Soft Computing.* **12**(3), 1180-1186.

Yelghi, A., and Köse, C. 2018. A modified firefly algorithm for global minimum optimization. *Applied Soft Computing.* **62**, 29-44.

Yin, X. 2010. S box construction and result analysis based on optimal tabu-genetic algorithm. *In the 2nd International Conference on Education Technology and Computer (ICETC), (*Vol. **3**, pp. 539 -542). IEEE.

Yong, W., and Peng, L. 2012. An improved method to obtaining S-box based on chaos and genetic algorithm. *HKIE Transactions.* **19**(4), 53-58.

Youssef, A. M., and Tavares, S. E. 2002. On Some Algebraic Structures in the AES Round Function. *IACR Cryptology ePrint Archive.* **2002**, 144.

Yu, S., Zhu, S., Ma, Y., and Mao, D. 2015. Enhancing firefly algorithm using generalized opposition-based learning. *Computing.* **97**(7), 741-754.

Zamli, K. Z., Alkazemi, B. Y., and Kendall, G. 2016. A tabu search hyper-heuristic strategy for t-way test suite generation. *Applied Soft Computing.* **44**, 57-74.

Zhang, L., Liu, L., Yang, X.-S., and Dai, Y. 2016. A novel hybrid firefly algorithm for global optimization. *PloSone.* **11**(9), e0163230.