Email: ifah@upm.edu.my

Office Address: Room 3.20. Block C, Faculty Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, Malaysia.

I have been appointed as Senior Lecturer at Department of Computer Science, Faculty Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor from 1st November 2011 until present. Currently, I am the Programme Coordinator of Master Information Security, Faculty Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, Malaysia. Also, I am also as a Research Associate and a member of INSPEM management meeting representing Cryptography Lab, Structure and Analysis, at Institute of Mathematical Research (INSPEM), UPM.

My research focuses on designing secure systems based on cryptographic techniques and finding new cryptographic techniques. I have involved with research related to block cipher, Elliptic Curve Cryptography, 3D Cellular Automata Cryptosystem, Searchable Ciphertext Policy Attribute Based Encryption (ABE) for medical record in blockchain and Iris authentication. My research interest related to authenticated encryption, lightweight block cipher for IOT, digital signature, formal verification of privacy, provable security, security solutions for IOT, cloud and blockchain.

List of publications:

Q1/Q2 Journal:

- Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Gutub, A. 2022. CSNTSteg: Color Spacing Normalization Text Steganography Model to Improve Capacity And Invisibility Of Hidden Data. IEEE Access.
- Thabit, R., Udzir, N. I., Yasin, S. M., Asmawi, A., Roslan, N. A., & Din, R. (2021). A Comparative Analysis of Arabic Text Steganography. Applied Sciences, 11(15), 6851.
- Hassan Mansur Hussien, **Sharifah Md Yasin**, Nur Izura Udzir, Mohd Izuan Hafez Ninggal, Sadeq Salman. 2021. Blockchain Technology in the Healthcare Industry: Trends and Opportunities. Journal of Industrial Information Integration Vol. 22, June 2021, 100217, pp. 1-64. https://doi.org/10.1016/j.jii.2021.100217
- Hassan Mansur Hussien, **Sharifah Md Yasin**, Nur Izura Udzir, and Mohd Izuan Hafez Ninggal. 2021. Blockchain-based access control scheme for secure

shared personal health records over decentralised storage. MDPI Sensors 2021, 21, 2462, pp. 1-36.
https://doi.org/10.3390/s21072462

- Amir Hamzah Abd Ghafar, Muhammad Rezal Kamel Ariffin, **Sharifah Md Yasin** and Siti Hasana Sapar. 2020. Partial Key Attack Given MSBs of CRT-RSA Private Keys. MDPI Mathematics 2020, Vol. 8, Issue 2188, pp. 1-20. doi:10.3390/math8122188
- Hasan Mansur Hussein, **Sharifah Md Yasin**, Nur Izura Udzir, A. A. Zaidan, B. B. Zaidan. 2019. Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. Journal of Medical Systems. Vol. 43 No. 320, pp. 1-35.

Scopus Journal:

- **Sharifah Md Yasin**, Ayman Majid Hamid, Nur Izura Udzir, Sherzod Turaev, Muhammad Rezal Kamel Ariffin. 2020. Key Dependent Dynamic S-Boxes Based on 3D Cellular Automata For Block Cipher. Journal of Theoretical and Applied Information Technology (JATIT), Vol. 98 No. 23, pp. 3808-3822.
- Reema Bin Thabit, Nur Izura Udzir, **Sharifah Md Yasin**, Aziah Asmawi, Nuur Alifah Roslan. 2020. A Comparative Analysis of Arabic Text Steganography. Journal Computer Speech and Language. (Accepted).
- Zeinab Vahdati, **Sharifah Md Yasin**, Ali Ghasempour, Mohammad Salehi. 2019. Comparison Of ECC And RSA Algorithms In IoT Devices. Journal Of Theoretical and Applied Information Technology (JATIT), Vol. 97, No. 16, pp. 4293-4308.
- Waleed K. AbdulRaheem, **Sharifah Md Yasin**, Nur Izura Udzir, Muhammad Rezal Kamel Ariffin. 2019. New Quintupling Point Arithmetic 5P Formulas For Lŏpez-Dahab Coordinate Over Binary Elliptic Curve Cryptography. (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 10 No. 7 (July) 2019, pp. 397- 401.
- Hassan Mansur Hussien, Zaiton Muda, **Sharifah Md Yasin** And, Nur Izura Udzir. 2019. Automatic Security Evaluation Of SPN-Structured Block Cipher Against Related-Key Differential Attacks Using Mixed Integer Linear Programming. Journal of Theoretical And Applied Information Technology (JATIT), Vol. 97, No. 7, pp. 1926-1936.
- Waleed K. AbdulRaheem, **Sharifah Md Yasin**, Nur Izura Udzir, Muhammad Rezal Kamel Ariffin. 2019. Improving the performance of {0,1,3}-NAF Recoding Algorithm for Elliptic Curve Scalar Multiplication. (IJACSA) International Journal of Advanced Computer Science and Applications, Volume 10 No. 4 (April) 2019, pp. 275-279.
- Hussien, H. M., Muda, Z., and **Yasin, S. M.** 2018. New Key Expansion Function Of Rijndael 128-Bit Resistance To The Related-Key Attacks. Journal of Information and Communication Technology, Vol. 17, No. 3 (July) 2018, pp: 409–434. https://doi.org/10.32890/jict2018.17.3.2802

- Nik Sakinah Nik Ab Aziz, **Sharifah Md Yasin** and Julia Juremi. 2019. The Review of Ternary Base Application for Adaptation in ECC. Journal of Advanced Research in Dynamical and Control Systems, Vol. 11, Special Issue No. 1, pp. 1398-1402.
- Nik Sakinah Nik Ab Aziz, **Sharifah Md Yasin** and Julia Juremi. 2018. The Review of Ternary Base Application for Adaptation in ECC. The 2nd Global Conference on Computing & Media Technology (2018), pp. 1-4.
- Julia Juremi, **Sharifah Md Yasin**, Nik Sakinah Nik Ab Aziz, Salasiah Sulaiman, Nurul Husna Mohd Saad. 2019. Determinant S-boxes for Substitution Function in Block Cipher Encryption Algorithm. Journal of Advanced Research in Dynamical and Control Systems, Vol. 11, Special Issue No. 1, pp. 1390-1397.
- Julia Juremi, **Sharifah Md Yasin**, Nik Sakinah Nik Ab Aziz, Salasiah Sulaiman, Nurul Husna Mohd Saad. 2018. Determinant S-boxes for Substitution Function in Block Cipher Encryption Algorithm. The 2nd Global Conference on Computing & Media Technology (2018), pp. 1-4.
- Chng Chern Wei, **Sharifah Md Yasin**, Mohd. Taufik Abdullah and Nur Izura Udzir. 2018. A Review of DNA-Based Block Cipher. International Journal of Computer Networks and Communications Security, Vol. 6, No. 9, September 2018, pp. 196–200.
- Chng Chern Wei, **Sharifah Md Yasin**, Mohd. Taufik Abdullah and Nur Izura Udzir. 2018. New DNA Based Dynamical S-Box for Block Cipher. Journal of Engineering Research and Application, Vol. 8, Issue 7 (Part -IV) July 2018, pp. 64-69. www.ijera.com.
- Julia Juremi, **Sharifah Md Yasin**, Salasiah Sulaiman, Nurul Husna Mohd Saad, Jazrin Ramli. 2018. A Survey on Various Dynamic S-box Implementation in Block Cipher Encryption Algorithm. Journal of Applied Technology and Innovation, Vol. 2, No. 1, pp. 1-4.
- Julia Juremi, Ramlan Mahmod, Zuriati Ahmad Zukarnain, **Sharifah Md Yasin**. (2017). Modified AES S-box Based on Determinant Matrix Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 7, Issue 1.
- Julia Juremi, **Sharifah Md Yasin**, Ramlan Mahmod, Zuriati Ahmad Zukarnain, Nur Izura Udzir. (2018). Determinant S-boxes for Substitution Function in BlockCipher Algorithm. Journal of Information Security and Applications. Manuscript number JISA_2018_251.
- Hassan Mansour Hussien Zaiton Muda, **Sharifah Md Yasin**. 2017. MILP-Based Approach To Evaluation Of Tweak-Aes-128 Bits Resistant To Related-Key Differential And Boomerang Attacks. UUM Press, International, pp. 1-28.
- Zaiton Muda, **Sharifah Md Yasin**. 2017. Image Orientation Based Watermarking Technique in Copyright Protection. Asian Research Publishing Network, International, pp. 629-644.
- Julia Juremi, Ramlan Mahmod, Zuriati Ahmad Zukarnain, Sharifah Md. Yasin. 2017. Modified AES S-Box Based on Determinant Matrix Algorithm. International Journal of Advanced Research in Computer Science and Software Engineering Vol. 7, Issue 1, pp. 110-116.
- Mohsen Bafandehkar, **Sharifah Md Yasin**, and Ramlan Mahmod 2016. Optimizing {0,1,3}-NAF Recoding Algorithm Using Block Method Technique in Elliptic Curve Cryptosystem. Journal Computer Science, Vol. 12, No. 11, pp. 534-544.

- Mohsen Bafandehkar, **Sharifah Md Yasin**, and Ramlan Mahmod 2015. A Literature Review on Scalar Recoding Algorithms in Elliptic Curve Cryptography. International Journal on Communications Antenna and Propagation (IRECAP), Vol. 5, No. 4, pp. 183-189.
- Miza Mumtaz Ahmad, **Sharifah Md Yasin**, Ramlan Mahmod, Mohamad Afendee Mohamed. 2015. X-Tract Recoding Algorithm For Minimal Hamming Weight Digit Set Conversion. Journal of Theoretical and Applied Information Technology JATIT, Vol. 75, No. 1, pp. 109-114.
- **Sharifah M.Yasin** and Zaiton Muda. 2015. Tripling Formulae of Elliptic Curve Over Binary Field in Lopez-Dahab Model. Journal of Theoretical and Applied Information Technology JATIT, Vol. 75, No 2, pp. 212-217.
- Zaiton Muda, Salasiah Sulaiman, **Sharifah Md Yasin** and Ramlan Mahmod. 2015. TShiftColumn: A New Transformation in 128-bit Rijndael Key Expansion to Improve Security Requirements. Journal of Theoretical and Applied Information Technology JATIT. Vol. 73. No. 1, pp. 130-136.
- **Sharifah M.Y.,** Ramlan Mahmod, Rozi Nor Haizan. 2015. Performance Analysis of Signed-digit {0,1,3}-NAF Scalar Multiplication Algorithm in Lopez-Dahab Model. Research Journal of Information Technology, pp. 1-21. DOI: 10.3923/rjit.2015.
- **Sharifah M.Y**., Rozi Nor Haizan, Jamilah Din, Zaiton Muda. 2014. {0,1,3}-NAF Representation and Algorithms for Lightweight Elliptic Curve Cryptosystem in Lopez Dahab Model. International Review on Computers and Software (IRECOS), 9(9):1541-1547. DOI: http://dx.doi.org/10.15866/irecos.v9i9.2659
- Mohsen Bafandehkar, **Sharifah Md Yasin**, Ramlan Mahmod, Zurina Mohd Hanapi, 2013. Comparison of ECC and RSA Algorithm in Resource Constrained Devices. International Conference on IT Convergence and Security (ICITCS), IEEE Conference Publications, pp. 1-3. DOI: 10.1109/ICITCS.2013.6717816
- Salasiah, S., Zaiton, M., Julia, J., Ramlan, M., **Sharifah, M.Y.** 2012. A New ShiftColumn Transformation: An Enhancement of Rijndael Key Scheduling. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 1(3):160-166.