Curriculum Vitae

Dr. Kunwar Singh

Address

Publications

Papers in SCI Journals

1. Kunwar Singh, C. Pandu Rangan, Richa Agarwal, Samir Sheshank "Lattice-based Unidirectional PRE and PRE+ Schemes ", IET Information Security (SCI), 2020 Accepted.

2. Kunwar Singh, C. Pandu Rangan, Richa Agarwal, Samir Sheshank "Provably Secure Lattice-Based Identity Based Unidirectional PRE and PRE+ Schemes ", Volume 54, Journal of Information Security and Applications (SCI) 2020.

3. Ch Koteswara Rao, Kunwar Singh "Securely Solving Privacy Preserving Minimum Spanning Tree Algorithms in Semi-honest Model", Vol.34 No.1, pp.1 - 10, Int. J. of Ad Hoc and Ubiquitous Computing (IJAHUC) (SCI) 2020.

4. Gaurav Srivastava, Richa Agrawal, Kunwar Singh, Rajeev Tripathi and Kshirasagar Naik "A Hierarchical Identity-based Security for Delay Tolerant Networks using Lattice-based Cryptography", Volume 13, Issue 1, pp 348 - 367 Peer-to-Peer Networking and Applications (SCI), Springer 2020.

5. KKC Deepti, Kunwar Singh: "Cryptanalysis of reduced round Salsa and ChaCha: Revisited". : Volume 13, Issue 6, November 2019, p. 591 – 602. IET Information Security (SCI).

6. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Identity Based Resplittable Threshold Public Key Encryption Scheme ", Volume 93:2, 289-307, International Journal of Computer Mathematics (SCI), June 2016, Taylor & Francis.

7. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Mix Network for Location Privacy in Mobile System", Volume 2015, Mobile Information Systems (SCIE), 2015, IOS Press.

Publications

Papers in SCOPUS Journals

1. Ch Koteswara Rao, Kunwar Singh "Oblivious Stable Sorting Protocol and Oblivious Binary Search Protocol for Secure Multi-party Computation ", Journal of High Speed Networks. Accepted.

2. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Universal Re-encryption for Mixnet", Journal of Information Science and Information Security (JISIS) (Scopus), volume 4, number 1, pp. 1-12, February, 2014.

3. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Identity Based Proxy Re-Encryption Scheme", Journal of Information Science and Information Security (JISIS) (Scopus), volume 3, number 3/4, pp. 38-51, November, 2013.

4. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice based efficient threshold public key encryption scheme", Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (jowua) (Scopus), volume: 4, number 4, pp. 93-107, November 2013. (This paper won **Best Paper Award** in international conference MIST 2013 and published in this journal)

5. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Forward-Secure Identity Based Encryption Schemes with Shorter Ciphertext", Journal of Information Science and Information Security (JISIS) (Scopus), volume 3, number 1/2, pp. 5-19, February, 2013.

6. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice Based Forward-Secure Identity Based Encryption Schemes", Journal of Information Science and Information security (JISIS) (Scopus), volume 2, number 3/4, pp. 118-128, November 2012.

Publications

Papers in Refereed Journals

1. Pratyush Dikshit and Kunwar Singh: "Weighted threshold ECDSA for securing bitcoin wallet", ACCENTS Transactions on Information Security, pp. 43-51, vol 2(6) 2017.

Presentations in International Conferences

1. Karthika SK, Kunwar Singh: "Theoretical Analysis of Biases in Chacha 128-bits "5th International Symposium on Mobile Internet Security (MobiSec 2021), Jeju Island, South Korea.

2. Sudarshan Parthasarathy, Akash Harikrishnan, Gautam Narayanan, Lohith J. J, Kunwar Singh "Secure Distributed Medical Record Storage using Blockchain and Emergency Sharing Using Multi-Party Computation", 3^{rd} International Workshop on Blockchains and Smart Contracts workshop (BSC 2021), Paris, France.

3. Ch Koteswara Rao, Kunwar Singh "Securely Solving Privacy Preserving Minimum Spanning Tree Algorithms in Semi-honest Model", international conference MobiSec 2018 held in Cebu, Phillipines.

4. Amalan Joseph Antony, Kunwar Singh: "Enhancing Privacy in a Blockchain-based Public Key Infrastructure". 2020 Third ISEA Conference on Security and Privacy (ISEA-ISAP), iit Guwahati. IEEE.

5. KKC Deepti, Kunwar Singh: "Cryptanalysis of Salsa and ChaCha: Revisited". 9^{th} EAI International Conference on Mobile Networks and Management (MONAMI 2017), December 13-15, 2017, Melbourne, Australia. Springer.

6. Pratyush Dikshit, Kunwar Singh: "Efficient Weighted Threshold ECDSA for Securing Bitcoin Wallet". Asia Security Privacy 2017, NIT Surat. IEEE.

7. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Lattice based Identity based Unidirectional Proxy Re-Encryption Scheme". Accepted in SPACE 2014, LNCS, Springer-Verlag, 2014.

8. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Efficient Lattice HIBE in the Standard Model with Shorter Public Parameters". AsiaARES 2014, Bali, Indonesia, April 2014, LNCS, Springer-Verlag, 2014.

9. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Cryptanalysis of Unidirectional Proxy Re-Encryption Scheme". AsiaARES 2014, Bali, Indonesia, April 2014, LNCS, Springer-Verlag, 2014.

10. Prashant Kumar Mishra, Kunwar Singh, Sudhanshu Baruntar: "ID-Based Threshold Signcryption and Group Unsigncryption ". SNDS 2012, Trivendrum, India, October 2012, pages 35-44. Springer-Verlag, 2012.

11. Kunwar Singh, C. Pandu Rangan, A. K. Banerjee: "Adaptively Secure Efficient Lattice (H)IBE in Standard Model with Short Public Parameters". SPACE 2012, Chennai, India, October 2012, LNCS, pages 153-172. Springer-Verlag, 2012.

12. Kunwar Singh: "Identity based signcryption revisited ". IEEE International Conference on Information Technology and e-Services (ICITeS'2012) March 24-26 Sousse, Tunisia.

Presentations in National Conferences

1. Pratyush Dikshit, Kunwar Singh: "Weighted Threshold ECDSA for Securing Bitcoin Wallet". NWC 2017, Shivamogga, Karnataka.