List of Publications

International Journal Publications

1. **Donghoon Chang**, Nilanjan Datta, Avijit Dutta, Bart Mennink, Mridul Nandi, Somitra Sanadhya, and Ferdinand Sibleyras, "Release of Unverified Plaintext: Tight Unified Model and Application to ANYDAE", Accepted to The IACR Transactions on Symmetric Cryptology (ToSC), 2019.
2. Naina Gupta, Arpan Jati, Anupam Chattopadhyay, Somitra Kumar Sanadhya, and **Donghoon Chang**, "Threshold Implementations of GIFT: A Trade-off Analysis", Accepted to IEEE Transactions on Information Forensics & Security, 2019.
3. **Donghoon Chang**, Mohona Ghosh , Arpan Jati, Abhishek Kumar and Somitra Kumar Sanadhya, "A Generalized Format Preserving Encryption Framework Using MDS Matrices,", Journal of Hardware and Systems Security, Springer Berlin Heidelberg, Volume 3, Issue 1, pp 3–11, March 2019.
4. Megha Agrawal, **Donghoon Chang**, Jinkeon Kang, "Deterministic Authenticated Encryption Scheme for Memory Constrained Devices," Cryptography 2018, 2(4), 37; https://doi.org/10.3390/cryptography2040037.
5. Akshima, **Donghoon Chang**, Aarushi Goel, Sweta Mishra, Somitra Kumar Sanadhya, " *Generation of Secure and Reliable Honeywords, Preventing False Detection*", IEEE Transactions on Dependable and Secure Computing, IEEE, pp. 1-18, April, 2018. Print ISSN: 1545-5971, DOI 10.1109/TDSC.2018.2824323.
6. Megha Agrawal, Tarun Kumar Bansal, **Donghoon Chang**, Amit Kumar Chauhan, Seokhie Hong, Jinkeon Kang and Somitra Kumar Sanadhya, "RCB: Leakage-Resilient Authenticated Encryption via Re-keying", Journal of Supercomputing (ISSN: 1573-0484) (SCI), September 2018, Volume 74, Issue 9, pp 4173–4198.
7. **Donghoon Chang**, Abhishek Kumar, Somitra Kumar Sanadhya, "Distinguishers for 4-branch and 8-branch Generalized Feistel Network", IEEE Access 5 (SCI-E), pp. 27857-27867 (2017).
8. Tarun Kumar Bansal, **Donghoon Chang**, Somitra Kumar Sanadhya, "Sponge based CCA2 secure asymmetric encryption for arbitrary length message", International Journal of Advanced Computer Technology (IJACT) 3(3), pp. 262-287, 2017.
9. Megha Agrawal, **Donghoon Chang**, Somitra Kumar Sanadhya, "A New Authenticated Encryption Technique for Handling Long Ciphertexts in Memory Constrained Devices", International Journal of Advanced Computer Technology (IJACT) 3(3), pp. 236-261, 2017.
10. **Donghoon Chang**, Somitra Kumar Sanadhya, Monika Singh., "Security Analysis of mvHash-B Similarity Hashing", Journal of Digital Forensics, Security and Law (JDFSL), Vol. 11 (2), 2016.
11. **Donghoon Chang**, Mridul Nandi, Jesang Lee, Jeachul Sung, Seokhie Hong, Jongin Lim, Haeryong Park and Kilsoo Chun. "Compression Function Design Principles Supporting Variable Output Lengths from a Single Small Function", IEICE Transaction on Fundamentals (SCI-E), vol E91-A, no.9, pp. 2607-2614, September 2008.

12. Wonil Lee, Mridul Nandi, Palash Sarkar, **Donghoon Chang**, Sangjin Lee and Kouichi Sakurai, "PGV-style Block-Cipher-Based Hash Families and Black-Box Analysis", IEICE Transaction on Fundamentals (SCI-E), vol E88-A, no.1, pp. 39-48, January 2005.
13. Wonil Lee, **Donghoon Chang**, Sangjin Lee, Soo Hak Sung, Mridul Nandi, "Construction of UOWHF : Two New Parallel Methods", IEICE Transaction on Fundamentals (SCI-E), vol E88-A, no.1, pp. 49-58, January 2005.

International Conference

1. **Donghoon Chang**, Vinjohn Chirakkal, Shubham Goswami, Munawar Hasan, Taekwon Jung, Jinkeon Kang, Seok-Cheol Kee, Dongkyu Lee, Ajit Pratap Singh, "Multi-lane Detection Using Instance Segmentation and Attentive Voting", 19th International Conference on Control, Automation and Systems (ICCAS 2019) Oct. 15~18, 2019; ICC Jeju, Jeju, Korea.
2. **Donghoon Chang**, Mohona Ghosh , Somitra Kumar Sanadhya , Monika Singh, Douglas White, "FbHash: A New Similarity Hashing Scheme for Digital Forensics,", Digital Forensic Research Workshop (DFRWS), accepted, March, 2019.
3. Megha Agrawal, Tianxiang Huang, Jianying Zhou and **Donghoon Chang**, "CAN-FD-Sec: Improving Security of CAN-FD Protocol", International Workshop on Cyber Security for Intelligent Transportation (CSITS), to be appeared, 2018.
4. Pawel Drozdowski, Surabhi Garg, Christian Rathgeb, Marta Gomez-Barrero, **Donghoon Chang**, Christoph Busch, "*Privacy-Preserving Indexing of Iris-Codes with Cancelable Bloom Filter-based Search Structures",* EUSIPCO 2018, Special Session: Security and Privacy in Biometrics, To be appeared.
5. **Donghoon Chang**, Amit Kumar Chauhan, Sandeep Kumar, Somitra Kumar Sanadhya, "Revocable Identity-Based Encryption from Codes with Rank Metric", CT-RSA 2018, 435-451.
6. **Donghoon Chang**, Mohona Ghosh, Arpan Jati, Abhishek Kumar and Somitra Sanadhya. "eSPF: A Family of Format-Preserving Encryption Algorithms using MDS Matrices", SPACE 2017, pp. 133-150.
7. **Donghoon Chang**, Mohona Ghosh, Kishan Chand Gupta, Arpan Jati, Abhishek Kumar, Dukjae Moon, Indranil Ghosh Ray and Somitra Kumar Sanadhya, "SPF: A New Family of Efficient Format-Preserving Encryption Algorithms", Inscrypt 2016, LNCS 10143.
8. Debapriya Basu Roy, Avik Chakraborti, **Donghoon Chang**, S V Dilip Kumar, Debdeep Mukhopadhyay and Mridul Nandi, "Fault Based Almost Universal Forgeries on CLOC and SILC", SPACE 2016, LNSC 10076.
9. **Donghoon Chang**, Amit Kumar Chauhan, Naina Gupta, Arpan Jati, and Somitra Sanadhya, "Exploiting the Leakage: Analysis of some Authenticated Encryption schemes", SPACE 2016, LNCS 10076.
10. **Donghoon Chang**, Sumesh Manjunath R., Somitra Kumar Sanadhya, "PPAE: Practical Parazoa Authenticated Encryption Family", ProvSec 2015: 198-211.

11. **Donghoon Chang**, Amit Kumar Chauhan, Muhammed Noufal K, Jinkeon Kang, "Apollo: End-to-End Verifiable Voting Protocol Using Mixnet and Hidden Tweaks", ICISC 2015: 194-209.
12. Akshima, **Donghoon Chang**, Mohona Ghosh, Aarushi Goel, Somitra Kumar Sanadhya, "Single Key Recovery Attacks on 9-Round Kalyna-128/256 and Kalyna-256/512", ICISC 2015: 119-135.
13. **Donghoon Chang**, Somitra Sanadhya and Nishant Sharma, "New HMAC Message Patches: Secret Patch and CrOw Patch", ICISS 2015, December 16 -20, 2015, Kolkata, India.
14. Akshima, **Donghoon Chang**, Mohona Ghosh, Aarushi Goel and Somitra Kumar Sanadhya, "Improved Meet-in-the-Middle Attacks on 7 and 8-round ARIA-192 and ARIA-256", Indocrypt 2015, December 06 -10, 2015, Bangalore, India.
15. **Donghoon Chang**, Somitra Kumar Sanadhya, Monika Singh and Robin Verma, "A collision attack on sdHash similarity hashing", SADFE 2015, September 30 – October 2, 2015, Malaga, Spain.
16. Tarun Kumar Bansal, **Donghoon Chang**, Somitra Kumar Sanadhya, "Sponge based CCA2 secure asymetric encryption for arbitrary length message", ACISP 2015, June 29-July 1, 2015, Brisbane, Australia.
17. Megha Agrawal, **Donghoon Chang**, Somitra Kumar Sanadhya, "sp-ALEM: Sponge based authenticated encryption scheme for memory constrained devices", ACISP 2015, June 29-July 1, 2015, Brisbane, Australia.
18. **Donghoon Chang**, Arpan Jati, Sweta Mishra, Somitra Kumar Sanadhya, "Time Memory Tradeoff Analysis of Graphs in Password Hashing Constructions", Passwords 2014, December 8-10, Trondheim, Norway.
19. **Donghoon Chang**, Arpan Jati, Sweta Mishra, Somitra Kumar Sanadhya, "Cryptographic module based approach for password hashing scheme", Passwords 2014, December 8-10, Trondheim, Norway.
20. **Donghoon Chang**, Arpan Jati, Sweta Mishra, Somitra Kumar Sanadhya, "Rig - A simple, secure and flexible design for Password Hashing", Inscrypt 2014, December 13-15, Beijing, China.
21. Megha Agrawal, **Donghoon Chang**, Mohona Ghosh, Somitra Kumar Sanadhya, "Collision attack on 4-branch Type-2 GFN based hash functions using sliced biclique cryptanalysis technique", Inscrypt 2014, December 13-15, Beijing, China.
22. Andrey Bogdanov, **Donghoon Chang**, Mohona Ghosh, Somitra Kumar Sanadhya, "Bicliques with Minimal Data and Time Complexity for AES", ICISC 2014, December 3-5, 2014, Seoul, Korea.
23. **Donghoon Chang**, Arnab Kumar, Pawel Morawiecki, Somitra Kumar Sanadhya, "1st and 2nd Preimage Attacks on 7, 8 and 9 Rounds of SHA3-224,256,384,512", SHA-3 2014 Workshop organized by NIST, August 22, 2014, UCSB, Santa Barbara, USA.
24. **Donghoon Chang**, Abhishek Kumar, Somitra Kumar Sanadhya, "Security analysis of GFN: 8 round distinguisher for 4-branch type-2 GFN", Indocrypt 2013, Mumbai, December 7-10, 2013.
25. **Donghoon Chang**, "Sufficient Conditions on Padding Schemes of Sponge Construction and Sponge-Based Authenticated-Encryption Scheme", INDOCRYPT 2012. Volume 7668/2012.

26. **Donghoon Chang**, Mridul Nandi and Moti Yung, "A Keyed Sponge Construction with Pseudorandomness in the Standard Model", The Third SHA-3 Candidate Conference, 2012.http://csrc.nist.gov/groups/ST/hash/sha-3/Round3/March2012/Program_SHA3_March2012.html
27. **Donghoon Chang**, Mridul Nandi and Moti Yung, "On the Security of Hash Functions Employing Blockcipher Postprocessing", FSE 2011. Volume 6733/2011.
28. **Donghoon Chang** and Mridul Nandi, "Improved indifferentiability security analysis of chopMD Hash Function", FSE 2008. Volume 5086/2008.
29. Eunjin Lee, **Donghoon Chang**, Jongsung Kim, Jaechul Sung and Seokhie Hong, "Second Preimage Attack on 3-Pass HAVAL and Partial Key-Recovery Attacks on HMAC/NMAC-3-Pass HAVAL", FSE 2008. Volume 5086/2008.
30. **Donghoon Chang**, Moti Yung, Jaechul Sung, Seokhie Hong and Sangjin Lee, "Preimage Attack on the Parallel FFT-Hashing Function", ACISP 2007. Volume 4586/2007.
31. Eunjin Lee, Deukjo Hong, **Donghoon Chang**, Seokhie Hong and Jongin Lim, "A Weak Key Class of XTEA for a Related-Key Rectangle Attack", VIETCRYPT 2006. Volume 4341/2006.
32. **Donghoon Chang**, Kishan Chand Gupta and Mridul Nandi, "RC4-Hash : A New Hash Function based on RC4", INDOCRYPT 2006. Volume 4329/2006.
33. **Donghoon Chang**, Sangjin Lee, Mridul Nandi and Moti Yung, "Indifferentiable Security Analysis of Popular Hash Function with prefix-free padding", ASIACRYPT 2006. Volume 4284/2006.
34. Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, **Donghoon Chang**, Jaesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim and Seongtaek Chee, "HIGHT: A New Block Cipher Suitable for Low-Resource Device", CHES 2006. Volume 4249/2006.
35. Deukjo Hong, **Donghoon Chang**, Jaechul Sung, Sangjin Lee, Seokhie Hong, Jaesang Lee, Dukjae Moon and Sungtaek Chee, "A New Dedicated 256-Bit Hash Function: FORK-256", FSE 2006. Volume 4047/2006.
36. Aaram Yun, Soo Hak Sung, Sangwoo Park, **Donghoon Chang**, Seokhie Hong and Hong-Su Cho, "Finding Collision on 45-Step HAS-160", ICISC 2005. Volume 3935/2006.
37. **Donghoon Chang**, Wonil Lee, Seokhie Hong, Jaechul Sung, Sangjin Lee and Soo Hak Sung, "Impossibility of Construction of OWHF and UOWHF from PGV Model Based on Block Cipher Secure Against ACPCA", INDOCRYPT 2004. Volume 3348/2004.
38. Wonil Lee, Mridul Nandi, Palash Sarkar, **Donghoon Chang**, Sangjin Lee and Kouichi Sakurai, "A Generalization of PGV Hash Functions and Its Security Analysis in Black-Box Model", ACISP 2004. Volume 3108/2004.
39. Wonil Lee, **Donghoon Chang**, Sangjin Lee, Soohak Sung and Mridul Nandi, "New parallel tree based constructions of UOWHF", ASIACRYPT 2003. Volume 2894/2003.
40. Seokhie Hong, Deukjo Hong, Youngdai Ko, **Donghoon Chang**, Wonil Lee and Sangjin Lee, "Differential Cryptanalysis of TEA and XTEA", ICISC 2003. Volume 2971/2004.

41. **Donghoon Chang**, Jaechul Sung, Soo Hak Sung, Sangjin Lee and Jongin Lim, "Full-Round Differential Attack on the Original Version of the Hash Function Proposed at PKC'98", SAC 2002. Volume 2595/2003.