Journal of Hardware and Systems Security (2019) 3:1–2
https://doi.org/10.1007/s41635-019-00067-9

Guest Editorial SPACE 2017 Special Issue in the Journal of Hardware and Systems Security (HaSS)

Sk Subidh Ali[1] · **Debdeep Mukhopadhyay**[2]

Received: 21 February 2019 / Accepted: 12 March 2019 / Published online: 23 March 2019

Abstract

This special issue of Hardware and Systems Security contains six papers shortlisted from the Seventh International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2017) conducted in Goa, Indian, December 13–17, 2017. SPACE 2017 was organized in cooperation with the International Association for Cryptologic Research (IACR) and Cryptology Research Society of India (CRSI).

This special issue of Hardware and Systems Security contains six papers shortlisted from the Seventh International Conference on Security, Privacy and Applied Cryptographic Engineering (SPACE 2017) conducted in Goa, India, December 13–17, 2017 [1]. SPACE 2017 was organized in cooperation with the International Association for Cryptologic Research (IACR) and Cryptology Research Society of India (CRSI). SPACE is considered to be one of the key international venues for the leading scientist to present recent development in the field of hardware security research.

SPACE 2017 received 49 anonymous submissions from about eight different countries. The submissions were reviewed in a double-blind mode by at least three members of the 36-member Program Committee. The Program Committee was aided by 50 external reviewers. The submission was evaluated based on their significance, novelty, technical quality, and relevance to the scope of hardware security and applied cryptography. After intensive review process, the Program Committee selected 14 papers for publications, corresponding to 28% acceptance rate.

The aim of this special issue is to extend the best contributions of SPACE 2017 in both theoretical and experimental aspects. Hence, out of 14 papers presented in SPACE 2017, top seven papers were selected and the corresponding authors were invited to submit extended manuscripts to this special issue of Hardware and Systems Security (HASS). These extended manuscripts went through scientific journal peer review process and finally six manuscripts were selected for the publication in this issue, with an effective acceptance rate of 12%.

This special issue covers a wide range of hardware security topics such as state-of-the-art side-channel analysis attack and defense mechanism, PUF, implementation aspects of crypto-primitives, and security issues in android OS.

The paper "IPA: An Instruction Profiling based Micro-Architectural Side-Channel Attack on Block Ciphers" by Manaar Alam et al. analyzes the leakage from the hardware performance counter and proposes a micro-architectural side-channel attack. It recovers the secret key by observing the number of instruction counts during the execution of an encryption algorithm as side-channel information to recover the secret key. The proposed attack analysis is performed on AES and Clefia. The results acquired from Intel as well as from AMD machines show that the proposed attack is more potent than the the state-of-the-art cache timing attacks. Overall, the paper presents interesting results on side-channel vulnerability of HPC.

The paper "A Generalized Format Preserving Encryption Framework Using MDS Matrices" by Abhishek Kumar et al. presents a new family of SPN-based Format Preserving Encryption (FPE) algorithms. The aim of these new alogorithms is to improve the performance and flexibility of the SPF. The proposed algorithms use a MDS matrix as the optimal diffusion of MDS matrix leads to an efficient and secure design. A detailed security and performance analysis

✉ Sk Subidh Ali
subidh@iitbhilai.ac.in

Debdeep Mukhopadhyay
debdeep@cse.iitkgp.ac.in

[1] Indian Institute of Technology Bhilai, Raipur, India

[2] Indian Institute of Technology Kharagpur, Kharagpur, India

is also provided corresponding to different use cases of the algorithms, which shows that the proposed design is approximately 10 times faster than the existing technique for most of the practical applications.

The paper "Variable-Length Bit Mapping and Error-Correcting Codes for Higher-Order Alphabet PUFs" by Vincent Immler et al. describes the lacuna in the implementation of PUF-based secret key. In general, PUF-based secret keys are implemented by either directly evaluating a binary output or by mapping symbols from a higher-order alphabet to a fixed-length bit sequence, which if combined with equidistant quantization may lead to significant bias in the derived secret. In order to improve this security drawback of exiting design technique, the paper proposes a variable-length bit mapping that utilizes the Levenshtein metric. The proposed new approach effectively counteracts the bias in the derived key already at the input side of the ECC. Overall, the proposed technique increases the effective output bit length of the secret key by over 40% as compared to state-of-the-art approaches.

The paper "Analysis of diagonal constants for extension of Salsa to 64 bit" by Bhagwan Bathe et al. presents a differential cryptanalysis of Salsa. The aim is to see the effect of diagonal constants on biases after certain rounds of operations. The authors have shown that if an input differential is created at the MSB of the third word of quarterround function, then after 4 rounds, the value of Measure of Uniformity in bias either increases or decreases which is determined by the specific pattern in 4 Least Significant Bits (LSB) of first word (which is constant) of quarterround function. Subsequently, the last two rotation constants of corresponding quarterround function will identify the pattern within that diagonal constant. This is indeed an interesting property of Salsa. Using this property of Salsa, the authors have designed a 64-bit Salsa 32-bit version of Salsa, which performs 1.6 to 1.7 times faster as compared to the similar implementation of 32-bit Salsa on a 64-bit machine.

The paper "Public-key Encryption with Integrated Keyword Search" by Vishal Saraswat et al. presents strong construction PKE+PEKS. The public key encryption with keyword search (PEKS) is a searching technique in encrypted data, which is majorly used in public cloud. The authors of the paper present a concrete PKE+PEKS scheme and prove that the scheme is both IND-PKE-CCA secure as well as IND-PEKS-CCA secure. The key advantages of the proposed scheme are of two folds: in one it is extremely fast as it uses asymmetric pairings on the other side the scheme has much shorter ciphertexts.

The paper "Certain Observations on ACORN v3 and Grain v1 – Implications towards TMDTO Attacks" by Akhilesh et al. presents advanced Time-Memory-Data Trade-Off attack. A stream cipher is vulnerable to Time-Memory-Data Trade-Off attack if the state size is less than 2.5 times than the key size. However, in general, the attack complexity is limited due to complexity in solving multiple equations deduced from state bits. The authors used SAT solving techniques to solve those equations and obtain better parameters. The technique is implemented on ACORN v3 and Grain v1. The results show improvement in the TMDTO attacks.

We hope that you enjoy reading this selection of top papers from SPACE 2017 and get benefited by the broad coverage and cutting edge research that is part of the SPACE community.

Acknowledgements We would like to thank all authors and reviewers for their sincere efforts in producing these high-quality articles. We also take this opportunity to extend our heartiest thank to the HaSS editors and administrative staff for their assistance in successfully delivering this special issue.

References

1. Ali SS, Danger J, Eisenbarth T (2017) Security, privacy, and applied cryptography engineering. In: 7th International Conference, SPACE 2017, Goa, India, December 13-17, 2017, Proceedings, Lecture Notes in Computer Science, vol 10662. Springer. https://doi.org/10.1007/978-3-319-71501-8