An Interdisciplinary Workshop on

Machine Learning for Cryptology

(November 22 – 23, 2024)

INDIAN STATISTICAL INSTITUTE
203, B. T. ROAD, KOLKATA – 700108

Organised by:
Centre for Artificial Intelligence and Machine Learning (CAIML), ISI Kolkata
and
Scientific Analysis Group (SAG), DRDO, Ministry of Defence, Government of India

Program Details

Day 1: November 22, 2024		
10:30 – 11:00	Registration	
11:00 – 11:30	Inaugural Session	Background Details and Welcoming to the Workshop
11:30 – 12:00	High Tea/Coffee Break	
12:00 – 13:00	Technical Session I	AI for enhancing and breaking ciphers: Recent results and research directions Saibal K. Pal Defence Research and Development Organisation, India
13:00 – 14:30	Lunch Break	
14:30 – 15:30	Technical Session II	On (Pseudo)Random Number Generation Mridul Nandi Indian Statistical Institute, Kolkata
15:30 – 16:00	Tea/Coffee Break	
16:00 – 17:00	Technical Session III	Physical Attacks on Post-Quantum Cryptography for Embedded Devices and its linkages to Machine Learning Prasanna Ravi Nanyang Technological University, Singapore
17:00 – 17:30	Photo Session	
17:30 – 18:30	Visit to the Geology Museum	
18:30 – 20:30	Banquet	
Day 2: November 23, 2024		
10:30 – 11:30	Technical Session IV	ML-based Improved Differential Distinguisher with High Accuracy Manoj Kumar Defence Research and Development Organisation, India
11:30 – 12:00	High Tea/Coffee Break	
12:00 – 13:00	Technical Session V	Leveraging Synergy to Design Neural Differential Distinguishers for Lightweight Block Ciphers Arpita Sarkar Indian Statistical Institute, Kolkata
13:00 – 14:30	Lunch Break	
14:30 – 15:30	Data Science Challenge Session	Presentations by the best performing team(s)
15:30 – 16:00	Tea/Coffee Break	
16:00 – 17:00	Technical Session VI	Robustness against Poisoning under Local Differential Privacy Amrita Roy Chowdhury University of Michigan, Ann Arbor, USA
17:00 – 17:30	Offering of Certificates	

VENUE for Different Sessions: Room No. 401, 4th Floor, Library Building, ISI, Kolkata
VENUE for Lunch and Banquet: Guest House, ISI, Kolkata
GEOLOGY MUSEUM: Ground Floor, PJA Building, ISI, Kolkata

Details of Technical Talks

AI for enhancing and breaking ciphers: Recent results and research directions

Saibal K. Pal

Defence Research and Development Organisation, India

Abstract: The last decade has attracted significant innovations & investments in the field of cryptography. Rapid growth in communications technology, digital and quantum computing and artificial intelligence have thrown new challenges and fuelled new developments in this domain. This talk would cover recent progress in cryptology and role of ML techniques for enhancement and automation of these human-intensive processes.

Interpretable AI, self-evolving ML models and hypernetworks with potential applications in cryptology would be covered. Progress in neural cryptanalysis and choice of neural architectures would be taken up with the goal of developing models that can outperform classical approaches. Specific role of Generative AI techniques for improving the strength of ciphers would also be elaborated.

Speaker's Bio: Dr. Saibal Kumar Pal is working as OS & Scientist 'H' and heads the Cryptology Division at DRDO, Scientific Analysis Group, Delhi. He has also served as the Chief Information Security Officer (CISO) of DRDO during the period 2017 – 2019. Dr. Pal completed Post-graduation in Computer Science from University of Allahabad & PhD from University of Delhi in the area of Information Security. He also holds a PhD in Brand Management. Dr. Pal has co-authored 6 books, 3 patents & has more than 300 peer-reviewed research publications. His areas of interest are Cryptography, Cyber Security, Computational Intelligence and Quantum Information Processing. He has contributed in a number of significant R&D projects as the Project Director and international collaborations as co-investigator. Dr. Pal is a recipient of Lab Scientist Award and DRDO Scientist of the Year Award.

On (Pseudo)Random Number Generation

Mridul Nandi

Indian Statistical Institute, Kolkata

Abstract: In this talk, we discuss (i) the need of random numbers in Cryptography and (ii) the methods to generate (pseudo) random number using classical computer. Although a true random number is what we aim for, generating pseudorandom number suffices our purpose. We briefly discuss what do we mean by pseudorandom number and see some method of analysis of randomness. We see how cryptographic primitives like blockcipher and stream ciphers are related to random number generators.

Speaker's Bio: Prof. Mridul Nandi is a Professor in the Applied Statistics Unit of the Indian Statistical Institute, Kolkata in India. His main research area is Symmetric Cryptography. My research focusses on cryptographic algorithms and security analysis. He completed BStat, MStat and Ph.D from Indian Statistical Institute, Kolkata in 1999, 2001 and 2005, respectively. Before joining Indian Statistical Institute, he was a Postdoctoral Fellow in the CACR, Waterloo University (worked with Professor Douglas Stinson), Scientist in IPN, CINVESTAV, Mexico, visiting researcher in National Institute of Standard and Technology and George Washington University, USA. Prof. Nandi is a CAESAR Winner.

Physical Attacks on Post-Quantum Cryptography for Embedded Devices and its linkages to Machine Learning

Prasanna Ravi

Nanyang Technological University, Singapore

Abstract: Large-scale quantum computers pose a significant threat to today's public key cryptography standards, such as RSA and ECC, as they can solve the underlying mathematical problems in polynomial time using Shor's algorithm, discovered in 1994. In response, the global cryptographic community has been developing quantum-resistant alternatives known as Post-Quantum Cryptography (PQC). To advance PQC adoption, the National Institute for Standards and Technology (NIST) began a standardization process in 2017, selecting four algorithms after five years of rigorous evaluation. These algorithms are now being integrated into secure communication systems, like Google Chrome and Apple's iMessage. Over time, PQC will need to be widely implemented across all software applications and hardware devices, including embedded systems in cyber-physical environments.

In embedded systems, where attackers may have physical access to devices, PQC introduces the challenge of defending against physical attacks like Side-Channel Analysis (SCA) and Fault Injection Analysis (FIA). These attacks exploit vulnerabilities in hardware implementations, and NIST has taken this into account by choosing PQC schemes that are more resilient and cost-effective to protect against physical threats. This talk will explore the susceptibility of NIST-standardized PQC algorithms, particularly Kyber (ML-KEM) and Dilithium (ML-DSA), particularly to side-channel attacks on embedded devices like microcontrollers and FPGAs. We will demonstrate that these algorithms possess inherent traits that make them vulnerable to such attacks. Several of these attacks have been shown to be more effective when using machine-learning techniques to analyse side-channel measurements resulting in easier key-recovery attacks. This talk mainly highlights the utilization of machine-learning approaches that enable sophisticated side-channel attacks on PQC implementations. This therefore raises the need for further research into countermeasures against physical attacks, particularly for PQC implementations, keeping in mind advanced attacks exploiting machine-learning based approaches.

Speaker's Bio: Dr. Prasanna Ravi is working as a Research Scientist at the Center for Hardware Assurance in Temasek Labs at Nanyang Technological University, Singapore. He obtained his PhD in the topic of Side-Channel Analysis (SCA) and Fault-Injection Analysis (FIA) of Post-Quantum Lattice-based Cryptography in 2023 from Nanyang Technological University, Singapore. Apart from using SCA and FIA to assess the strength of cryptographic implementations, he also works on using SCA and FIA to test the security features of embedded devices such as Secure Boot, Debug Interface Protection, Trusted Execution Environment.

ML-based Improved Differential Distinguisher with High Accuracy

Manoj Kumar

Defence Research and Development Organisation, India

Abstract: The first application of ML in cryptanalysis was proposed by Gohr at CRYPTO 2019 through an ML based differential distinguisher for SPECK32/64. Yadav and Kumar proposed the first extension of ML with classical differential distinguisher at Latincrypt-2021. This distinguisher was called as differential-ML distinguisher which covered more rounds then the ML and classical alone. ML based differential cryptanalysis is based on the machine learning model that uses encrypted data to learn its features using available compute power. This poses a restriction on the accuracy of ML distinguisher for increased number of rounds and ciphers with large block size. Moreover, we can still construct the distinguisher but the accuracy becomes very low in such cases.

In this talk, a new approach to improve the accuracy of a differential distinguisher using machine learning will be presented. The construction of high accuracy ML based distinguishers using full/partial output blocks will be discussed for GIFT-128 and ASCON permutation. The application of the approach to construct 7-round distinguisher for GIFT-128 and 4-round distinguisher for ASCON will be presented with improvements in the existing results. Differential-ML based distinguisher for 8 rounds of GIFT-128 with 99.8% accuracy and 2^18 data complexity will also be discussed which is the best ML based distinguihser in terms of accuracy.

Speaker's Bio: Dr. Manoj Kumar is currently working as a Scientist 'E' in the Scientific Analysis Group, Defence Research and Development Organisation, Delhi, India. His primary areas of research encompass Cryptology, Block Cipher, Hash Function and Differential Cryptanalysis. He has more than 20 publications to his credit in different journals and conferences. Dr. Kumar has designed multiple novel lightweight block ciphers and hash functions in the last couple of decades. Some of these include RAZOR, FeW, HeW and Neeva.

Leveraging Synergy to Design Neural Differential Distinguishers for Lightweight Block Ciphers

Arpita Sarkar

Indian Statistical Institute, Kolkata

Abstract: Lightweight block ciphers like SPECK, SIMON, and PRESENT are widely deployed in resource-constrained environments, ensuring their resilience against differential cryptanalysis remains essential. Recent developments in machine learning-assisted cryptanalysis, such as Gohr's neural differential distinguishers (NDDs), have paved the way for breakthroughs by outperforming traditional methods on reduced-round ciphers. This talk embarks on a journey to expand these capabilities by introducing a novel data fusion technique, enabling more robust NDDs for a wider array of round-reduced ciphers, including SPECK, SIMON, and PRESENT.

Our data fusion approach combines ciphertexts of successive rounds to capture not only individual round information but also the synergistic (cooperative) interactions between rounds, which significantly boost the distinguishing power of

our neural models. This results in notably higher accuracy and allows us to break through more cipher rounds than previous works.

I will present findings that demonstrate the effectiveness of this approach, with our NDDs successfully analyzing up to 9 rounds of SPECK 32/64, 8 rounds of SPECK 64/128, 11 rounds of SIMON 32/64, 12 rounds of SIMON 48/96, 14 rounds of SIMON 64/128, and 9 rounds of PRESENT 64/80. These results highlight the promise of machine learning-assisted cryptanalysis in enhancing lightweight cipher security and mark a significant advancement in leveraging round interactions through data fusion.

Speaker's Bio: Arpita Sarkar is a Post-Doctoral Fellow at the Centre for Artificial Intelligence and Machine Learning, Indian Statistical Institute (ISI), Kolkata. She has specialized in machine learning-assisted cryptanalysis, cryptography, network security, and biometric cryptosystems. Her current research focuses on constructing neural differential distinguishers for lightweight block ciphers such as SPECK, SIMON, and PRESENT, employing novel data fusion techniques to enhance differential cryptanalysis. With prior experience at IIT Guwahati's MARS Lab, she brings over three years of postdoctoral research expertise to her work in advancing cryptographic security through innovative machine learning methods.

Robustness against Poisoning under Local Differential Privacy

Amrita Roy Chowdhury

University of Michigan, Ann Arbor, USA

Abstract: Today, data is generated on billions of smart devices at the edge, leading to a decentralized data ecosystem comprising multiple data owners (clients) and a service provider (server). The clients interact with the server with their personal data for specific services, while the server performs analysis on the joint dataset. However, as an untrusted entity, the server is often incentivized to extract as much information as possible, potentially compromising the clients' privacy. Local Differential Privacy (LDP) has emerged as a leading solution for privacy in decentralized data analytics. Yet, as its adoption grows, it is essential to examine its vulnerabilities. The decentralized nature of LDP makes it vulnerable to poisoning attacks, where adversaries can inject fake clients that provide poisoned or malformed data. In this talk, we will explore solutions to provide provable robustness against such attacks. Specifically, we will analyze how LDP protocols possess a unique characteristic that distinguishes them from non-private ones —the clear separation between the input and the final response (obtained after randomization). This separation provides adversaries with two distinct opportunities to tamper with the data. We will discuss strategies to mitigate both types of tampering by applying them in real-world settings and exploring the associated challenges.

Speaker's Bio: Amrita Roy Chowdhury is an Assistant Professor at the University of Michigan, Ann Arbor. Her work explores the synergy between differential privacy and cryptography through novel algorithms that expose the rich interconnections between the two areas, both in theory and practice. She has been recognized as a Rising Star in EECS in 2020 and 2021, and a UChicago Rising Star in Data Science, 2021. She is also the recipient of the 2021 CRA/CCC Computing Innovations Fellowship.