# 12th International Conference on Security, Privacy, and Applied Cryptography Engineering

# SPACE 2022

@

LNMIIT Jaipur

December 9-12, 2022

LNMIIT

The LNM Institute of Information Technology

Dr. Jayaprakash Kar

## Brief Summary

International Conference on Security, Privacy and Applied Cryptographic Engineering 2022 (SPACE 2022) is twelfth in the series of conferences which started in 2011. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering and will be held in cooperation with International Association for Cryptologic Research (IACR).SPACE 2022 will be held from 9th to 12th December, 2022. The program co-chairs for SPACE 2022 are Lejla Batina (Radboud University, The Netherlands), Stjepan Picek (TU Delft, The Netherlands) and Mainack Mondal (Indian Institute of Technology, Kharagpur).

## About the Event

### Event Overview

- **Date:** **December 09–12, 2022**
- **Venue:** The event was held in Hybrid mode at the LNMIIT Jaipur.
- **Organizers:** The LNMIIT Jaipur,<br>General Chair, Jayaprakash Kar<br>Organizing Chair, Dr. Shweta Bhandari

**Resource Person/s**:

1. Ingrid Verbauwhede, KU Leuven, Belgium
2. Jeyavijayan Rajendran, TAMU, USA
3. Chester Rebeiro, IIT Madras, India
4. Nele Mentens, KU Leuven, Belgium
5. Sanjay K. Jha, UNSW, Sydney
6. Łukasz Chmielewski, Radboud University The Netherlands
7. Lejla Batina, Radboud University The Netherlands
8. Stjepan Picek, Radboud University The Netherlands
9. Sikhar Patranabis, IBM Research, India
10. Nitin Singh, IBM Research, India
11. Matthias Kannwischer, Academica Sinica Taiwan

### Purpose

International Conference on Security, Privacy and Applied Cryptographic Engineering 2022 (SPACE 2022) is twelfth in the series of conferences which started in 2011. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering and will be held in cooperation with International Association for Cryptologic Research (IACR).SPACE 2022 will be held from 9th to 12th December, 2022. The program co-chairs for SPACE 2022 are Lejla Batina (Radboud University, The Netherlands), Stjepan Picek (TU Delft, The Netherlands) and Mainack Mondal (Indian Institute of Technology, Kharagpur).

### Outcome:

17 Research papers were presented and published. The proceeding is available at:
https://link.springer.com/book/10.1007/978-3-031-22829-2#toc

### Editors of the proceedings are:

Lejla Batina,
Radboud University,
The Netherlands

Stjepan Picek,
Radboud University,
The Netherlands

Mainack Mondal,
Indian Institute of Technology,
Kharagpur, India

## About the conference

The 12th International Conference on Security, Privacy, and Applied Cryptography Engineering 2022 (SPACE 2022), was held during December 9–12, 2022. This annual event is devoted to various aspects of security, privacy, applied cryptography, and cryptographic engineering. This is a challenging field, requiring expertise from diverse domains, ranging from mathematics and computer science to circuit design. The event was hosted by the Center for Cryptography, Cyber Security and Digital Forensics (C3-SDF) at The LNM Institute of Information Technology, Jaipur, India. This year we received 61 submissions from authors in many different countries, mainly from Asia and Europe. The submissions were evaluated based on their significance, novelty, technical quality, and relevance to the SPACE conference. The submissions were reviewed in a double-blind mode by at least two members of the Program Committee, which consisted of 47 members from all over the world. After an extensive review process, 18 papers were accepted for presentation at the conference, leading to an acceptance rate of 29.5%. The program also included five keynotes and four tutorials on various aspects of applied cryptology, security, and privacy delivered by world-renowned researchers: Ingrid Verbauwhede, Nele Mentens, Jeyavijayan "JV" Rajendran, Chester Rebeiro, Sanjay K. Jha, Łukasz Chmielewski, Sikhar Patranabis, Nitin Singh, and Matthias Kannwischer. We sincerely thank the invited speakers for accepting our invitations in spite of their busy schedules. As in previous editions, SPACE 2022 was organized in cooperation with the International Association for Cryptologic Research (IACR). We are grateful to general chairs Jayaprakash Kar and Debdeep Mukhopadhyay for their willingness to host it physically at LMNIT Jaipur. There is a long list of volunteers who invested their time and energy to put together the conference. We are grateful to all the members of the Program Committee and their sub-reviewers for all their hard work in the evaluation of the submitted papers. We thank our publisher Springer for agreeing to continue to publish the SPACE proceedings as a volume in the Lecture Notes in Computer Science (LNCS) series. We are grateful to the local Organizing Committee who invested a lot of time and effort in order for the conference to run smoothly. Last, but not least, our sincere thanks go to all the authors who submitted papers to SPACE 2022 and everyone who participated (either in person or virtually).
December 2022
Lejla Batina
Stjepan Picek
Mainack Monda

| | |
|---|---|
| **Chief Patron** | Rahul Banerjee LNMIIT Jaipur, India |
| **General Chair** | Jayaprakash Kar LNMIIT Jaipur, India |
| | Debdeep Mukhopadhyay Indian Institute of Technology, Kharagpur, India |
| **Organizing Chair** | Shweta Bhandari LNMIIT Jaipur, India |

## Organizing Committee

Sakthi Balan LNMIIT Jaipur, India
Subrat Dash LNMIIT Jaipur, India
Usha Kanoongo LNMIIT Jaipur, India
Mukesh Jadon LNMIIT Jaipur, India
Sandeep Saini  LNMIIT Jaipur, India
Chirag Kumar LNMIIT Jaipur, India
Kusum Lata LNMIIT Jaipur, India
Mukesh Sharma  LNMIIT Jaipur, India

**Program Committee Chairs**

Lejla Batina Radboud University, The Netherlands
Stjepan Picek, Radboud University, The Netherlands
Mainack Mondal, Indian Institute of Technology, Kharagpur, India

**Program Committee**

| | |
|---|---|
| Amr Youssef | Concordia University, Canada |
| Anupam Chattopadhyay | Nanyang Technological University, Singapore |
| Bodhisatwa Mazumdar | Indian Institute of Technology, Indore, India |
| Bohan Yang | Tsinghua University, China |
| Chester Rebeiro | Indian Institute of Technology, Madras, India |
| Chitchanok Chuengsatiansup | University of Adelaide, Australia |
| Claude Carlet | University of Bergen, Norway & University of Paris 8, France |
| Debdeep Mukhopadhyay (General co- chair) | Indian Institute of Technology, Kharagpur, India |
| Dirmanto Jap | Temasek Lab, Nanyang Technological University, Singapore |
| Domenic Forte | University of. Florida, USA |
| Eran Toch | Tel Aviv University, Israel |
| Fan Zhang | Zhejiang University, China |
| Guilherme Perin | TU Delft, The Netherlands |
| Ileana Buhan | Radboud University, The Netherlands |
| Jakub Breier | Silicon Austria Labs, Austria |
| Jayprakash Kar (General chair) | The LNM Institute of Information Technology, Jaipur, India |
| Jean-Luc Danger | Télécom Paris, France |
| Kazuo Sakiyama | University of Electro-Communications, Tokyo, Japan |
| Kerstin Lemke-Rust | Bonn-Rhein-Sieg University of Applied Sciences, Germany |
| Kostas Papagiannopoulos | University of Amsterdam, The Netherlands |
| Lejla Batina (PC co-chair) | Radboud University, The Netherlands |
| Luca Mariot | TU Delft, The Netherlands |
| Lukasz Chmielewski | Radboud University, The Netherlands |
| Mael Gay | University of Stuttgart |
| Mainack Mondal (PC co-chair) | Indian Institute of Technology, Kharagpur, India |
| Marc Stoettinger | Hessen3C, Germany |
| Marc Manzano TII | Abu Dhabi |
| Martin Henze | Fraunhofer FKIE, Germany |

| | |
|---|---|
| Md Masoom Rabbani | KU Leuven, Belgium |
| Nadia El Mrabet | SAS - CGCP – EMSE |
| Nalla Anandakumar Nachimuthu | University of Florida, USA |
| Naofumi Homma | Tohoku University, Japan |
| Olga Gadyatskaya | LIACS, Leiden University, The Netherlands |
| Peter Schwabe | MPI-SP, Germany & Radboud University, The Netherlands |
| Rahul Chatterjee | University of Wisconsin-Madison |
| Rajat Subhra Chakraborty | Indian Institute of Technology, Kharagpur, India |
| Rajesh Pillai | SAG, DRDO |
| Ruben Niederhagen | University of Southern Denmark, Denmark |
| Sébastien Canard | Orange Labs |
| Shivam Bhasin | Temasek Lab, Nanyang Technological University, Singapore |
| Sikhar Patranabis | Visa Research, USA |
| Silvia Mella | STMicroelectronics, Italy |
| Sk Subidh Ali | Indian Institute of Technology, Bhilai, India |
| Somitra Sanadhya | Indian Institute of Technology, Jodhpur, India |
| Soumyajit Dey | Indian Institute of Technology, Kharagpur, India |
| Stjepan Picek (PC co-chair) | Radboud University, The Netherlands |
| Sujoy Sinha Roy | IAIK, TU Graz, Austria |
| Urbi Chatterjee | Indian Institute of Technology, Kanpur, India |
| Vishal Saraswat | Bosch Engineering and Business Solutions, Bengaluru, India |

## Additional Reviewers

| | |
|---|---|
| Martin Serror | Fraunhofer FKIE, Germany |
| Wenping Zhu | Tsinghua University, China |
| Soumyadyuti Ghosh | Indian Institute of Technology, Kharagpur, India |
| Rajat Sadhukhan | Indian Institute of Technology, Kharagpur, India |
| Durba Chatterjee | Indian Institute of Technology, Kharagpur, India |

**Number of Participants :-** 46

## Sponsors & Co-Organizers

National Centre of Excellence
CYBERSECURITY TECHNOLOGY AND ENTREPRENEURSHIP

DRDO
DEFENCE R&D ORGANISATION
MINISTRY OF DEFENCE

SAFE

Springer
Lecture Notes in Computer Science

tcs Research

# Invited Talks

### Hardware: an essential partner to cryptography

Ingrid Verbauwhede
KU Leuven, Belgium

Cryptography is a beautiful branch of mathematics with a nice purpose of providing information security. To be useful in practical applications, the algorithms run on hardware or software, with software ultimately running also on hardware processors. This presentation covers multiple links of this relation between hardware and cryptography. The goal is to provide insights to the cryptographer, so that more efficient and secure cryptographic algorithms and protocols are developed. Important topics linking both include:
Hardware provides the means to accelerate the computationally demanding operations, as is currently the case for the new generation of post-quantum algorithms.

A very nice aspect of cryptography is that it reduces what needs to be kept secret to the keys, while the algorithms can be publicly known. The hardware is responsible to keep the key(s) secret. Side-channel, fault-attacks and other physical attacks make this a challenging task. Provable Secure mathematical countermeasures against physical attacks rely on models to abstract how the hardware behaves. Unfortunately, the models are often the weak link between theory and practice and it results in broken implementations. Hardware also provides essential building blocks to security. Protocols rely on nonces and freshness from random numbers. Generating full entropy random numbers is a challenge. We can conclude that hardware is an essential partner to cryptography to provide the promised information security.

### Building Secure Systems Bottom Up: Hunting down hardware security vulnerabilities.

Jeyavijayan Rajendran
TAMU, USA

Hardware is at the heart of computing systems. For decades, software was considered error-prone and vulnerable. However, recent years have seen a rise in attacks exploiting hardware vulnerabilities and exploits. Such vulnerabilities are prevalent in hardware for several reasons: First, the existing functional verification and validation approaches do not account for security, motivating the need for new and radical approaches such as hardware fuzzing. Second, existing defense solutions, mostly based on heuristics, do not undergo rigorous red-teaming exercises like cryptographic algorithms; I will talk about how emerging artificial intelligence (AI) can rapidly help red-team such techniques. Last and most important, students and practitioners who are typically trained in designing, testing, and verification are not rigorously trained in cybersecurity -- for many reasons, including a lack of resources, time, and methodologies; I will talk about how AI can be incorporated into (hardware) cybersecurity education.

### Towards Secure Computing Systems

Chester Rebeiro
IIT Madras, India

Over the last four decades, microprocessor research has focused on improving performance. Various micro architectural features such as cache memories, branch prediction, superscalar, speculative and out-of-order execution, were developed to facilitate this. Side-by-side, features such as multiprogramming, multicore and hardware multithreading were incorporated to increase throughput. These features allowed multiple users to simultaneously share a processor. To isolate one user's program from another, rudimentary security schemes such as protection rings and page table access control bits were used. Very soon it was realized that these security schemes were insufficient. Vulnerabilities in software permitted user space programs to gain privileged access. Shared hardware became a source of information leaks that could undermine the isolation provided. The very features in the processor that were incorporated to boost performance and throughput have now become a security liability.

Hardening microprocessors for security requires rethinking of processor design, where security is considered as a primary design criteria along with performance, energy, and area. This is quite a challenge because incorporating security often comes with significant overheads. Tradeoffs would need to be made to achieve sufficient security with acceptable overheads in the other design parameters. Furthermore, security threats can arise across the computing stack — from hardware, micro-architecture, to system and application software. One solution will not fix all threats; each threat would need to be handled separately. In this talk, we will discuss some of our recent and ongoing research in developing secure microprocessors. We will discuss Hardware enabled memory protection schemes and the design of power attack protected microprocessors; micro-compartments, and support for functional programming languages that can considerably reduce software vulnerabilities.

### Security challenges and opportunities in emerging device technologies

Nele Mentens
KU Leuven, Belgium

While traditional chips in bulk silicon technology are widely used for reliable and highly efficient systems, there are applications that call for devices in other technologies. On the one hand, novel device technologies need to be re-evaluated with respect to potential threats and attacks, and how these can be faced with existing and novel security solutions and methods. On the other hand, emerging device technologies bring opportunities for building the secure systems of the future. This talk gives an overview of the minimal hardware resources that are needed to build secure systems and of the state of the art in security research in emerging device technologies.

### Security Challenges in Internet of Things (IoT) and Cyber-Physical Systems (CPS)

Sanjay K. Jha
UNSW, Sydney

In this talk, I will introduce the broad range of research under the UNSW Institute for Cyber Security. Then I will discuss technical work close to the title of this talk: on how the community is converging towards the IoT vision having worked in wireless sensor networking and Machine-2-Machine (M2M) communication. This will follow a general discussion of security challenges in IoT. I will discuss some results from my recent projects on security in the IoT domain. This will include physical layer secure key generation, and application of advanced ML techniques to event spoofing attacks, and traffic obfuscation to investigate the privacy of a Smart Home. I will conclude my talk with a description of a new project on Distributed Energy Resource Management Security.

### Attacking Real-World Crypto with Side-Channel Analysis

Łukasz Chmielewski
Radboud University The Netherlands

Modern cryptography has produced a multitude of ciphers that protect our daily lives including secure authentication, electronic transactions, etc. However, once the cipher is implemented on a physical device (microprocessor, FPGA, ASIC, etc.) it becomes vulnerable to side-channel and fault attacks. Side-channel attacks pose a unique challenge as an intersection of cryptography, electronics, and statistics and pervading all aspects of modern hardware security. The attackers monitor closely the power consumption or electromagnetic emission of a cryptographic device and they are able to extract the secret key using statistical techniques. This tutorial will provide an overview of various classes of side-channel attacks, showcasing the core techniques for key recovery. During the tutorial, the students will get the chance to develop some basic side-channel analysis tools in Python. Subsequently, they will use the tools to attack real-world datasets aiming at secret key extraction.

### Profiling Side-channel Analysis: From Template Attack to Deep Learning

Lejla Batina
Radboud University The Netherlands

Modern cryptography has produced a multitude of secure ciphers that protect our daily electronic transactions. However, once the cipher is implemented on a physical device (microprocessor, FPGA, ASIC, etc.) it becomes vulnerable to side-channel attacks. Side-channel attacks pose a unique challenge as an intersection of cryptography, electronics, and statistics and pervading all aspects of modern hardware security. The attacks closely monitor the power consumption or electromagnetic emission of a cryptographic device and they are able to extract the secret key using statistical techniques. More recently, we are witnessing the up-rise of deep learning techniques in SCA, even for targets protected with countermeasures. In this tutorial, we will start with template attacks and progress to the machine learning and deep learning techniques, finishing with state-of-the-art and future challenges

### Profiling Side-channel Analysis: From Template Attack to Deep Learning

Stjepan Picek
Radboud University The Netherlands

Modern cryptography has produced a multitude of secure ciphers that protect our daily electronic transactions. However, once the cipher is implemented on a physical device (microprocessor, FPGA, ASIC, etc.) it becomes vulnerable to side-channel attacks. Side-channel attacks pose a unique challenge as an intersection of cryptography, electronics, and statistics and pervading all aspects of modern hardware security. The attacks closely monitor the power consumption or electromagnetic emission of a cryptographic device and they are able to extract the secret key using statistical techniques. More recently, we are witnessing the up-rise of deep learning techniques in SCA, even for targets protected with countermeasures. In this tutorial, we will start with template attacks and progress to the machine learning and deep learning techniques, finishing with state-of-the-art and future challenges

### Zero-Knowledge Proofs in Practice: Demystifying Blockchain Rollups

Sikhar Patranabis
IBM Research, India

How does one convince you that a Sudoku puzzle is solvable without revealing the solution itself? Can someone convince you that they own a bitcoin without revealing the actual bitcoin? Sounds impossible? Zero-knowledge proof (ZKP) is a revolutionary cryptographic technique that enables the seemingly impossible, such as the above.

In a more real-world setting, ZKP allows a cloud server to convince its clients about the correctness of an expensive computation, while making minimal demands on the clients' storage and compute capabilities. It turns out that this capability is what makes ZKP the "secret sauce" behind one of the trendiest buzzwords in the blockchain world - the "rollups".

In this tutorial, we will walk the participants through an interactive and (hopefully) fun hands-on exercise of building a demo rollup on a toy Ethereum network (with "fake" Ether as the cryptocurrency). The entire tutorial will use a gamut of open-source tools for emulating a blockchain network (e.g., Ganache), interacting with the blockchain network (e.g., Truffle), and generating, verifying, deploying ZKPs in smart contracts (using Circom and SnarkJS). We will combine these tools to achieve the end-goal of implementing a prototype rollup system that illustrates the core challenges behind popular layer-2 offerings from Polygon, zkSync etc. We will conclude by foreshadowing an alternative approach to designing rollups that extends the ideas in the tutorial, and is plausibly more scalable in certain settings.

In addition to the above interactive exercise, we will also provide the necessary background on blockchain rollups and ZKPs. The content of the tutorial should be accessible to CS/ECE/EE undergraduates. No background in cryptography will be assumed. Some basic familiarity with blockchain is likely to be useful, though not mandatory.

The presenters also acknowledge Abhishek Singh (research engineer at IBM Research India) for his contributions and support towards the material presented in the tutorial.

## Zero-Knowledge Proofs in Practice: Demystifying Blockchain Rollups

Nitin Singh
IBM Research, India

How does one convince you that a Sudoku puzzle is solvable without revealing the solution itself? Can someone convince you that they own a bitcoin without revealing the actual bitcoin? Sounds impossible? Zero-knowledge proof (ZKP) is a revolutionary cryptographic technique that enables the seemingly impossible, such as the above. In a more real-world setting, ZKP allows a cloud server to convince its clients about the correctness of an expensive computation, while making minimal demands on the clients' storage and compute capabilities. It turns out that this capability is what makes ZKP the "secret sauce" behind one of the trendiest buzzwords in the blockchain world - the "rollups". In this tutorial, we will walk the participants through an interactive and (hopefully) fun hands-on exercise of building a demo rollup on a toy Ethereum network (with "fake" Ether as the cryptocurrency). The entire tutorial will use a gamut of open-source tools for emulating a blockchain network (e.g., Ganache), interacting with the blockchain network (e.g., Truffle), and generating, verifying, deploying ZKPs in smart contracts (using Circom and SnarkJS). We will combine these tools to achieve the end-goal of implementing a prototype rollup system that illustrates the core challenges behind popular layer-2 offerings from Polygon, zkSync etc. We will conclude by foreshadowing an alternative approach to designing rollups that extends the ideas in the tutorial, and is plausibly more scalable in certain settings.

In addition to the above interactive exercise, we will also provide the necessary background on blockchain rollups and ZKPs. The content of the tutorial should be accessible to CS/ECE/EE undergraduates. No background in cryptography will be assumed. Some basic familiarity with blockchain is likely to be useful, though not mandatory.
The presenters also acknowledge Abhishek Singh (research engineer at IBM Research India) for his contributions and support towards the material presented in the tutorial.

### Implementing Kyber and Dilithium

Matthias Kannwischer
Academica Sinica Taiwan

In July 2022, the US National Institute of Standards and Technology (NIST) announced the first set of post-quantum schemes to be standardized: Kyber, Dilithium, Falcon, and SPHINCS+. It is expected that NIST will publish its first post-quantum cryptography standard including those schemes soon. This tutorial will cover the implementation of the lattice-based key-encapsulation mechanism Kyber and the digital signature scheme Dilithium. I will introduce the core construction of the schemes and essential implementation techniques. This will cover number-theoretic transforms, Montgomery multiplication, and Plantard multiplication.
Participants will then implement their own number-theoretic transforms for Kyber and Dilithium using Arm Cortex-M4 assembly. Instructions will be provided to functionally test the implementations on an Arm Cortex-M4 emulated using qemu (version 5.2 or newer). For measuring the performance, a small number of STM32F407 development boards will available during the tutorial.
Participants should follow the pre-tutorial instructions available at the Github link. In particular, please install arm-none-eabi-gcc, qemu, and st-link. The 'hello world' program should successfully run on qemu before the tutorial.

## Accepted and Published Papers

### Symmetric Cryptography-

1. Modeling Large S-box in MILP and a (Related-key) Differential Attack on Full Round PIPO-64/128 Tarun Yadav and Manoj Kumar (Scientific Analysis Group, DRDO, India
2. Light but Tight: Lightweight Composition of Serialized S-Boxes with Diffusion Layers for Strong Ciphers Rajat Sadhukhan, Anirban Chakraborty, Nilanjan Datta, Sikhar Patranabis and Debdeep Mukhopadhyay (IIT Kharagpur, India / IAI, TCG Crest, India / IBM Research, India)
3. Hardware Implementation of Masked SKINNY SBox with Application to AEAD Mustafa Khairallah and Shivam Bhasin (NTU Singapore, Singapore / Seagate research, Singapore)

4. Bias Cancellation of MixColumns Subhadeep Banik, Andrea Caforio, Kostas Papagiannopoulos and Francesco Regazzoni (Università della Svizzera Italiana, Lugano, Switzerland / LASEC, Ecole Polytechnique Fédérale de Lausanne, Switzerland / University of Amsterdam, The Netherlands)
5. Big Brother Is Watching You: A Closer Look At Backdoor Construction Anubhab Baksi, Arghya Bhattacharjee, Jakub Breier, Takanori Isobe and Mridul Nandi (NTU Singapore, Singapore / ISI Kolkata, India / Silicon Austria Labs, Graz, Austria / University of Hyogo, Kobe, Japan)

**Public-Key Cryptography, Post-quantum Cryptography, Zero Knowledge Proofs-**

6. Protecting the most significant bits in scalar multiplication algorithms Estuardo Alpirez Bock, Lukasz Chmielewski and Konstantina Miteloudi (Aalto University, Finland / Masaryk University, Czech Republic / Radboud University, Nijmegen, The Netherlands)
7. KEMTLS vs. Post-Quantum TLS: Performance on Embedded Systems Ruben Gonzalez and Thom Wiggers (Neodyme AG, Garching, Germany / Radboud University, Nijmegen, The Netherlands)
8. Card-based zero-knowledge proof for the nearest neighbor property: Zero-knowledge proof of ABC end view Takuro Fukasawa and Yoshifumi Manabe (Kogakuin University, Shinjuku,Tokyo, Japan)
9. Combining Montgomery Multiplication with Tag Tracing for the Pollard ' s Rho Algorithm in Prime Order Fields Madhurima Mukhopadhyay and Palash Sarkar (IIT Kanpur, India / ISI Kolkata, India)

**Hardware Security and AI-**

10. Dual-Tone Multi-Frequency Assisted Acoustic Side Channel Attack to Retrieve Dialled Call Log Abhishek Revskar, Mahendra Rathor and Urbi Chatterjee (IIT Kanpur, India)
11. What Do You See? Transforming Fault Injection Target Characterizations Marina Krček (Delft University of Technology, The Netherlands)
12. HWGN2: Side-channel Protected NNs through Secure and Private Function Evaluation Mohammad Hashemi, Steffi Roy, Domenic Forte and Fatemeh Ganji (Worcester Polytechnic Institute, MA, USA / University of Florida, Florida, USA)
13. Machine Learning Attacks on Low-Cost Reconfigurable XRRO and XRBR PUF Designs Manthan Kojage, Neelofar Hassan and Urbi Chatterjee (IIT Kanpur, India)
14. How Many Cameras Do You Need? Adversarial Attacks and Countermeasures for Robust Perception in Autonomous Vehicles Tu A. Ngo, Reuben J. Chia, Jonathan Chan, Nandish Chattopadhyay and Anupam Chattopadhyay (NTU Singapore, Singapore)

SMarT: A SMT based Privacy Preserving Smart Meter Streaming Methodology Soumyadyuti Ghosh, Soumyajit Dey and Debdeep Mukhopadhyay (IIT Kharagpur, India)

**Network Security, Authentication, and Privacy-**

15. An analysis of the hardware-friendliness of AMQ data structures for network security Arish Sateesan, Jo Vliegen and Nele Mentens (imec-COSIC/ES&S, ESAT, KU Leuven, Belgium / LIACS, Leiden University, The Netherlands)
16. SMarT: A SMT based Privacy Preserving Smart Meter Streaming Methodology Soumyadyuti Ghosh, Soumyajit Dey and Debdeep Mukhopadhyay (IIT Kharagpur, India)
17. RemOD: Operational Drift-adaptive Intrusion Detection Vikas Maurya, Nanda Rani and Sandeep Shukla (IIT Kanpur, India) A short note on a paper titled A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection using Topology Code for local registration and security enhancement SrinivasaRao SubramanyaRao (Cybersecurity Researcher and Consultant, Canberra, Australia)
18. A short note on a paper titled A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection using Topology Code for local registration and security enhancement SrinivasaRao SubramanyaRao (Cybersecurity Researcher and Consultant, Canberra, Australia)

**Few snaps**

Some of the pictures of the conference are shown below:

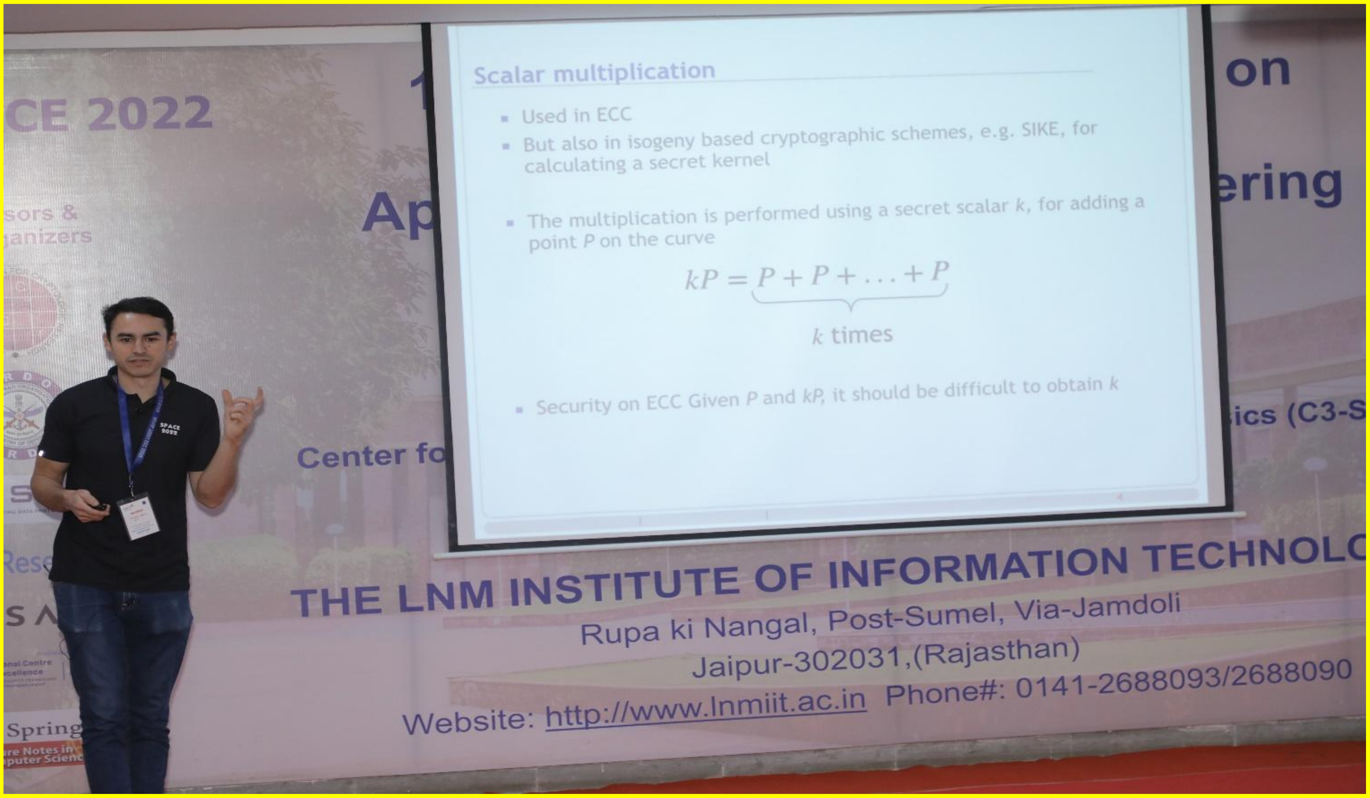
SPACE 2022
12th International Conference on
Security, Priva
ed Cryptogra
neering
December 9-
Sponsors & Co-organizers
LNMIIT
DSCI
tcs Research
SAFE

SPACE 2022
Sponsors & Co-organizers
on
Ap
ering
LNMIIT
The LNM Institute of Information Technology
Sponsors & Co-organizers
Center fo
sics (C3-SDF)
KU LEUVEN
DSCI
tcs Research
SAFE
C-HERD
Springer
Lecture Notes in Computer Science
THE LNM INSTITUTE OF INFORMATION TECHNOLOGY
Rupa ki Nangal, Post-Sumel, Via-Jamdoli
Jaipur-302031,(Rajasthan)
Website: http://www.lnmiit.ac.in Phone#: 0141-2688093/2688090

the real measurements
amming weight of the
(1)
ering
Co-organizers
NAL ASSOCIATION FOR CRYPTOLOG
GROTH16
PLONK
There is a valid sigs
s (C3-SD
AMATIO
NNOLOGY
hel, Via-Jar
jasthan)
e#: 0141-268
88090
National Centre of Excellence
C-HERD
Springer
Lecture Notes in Computer Science

SPACE 2022
12th International Conference on Security, Privacy and Applied Cryptographic Engineering
December 9-12, 2022
Organized by:
Center for Cryptography, Cyber Security and Digital Forensics (C3-SDF)
The LNMIIT, Jaipur, India
THE LNM INSTITUTE OF INFORMATION TECHNOLOGY
LNMIIT
The LNM Institute of Information Technology
Sponsors & Co-organizers
DSCI
TCS Research
SAFE

LNMIIT
The LNM Institute of Information Technology
Sponsors & Co-organizers



## Scalar multiplication

- Used in ECC
- But also in isogeny based cryptographic schemes, e.g. SIKE, for calculating a secret kernel
- The multiplication is performed using a secret scalar $k$, for adding a point $P$ on the curve

$$kP = \underbrace{P + P + \ldots + P}_{k \text{ times}}$$

- Security on ECC Given $P$ and $kP$, it should be difficult to obtain $k$

CE 2022
on
Ap
ering
sors &
ganizers
Center fo
ics (C3-S
SPACE 2022
THE LNM INSTITUTE OF INFORMATION TECHNOLO
Rupa ki Nangal, Post-Sumel, Via-Jamdoli
Jaipur-302031,(Rajasthan)
Website: http://www.lnmiit.ac.in Phone#: 0141-2688093/2688090