## Leakage Resilience of the Duplex and Suffix Sponge Construction With Application to ISAP

### (Dr. Bart Mennink, Radboud University)

Abstract: Side-channel attacks, especially differential power analysis (DPA), pose a serious threat to cryptographic implementations deployed in a malicious environment. One way to counter side-channel attacks is to design cryptographic schemes to withstand them, an area that is covered among others by leakage resilient cryptography. So far, however, leakage resilient cryptography has predominantly focused on block cipher based designs, and insights in permutation based leakage resilient cryptography were scarce. This presentation covers three recent results on permutation based leakage resilience.

First, we consider leakage resilience of the keyed duplex construction: we present a model for leakage resilient duplexing, derive a fine-grained bound on the security of the keyed duplex in said model, and demonstrate how to use the duplex for encryption in a leakage resilient manner. Second, we prove leakage resilience of the suffix keyed sponge construction, a pseudorandom function that consists of hashing its data using the (keyless) sponge construction, transforming part of the state using the secret key, and generating the tag from the output of a final permutation call. Third, we consider the ISAP authenticated encryption scheme, a finalist in the NIST Lightweight Cryptography competition. We demonstrate how the first two results can be combined to obtain a bound on the leakage resilience of the ISAP construction.

## Security and Privacy issues in Machine Learning

### (Dr. Sourav Sengupta, NTU Singapore)

Abstract : In the evolving arena of Machine Learning, usability, efficiency and scalability have taken the front-stage during the last couple of decades. The industry did not pay too much attention to security and privacy of data or models in the context of ML and AI in the first lap of the run, till legal and regulatory frameworks like GDPR and PDPA knocked at our doors. In the second lap of ML and AI development, we see the industry getting more cautious about the privacy of data as well as the security of models. Hopefully, in the next lap, ML and AI engineers will consider security and privacy by design into the models and applications they build, so that it is not an afterthought any more. In this talk, we will touch upon a few important security and privacy issues in ML and AI, with an emphasis on Federated Learning, where the model leverages on distributed (local) training to aggregate the knowledge from multiple nodes training in parallel. Although some familiarity with Cryptography and Machine Learning will help, no prior knowledge on Federated Learning is expected. Just bring your interest and questions!

## Deniable Fully Homomorphic Encryption from LWE

## (Dr. Shweta Agrawal, IIT Madras)

Abstract: We define and construct Deniable Fully Homomorphic Encryption based on the Learning With Errors (LWE) polynomial hardness assumption. Deniable FHE enables storing encrypted data in the cloud to be processed securely without decryption, maintaining deniability of the encrypted data, as well the prevention of vote-buying in electronic voting schemes where encrypted votes can be tallied without decryption.

Our constructions achieve compactness independently of the level of deniability- both the size of the public key and the size of the ciphertexts are bounded by a fixed polynomial, independent of the faking probability achieved by the scheme. This is in contrast to all previous constructions of deniable encryption schemes (even without requiring homomorphisms) which are based on polynomial hardness assumptions, originating with the seminal work of Canetti, Dwork, Naor and Ostrovsky (CRYPTO 1997) in which the ciphertext size grows with the inverse of the faking probability. Canetti et al. argued that this dependence “seems inherent”, but our constructions illustrate this is not the case. The running time of our encryption algorithm depends on the inverse of the faking probability, thus the scheme falls short of achieving simultaneously compactness, negligible deniability and polynomial encryption time. Yet, we believe that achieving compactness is a fundamental step on the way to achieving all properties simultaneously as has been the historical journey for other primitives such as functional encryption.

Interestingly, we note that our constructions support large message spaces, whereas previous constructions were bit by bit, and can be run in online-offline model of encryption, where the bulk of computation is independent of the message and may be performed in an offline pre-processing phase. The running time of the online phase, is independent of the faking probability, whereas the offline encryption run-time grows with the inverse of the faking probability. At the heart of our constructions is a new way to use bootstrapping to obliviously generate FHE ciphertexts so that it supports faking under coercion.

This is a joint work with Saleet Mossel and Shafi Goldwasser

## 3PAA: A Private PUF Protocol for Anonymous Authentication

## (Dr. Urbi Chatterjee, IIT Kanpur)

Abstract: Anonymous authentication (AA) schemes are used by an application provider to grant services to its *n* users for pre-defined *k* times after they have authenticated themselves anonymously. These privacy-preserving cryptographic schemes are essentially based on the secret key that is embedded in a trusted platform module (TPM). In this work, we propose a private physically unclonable function (PUF) based scheme that overcomes the shortcomings of prior attempts to incorporate PUF for AA schemes. Traditional PUF based authentication protocols have their limitations as they only work based on challenge-response pairs (CRPs) exposed to the verifier, thus violating the principle of anonymity. Here, we ensure that even if the PUF instance is private to the user, it can be used for authentication to the application provider. Besides, no

raw CRPs need to be stored in a secure database, thus making it more difficult for an adversary to launch model-building attacks on the deployed PUFs. We reduce the execution time from *O(n)* to *O(1)* and storage overhead from *O(nk)* to *O(n)* compared to state-of-the-art AA protocols and also dispense the necessity of maintaining a revocation list for the compromised keys. In addition, we provide security proofs of the protocol under Elliptic Curve Diffie-Hellman assumption and decisional uniqueness assumption of a PUF. A prototype of the protocol has been implemented on a Z-Turn board integrated with dual-core ARM Cortex-A9 processor and Artix-7 FPGA. The resource footprint and performance characterization results show that the proposed scheme is suitable for implementation on resource-constrained platforms.

## Searchable Symmetric Encryption: Recent Progress and Challenges

**(Dr. Sikhar Patranabis, VISA Research, USA)**

Abstract**:** Recent developments in cloud computing allow entities to outsource the storage and processing of large databases to third party service-providers. However, outsourcing leads to concerns surrounding data confidentiality. This motivates cryptographic techniques that allow entities to encrypt their data prior to outsourcing, while retaining the ability to compute directly over the encrypted data (without decryption). Elegant cryptographic solutions such as fully homomorphic encryption achieve this in theory, but continue to be unsuitable for practical deployment due to large performance overheads.

In this talk, I will present a discussion on searchable symmetric encryption (SSE) – a family of cryptographic schemes that allow computing a restricted class of functions over outsourced symmetrically encrypted databases. The primary goal of SSE is to identify and achieve the right balance between efficiency, security and search functionality to be deployable in practice. I will present an overview of the key challenges – both theoretical and practical – in striking such a balance.

Next, I will present my past and ongoing research on SSE schemes that can process Boolean queries over symmetrically encrypted document collections. I will describe some cryptographic techniques that allow such queries in a (provably) secure yet efficient manner while minimizing both information leakage and query latencies. These techniques rely on standard cryptographic assumptions.

I will conclude with some open questions on SSE for richer query types and alternative database families, and implementation challenges for SSE from a computer systems perspective.

[Based on joint works with Debdeep Mukhopadhyay at CCS' 18 and NDSS' 21. No prior background on cryptography will be needed.]

## Introduction of Boomerang-Type Attacks

### (Dr. Yu Sasaki, NTT Japan)

Abstract: A boomerang attack, devised by David Wagner in 1999, is a type of differential cryptanalysis that divides a target cipher into two parts andcombines two independently constructed differential characteristics for two parts. A lot of follow-up works have been done to improve the boomerang attack. The goal of this talk is to introduce basics of the boomerang attack and revisit its progress.

## Link between Multi-User and Single-User Security Revisited

### (Dr. Benoît Cogliati, CISPA Germany)

Abstract: In this talk, we reflect on the use of the computational advantage of a primitive to prove the security of mode of operations. In particular, we explore a new way of using the single-user advantage of a block cipher in order to derive some of its statistical properties. As an illustration, we study a variable-input-length PRF and show how the computational term of the multi-user security bound can be optimized using our technique."

## Quantum Key Distribution ; Past, Present and Future

### (Dr. Arpita Maitra, TCG-CREST, IAI)

Abstract: In this talk we are going to discuss Quantum Key Distribution (QKD) protocol, its journey from BB84 to Device Independent QKD. QKD is now stepping out from the laboratory set up. Countries like China, USA, Germany etc., to name a few, are establishing the quantum network for successful QKD. Finally, we will discuss security related issues.

## Threshold Symmetric-key Encryptions

### (Dr. Pratyay Mukherjee, VISA Research, USA)

Abstract: In today's highly digitalized society, the role of encryption has become extremely important in order to protect data. However, that reduces the problem of protecting terabytes of data into a short (e.g. 256 bits) key. Enterprises typically store encryption keys using hardware solutions such as Hardware Security Modules (HSM). However, HSMs suffer from several issues like being prone to side-channels, offering limited flexibility, and being quite expensive etc. Threshold Cryptography offers an alternative solution where keys can be protected by distributing them on to multiple servers and never allowing reconstruction, thereby avoiding a single-point of failure. So, even if upto a threshold number of servers are totally compromised the scheme remains secure. In this talk I will be focusing on our recent works on Threshold Symmetric-key Encryptions.

First, I shall talk about the unique features offered by Threshold Symmetric-key Encryptions compared to alternatives such as Multiparty Computations or Threshold Public-key Encryptions. Then I shall describe our first solution from the CCS'18 paper (aka DiSE, also presented at Real World Crypto 2020), in that we define, design and implement Threshold Symmetric-key Encryption schemes for the first time. Our solutions are simple and extremely efficient. Then I will discuss two follow ups, (i) a scheme secure against adaptive corruption (IndoCrypt'20) as opposed to static corruption (where the set of compromised servers stay the same throughout) and (ii) a scheme that offers highly amortized soltuion (upto 30x speed up compared to DiSE) for massive data encryption (CCS'21).

The talk is based on the following papers.

1.DiSE: Distributed Symmetric-key Encryption
with Shashank Agrawal, Payman Mohassel, Peter Rindal
in CCS 2018, extended abstract accepted in Real World Crypto, 2020.

2. Adaptively secure Threshold Symmetric-key Encryption
in INDOCRYPT 2020.

3. Amortized Threshold Symmetric-key Encryption
with Mihai Christodorescu, Sivanarayana Gaddam, Rohit Sinha
to appear in CCS 2021.

## keccak - A Symmetric Perspective

## (Dr. Dhiman Saha, IIT Bhilai)

Abstract: Keccak - the winner of SHA-3 competition is one of the most widely analysed cryptographic hash functions. In this talk, we focus on Keccak from a symmetric view-point. We first define what one means by symmetry in the context of the internal state of Keccak. Next we highlight how internal symmetry presents itself in Keccak by construction which has been systematically treated by the designers themselves. We then look at some third-party cryptanalytic results that exploit the evolution of symmetry through the round functions to find collisions and distinguishing attacks on both the internal permutations as well as the hash-function.

## Quantum Security of Symmetric Cryptography

## (Dr. Gaëtan Leurent, INRIA, France)

Abstract: Due to Shor's algorithm, quantum computers are a severe threat for public-key cryptography. This motivated the cryptographic community to search for quantum-safe solutions. On the other hand, the impact of quantum computing on secret key cryptography is not as well understood. The main known applicable result is Grover's algorithm that gives a quadratic speed-up for exhaustive search. In this talk, we give an overview of quantum cryptanalysis of symmetric-key ciphers, considering different security models with classical queries or quantum queries. First, we consider a quantum version of differential cryptanalysis. This usually results in a quadratic speedup, but there are many details to consider. Then, we consider modes of operation, with a devastating attack against many classical MACs using Simon's

algorithm. Finally, we describe Saturnin, an Authenticated Encryption algorithm designed to resists quantum attacks.

## Automating Fault Attack Detection and Mitigation in Block Cipher Implementations

**(Dr. Chester Rebeiro, IIT Madras)**

Cipher implementations are highly vulnerable to a potent class of physical attacks known as fault injection attacks. A single precisely injected fault during the cipher execution is sufficient to reveal the entire secret key of strong ciphers like the AES. However, only a small subset of the injected faults are exploitable. Identifying these fault locations, has for a long time been a manual and difficult task. The fault vulnerablelocations, not just depend on the cipher algorithm but also the implementation. For example, fault locations of two different implementations of the AES cipher is different.

In this talk we summarise our efforts at designing tools that could automatically identify fault vulnerable locations in block cipher implementations. Given an implementation of a block cipher, the tools can identify the vulnerable instructions and also order them according to their vulnerability score. These tools can be incorporated in off the shelf compilers to enable the first fault attack aware compilation for cipher implementations.