# Selected Areas in Cryptography 2025

August 11–15, 2025

Kurt Pan @ ZKPunk

September 25, 2025

## Contents



## 1 A tutorial on Post-Quantum cryptography

Slides

**Doug Stinson**, University of Waterloo, Canada

We begin with a short introduction to quantum computing and its potential impact on current cryptographic algorithms and we summarize the ongoing NIST standardization process for post-quantum cryptography. We briefly review some important cryptographic tools that are used in the design of post-quantum cryptography, including pseudorandom generators and

functions, the random oracle model and key encapsulation mechanisms. Then we discuss the main approaches to post-quantum cryptography, emphasizing the underlying mathematical techniques. These include: - hash-based signature schemes - code-based cryptography (e.g., McEliece, Niederreiter, BIKE, HQC) - lattice-based cryptography (e.g., NTRU, Regev, Kyber, Dilithium) - multivariate cryptography (e.g., Oil and Vinegar) We assume a basic background in cryptography, algebra and number theory.

## 2 A Guided Tour through the Jungle of Arithmetization-Oriented Primitives

Slides || Slides

**Clémence Bouvier**, Inria Nancy, France

In the last few years, a large number of symmetric primitives have been introduced following the emergence of advanced protocols such as multi-party computation (MPC), in combination with a fully homomorphic encryption (FHE) or in various systems of zero-knowledge proofs (ZKP). These primitives, also known as Arithmetization-Oriented Primitives (AOPs), are based on a specific arithmetic and an unusual environment in symmetric cryptography. In this lecture, we will present the context that led to the emergence of AOPs and propose different ways of classifying them. We will also discuss the latest advances in design and security analysis.

## 3 AI to the Rescue: Where AI Meets Cryptography

Slides

**Stjepan Picek**, University of Zagreb, Croatia and Radboud University, Nijmegen, The Netherlands

In recent years, artificial intelligence (AI) has become an emerging technology to assess security and privacy. Despite difficult beginnings, today, AI is also used in cryptography, allowing faster (and sometimes) better results than other techniques. AI is successfully applied in a range of cryptographic contexts, including profiled side-channel attacks using neural networks, modeling and attacking physically unclonable functions, detection and classification of hardware Trojans, and even assisting differential cryptanalysis.

However, this convergence of AI and cryptography brings a unique set of challenges. The black-box nature of many AI models, the difficulty of ensuring reproducibility, and concerns around adversarial manipulation all pose significant obstacles. In the first part of the talk, we will highlight success stories where AI improved state-of-the-art in cryptography. In the second part of the talk, we will examine what cryptography can do for the security of machine learning. We will cover examples like differential cryptanalysis used for model stealing, indistinguishable backdoors, and cryptography enabling privacy for neural networks. Finally, we will conclude the talk by discussing diverse challenges and future research directions.

## 4 Reducing the Number of Qubits in Quantum Factoring

Slides

**Pierre-Alain Fouque**, University of Rennes and Institut Universitaire de France, France

In this talk, I will recall Shor's quantum algorithm, then its version by Ekera-Hastad through the computation of short discrete-log, before describing our improvement via May-Schlieper hashing technique.

## 5 Deep Neural Cryptography

Slides

**Adi Shamir**, Weizmann Institute of Science, Israel

The wide adoption of deep neural networks (DNNs) raises the question of how can we equip them with a desired cryptographic functionality (e.g., to decrypt an encrypted input, to verify that this input is authorized, or to hide a secure watermark in the output). The problem is that cryptographic primitives are typically designed to run on digital computers that use Boolean gates to map sequences of bits to sequences of bits, whereas DNNs are a special type of analog computer that uses linear mappings and ReLUs to map vectors of real numbers to vectors of real numbers. In this talk I will describe a new theory of security when digital cryptographic primitives are implemented as ReLU-based DNNs, show that natural implementation

techniques are highly insecure, and finally develop a new and completely practical method for implementing any desired cryptographic functionality as a standard ReLU-based DNN in a provably secure and correct way.

## 6 Air-FRI: Acceleration of the FRI Protocol on the GPU for zkSNARK Applications

Paper || Slides

This paper presents Air-FRI, a novel GPU-enabled software implementation of the Fast Reed-Solomon Interactive Oracle Proof of Proximity (FRI) protocol, which is a core component in post-quantum zkSNARKs that reduces computational complexity in systems with substantial mathematical instances. Existing schemes that implement the FRI protocol entail significant computational times due to large proof sizes. Our optimized solution includes a parallelized computation of Reed-Solomon codewords, the precomputation of time-intensive finite field operations, non-interactiveness, and the application of a unified Merkle tree commitment to authenticate the entire proof. Together, the implemented optimizations yield a solution that significantly reduces prover and verifier times while minimizing proof size, addressing both scalability and performance challenges in zkSNARK-based algorithms. Performance evaluations conducted by us across two security levels confirm the implementation's high throughput, establishing it as a promising solution for practicable privacy-preservation. Our results show a 93.3% improvement on an average in the speed of the protocol on the GPU as compared to a non-GPU solution for the same parameters, which includes the execution time of all of its sub-phases: the commit phase, the query phase, and the round consistency checks to ensure correctness of the proof.

## 7 Accelerating Post-quantum Secure zkSNARKs by Optimizing Additive FFT

Paper || Slides

In this paper, we propose leveraging the Cantor special basis in post-quantum secure zkSNARKs operating over binary extension fields. This approach enables the optimization of the additive Fast Fourier Transform (FFT) algorithm in Aurora, a post-quantum secure zkSNARK, by replacing

the previously used Gao–Mateer FFT with the Cantor and LCH FFTs. Our implementation demonstrates a significant reduction in computation time for Aurora, with the potential to accelerate other zkSNARKs utilizing additive FFTs. Additionally, we present a detailed theoretical analysis of the computational costs of the Cantor FFT algorithm, providing exact counts of additions, multiplications, and precomputation overhead. Furthermore, we analyze the FFT call complexity within the encoding of the Rank-1 Constraint System in the Aurora zkSNARK.