Graduate School Event

Thesis Defense: Theory and Applications of Verifiable Delay Functions

Charlotte Hoffmann (Pietrzak Group)

Pietrzak Group

Host: Maximilian Jösch

Verifiable Delay Functions (VDFs) introduced by Boneh et al. (CRYPTO'18) are functions that require a prescribed number of sequential steps T to evaluate, yet their output can be verified in time much faster than T. Since their introduction, VDFs have gained a lot of attention due to their applications in blockchain protocols, randomness beacons, timestamping and deniability. This thesis explores the theory and applications of VDFs, focusing on enhancing their soundness, efficiency and practicality.The only practical VDFs known to date are based on repeated squaring in hidden order groups. Consider the function VDF(x,T)=x^(2^T). The iterated squaring assumption states that, for a random group element x, the result of VDF cannot be computed significantly faster than performing T sequential squarings if the group order is unknown. To make the result verifiable a prover can compute a proof of exponentiation (PoE) \pi. Given \pi, the output of VDF can be verified in time much less than T.We first present new constructions of statistically sound proofs of exponentiation, which are an important building block in the construction of SNARKs (Succinct Non-Interactive Argument of Knowledge). Statistical soundness means that the proofs remain secure against computationally unbounded adversaries, in particular, it remains secure even when the group order is known. We thereby address limitations in previous PoE protocols which either required (non-standard) hardness assumptions or a lot of parallel repetitions. Our construction significantly reduces the proof size of statistically sound PoEs that allow for a structured exponent, which leads to better efficiency of SNARKs and other applications.Secondly, we introduce improved batching techniques for PoEs, which allow multiple proofs to be aggregated and verified with minimal overhead. These protocols optimize communication and computation complexity in large-scale blockchain environments and enable scalable remote benchmarking of parallel computation resources.We then construct VDFs with enhanced properties such as zero-knowledge and watermarkability. It was shown by Arun, Bonneau and Clark (ASIACRYPT'22) that these features enable new cryptographic primitives called short-lived proofs and signatures. The validity of such proofs and signatures expires after a predefined amount of time T, i.e., they are deniable after time T. Our constructions improve upon the constructions by Arun, Bonneau and Clark in several dimensions (faster forging times, arguably weaker assumptions).Finally, we apply PoEs in the realm of primality testing, providing cryptographically sound proofs of non-primality for large Proth numbers. This work gives a surprising application of VDFs in the area of computational number theory.Together, our contributions advance both the theoretical foundations and the real-world usability of VDFs in general and in particular of PoEs, making them more adaptable and secure for current and emerging cryptographic applications.

Friday, October 17, 2025 01:30pm - 02:30pm

Central Bldg / 01 / Mondi 4 (01.01.011) and Zoom

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station. Please find a schedule of the ISTA Shuttle on our webpage: https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.