Speaker: Dmitrii Koshelev
Title: Batching Cipolla-Lehmer-Müller's square root algorithm with hashing to elliptic curves

Abstract. The talk is dedicated to a novel hash function $\mathcal{H}$ to any elliptic curve of j-invariant $\neq 0, 1728$ over a finite field $\mathbb{F}_q$ of large characteristic. The unique bottleneck of $\mathcal{H}$ consists in extracting a square root in $\mathbb{F}_q$ as well as for most hash functions. However, $\mathcal{H}$ is designed in such a way that the root can be found by (Cipolla-Lehmer-Müller's algorithm in constant time. Violation of this security condition is known to be the only obstacle to applying the given algorithm in the cryptographic context. When the field $\mathbb{F}_q$ is highly 2-adic and $q \equiv 1 \bmod 3$, the new batching technique is the state-of-the-art hash- ing solution except for some sporadic curves. Indeed, Müller's algorithm costs $\approx 2\log_2(q)$ multiplications in $\mathbb{F}_q$. In turn, (constant-time) Tonelli-Shanks's square root algorithm has asymptotic complexity $O(\log(q) + \nu^2)$, where ν is the 2-adicity of $\mathbb{F}_q$. As an example, Müller's algorithm needs ≈ 4561 fewer multiplications in the field $\mathbb{F}_q$ (whose $\nu = 96$) of the standardized curve NIST P-224. In other words, there is an acceleration of about 11 times.