Uni/Multi variate polynomial embeddings for zkSNARKs

Guang Gong

University of Waterloo, Canada

A zero-knowledge proof is a cryptographic primitive that enables a prover to convince a verifier the validity of a mathematical statement (an NP statement) without reveal any secret inputs. A special case, called zero-knowledge Succinct Non-interactive ARgument of Knowledge (zkSNARK) is particularly designed for arithmetic circuit proof systems which have important applications in blockchain privacy. The major computations in the type of zkSNARK proofs with post-quantum security are polynomial evaluations and Lagrange interpolations over finite fields. In this talk, I will show our new work on deviation of the concrete complexities of provers, proof sizes and verifiers instead of just using big notation. Given a sequence over a finite field, in coding and sequences research, we understand that there are two representations of the sequence, one is a univariate polynomial and the other, a multivariate polynomial. This is exactly what is done in those proof systems to transform the proof of a R1CS system (more general than a circuit system) to evaluate uni/multi variate polynomials at some random points in the finite field. We will use two zkSNARK schemes, i.e., Polaris, univariate polynomial representation and Spartan, multivariate polynomial representation, as examples to show our analysis.