IPM Biennial Conference on
Combinatorics and Computing,
May 20-22, 2025, School of Mathematics, IPM, Tehran
40 Years in Designs: Celebrating the Life and Achievments of
Professor Gholamreza B. Khosrovshahi

LUNA: Quasi-Optimally Succinct Designated-Verifier Zero-Knowledge Arguments from Lattices

Amin Sakzad
Monash University, Australia

We introduce the *first* candidate Lattice-based designated verifier (DV) zero knowledge sUccinct Non-interactive Argument (ZKSNARG) protocol, named LUNA, with quasi-optimal proof length (quasi-linear in the security/privacy parameter). By simply relying on mildly stronger security assumptions, LUNA is also a candidate ZK-SNARK (i.e. argument of knowledge). LUNA achieves significant improvements in concrete proof sizes, reaching below 6 KB (compared to > 32 KB in prior work) for 128-bit security/privacy level. To achieve our quasi-optimal succinct LUNA, we give a new regularity result for 'private' re-randomization of Module LWE (MLWE) samples using discrete Gaussian randomization vectors, also known as a lattice-based leftover hash lemma with leakage, which applies with a discrete Gaussian re-randomization parameter that is *polynomial* in the statistical privacy parameter (avoiding exponential smudging), and hides the coset of the re-randomization vector support set. Along the way, we derive bounds on the smoothing parameter of the intersection of short integer solution (SIS), gadget, and Gaussian perp module lattices over the power of 2 cyclotomic rings. We then introduce a new candidate linear-only homomorphic encryption scheme called Module Half-GSW (HGSW), and apply our regularity theorem to provide smudging-free circuitprivate homomorphic linear operations for Module HGSW. Our implementation and experimental performance evaluation show that, for typical instance sizes, Module HGSW provides favourable performance for ZK-SNARG applications involving lightweight verifiers. It enables significantly (around $5\times$) shorter proof lengths while speeding up CRS generation and encryption time by 4 - $16\times$ and speeding up decryption time by $4.3\times$, while incurring just 1.2 - $2\times$ time overhead in linear homomorphic proof generation operations, compared to a Regev encryption used in prior work in the ZK-SNARG context. We believe our techniques are of independent interest and will find application in other privacy-preserving applications of lattice-based cryptography.

This is a joint work with Ron Steinfeld, Muhammed F. Esgin, Veronika Kuchta, Mert Yassi, and Raymond K. Zhao.