STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Dhiraj K. Pandey
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering and Science Department of Computer Science
Date:	Monday, May 20, 2024
Time/Location:	10:00 AM EDT/GS 222
Title:	Pseudorandom Functions from Burnside Learning Problems
Chairperson:	Dr. Antonio R. Nicolosi, Department of Computer Science, Stevens Institute of Technology
Committee Members:	Dr. Susanne Wetzel, Department of Computer Science, Stevens Institute of Technology Dr. Wendy Hui Wang, Department of Computer Science, Stevens Institute of Technology Dr. Alexander Ushakov, Department of Mathematical Sciences, Stevens Institute of Technology Dr. Nelly Fazio, Department of Computer Science, City College of New York/CUNY

ABSTRACT

Learning homomorphisms with noise (LHN) is a group-theoretic learning problem generalizing quantum-safe computational assumptions like learning parity with noise (LPN) and well-established learning with errors (LWE). The LHN problem associated with Burnside groups of exponent three is referred to as learning Burnside homomorphisms with noise (B_n-LHN). In a nutshell, the B_n-LHN problem focuses on recovering a secret homomorphism between Burnside groups, given polynomially many noisy samples. Previous work assessed important combinatorial properties and basic cryptographic applications of the B_n-LHN problem, but did not address efficient constructions of a fundamental cryptographic primitive known as pseudorandom function (PRF).

This dissertation presents a derandomization technique for the B_n-LHN problem that results in a novel computational assumption, referred to as learning Burnside homomorphisms with rounding (B_n-LHR), that does not rely on an underlying noise distribution. It then establishes its security by exhibiting a complexity reduction from the B_n-LHN problem. Overall, this enables the application of standard cryptographic constructions that do not easily accommodate the presence of noise, while still achieving security guarantees comparable to the original B_n-LHN assumption.

This work then introduces three novel PRF constructions based on the decisional B_n-LHR assumption. The first construction relies on pseudorandom synthesizers (PRSs) and entails a very large PRF secret-key. The second construction attains better key-size parameters by first deriving a length-doubling pseudorandom generator (PRG) from a weak PRF family, and then employing said PRG as an intermediate function in the

seminal PRG-to-PRF construction of Goldreich, Goldwasser, and Micali (GGM). Finally, the third construction enhances the PRF design by introducing a PRG with associated public parameters.

As a second direction, this dissertation outlines the design of three progressively refined PRF constructions grounded in the original B_n-LHN assumption. All the designs capitalize on the low entropy of noise elements within the Burnside group and hold promise for even more efficient Burnside-based PRF constructions. Finally, to maximize the efficiency of these PRF constructions, this work also investigates approaches to improve computations over Burnside groups. In particular, it explores optimizations of its group operation and carries out an in-depth analysis of the Burnside noise distribution. This latter analysis contributes valuable insights into establishing the hardness connection between the B_n-LHN and the B_n-LHR problems.