Partial Vandermonde Problems and PASS Encrypt

Katharina Boudgoust

Univ Rennes, IRISA, CNRS

This work contributes in the field of lattice-based cryptography, a research domain of public key cryptography that was initiated at the end of the 1990s by two different branches. On the one had, there have been proposals benefiting from strong theoretical connections to presumed hard worst-case lattice problems, leading to the development of public key cryptography based on the Short Integer Solution (SIS) and Learning With Errors (LWE) problems. On the other hand, very efficient schemes basing their security on average-case structured lattice problems have been introduced, one popular among them is the NTRU encryption scheme.

Following the latter approach, Hoffstein et al. (HPS$^+$14) propose a digital signature scheme called PASS Sign, whose security is based on the difficulty of recovering a polynomial of small norm having access only to a partial list of its Vandermonde transform. This task can be phrased as an instance of some lattice problem. Shortly afterwards, Hoffstein and Silverman (HS15) introduce PASS Encrypt, a public key encryption scheme whose computational building blocks are closely related to the ones of PASS Sign. It is very efficient and fulfills additive and multiplicative homomorphic properties. The algebraic structure and homomorphic properties of PASS Encrypt and the underlying partial Vandermonde problems, make them a natural starting point for the design of efficient cryptographic primitives. For example, such properties are recently exploited in the context of PASS Sign to construct compact aggregate signature schemes (DHSS20), and it is plausible that combining PASS Encrypt and PASS Sign may form the basis for various compact and efficient privacy-preserving primitives such as group signatures. Unfortunately, a main problem with PASS Encrypt to date is that its security is not well understood, no proof of security was given in (HS15) with respect to the hardness of explicit computational problems, and the scheme is deterministic and hence does not satisfy the standard notion of IND-CPA security.

In a collaboration with Amin Sakzad and Ron Steinfeld (BSS21), we make progress towards understanding the hardness assumptions needed to prove the security of PASS Encrypt. We study the Partial Vandermonde Knapsack problem (PV-Knap) and emphasize its connection to (average-case) ideal lattices. We enlarge the landscape of problems that use the partial Vandermonde matrix by defining a new variant of LWE, called Partial Vandermonde Learning With Errors (PV-LWE). Later, we show the equivalence of PV-Knap and PV-LWE by exploiting the same duality connection that we have for standard Knapsack problems and LWE. In order to provide a security proof for PASS Encrypt, we need to define a variant of PV-Knap, that we call the PASS problem. This problem serves (together with the decision version of PV-Knap) as the underlying hardness assumption for (a slightly modified version of) PASS Encrypt. Furthermore, we present the scheme together with the security proof. We conclude the presentation with some interesting open questions regarding problems using the partial Vandermonde transform.

The presentation focuses on parts of (BSS21) that are already published in the PhD manuscript (Bou21).

References

[Bou21] Katharina Boudgoust. Theoretical hardness of algebraically structured learning with errors, 2021.

[BSS21] Katharina Boudgoust, Amin Sakzad, and Ron Steinfeld. Vandermonde meets regev: Public key encryption schemes based on partial vandermonde problems, 2021. Currently under submission.

[DHSS20] Yarkin Doröz, Jeffrey Hoffstein, Joseph H. Silverman, and Berk Sunar. MMSAT: A scheme for multimessage multiuser signature aggregation. *IACR Cryptol. ePrint Arch.*, page 520, 2020.

[HPS$^+$14] Jeffrey Hoffstein, Jill Pipher, John M. Schanck, Joseph H. Silverman, and William Whyte. Practical signatures from the partial fourier recovery problem. In *ACNS*, volume 8479 of *Lecture Notes in Computer Science*, pages 476–493. Springer, 2014.

[HS15] Jeffrey Hoffstein and Joseph H. Silverman. Pass-encrypt: a public key cryptosystem based on partial evaluation of polynomials. *Des. Codes Cryptogr.*, 77(2-3):541–552, 2015.