Practical cryptanalysis of pseudorandom correlation generators based on quasi-Abelian syndrome decoding

Mickael Hamdad*[1]

[1]Faculté des sciences et ingénierie de Sorbonne Université – Laboratoire d'Informatique de Paris 6 – France

Résumé

Quasi-Abelian Syndrome Decoding (QA-SD) is a recently introduced generalization of Ring-LPN that uses multivariate polynomials rings. As opposed to Ring-LPN, it enables the use of small finite field such as GF(3) and GF(4). It was introduced by Bombar et al (Crypto 2023) in order to obtain pseudorandom correlation generators for Beaver triples over small fields. This theoretical work was turned into a concrete and efficient protocol called F4OLEage by Bombar et al. (Asiacrypt 2024) that allows several parties to generate Beaver triples over GF(2). We propose efficient algorithms to solve the decoding problem underlying the QA-SD assumption. We observe that it reduce to a sparse multivariate polynomial interpolation problem over a small finite field where the adversary only has access to random evaluation points, a blind spot in the otherwise rich landscape of sparse multivariate interpolation. We develop new algorithms for this problem: using simple techniques we interpolate polynomials with up to two monomials. By sending the problem to the field of complex numbers and using convex optimization techniques inspired by the field of "compressed sensing", we can interpolate polynomials with more terms. This enables us to break in practice parameters proposed by Bombar et al. at Crypto'23 and Asiacrypt'24 as well as Li et al. at Eurocrypt'25 (IACR flagship conferences Grand Slam). In the case of the F4OLEage protocol, our implementation distinguishes the output of the pseudorandom correlation generator from random with advantage 60% in a few hours. This not only invalidates the security proofs, but it yields real-life privacy attacks against multiparty protocols using the Beaver triples generated by the broken pseudorandom correlation generators. Collaboration avec Charles Bouillaguet, Claire Delaplace et Damien Vergnaud

*Intervenant