Shared Permutation for Syndrome Decoding: New Zero-Knowledge Protocol and Code-Based Signature

Thibauld Feneuil[1,2], Antoine Joux[3], and Matthieu Rivain[1]

[1] CryptoExperts, Paris, France
[2] Sorbonne Université, CNRS, INRIA, Institut de Mathématiques de Jussieu-Paris Rive Gauche, Ouragan, Paris, France
[3] CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

{thibauld.feneuil,matthieu.rivain}@cryptoexperts.com
joux@cispa.de

Speaker: Thibauld Feneuil, PhD Student.
The talk would be about the article with the same name, available at

https://eprint.iacr.org/2021/1576.

Abstract. Zero-knowledge proofs are an important tool for many cryptographic protocols and applications. The threat of a coming quantum computer motivates the research for new zero-knowledge proof techniques for (or based on) post-quantum cryptographic problems. One of the few directions is code-based cryptography for which the strongest problem is the *syndrome decoding* (SD) of random linear codes. This problem is known to be NP-hard and the cryptanalysis state of affairs has been stable for many years.

In a pioneering work from three decades ago, Stern proposed a zero-knowledge protocol to prove the knowledge of a solution to a syndrome decoding instance. This protocol achieves a *soundness error* of 2/3 which means that a malicious prover can fool the verifier with probability 2/3. Although an arbitrary security of $(2/3)^\tau$ can be achieved by repeating the protocol τ times, the induced communication cost is significant, which is partly due to this high soundness error. Since the work of Stern, a few papers have proposed optimizations and implementations but for random linear codes with standard security levels, the communication cost is still heavy.

In the presented paper, we propose a new zero-knowledge protocol for the SD problem which achieves a soundness error of $1/n$ with complexity $\mathcal{O}(n)$ for an *arbitrary* chosen n. In a nutshell, and as in Stern protocol, the solution x is masked by the application of a random permutation σ. However instead of revealing either $\sigma(x)$ or σ, we always reveal $\sigma(x)$ and prove the existence of a permutation σ. To this purpose, we decompose σ into n masked permutations $\sigma(\cdot) + s := (\sigma_1(\cdot) + s_1) \circ \cdots \circ (\sigma_n(\cdot) + s_n)$ which are all committed by the prover and we let the verifier choose $n - 1$ of them to be revealed. This way, we can maintain the privacy of σ while obtaining the desired soundness error of $1/n$.

Our construction requires the verifier to *trust* some of the variables sent by the prover which can be ensured through a *cut-and-choose* approach. We provide an optimized version of our zero-knowledge protocol which achieves arbitrary soundness through parallel repetitions and merged cut-and-choose phase. For a soundness error of 2^{-128}, the communication cost can be made lower than 15 KB. While turning this protocol into a signature scheme, we achieve a signature size of 17 KB for a 128-bit security. This represents a significant improvement over previous constructions based on the syndrome decoding problem for random linear codes.