Fast Pseudorandom Correlation Functions from Sparse LPN with Applications to Two-Party ECDSA and Schnorr

Lennart Braun*[1], Geoffroy Couteau[1], Kelsey Melissaris[2], Mahshid Riahinia[3], and Elahe Sadeghi[4]

[1]Institut de Recherche en Informatique Fondamentale – Centre National de la Recherche Scientifique, Université Paris Cité – France

[2]Institut de Recherche en Informatique Fondamentale – Centre National de la Recherche Scientifique, Université Paris Cité – France

[3]Département d'informatique - ENS-PSL – École normale supérieure - Paris, Institut National de Recherche en Informatique et en Automatique, Centre National de la Recherche Scientifique – France

[4]University of Texas at Austin [Austin] – États-Unis

Résumé

Pseudorandom correlation functions (PCFs) allow two parties holding short correlated keys to generate on-the-fly any target amount of correlated (pseudo)randomness without further communication. We introduce a new and efficient PCF for the oblivious transfer (OT) and vector oblivious linear evaluation (VOLE) correlations whose security reduces to the sparse learning parity with noise (LPN) assumption in the random oracle model. Our construction is the first to achieve high concrete efficiency while relying on well-established assumptions: previous candidates either required introducing new assumptions, or had poor concrete performances. We complement our result with an in-depth analysis of the sparse LPN assumption, providing new insight on how to evaluate the strength of concrete sets of parameters. Additionally we show how to use a PCF for VOLE for two-round, two-party, stateless and deterministic signing protocols with extremely low communication (96 byte for Schnorr, 128 byte for ECDSA). Collaboration with:
- Geoffroy Couteau (Université Paris Cité, CNRS, IRIF, France)
- Kelsey Melissaris (Chalmers University of Technology, Göteborg, Sweden)
- Mahshid Riahinia (DIENS, École normale supérieure, CNRS, Paris, France)
- Elahe Sadeghi (University of Texas at Austin, Texas, USA)

*Intervenant