From: Talks
To: Apon, Daniel C. (Fed)
Subject: [Talks] Today"s talks
Date: Friday, February 22, 2019 12:31:12 AM

Today's talks

Simple and More Efficient PRFs with Tight Security from LWE and Matrix-DDH

Rafael Kurek
3400 A.V. Williams Building (AVW)
Friday, February 22, 2019, 1:00-2:00 pm

Abstract

We construct efficient and tightly secure pseudorandom functions (PRFs) with only logarithmic security loss and short secret keys. This yields very simple and efficient variants of well-known constructions, including those of Naor-Reingold (FOCS 1997) and Lewko-Waters (ACM CCS 2009). Most importantly, in combination with the construction of Banerjee, Peikert and Rosen (EUROCRYPT 2012) we obtain the currently most efficient LWE-based PRF from a weak LWE-assumption with a much smaller modulus than the original construction. In comparison to the only previous construction with this property, which is due to Doettling and Schroeder (CRYPTO 2015), we use a modulus of similar size, but only a single instance of the underlying PRF, instead of \lambda \omega(log \lambda) parallel instances, where \lambda is the security parameter. Like Doettling and Schroeder, our security proof is only almost back-box, due to the fact that the number of queries made by the adversary and its advantage must be known a-priori.

Technically, we introduce all-prefix universal hash functions (APUHFs), which are hash functions that are (almost-)universal, even if any prefix of the output is considered. We give simple and very efficient constructions of APUHFs, and show how they can be combined with the augmented cascade of Boneh et al. (ACM CCS 2010) to obtain our results. Along the way, we develop a new and more direct way to prove security of PRFs based on the augmented cascade.

This talk is part of the following lists: Crypto Reading Group

---