Workshop on Lattices and Multilinear Maps
Friday December 4, 2015

Multilinear Maps and their Cryptanalysis
Jung Hee Cheon (Seoul)

We discuss approximate multilinear maps and their cryptanalysis. After being introduced by Boneh and Silverberg in 2002, multilinear maps were regarded as a source of many interesting cryptographic constructions including multiparty key exchange and broadcast encryption. It has taken 10 years to have the first plausible candidates by Garg, Gentry and Halevi (GGH13). Later, two more schemes have been suggested, one by Coron, Lepoint and Tibouchi (CLT13) and the other by Gentry, Gorbunov, Halevi (GGH15). They draw lots of attention and yield several interesting new cryptographic primitives such as Functional Encryption (FE), indistinguishable Obfuscation (iO) and Key Homomorphic Pseudo Random Functions.

Recently, all of these constructions are suffering serious attacks. In this talk, we introduce recent constructions and describe a polynomial-time cryptanalysis of CLT13, GGH13, and GGH15. As a fix of CLT13, Coron, Lepoint, and Tibouchi proposed another candidate of new multilinear maps over the integers (CLT15) in Crypto 2015. We also describe an attack on CLT15. As a consequence, we don't have any plausible candidates of Mmaps at this moment. We conclude this talk by giving an open question: how to break private multilinear maps which leads to an attack on iO schemes; or how to make a security argument.

Obfuscation
Amit Sahai (UCLA)

The talk will give an overview of some definitions and constructions in the theory of obfuscation.

Weak instances of Ring-LWE revisited
Fre Vercauteren (KU Leuven)

Recently several papers by Lauter et al. have introduced families of number fields and corresponding moduli for which either decision and/or search Ring-LWE appears to be weak. In this talk we will revisit these papers to derive stronger results and explain the importance of a detailed analysis of the singular value decomposition of the canonical embedding. We will show that all these weak cases follow from special properties of their singular value decomposition.

Some Remarks on Small Secret LWE
Martin Albrecht (Royal Holloway, London)

Hardness: Reductions [BLPRS13]

> "A major part of our reduction [...] is therefore dedicated to showing reduction from LWE (in dimension n) with arbitrary secret in $\mathbb{Z}_q^n$ to LWE (in dimension $n \log_2 q$) with a secret chosen uniformly over $\{0, 1\}$."

Hardness: Algorithms [BaiGal14]

> "[This work] suggests that this is overkill and that even $n \log \log n$ may be more than sufficient."

Hardness: Constructions [GenHalSma12]

> "This brings up the question of whether one can get better attacks against LWE instances with a very sparse secret (much smaller than even the noise). [...] In terms of attacks, the only attack that we could find that takes advantage of this sparse key is by applying the reduction technique of Applebaum et al. to switch the key with part of the error vector, thus getting a smaller LWE error."