Public key cryptography based on graph problems

Péter Hudoba

Department of Computer Algebra - PhD School of Computer Science - Eötvös Loránd University, Budapest

peter.hudoba@inf.elte.hu

Post-quantum cryptography will be important in the future, because with Shor's algorithm, RSA and other cryptosystems based on the hardness of the factorization or discrete logarithm will be breakable in polynomial time with a quantum computer that has enough qubits. There are candidate systems for post-quantum cryptography [1,2,3,4], but their speed and space requirements are too high.

In this talk we propose some new methods for public key encryption based mainly on graph problems. We implemented our schemes to measure the differences and the efficiency of the new algorithms. With further deveopment of these new algorithms we plan to aquire a more efficient and provably secure public key encryption scheme that is based on different assumptions than the classical ones, so it resists attacks based on Shor's algorithm.

As an example we constructed a new public key encryption scheme based on the combinatorial NP-complete clique problem and the well-known lattice problem called learning parity with noise.

References

[1] Benny Applebaum, Boaz Barak and Avi Wigderson. Public-key cryptography from different assumptions. In Proceedings of the forty-second ACM symposium on Theory of computing, pages 171-180. ACM, 2010.

[2] Michael Alekhnovich. More on average case vs approximation complexity. In Foundations of Computer Science, 2003. Proceedings. 44th Annual IEEE Symposium on, pages 298-307. IEEE, 2003.

[3] Alexandre Duc and Serge Vaudenay. HELEN: A Public-Key Cryptosystem Based on the LPN and the Decisional Minimal Distance Problems. In Progress in Cryptology–AFRICACRYPT 2013, pages 107–126. Springer,2013.

[4] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In Proceedings of the forty-first annual ACM symposium on Theory of computing, pages 333–342. ACM, 2009.