Cryptography based on Erdős-Rényi random graphs

Peter Hudoba

Eötvös Loránd University
peter.hudoba@inf.elte.hu

Abstract

In this paper we propose a new method for public key encryption. The scheme's security is based on the independent set (which related to the clique problem) and learning parity with noise problems. The relevance of this approach is justified by its post-quantum nature: unlike RSA and other cryptosystems based on the hardness of factorization or discrete logarithm which could be broken by a suitable large quantum device, no known quantum attacks are known against our candidate system. We examine the time complexity of our scheme and compare it to RSA. We give a basic version of the algorithm and then an improvement of that which has a better encrypted size / message size ratio, therefore that would be more useful in practice.

Keywords: security, post-quantum cryptography, Erdős-Rényi, clique problem, independent set, learning parity with noise

MSC: 94A60

References

[1] Bernstein, D., J.Introduction to post-quantum cryptography, *Post-quantum cryptography* Springer Berlin Heidelberg, 2009. p. 1-14.

[2] Applebaum, B. , Barak, B., Wigderson, A. Public-key cryptography from different assumptions, *Proceedings of the forty-second ACM symposium on Theory of computing* pages 171-180. ACM, 2010.

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

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