The cubic Pell equation and Rédei rational functions for a novel RSA–like cryptosystem

Francesco M. Saettone (University of Turin)

1 Abstract

RSA cryptosystem is one of the most famous and used public key scheme and is based on the existence of an one–way trapdoor function, which is easy to compute and difficult to invert without knowing some information. However, some attacks are possible when, e.g., the private key is small [8] or the public key is small [2]. Moreover, RSA leaks some vulnerabilities in broadcast applications [4]. Hence, during the years, RSA–like schemes (see, e.g., [3], [5], [6], [7]) have been proposed in order to overcome some of the previous vulnerabilities.
In this talk, we present a novel RSA–like cryptosystem [1]. Specifically, we define a novel product that arises from a cubic field connected to the cubic Pell equation. We discuss some interesting properties and remarks about this product that can also be evaluated through a generalization of the Rédei rational functions. We then exploit these results to construct a novel RSA–like scheme that is more secure than RSA in broadcast applications. Moreover, our scheme is robust against the Wiener attack and against other kind of attacks that exploit the knowledge of a linear relation occurring between two plaintexts.
Our scheme is based on a particular group equipped with a non–standard product that we have found working on a cubic field related to the cubic Pell equation. In fact, we would like to point out that in this work we give a first idea about the potentiality of this group in cryptographic applications, with the aim of providing an original point of view for exploiting number theory in cryptography and opening new studies.

References

[1] N. Murru, F.M. Saettone, A novel RSA–like cryptosystem based on a product related to the cubic Pell equation and Rédei rational functions, Preprint, 2017.

[2] D. Coppersmith, Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptol., Vol. 10, No. 4, 233–260, 1997.

[3] N. Demytko, A new elliptic curve based analogue of RSA, Eurocrypt 1993, LNCS 765, Springer-Verlag, 40–49, 1994.

[4] J. Hastad, On using RSA with low exponent in a public key network, Advances in Cryptology, CRYPTO85 Proceedings, Springer, 403–408, 1986.

[5] K. Koyama, U. M. Maurer, T. Okamoto, S. A. Vanstone, New public–key schemes based on elliptic curves over the ring $\mathbb{Z}_n$, Advances in Cryptology, CRYPTO'91, Springer, 252–266, 1992.

[6] J. H. Loxtou, D. S. P. Khoo, G. J. Bird, J. Seberry, A cubic RSA code equivalent to factorization, Journal of Cryptology, Vol. 5, No. 2, 139–150, 1992.

[7] D. Naccache, J. Stern, A new public–key cryptosystem, Eurocrypt 1997, LNCS 1233, Springer–Verlag, 27–36, 1998.

[8] M. J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inform. Theory, Vol. 36, 553–558, 1990.