On the Security of Biquadratic C^* Public-Key Cryptosystems

P. Felke

Abstract

Since ETSI and NIST speed up the transition to post-quantum cryptography, i.e. cryptography that resists not only all classical but also all known quantum computer aided attacks multivariate cryptosystems have become of great interest again. One of the most elegant systems of that kind were introduced by Imai and Matsumoto in 1988 called C^* [2]. It was broken by Dobbertin in a classified work from 1993 he did for the german federal office for information security and later by Patarin [1], [3]. Since then the construction of multivariate systems sharing as much as possible of the nice properties of C^* have become of particular interest. Having broken C^* Dobbertin introduced in his work a system where the central mapping is of the form $X^d, d = 1+q^{i_1}+q^{i_2}+q^{i_3}, 0 < i_1 < i_2 < i_3 < n$, $\gcd(d, q^n - 1) = 1$ over a finite field $\mathbb{F}_{q^n}, q = 2^m$, which shares almost all properties of C^* and he therefore called biquadratic C^*. Being based on monomials of degree 4 its major drawback was its keysize one has to accept for practical usage. He showed that systems based on monomials of degree 3 are insecure. To encourage further research on biquadratic C^* after its declassification in 2001 Dobbertin placed a challenge called „CryptoChallenge 11“over 5000 € in cooperation with Faugère and the author of this abstract in the MysteryTwister-Competition hosted by the Horst-Görtz-Institute in 2005 [1]. The challenge remained unbroken and the security of these systems an open problem. Due to the above mentioned initiative in post-quantum cryptography systems with bigger keysizes are not out of scope anymore and it is about time to resume its security analysis. In this paper we will give a mathematical proof that biquadratic C^* can be broken with algorithms like F_4, F_5 in running time $O\left(\binom{n+7}{n}^{\omega}\right)$ and a required memory of $O\left(\binom{n+7}{n}^{2}\right)$. If we assume a fast implementation of gaussian elimination ω can be estimated by $2,373$. As a corollary we have that „CryptoChallenge 11“(parameters $d = 1 + q + q^3 + q^{12}, m = 4, n = 25$) can be broken with a running time of $O\left(\binom{25+7}{25}^{2,373}\right) \approx 2^{52}$ and a required memory of $O\left(\binom{25+7}{25}^{2}\right) \approx 1,3$ Tb. While this maybe fine for deployment in competitions like MysteryTwister this result renders biquadratic C^* insecure for usage in post-quantum cryptography. Furthermore it buries another path to go in the design of multivariate cryptosystems.

References

[1] H. Dobbertin, J. Faugère, P. Felke: “CryptoChallenge 11”

[2] H. Imai, T. Matsumoto: “Public Quadratic Polynomial-tuples for efficient signature-verification “, Eurocrypt ‘88

[3] J. Patarin: “Cryptanalysis of the Matsumoto and Imai Public Key Scheme of Eurocrypt ’88”, Crypto ‘95