A Geometric View of Cryptographic Equation Solving

Sean Murphy and Maura Paterson[*]
Royal Holloway, University of London

August 13, 2007

Extended Abstract

The apparent difficulty of finding a solution to a set of multivariate quadratic equations underlies the security of multivariate cryptography and can present an impediment to the successful application of algebraic attacks. Methods for finding such a solution are thus of considerable interest for the purposes of cryptanalysis. Several algebraic techniques for solving systems of multivariate quadratic equations have been proposed in the literature, including Relinearization [2] and the XL algorithm [1]. In this talk we show that considering the underlying geometry can provide additional insight into the behaviour of such techniques.

Suppose that $\mathcal{S} = \{f_1, f_2, \ldots, f_m\}$ is a set of m homogeneous quadratic equations in $n+1$ variables $(x_0, x_1, \ldots, x_n)$ with a finite (up to scalar multiplication) number of common solutions over the algebraic closure of some finite field GF(q). The equation $f_i(x_0, x_1, \ldots, x_n) = 0$ describes a (non-empty) set of points in the n-dimensional projective space over GF(q), referred to as a quadric; points that lie on all m quadrics correspond to solutions of the system of equations. Consider a change of coordinates induced by some invertible $(n+1) \times (n+1)$ matrix M with entries from GF(q) that sends a point P to the point $M \cdot P$. Such a transformation does not affect the behaviour of the system of quadrics: for instance, the number of common solutions is unaffected. This suggests that it might make sense to consider methods for solving such systems whose behaviour, like that of the system itself, does not depend on the choice of coordinates.

The XL algorithm for solving a set $\mathcal{S}$ of quadratic equations involves finding a bivariate polynomial in the ideal generated by the polynomials of $\mathcal{S}$, which is then factored in an attempt to find information about any solutions to the system. (We note that the orignal XL paper was phrased in terms of nonhomogeneous equations and finding a univariate equation in

[*] M. Paterson was supported by EPSRC research grand GR/S42637

the ideal.) However, if we decide to change coordinates, a bivariate polynomial can become one containing a higher number of variables. Thus we see that choice of coordinates can alter properties considered critical to the success of the XL algorithm, such as the number of monomials involved in the polynomials of $\mathcal{S}$. By considering the underlying geometry we propose a generalisation of the XL algorithm, which we term the GeometricXL algorithm [3], whose behaviour does not depend on the choice of coordinates. We show how this algorithm (and, consequently, the original XL algorithm) relates to the problem of finding a matrix of low rank in the linear span of a collection of matrices, a problem sometimes known as the MinRank problem. Furthermore, we demonstrate that the GeometricXL algorithm can solve certain equation systems that are not easily soluble by the XL algorithm or by Groebner basis methods. These results are explained in detail in [3].

References

[1] Nicolas Courtois, Alexander Klimov, Jacques Patarin, and Adi Shamir. Efficient algorithms for solving overdefined systems of multivariate polynomial equations. In *Advances in cryptology—EUROCRYPT 2000 (Bruges)*, volume 1807 of *Lecture Notes in Comput. Sci.*, pages 392–407. Springer, Berlin, 2000.

[2] Aviad Kipnis and Adi Shamir. Cryptanalysis of the HFE public key cryptosystem by relinearization. In *Advances in cryptology—CRYPTO '99 (Santa Barbara, CA)*, volume 1666 of *Lecture Notes in Comput. Sci.*, pages 19–30. Springer, Berlin, 1999.

[3] Sean Murphy and Maura Paterson. A geometric view of cryptographic equation solving. Technical Report RHUL-MA-2007-4, Department of Mathematics, Royal Holloway, University of London, 2007, available at `http://www.rhul.ac.uk/mathematics/techreports`.