A Brief Introduction to the Extended Linearization Method (or XL Algorithm) for Solving Polynomial Systems of Equations

Gregory V. Bard[1]

[1] *University of Wisconsin—Stout, Wisconsin, USA, bardg@uwstout.edu*

While it works over any coefficient field, the XL Algorithm was developed to solve polynomial systems of equations mod 2. Such polynomial systems arise during the cryptanalysis of many ciphers [10]. The XL algorithm has been the subject of numerous papers since its original appearance [4] [5] [6] [7] [8] [9], and the algorithm featured in the Ph.D. dissertation of Nicolas Courtois [3].

The algorithm can be thought of as converting the original polynomial system of equations into an enormous linear algebra problem. Each monomial of the polynomial system becomes a variable in the linear system, and thus a column in the XL matrix [10]. The equations are each multiplied by all possible monomials of degree up to some fixed degree, generating a very large number of rows. One then computes the RREF of the resulting matrix. If certain parameters are carefully chosen at the start, then the solution to the polynomial system will be obtained.

This also leads to an interesting paradox, an exciting connection to the theory of NP-Completeness. Computing the RREF of a matrix is a cubic-time (or faster) problem, but solving a polynomial system of equations is an NP-Complete problem. How then, can the act of solving a polynomial system, which is believed to be very hard, be reduced to the act of solving a linear system, which is believed to be very easy? This seems to imply $P = NP$, which would be a surprise. The resolution of this paradox is that the matrix is so large, that its size is exponentially large in comparison to the original polynomial system of equations. This is the origin of the name, "XL," as it stands for eXtended Linearization, but is also the designation that means "extra large" for items of clothing.

There are several successor algorithms that are enhancements of the XL algorithm, including MutantXL [13] [2] [11]. The F4 family of algorithms, discovered independently by Jean-Charles Faugere [12], and his coauthors, can also be shown to be equivalent (or very similar) to the XL algorithm in many cases, and has many follow-on papers as well.

To be concise, this talk will focus only on the original XL paper (making the talk extremely well-suited to beginners), and if time permits, the connections to NP-Completeness will be sketched, but there will not be time for proofs. Further information on the XL family of algorithms can be found in Chapter 12.4, "The XL

Algorithm," of *Algebraic Cryptanalysis* [1], a monograph written by the speaker, and published by Springer in 2009.

References

[1] G. Bard, *Algebraic Cryptanalysis*, Springer, 2009.

[2] J. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed. "MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis." Dagstuhl seminar proceedings Report No. 09031. 2009.

[3] N. Courtois. *The security of cryptographic primitives based on multivariate algebraic problems: MQ, MinRank, IP, HFE*. Ph.D. Thesis, University of Paris VI (2001). Available at `http://www.nicolascourtois.net/phd.pdf`

[4] N. Courtois. "The security of Hidden Field Equations (HFE)." Proceedings of the CryptographersÕ Track, RSA Conference, (RSA'01). *Lecture Notes in Computer Science*, **Vol. 2020**. Springer, 2001. Pp. 266–281.

[5] N. Courtois. "Higher order correlation attacks, XL algorithm and cryptanalysis of Toyocrypt." Proceedings of International Conference on Information Security and Cryptology (ICSC'02), *Lecture Notes in Computer Science*, **Vol. 2587**. Springer, 2002. Pp. 182–199.

[6] N. Courtois. "Fast algebraic attacks on stream ciphers with linear feedback." Advances in Cryptology—Proceedings of (CRYPTO'03), *Lecture Notes in Computer Science*, **Vol. 2729**. Springer, 2003. Pp. 176–194.

[7] N. Courtois. "Generic attacks and the security of Quartz." Public Key Cryptography (PKCÕ03). *Lecture Notes in Computer Science*, **Vol. 2567**. Springer, 2003. Pp. 351–364.

[8] N. Courtois. "Algebraic attacks on combiners with memory and several outputs." Proceedings of International Conference on Information Security and Cryptology (ICISC'04). *Lecture Notes in Computer Science*, **Vol. 3506**. Springer, 2004. Pp. 3–20.

[9] . N. Courtois and G. Bard. "Algebraic cryptanalysis of the data encryption standard." Proceedings of the 11th IMA international conference on Cryptography and Coding (IMACC'07). *Lecture Notes in Computer Science*, **Vol. 4887**. Springer, 2008. Pp 152–169.

[10] N. Courtois, A. Klimov, J. Patarin, A. Shamir. "Efficient Algorithms for Solving Over-defined Systems of Multivariate Polynomial Equations." Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT'00). *Lecture Notes in Computer Science*, **Vol. 1807**. Springer, 2000. Pp. 392–407.

[11] J. Ding, J. Buchmann, M.S.E. Mohamed, W.S.A. Mohamed, R. P. Weinmann. "MutantXL." Proceedings of the 1st international conference on Symbolic Computation and Cryptography (SCC'08). LMIB. 2008. Pp. 16–22.

[12] J. C. Faugere. "A new efficient algorithm for computing Groebner bases (F4)." *Pure and Applied Algebra*. **Vol. 139**. 1999. Pp. 61–88.

[13] M. S. E. Mohamed, W. S. A. E. Mohamed, J. Ding, J. Buchmann. "MXL2: Solving Polynomial Equations over GF(2) using an Improved Mutant Strategy." Proceedings of The Second international Workshop on Post-Quantum Cryptography (PQCrypto'08). *Lecture Notes in Computer Science*, **Vol. 5299**. Springer, 2008. Pp. 203–215.