Goubin, Louis; **Courtois, Nicolas T.**

Cryptanalysis of the TTM cryptosystem. (English) Zbl 0980.94017

Okamoto, Tatsuaki (ed.), Advances in cryptology - ASIACRYPT 2000. 6th international conference on the Theory and application of cryptology and information security, Kyoto, Japan, December 3-7, 2000. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1976, 44-57 (2000).

Summary: *H. Fell* and *W. Diffie* proposed constructing trapdoor functions with multivariate equations [Proc. Crypto '85, Lect. Notes Comput. Sci. 218, 340-349 (1985)]. They used several sequentially solved stages that combine into a triangular system we call T. In the present paper, we study a more general family of TPM (for "Triangle Plus Minus") schemes: a triangular construction mixed with some u random polynomials and with some r of the beginning equations removed. We go beyond all previous attacks proposed on such cryptosystems using a low degree component of the inverse function. The cryptanalysis of TPM is reduced to a simple linear algebra problem called MinRank(r): Find a linear combination of given matrices that has a small rank r. We introduce a new attack for MinRank called 'Kernel Attack' that works for q^r small. We explain that TPM schemes can be used in encryption only if q^r is small and therefore they are not secure. As an application, we show that the TTM cryptosystem proposed by *T. T. Moh* at CrypTec'99 (*) [Communications in Algebra 27, 2207-2222 (1999; Zbl 0933.94022) and Proc. CrypTEC'99, Int. Workshop Cryptographic Techniques and E-commerce, Hong-Kong City University Press, 63-69 (1999), available at http://www.usdsi.com/cryptec.ps] reduces to MinRank(2). Thus, though the cleartext size is 512 bits, we break it in $\mathcal{O}(2^{52})$. The particular TTM of (*) can be broken in $\mathcal{O}(2^{28})$ due to additional weaknesses, and we needed only a few minutes to solve the challenge TTM 2.1. from the website of the TTM selling company, US Data Security. We also studied TPM in signature, possible only if q^u small. It is equally insecure: the 'Degeneracy Attack' we introduce runs in $q^u \cdot$ polynomial.

For the entire collection see [Zbl 0952.00064].

MSC:

94A60 Cryptography

Keywords:

trapdoor functions; multivariate equations; cryptanalysis; TPM schemes; TTM cryptosystem; signature