Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards

Nicolas T. Courtois[1], Karsten Nohl[2], and Sean O'Neil[3]

[1] University College London, UK
[2] University of Virginia, USA
[3] VEST Corporation, France

Disclaimer: this paper is an early announcement of a research in progress.

Abstract. MiFare Crypto 1 is a lightweight stream cipher used in London's Oyster card, Netherland's OV-Chipcard, US Boston's CharlieCard, and in numerous wireless access control and ticketing systems worldwide. Recently, researchers have been able to recover this algorithm by reverse engineering [11, 13].
We have examined MiFare from the point of view of the so called *algebraic attacks*. We can recover the full 48-bit key of the MiFare algorithm in 200 seconds on a PC, given 1 known IV (from one single encryption).
The security of this cipher is therefore close to zero. This is particularly shocking, given the fact that, according to the Dutch press, 1 billion of MiFare Classic chips are used worldwide, including many government security systems.
Keywords: London Oyster card, Dutch public transit OV-Chipcard, Boston's CharlieCard RFID tags, Mifare Crypto 1 algorithm, stream ciphers, algebraic cryptanalysis, Boolean functions, Gröbner bases, SAT solvers.

1 Background

Recently, several researchers have been able to reverse-engineer the MiFare Classic cryptographic algorithm Crypto-1 that is used (among others) in London's Oyster card, Netherland's OV-Chipcard, US Boston's CharlieCard, and in numerous wireless access control and ticketing systems worldwide [11, 13].

The MiFare cipher is a proprietary algorithm and its specification was not published so far. The researchers have been fair play: they informed the authorities and announced that the industry should have some time to upgrade their systems. However this does not make the system very secure: if we do not publish Crypto 1 for the time being, hackers will without doubt recover it very soon.

How secure are these algorithms? Dutch researchers exploited mostly the protocol vulnerabilities of MiFare [13]. After a report by the Dutch security agency TNO that found the MiFare Classic tags to be secure enough for some applications [17], Karsten Nohl announced the first cryptographic attack on the system [12]. This attack exploits statistical weaknesses of the cipher, in combination with a weakness in the random number generator in the tag reader. By combining these two vulnerabilities, cards can be cloned within minutes on a PC [12].

We have examined MiFare from the point of view of the *algebraic attacks*. These are general-purpose attack techniques developed in the last years by Courtois, Meier, Faugère *et al.* Our attacks are purely cryptographic attacks that work independently of the quality of the random numbers. Furthermore, our new attacks are an order of magnitude faster and also do not require any active interaction with the reader or the card to find the secret key.

2 How to Solve It - Algebraic Attacks on MiFare

Our attack is an *algebraic attack* in the sense that it recovers the secret key by solving a large system of polynomial equations [1, 2]. Equations are written using a method that is identical to one of the algebraic attacks on the DES described in [4]. We write a system of symbolic Boolean equations that involves the output bits, the key bits, the IV bits, and a large number of intermediate variables. The encryption process is decomposed into a large number of very simple elementary steps. Each of these simple steps is described algebraically as a small set of simple algebraic equations of low degree, with variables over $GF(2)$.

One of the method for solving such equations is to use the so called Gröbner bases, which have in the past allowed the researchers to break several stream ciphers [2, 6]. However, a new particularly efficient technique of algebraic cryptanalysis with SAT solvers was discovered recently [4, 5]. Accordingly, the resulting system of equations is converted to a SAT problem by the conversion algorithm described in [5]. Then a well-known open-source SAT solver program is executed, [10] which finds a solution to the system of equations.

In our attacks we require about 50 bits of the keystream output by the stream cipher to recover the secret key (or the initial state). This is the minimum required to determine the key uniquely, and we do not need much more. These 50 bits may come from one single or several encryptions with different IVs. An elegant way of recovering the keystream from MiFare Classic cards has recently been presented by de Koning Gans et al. [7].

3 Summary of Claims

We can recover the full 48-bit key of MiFare Crypto-1 algorithm in 200 seconds on one 1.66 GHz Centrino CPU, given 1 known IV and 50 output bits (from one single encryption).

With 4 chosen IVs we can recover the key in 12 seconds.

In addition we expect to be able to crack the MiFare cipher as it is used in widely deployed products such as London Oyster cards. We attack this application of MiFare in the weakest possible scenario – passive eavesdropping of one single transaction. This is currently being confirmed and implemented in practice. Preliminary results indicate that the whole attack (collecting data, finding the secret key, and creating a clone card) should not take more than a few minutes. More details will be published soon.

References

1. Nicolas Courtois and Josef Pieprzyk: *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations,* Asiacrypt 2002, LNCS 2501, pp.267-287, Springer.
2. Nicolas Courtois and Willi Meier: *Algebraic Attacks on Stream Ciphers with Linear Feedback,* Eurocrypt 2003, Warsaw, Poland, LNCS 2656, pp. 345-359, Springer.
3. Nicolas Courtois: *General Principles of Algebraic Attacks and New Design Criteria for Components of Symmetric Ciphers,* in AES 4 Conference, Bonn May 10-12 2004, LNCS 3373, pp. 67-83, Springer, 2005.
4. Nicolas Courtois and Gregory V. Bard: *Algebraic Cryptanalysis of the Data Encryption Standard,* In Cryptography and Coding, 11-th IMA Conference, Cirencester, UK, 18-20 December 2007. Springer LNCS.
5. Gregory V. Bard, Nicolas T. Courtois and Chris Jefferson: *Efficient Methods for Conversion and Solution of Sparse Systems of Low-Degree Multivariate Polynomials over GF(2) via SAT-Solvers,* Available at http://eprint.iacr.org/2007/024/.
6. Gwenolé Ars, Jean-Charles Faugère: *An Algebraic Cryptanalysis of Nonlinear Filter Generators using Gröbner Bases,* INRIA research report, available at https://hal.ccsd.cnrs.fr/.
7. Gerhard de Koning Gans, Jaap-Henk Hoepman, Flavio D. Garcia: *A Practical Attack on the MIFARE Classic,* Internet preprint, 15 Mar 2008, at http://aps.arxiv.org/abs/0803.2285.
8. J. Hulsbosch: *Analyse van de zwakheden van het DES-algoritme door middel van formele codering,* Master thesis, K. U. Leuven, Belgium, 1982.
9. Fabio Massacci and Laura Marraro: *Logical cryptanalysis as a SAT-problem: Encoding and analysis of the U.SS. Data Encryption Standard,* In Journal of Automated Reasoning, vol 24, pp. 165-203. 2000. Essentially the same paper appears in the proceedings of SAT-2000 conference, Highlights of Satisfiability Research at the Year 2000, J. Gent, H. van Maaren, and T. Walsh, Eds, pp. 343-376, IOS Press, Amsterdam, 2000.
10. MiniSat 2.0. An open-source SAT solver package, by Niklas Eén, Niklas Sörensson, available from http://www.cs.chalmers.se/Cs/Research/FormalMethods/MiniSat/
11. Karsten Nohl, Henryk Plötz: *Mifare - Little security despite Obscurity,* See http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
12. Karsten Nohl: *Cryptanalysis of Crypto-1,* Short paper available at http://www.cs.virginia.edu/ kn5f/Mifare.Cryptanalysis.htm
13. Ronny Wichers Schreur, Peter van Rossum, Flavio Garcia, Wouter Teepe, Jaap-Henk Hoepman, Bart Jacobs, Gerhard de Koning Gans, Roel Verdult, Ruben Muijrers, Ravindra Kali, Vinesh Kali: *Security Flaw in Mifare Classic,* Press release, Digital Security group, Radboud University Nijmegen, March 12, 2008, http://www.sos.cs.ru.nl/applications/rfid/pressrelease.en.html.
14. Claude Elwood Shannon: *Communication theory of secrecy systems,* , Bell System Technical Journal 28 (1949), see in particular page 704.
15. I. Schaumuller-Bichl: *Cryptanalysis of the Data Encryption Standard by the Method of Formal Coding,* In Cryptography, Proc. Burg Feuerstein 1982, LNCS 149, T. Beth editor, Springer-Verlag, 1983.
16. Tanenbaum, A. News Summary of Broken Dutch Public Transit Card. See www.cs.vu.nl/ ast/ov-chip-card,
17. Security Analysis of the Dutch OV-Chipkaart, Public excerpt of TNO report 34642, see www.tno.nl.