Algebraic and Slide Attacks on KeeLoq



Nicolas T. Courtois ¹ Gregory V. Bard ²

¹ - University College of London, UK
² - University of Maryland, US
³ MARYLAN



KeeLoq

Block cipher used to unlock doors and the alarm in Chrysler, Daewoo, Fiat, GM, Honda, Jaguar, Toyota, Volvo, Volkswagen, etc...





How Much Worth is KeeLoq

- Designed in the 80's by Willem Smit.
- In 1995 sold to Microchip Inc for more than 10 Million of US\$.







Algebraic Cryptanalysis [Shannon]

Breaking a « good » cipher should require:

"as much work as solving a system of simultaneous equations in a large number of unknowns of a complex type"

[Shannon, 1949]







KeeLoq Encryption

Block Cipher

- Highly unbalanced Feistel
- •528 rounds
- •32-bit block / state
- •64-bit key
- •1 bit updated / round
- •1 key bit / round only !

KeeLoq Encryption

Sliding property:

periodic cipher with period 64.

Courtois, Bard, 2007





Algebraic Attacks on KeeLoq

We have found MANY attacks.

One is particularly simple:







KeeLoq and Sliding

Classical Sliding Attack [Grossman-Tuckerman 1977]:

- Take 2^{n/2} known plaintexts (here n=32, easy !)
- We have a "slid pair" (P_i, P_j) s.t.







Classical Sliding – Not Easy

Classical Sliding Attack [Grossman-Tuckerman 1977]: • Take 2^{n/2} known plaintexts (here n=32, easy !) • We have a "slid pair" (P_i,P_i).





Algebraic Sliding

Answer [our attack]:





Algebraic Attack:

We are able to use C_i,C_j directly ! Merge 2 systems of equations:





System of Equations

64-bit key. Two pairs on 32 bits. Just enough information.

Attack:

- Write an MQ system.
 - Gröbner Bases methods miserably fail.
- Convert to a SAT problem
 - [Cf. Courtois, Jefferson, Bard eprint/2007/024/].
- Solve it.

11

• Takes 2.3 seconds on a PC with MiniSat 2.0.





Attack Summary:

Given about 2¹⁶ KP.

- We try all 2^{32} pairs (P_i, P_j) .
- If OK, it takes 2.3 seconds to find the 64-bit key.
- If no result early abort.

Total attack complexity about 2⁶⁴ CPU clocks which is about 2⁵³ KeeLoq encryptions.

KeeLoq is badly broken.

Practical attack, tested and implemented.





Other Attacks

Our fastest attack: about 2³⁷ KeeLoq encryptions, but more KP, see:

See eprint.iacr.org/2007/062/

