

How to Steal Cars – A Practical Attack on KeeLoq[®]

Eli Biham¹ Orr Dunkelman² Sebastiaan Indestege²
Nathan Keller³ Bart Preneel²

¹Computer Science Department, Technion, Israel.

²Dept. ESAT/SCD-COSIC, K.U.Leuven, Belgium.

³Einstein Institute of Mathematics, Hebrew University, Israel.

CRYPTO 2007 Rump Session



What?

- ▶ Lightweight block cipher
- ▶ 32-bit block size
- ▶ 64-bit key
- ▶ Sold by Microchip[®] Inc.



Where Is It Used?

- ▶ Remote keyless entry applications
- ▶ Car locks and alarms

Cars?



- ▶ Supposedly all use KeeLoq[®]

Previous Attacks on KeeLoq[®]

Attack Type	Data	Time	Memory	Reference
Slide/Guess&Det.	2^{32} KP	2^{52}	16 GB	[B07]
Slide/Guess&Det.	2^{32} KP	$2^{50.6}$	16 GB	[B07b]
Slide/Algebraic	2^{16} KP	$2^{65.4}$?	[CB07]
Slide/Algebraic	2^{16} KP	$2^{51.4}$?	[CB07]
Slide/Fixed Points	2^{32} KP	2^{43}	> 16 GB	[CB07]
Slide/Cycle	2^{32} KP	$(2^{35.4})$	16.5 GB	[CB07]
Slide/Cycle/Guess&Det.	2^{32} KP	(2^{37})	16.5 GB	[B07b]



Our Attacks on KeeLoq[®]

Key Recovery Attack

- ▶ Based on:
 - ▶ Slide Attack
 - ▶ Meet-in-the-Middle
- ▶ 2^{16} Known (or Chosen) Plaintexts
- ▶ $2^{44.5}$ KeeLoq[®] Encryptions
- ▶ **< 3 MB** Memory



"Slide"



"Meet-in-the-Middle"

Our Attacks on KeeLoq[®] (cont.)

“Secure Learning” Key Derivation Procedure

- ▶ The manufacturer has a master secret
- ▶ For each car there is a unique identifier (known to the attacker)
- ▶ The XOR of these two gives the secret key used in this car.



Conclusion

- ▶ Finding **one** KeeLoq key leaks the **master secret**.

Our Attacks in Practice

Gathering Data

- ▶ “Identify Friend or Foe” (IFF) protocol
- ▶ Get 2^{16} chosen plaintexts in \approx **65 min.!**



Attack Implementation

- ▶ Fully implemented and tested
- ▶ $< 2^{16} \cdot 5$ minutes on an AMD Athlon 64 X2 4200+
- ▶ **€10 000**, 50 Dual Core machines, about **two days**
- ▶ Up to **500×** faster than previously known attacks

Conclusions

- ▶ KeeLoq[®] is badly broken
- ▶ Soon, cryptographers will all drive expensive cars*



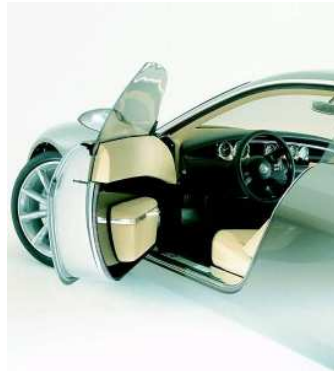
Attack Type	Data	Time	Memory
Slide/Meet-in-the-Middle	2^{16} KP	500 CPU days	≈ 3 MB
Slide/Meet-in-the-Middle	2^{16} CP	218 CPU days	≈ 2 MB

<http://www.cosic.esat.kuleuven.be/keeloq/>

*Not all conclusions are to be taken too seriously. . .

References

- [B07] Andrey Bogdanov
Cryptanalysis of the KeeLoq block cipher
Cryptology ePrint Archive,
Report 2007/055
<http://eprint.iacr.org/2007/055/>
- [B07b] Andrey Bogdanov
Attacks on the KeeLoq Block Cipher and
Authentication Systems
3rd Conference on RFID Security 2007
RFIDSec 2007 (to appear)
- [CB07] Nicolas T. Courtois and Gregory V. Bard
Algebraic and Slide Attacks on KeeLoq
Cryptology ePrint Archive,
Report 2007/062
<http://eprint.iacr.org/2007/062/>



<http://www.cosic.esat.kuleuven.be/keeloq/>