Master Project Proposal
Rajesh Bachani (s061332)
Supervisor: Dr. Erik Zenner, MAT Department
Technical University of Denmark

CRYPTANALYSIS OF HITAG2 CIPHER

INTRODUCTION

The HiTag2 cipher is a stream cipher designed by Philips Semiconductors, which is used in RFID tags. In HiTag2 products, communication between the RFID reader and the RFID tags is protected using this stream cipher. An incomplete graphical description of the cipher is given at the link [1]. The cipher has recently been reverse engineered, and thus not much documentation is available. The main documents are the graphical description and the source code of the cipher, both available at [1], and the data sheet of the Tag IC [3], which contains a section on a high-level working of the HiTag2 modes in the microcontroller.

PROJECT

Main Work

The main work in the project would be to do a cryptanalysis of the HiTag2 cipher. The cryptanalysis of A5/1 cipher [2] would be used as a starting point i.e. idea applied in breaking A5/1 would be used in breaking HiTag2, at least initially in the cryptanalysis. A5/1 is a symmetric key encryption algorithm used in GSM, for encrypting the channel between the mobile phone and the base station. In the A5/1 cryptanalysis paper [2], implementation approaches are described which can be used in finding the secret key used in the encryption. The attacks are carried on a PC and are based on time-memory tradeoff. With a more cost on memory (pre-computation) the attack can be carried out in real time, while with less amount of pre-computations, the attack is carried out in a longer time, since finding the secret parameters requires more number of matches.

Much of the inspiration in the assumption that ‘HiTag2 is breakable’ comes from the key length being used in the cipher, which is just 48 bits. But in addition, it seems that the design of the cipher itself could have some flaws. So, in addition to breaking the cipher using exhaustive search (time) or table lookups (memory), we are also going to focus in finding algorithmic flaws in the cipher. Since the cipher is designed with heavy space and power constraints, it is quite likely that the design would have several weaknesses. We would be analyzing the cipher in this aspect, as well.

Further Work

There are a number of possibilities where the project could head towards the end. Some of them are mentioned below. The direction in which the project moves would be duly discussed with the supervisor in every respect.

1. The demonstration of the time-memory tradeoff attacks could be either implemented on a PC or on FPGA.

2. In addition to the time-memory tradeoff attacks, we could choose attacks known on other stream ciphers, and investigate their applicability on the HiTag2 cipher.

3. Moreover, we could pick up other similar stream ciphers (ciphers used in similar applications) like Mifare, and do a comparison of them with HiTag2 using relevant parameters defining their security.

Important Dates

Project Duration – 5 months
Start Date – 10th March 2008
Vacation – 15th May to 15th June
End Date – 10th September 2008

REFERENCE

[1] http://cryptolib.com/ciphers/hitag2/

[2] Alex Biryukov, Adi Shamir, David Wagner, Real Time Cryptanalysis of A5/1 on a PC, Proceedings of the 7th International Workshop on Fast Software Encryption, p.1-18, April 10-12, 2000

[3] Datasheet for PCF7952ATT, Active Tag IC and Processor (ACTIC-Pro), Preliminary Specification, Philips Semiconductors, March 23, 2005.