Breaking KEELQ in a Flash: On Extracting Keys at Lightning Speed*

Markus Kasper, Timo Kasper, Amir Moradi, and Christof Paar
Horst Görtz Institute for IT Security, Ruhr University Bochum, Germany
{mkasper,tkasper,moradi,cpaar}@crypto.rub.de

Abstract. We present the first simple power analysis (SPA) of software implementations of KEELQ. Our attack drastically reduces the efforts required for a complete break of remote keyless entry (RKE) systems based on KEELQ. We analyze implementations of KEELQ on microcontrollers and exploit timing vulnerabilities to develop an attack that allows for a practical key recovery within seconds of computation time, thereby significantly outperforming all existing attacks: Only one single measurement of a section of a KEELQ decryption is sufficient to extract the 64 bit master key of commercial products, without the prior knowledge of neither plaintext nor ciphertext. We further introduce techniques for effectively realizing an automatic SPA and a method for circumventing a simple countermeasure, that can also be applied for analyzing other implementations of cryptography on microcontrollers.

1 Motivation

Due to its wide deployment in RKE systems, the KEELQ cipher has come to the attention of cryptographers in 2007 [1]. Several improved cryptanalytical attacks followed, but still, their complexity and other requirements make them impractical for real-world products.

This situation extremely changed with the first differential power analysis (DPA) of KEELQ as presented on CRYPTO 2008 [5]. The paper describes how secret keys can be revealed in practice from the power consumption of KEELQ implementations in hardware and software. In Sect. 3.3 we reflect, how especially knowing his master key allows for devastating attacks on all systems of a manufacturer. Unfortunately - from the attacker’s point of view - the extraction of the master key remains difficult and requires some efforts, because the software implementations programmed into the receivers are very hard to analyze using DPA, as discussed in Sect. 4.

We illustrate in the following, that in some cases performing a key recovery by SPA is much easier and much more efficient than by DPA, and demonstrate that SPA constitutes a remedy for the open problem of extracting the master key from KEELQ software implementations. Starting from a specific unprotected

* The work described in this paper has been supported in part by the European Commission through the ICT programme under contract ICT-2007-216676 ECRYPT II.
software implementation of the algorithm - as recommended by Microchip - we develop a highly effective SPA attack in Sect. 5. Usually, an SPA is performed based on tedious visual inspection, as detailed in Sect. 5.2 or by massive profiling of a similar device, which takes a lot of efforts and time. In Sect. 5.3 a non-heuristic method to avoid the visual inspection in some types of SPA attacks is presented, enabling a full key recovery from just a single measurement of the power consumption. We practically verify our findings by attacking some commercial KeeLoq implementations on PIC 8-bit microcontrollers and proof the effectiveness of our methods, even in the presence of a simple countermeasure. Removing the effect of reoccurring disturbing patterns in the traces, that hinder DPA and SPA in the first place, is detailed in Sect. 6. Before developing our new attack, we give some necessary background information about power analysis in Sect. 2 and briefly introduce KeeLoq RKE systems in Sect. 3. Finally, the effectiveness of DPA and SPA in the case of KeeLoq is discussed in Sect. 7.

This article meliorates the CRYPTO 2008 attacks in terms of a great reduction of the required time and computations to recover secret master keys of different manufacturers and hence allows to completely circumvent many KeeLoq systems in the field with almost no effort.

2 Power Analysis in a Nutshell

In contrast to a mathematical cryptanalysis which requires pairs of plain- and ciphertexts, in the context of power analysis knowing either the input or the output of the cipher is sufficient to mount a key-recovery attack. By measuring and evaluating the power consumption of a cryptographic device, information-dependent leakage is exploited and combined with the knowledge about the plaintext or ciphertext in order to extract, e.g., a secret key. Since intermediate results of the computations can be derived from the leakage, e.g., from the Hamming weight of the data processed in a software implementation, a divide-and-conquer strategy becomes possible, i.e., the secret key could be recovered bit by bit.

2.1 Preprocessing

For unknown implementations, it is often difficult to find an appropriate trigger point for starting the oscilloscope, e.g., a special feature in the traces, that reoccurs at the same instant in each measurement. Accordingly, the alignment of the measurements typically needs to be improved as a first preprocessing step after the acquisition. Furthermore, traces can be very large or too noisy for an effective evaluation – thus they might need to be compressed or averaged prior to statistical analysis.

Peak Extraction. The dynamic power consumption is the dominant factor disclosing the processed data of complementary metal oxide semiconductor (CMOS) circuits. The corresponding peaks appearing in the measurements on each edge of the clock hence play a prominent role for power analysis. Processing only