Cryptology ePrint Archive: Report 2011/242

Cryptanalysis of KeeLoq code-hopping using a Single FPGA

Idan Sheetrit and Avishai Wool

Abstract: The KeeLoq cipher is used in many wireless car door systems and garage openers. Recently the algorithm was studied and several attacks have been published. When a random seed is not used the attack on the system is fairly straight-forward. However when a seed is shared between the remote control and the receiver previous research suggested using highly parallel crypto hardware (like COPACOBANA) for breaking the cipher within reasonable time.

In this paper we show that highly-parallel hardware is not necessary: our attack uses a single FPGA for breaking KeeLoq when using a 48-bit random seed in 17 hours using a mid-range Virtex-4, and less than 3 hours using a high-end Virtex-6 chip. We achieve these results using a combination of algorithmic improvements, FPGA design methodology, and Xilinx-specific features.

Category / Keywords: secret-key cryptography /

Date: received 15 May 2011

Contact author: yash at eng tau ac il