Breaking Hitag-2 with COPACOBANA

Petr Stembera, Martin Novotny
Czech Technical University, Praque

Abstract

The Hitag2 stream cipher is used in many real-world applications, such as car immobilizers and door opening systems, as well as for the access control of buildings. The short length of the 48-bit secret key employed makes the cipher vulnerable to a brute-force attack, i.e., exhaustive key search. In this paper we develop the first hardware architecture for the cryptanalysis of Hitag2 by means of exhaustive key search.

Our implementation on the Cost-Optimized Parallel Code-Breaker COPACOBANA is able to reveal the secret key of a Hitag2 transponder in less than 2 hours (103.5 minutes) in the worst case. The speed of our approach outperforms all previously proposed attacks and requires only 2 sniffed communications between a car and a tag. Our findings thus define a new lower limit for the cloning of car keys in practice. Moreover, the attack is arbitrarily parallelizable and could thus be run on multiple COPACOBANAs to decrease the time to find the secret key.