KeeLoq on COPACOBANA

KeeLoq algorithm is widely used on remote key-less entry systems, e.g., remote of garage door openers and the central lock of some vehicles. The algorithm has been analyzed by several researches, and some cryptanalytical attacks are possible on the KeeLoq algorithm. KeeLoq is used mainly on two different application scenarios: i) rolling code scheme and ii) challenge-response protocol. In the first case, the remote control has a counter inside which is incremented by each time when a button (of the remote) is pressed. The counter value is contributed in the plaintext of the KeeLoq encryption algorithm, and finally the ciphertext is sent by the remote to the receiver which is inside a car, a garage, or a house. Since the plaintext is not obvious when monitoring the communication, the cryptanalysis attacks on the KeeLoq algorithm are not possible, and only side-channel attacks which have been done before are applicable. However, in the second application scenario (challenge-response) both the plaintext and ciphertext are available for the attacker, and the any of the cryptanalysis methods is possible. The best attack which has been proposed so far needs $2^{16}$ pairs of plaintext and ciphertext has been published in 2008. It has been implemented on 50-core PCs and can recover the secret key in average around 4 days.

On the other hand, the Cost-Optimized Parallel Code-Breaker COPACOBANA, which is an FPGA-based machine optimized for running cryptanalytical algorithms and consists of 120 SPAR-TAN III FPGAs, is suitable for parallel computation problems. The aim of this project is to try implementing the already verified attack on COPACOBANA. Since the attack needs at least $2^{16}$ 64-bit plaintext-ciphertexts and must generate and search inside some other tables during the attack, implementing the attack on COPACOBANA, which has a low amount of memory and suffers from low communication speed, will face to many challenges to be solved. In fact, the most of the work in this project would be to manage the usage of memory and communication bottleneck.

Contact
If this sounds interesting to you, please contact Dr. Amir Moradi, moradi@crypto.rub.de