Speed and Area-Optimized Password Search of bcrypt on FPGAs

F. Wiemer, R. Zimmermann

Abstract

Password-based Key Derivation functions are used to generate key material from a given password, wasting computation time to reduce the efficiency of (bruteforce) attacks. The most promising alternatives to the current standard, PBKDF2, are bcrypt and scrypt. The current Password Hashing Competition (PHC) [1] aims at providing new alternatives, learning from attacks of bcrypt and scrypt. In this context, bcrypt is considered to be resilient to hardware attacks both on ASICs/FPGAs and GPUs [2].
In December 2013, [3] presented multiple energy-efficient implementations of bcrypt. The FPGA implementation was build using a Zedboard - combining an ARM with an FPGA and outsourced only a fragment of bcrypt to the FPGA, running 14 cores in parallel at 100 MHz. Nevertheless, the design lead to a highly unbalanced resource utilization.
In this work, we present a bcrypt password-search on the same Zedboard, which runs the full bcrypt algorithm on-chip. In addition, it also features an on-chip password generation for bruteforce attacks.
The design is still work in progress, but implements at the current state 24 full bcrypt cores running at 200 MHz and improves the results of [3] by a factor of roughly 4 without using the full potential of the ARM processor.

1 `https://password-hashing.net`

2 `http://www.openwall.com/presentations/Passwords12-The-Future-Of-Hashing/`

3 `http://www.openwall.com/presentations/Passwords13-Energy-Efficient-Cracking/`