Parallelization of Brute-Force Attack on MD5 Hash Algorithm on FPGA

Submitted by grigby1 on Fri, 09/04/2020 - 3:37pm

Title	Parallelization of Brute-Force Attack on MD5 Hash Algorithm on FPGA
Publication Type	Conference Paper
Year of Publication	2019
Authors	Gillela, Maruthi, Prenosil, Vaclav, Ginjala, Venkat Reddy
Conference Name	2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)
Keywords	32/34/26-instance parallelization, brute force attacks, Computer architecture, cryptography, field programmable gate arrays, Generators, GPU, guess password generation, Hardware, Hardware design languages, Hardware Implementation, HDL, human factors, IP core, LUT, MD5 hash algorithm, MD5 hash generation, password, pipeline processing, policy-based governance, pre-image brute-force attack, pubcrawl, single Virtex-7 FPGA device
Abstract	FPGA implementation of MD5 hash algorithm is faster than its software counterpart, but a pre-image brute-force attack on MD5 hash still needs 2?(128) iterations theoretically. This work attempts to improve the speed of the brute-force attack on the MD5 algorithm using hardware implementation. A full 64-stage pipelining is done for MD5 hash generation and three architectures are presented for guess password generation. A 32/34/26-instance parallelization of MD5 hash generator and password generator pair is done to search for a password that was hashed using the MD5 algorithm. Total performance of about 6G trials/second has been achieved using a single Virtex-7 FPGA device.
DOI	10.1109/VLSID.2019.00034
Citation Key	gillela_parallelization_2019

Cryptography Hardware Implementation computer architecture Hardware Generators pubcrawl password Human Factors policy-based governance gpu field programmable gate arrays 32/34/26-instance parallelization guess password generation Hardware design languages HDL IP core LUT MD5 hash algorithm MD5 hash generation pipeline processing pre-image brute-force attack single Virtex-7 FPGA device brute force attacks