A High-Performance Parallel Computation Hardware Architecture in ASIC of SHA-256 Hash

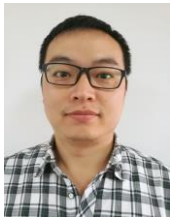
Xiaoyong Zhang*, Ruizhen Wu*, Mingming Wang*, Lin Wang*

**Intel Mobile Communications Technology (Xi'an) Ltd, Xi'an Shaanxi Province*

xiao-yong.zhang@intel.com, ruizhen.wu@intel.com, mingming.wang@intel.com, lin.b.wang@intel.com

***Abstract*—The SHA-256 is playing an important role in various applications, such as e-transactions and bitcoins. To achieve more profits, the SHA-256 computation capacity is a main research direction of Hashing Algorithm. In this paper, a high-performance hardware architecture of SHA-256 hash is proposed. The computation of SHA-256 is rescheduled based on hardware characterises. Three pipelines are used to replace the critical path in the round functions which can shorten the long critical path, and divide the computation chain into independent parts. Multi-computation of SHA-256 is working in parallel pipelines, indicating that the computation capacity can be 3 times of standard SHA-256 implementation. The proposed SHA-256 hardware architecture has been implemented and synthesized with Intel 14nm technology. Simulation and synthesis results show the proposed SHA-256 hashing throughput can be improved by 3 times with 50.7% power reduction, at an area cost of 2.9 times compared to the standard implementation.**

***Keyword*—About Cryptography; Application specific integrated circuits; High-speed integrated circuits; Low-power**



Xiaoyong, Zhang was born in China, Nov 5th 1980. Bachelor. The first bachelor degree was earned in automation, in School of Marine Science and Technology, Northwestern Polytechnical University, Shaanxi Province, China, in 2003, and the second bachelor degree was earned in electronic science and technology, in Institute of Microelectronics, Tsinghua University, Beijing City, China, in 2005.
He has worked in Xi'an, Shaanxi Province, China, since 2005, in the wireless department for Infineon Technology at first, which was acquired later by Intel in 2011. His current job is hardware design and validation.

Ruizhen, Wu was born in China, Jan 1st 1986. PhD. The PhD was earned in School of Microelectronics of XIDIAN University, Shaanxi Province, China, in 2014. The major field of study is Asynchronous Circuits design and 5G CODEC.
He has worked in Hangzhou, Zhejiang Province, China, since 2014, in the 2012 communication lab of Huawei at first, and Intel iCDG in Xi'an, Shaanxi Province since 2016.

Mingming, Wang was born in China, Oct 1st 1986. Master. The Master degree was earned in Computer Application Technology in Xi'an University of posts & Telecommunications, Shaanxi Province, China, in 2011, and the bachelor degree was earned in electronic science and technology, in Xi'an University of posts & Telecommunications, Shaanxi Province, China in 2008.
He has worked in Intel iCDG Xi'an, Shaanxi Province, China since 2011.

Lin, Wang was born in China, Dec. 1st. 1971. Master of Sci. The master degree was earned in Dept. of Electrical Engineering, Fudan University, Shanghai, China, in 1998. His majority is microelectronics and physics on semiconductor and semiconductor device.
He worked in Shanghai Nortel Semiconductor and Broadcom, focusing on communication chip development after his graduation.
He is now the Director of Digital Design in Intel Xi'an, Shaanxi Province, China, ever since 2005.