计算机应用 2012, 32(03) 864-866 DOI: 10.3724/SP.J.1087.2012.00864 ISSN: 1001-9081 CN: 51-1307/TP



典型应用

# Keccak算法|海绵结构|哈希算法|可重构|现场可编程门阵列

吴武飞[1],王奕[1,2,3],李仁发[1,2,3]

1.湖南大学 嵌入式系统与网络实验室, 长沙 410082;
2.湖南大学 湖南省研究生培养创新基地, 长沙 410082;
3.湖南大学 网络与信息安全湖南省重点实验室, 长沙 410082

**摘要:** 在分析研究Keccak算法的基础上,针对现有Keccak算法的硬件实现方案版本单一,应用不灵活的问题,设计了一种高性能可重构的Keccak算法硬件实现方案。实验结果表明:该方案在Xilinx 公司的现场可编程门阵列(FPGA)Virtex-5平台上的时钟频率可达214MHz,占用1607slices;该方案具有吞吐量高(9131Mbps),应用灵活性好,可支持4种不同参数版本的优点。

**关键词:** KECCAK 海绵结构 哈希算法 可重构 现场可编程门阵列(FPGA)

## Reconfigurable Keccak algorithm and its implementation on FPGA platform

WU Wu-fei[1], WANG Yi[1,2,3], LI Ren-fa[1,2,3]

1.Embedded Systems and Networking Laboratory, Hunan University, Changsha Hunan 410082, China;
2.Hunan Province Graduate Innovation Base, Hunan University, Changsha Hunan 410082, China;
3.Hunan Province Key Laboratory of Network and Information Security, Hunan University, Changsha Hunan 410082, China

Abstract: Based on the analysis of Keccak algorithm, concerning the situation that the existing hardware implementations of Keccak algorithm lack of flexibility and could only support one version, this paper proposed a new reconfigurable Keccak hardware implementation, which could support four versions algorithms. The proposed design achieved 214MHz clock frequency using 1607slices when being ported to Xilinx Virtex-5 FPGA platform. The experimental results show that the proposed design has the advantages of high throughput (9131Mbps), good flexibility and supporting four versions.

Keywords: Keccak algorithm sponge structure Hash algorithm reconfigurability Field-Programmable Gate Array (FPGA)

**收稿日期** 2011-08-11 **修回日期** 2011-11-10 **网络版发布日期** 2012-03-01

DOI: 10.3724/SP.J.1087.2012.00864

**基金项目**:

国家自然科学基金资助项目(60873074,60673061);长沙市科技计划项目(K1003028-11)。

**通讯作者**: 王奕

**作者简介**: 吴武飞(1986-),男,江西安义人,硕士研究生,CCF会员,主要研究方向:嵌入式系统;王奕(1977-),女,河南洛阳人,讲师,博士,CCF会员,主要研究方向:功耗攻击以及防御、嵌入式安全;李仁发(1957-),男,湖南宜章人,教授,博士,CCF会员,主要研究方向:嵌入式计算、无线传感网络、CPS。
**作者**Email: estelle.ywang@gmail.com

**参考文献:**

[1]National Institute of Standards and Technology. FIPS 180-1, Secure Hash standard [S]. Virginia: FIPS, 1993.

[2]WANG X, YU H, YIN Y L. Efficient collision search attacks on SHA-0[C]// Proceedings of CRYPTO 2005, LNCS 3621. Berlin: Springer-Verlag, 2005: 1-16.

[3]WANG X, YIN Y L, YU H. Finding collisions in the full SHA-1[C]// Proceedings of CRYPTO 2005, LNCS 3621. Berlin: Springer-Verlag, 2005:17-36.

[4]WANG X, YU H. How to break MD5 and other Hash functions[C]// Proceedings of EUROCRYPT 2005, LNCS 3494. Berlin: Springer-Verlag, 2005:19-35.

[5]BERTONI G, DAEMEN J, PEETERS M, et al. Keccak specifications [EB/OL]. [2010-05-20]. http://keccak.noekeon.org/Keccak-specifications.pdf.

[6]李长可. 基于FPGA可重构快速密码芯片设计[J]. 计算机测量与控制,2011,19(7):1665-1667.

[7]杨宏志,韩文报,董博. 类AES分组密码统一框架及其FPGA实现[J]. 计算机科学,2010,37(4):103-105.

[8]BALDWIN B, HANLEY N, HAMILTON M, et al. FPGA implementations of the round two SHA-3 candidates[EB/OL]. [2010-05-20]. http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/Aug2010/documents/papers/BALDWIN_FPGA_SHA3.pdf.

[9]MATSUO S, KNEZEVIC M, SCHAUMONT P, et al. How can we conduct "fair and consistent" hard-ware evaluation for SHA3 candidate [EB/OL]. [2010-05-20]. http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/.

[10]STR MBERGSON J. Implementation of the Keccak Hash function in FPGA devices[EB/OL]. [2010-05-20]. http://www.stromb ergson.com/kryptoblog/2008/12/17/implementation-av-keccak-i-fpga-teknologi/.

[11]HOMSIRIKAMOL E, ROGAWSKI M, GAJ K. Comparing hardware performance of fourteen round two SHA-3 candidates using FPGAs[EB/OL]. [2010-05-20]. http://eprint.iacr.org/2010/445.pdf.

[12]BERTONI G, DAEMEN J, PEETERS M, et al. Keccak implementation overview [EB/OL]. [2010-05-20]. http://keccak.noekeon.org/Keccak-implementation-3.0.pdf.

[13]BERTONI G, DAEMEN J, PEETERS M, et al. Sponge functions [EB/OL]. [2010-05-20]. http://sponge.noekeon.org/SpongeFunctions.pdf.

[14]BERTONI G, DAEMEN J, PEETERS M, et al. Keccak sponge function family main document [EB/OL]. [2010-05-20]. http://keccak.noekeon.org/Keccak-main-2.1.pdf.

[15]BERTONI G, DAEMEN J, PEETERS M, et al. The Keccak reference version 3.0[EB/OL]. [2010-05-20]. http://keccak.noekeon.org/Keccak-reference-3.0.pdf.

**本刊中的类似文章**

1．董继光 陈卫卫 田浪军 吴海佳.大规模云存储系统副本布局研究[J]. 计算机应用, 2012,32(03): 620-624

2．陈乃金.基于深度优先贪婪搜索的可重构硬件任务划分算法[J]. 计算机应用, 2012,32(01): 158-162

3．宋庆增 顾军华.共轭梯度求解器的FPGA设计与实现[J]. 计算机应用, 2011,31(09): 2571-2573

4．蔡富强 郭兵 沈艳 王继禾 伍元胜.基于放置代价的可重构系统任务统一调度算法[J]. 计算机应用, 2010,30(11): 2870-2872

5．刘陶刚 赵荣彩 姚远 瞿进.分块存储的滑动窗口数据重用技术[J]. 计算机应用, 2010,30(05): 1371-1375

6．王景中 杜飞.矩阵型布鲁姆过滤器在病毒过滤防火墙中的研究[J]. 计算机应用, 2009,29(11): 2939-2941

7．赵欢 苏小昆 李仁发.一种低功耗动态可重构cache方案[J]. 计算机应用, 2009,29(05): 1446-1451

8．蔡启先 蔡洪波 黄晓璐 蔡启仲 .基于FPGA的动态可重构体系结构研究[J]. 计算机应用, 2006,26(7): 1741-1743

9．王伟; 李仁发; 吴强.动态可重构环境下循环计算的位宽优化[J]. 计算机应用, 2006,26(5): 1237-1240

10．张慧翔; 张新家.一种业务逻辑可重构的三层应用服务器设计与实现[J]. 计算机应用, 2006,26(4): 853-856