学号： 131199

**东 南 大 学**

**学术型研究生学位论文开题报告**

|  |  |
| --- | --- |
| 院（系、所） | 电子科学与工程学院 |
| 学科（专 业） | 微电子学与固体物理学 |
| 研究生姓名 | 李小泉 |
| 学科门类与学位级别 | 工学硕士 |
| 导师姓名 | 孙伟锋 |
| 入学年月 | 2013年9月 |
| 开题报告日期 | 2015年11月11日 |

填 表 须 知

1. 论文开题报告由研究生本人向审议小组报告并听取意见后，由研究生本人填写此表。
2. 论文开题报告填写完成后，必须经导师审批，通过后方能提交。

3、博士生应在第四学期内、硕士生应在第三学期内完成此开题报告。开题报告经研究生秘书在网上审核确认（硕士生至少半年、博士生至少一年）后方可申请答辩。

4、研究生开题前应填写查新报告。查新报告对理、工、医、管等学科博士生作为必要环节。博士生查新工作可委托图书馆负责，也可在完成网络文献检索类研究生课程的学习或参加学校组织的网络文献检索培训后，自行组织查新检索，自行组织查新需要详细文献查新述评作为附件。自行查新报告须经导师审查后由开题报告审核专家组审核签字（或盖章）。硕士生和文科博士生开题查新参考上述办法，不作硬性要求。

5、本表一式两份，一份研究生自留放入本人“研究生档案材料袋”；一份由院（系、所）保存并归入院（系、所）研究生教学档案。

6、学科门类与学位级别指的是工学（或理学等）博士、硕士。

7、本表下载区：[http://seugs.seu.edu.cn/s/97/t/1707/aa/b8/info43704.htm](http://seugs.seu.edu.cn/s/97/t/1707/aa/b8/info43704.htm%20)  。本表电子文档打印时用A4纸张，格式不变，内容较多可以加页。

一、学位论文开题报告

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 论 文 题 目 | 面向分组加密算法的可重构阵列PE研究与设计 | | | | | | | | |
| 研 究  方 向 | 可重构阵列PE | | | | | | | | |
| 题 目 来 源 | 国家 | 部委 | 省 | 市 | 厂、矿 | 自选 | 有无合同 | 经费数 | 备注 |
|  |  |  |  |  | √ | 无 |  |  |
| 题 目  类 型 | 基础  研究 | 应用  研究 | 综合研究 | 其它 |  | | | | |
|  |  | √ |  |  | | | | |
| 论文开题前上网检索情况（硕士生可不作要求；理、工、医、管学科博士生应填写并附查新报告） |  | | | | | | | | |
| 开题报告内容  （包括：立题依据及价值、研究内容及方法、可行性分析、预期的成果、预计的困难及解决办法）   1. **立题依据及价值** 2. **课题背景**   随着计算机技术和通信技术的发展，信息安全问题逐渐成为人们关注的社会问题，密码技术是保证信息的机密性、安全性和可用性等安全要求的基本手段。密码算法是现代安全应用的基础，也是信息系统安全性的根本所在，实现高效灵活的密码算法是高性能信息系统的重要指标和根本保障，因此也成为信息安全领域的重要课题。  密码算法应用常常需要处理较大的信息量，或具有较大的计算强度，通用处理器常常不能满足其速度要求，安全性也不如专用硬件，因此国内外对密码处理专用硬件的研究和开发十分活跃。密码算法的主要硬件加速方式可分为三类：特定密码算法ASIC、密码算法处理器和可重构密码处理结构。  随着移动互联网的飞速发展，对系统安全性的要求也越来越迫切，保障系统安全所需投入的处理资源将越来越多，安全应用的范围也会越来越广，密码算法与可重构技术的结合，可以满足性能和安全方面的需求，具体地，可重构密码系统架构在这一应用领域的优势体现在以下几点[1]：  （1）可重构系统的计算能力能够满足密码算法的性能需求，结构能够根据特定的密钥定制硬件，使算法执行更加高效；  （2）可重构系统可以根据实际需求改变硬件实现的算法，使同一硬件能够高效地支持种类繁多的算法，具有很大的灵活性；  （3）可重构系统具有扩展性，能够适应不断被提出新的更安全的算法，同时支持随时修改密钥，满足某些特殊情况下的白片需求。   1. **国内外研究现状** 2. **研究内容及方法** 3. **研究基础**   课题的研究基础主要来自学术上发表的关于低功耗互连的论文，商业上的文档中会对各自的FPGA的互连架构有一个总体的描述，缺乏对具体细节的描述；课题开始时对大量的低功耗互连方案做了总结和归类。    **图1 FPGA互连结构**  从FPGA的结构图中可以看出FPGA互连架构中所包含的三个主要部件：连线、开关盒、连接盒。大部分的论文都是讨论这三个部件的具体参数对FPGA的功耗的影响，从而获得功耗最优的互连架构参数。   * 连线   FPGA的连线负责将不同的逻辑块连接到一起。连线的长度、比例、分布都是互连架构中的主要参数。  短线：更高的灵活性，更低的能量消耗，  长线：灵活性低，更高的能量消耗    **图2 FPGA中的连线分布**  但如果用短线组成长线，那么开销会变大，因为需要开关盒去连接这些短线，如果长线作为短线使用则浪费了一部分长度没有被使用[21]  连线的长度、比例的确定：  依据：延迟、面积、功耗   * 长度为4的连线能获得最好的延时和面积效益[21][22] * 长度为4和8的组合能达到最好的连延时和面积效益[21][22] * 长度为3的连线下FPGA的功耗延迟积最低[23] * 开关盒   C:\Users\Bean\AppData\Local\YNote\Data\605972145@qq.com\cb312feaadd342efa0b1cace95761a95\clipboard.png 开关盒主要负责将不同方向的连线连接到一起，或者是将短线连接成长线使用，对于互连架构，可以探索的方向是开关盒的种类，开关盒中连线的种类，开关盒的连通系数Fs以及开关盒和连线的搭配问题。   * 开关盒的种类   不同的开关盒在连通性、面积、功耗上的差别[25] **图3 不同种类开关盒的拓扑结构**   * 开关盒里的连线的性质   双向和单向连线[24]   * 开关盒的连通系数Fs   主要是连通性与面积与功耗之间的权衡   * 不同开关盒配对不同的连线的效果   **图4. 开关盒中单向和双向连线**   * 连接盒   CLB、IP等模块与连线的连通接口，复杂性主要体现在两个参数Fcin和Fcout上。  Fcin与Fcout定义如下：  Fc定义了模块与互连的连通性，根据连通度需求在0~1之间权衡选值。文献[34]指出设置  Fcin为0.8，Fcout为0.3最有利于低功耗设计。   * 工具链   学术上FPGA架构探索都在多伦多大学的开源工具链VPR(versatile place and route)上进行，它提供了一个完整的编译工具链，从电路设计到最后布线结束的二进制流文件，工具链还集成了用于时序、面积、功耗分析的工具。VPR程序能够根据用户的输入参数，自动生成相应的逻辑和互连结构，从而非常方便结构研究人员对不同结构做出比较。当提出新的架构超出VPR本身支持的范围以外时，只需要对工具链做适应性修改。   1. **研究内容**   本课从现有的研究论文出发，根据合理的连通性划分，分别探索在不同连通性需求下的最佳结构确定。  合理的连通性区域划分[12][13][14]  连通性区域划分合理的，开关盒和连线优化组合的FPGA互连架构  连线组合[8][21][22][23]  开关盒组合[9][11][24][25]  **图5 研究内容**  性能区域划分   * 不同的区域被使用的概率不同 * 当设计足够大，所有的资源都被利用上以后，不同的区域的连通性需求也不相同   当明确每一个区域的连通性以后，从功耗的角度出发选择合适的设计参数   * 互连线长度、比例 * 开关盒的种类、单双向性、Fs * 开关盒和连线的搭配 * 连接盒的Fc参数确定      1. **设计方案**  * 总体方案   先从大量的测试集的统计结果来获得一般电路在FPGA上实现后的统计的连通性需求分布，然后通过对不同区域的互连架构参数进行探索，找到这些参数针对低功耗的最优值；在VPR原始版本的基础上对其进行新架构的适应性修改，在修改后的VPR上对新的互连架构进行验证。  **图6 总体方案**   * 连通性区域划分   连通性分析的输入是电路布局布线后的结果，通过对不同区域的连线、开关等的使用情况建立一套评判标准来定义不同区域的连通因子。将连通因子在某一个范围的区域划分成一个区域，整个FPGA被划分成不同连通性区域的拓扑架构。  [Routing Close-up]  C:\Users\Bean\AppData\Local\YNote\Data\605972145@qq.com\55b4f2610e6340c7b0ddb78aec172c97\clipboard.png  **图7 从布线结果中提取连通因子**   * 互连架构生成   不同连通性区域的互连架构参数探索  高连通性：短连线，较大的Fs和Fc参数，使用复杂的开关盒（welton)，沟道宽度（W）大，双向的开关盒连线（合理选择，如何在保证连通性的情况下尽可能地降低功耗）  低连通性：更多的长线，较小的Fs和Fc参数，使用简单的的开关盒（Disjoint)，单向的开关盒连线，较小的沟道宽度  互连架构参数的确定从理论出发，但是最终的确定还是要将整个架构生成以后放到编译工具链中验证后才能确定。   * CAD工具流设计   选择在学术上被大量采用的VPR工具作为工具平台，这是多伦多大学维护的一个开源的编译工具链，课题会在VPR原始版本的基础上对其进行新架构的适应性修改。   * 异构互连的FPGA架构在VPR工具链中生成 * 布局布线对新架构的支持 * 针对新架构的面积、延时、功耗、分析。   **图8 编译工具链修改**   * 架构验证   目标架构：采用VTR7.0套件里的Stratix IV FPGA架构，由于某些架构信息的缺失，所以只能称之为近似架构。商业架构非常复杂，比较完整（去除加密部分）的架构描述对应的xml文件有十几万行，但是其中大多都是与互连无关的IP，因此在做探索时会去掉无关的IP，保留Stratix IV 原有的互连结构。  测试集选择：选择在学术界被广泛采用的MCNC测试集。  **图9 测试框架**   1. **可行性分析**   本课题以学术上的论文为基础，选取合理的连通性划分方式，从已有的论文出发确定每一个区域中各个架构参数，将论文中互连架构低功耗探索的结论应用到不同的连通性区域，并对其进行验证。目前学术上已经有许多论文在这些方面做出了探索，并得出了许多可用的结。  课题选择在学术上被大量采用的VPR工具作为工具平台，这是多伦多大学维护的一个开源的编译工具链，课题会在VPR原始版本的基础上对其进行新架构的适应性修改；由于VPR的良好的可扩展性，因此这种方式是学术上对FPGA的架构探索所采用的普遍模式。   1. **预期的成果**  * 连通性区域划分合理的，开关盒和连线优化组合的FPGA互连架构，并且该架构在延迟和功耗的优化结果上要优于对比论文。 * 支持异构互连探索的编译工具链，该工具链要保证整个架构的验证和对比。 * 发表一篇高水平论文  1. **预计的困难及解决办法**  * 连通性区域划分的依据获取   从大量的测试集的统计结果来获得一般电路在FPGA上实现后的统计的连通性需求分布。对于具体的连通性情况要对每一个电路的布线结果作分析，统计不同区域的连通性情况，并用图表的形式把它描述出来。   * 不同连通性区域架构参数的确定   对于不同的连通性区域的架构参数，前人的论文研究可以作为确定的基础，从这些基础出发可以获取某些连通性区域参数的一个指导值，然后通过对这些参数进行验证探索，找到这些参数的最优值。当所有区域的架构参数都被低功耗优化以后整个架构在理论上就确定了。   * 异构互连的FPGA架构在VPR工具链中生成   对于异构互连的架构探索，很大一部分努力是对现有的基础工具链的扩展。VPR的架构生成是参数化的，这为我们定义自己的架构停供了方便，但同时也意味着无法对架构更改太多，许多架构特性都是被确定了的，一旦新的架构超出这个范围，那么原来的参数生成架构的方法就不一定能适用，或者新的架构与原来的一套方法会存在许多的冲突。对于异构互连，这些冲突是显而易见的，因此如何在参数生成架构的模式下生成异构互连架构是一个很大的困难，而目前并没有一个好的方案来解决这个问题。   1. **参考文献**   [1]王莉．密码算法的可重构系统实现研究[D]：[博士学位论文]．湖南：国防科学技术大学，2004  [2] C. Chen, S. Mitra, H.-S. P. Wong, R. T. Howe, J. Watt, D. Lewis,J. Provine, K. Akarvardar, S. Chong, N. Patil, and R. Parsa, “Efficient FPGAs using nanoelectromechanical relays,” in Proc. 18th Annu. Int.Symp. Field Program. Gate Arrays, 2010, pp. 273–282  [3] S. Tanachutiwat, M. Liu, and W. Wang, “FPGA based on integration of CMOS and RRAM,” IEEE Trans. Very Large Scale Integr. (VLSI) Syst.,vol. 19, no. 11, pp. 2023–2032, Nov. 2011.  [4] E. Ahmed and J. Rose, “The effect of LUT and clustersize on deep-submicron FPGA performance and density,” IEEE Trans. VLSI Syst., vol. 12, no. 3, pp. 288–298, Mar. 2004.  [5] C. Dong, C. Deming, S. Haruehanroengra, and W. Wang, “3-D nFPGA: A reconﬁgurable architecture for 3-D CMOS/nanomaterial hybrid digital circuits,” IEEE Trans. Circuits Syst. I, Regular Papers, vol. 54, no. 11, pp. 2489–2501, Nov. 2007.  [6] F. Li, Y. Lin, L. He, D. Chen, and J. Cong, “Power modeling and characteristics of ﬁeld programmable gate arrays,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 24, no. 11,pp. 1712–1724, Nov. 2005.  [7] F. Li, Y. Lin, L. He, D. Chen, and J. Cong, “Power modeling and characteristics of ﬁeld programmable gate arrays,” IEEE Trans.Comput.-Aided Design Integr. Circuits Syst., vol. 24, no. 11,pp. 1712–1724, Nov. 2005.  [8] Lin, Mingjie, and Abbas El Gamal. "A low-power field-programmable gate array routing fabric." Very Large Scale Integration (VLSI) Systems, IEEE Transactions on 17.10 (2009): 1481-1494.  [9] Sivaswamy, Satish, et al. "HARP: hard-wired routing pattern FPGAs."Proceedings of the 2005 ACM/SIGDA 13th international symposium on Field-programmable gate arrays. ACM, 2005. [10] SHAO, Hai-bo, Ke-jie MA, and Ling-li WANG. "Low Power Interconnects Design for General Switch Box Based FPGA." Journal of Fudan University (Natural Science) 1 (2012): 011.  [11] Rahman, Arifur, et al. "Heterogeneous routing architecture for low-power FPGA fabric." Custom Integrated Circuits Conference, 2005. Proceedings of the IEEE 2005. IEEE, 2005.  [12] Siozios, Kostas, Dimitrios Soudris, and Antonios Thanailakis. "A Software-Supported Methodology for Designing General-Purpose Interconnection Networks for Reconfigurable Architectures." International Journal of Computer Systems Science & Engineering 4.3 (2008).  [13] Siozios, Kostas, and Dimitrios Soudris. "Wire segment length and switch box co-optimization for FPGA architectures." Field Programmable Logic and Applications, 2006. FPL'06. International Conference on. IEEE, 2006.  [14] Siozios, Kostas, et al. "Designing heterogeneous FPGAs with multiple SBs."Reconfigurable Computing: Architectures, Tools and Applications. Springer Berlin Heidelberg, 2007. 91-96.  [15] Von Herzen B. Interconnect array formed at least in part with repeated application of an interconnect pattern: U.S. Patent 7,501,341[P]. 2009-3-10.  [16] Wu P Y, Wheeler R L. Interconnect pattern for semiconductor packaging: U.S. Patent 8,743,559[P]. 2014-6-3.  [17] Das S, Kao S W, Rahman A, et al. Structures and methods for heterogeneous low power programmable logic device: U.S. Patent 7,477,073[P]. 2009-1-13.  [18] Anderson J B, Cline R L, Lakka S, et al. Integrated circuit with a selectable interconnect circuit for low power or high performance operation: U.S. Patent 7,893,712[P]. 2011-2-22.  [19] New B J. FPGA architecture with mixed interconnect resources optimized for fast and low-power routing and methods of utilizing the same: U.S. Patent 6,930,510[P]. 2005-8-16.  [20] Shi H, Xie Y. Method of optimizing interconnect distribution to improve signal integrity: U.S. Patent 7,472,367[P]. 2008-12-30.  [21] Lin, Mingjie, and Abbas El Gamal. "TORCH: A design tool for routing channel segmentation in FPGAs." Proceedings of the 16th international ACM/SIGDA symposium on Field programmable gate arrays. ACM, 2008.  [22] V. Betz and J. Rose, \FPGA routing architecture:segmentation and buering to optimize speed and density," in Proceedings of the 1999 ACM/SIGDA Seventh International Symposium on Field-Programmable Gate Arrays, pp. 59 { 68, 1999.  [23] R. Tu and B.-X. Shao, \Energy/performance/area trade os in nanometer FPGA segmented routing architecture," in Solid-State and Integrated Circuit Technology, 2006. ICSICT '06. 8th International Conference on, pp. 1954-956, 2006.  [24] Lemieux G, Lee E, Tom M, Yu A (2004) Directional and single-driver wires in fpga interconnect. In Proceedings of the international conference on ﬁeld-programmable technology, pp41–48  [25] BETZ,V., ROSE,J., AND MARQUARDT ,A. 1999. Architecture and CAD For Deep-Submicron FPGAs.Kluwer Academic Publishers, Norwell, MA.  [26] Shang, Li, Alireza S. Kaviani, and Kusuma Bathala. "Dynamic power consumption in Virtex™-II FPGA family." Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays. ACM, 2002.  [27] Mondal, Somsubhra, and Seda Ogrenci Memik. "A low power FPGA routing architecture." Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on. IEEE, 2005.  [28] CE, L. I.; YIPING, D. O. N. G.; WATANABE, Takahiro. Low power placement and routing for the coarse-grained power gating FPGA architecture. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2011, 94.12: 2519-2527.  [29] GAYASEN, Aman, et al. Reducing leakage energy in FPGAs using region-constrained placement. In: Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays. ACM, 2004. p. 51-58.  [30] Gayasen, Aman, et al. "A Dual-V dd Low Power FPGA Architecture." Field Programmable Logic and Application. Springer Berlin Heidelberg, 2004. 145-157.  [31] Rahman, Arifur, et al. "Heterogeneous routing architecture for low-power FPGA fabric." Custom Integrated Circuits Conference, 2005. Proceedings of the IEEE 2005. IEEE, 2005.  [32] George, Varghese, Hui Zhang, and Jan Rabaey. "The design of a low energy FPGA." Proceedings of the 1999 international symposium on Low power electronics and design. ACM, 1999.  [33] Betz, Vaughn, and Jonathan Rose. "VPR: A new packing, placement and routing tool for FPGA research." Field-Programmable Logic and Applications. Springer Berlin Heidelberg, 1997.  [34]徐新民; 尚丽娜; 严晓浪. FPGA 的布线结构参数 Fc 对其功耗的影响. 高技术通讯, 2006, 15.10: 16-20.  研究生签名：  年 月 日 | | | | | | | | | |

二、学位论文工作实施进度与安排

|  |  |  |
| --- | --- | --- |
| 起讫  日期 | 工 作 内 容 和 要 求 | 备 注 |
| 2014.12 | 熟悉VTR工具流，运行一组benchmark |  |
| 2015.1~2015.2 | 编写布线结果的profiler工具 |  |
| 2015．3~2015. 4 | 编写异构扩展的布局布线工具 |  |
| 2015.5~2015.7 | 建立异构扩展的面积、延迟、功耗模型 |  |
| 2015.8~2015.9 | 编写架构生成工具，专利撰写 |  |
| 2015.10~2015.12 | 在完成的工具链上进行互连架构探索，高水平论文撰写 |  |
| 2016.1~2016.3 | 毕业论文撰写及答辩 |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| 指  导  教  师  对  开  题  报  告  的  综  合  意  见 | 指导教师（签名）  年 月 日 |  |
| 开  题  报  告  审  议  情  况  记  录 | １、审议小组成员（一般3-5人）：  组长：杨军  成员：曹鹏 刘新宁 戚隆宁 单伟伟  ２、审议小组意见记录  ３、投票表决结果  审议小组出席 人；通过 人；不通过 人。  开题报告质量 （优、良、中、通过）  ４、审议小组组长（签名）  审议小组成员（签名）  年 月 日 |  |
| 院（系、所）意见：  院（系、所）负责人签名（或印章）  年 月 日 | |  |
| 备注： | |  |