# 最新开题报告内容格式汇总

来源：网络 作者：尘埃落定 更新时间：2021-02-25

*报告是指向上级机关汇报本单位、本部门、本地区工作情况、做法、经验以及问题的报告，那么什么样的报告才是有效的呢？下面是小编为大家整理的报告范文，仅供参考，大家一起来看看吧。1.开题报告方法介绍：开题报告是指开题者对科研课题的一种文字说明材料。...*

报告是指向上级机关汇报本单位、本部门、本地区工作情况、做法、经验以及问题的报告，那么什么样的报告才是有效的呢？下面是小编为大家整理的报告范文，仅供参考，大家一起来看看吧。

1.开题报告方法介绍：

开题报告是指开题者对科研课题的一种文字说明材料。这是一种新的应用写作文体，这种文字体裁是随着现代科学研究活动计划性的增强和科研选题程序化管理的需要应运而生的。开题报告一般为表格式，它把要报告的每一项内容转换成相应的栏目，既便于开题报告按目填写，避免遗漏；又便于评审者一目了然，把握要点。

2.开题报告的基本内容及其顺序：

一.开题报告封面：

论文题目、系别、专业、年级、姓名、导师。

二.论文的背景、目的和意义

目的要明确，充分阐明该课题的重要性：

1.论文的背景；

2.理论意义；

3.现实意义

三.国内外研究概况

应结合毕业设计题目，与参考文献相联系，是参考文献的概括：

1.理论的渊源及演进过程；

2.国内有关研究的综述；

3.国外有关研究的综述

四.论文的理论依据、研究方法、研究内容

（思想明确、清晰，方法正确、到位，应结合所要研究内容，有针对性）

五.研究条件和可能存在的问题

六.预期的结果

七.论文拟撰写的主要内容（论文提纲）

八.论文工作进度安排

（内容要丰富，不要写得太简单，要充实，按每周填写，可2-3周，但至少很5个

时间段，任务要具体，能充分反映研究内容）

九.参考文献

下面是开题报告模板：

xxxxx大学毕业设计（论文）开题报告

课题名称：

学生姓名：

学号：

指导教师：

职称：所在学院：专业名称：

开题报告范例

题目：AES（高级数据加密标准）加解密电路的设计

学号

姓名

指导教师

院（系）专业

华中科技大学教务处制

i

选题报告要求

一.课题的来源、目的、意义。国内外基本研究情况。

二.预计达到的目标、关键理论和技术、技术指标、完成课题的方案和主要措施。

三.课题研究进展计划。

四.主要参考文献。

五.指导教师评语，教研室（系.所）审查意见。

ii

一．课题的来源.目的.意义。国内外基本研究情况。

1.1课题的来源.目的.意义。

AES简介：

1977年1月数据加密标准DES（DataEncryptionStandard）正式向社会公布，它是世界上第一个公认的实用分组密码算法标准。但DES在经过20年的实践应用后，现在已被认为是不可靠的。1997年1月2日美国国家标准和技术研究所（NIST）发布了高级加密标准（AES-FIPS）的研发计划，并于同年9月12日正式发布了征集候选算法公告“‘，NIST希望确定一种保护敏感信息的公开.免费并且全球通用的算法作为AES，以代替DES。在征集公告中，NIST对算法的基本要求是：算法必须是私钥体制的分组密码，支持128位分组长度和129，192，256bits密钥长度。经过三轮遴选，Rijndael最终胜出。2001年11月26日联邦信息处理标准出版社发布了正式的AES标准即FIPSPUBS197，其中制定的标准生效时间为2002年5月26日。Rijndael算法是一种可变分组长度和密钥长度的迭代型分组密码，它的分组长度和密钥长度均可独立地指定为128bits，192bits，256bits，它以其安全性和多方面的优良性能，成为AES的最佳选择。Rijndael算法能抵抗现在的所有己知密码攻击，它在广泛的计算环境中的硬件和软件实现性能都表现得非常优秀，它的密钥建立时间极短且灵活性强，它极低的内存要求使其非常适合在存储器受限的环境中使用，并且表现出很好的性能。

课题来源：

本课题来源于国家863高技术研究发展计划“低成本，低功耗，高安全性无线传感器网络节点芯片设计”（2006AA01Z226）

湖北省自然科学基金资助项目“微传感器系统SOC集成技术研究”（2006ABA080）

华中科技大学校基金重点资助项目“信息安全片上系统（SOC）的防护机制研究”（2006Z011B）；

课题目的：

随着计算机应用范围的不断扩大，特别是在Internet高速发展的今天，如何保障计算机用户通过网络所传递的数据的私密性，如何保障涉密信息能够安全的利用计算机来进行处理等计算机和网络应用中信息安全的问题日益引起人们的关注。随着Internet的不断发展，基于Internet的应用的领域和深度与日俱增，电子商务，电子政务等与人们日常生活和工作息息相关的Internet应用也正越来越为人们所接受。当人们在享受这些应用带来的高效和便捷的同时，也时刻面临着各式各样的信息安全问题，而这些问题也正成为当前影响Internet应用继续发iii

展的瓶颈。利用数据加密算法，尤其是新的高级数据加密标准AES，对数据进行加密来保障信息传输与存储的安全性已经被证明是行之有效的。因而，研究数据加密算法的实现与加解密电路的设计对于解决Internet应用中的各项安全问题就有着很重要的作用。

本课题的目的旨在通过仔细研究和分析高级加密标准AES，在此基础上对AES算法的ASIC结构进行优化，设计出密码芯片。同时在设计中学习大规模集成电路的设计方法和设计流程，一些仿真，综合软件的应用，VHDL语言的编写，为以后的工作和进一步学习打下坚实的基础。

课题意义：

随着Internet的快速发展，基于Internet的各种应用也日益增长。但是，由于Internet是一个极度开放的环境，任何人都可以在任何时间.任何地点接入Internet获取所需的信息，这也使得在Internet上信息传输及存储的安全问题成为影响Internet应用发展的重要因素。信息安全技术也就成为了人们研究

Internet应用的新热点。信息安全的研究包括密码理论与技术.安全协议与技术.安全体系结构理论.信息对抗理论与技术.网络安全与安全产品等领域，其中密码算法的理论与实现研究是信息安全研究的基础。而确保数据加密算法实现的可靠性和安全性对于算法理论应用到各种安全产品中起到了至关重要的作用。AES产品取代DES产品己是必然。对AES的实现和应用进行探讨和研究就具有较大的理论和现实意义。

1.2国内外基本研究情况

目前AES算法的理论研究主要集中在设计原理.安全性能分析和统计性能分析上。

对于设计原理，主要研究算法设计遵循的原则和整体结构。AES算法所遵循的是安全性和实现性原则，在整体结构上采用的是SP网络结构。对于安全性能，主要研究AES算法抵抗现有已知密码攻击的能力。当前主要攻击手段有：强力攻击.差分密码分析，线性密码分析，Square攻击和插值攻击等。目前密码分析又有了新的进展，积分分析.功耗分析和代数攻击成为新的研究方向。对于统计性能，主要研究算法随机化数据的能力，目前国内外研究都比较少。

AES密码算法通常用软件或硬件实现。软件实现易受使用条件限制，而且易受到破坏，影响数据传输质量。硬件实现是用专用芯片实现密码算法，通过芯片对数据进行加密。密码专用芯片是实现信息安全与保密的基础核心产品，具有高保密性，高加密速率，高可靠性，体积小，重量轻，易于实现复杂功能，易于嵌入，总体成本低等优点，因此AES密码芯片在无线通信和Internet应用有着广耗。

2.3技术指标

要使最后设计的加密电路面积尽量小，速度尽量快，另外，也要满足高吞吐量的要求。

2.4完成课题的方案和主要措施

本课题中要实现基于AES的硬件结构的设计与仿真，预备以以下方案步骤实施：

1.S盒子的设计与仿真。

2.列混合变换和密钥加法的组合模快的设计与仿真。

3.轮密钥的产生模块的设计与仿真。

4.对整体AES芯片的逻辑综合物理设计仿真与分析。

主要措施：

1.对于SubBytes和InvSubBytes的设计，复用加解密中不同的两个S-BOX的求逆模块，以实现加解密时的字节替换功能。在轮结构中集成四块字节替换模块，实现一个字的替换。

2.对于AddRoundkey和InvMixColumns的设计，在常规轮中把加解密时的密钥加与列混合变换集成在同一模块，通过加解密信号的选择实现了加解密的功能，这样就可以消除加解密硬件结构的差异，同时也简化了解密时轮密钥处理的复杂性。

3.采用流水线结构，数据加解密是本设计的主要模块，为了提高其数据吞吐速率，采用流水线结构，可以大大的提高芯片的吞吐量。

4.采用门控时钟技术，密钥生成与加解密操作分时进行，降低芯片的功耗，增加了稳定性。

三.课题研究进展计划。

3月5日——3月17日：查找资料；

3月18日——3月31日：翻译英文文献；

4月1日——5月19日：毕业设计主要工作；

5月20日——6月8日：撰写论文；

6月13日：答辩。

四．参考文献

[1]Daemen J,Rijmen V.谷大武,徐胜波译.高级加密标准(AES)算法Rijndael的设计[M].北京:清华大学出版社,2003.

[2]任艳颖,王彬编著.IC设计基础.西安:西安电子科技大学出版社,2003.

[3]WolkerstorferJ.,Oswald E.,Lamberger M.:An ASIC Implementation of the AES S-boxes[C]// C Boyd ed.ASIACRYPT 2001. Heidelberg Berlin: Springer-Verlag,2001:239-254.

[4]P Chodowiec,K Gaj.Very Compact FPGA Implementation of the AES Algorithm [C]//C D Walter et al. Hardware and Embedded Systems (CHES 2003).Berlin Heidelberg: Springer-Verlag, 2003:319–333.

本文档由范文网【dddot.com】收集整理，更多优质范文文档请移步dddot.com站内查找