华南理工大学

South China University of Technology

工程硕士学位论文

基于 AES 与 ECC 的游戏数据混合加密研究与实现

作 者 姓 名	黎俊男
工 程 领 域	软件工程
校内指导教师	应伟勤 副教授
校外指导教师	韩超 高级工程师
所 在 学 院	软件学院
论文提交日期	2018.11.21

Research and aggregate of game data mixed encryption based on AES and ECC

A Dissertation Submitted for the Degree of Master

Candidate：Li Junnan

Supervisor：Prof. Ying Weiqin

Senior Engineer Han Chao

South China University of Technology

Guangzhou, China

分类号： TP3 **学校代号：10561**

学 号： 201320702036

华南理工大学硕士学位论文

基于AES与ECC的游戏数据混合加密研究与实现

作者姓名：黎俊男 指导教师姓名、职称：应伟勤 副教授；韩超高级工程师

申请学位级别： 工程硕士 工程领域名称：软件工程

论文形式：☐产品研发 ☐工程设计 ☑应用研究 ☐工程/项目管理 ☐调研报告

研究方向：软件技术开发

论文提交日期：2018 年 11 月 21 日 论文答辩日期：2018 年 11 月 26 日

学位授予单位：华南理工大学 学位授予日期： 年 月 日

答辩委员会成员：

主席：刘琼

委员：应伟勤、杨磊、彭绍武、杨敬锋

华南理工大学
学位论文原创性声明

本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包含任何其他个人或集体已经发表或撰写的成果作品。对本文的研究做出重要贡献的个人和集体，均已在文中以明确方式标明。本人完全意识到本声明的法律后果由本人承担。

作者签名：黎俊勇　　日期：2018年11月21日

学位论文版权使用授权书

本学位论文作者完全了解学校有关保留、使用学位论文的规定，即：研究生在校攻读学位期间论文工作的知识产权单位属华南理工大学。学校有权保存并向国家有关部门或机构送交论文的复印件和电子版，允许学位论文被查阅（除在保密期内的保密论文外）；学校可以公布学位论文的全部或部分内容，可以允许采用影印、缩印或其它复制手段保存、汇编学位论文。本人电子文档的内容和纸质论文的内容相一致。

本学位论文属于：

□保密，在_____年解密后适用本授权书。

☑不保密，同意在校园网上发布，供校内师生和与学校有共享协议的单位浏览；同意将本人学位论文提交中国学术期刊(光盘版)电子杂志社全文出版和编入 CNKI《中国知识资源总库》，传播学位论文的全部或部分内容。

（请在以上相应方框内打“ √ ”）

作者签名：黎俊勇　　日期：2018.11.21

指导教师签名：庄伟勤　　日期：2018.11.21

摘　要

网络信息化的快速发展造就了网络游戏的产生，传统游戏开始向网络游戏转型。网络游戏能够打破时间和空间的限制，将来自世界各地的不同人群共同组合在一起，构建了一个虚拟世界，正是基于此 internet 连接着世界各地玩家，随着发展，网游开始进军移动端。当前网络游戏主要是将 PC 端与手机端进行结合，通过 internet 将网络游戏内部虚拟的资料、货币等信息传输到客户端中，这就可能关系到游戏数据信息的保密性和防护性的问题。由于是当前网络游戏行业内部并未形成统一的安全标准和原则。无论是银行还是证券以及电子商务等领域，均使用到了密码学的相关理论，这主要起因为密码学能够有效保护数据。当前随着学术界的不断研究，密码学已经呈现出较为繁盛的局面，因此将密码学引入到网络游戏当中具有可行性，能够促进数据传输的安全性提升。网络游戏作为一个新兴的产业发展迅速，主要是因为其拥有庞大的市场，因此急需解决其游戏数据传输中所面对的安全问题，例如本文中将要提到的虚拟财产保护、团体对抗、用户数据资料保护等问题。

本文主要是通过分析网络游戏通信构架，找出其所存在的安全问题，并根据分析结果进行网络游戏安全评估模型构建，并对游戏所存在的安全隐患进行排除，以更加安全可靠的通信架构代替原有的通信架构，再结合密码学相关安全理论进行游戏数据传输保护。根据实际情况以及需要，构建出适合自身的网络游戏安全通信引擎，以此保障网络数据传输的安全，提升运算效率。

研究了一般意义上的椭圆曲线数据防护出现的问题。此种计算其实作为具有有限域的标量乘计算。一般算法的标量乘计算通常是作用二进制的加和运算，不足之处为如果变量的值持续变大时，计算效果就不尽如人意，将会阻碍到椭圆曲线加密(Elliptic Curve Cryptography, 简称 ECC)计算的整体过程。文章在充分研究了一般意义上的椭圆曲线加密技术以及 Frobenius 格式的应用，构建了更加完善的新的主要立足于无线传感器技术的 Frobenius 椭圆曲线加密技术，此种加密计算对比于一般的 ECC 加密计算更加迅速，功率较小。在综合考虑了 ECC 与 高级加密标准（Advanced Encryption Standard，简称 AES） 这样两种比较成熟的计算方法的益处的同时，提出了基于改进 ECC 和 AES 的混合加密算法。利用更加安全化的 ECC 计算实现对称加密计算的密钥，同时利用加密计算迅速的 AES 计算作为加密明文，而且利用哈希消息认证码（Keyed-Hashing for Message Authentication，简称 HMAC）算法，论证此种方法的准确性，文章利用 VC++

程序构建来具体的计算系统，同时处在 Windows 系统下开始验证。利用综合性的加密运算开展各种无线传感器的资料进行多次检测。最终结果证明综合性的加密计算效果要强于一般意义上的椭圆曲线计算和 RSA 综合计算方法。将算法应用于《深海游击队》系统，并设计与实现系统，最后针对系统进行了测试。采用混合加密算法的网络游戏安全通信引擎，较好地保障了网络数据传输的安全，也有效地提升了运算效率。

关键词：AES；ECC；混合加密；消息认证；游戏数据

Abstract

The rapid development of network informatization has brought about the emergence of online games, and traditional games have begun to transform to online games. Online games can break the time and space constraints, from different groups of people from all over the world together to build a virtual world, it is based on this Internet connecting players around the world, with the development of online games have begun to move towards the mobile side. At present, the network game mainly combines the PC end with the mobile end, and transmits the virtual information, such as money and other information to the client side through the Internet, which leads to the problem of information leakage and theft and other illegal game property information. However, the current online game industry does not form unified safety standards and principles.

This paper mainly analyzes the network game communication architecture, finds out its security problems, and builds the network game security evaluation model based on the analysis results, and eliminates the security risks of the game, replaces the original communication architecture with a more secure and reliable communication architecture, in combination with cryptography correlation. Security theory protects game data transmission. According to the actual situation and needs, construct a suitable network game security communication engine, in order to protect the security of network data transmission, improve transport efficiency.

The problem of data protection of elliptic curve in general is studied. This calculation is actually a scalar multiplication with a finite field. The general calculation of scalar multiplication is usually the addition and operation of binary. The disadvantage is that if the value of the variable continues to increase, the calculation effect is not satisfactory, which will hinder the whole process of ECC (Elliptic Curve Cryptography)calculation. In this paper, the Frobenius elliptical curve encryption technology in the general sense and the application of Frobenius format are fully studied, and a more perfect new Frobenius elliptical curve encryption technology, which is mainly based on wireless sensor technology, is constructed. While combining the benefits of two more mature computing methods, such as ECC and AES(Advanced Encryption Standard), the co-encryption method of ECC and AES is constructed. The key of symmetric encryption algorithm is managed by ECC algorithm with higher security, plaintext is encrypted by AES algorithm with faster encryption speed, and message authentication algorithm is added by HMAC (cryptographic hash operation authentication code, Keyed-Hashing for Message Authentication). In order to verify the

feasibility of the algorithm, this paper uses VC++ programming language to write the algorithm program, and in Windows environment simulation. Experiments on different sizes of wireless sensor network packets using hybrid encryption algorithm show that the performance of hybrid encryption algorithm is better than that of traditional elliptic curve algorithm and RSA hybrid encryption algorithm.

In addition, this paper also tested the engine, and began to prepare relevant test cases, research and development of a data encryption and transmission efficiency test procedures, whether banks, securities and e-commerce and other fields, have used the relevant cryptography theory, mainly because cryptography can effectively protect data. At present, with the continuous study of academia, cryptography has shown a more prosperous situation, so it is feasible to introduce cryptography into online games, which can promote the security of data transmission. As a new industry, online game develops rapidly, mainly because it has a huge market, so it is urgent to solve the security problems in its game data transmission.

Keywords: AES; ECC; Hybrid encryption; Message authentication; Game data

目　录

表目录

图目录

第一章 绪论

1.1 网络游戏现状及特性

加密是将明文信息隐匿起来，使之在缺少特殊信息时不可读。虽然加密作为通信保密的手段已经存在了几个世纪，但是，只有那些对安全要求特别高的组织和个人才会使用它。在 20 世纪 70 年代中期，强加密（Strong Encryption）的使用开始从政府保密机构延伸至公共领域， 并且目前已经成为保护许多广泛使用系统的方法，比如因特网电子商务、手机网络和银行自动取款机等。以网络为媒介实现信息传输所构成的社区用以娱乐便是网络游戏，网络游戏充分体现了网络世界与文化相互交融的特性。网络以此在网络游戏当中具备更加深层次的含义，处理计算机互联网之外还包含了电信网、微波通信、移动互联网、有限电视网和卫星通信等在内，它们共同构成信息的互联互通。所以网络游戏是综合汇聚多个行业形成的，主要包括了网络产业、信息产业以及娱乐产业等在内，因此是信息化时代的文化产物。

从以往的资料分析可以看出，单机游戏盛行于多年前，玩家通过单机游戏丰富了自身的娱乐生活，但是随着人们物质文化的增长，传统的单机游戏已经不能够满足玩家的需求，因此单机游戏开始呈现下行的趋势，玩家人数也急剧下降，玩家希望能够具有更多模式和玩法的游戏替代传统的单机游戏。

互联网首次以商业运行的方式出现在我国主要是从上世纪末开始，互联网将玩家之间进行实时联通，玩家依靠互联网进行沟通以及交流，因此而产生了新型的游戏模式，网络游戏因此而产生，在短短的时间内便快速发展，影响范围越来越广，吸引力大量玩家。网络游戏基于互联网进行游戏，因此能够进行实时交流，所以玩家更能感同身受，代入感更强，所以得到大家的赞赏，发展速度也相当惊人。

网络游戏虽然被认为当时最火爆的互联网运作模式，其市场前景也受到众人的一直看好，但是其发展速度以及影响范围的迅速夸大令人震惊，在互联网市场占有的份额呈直线增长。

相较于普通应用，网络游戏自然有其独特之处：

互动性：网络游戏能够实现玩家之间的交流和互动，正是因为其强大的互动性特征为收获大量用户。网络游戏客户范围和跨度较大，各个年龄阶段以及各类人群均能够成为其用户。玩家在网络游戏中能够获得超强的体验度，因此娱乐性很强，网络游戏能打破时间和空间的限制，将世界各地的玩家聚集在一起进行组队和比拼，在整个网络游戏

当中充分模拟现实生活，其各类成果会累加，这也是玩家长时间存在的主要原因。

增值性：这一特性与单机游戏和其他应用具有本质差异。在网络游戏当中，玩家能够通过自身能力以及充值获取相应的游戏币以及游戏积分，这些积分和游戏币会随着玩家的游戏时间而不断积累，因此能够在网络游戏当中添加许多增值业务，从事实现成果流转和交易，这其中游戏币以及道具是最主要的增值项目。

安全性：网络游戏的安全十分重要。不同于以往的单机游戏，单机游戏因为缺乏互联网的联通，因此在操作中始终以个人为中心，所有操作只对个人发生作用，但是网络游戏中所有玩家都是联系在一起的，因此个人相关数据的改变会对整个网游世界玩家产生一定的影响，因此需要特别注意其中的平衡性问题，为所有玩家营造一个公平竞争的环境。所以在网络游戏中需要特别注重通信安全，保障用户资料以及相应的增值数据不被随意篡改，当前网络游戏主要是通过加密机制、签名机制、存取控制以及安全管理等方式进行网游平台安全管理。

运营性：网络游戏集合了单机游戏的娱乐性以及互联网的互动性于一身，在其内部形成一个完整的体系，因此不能使用普通应用程序的运营模式。游戏开发商对于游戏系统的管理往往需要多部门协调完成，因此在完成一个网络游戏的而运营需要经历宣传、策划、晒场、管理以及技术等方面的综合分析和实现，网络游戏更像是为玩家随时提供服务业务，而并非软件交易。

1.2 网络游戏安全现状

网络游戏随着信息技术的发展而越发成熟，但是在发展的过程中却存在较大的安全隐患，玩家与服务器之间建立的联系被各类非法入侵所破坏，外挂的出现使得游戏平衡被打破，在游戏世界当中出现盗窃游戏币、诈骗等现象，上述非法行为严重阻碍了网络游戏的发展。玩家面对私服以及外挂等产品丧失了对游戏的信心，逐渐开始退出网络游戏，因此网络游戏市场逐渐萎缩，在某些游戏当中甚至长期存在盗号的问题，所以玩家对游戏所提供的安全机制产生怀疑，大量玩家主动退出游戏世界。

面对当前网络游戏中存在的安全问题，其解决方案主要包括：

1.防火墙是当前对于网络游戏服务器数据库进行防护的主要手段，防火墙能够在很大程度上将黑客以及攻击者阻挡在外，游戏开发商会在相应的安全模块进行防火墙配置，其主要是将进入游戏服务器的端口进行关闭，将游戏服务器中所必须的端口进行开放，并实时进行端口监测，防止端口遭到入侵，并对操作系统进行测试，将系统中的漏

洞进行修复，解决发现的安全隐患，为了确保系统有效运行，需要对其进行安全检测，并按照时间设定将服务器中的数据进行备份，防止意外情况发生。

2.如果客户端并未采取强有力的安全防护措施，那么极容易被黑客入侵，黑客会将木马程序直接安装到客户端当中，木马会将登陆此客户端的玩家信息数据传输给黑客，因此容易造成游戏内财产的丢失。但是面对这样的情况，游戏的开发商以及运营商目前并不能有效解决上述问题，防止问题的措施主要从晚间客户端入手，晚间可以对游戏进行木马扫描以及防火墙设定，这样就能将木马进行排除，但是玩家的安全措施手段并非完全可靠，但是能起到一定的作用。

3.当前对称加密算法是开发商加密游戏数据最主要的方式，此外在系统中与玩家进行合作将玩家举报对象进行核实，从而对非法玩家进行封杀。但是举报封杀的方式往往需要玩家的协作，实际操作中作用并不明显，加密算法在实际运行中也就受到攻击或者破译，从而失去其安全效力。为了应对这样的状况，以“梦幻西游”为代表的游戏将多种加密算法结合，并在一定的时间内进行随机更换，并实时监控客户端账号与服务器之间的交互内容，一旦出现非法行为或者数据，立即进行核查，因此起到相当强的保护作用。

就目前国内外研究现状而言，研究成果较少，并且由于行业的性质以及兴起时间较短，并未有相关规范，但是目前网络游戏急需更高的安全性。

1.3 研究内容

基于全面了解网游程序的通信结构，通过检索相关资料文献的同时进行细心研究，然后研究目前关键的网络黑客技术和网络防护技术，得出网络防护所必须的安全信息。开展网游的整体性研究，同时立足于网游的主要特征，之后把目前所面临的主要的安全问题进行系统性的研究总结，同时对于系统结构的升级优化给出可行性的建议，而且综合考虑以上的所有信息构建更加全面的网游防护结构构型。为加强网游的防护性能，同时验证整体结构的安全性，对于数据开展密码学连接，得以确保网游的结构完整和信赖度。文章充分研究了网游的通信结构，发现网游出现的防护性不足的成因，同时依据研究结果开展的网游防护构型的构建，开展对于游戏的安全性能问题解决方案的研究，通过建立更加稳定和可靠的通信结构来更换普通的通信结构，对于数据开展密码学连接开展安全技能的研究对于游戏信息开展防护。依据分析的结论，总结出关于对称计算的 AES 和非对称计算的 ECC 的途径开展游戏信息的加密数据的构建。此途径结构的 ECC

计算综合了 AES 计算的密钥，利用 AES 计算进行加密信息的建立。这样的综合性的计算的利处就在于充分利用对称计算的 AES 和非对称计算的 ECC 计算方法的特点, 能够做到快速计算同时更加安全稳定便于管理密钥。

文章的主要工作状况如下：

1. 研究了一般意义上的椭圆曲线数据防护出现的问题。此种计算其实作为具有有限域的标量乘计算。一般计算的标量乘计算通常是用作二进制的加和运算，不足之处为如果变量的值持续变大时，计算效果就不尽如人意，将会阻碍到整体 ECC 计算的过程。文章在充分研究了一般意义上的椭圆曲线加密技术以及 Frobenius 格式的应用上，构建了更加完善的新的主要立足于无线传感器技术的 Frobenius 椭圆曲线加密技术，此种加密计算对比于一般的 ECC 加密计算更加迅速，功率较小。

2. 在综合了 ECC 和 AES 这样两种比较成熟的计算方法的特点的同时，构建了 ECC 和 AES 的共同加密的计算方法。利用更加安全化的 ECC 计算实现对称加密计算的密钥，同时利用加密计算迅速的 AES 计算作为加密明文，适用于 HMAC 算法。

3. 论证此种方法的准确性，文章利用 VC++程序构建来具体的计算系统，同时处在 Windows 系统下开始验证。利用综合性的加密运算开展各种无线传感器的资料进行多次检测。

1.4 研究组织架构

以下为本文主要结构安排：

第二章对本文所涉及到的相关安全技术进行分析；

第三章网络游戏数据加密的需求分析，结合互联网风险、具有破坏性的分析，网络游戏安全风险以及具体的攻击技术分析研究。

第四章针对网络游戏数据加密算法的研究，结合椭圆曲线的相关理论，改进了加密计算实现的难点以及算法设计，并针对改进的算法进行性能评估。

第五章针对改进的算法进行游戏数据混合加密算法的《深海游击队》游戏的设计与实现，在融合了 AES、ECC（改进后）、HMAC 等计算方法优势的基础上，提出了混合加密算法。该算法从计算效率提升方面进行考虑，同时确保了信息传输的高安全性需求，在数据包的加密安全实现上，采用了高安全性的对称加密算法 AES；在密钥的密秘分配管理上，采用了公开性较好的 ECC 非对称加密算法；在信息签名及认证的安全性实现上，采用了 HMAC 算法及 ECC 算法。因此，混合加密算法结合了上述三种算法的

优势，在网络信息的安全传输中，能实现信息传输的高安全性需求、高传输效率需求以及完整性需求，并大量降低了传输能耗。将算法应用于《深海游击队》系统，并设计与实现系统，最后针对系统进行了测试。

最后为结论与展望。

第二章 相关理论与技术

网络信息技术的发展必然会产生较多的网络安全问题，当前互联网安全问题已经成为阻碍其发展的最大因素。当前主要以病毒、黑客程序、远程监听以及邮件炸弹等形式的网络入侵最为泛滥，对人们的信息安全造成巨大的威胁。特别是病毒和黑客对人们造成不可估计的损失，因此人们在使用互联网的过程当中最怕遇到他们。

信息安全主要体现在信息的加密程度，人们将信息进行加密等操作主要是为了防止机密数据和信息的泄露，不能让攻击者轻易就破译相关信息文件，因此加密对于信息保密来说非常重要。简而言之，加密就是将数据内部顺序依照某种特定的规则进行组织，当合法接收者获取数据后能够很快进行数据破译，但是非法的用户在获取数据后，即使耗费大量时间和精力也不一定能将数据恢复到原状。因此数据加密手段在信息传输中使用广泛，将信息加密与密码学进行结合也是当前最主要的研究方向。因为网络游戏主要是借助网络进行数据传递，因此存在较多的不安全因素，所以在此过程中必须采用加密的手段进行数据传输安全性的保障。

密码学为当下的网络安全提供了重要的理论指导，以下为密码学中的某些概念介绍：

加密（编码）：将数据当中各类符号按照规则进行转换；

解密（解码）：将加密后的文件转换为原文件；

密码系统：主要负责加密以及解密两个操作；

明文：用于输入算法，数据能够被轻易解读；

密文：用于输出算法，明文加密后变成为密文；

密钥：用于输入加密算法，与明文互不相关。依据密钥的不同以算法为依据进行输出，并借助密钥进行算法变化。

图 2 - 1 所示为密码的编制过程。

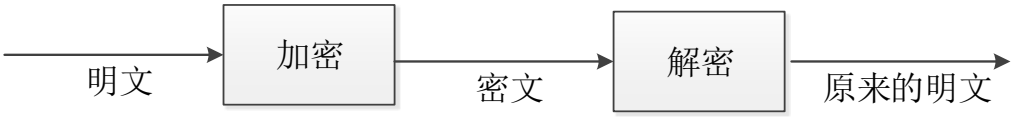

图 2 - 1 密码编制示意图

2.1 对称和非对称加密算法

对称加密算法以及非对称加密算法是当前主要的两类加密算法。

对称密码技术在实际当中运用广泛，主要是负责数据的加密以及解密，因此在行业

内将其称作常规加密技术或者但密钥加密技术。当双方实现通信后，如果要对同一文件进行加密或者解密操作，需要借助密码才能完成，而且双方面必须完全相同，这也是对称密码技术进行安全保障最主要的手段。

对称加密算法还能够进行细分，此过程中主要依据加解密对象为依据，如果是将明文内部存在的单个比特进行加解密，这样的算法被称作序列密码算法。还有一种算法主要是将明文划分为不同的组别，每个组由若干个比特或者字符构成，然后以组为单位进行加解密操作，此类算法为分组密码算法。

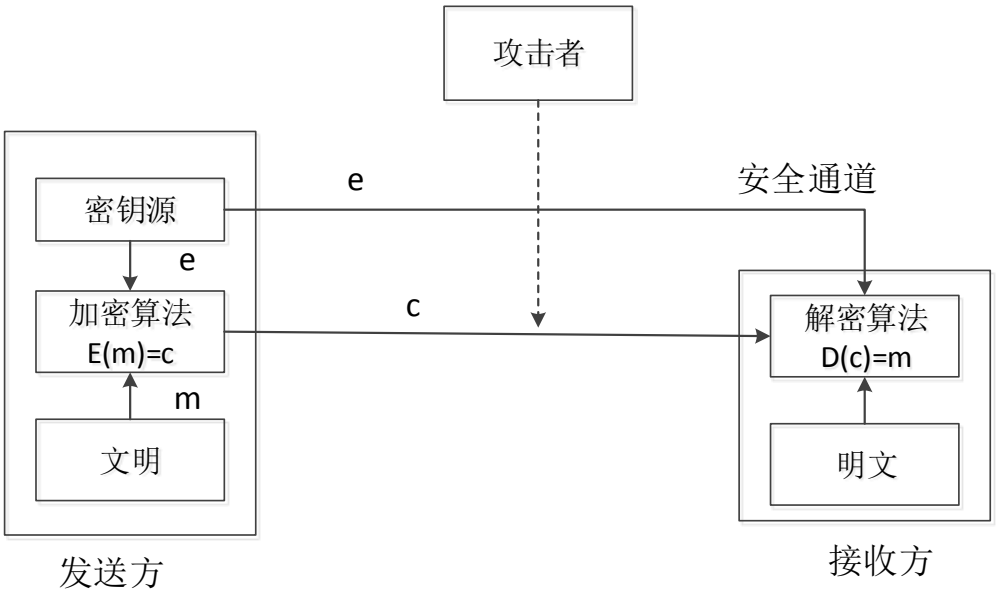

图 2-2 基于对称加密的数据通信

上图所示对通信双方安全通信中所采取的对称密钥 e 加密技术进行了阐述，以下为其信息安全处理主要的几个步骤：

随机数发生器需要先对数据进行加密，此过程中发送方会获取密钥，在完成后将文件安全发送到对方手中；

在发送的文件当中，如果存在明文信息，发送方会借助密钥以及加密算法进行加密，当加密完成后形成密文 c，此时发送方可以通过正常渠道进行文件传输；

发送方会将密钥告知接收方，当接收方受到文件后会利用密钥 e 解密密文，这时候接收方便能够获取最初的明文信息。

快速加密以及解密是对称加密被广泛使用的原因，也是其主要特点，这样的加密方式在面对庞大数据时候能够发挥较大作用，但是前提是必须确保密钥的安全。对称加密技术受到密钥交换环节的限制，只有双方进行密钥交换接收方才能成功进行解密，但是当用户量急剧上升的时候，无法对庞大的密钥进行管理。而且再次过程中谁也无法保证

密钥交换的绝对安全，因此实际运用此类加密算法时通常会定期更换密钥，有的人为了确保安全，传输不同的文件会采用不同的密钥，这就造成传输效率的低下，并且整个过程很繁琐，所以并不完全使用当下的环境。

公钥密码技术就是我们通常所说的非对称密码技术，此类算法最早产生于上世纪七十年代。通信双方密码不对称是该算法最主要的特征。在此算法当中将密钥进行配对，形成公钥和私钥两种密钥，这两种密钥相互作用，只能运用对方将一方加密的文件进行解密。

这也是非对称密码技术的关键所在，如果采用对称密码技术，那么在密钥传输过程中极易被窃取。但是在非对称加密中公钥向所有人开放，因此不存在泄露问题，而私钥能够实现密文解密，这样就不会造成密钥丢失或者泄露等安全问题。

值得注意的是，在制作公钥、加密算法以及密文当中，不能够涉及到能够推演出私钥的任何信息。因此，非对称密码算法必须具备以下要求：

用户可以轻松依靠算法获取相匹配的公钥发送方和私钥接收方；

用户如果掌握了公钥以及明文，能够轻易用算法使之转变为密文；

用户可以依靠私钥将公钥加密的密文进行解密；

公钥不能通过计算获取私钥的任何信息；

攻击者将明文借助公钥进行加密，此时可以依靠算法获取明文；

公钥和私钥必须同时具备加密以及解密的功能；

图 2 - 3 所示为双方通信中公钥和私钥加密解密的流程示意：

发送方需要从公共渠道当中接收方传输的公钥，公钥并不需要加密；

发送方接收到公钥后用之将明文信息加密，使之转变为密文，然后再将获取的二米文信息传输给接收方；

接收方接收到密文后，借助相匹配的私钥进行解密，然后会成果获取最初明文。

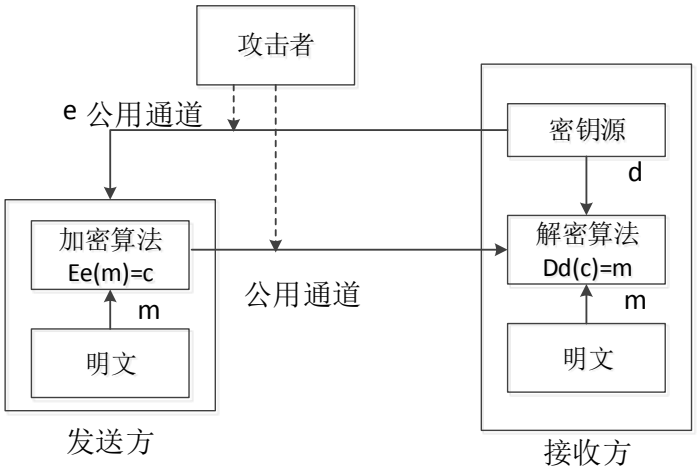

图 2 - 3 基于非对称加密的数据通信

2.2 哈希函数

本文在使用过程中，会结合哈希函数进行密钥安全的设计，实现函数整体的设计，进一步优化系统函数。H 代表还需函数，x 为其输入，本质为能够转变的长串，y 为其返回的不可变长串，那么此时 x 的哈希值为 y，通常写作 y=H(X)。

压缩函数是单向还需函数的基础，如图 2 - 4 所示。

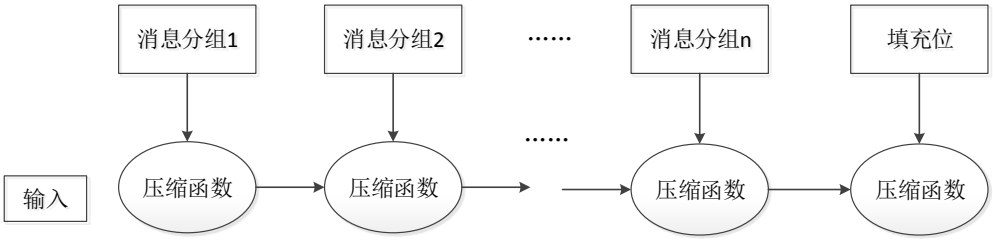

图 2 - 4 哈希函数工作模式

以下为单向哈希函数的主要特性：

H(X)分组时不收数据值大小的限制；

H(X)输出值不变，即使输入数值不同；

H(X)需要在固定 x 值是能够通过简单计算获取；

H(X)不可逆行计算，不能够根据输出的哈希值倒推 x 值。

哈希函数的碰撞是其主要特性，因此对其碰撞难度计算是确保哈希函数安全的主要方法。

弱抗碰撞性的哈希函数：

当给定某条消息的散列值时，单向散列函数必须确保要找到和该条消息具有相同散列值的另外一条消息是非常困难的。

强抗碰撞性的哈希函数：

是指要找到散列值相同的两条不同的消息是非常困难的。

在密码学上通常要求哈希函数具备以下特征才能认为哈希函数可靠：

哈希函数为单向函数；

哈希函数必须属于弱抗碰撞或者强抗碰撞哈希函数中的一类；

在哈希函数中无论 x 取值为何，都能够轻易计算出哈希值。

与加密和签名等技术相比，哈希函数具备的优势在于速度快，所以哈希函数主要适用于验证数字签名的完整性，如果需要验证同一个数据是否属于合法数据或者数据是否有缺失，可以通过哈希函数与非对称加密两种方法结合进行。

2.3 数字签名与信封

2.3.1 数字签名

签名在现实中主要作为凭证，比如在合同中签名代表资源统一合同内容，具有相当强的约束力，并在日后纠纷发生之后当作证据。电子签名适用于互联网上，主要和手写签名含义相同，因此在电子商务领域得到大力推广。

哈希函数于非对称函数的容和使用能够对信息的缺失以及有效性进行验证。信息是否确实能够看出信息是否存在非法修改行为，有效性则是体现在信息发出者的身份是否合法，以此排除黑客。数字签名便是二者的结合。

通信双方首先需要固定一个哈希函数，再将报文计算获取与之相对应的报文哈希值，通常只要对报文任一部委进行修改，那么报文所产生的哈希值将与先前所得哈希值大相径庭，因此可以通过这个手段确保报文完整。私人秘钥还需要将报文哈希值进行加密操作，加密完成后将二者结合发送到接受者手中，在此过程中数字签名就是报文。图 2 - 5 所示为数字签名创建的完整流程。

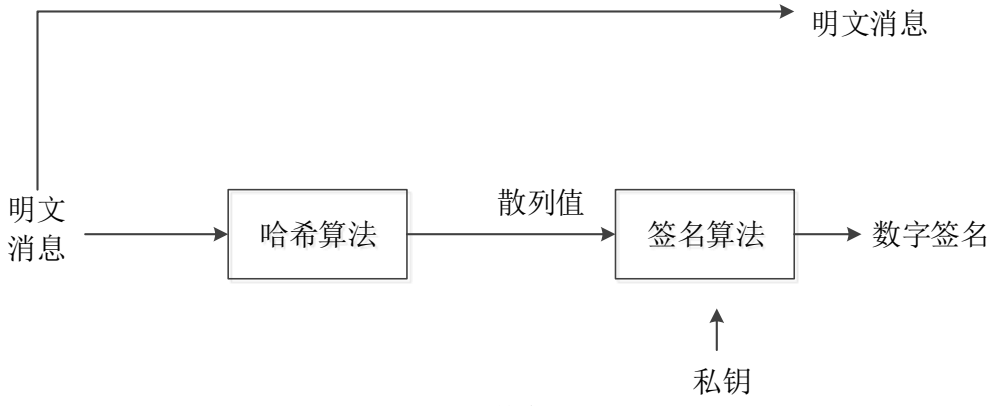

图 2 - 5 创建数字签名

一旦数字签名到达接收方手中，需要借助哈希算法进行报文哈希值获取，之后再将

所得哈希值与公钥解密所得哈希值进行分析比对，在此过程中发送者私钥和公钥是相互对应的，因此连这个和完全符合才能够解密报文，所以数据无法被修改。图 2 - 6 所示为验证数字签名的完整流程。

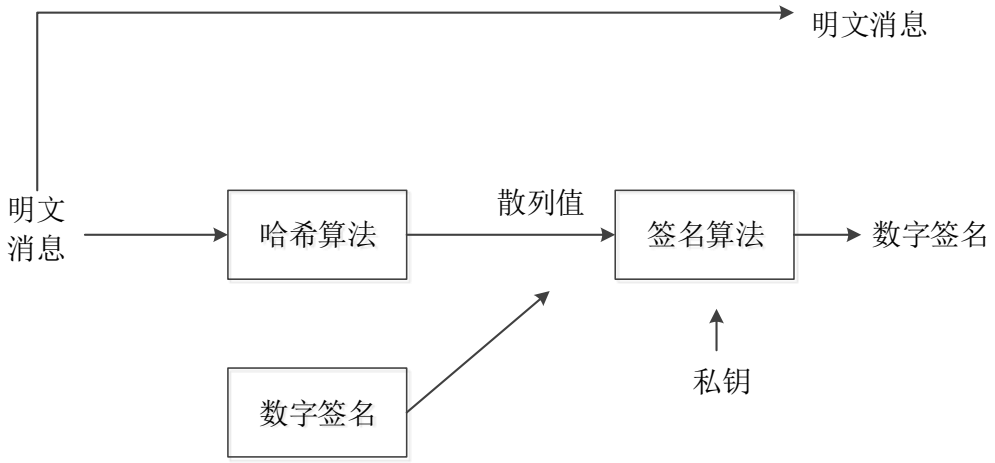

图 2 - 6 验证数字签名

当前数字签名也会遭受到相应的攻击，其中无消息攻击是借助公开的公钥攻击签名，攻击者无法获取密钥；此外还存在已知消息攻击，攻击者获取相应的签名后，攻击签名的而行为。详细划分的话，已知消息攻击还能够细分为以下四种，划分依据主要是已知消息的选取方式：

简单已知消息攻击：我们以 M1、M2、M3….代替各类消息，当攻击者获得个消息的签名后对这些消息进行随机攻击；

普遍选择消息攻击：攻击者在消息 M1、M2、M3….当中选择需要攻击的消息，再获取器对应的签名，但是此项攻击前提是未获得消息的公钥；

又向选择消息攻击：攻击者在消息 M1、M2、M3….当中选择需要攻击的消息，再获取器对应的签名，但是此项攻击前提是已获得消息的公钥；

适应性选择消息攻击：此种攻击主要是表现在承接消息签名，获取一个签名之后根据这个签名攻击其他的签名。

综上所述，各类攻击基本原理大致相同，但是攻击程度却有所差异，在所有的攻击方式当中以适应性选择消息攻击力度最大，因此在实际中大多防备此种签名攻击方式。

2.3.2 数字信封技术

数字信封技术针对对称加密、公钥加密的优势、劣势进行了综合，取长补短后提升了算法的性能及信息的传输安全[29]。其具体的实现步骤分成：

（1）通过对称加密，随机进行会话密钥生成，并完成信息 C 的加密。

（2）采用非对称密钥公钥加密会话密钥，并完成 Eb（密钥包）的生成。

（3）向各信息接受节点进行 Eb 的发送。

（4）Eb 被接受节点接收并通过私钥解密获取其对称密钥。

（5）通过对称密钥解密加密信息形成明文信息，完成其加密安全传输。

在下图 2 - 7 中，本文列举了 bob、alice 信息的数字信封实现流程图。

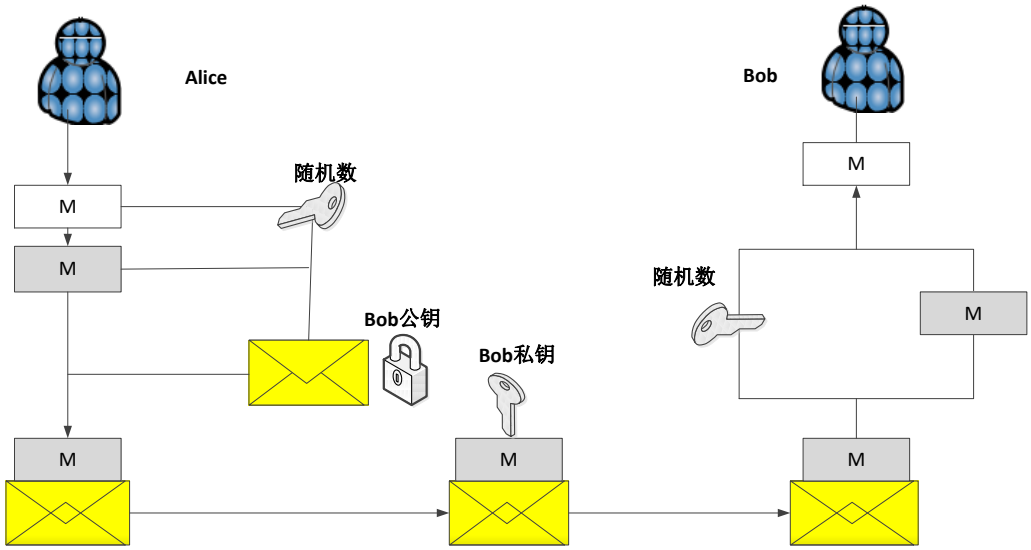

图 2 - 7 bob、alice 信息的数字信封实现流程图

在信息的数字信封加密安全实现中，其运用了双层加密计算方法[30]，即内层运用了单次单密的对称加密计算方法，外层运用了公钥加密计算方法，通过结合两者的优势，实现了信息传输的高安全性、高性能。

2.4 密钥相关技术

2.4.1 自动密钥分配

互联网大世界当中，密钥的安全直接决定着加密是否具有意义，一旦密钥丢失或者被窃取，那么对于加密来说毫无意义，因此需要严格管理密钥，主要涉及到密钥的产生、检验、保存以及传输和销毁等环节，密钥的分配也叫做密钥传输，此环节最容易出现安全问题。所以长期以来密码学以密钥分配为研究对象，力图实现密码技术的提升。

以往传统的密钥分配方式较为普通，通常采取人工进行传输，这种方式效果明显，但是随着文件量的加大，人工已经不适应当前的大环境，因此需要更加安全高效的分配方式。互联网传输的出现使得传输和加密环节速度飞速上升，人工效率过低根本无法为其提供保障，因此在密钥分配领域必须引入信息化技术。

当前密钥自动分配较为典型的由基于对称密码体制以及基于公开密钥密码体制两类方法。无论是哪一中分配方式，均需要与第三方进行合作，且必须确保第三方安全以

及可靠。

图 2 - 8 所示为基于可信赖第三方所构建的通信模型。

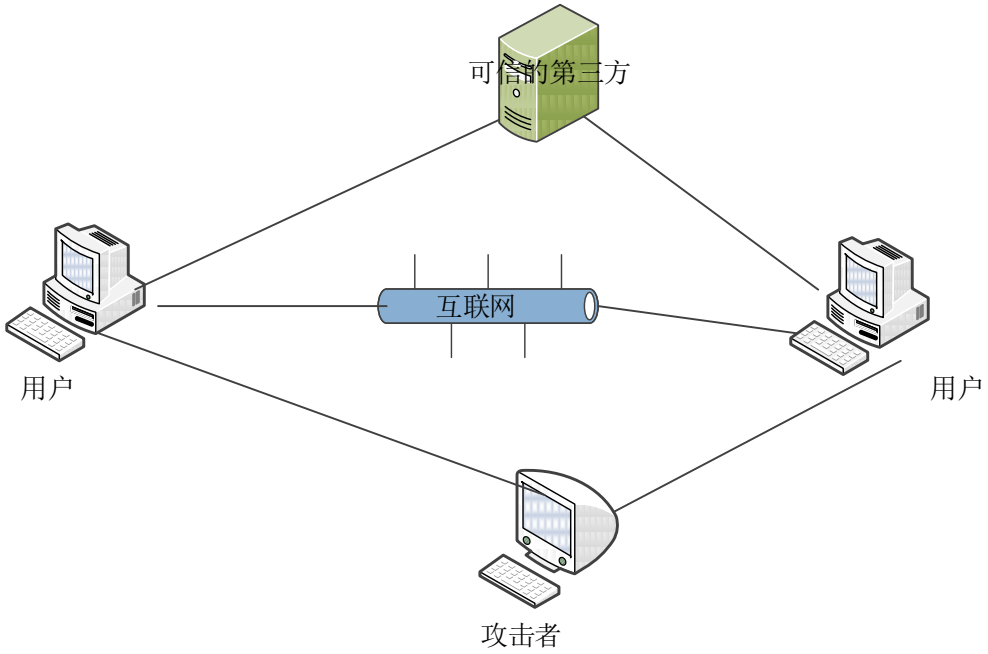

图 2 - 8 基于可信赖第三方的通信模型

此模型适用于当前所有的网络游戏，游戏服务器在加密以及密钥分配过程中充当管理者和控制者。

当前基于 PKI 分层结构的密钥自动分配正在快速发展，这主要是基于其高效率以及高安全性和可靠性。PKI 体系结构时应对互联网安全问题最为有效的方法，其在世界范围内被广泛运用和研究。

通过证书对公钥进行管理是 PKI 体系结构最主要的特点，其将包括用户公钥以及重要信息在内的全部信息进行融合，并借助互联网对用户权限和身份进行检验，PKI 体系主动将公钥面以及对称密码进行融合，因此一个基于互联网的而谜语自动分配管理机制便形成，具有超强的安全性和完整性。

2.4.2 对称密钥的密码体制

在传统的信息加密实现中，最常用的是对称密钥计算方法，该方法在信息的加密、解密实现中，运用了数学理论知识，采用推理方式及非线性计算实现，一般情况下，其加密、解密的密钥是一致的。在传统的信息加密实现中，需要在信息交互前，信息双方进行私钥的共约，因此在信息的交互实现中，其安全保证是依托信息双方的密钥实现的。假设信息在交互实现过程中，其中一方的信息密钥遭到泄露，而会影响到信息交互的安全，出现信息被破解的情况，存在一定的信息交互不安全因素，为此，需要从私密性上

针对信息交互实现过程的密钥安全进行安全性设计考虑。在传统的信息加密实现中，其加密计算表达式如 2.1 所展示，解密计算表达式如 2.2 所展示。同时，其加密计算实现根据计算方法的不同，又可以分成分组、序列两种[19]。其中明文信息的交互实现中，加密计算中的序列方式只能针对比特信息实现单次单个加密，而加密计算中的分组方式则能对比特信息实现单次按组进行加密。同时在互联网信息的交互安全性抗捕设计上，对称加密方式可确保信息交互的单次密钥实现，即使信息交互过程中，出现了密钥泄露，也不会对信息交互过程产生严重的影响。信息交互中的加密、解密关系如表达式 2.3 所展示。

$$E_K(M) = C \qquad (2.1)$$

$$D_K(C) = M \qquad (2.2)$$

$$D_K\big(E_K(M)\big) = M \qquad (2.3)$$

如今现在大部分的对称密钥加密计算包括：

（1） DES 加密

早在 70 年代由 IBM 企业研发出的 DES 是一种经国家检测合格的对称密钥加密算法，属于对称加密中的传统加密区组，该算法在 1976 年 11 月应用于美标准局、标准协会等机构中长达 10 年时间[18]，其使用效果较好，促进了使用面的推广。在对称加密实现中，其加密、解密中的密钥设计是相一致的[19]。DES 总长度等于 56bits 明文加密等待长度加上 8bits 检验长度，其具体实现流程如下图 3 - 1 所展示。

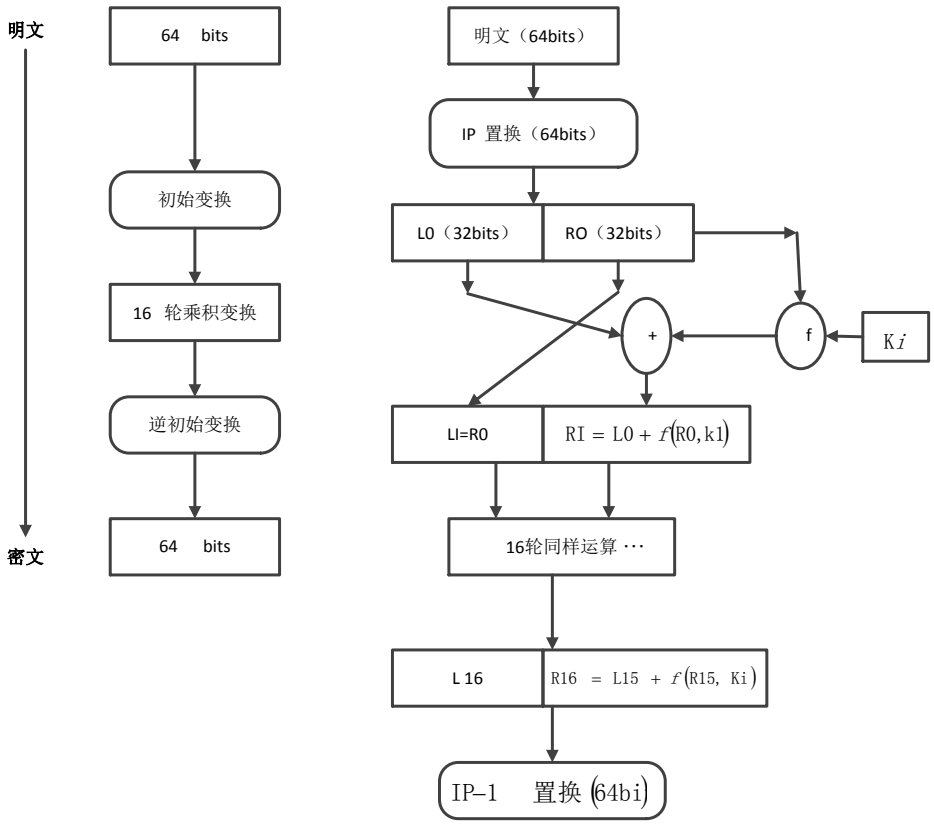

图 2 - 9 DES 的实现流程展示

在上图 2 - 9 中，其右边部分主要展示明文 DES 加密的具体实现，首先明文在加密前，需通过函数 f 进行 16 次乘积变换计算、平分其加密内容，再进行平分信息内容的合并及初始化逆变换、置换计算，最后采用异计算不断向左循环移动，完成信息的置换，直至计算 16 次完成，DES 加密才结束。而在 DES 解密实现中，其计算过程同加密类同，不同之处在于，每次加密计算是顺序进行，即 K1、K2……K16；而每次解密计算则是逆序进行，即 K16、K15……K1。在每次加密密钥计算中，其产生的新密钥将不断向右循环移动，且完成信息的置换。

DES（数据加密标准，Data Encryption Standard）加密计算受计算机高处理能力的提升影响，可破解其 512 位加密密钥，从而也威胁着其 1024 位密钥的安全。但其加密速度较 RSA 计算方法快了 100 倍，甚至比其它专业加密快了 1000 倍，具有其它加密技术所无法匹敌的独有优势，同时该加密计算方法还可以同 ECC 等加密计算方法进行组合运用，称之为加密混合计算方法，最大程度地发挥了两者的优势。

DES 加密计算方法的不足之处表现在：

1、密钥的位数设计较少，不能满足计算机的现代化需求。

2、在密钥计算中，会产生弱密钥。假设某交互信息的密钥等于 K，则其下会产生

出 1-16 位的子密钥，这些密码被称之为弱密钥[20]，其表达式为：

$$DES(DES(M,k),k) = M \quad (2.4)$$

$$DES^{-1}(DES^{-1}(M,k),k) = M \quad (2.5)$$

$$DES(M,k) = DES^{-1}(M,k) \quad (2.6)$$

3、假设 C=DES(M，K)，则 C、M、K 的对称非操作表达式为 C ‘=DES（M’，K’），即表明 DES 密钥间存在对称互补的情况，不利于信息 DES 加密的安全，很容易受到破解威胁。

（2） AES 加密

作为一种 NIST 替代 DES 的新加密计算方法，AES 常使用在电子数据加密实现中，其密钥通过迭代计算形成对称密码块，可分别加密、解密 128 位、192 位、256 位等不同的电子数据[21]。AES 加密计算方法不同于公钥加密计算方法表现在，针对信息交互实现的加密，密钥呈对称状，且加密、解密的密钥相同，因此同样具有对称加密的高速计算优势，因此在数据信息的加密中应用较广。

2.4.3 DES 加密与 AES 加密的对比分析

虽然 DES 加密、AES 加密两种加密计算方法在密码的分组上都呈对称关系，但同时也存在一定的区别，具体如下：

1、加密实现区别：AES 加密对硬件、软件的要求都相对较低，且计算效率很高，因此容易在软件、硬件平台上进行操作；DES 加密对软件要求高，而对硬件要求低，因此比较容易在硬件平台上进行操作，而很难在软件上进行操作；

2、安全实现区别：AES 加密较 DES 加密安全性高，至今没有出现破解情况，而 DES 加密则被破解过。

3、密钥长度区别：AES 加密没有限定密钥的长度，而 DES 加密则限定了密钥的长度必须等于 64 位，

（3） 对称加密的不足

1、密钥在各节点间的传输必须保证其安全，如果某节点密钥遭到窃取，则其全部加密信息内容会被全部破解、公开。

2、假设某节点密钥遭到窃取、破解后，其不合法节点将破解其传输的信息内容或伪装成某一节点，进行虚假信息的传输，造成信息传输混乱。

3、对称加密计算方法在管理节点密钥时，假设其全部节点都有自己的独立密钥，则增加了对称加密计算方法的管理难度[22]。可以设想，假设网络的节点数等于 20，则

其通信密钥数等于 M（M-1/2），即 380 个，以此类推，因此当 WSN（无线传感器网络，Wireless Sensor Networks）的数量不断增加时，不能实现对密钥的有效管理。

2.4.4 公钥密码体制

在公钥的加密、解密计算实现中，需使用到的密钥数等于 2 个，分别是公钥、私钥，使用在信息的加密、解密实现中，因此具有较好的安全性。假设信息在传输中，由于其公钥对各节点是公开的，因此容易受到窃取，但其私钥不是公开的，因此即使其公钥被窃，也不能对信息内容进行破解。

1976 年学者 helman、diffie 在信息的加密研究中发明了加密公钥计算方法，其运用数据函数实现了不相关密钥数据的加密。公钥加密与对称加密相比较，在信息的加密、解密计算中，对称加密只有 1 种，公钥加密则有 2 种不同的密钥，因此较对称加密更具安全性，其表达式为[17]：

$$E_{K1}(M) = C \qquad (2.7)$$

$$D_{K2}(C) = M \qquad (2.8)$$

$$D_{K2}\big(E_{K1}(M)\big) = M \qquad (2.9)$$

在信息的加密实现中，其加密计算方法并不重要，重要的是密钥的安全性。因此在 RSA 加密、ECC 加密在加密、解密计算中都使用了 2 种不同的公钥，其具体的信息加密实现步骤，如下面所例举的发送与接收的交互实现描述。

1、在公钥密码体制的选择上，发送方和接收方的选择一致。

2、接收方由发送方传输来的公钥，并完成自身信息的加密。

3、接收方把加密信息传输给发送方。

4、发送方接收信息并通过自身的私钥完成信息的破解。

因此，在对称加密实现中，可以通过公钥密码的应用，来提升其管理效率。

信息在网络中通过无线传感器进行传输时，也使用到了公钥密码体制，在网络中，信息传输的所有节点都有公开的公钥，但其私钥是不公开的，因此具有较强的安全性，其具体实现描述如下：

1、通过数据库，发送方可以获取接收方公钥密码信息。

2、发送方获取接收方公钥并完成自身信息的加密，再向 bob 进行传输。

3、接收方接收发送方信息并通过自身的私钥完成信息的破解。

目前，使用较多的公钥密码体制如 ELGAMAL、ECC[23]、RSA 等等。

2.4.4.1 RSA 加密

1977 年学者 Shanmir、Adleman、Rivest 在研究质数加密计算中研究出了 RSA 公钥加密计算方法，其具体实现运用了模幂、单向陷门函数、最优等计算方法，确保了大数因子的分解安全[24]。在加密实现中，针对大数因子 N 的时间、位数分解，其计算速度高达 1 秒 100 万次，计算次数约 1350 次，可分解出的时间、位数为 4305 年、500bi[25]，具有很强的安全性，其加密步骤为：

1、密钥初始操作

（1）P、q 分别为大数因子中的不同质数，且 p*q=N。

（2）运用欧拉函数计算大于 N 的整数互质数，表示为（q-1）*（p-1）。

（3）选择一整数，假设其等于 e，且小于（q-1）*（p-1），两者间呈互质关系，其表达式 d 等于（d*e）$\equiv$1(mod((p-1)(q-1)))

其中 d、p、q 分别代表了大数因子的私钥，而 k=｛e,n｝代表了大数因子的公钥。公钥可以被获取，但密钥则不能。

2、RSA 加密

（1）节点完成信息 C 的发送，并接受其它节点信息公钥（K），其中 k 等于｛e,n｝。

（2）根据公钥 K，完成对信息 C 的加密，其表达式为 $M^e \bmod n$，其中 n 大于 m，m 大于 0。

（3）把加密信息 C 向接收节点进行发送。

3、RSA 解密

（1）接收节点信息，并通过私钥 K^{-1} 进行解密，其私钥表达式为｛d，p，q｝，解密表达式 M 等于 $C^d \bmod N$。

由于 RSA 解密实现操作简单、易学，因此不能满足高处理速度的计算机计算需求以及网络的正常信息传输需求，为了提高其对信息传输的安全保障、抗捕保障，RSA 在密钥的长度设计上进行改进，由原来的 512 位提升至 1024 位，虽然实现了信息的安全传输[26]，但同时也存在一定的不良影响，会由于加密计算时间的增加而增加硬件负载。

2.4.4.2 ECC 加密

1985 年学者 Miller、Koblitz 在研究离散对数有限循环群的加密实现中，研究出了 ECC 公钥加密计算方法，其优势表现在，计算的量少、速度快、安全性高且对网络、通信的空间、带宽等没有高要求[28]，易实现，同时其有限的密钥群可通过不同参数选择进行大量椭圆曲线的生成进行密钥群的构造，还可以避免其计算过程中出现亚指计算，因此受到广泛关注与亲睐。

目前，各国学者针对 ECC 公钥加密的研究，主要体现在：

（1）标量乘计算速度的提升研究

标量乘计算速度的提升研究是 ECC 加密实现的重要内容之一，其具体提升分成有限域底层的计算速度提升以及有限 ECC 点群的上层计算速度提升。通过展开研究，可以针对加密计算性能进行改善，实现有限或中 ECC 加密的计算。在本文中，针对标量乘计算速度的提升研究，主要表现在有限 ECC 点群的上层计算速度提升上。

（2）椭圆曲线的最优选择

ECC 加密的有限密钥群可通过不同参数（D=（q，F_r，a，b，p，n，h））选择进行大量椭圆曲线的生成#（E（F_q））来构造密钥群。因此，D、#（E（F_q））成为其研究的核心。

（3）WSN 与 BCC 加密的结合实现

BCC 加密对计算环境的要求不高，因此 WSN 从使用成本考虑，运用 ECC 加密来实现其信息传输的安全性，吸引了国内学者的研究。

（4）硬件性能提升

假设信息在硬件传输中实现 ECC 加密，会提升其安全性、传输效率，如果能结合指数加密，则可以提升硬件的性能，成为各国学者的研究方向。

（5）ECC 加密协议研究

ECC 的加密实现需要具体适用的安全协议，从目已有的安全协议上看，其数量很少，不能满足加密需求，需要各国学者展开研究。

2.5 消息的认证

在信息的安全传输中，信息的认证实际上是指带密钥函数 Hash，最早由学者 m.bellare 研究出其构造法[32]。信息认证作为信息传输双方的通信验证机制，以实现信息的完整传输[31]。

2.5.1 信息的认证实现流程

信息传输双方在进行信息传输前需要协商选择散列函数以计算信息的摘要值，当信息 M 通过节点 P 会话密钥完成加密、发送，再由散列函数计算其摘要值得出认证码 MAC（T_K（M））， 最后向接受节点 q 进行信息、认证码的发送。当信息、认证码被接受节点接收并通过私钥、散列函数解密、计算、比较其摘要值内容的完整性，具体流程图如下图 2 - 10 所展示。

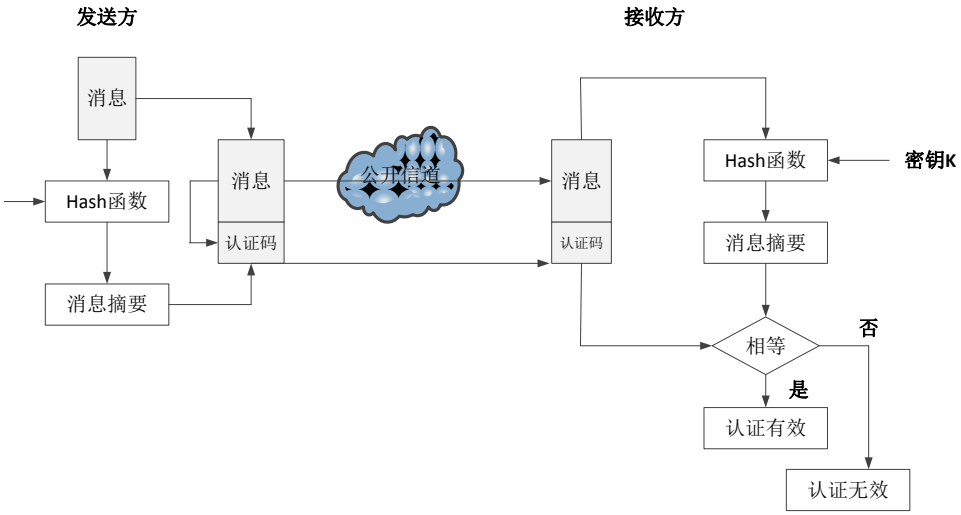

图 2 - 10 信息的认证实现流程图

在信息的认证实现中，为了保证其信息的完整性，运用了非对称加密计算。

2.5.2 信息的认证方式

（1）信息加密函数认证方式是指，通过对称、非对称的加密函数方式，完成信息内容的加密、发送[33]。

（2）信息加密散列函数认证方式是指，hash（散列函数）可以通过数学计算来改变并认证信息的长度值为固定的摘要值[34]。

（3）信息认证码的认证方式是指，通过公开函数处理接收到的加密信息并生成认证码完成信息的认证，一般使用在加密信息摘要值、MAC 计算的信息认证中[35]。

综上所述，在网络信息的安全传输中，其安全性较高的加密体制为公钥、对称两种加密体制。

2.6 本章小结

本章节依次介绍了密码学技术的发展、WSN 密钥分类以及对称加密、公开加密、DES 加密、AES 加密、ECC 加密、指数加密等计算方法，最后介绍了数字信封技术、信息认证技术，并展开了对比、分析。

第三章 网络游戏数据加密需求分析

本章主要是基于当前所存在的网络游戏体系进行研究，对网络游戏安全评估进行模型构建。本章将网络游戏数据环节作为研究重点，对互联网进行安全分析，主要体现在条对传输协议 TCP/IP 等方面进行安全分析，并针对当前网络环境以及网络游戏面临的威胁进行深入探讨，并研究了攻击网络游戏的主要手段和技术。

3.1 互联网安全风险分析

互联网实现了全球范围内的信息交流以及共享，当前互联网主要是基于 TCP/IP 进行网络互连，但是这样的互联协议安全性并不高，因此产生大量安全威胁和风险：

明文传输是 TCP/IP 主要的传输方式，当互联网运用到 FTP\HTTP 等时极容易出现账号信息和口令的丢失现象，攻击者能够轻易获取相关信息；

攻击者可以将节点的 IP 地址进行修改，并通过伪装成合法地址发起攻击行为；

源路由选择欺骗：为了更好地进行测试工作，IP 数据包会产生 IP 源路由，并能够将节点进行设置，正是基于此项设定攻击者伪装进行非法连接；

路由选择信息协议攻击：动态路由信息由 RIP 协议发布在局域网中，当节点获取信息时并不对对其进行相关的验证，因此攻击者借助这个特点伪装为 ICMP 信息发动攻击，主要攻击对象为路由器以及主机；

鉴别攻击：安全认证技术的缺失导致用户身份检验只停留在 IP 地址和写一段层面，因此可能导致非法用户入侵；

TCP 序号欺骗：通过一定的手段能够获取 TCP 序列号，基于序列号创建相应的 IP 包发起网络攻击。

为了保障互联网安全，世界范围内的研究主要针对不同问题开发出各类安全机制，在所有的安全技术手段当中以加密和认证机制最为有效，此外还加强了信息保密技术、身份验证以及不可否认等相应服务的技术水平。

网络通信的加密以及认证机制可以以 TCP/IP 结构特点的层次性进行划分，其实现方式主要是以下几方面，分别为基于链路层的安全性、基于应用层的安全性、基于传输层的安全性以及基于互联网层的安全性。

基于链路层的加密和认证

基于链路层的加密以及认证机制主要作用于两个点之间，首先将中间路由器中的数据进行解密操作，完后才能后对另外的链路进行加密。路由器上的数据均以明文方式呈

现，因此如果路由器存在病毒或者漏洞，极容易将明文泄露，所以在实际运用中采用此种方法的较少。

基于 internet 层的加密和认证

将 IP 包在网络两端的通道上进行获取，然后解析 IP 包，对其进行加密、解密以及封装等处理，以此实现网与主机之间三种对应连接方式。IP 通道以及 VPN 通常就会采用 IP 包加密和认证技术进行安全防护。

基于传输层的加密和认证

传输层主要作用于进程之间，其主要是通过在两个能够信任的差 US 农户服务上面建立另外一个层，以此将两个层今次那个连接，并通过该层实现加密优化和升级。SSL 协议以及 SSL/PCT 协议是其最为重要的两类协议。

基于应用层的加密和认证

将安全加密机制设置带引用层的服务之中，以此在适当时候依据服务类型进行安全协议选择，通常以互联网邮件扩展、安全超文本传输协议、安全电子交易以及私有强化邮件使用最为广泛。

3.2 具有破坏性的非法攻击

当前主要是外挂、木马盗号以及网络嗅探器能够对网络游戏的数据传输环节造成较为严重的威胁。除此以外，黑客也是威胁游戏的主要力量，他们市场对游戏服务器发起攻击，试图盗取账号以及游戏资料。网络游戏服务器通常具有较强的低于能力，因为其本身存在于防护力超强的环境当中，因此网络攻击似乎并不会对其产生任何影响，所以在本文中并不会对其进行过多阐述和研究。

游戏外挂主要是玩家用于游戏破解，其主要是玩家用于修改网络游戏内部资料以及自动代替玩家进行相关游戏操作，通过外挂玩家可以最大程度节约成本，但是却能够收获巨大的价值或者快速升级。

游戏外挂具有专门性，不同的游戏需要设计不同的外挂，因此不可能出现通用外挂，所以依据外挂所适用的游戏将外挂划分为两大类：第一种是玩家为了将游戏内部的不需要的操作或者重复的操作进行过滤，从来最快时间获取大量游戏币或者升级。第二种是对游戏内部资料信息进行篡改，将外挂数据包伪装为正常数据，然后到达游戏内部将相关数据进行非法修改，以此实现玩家各类需求。但是这样的外挂是需要专门研发的，因此往往在不同版本中并不能使用同一外挂，不同游戏需要借助相应的数据包实现与客户

端的对接，所以外挂程序要向实现客户端修改，必须充分掌握网络游戏数据，以此伪造出服务器认为合法的数据包。此种类型外挂不容易被发现，因此在现在的网络游戏中大量存在，威胁游戏平衡和安全。

盗号木马，属于网络木马中的一种，其主要作用是将玩家的账号以及面等信息进行盗取，并将所得信息反馈给木马指定单位。木马盗号的原理较为简单，通常是通过安装监视程序记录玩家登陆游戏客户端时所输入的密码和账号，并将其发送到攻击者邮箱内。

网络嗅探，主要是用于窃取相应的网络资料，但是其最大特点是不易被发现。由被动嗅探和主动嗅探构成，被动嗅探主要是基于数据链内部共享机制得以实现。正是基于共享才能将服务器内某一资料传送给所有机器。当以太网获取相应报文后，会检验发送地址是否合法，并在此过程中查看是否需要自身接收，需要就直接将该报文传输到系统当中，如果不需要直接将报文扔掉。主动嗅探主要是借助 ARP 包进行，自身先生成一个虚拟的 ARP 包，一旦系统报文当中存在一定的隐蔽文件或者账号信息，嗅探器会自动将其获取，此种方式不仅对一台机器造成威胁，还会对局域网内及其造成连带威胁，攻击者借此进行权限非法获取，从而对网络结构进行非法修改。通过上述原因可以看出嗅探器对于整个互联网威胁较大，一旦网络游戏被安装嗅探器，那么客户端与网络游戏服务器之间的交互信息将毫无保留地被盗取，攻击者能够借助嗅探器获取玩家账号和密码等信息。

3.3 网络游戏安全风险

3.3.1 框架协议分析

网络游戏通过互联网实现客户端和服务器的数据传输，在此过程中需要借助 TCP/IP 协议。TCP/IP 协议主要是作用于互联网和计算机之间，进行通信处理，通常将他们称之为协议族。其最早产生于上世纪七十年代的美国，由国防部为广域网所专门制定的网络体系结构，主要是为了将协议进行统一，有利于工作开展。Internet 网络正是基于 TCP/IP 而创建，经过长时间的发展目前已经成为全球最大的计算机网络，TCP/IP 成为行业协议模型也主要是得益于互联网的发展。TCP/IP 内部主要由 TCP、UDP、FTP 等众多的协议构成，他们之间形成一个群体，因此将其比作协议族，完整的 TCP/IP 协议包含上述所有的协议。

大型网络游戏通常使用 TCP，而 UDP 则主要是存在于内网应用，这是因为内网较

为隐蔽，无法获取双方地址。

互联网的发展使得 TCP/IP 协议成为协议标准，因此 TCP 和 UDP 成为当今互联网游戏中使用最为普遍的协议。TCP 协议更加适合大型的 C/S 架构的网络游戏，而 UDP 协议则适用于小型的 p2p 休闲游戏，因为 UDP 传输速度较 TCP 更快。

通过深入研究当前网络游戏所存在的体系结构，将所存在的安全漏洞全部找出，并根据漏洞特点进行优化，尽量弥补漏洞。

图 3 - 1 所示为网络安全总体分析图。

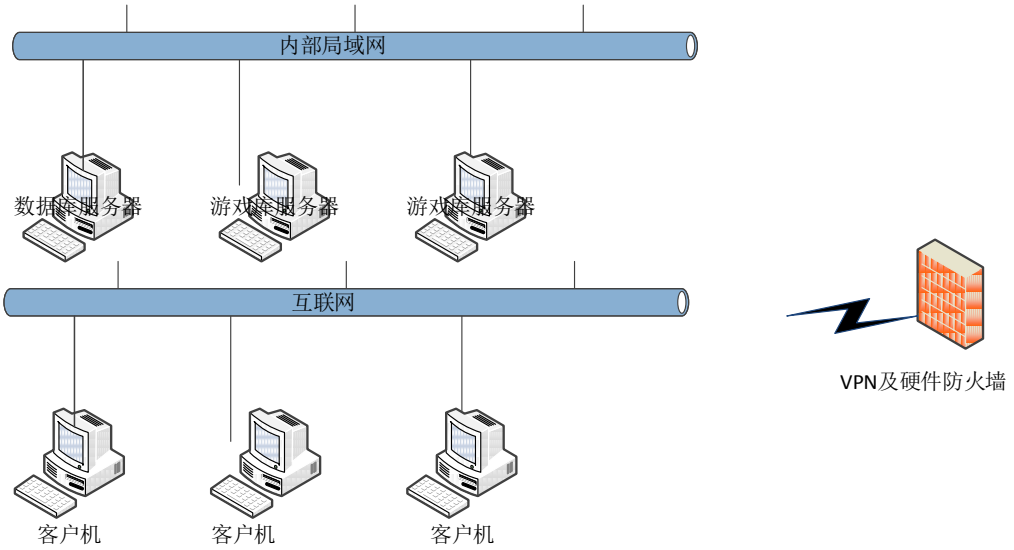

图 3 - 1 网络游戏安全总体分析

3.3.2 用户数据资料保护

用户名以及口令是保障玩家网络游戏虚拟财产最重要的方式，但是以往通常采用固定的口令和密码登录游戏，因此在这个过程中极易产生账号被盗等问题。攻击者只需要在游戏客户端安装相应的木马监控程序便能够在玩家键盘输入面和账号的时候获取玩家信息，并通过木马将相关信息发送到指定的邮箱，玩家账号和面因此而失窃。因此为了解决上述问题，以 qq 为代表的软件首先采用 HOOK 键盘进行密码输入，这样能够通过真假键混合给木马程序造成错误的账号面信息。此方法较为实用，为增强抵抗木马病毒起到一定作用，但是在键盘接口层面依然存在缺陷，攻击者可以通过该缺陷进行信息窃取，所以这样的 nprotect 技术仍然不能完全阻止木马入侵。

静态形式的口令密码因其长期的不变性造成账号泄露风险增大，对于玩家游戏账户和财产的保护作用并不大。因此动态口令能够避免这些安全问题，但是使用动态口令的前提是安装动态口令发生器，因此成本较高，所以并未大规模普及。为了满足当前庞大的手机市场对于安全机制的需求，可以以一种变形动态口令机制代替上述动态口令。以

下是对其进行简单概述：

玩家在账号注册时需要对手机进行验证，当玩家退出游戏时，系统将下次登录密码发送到注册手机上。当玩家再次登录游戏时，将口令输入用以进行哈希函数加密，并通过哈希算法获取客户端哈希值，当计算完成服务器接受玩家登录请求，并进行核准。

服务器端在发送口令时会将口令保存，因此在接收到客户端哈希值后服务器端自动计算哈希值，并将二者进行对比，对比符合则成功登录，如果比对结果不同那么此时会将账号锁定为非法登录。

当玩家进入游戏后，动态口令会在服务器以及客户端同时生成，并会在设定的时间内进行变动。

将动态口令当作密钥进行程序端哈希值计算主要具有以下优势：

（1）动态口令以此使用后便失效，因此木马所盗取的口令已经失去登录效力；

（2）客户端程序能够在哈希值的帮助下进行合法登录，因此能够有效应对外挂；

（3）登陆中所涉及的全部是密文，因此不存在明文窃取密码的行为；

（4）将动态口令进行加密能够有效应对黑客盗取，其特定的格式以及内容不肯轻易被解析，因此对于防止外挂具有良好的作用；

（5）这样的防入侵形式能够有效降低成本，短信服务器构建过程中所产生的费用可以转移到玩家账户，并让玩家自主决定对服务的使用。

3.3.3 团体对抗

网络游戏往往会具有庞大的玩家量，因此它们会相互组件各类团体维护共同利益。因此在团体之间进行交互等行为均会产生较多的安全威胁。因此主要是解决团体代表人的选择以及对方团体诚信度问题，在这其中可能会出现间谍等情况，因此需要着重研究团体内部安全问题。

3.3.4 虚拟财产的保护

互联网与生活和工作融为一体，因此互联网中必然涉及大量的虚拟财产。所有的虚拟财产均具备真实的价值，因此对于此类有价值的虚拟物进行盗窃等行为均属于盗窃罪。正是基于虚拟财产的诞生，许多互联网虚拟产业开始逐渐成型，银行以及电商等均开始逐渐朝着虚拟财产转变。

虚拟财产如果要进行复制，那么并不需要多复杂的操作，如果黑客窃取相关技术会对整个虚拟财产市场造成严重的破坏。无论是运营商还是玩家均会因为这样的行为而承

受巨大的亏损，对于整个网络游戏市场和互联网市场都是致命的打击。但是目前世界上并未采取有效方式保障互联网虚拟资产安全以及不被复制等情况。

本文进行假设，将玩家资产与账户相分离，建立专门的虚拟资产银行用以存放虚拟资产，服务器则主要负责账户信息保存。此虚拟财产银行会将存入的虚拟财产进行编码认证，以此赋予其特殊的地位，这样就能够通过虚拟银行实现财产的唯一和不可复制。要对所有虚拟财产进行认证，关键在于序列号编写，将虚拟财产与序列号进行绑定。

3.3.5 潜信道或阈下信道研究

上世纪七十年代末，美国最早提出用于信息隐藏的阈下信道技术，其原理主要是秘密地将一条信道建立在公共信道当中，用以传输机密文件。

网络游戏联系着世界各国，因此其信道还会涉及到国家战争、恐怖袭击以及其他国际问题。网络游戏能够实现双方秘密互动，主要是基于信道传输序列信息。要相对信道内的信息进行检验和监控十分困难和复杂，因此需要严格掌握信道技术，打击信道非法传输行为。

3.4 攻击技术分析

要想破解网络游戏攻击行为主要从理论和技术两方面进行。对密码进行研究是理论破解的核心，技术破解核心是网络传输环节，主要是在传输过程中将客户端与服务器传输的数据盗取。本文通过研究发现，当前主要以注入非法动态库、网络嗅探以及拦截 SPI 接口等方式进行网络数据截获。

3.4.1 注入非法动态库

在 windows 系统当中，进程与地址一一对应。指针是实现地址和内存之间相互转换的重要工具，将固定的进程安放到固定的内存地址当中。而且各个进城之间并没有固定的联系，所以当某个进程发生错误时并不会影响其他进程。用户以及相关管理人员能够根据独立空间地址进行各自操作，但是外挂等会将 DDL 注入到另外的进程地址空间，一旦成功便能够操纵此进程。

基于上述原因需要将相应的网络数据进行拦截，通过函数 Winsock Api 对数据传输进行检验，一旦发现进程试图操作 API 函数，那么需要将该进程网络数据进行拦截，其中函数中俄李繁多，在此不多举例，主要有 TCP 协议以及 UDP 协议两大类。

3.4.2 对 SPI 接口拦截

Winsock2 主要是提供应用程序编程接口，以及为传输服务和解析服务提供 SPI 接

口。DDL 是传输服务提供者存在的主要方式，其通过固定的函数实现与外部对接，此函数为 WSPStartup，服务者类型主要由 LPWSAPRTOCOL-INFOW 参数决定。一旦网络应用将 socket 进行启动，anemia 会产生三种参数实现应用程序相关功能。WSPStartupup 是调动函数指针的主要方式，以此只需对该函数进行相关修改便能够实现破译。要向获取所有的指针只需要将下层 WSPStartup 函数调动即可获取，然后将中转在底层函数实现。

3.4.3 嗅探技术

嗅探主要有主动和被动的区别，基于数据链层的技术为被动嗅探，只需要对一台计算器进行嗅探便能够获取所有局域网内部的计算机获取的信息。以太网会将收到的报文进行检验，如果需要接受报文则将报文传输给操作系统，不需要则直接忽视。主动嗅探主要是借助 ARP 包进行，自身先生成一个虚拟的 ARP 包，一旦系统报文当中存在一定的隐蔽文件或者账号信息，嗅探器会自动将其获取，此种方式不仅对一台机器造成威胁，还会对局域网内及其造成连带威胁，攻击者借此进行权限非法获取，从而对网络结构进行非法修改。通过上述原因可以看出嗅探器对于整个互联网威胁较大，一旦网络游戏被安装嗅探器，那么客户端与网络游戏服务器之间的交互信息将毫无保留地被盗取，攻击者能够借助嗅探器获取玩家账号和密码等信息。

图 3 - 2 所示为局域网嗅探示意图。

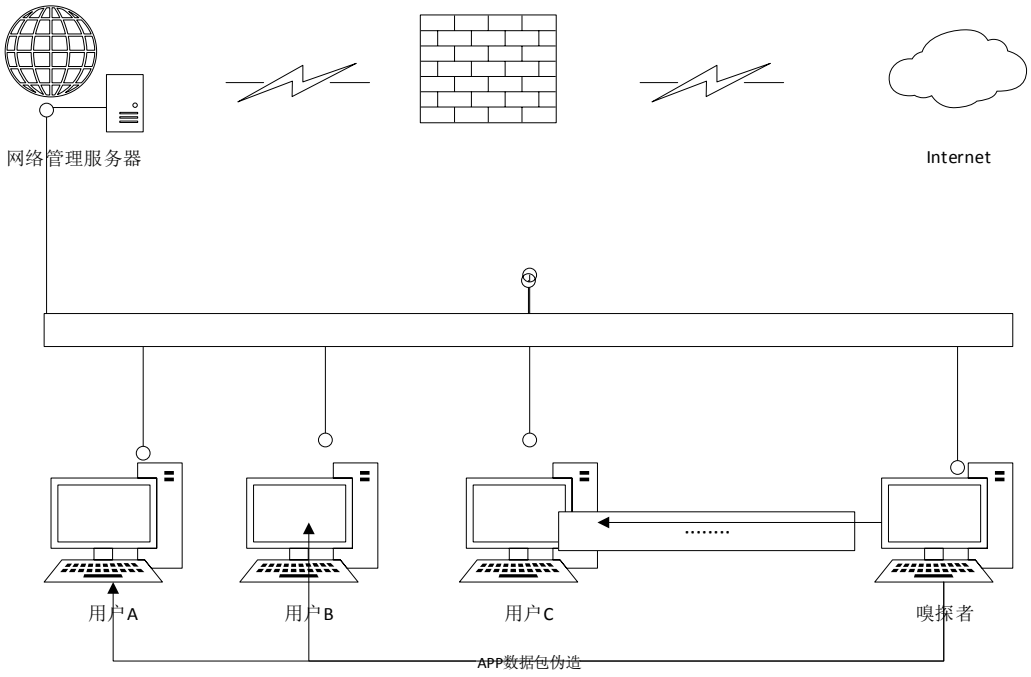

图 3 - 2 局域网嗅探示意图

3.5 本章小结

本章主要是基于当前所存在的网络游戏体系进行研究，对网络游戏安全评估进行模型构建。首先将网络游戏数据环节作为研究重点，对互联网进行安全分析，主要体现在条对传输协议 TCP/IP 等方面进行安全分析，并针对当前网络环境以及网络游戏面临的威胁进行深入探讨，并研究了攻击网络游戏的主要手段和技术。

第四章 网络游戏数据加密算法研究

WSN 加密算法是在 ECC 加密算法的基础上进行改进提出的，可以减少有限域上椭圆曲线的点计算时间以及能耗、计算难度等。

4.1 椭圆曲线的相关理论

在 ECC 密码体制的构造中，其基础部分是韦尔斯特拉斯椭圆公式，其中 F 表示域，a、b 分别表示域中的两个点，其公式为：$y^2+xy=x^2+ax^2+b$，其中 x、y 的值是无穷值。

4.1.1 标量乘计算

在椭圆曲线的计算中，标量乘计算非常重要，其具体实现是，先针对椭圆曲线选择加密计算方法同时在曲线上选择 P 点，并计算其 K 个点乘值，其表达式为：

$$Q = kP = P + P + \cdots + P$$

$$Q = kP = \underbrace{P + P + \cdots P}_{\text{k 个 P 相加}} \tag{4.1}$$

标量乘计算在 ECC 加密实现中是非常重要的，其可以快速提升其计算效率，具体计算包括以下三种：

1、假设 P 值不变，K 值变化，则需要依次进行优化计算、预计算等步骤，并对计算结果进行保存。

2、假设 P 值变化，K 值不变，则需要针对 k（改进标量）进行优化计算。

3、结合上述两种情况进行优化计算。

4.1.2 椭圆曲线加法计算

假设椭圆曲线的有限域值为 F，选择其计算方程为 C，则运用弦和切线理论可以得出，C（F）上 P 点、Q 点两者进行加法计算，其结果等于 R 点，这种加法计算称之为交换群，其具体计算规则如下：

（1）椭圆曲线用 C 表示，假设其上有点 P、Q，其坐标值分别位于（X_1，Y_1）、（X_2，Y_2），则可以计算出 R 点，其坐标值为（X_3，Y_3）。具体如下图 4 - 1 所展示。

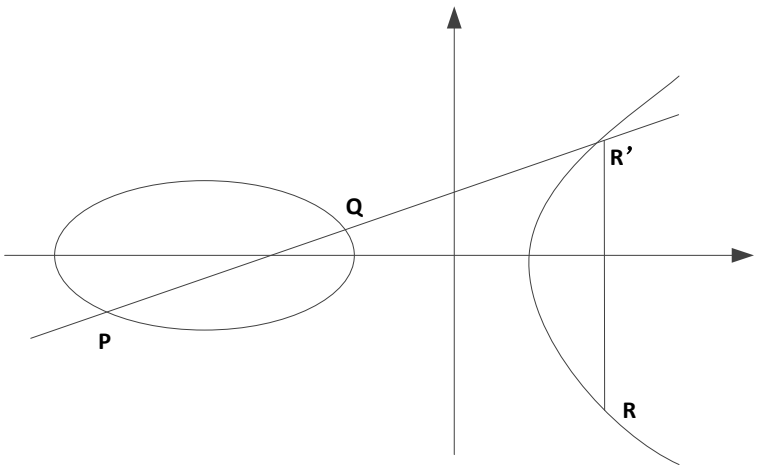

图 4 - 1 椭圆曲线的加点计算

（2）上图中，P=Q，椭圆曲线用 C 表示，假设其上有点 P、Q，其坐标值分别位于（X_1，Y_1）、（X_2，Y_2），则可以计算出 R 点，其坐标值为（X_3，Y_3），即 P 切割了 C，其切割点 R 位于 PQ、C 之间，即 X 的对称点。具体如下图 4 - 2 所展示。

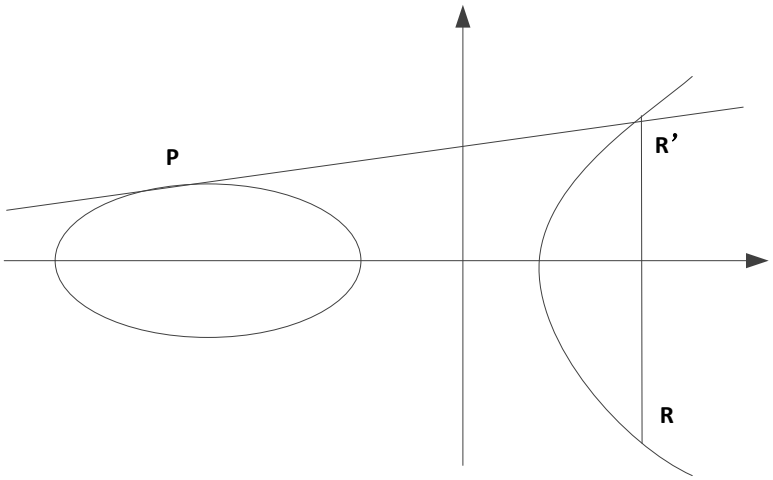

图 4 - 2 椭圆曲线的倍点计算

4.1.3 加法交换群的运算规则

假设椭圆曲线用 E 表示，其上有点 P、Q，则其计算规则分成：

$$\phi : E_C(F_{2^m}) \to E_C(F_{2^m})$$

$$\phi(\infty) = \infty, \phi(\chi, y) = (\chi^2, y^2) \qquad (4.2)$$

$$\Gamma(\phi) = 2, \Gamma(\phi - 1) = 2^{2-C}$$

$$\Gamma(\phi^m - 1) = \#E_C(F_2^m), \Gamma(\phi^m - 1)/(\phi - 1) = \#E_C(F_2^m)/2^{2-C}$$

$$\Gamma_L = \left\{\chi_0 + \chi_1\tau + \chi_2\tau^2 + \cdots + \chi_{L-1}\tau^{L-1} \middle| \chi_j \in C\right\} \qquad (4.3)$$

$$kP = \left(\sum_{i=0}^{L} \mu_i \phi^i\right)P = (\mu_L\phi^L + \cdots + \mu_1\phi + \mu_0)P = \mu_L\phi^L(P) + \cdots + \mu_1\phi(p) + \mu_1 P \qquad (4.4)$$

4.2 改进椭圆曲线算法的参量选择

在进行椭圆曲线加密计算时，需要结合参数 p（椭圆方程系数）、a（椭圆方程系数）、b（椭圆方程系数）、G（（椭圆基点）、n（基点阶）、h（m/n 的整数）进行其曲线 T 的确定。参数的选择对椭圆曲线加密的结果影响非常大，关系到其信息传输的安全、稳定，具体选择条件分成：

（1）P 值的增加虽然可以提升信息加密的安全程度，但同时也会降低其计算效率，因此最优取值为 200。

（2）P 值不等于椭圆基点阶值* （m/n）的整数值

（3）pt 不等于 1modn，其中 t≤20 且≥1。

（4）$4a^3+27b^2$ 的加法计算结果不等于 0。

（5）N 值小于或等于 4 且等于素数。

4.3 改进 ECC 加密计算

1）环境初始化及密钥生成

假设椭圆域值用 F_2 表示，曲线用 T 表示，则其 N 值（素数阶）的对应点值 G 的坐标值为（X_P，Y_P），其私钥 D、公钥 PK 的值分别表示为[1，n-1]、dG。

2）加密实现

（1）完成 B 节点公钥 PK_B 的查找

（2）椭圆域值用 F_2 表示，其上的信息元素用 M 表示，则 M 归属于 F2 中。

（3）整数 K 值由随机方式进行产生，其值在范围为[1，N-1]。

（4）对点 KG 进行计算，其坐标值用（X_1，Y_1）表示。

（5）对点 KPK_B 进行计算，其坐标值用（X_2，Y_2）表示。

（6）对 C 值进行计算，其值为 MX_2。

（7）向 B 节点进行加密信息的发送，其内容为（X_1，Y_1，C）

3）解密实现

（1）针对（X_2，Y_2）点使用 PK_B 公钥进行解密，而针对（X_1，Y_1）点 d_b 则使用 d_b 私钥进行解密。

（2）针对信息 M 值的恢复通过 CX_2^{-1} 进行计算实现。

改进 ECC 加密计算实现流程设计如下图 4 - 3 所展示。

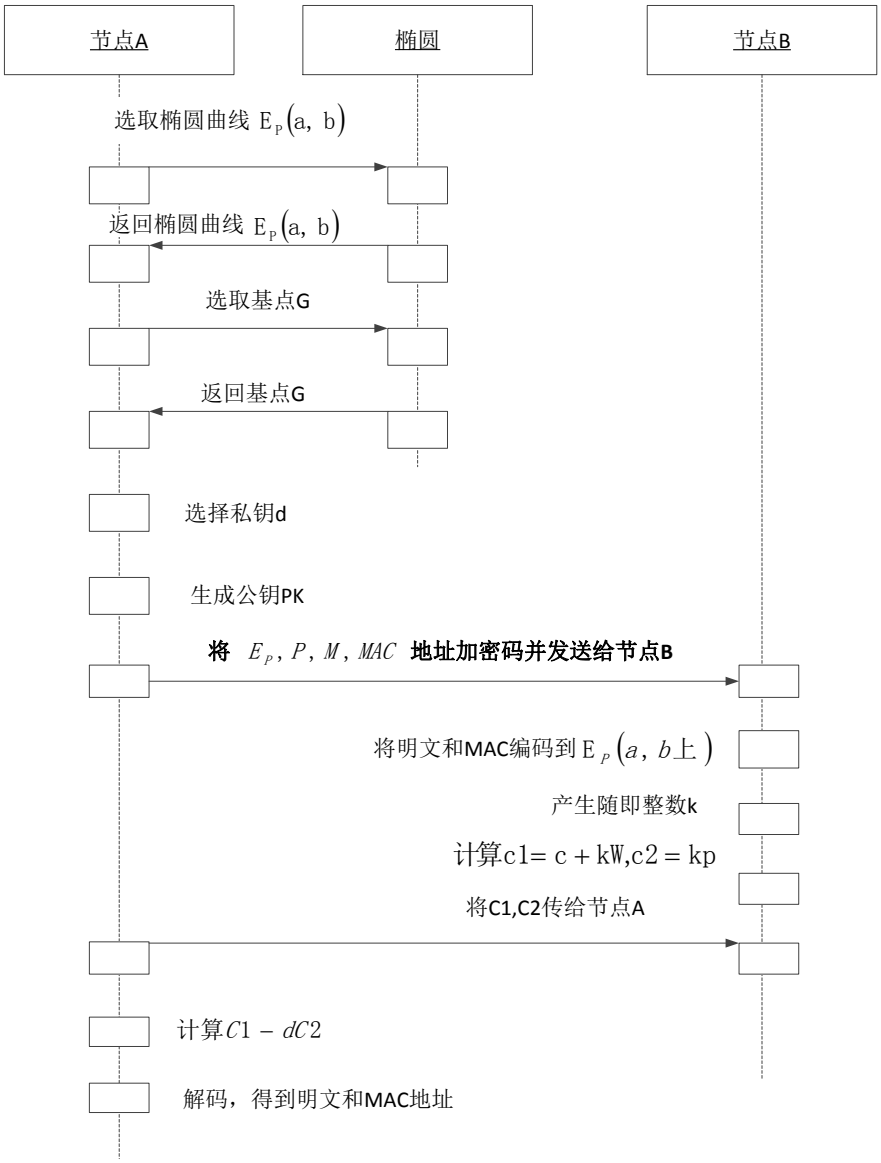

图 4 - 3 改进 ECC 加密计算实现流程图

4.4 改进 ECC 加密计算实现的难点

在改进 ECC 加密计算实现中，其最重要的是标量乘的改进，存在离散对数逆运算难点，主要分成加法计算实现（公式 4.5 和公式 4.6）、倍乘计算（公式 4.7 和公式 4.8）实现。

$$x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \quad (4.5)$$

$$y_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3) - y_1 \quad (4.6)$$

$$x_3 = \left(\frac{3x_1^2+\alpha}{2y_1}\right) - 2x_1 \quad (4.7)$$

$$y_3 = \left(\frac{3x_1^2+\alpha}{2y_1}\right)(x_1 - x_2) - y_1 \quad (4.8)$$

4.5 标量乘计算

4.5.1 二进制的传统算法

在传统变量计算中，常使用二进制算法，在下面列举的公式 4.9 中，展示了传统二进制的算法表达式 K[40]。

$$k = \sum_{l=0}^{l-1} k_i \cdot 2^i = k_0 + k_1 \cdot 2 + \cdots + k_{l-1} \cdot 2^{l-1}, k_i \in \{0,1\} \quad (4.9)$$

$$kP = [k_0 + k_1 \cdot 2 + \cdots + k_{l-2} \cdot 2^{l-2} + k_{l-1} \cdot 2^{l-1}] = 2[\ldots 2[2(2k_{l-1}P + 2^{l-1}P) + k_{l-3}P] + \cdots + k_1 P] + k_0 P \quad (4.10)$$

传统算法针对点的加法二进制计算时，要求其 K 展开式中的复杂度与位数不等于 0；而传统算法针对椭圆点倍乘二进制计算时，要求其 K 展开式中的复杂度与位数值相同。假设在 K 表达式中，其值为随机产生，同时与 0、1 位数一致，那么进行平均计算时，其 1 倍点值同平均点值的加法计算表达式等于：

$$\frac{1}{2}A + lD \quad (4.11)$$

传统的二进制算法在标量乘计算中，其计算变量会随着值的增加而降低计算效率及性能。

4.5.2 窗口 NAF 算法

在标量乘计算中，使用最广的计算方法包括滑动窗口计算方法 M-进制计算方法等等，其属于在标量乘传统计算方法上进行改进实现的。在改进实现中，假设标量乘传输信息块的计算宽为ω，且大于 1，这种以传输信息块宽进行计算的方法，称之为标量乘窗口算法。

而结合标量乘窗口算法、NAF 二进制算法，得出了窗口 NAF 算法，该算法在计算中，K_I 不等于 0 且为奇数，当ω值连续出现时，其值除 1 位非 0 值外，其余全等于 0，其 NAF 长用ι表示，其 NAFω（K）的计算实现如下：

表 4-1 实现情况步骤 1

假设条件	其中 NAF\omega（K\iota -1……K\iotaK0）=(K) 先预计算 NAF \omega 的值，K 值（正整数），
输入	预计算的值\omega、K
输出	窗口 NAF 算法值 NAF\omega（K）

判定	（1）假设 I 值等于 0 （2）假设 K 值大于或等于 1 时，则执行循环计算 假设 K 值为奇数时，其 kmod2\omega 值与 KI 值一致，则 K-KI 等于 K 值 假设 K 值不是奇数时，则 KI 值为 0 即 2.3 K 与 K/2 的值一致，而 I+1=I 值。 （3） 值返回

表 4-2 实现情况步骤 2

假设条件	标量乘值为 KP，其计算表达式等于 ，其中 K 是整数，其窗口 NAF 算法计算 KP
输入	计算的窗口值\omega、K
输出	窗口 NAF 算法值 KP
判定	（1）窗口 NAF 算法计算的 NAFω（K）值的表达式为：$\sum_{l=0}^{l-1} k_i 2^i$ （2）假设 i 值范围等于｛1、3、5……$2\omega^{-1}$-1｝，则其 P_l、IP 的计算结果一致。 （3）Q 值返回 假设 NAFω（K）的长用ι表示、宽用ω表示，则其计算结果约有 1/（ω +1）机率不等于 0，假设其ι值大于 K 的展开值等于 1 时，其针对窗口 NAF 算法的时间复杂度计算表达式为： $[lD + (2^{\varpi-2} - 1)A] + \left[\frac{m}{\varpi+1}A + mD\right]$ （4.12）

4.6 性能评估

针对 ECC 传统加密计算方法中的倍点计算，是通过二进制传统算法进行实现的，通过对该算法进行改进，在椭圆曲线的点加计算中，其计算次数降低至 3N/2 次，在信息的传输中，可同时实现信息、MAC 信息的传输，提升了信息加密计算的效率，实现了信息的安全、稳定、高效传输。为此，本文还建立了模拟仿真 matlab7.1 实验平台，针对其算法的结果，进行了综合性能的分析与评价。

4.6.1 安全性分析

信息通过传感器节点进行传输时，由于节点存在计算能力弱、储存空间不足等劣势，

因此限制了信息加密的长度值。Certieom 企业在 ECC 算法实验中，通过实验得出，该算法的密钥长度短，对带宽、储存要求低，传输安全性高，有效地改进了 WSN 算法的不足，其在信息的破解防范上，优于其它算法，具体如下图 4-4 所展示。

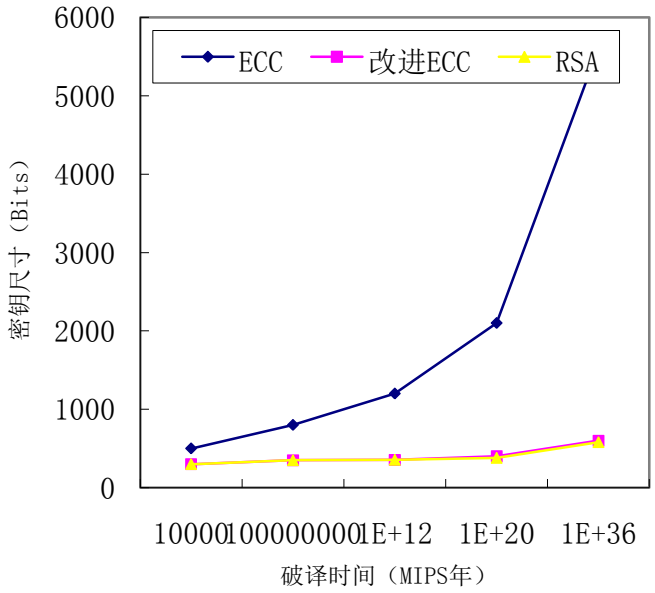

图 4-4 密钥破译实验结果对比图

在图 4-4 中，展示了 ECC、改进 ECC、RSA 三种加密算法在密钥破译安全性上的实验结果对比图。其中密钥破译时间小于 1000bits 时，三种加密算法的安全性都较高，其空间复杂度变化大致相同，而当密钥破译时间增加时，则三者的空间复杂度发生了不同的变化，可以看出改进 ECC 算法的表现最优。按照图中的表现趋势，随着时间越长，密钥的变化性越强，进而越能增加系统的安全性。

4.6.2 算法效率分析

在下图 4-5 中，展示了 ECC、改进 ECC、RSA 三种加密算法的加密时间、数据包的复杂度变化对比图，从图中可以看出，改进 ECC 算法计算结果最优，其计算效率量高、耗时量少。

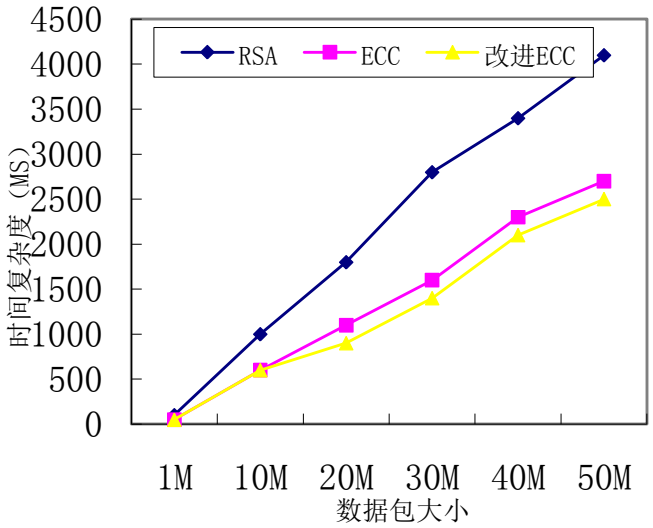

图 4-5 加密算法效率实验对比图

4.6.3 算法能耗分析

通过算法能耗的理论分析，其与算法时间的复杂度变化间存在密切的关系，即时间复杂度高能耗高。为此，本文针对 ECC、改进 ECC、RSA 三种加密算法的能耗展开了分析，其能耗分析结果从高到低排列依次是 RSA 算法、ECC 算法、改进 ECC 算法，可见改进 ECC 算法的计算结果最优。

4.7 本章小结

本章节先详细描述 WSN 改进的方案，并阐述了其替代的意义、验证码、范式 Frobenius 等，接着详细介绍了改进 ECC 加密算法，并介绍了其使用的领域，最后针对 ECC、改进 ECC、RSA 三种加密算法的安全、能耗、效率等计算结果进行了仿真实验、对比、分析，得出改进 ECC 算法的计算结果最优。

第五章 基于 AES 与 ECC 的游戏数据混合加密算法实现

在融合了 AES、前一章改进后的 ECC、HMAC 等计算方法优势的基础上，提出了混合加密算法。该算法从计算效率提升方面进行考虑，同时确保了信息传输的高安全性需求，在数据包的加密安全实现上，采用了高安全性的对称加密算法 AES；在密钥的密秘分配管理上，采用了公开性较好的 ECC 非对称加密算法；在信息签名及认证的安全性实现上，采用了 HMAC 算法及 ECC 算法。因此，混合加密算法结合了上述三种算法的优势，在网络信息的安全传输中，能实现信息传输的高安全性需求、高传输效率需求以及完整性需求，并大量降低了传输能耗。为此，本文针对混合加密算法进行了可行性验证，确定验证环境为 win7 ms visual studio 2008(c++)，验证了信息在无线传感器中的网络传输效果，其结果表明，优于 ECC、RSA 等加密算法。同时，结合加密算法，在原有基础上，设计了《深海游击队》系统，以说明系统应用的可行性。

5.1 游戏需求分析

5.1.1 功能性需求分析

《深海游击队》这款游戏属于休闲娱乐类，主要玩法在于寻宝与捕鱼，玩家通过对直升机进行操作进而完成寻宝与捕鱼的目的。每当玩家捕捉到鱼类或者搜寻到一些宝物，那么这些物品所对应的积分就会给予玩家，并不断进行叠加。在这个过程中，直升机的油量往往是决定游戏进度的最大因素，一旦油量用完，那么游戏就会自动结束，在捕鱼的过程中，玩家可以对一些特殊道具进行使用来对直升机的油量进行补充。但是在游戏过程中，炸弹与鲨鱼可以大幅度地将直升机的油量减少，当出现的炸弹与鲨鱼过多时，可能直接使得直升机油量耗完进而结束游戏。

游戏功能的主要要求是以下几个方面：

（1）游戏界面

与同种类的电脑游戏相同，本项目游戏对游戏过程中出现的各类声音要素与动画要素进行了综合，玩家在游戏中的基本感知就是从中予以获取。所以，游戏最重要的一部分内容就是游戏的界面设计，玩家对游戏的接受程度及其感知都直接取决于游戏界面。《深海游击队》对多种卡通与动画要素进行了综合，使其体现在游戏界面中，真正地让玩家在过程中感到轻松与有趣，使得他们做到真正的娱乐，对于大部分玩家的口味而言其都是符合的。

（2）操作方式

本游戏的操作方式是玩家在游戏汇总通过各种方法与角色进行全方位的交互。在当前所有的智能手机中，基本上其能够运行全部的热门游戏，而手机游戏最为主要的操作方式也变成了触屏操作。这是因为触屏操作具有简单快捷、自由方便的优势，可以最大化地将玩家的游戏体验予以提升。本游戏除了对触屏的操作方式进行使用，也对游戏的控制键进行了精简，玩家只需要对两个方向按钮及一个吊钩操控按钮进行控制就能够实现游戏的操作，可以说是相当的便捷了。

（3）游戏趣味

对于一款游戏而言，要想将消费者的注意力吸引并使他们对游戏的接受度得到增强，那么游戏的趣味性就必须足够丰富。通过有关统计，目前玩家最喜欢的热门游戏类之一就是寻宝与捕鱼类的游戏。而传统捕鱼类游戏的所有优点都在本游戏中得到了综合，并且开发者基于此来最大化地将游戏的趣味性予以提升，使得玩家可以在比较轻松的氛围中感受到游戏的乐趣，同时在游戏过程中也不缺乏应有的刺激与紧张。

（4）游戏时间

游戏时间指的是玩家操作游戏进行娱乐的总的时间，而玩家的游戏次数与接受程度则直接取决于游戏时间的长度。长时间上班并且没有整体的游戏时间的上班族是手机游戏的主要受众，因此玩家多是利用闲散的时间来进行游戏。所以在开发本游戏项目时，针对此种情况进行了有关设计，提供了较短时间的单局游戏，将保存游戏、继续游戏、暂停游戏的功能提供给了玩家，使得他们能够随时随地开启游戏之旅，将最好的用户体验予以提供。

5.1.2 用户需求分析

上班族是本游戏项目的主要受众，因为他们长时间上班而没有整体的游戏时间，并且生活节奏较快，压力也较大。而本游戏能够使得他们在闲散的时间中感受到游戏的快乐与轻松，进而将压力予以释放，是他们不可多得的娱乐选择。

5.1.3 非功能性需求分析

本游戏项目的开发是基于 IOS 平台实现的，平台的硬件条件会限制应用程序的运行。由于有大量的画面种类与动画元素包含在本游戏中，在运行游戏时必须有着较高要求的屏幕清晰度及电脑显存，若是屏幕的分辨率与像素不够高，那么游戏的体验感将会大幅降低。要想较好地运行本游戏，设备必须具备 128M 以上的内存，并且设备的系统版本不能高于 IOS13。游戏的开发程序受限于 CORONA 的研发进度，下面将提供有关

操作系统与电脑硬件的需求：

操作系统：可以使用 Vista、MAC7 及 Xp 系统；

处理器：不能低于 1GHZ 的处理频率；

硬盘空间：必须高于 40MB；

内存空间：必须高于 2G；

图像处理系统：不低于 OpenG11.3；

5.2 系统总体设计

在开发设计《深海游击队》这款游戏时，对苹果公司的引擎技术进行了整体使用，引擎模拟器选用了 CORONA，而编辑器则对 SCITE 进行了应用，实现了在 MAC 体系下载编译源文件的功能，进而将可执行的文件.APP 予以获取，接着在 IOS 设备中进行安装并完成有关的测试工作。通过以下流程完成了本游戏项目的开发与设计工作。

5.2.1 系统设计

本游戏项目的操作阶段由五个部分所构成，具体可见下图。

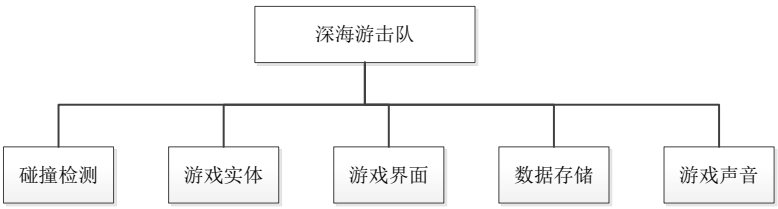

图 5 - 1 《深海游击队》层次图

从上图中我们可以获悉，游戏的逼真效果通过游戏声音的作用来予以提升，进而衬托游戏的各个环节；而信息储存主要指的是记录玩家在游戏过程中的各种信息，游戏分数及玩家等级等都包含其中；借助相关的操作界面，玩家可以对游戏场景进行切换，而海底的各类鱼种及各类捕捞设备等都存在于游戏实体中；对捕捞操作的成功与否的检验需要由碰撞检测来予以实现。具体可以见下文。

（1）游戏界面

调节音频、得分记录、游戏的完成、暂停及开始等都包含在游戏的界面之中。而得分条、控制条及游戏环境设置等包含于界面栏中；在其他的界面栏中又包括了功能性按钮、界面提示及广告去除等。游戏的具体界面层次可见下图。

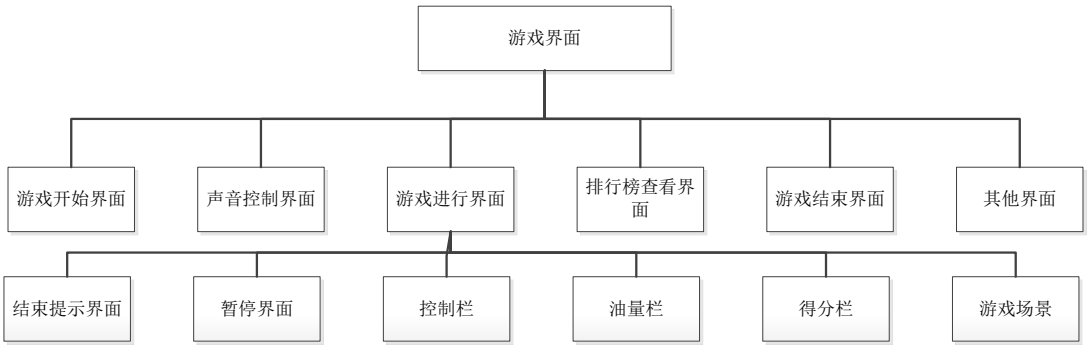

图 5-2 游戏界面层次图

（2）游戏实体

在游戏过程中出现的所有角色，如宝藏、精灵、打捞设备及各类海底生物等就是指的游戏实体。

（3）存储数据

在本游戏项目中，玩家在游戏过程中所产生的各种信息及游戏的基础性配置配置信息等都包含在有关的数据之中。游戏程序对不同的储存器进行了应用，通过不同的软件实现储存游戏所有开发资料数据的功能。

（4）游戏声音

对于一个游戏而言，声音与音效是其最为关键的构成要素，只有通过这两者的有效结合才能将身临其境的逼真体验提供给用户。在 IOS 平台中，其对 WAV、AAC、IBLC、IMA4 及 MP4 等多种音频格式都提供了支持。在本项目中，背景音乐与声音特效两部分共同构成了声音这一项目。

（5）碰撞检测

游戏的碰撞检测是游戏研发后期最为关键的一个项目。在本项目的碰撞检测中，对包围盒子法进行了应用。所谓包围盒子法，指的是通过一个虚拟的盒子来包围所有的精灵，通过此过程来对各个精灵盒子中是否有重合情况的存在进行验证。若是重合不存在，就表示碰撞是不存在的。下图具体呈现了鲸鱼与海豚这两类游戏实体的碰撞检测流程。

图 5-3 碰撞检测包围盒

在碰撞检测项目汇总，既能够检测游戏游戏和实体是否出现了碰撞，也可以对碰撞的后果及其具体的时间等要素进行检测。通过这一流程，可以及时地发现游戏设计过程中的薄弱环节，进而及时地优化并改善这一环节，最终将玩家的游戏体验与游戏的品质予以提升。

5.2.2 框架设计

结构设计的关键之处在于，用相互独立但是又具备联系的单独的个体来划分较为复杂的软件体系，在综合了每一个独立个体的实际功能之后将软件的工作效率予以提升。对体系的构成与工作流程记性详细地了解之后，就可以开始设计、开发、优化、升级游戏系统了。在本项目中，对系统进行修改与优化的权限包含在软件框架中。下图呈现了本游戏项目的具体结构设计流程：

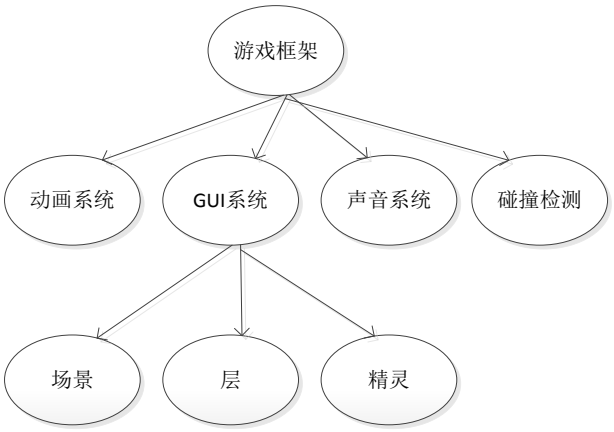

图 5 - 4 游戏框架设计

我们对 GUI 体系进行了应用来实现整个游戏的界面设计，从下往上，分别对 LAYER/SPRITE 等游戏组件进行使用来完成游戏界面设计。下图呈现了精灵与各层之间的关系：

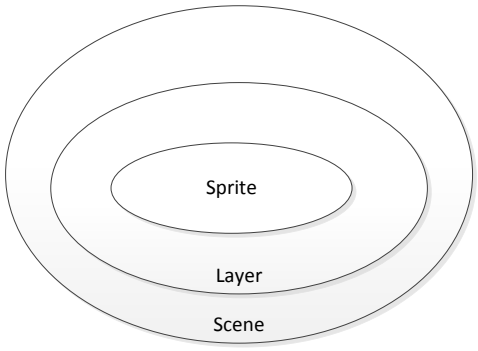

图 5 - 5 精灵、层和场景之间的关系结构

5.2.3 数据持久化

在本体系中，游戏数据的持久性可以通过 PLIST 格式与 SQLITE 体系来进行加强。对于游戏中不同的场景部分而言，其难易程度也是有所差异的，而信息的持久化通过 PLIST 来予以实现。

（1）游戏的配置数据

由于休闲益智类游戏是《深海游击队》的类别，所以我们必须基于游戏的级别与关卡来对有关的参数进行配置。在配置文件中，数组位于第一层。我们以信息的从属关系及其类型为基础，对游戏的配置界面的文件进行了设计。

（2）玩家数据

通过具体地分析本游戏项目的特性，我们使用了沙盒类文件夹来对玩家的有关数据进行储存，比如玩家的星级、实际得分、最高分及直升机油量等信息都包含在其中。

5.3 系统详细设计与实现

5.3.1 游戏主程序

在设计本游戏项目时，我们在游戏的框架搭建过程中应用了 CORONA 技术，而此框架还有一个别名叫 StageObjec，因为在创建对象时，体系会在组对象的架构层的顶端将其自动保存。在游戏框架中，其会在 stage 内增加每一个新加入的对象的组对象，并且其会自动地排列在全部组对象之后。所以其通常会最先在界面中得到显示。

我们将游戏研发时有关重点类的归类操作予以完成，详细的流程为：

1、 设置程序设计类中的“精灵”类别

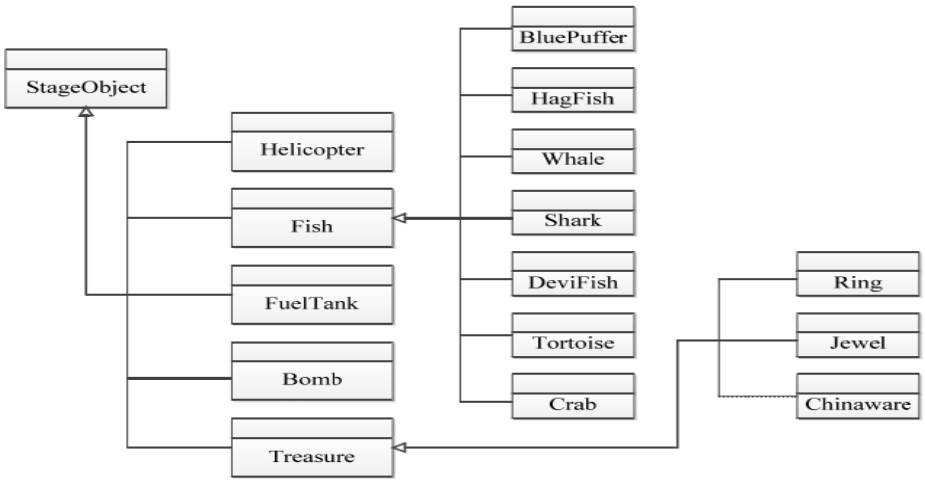

图 5-6 “精灵”类设计中的架构图

从上图中我们可以获悉，其具体的呈现了“精灵”类的结构设计，此架构中的内容及其各项目之间的联系都清楚的在图中进行了呈现。

2、游戏操作中的按键类设置

在游戏的画面设置中，设置了油耗按键、分数按键及游戏控制的各种方向键，具体可见下图：

从上图中我们可以获悉，其主要展示了游戏操作的按键类设置，其中，对游戏内容的分类工作进行设置的是 ScoreBar，其主要用于呈现用户的分数及游戏的进度等信息；而其它各项都有其具体的功能设置内容。

3、游戏中的场景设置

设置游戏的场景是一款游戏研发的主要项目，不同的场景设置会在不同的游戏环节中得以体现，而在设置游戏场景时，需要以游戏的内容为基础，并将其呈现在游戏画面中，进而将与游戏者的互动予以实现。在本项目中，基于游戏的内容具体地划分了游戏的场景类，并用不同的小层级来细分了不同类的场景，同时完成了不同层级之间的连接联系，最终将一个动态的场景予以构成。具体可见下图。

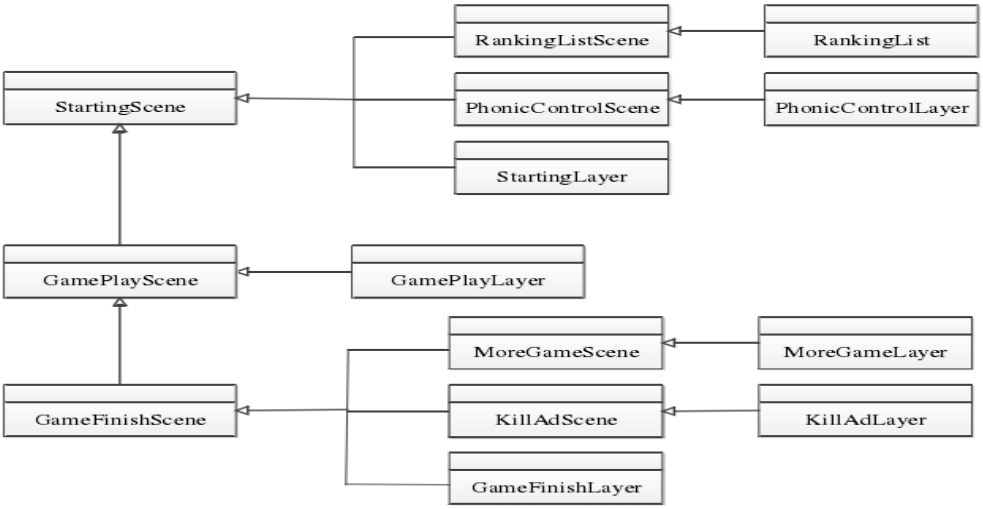

图 5 - 7　游戏中不同场景的类和它的层级图

5.3.2　Plist 游戏的读写

管理游戏的内容及游戏过程中的有关数据是游戏的读写研发设计的主要内容。资料记录、信息更改及信息获取等都包含其中。

在游戏过程中，游戏内容与游戏环境是不会影响游戏的读写功能的，其通常具有固定的表现形式。

从下图中我们可以获悉，游戏场景的层级的呈现是 MyShareData 类，其在信息库中被使用较多，主要用于对游戏过程中玩家的排名、等级及其得分等信息进行记录与存储，同时其会基于自身的特性来自主操作这些信息，比如修改其中的一些数据等。

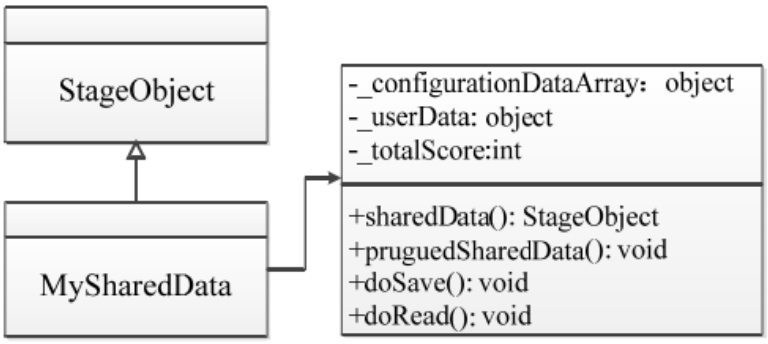

图 5 - 8　游戏场景中 MyShareData 的类

5.3.3　精灵动画的设置

在设计精灵动画时，首先应当完成制作动画图片的工作，这样才可以通过显示方法呈现动画图片进而将动画的功能予以实现。具体可见下图。

图 5 - 9 精灵动画中的图

在本项目中，下图为制作游戏精灵动画的过程，在过程中通过 LUA 码来进行编写，在体系内储存已经制作完成的动画图片，并借助一定的计算来动态地展示图片是其主要的功能。

图 5 - 10 游戏中八爪鱼的动画编写

从上图中我们可以获悉，在编写游戏中的八爪鱼动画时，每当编写完成一个动画画面，体系中就有一个 LUA 脚本文件生成，一张动画中的一张图是这个脚本文件的实质。我们基于不同的归类方法在体系文件中储存全部已经制作出来的动画图片。在体系内同时保存了动画图片及有关程序。

5.3.4 声音系统的设计

本项目对于特效音乐与背景音乐的整体性与协调性尤其看重。首先我们应当对背景音乐进行考量，接着才是对特效音乐进行设计。从技术上来说，本项目使用了 CORONA 的音频体系来加载游戏的声音。

下图具体地呈现了本游戏项目中所需的音效列表。

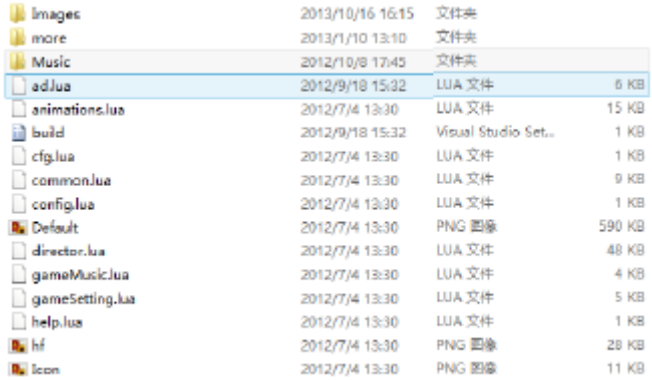

图 5 - 11 《深海游击队》游戏音效

5.3.5 碰撞检测设计

在对游戏的过程进行设计时，应当对精灵之间是否有碰撞存在进行反复检测，若有接触出现在其连接面之间，就说明碰撞是存在的，对于这一类的问题需要对 began 函数进行调用来予以解决，具体可见下图。

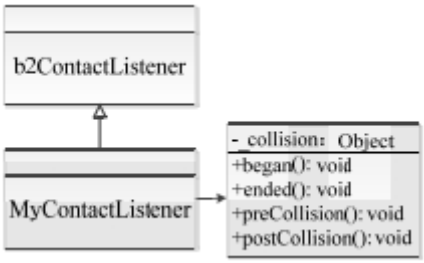

图 5 - 12　碰撞监听类类图

5.3.6　算法详细设计

混合加密算法在信息加密传输中，结合了 AES 算法、ECC 算法、HMAC 信息认证的优势，其具体架构设计如下 5-13 所展示。

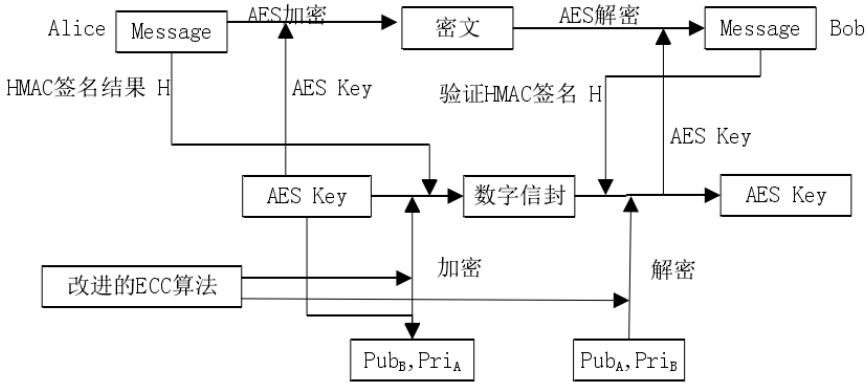

图 5 - 13 混合加密算法的架构设计展示

混合加密算法针对明文信息的加密传输，既考虑了 AES 算法传输效率高的优势，也考虑了 ECC 算法传输安全性高、密钥传输的优势。因此当明文信息进行传输时，采用了 ECC 算法进行加密，利用该算法的公钥及随机方式下生成的会话密钥完成信息包的加密，确保信息安全、有效地传输实现。

混合加密算法在计算中，分别择优选择了 AES 算法、ECC 算法的 128 比特、256 比特以及函数 HMAC，可实现明文信息 C 在加密传输过程的防破译保护，提高安全性，防止非法侵害。

（1）　HMAC 散列算法

在 MD5 算法、SHA-1 算法的研究基础上产生了以信息认证为主的 HMAC 算法，该算法在计算信息摘要时，采用了二次散列迭代计算，其中密钥用 k 表示，信息用 m 表示，散列函数用 h 表示，补齐用 o 表示，序列用 opad、ipad 表示，异计算用⊕表示，连接用 l 表示，具体表达式为[47]：

$$HMAC(K,M) = H(K \oplus opad \,l\, h(k \oplus ipad \,l\, m)) \qquad 5.1$$

在下图 5 - 14 中，展示了 HMAC 算法的结构设计及具体描述。

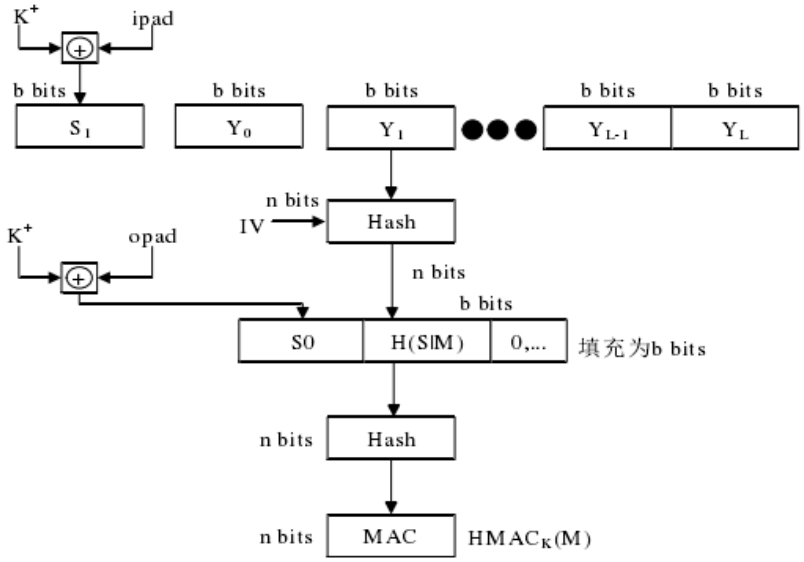

图 5 - 14　HMAC 算法的结构设计

具体描述：

1）新建序列组长要求等于 b bits，如低于组长要求采用 0 进行补位。

2）异计算新建序列与 ipad 序列。

3）针对异计算结果，接收信息 M。

4）运用散列函数计算 M 摘要值。

5）异计算新建序列与 opad 序列。

6）针对异计算结果，接收摘要信息。

7）运用散列函数计算，完成信息认证。

由于 HMAC 算法针对函数 hash 值域变化影响、缺陷影响等进行了考虑，其密钥可随机产生、更新，提升了信息传输的安全性[48]。

数字信封加密计算针对对称加密、公钥加密的优势、劣势进行了综合、取长补短后提升了算法的性能及信息的传输安全[49]。其具体实现分成：

1）通过对称加密，随机进行会话密钥生成，并完成信息 WSN 的加密。

2）传输 ECC 公钥到接受节点，完成信息 AES 加密，生成密钥。

3）向各信息接受节点进行会话密钥的发送。

4）接受节点接收并通过私钥解密获取 AES 密钥，通过密钥解密加密信息形成明文信息，完成信息安全传输。

其发送、接收节点的加密、解密表达式分别如 5.2、5.3 所展示[50]。

$$C_1 = E_{KAES}(M)$$

$$C_2 = E_{KPB}(M_{AES}) \qquad (5.2)$$

$$K_{AES} = D_{KSB}(C2)$$

$$M = D_{KAES}(C_1) \qquad (5.3)$$

（2） 混合加密算法设计

1）明文加密设计：AES 算法加密明文 M 形成加密文件 C 及密钥 KA。

2）密钥设计：ECC 算法加密密钥 KA 形成密钥模块 AES。

3）信息认证设计：HMAC 算法签名明文 M 得出明文摘要。

4）接收节点 B 同时接收加密文件 C、密钥模块 AES、签名信息。

在下图 5 - 15 中，具体展示了加密设计流程。

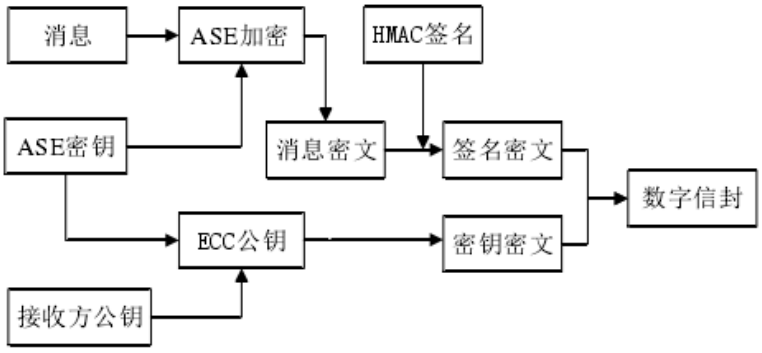

图 5 - 15 加密设计流程展示

1）解密密钥设计：ECC 算法完成密钥模块 AES 的解密获取密钥 KA。

2）解密密文设计：加密文件 C 通过密钥 KA 进行解密形成明文信息 M。

3）验证信息的签名，根据接收的摘要信息对比发送的摘要信息，验证其一致性，信息一致表明其传输安全。

在下图 5 - 16 中，展示了解密设计流程。

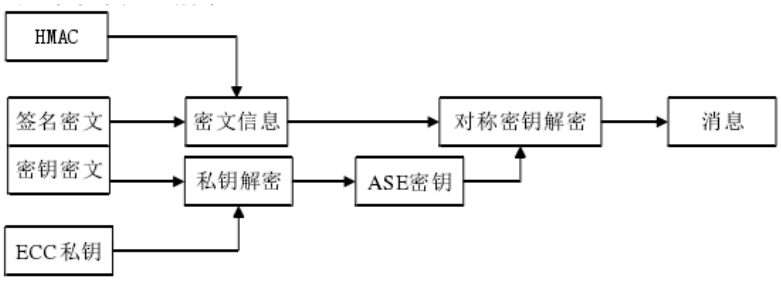

图 5 - 16 解密设计流程展示

WSN 通信加密传输的安全设计核心是确保公钥的交换安全，同时信息在网络传输

中需要遵守公钥交换标准 PKI，该标准比较复杂。为了安全地实现 WSN 信息加密传输，在本文中，运用 ECC 算法替代 RSA 算法来简化复杂的 PKI 公钥交换实现。

5.3.7 系统的主要接口及模块

（1）ECC 算法的 EccEncryptor()加密模块

EccEncryptor()加密模块可实现 ECC 密钥的自动生成、保存，同时接收节点公钥完成会话密钥加密，如下图 5 - 17 所展示。

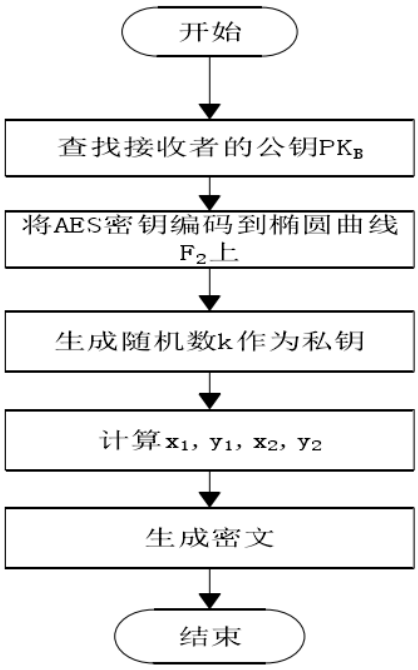

图 5 - 17 ECC 算法的加密实现流程展示

EccEncryptor()加密模块接口包括：AES 会话密钥加密时间输出接口 EccEncryptor：：generateKey(const std：：string& name)、ECC 的私钥接口 CryptoPP::ECIES<ECC ALGORITHM>::PrivateKey PrivateKey 、ECC 的公钥接口 PrivateKey .MakePublicKey(PublicKey)、密钥编码接口 CryptoPP::HexEncoder priEnc()。

（2）ECC 算法的 EccDecryptor(const std::string&to)解密模块

在下图 5 - 18 中，展示了 ECC 算法的解密实现流程，该模块的功能是通过接收节点公钥、装载私钥来解密 AES 的会话密钥。

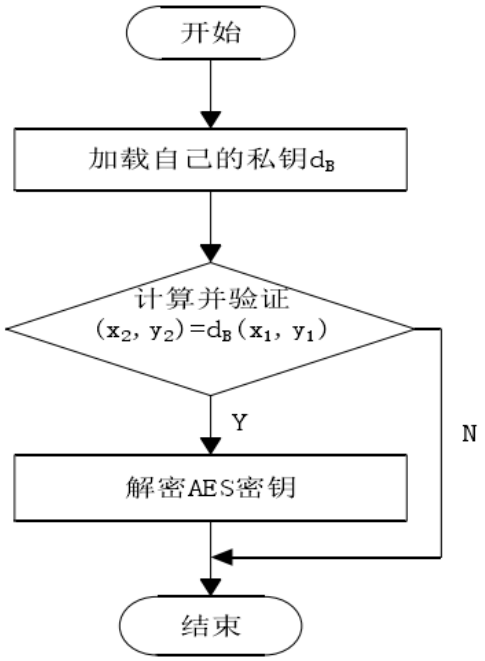

图 5 - 18 ECC 算法的解密实现流程展示

EccDecryptor(const std::string&to)解密模块接口包括：私钥编码接口 FileSource pubFile(priFilename.c___str(),true,new HexDecoder) 、参数加密接口 decryptor.Decrypt(mg,reinterpret _cast<const unsigned char *>in.c _str()),inlen,outBuf)。

（3）AES 算法的 AesEncryptor()加密模块

在下图 5 - 19 中，展示了 AES 算法的加密实现流程，该模块的功能是针对信息的节点发出方、接收方面，完成两者间信息传输的加密。

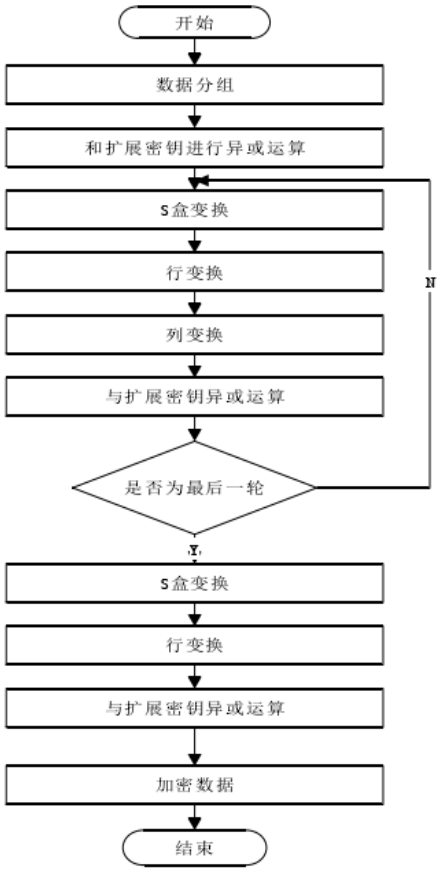

图 5 - 19 AES 算法的加密实现流程展示

AesEncryptor() 加密模块模块接口包括：密钥发布接口 vid AesEncryptor::updateKEY()、HexEncoder 密钥编码接口 AesEncryptor:;key()、HexEncoder 向量编码接口 AesEncryptor::in()、AES CTR 信息加密接口 AesEncryptor::encryptFile(const std::string&in,const std::string&out) 、 Stream TransformationFilter 过滤包装接口 FileSource(in.c_str(),true,new StreamTransformationFilter(aes,new FileSink(out.c_str()))。

（4）AES 算法的 AesDecryptor()解密模块

在下图 5 - 20 中，展示了 AesDecryptor()解密模块的实现流程，具体分成：

1）在 AES 算法中，会话密钥 key 由系统随机产生并完成信息向量 iv 初始化。

2）通过 key 加密明文信息。

3）信息发送、接收双方在随机方式下，进行密钥 ECC 生成。

4）ECC 公钥被 WSN 节点获取并加密 key。

5）向 WSN 节点发送加密后的 key 及加密明文。

6）WSN 节点收到 key 并通过私钥解密获取 AES 密钥以及 IV。

7）利用获取的密钥解密加密信息。

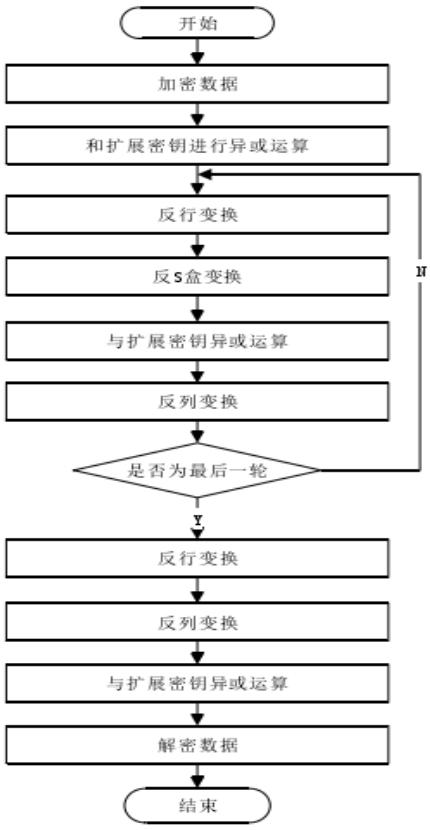

图 5 - 20 AES 算法的解密实现流程展示

在 AES 算法的解密实现流程中，其接口 AesDecryptor::setKey 的功能是使用编码器 hexEncoder 按十六位进制对 key、iv 进行编码、转换，完成输出。

5.3.8 游戏实现

在对游戏的过程进行设计时，应当对精灵之间是否有碰撞存在进行反复检测，若有接触出现在其连接面之间，就说明碰撞是存在的，对于这一类的问题需要对 began 函数进行调用来予以解决，具体可见下图。

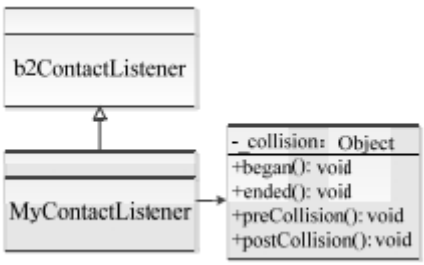

图 5 - 21 碰撞监听类类图

5.4 系统测试

5.4.1 界面测试

由于 LUA 是 CORONA 模拟器测试文件的类型，未完成编译的程序是其测试的对象。因此我们可以在其被打包整理之前较为便捷地优化所有的文件。若有问题出现于检测的过程中，就需要将游戏所在的文件夹予以返回。corona 动画库功能中的一项内容是 Sprite sheets，测试动画的效果是其主要的功能，具体可见下图 5 - 22。

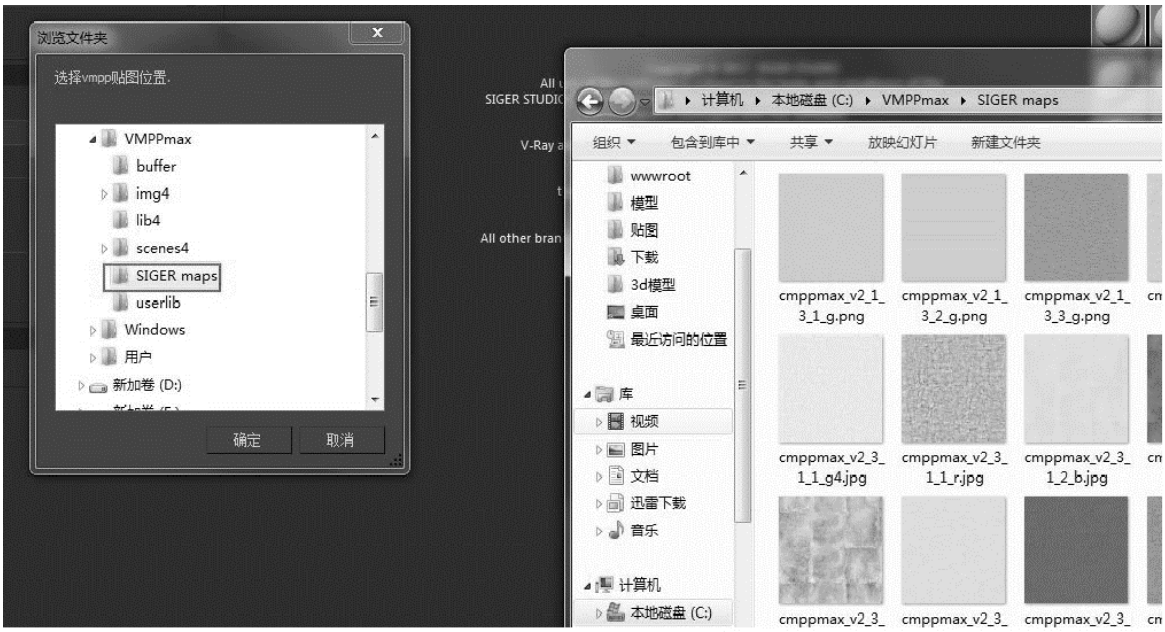

图 5 - 22 Corona 动画功能库

在 MAC 平台中，我们通过 IPOD 来对游戏的操作界面进行真机测试，具体可见下图。

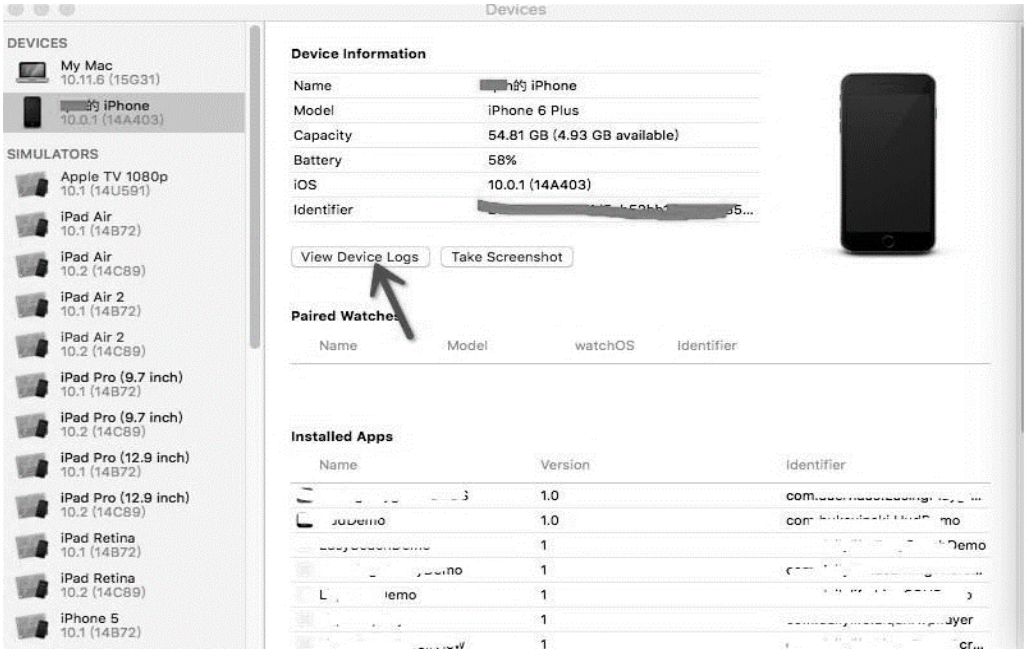

图 5 - 23 CXODE 真机测试过程

在整体测试流程中，其中的关键点在于联机测试。由于模拟环境与真机设备之间通

常是有一定的差异存在的，所以可能会有不同的效果出现。若有问题出现，则需要借助 LUA 源代码来二次修改有关程序。

5.4.2 算法测试

针对信息加密传输仿真模拟，其模仿平台由 intel core(tm)i5 型号 CPU、2.4HGz 主频、Win7 64 位操作系统、DDR3 3G 内存以及 MS Visual Studio 2008(c++)编码环境组成。

混合算法的仿真模拟：

1、ECC 密钥生成操作提示界面如下图 5 - 24 所展示，通过运行 dos 系统目录 bin 下的命令 wsnsec 实现。

图 5 - 24 混合算法 ECC 密钥生成提示界面展示

命令 wsnsec-k 中含有 1 个参数，该参数为节点名，可实现 ECC 密钥的密钥对生成；命令 wsnsec-e 有 3 个参数，依次是信息发出节点名参数、加密信息参数、信息接收节点名参数，可实现信息的加密传输；命令 wsnsec-d 有 3 个参数，依次是信息加密参数、信息发出节点名参数、信息接收节点名参数，可实现信息的解密传输。

在下图 5 - 25 中，展示了命令 wsnsec-k 在节点 bob、alice 处的 ECC 密钥生成界面图。

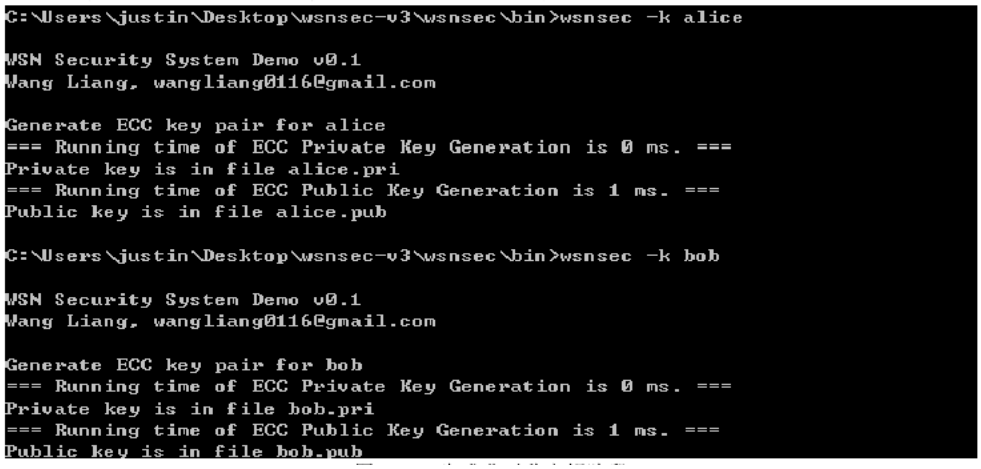

图 5 -25 混合算法 ECC 密钥的非对称生成界面展示

2、数据包、密钥、签名的混合加密实现

在下图 5 - 26 中，展示了命令 wsnsec-e 完成数据包、AES 密钥的加密以及密文、密钥块的生成。

```
D:\code\wsnsecv0.4\wsnsec\bin>wsnsec -e message1.txt alice bob

WSN Security System Demo v0.1
Wang Liang, wangliang0116@gmail.com

Encrypt message text with session key.
AES encryption of data in file.
Plain text file: message1.txt
=== Running time of AES Encryption is 10 ms. ===
Encrypted text file: message1-alice-bob.enc
Encrypt session key with public key.
ECC encryption with public key of bob.
=== Running time of ECC Encryption is 1 ms. ===
Encrypted session key is persisted in message1-alice-bob.key
Encrypt session iv with public key.
ECC encryption with public key of bob.
=== Running time of ECC Encryption is 1 ms. ===
Encrypted session iv is persisted in message1-alice-bob.key
Signature with HMAC and private key.
Sign message data in file message1-alice-bob.enc with HMAC.
=== Running time of HMAC Signature is 6 ms. ===
Sign with private key of alice.
Signature is persisted in message1-alice-bob.key
```

图 5 - 26 混合算法的加密实现展示

3、数据包、密钥、信息认证的混合解密实现

在下图 5 - 27 中，展示了命令 wsnsec-d 解密密文的实现。

```
D:\code\wsnsecv0.4\wsnsec\bin>wsnsec -d message1-alice-bob.enc alice bob

WSN Security System Demo v0.1
Wang Liang, wangliang0116@gmail.com

Decrypt session key with private key.
ECC decryption with private key of bob.
=== Running time of ECC Decryption is 1 ms. ===
Decrypt session iv with private key.
ECC decryption with private key of bob.
=== Running time of ECC Decryption is 1 ms. ===
Signature verification with HMAC and public key.
Verify signature with public key of alice.
Verify signature with HMAC.
Signature verified.
Decrypt message text with session key.
AES decryption of data in file.
Encrypted text file: message1-alice-bob.enc
=== Running time of AES Decryption is 10 ms. ===
Decrypted text file: message1-alice-bob.dec
```

图 5 - 27 密文的解密实现

算法的性能测试上，主要结合了不同的数据抓取实现。针对算法的性能分析，本文选择通过无线传感器，对其传输的数据包进行抓取，完成加密 100 次后，展开具体性能分析。

1、分析不同算法的时间复杂度

在下表 5 - 1 中，展示了 ECC 算法、RSA+AES 算法、ECC+AES 算法的密钥生成耗时，其对比图如 5 - 28 所展示。

表 5 - 1 不同算法的密钥生成耗时对比表

数据包大小（单位M）	ECC 算法密钥生成耗时	RSA 算法+AES 算法密钥生成耗时	ECC 算法+AES 算法密钥生成耗时
1	1 毫秒	17.3 毫秒	1 毫秒
10	1 毫秒	18 毫秒	1 毫秒
20	1 毫秒	18.7 毫秒	1 毫秒
30	1 毫秒	21.6 毫秒	1 毫秒
40	1 毫秒	23.2 毫秒	1 毫秒
50	1 毫秒	23.7 毫秒	1 毫秒

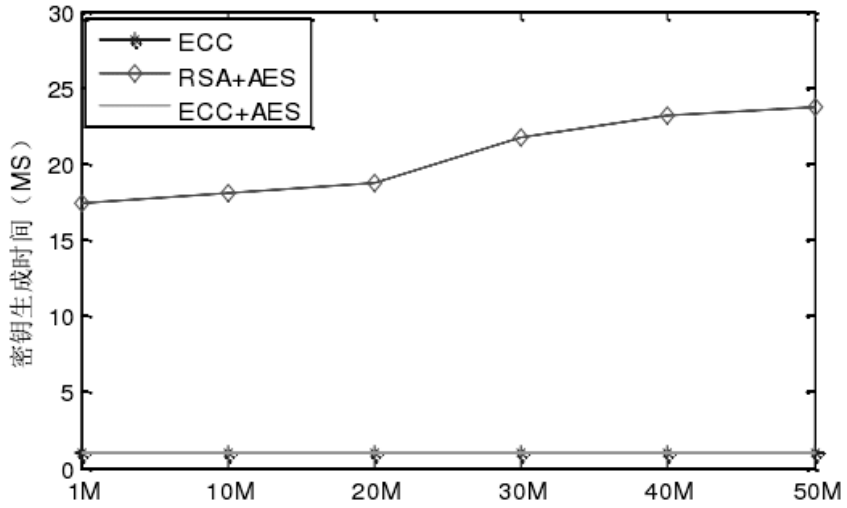

图 5 - 28 不同算法的密钥生成耗时对比展示

在表 5 - 1、图 5 - 28 中，混合算法、ECC 算法两者的密钥生成耗时不受数据包大小的影响，均是 1 毫秒，生成速度快。而 RSA 混合算法的密钥生成耗时则会受到数据包的大小影响，即数据包大小增加时，其密钥生成耗时也会随之增加。

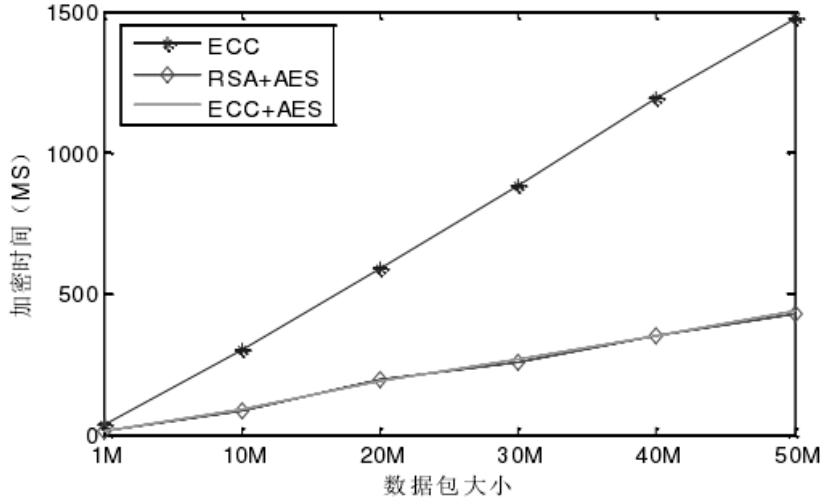

图 5 - 29 不同算法的数据包加密耗时对比展示

在下表 5 - 2 中，展示了 ECC 算法、RSA+AES 算法、ECC+AES 算法的数据包加密耗时，其对比图如 5 - 29 所展示。

表 5 - 2 不同算法的数据包加密耗时对比表

数据包大小（单位 M）	ECC 算法耗时	RSA 算法+AES 算法耗时	同 ECC 算法的耗时比	ECC 算法+AES 算法耗时	同 ECC 算法的耗时比
1	38.6 毫秒	12.2 毫秒	67%	15.6 毫秒	58%
10	298.8 毫秒	85.2 毫秒	70%	89.2 毫秒	69%
20	588.7 毫秒	196.1 毫秒	66%	188.2 毫秒	67%
30	881.2 毫秒	255 毫秒	70%	267.2 毫秒	69%
40	1192.7 毫秒	351 毫秒	69%	351 毫秒	70%
50	1476.3 毫秒	429.2 毫秒	70%	437.6 毫秒	69%

在表 5 - 2、图 5 - 29 中，ECC 算法、RSA+AES 算法、ECC+AES 算法在数据包加密耗时时，都会受到数据包大小的影响，表现为正相，当数据包大小增加时，其数据包加密耗时也会随之增加。从数据包加密耗时对比情况来看，混合算法优于其它算法。而 ECC 混合算法适用于小数据包的快速加密实现，RSA 混合算法则适用于大数据包的快速加密实现。

在下表 5 - 3 中，展示了 RSA+AES 算法、ECC+AES 算法的数据包签名耗时，其对比图如 5 - 30 所展示。

表 5 - 3 RSA+AES 算法、ECC+AES 算法的数据包签名耗时对比

数据包大小（单位 M）	RSA 算法+AES 算法耗时	ECC 算法+AES 算法耗时
1	7.1 毫秒	6 毫秒
10	54.6 毫秒	54.5 毫秒
20	117.2 毫秒	116.7 毫秒
30	172.1 毫秒	167.2 毫秒
40	212.8 毫秒	201 毫秒
50	269.5 毫秒	262 毫秒

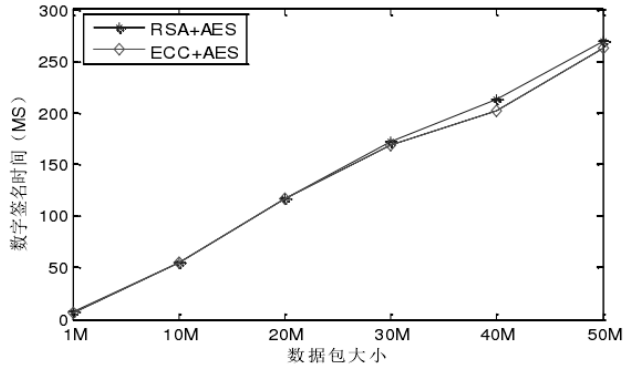

图 5 - 30 不同算法的数据包签名耗时对比展示

在表 5 - 3、图 5 - 30 中，RSA+AES 算法、ECC+AES 算法在数据包签名耗时时，都会受到数据包大小的影响，表现为正相，当数据包大小增加时，其数据包签名耗时也会随之增加。从数据包签名耗时对比情况来看，ECC 混合算法优于 RSA 混合算法。

在下表 5 - 4 中，展示了 ECC 算法、RSA+AES 算法、ECC+AES 算法的数据包解密耗时，其对比图如 5 - 31 所展示。

表 5 - 4 不同算法的数据包解密耗时对比表

数据包大小（单位 M）	ECC 算法耗时	RSA 算法+AES 算法耗时	同 ECC 算法的耗时比	ECC 算法+AES 算法耗时	同 ECC 算法的耗时比
1	39 毫秒	15.3 毫秒	60%	15.1 毫秒	60%
10	300.2 毫秒	88.5 毫秒	69%	88 毫秒	70%
20	591.6 毫秒	185.2 毫秒	68%	190 毫秒	67%
30	883.2 毫秒	261.3 毫秒	69%	264.5 毫秒	69%
40	1183.7 毫秒	345.3 毫秒	70%	348.8 毫秒	70%
50	1475.5 毫秒	429.6 毫秒	70%	432.2 毫秒	70%

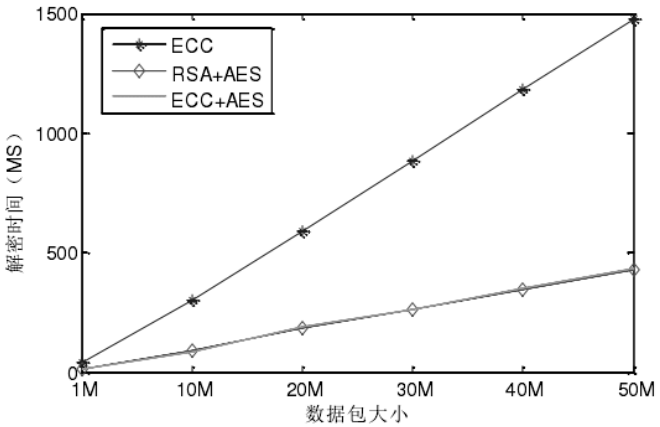

图 5 - 31 不同算法的数据包解密耗时对比展示

在表 5 - 4、图 5 - 31 中，ECC 算法、RSA+AES 算法、ECC+AES 算法针对数据包的解密耗时都会受到数据包大小的影响，表现为正相，当数据包大小增加时，其数据包解密耗时也会随之增加。从数据包解密耗时对比情况来看，ECC 混合算法、RSA 混合算法优于其它算法，且两种混合算法的结果比较接近。

在下表 5 - 5 中，展示了 ECC 算法、RSA+AES 算法、ECC+AES 算法的运行总耗时，其对比图如 5 - 32 所展示。

表 5 - 5 不同算法的运行总耗时对比表

数据包大小（单位 M）	ECC 算法耗时	RSA 算法+AES 算法耗时	同 ECC 算法的耗时比	ECC 算法+AES 算法耗时	同 ECC 算法的耗时比
1	78.6 毫秒	64.2 毫秒	17%	37 毫秒	51%
10	600.1 毫秒	246.6 毫秒	58%	232 毫秒	60%
20	1181.4 毫秒	517.5 毫秒	55%	496.1 毫秒	57%
30	1765.5 毫秒	700.3 毫秒	59%	701.1 毫秒	59%
40	2377.5 毫秒	933.4 毫秒	60%	922 毫秒	60%
50	2952 毫秒	1152.3 毫秒	60%	1143 毫秒	60%

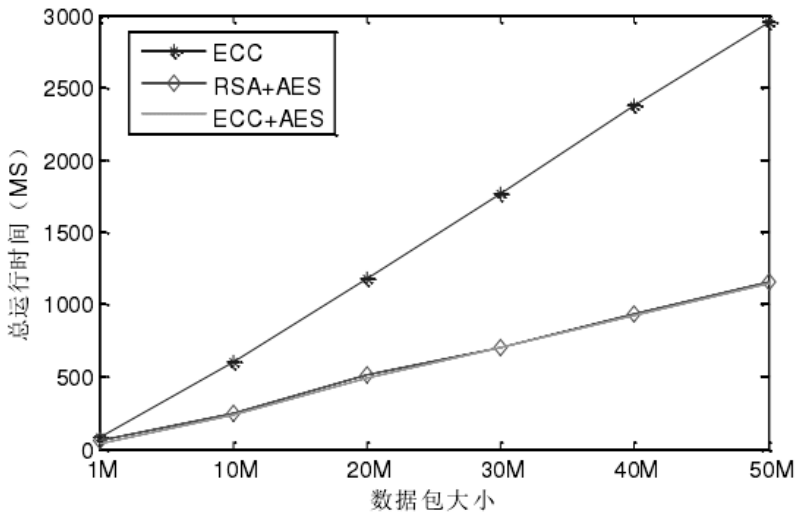

图 5 - 32 不同算法的运行总耗时对比展示

在表 5 - 5、图 5 - 32 中，ECC 算法、RSA+AES 算法、ECC+AES 算法的运行总耗时都会受到数据包大小的影响，表现为正相，当数据包大小增加时，其运行总耗时也会随之增加。从运行总耗时对比情况来看，ECC 混合算法、RSA 混合算法优于其它算法，且两种混合算法的结果比较接近。

2、安全性分析

ECC 混合算法结合了 AES 算法的对称加密优势，提升了信息传输的安全性；同时也结合了 ECC 算法的非对称加密优势，提高了密钥的安全性。为此，本文针对混合算法的高安全性进行了假设分析，设备采用 1 台 $4*10^4$/秒计算能力的计算机执行 ECC365 天加点计算，其表达式为（$4*10^4$）*（60*60*24*365），计算结果约等于 2^{40}。如果计算机的计算速度提高到 1000MIPS 且台数增至 1 万，则 ECC 加点计算结果约为 2^{160}，在这种情况下，要破解其离散对数，所需时间约 6000 年，很难实现，可见其安全性非常高。

3、密钥管理分析

文章关于密钥管理的论述，充分考虑了密钥的升级、监管，利用了非对称密钥计算，能够较为高效的管理密钥。对于对称密钥的计算，由于受节点数的影响，且要求信息传送、接收中的每对节点信息的密钥都不能相同，造成密钥量非常大，其总量为 n(n-1)/2，很难实现有效管理及快速更新。

4、能耗分析

从理论角度进行算法的能耗分析，认为其同节点数、算法耗时等有密切关系[47]，并随着节点数增加、算法耗时的增加而增加。通过对不同算法的能耗分析得出，其能耗从小到大依次是 ECC 混合算法、RSA 混合算法、ECC 算法。

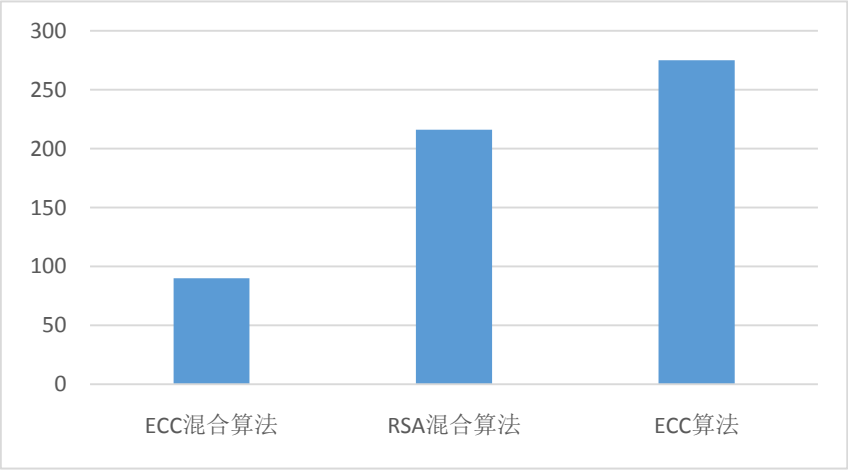

图 5 -33 不同算法能耗分析比

由此可以总结出混合算法的优势：

（1）信息传输前，不需要进行密钥密发。

（2）信息传输安全只需对 AES 密钥进行有效管理。

（3）时间复杂度小，耗时少。

（4）发送密钥的同时可完成数字签名。

5.4.3 内存测试

一般来说，用户将程序打开之后，程序的状态就会一直为工作状态，此外，一般手机都具有相对有限的储存功能，所以手机的内存通常会影响程序的运行，其运行速率会由于手机打开过多的程序而降低，甚至发生手机死机的情况。所以，要想有效地提升手机的运行速率，关键在于避免手机储存流量的损耗及将手机内存的使用效率予以提升。在对 IOS 进行测试时，其中的关键内容则为检测程序使用内存。

对游戏内容进行检测时，若之前的编译码已经有问题出现过，那么红色的提示将会出现。接着开发者可以打开此程序并修改其中的内容。具体流程可见下图 5 - 34。

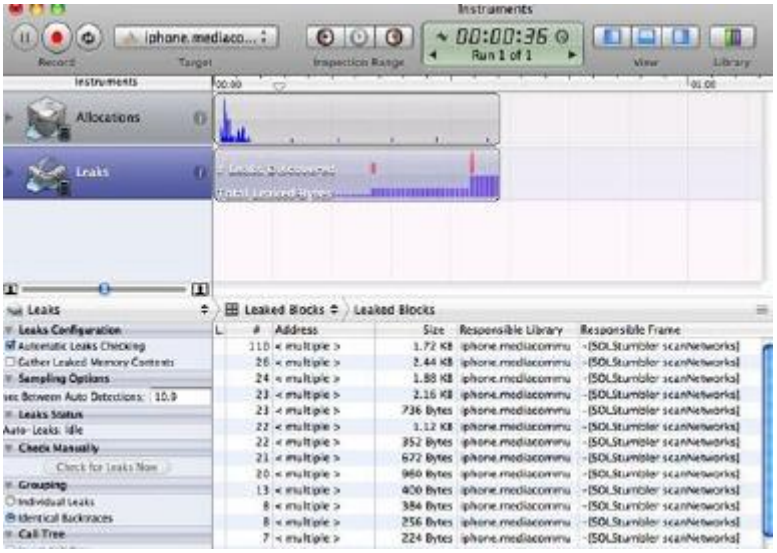

图 5 - 34 内存泄漏情况示意图

通过以上的方法，可以逐步地检测游戏的内容，防止出现内存泄露的情况，这样就能够有效地将程序的运行速率予以提升。

5.5 本章小结

在本章节中，先分别介绍了 ECC 算法、AES 算法、HMAC 算法、ECC 混合算法、AES 混合算法及存在的问题，并对比了其优势与不足，接着重点阐述了混合加密算法的开发、运行平台、设计架构、系统模块及接口，并针对游戏进行了设计并实现系统，最后通过系统测试验证，该算法能够正常应用于实际的游戏中，提高了加密效果。

第六章 结论与展望

6.1 总结

综上所述，本文对国内外相关研究资料进行分析，并就当前主要的网络攻击方式以及技术，总结出网络安全所需要进行防护的数据。对网络游戏进行综合分析，以网络游戏的特点为依据进行研究，并将其中所存在的安全威胁问题进行分析总结，并就系统优化以及升级提出相关意见，并基于上述资料建立网络游戏安全体系评估模型。为了使得网络游戏安全性提升，对其框架进行安全检查，并在数据传输方面结合密码学进行改进，使得网络游戏整体更加安全可靠。

（1）本文主要是通过分析网络游戏通信构架，找出其所存在的安全问题，并根据分析结果进行网络游戏安全评估模型构建，并对游戏所存在的安全隐患进行排除，以更加安全可靠的通信架构代替原有的通信架构，在结合密码学相关安全理论进行游戏数据传输保护。根据实际情况以及需要，构建出适合自身的网络游戏安全通信引擎，以此保障网络数据传输的安全，提升运算效率。

（2）研究了一般意义上的椭圆曲线数据防护出现的问题。此种计算其实作为具有有限域的标量乘计算。一般计算的标量乘计算通常是用作二进制的加和运算，不足之处为如果变量的值持续变大时，计算效果就不尽如人意，将会阻碍到整体 ECC 计算的过程。文章在充分研究了一般意义上的椭圆曲线加密技术以及 Frobenius 格式的应用上，构建了更加完善的新的主要立足于无线传感器技术的 Frobenius 椭圆曲线加密技术，此种加密计算对比于一般的 ECC 加密计算更加迅速，功率较小。

（3）在综合了 ECC 和 AES 这样两种比较成熟的计算方法的特点的同时，构建了 ECC 和 AES 的共同加密的计算方法。利用更加安全化的 ECC 计算实现对称加密计算的密钥，同时利用加密计算迅速的 AES 计算作为加密明文，适用于 HMAC 算法。

（4）论证此种方法的准确性，文章利用 VC++程序构建来具体的计算系统，同时处在 Windows 系统下开始验证。利用综合性的加密运算开展各种无线传感器的资料进行多次检测。

6.2 展望

本文研究工作还存在以下不足, 或有待将来继续改进之处:

（1）针对算法的无线传感器仿真实验，由于条件受限，只能依托 PC 环境完成，分别仿真模拟检测了信息传输中的加密实现、数字签名实现、信息认证实现、解密实现等，

而没有针对信息的传输过程进行系统模拟，缺乏其公钥分发机制的设计、检测。

（2）针对算法的无线传感器仿真实验，只针对 PC 环境进行了开源设计，而缺少无线传感器的嵌入优化设计，在算法的实现对比上，也缺乏其环境对比分析。

（3）在仿真模拟环节，虽然针对算法的架构、性能进行了对比分析，但对比结果比较粗略，不够精准。

（4）由于目前条件所限，未能在大型网络游戏平台验证，后续工作会寻找成熟大型游戏平台进行合作。

参考文献

[1]Shahryar Toughi,Mohammad H. Fathi,Yoones A. Sekhavat. An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System[J]. Signal Processing,2017,14-16.

[2]Natassya B.F. Silva,Daniel F. Pigatto,Paulo S. Martins,Kalinka R.L.J.C Branco. Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer[J]. Journal of Network and Computer Applications,2016,60-70.

[3]Rawya Rizk,Yasmin Alkady. Two-phase hybrid cryptography algorithm for wireless sensor networks[J]. Journal of Electrical Systems and Information Technology,2015,2(3):11-15.

[4]Sridhar C. Iyer,R.R. Sedamkar,Shiwani Gupta. A Novel Idea on Multimedia Encryption Using Hybrid Crypto Approach[J]. Procedia Computer Science,2016,79（12）：11-15.

[5]Wen-Ta Tsai,Cheng-Yang Lin,Chuan-Ming Tseng. Electrochemical carburization of pure iron in 1M Na 2 SO 4 aqueous solution with the presence of supercritical carbon dioxide[J]. Electrochemistry Communications,2014,49（11）：12-19.

[6]Nithin Nagaraj. One-Time Pad as a nonlinear dynamical system[J]. Communications in Nonlinear Science and Numerical Simulation,2012,17(11)：13-15.

[7]Nishtha Mathur,Rajesh Bansode. AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection[J]. Procedia Computer Science,2016,9（10）：19-21.

[8]Ai Ning Li,Sheng Li Hu,Jin Qing Chi,Peng Bo Wu. Research on Information Security Transmission Mechanism of Hospital Management System[J]. Applied Mechanics and Materials,2015,3682(701)：18-24.

[9]Xin Zheng Zhang,Ya Juan Zhang. On Data Security and Encryption Algorithms in Cloud Environment[J]. Applied Mechanics and Materials,2015,3682(701):11-19.

[10]缪昌照,徐俊武.AES 与 ECC 混合加密算法研究[J].软件导刊,2016,15(11):63-64.

[11]缪昌照. 不停车收费系统网络信息加密技术的研究与实现[D].武汉工程大学,2016.

[12]龙辉. 基于 ECC-AES 混合加密的智能配电网安全通信方案设计[D].湘潭大学,2016.

[13]郭晓东. 基于改进混合数据加密的营配协同系统研究及应用[D].重庆大学,2016.

[14]卜万锦. 广域保护系统通信与保密算法研究[D].哈尔滨工业大学,2015.

[15]吉兵. 基于无线传感器网络的 AES-ECC 加密系统的研究[D].新疆大学,2015.

[16]马擎宇,张东.基于 AES 和 ECC 的遥测数据加密技术研究与实现[J].舰船电子工程,2015,35(04):78-81.

[17]吉兵,汪烈军.WSNs 中基于 FPGA 的 AES-ECC 新型加密系统[J].激光杂志,2014,35(07):39-42.

[18]何清平,邹候文,杨汝.AES 与 ECC 混合密码体制的研究[J].广州大学学报(自然科学版),2014,13(02):76-80.

[19]沈泓. 混合加密系统在网络游戏虚拟财产保护中的应用[D].复旦大学,2014.

[20]王亮. 基于 WSN 的 ECC 与 AES 混合加密算法研究[D].江西理工大学,2013.

[21]张军.基于 AES 与 ECC 的混合密码体制在电子邮件中的运用[J].乐山师范学院学报,2013,28(12):55-56.

[22]赵海燕.探索密码的精彩之旅——读《密码俱乐部——用数学做加密和解密的游戏》[J].中学生数理化(八年级数学)(配合人教社教材),2013(10):32-33.

[23]张建安.混合密码技术在网络安全传输模型设计中的应用[J].信息安全与技术,2013,4(04):16-18.

[24]梁贺. 基于 G2B 和 G2E 网络的安全技术研究[D].沈阳理工大学,2013.

[25]黄鹄泉. 基于 SoC 的加密 IP 核的测试系统设计与实现[D].哈尔滨工业大学,2013.

[26]潘峥嵘,朱丽丽.ECC 与 AES 混合加密算法在射频 CPU 卡安全机制中的应用[J].计算机系统应用,2012,21(09):162-165.

[27]吴骞. AES 与椭圆曲线的加_解密算法在电子邮件系统中的应用[D].电子科技大学,2012.

[28]刘金荷. RFID 系统安全性研究[D].华北电力大学,2012.

[29]王红珍,李竹林.基于 AES 和 ECC 的混合加密系统的设计与实现[J].电子设计工程,2012,20(04):9-11.

[30]葛宏华,丁秀欢.基于 AES 和 ECC 的混合密码体制[J].科技信息,2011(09):455-457.

[31]周杰. 基于 AES 和 ECC 的加密体制研究及硬件实现[D].西安电子科技大学,2011.

[32]王常林. 基于 FIX 协议的网上证券交易系统的研究与实现[D].江苏科技大学,2010.

[33]人月小子.加密就像做游戏 你来摆我来猜[J].电脑爱好者,2009(18):60-61.

[34]王常林,吴斌.基于 AES 算法和改进 ECC 算法的混合加密方案[J].科学技术与工程,2009,9(18):5379-5382+5391.

[35]徐卉.WLAN 数据加密技术中 AES 算法的分析与改进[J].微型电脑应用,2009,25(06):58-59+53+6.

[36].你敢玩密码吗[J].数学大王(五六年级),2009(06):8-9.

[37]徐卉.WLAN 数据加密技术中 AES 算法的分析与改进[J].电脑知识与技术,2009,5(03):591-592+609.

[38]赵春颖. 基于 USBKey 的网游数据加密技术的研究与应用[D].北方工业大学,2009.

[39]张艳艳.基于 AES 和 ECC 的 WAP 安全模型研究[J].计算机与数字工程,2008(11):94-97.

[40]郑广思. 移动电子商务安全性研究[D].辽宁工程技术大学,2008.

[41]张勇. AES 与 ECC 相结合的混合密码体制的研究及应用[D].辽宁工程技术大学,2008.

[42]阮进军.基于 AES 与 ECC 的试卷管理系统的研究与设计[J].福建电脑,2008(05):130-131.

[43]陈娟. 基于 IPSec VPN 数据安全性的混合加密算法研究[D].成都理工大学,2008.

[44]周明星,周建江,杨小东,张贵仓.一种基于 AES、ECC 和 Tate 配对的签名加密算法[J].计算机应用与软件,2008(03):9-11.

[45]黄科文. ECC 和 AES 混合加密技术在移动 Agent 安全中的研究与实现[D].南京航空航天大学,2008.

[46]曹阳,权双燕.基于 AES 与 ECC 的混合型数字签名[J].科技信息(学术研究),2008(01):203-204.

[47]杨大全,王海军,赵士青,杨佳宁.网络游戏中数据加密与解密技术的研究[J].沈阳工业大学学报,2007(05):578-581.

[48]付潇潇,王世民.基于 RSA 加密算法的扑克游戏[J].北京工商大学学报(自然科学版),2007(05):60-63.

[49]李欣妍.基于 AES 和 ECC 密码体制数字信封的运用[J].甘肃联合大学学报(自然科学版),2007(05):88-90.

[50]张勇,邢长征.AES 和 ECC 相结合的数据加密技术的研究[J].计算机安全,2007(07):19-21.

[51]闫茂德,纪志强,贺昱曜,张阳.AES 与 ECC 混合加密算法的无线数据通信系统设计[J].微电子学与计算机,2007(07):135-138.

[52]张丞. 基于 AES 和 ECC 的混合密码体制研究及应用[D].成都理工大学,2007.

[53]董尼.基于 AES 与 ECC 的电子公文系统的研究与实现[J].福建电脑,2007(04):134+162.

[54]孙娜,刘念.基于 AES、ECC 混合密码体制的电子签章系统[J].网络安全技术与应用,2007(02):88-89+79.

[55]王海军. 网络游戏中外挂防御技术的研究与设计[D].沈阳工业大学,2007.

[56]鹿钦鹤. 高级加密算法的研究[D].长春理工大学,2007.

[57]Jing Wang,Xiaoyang Zeng,Jun Chen. A VLSI implementation of ECC combined with AES[A]. Chinese Institute of Electronics（CIE）.2006:6（11）： 12-16.

[58]董尼,沈明玉,罗维思. 基于 AES 与 ECC 的混合密码体制的研究与实现[A]. 2006:4(12):11-14.

[59]杨成卫.基于 AES 和 ECC 的混合密码系统研究[J].河南科学,2006(02):274-276.

[60]唐学琴. 增强 IPsec VPN 数据安全性的混合加密算法研究[D].武汉理工大学,2006.

[61].首届数学文化节 第二轮活动“能力素质挑战”书面问题解答[J].时代数学学习(七年级),2006(03):34-43.

[62]俞经善,王晶,杨川龙.基于 ECC 和 AES 相结合的加密系统的实现[J].信息技术,2006(02):44-46.

[63]游戏达人.破解 StarForce3 不拔光驱也能玩加密游戏[J].电脑爱好者,2005(13):39.

[64]贾可,周启海.网络游戏安全性的数据健壮加密方案[J].西南科技大学学报(自然科学版),2005(02):13-15+30.

[65]陈波. 智能卡技术研究与开发[D].武汉理工大学,2005.

攻读硕士学位期间取得的研究成果

一、已发表（包括已接受待发表）的论文，以及已投稿、或已成文打算投稿、或拟成文投稿的论文情况**（只填写与学位论文内容相关的部分）：**

序号	作者（全体作者，按顺序排列）	题　　目	发表或投稿刊物名称、级别	发表的卷期、年月、页码	相当于学位论文的哪一部分（章、节）	被索引收录情况

注：在“发表的卷期、年月、页码”栏：
1 如果论文已发表，请填写发表的卷期、年月、页码；
2 如果论文已被接受，填写将要发表的卷期、年月；
3 以上都不是，请据实填写“已投稿”，“拟投稿”。
不够请另加页。

二、与学位内容相关的其它成果（包括专利、著作、获奖项目等）

致 谢

硕士研究生的学习即将结束，而我又将开启另一个新的征程。华南理工大学的老师们丰富的学识，温文尔雅的态度深深吸引了我求学的态度和欲望。忠心感谢我的指导老师在我硕士研究生最后学习阶段——毕业设计阶段给自己的指导，从最初开题报告的定题，到资料收集、写作、修改，再到最终的论文定稿，指导老师给了我耐心的指导和无私的帮助。论文初稿上的一次次批注、一次次的修改都是老师给的专业意见，导师严谨的治学态度，开拓进取的精神和高度的责任心都将使我受益终生。在此我向指导老师表示我诚挚的谢意。同时，感谢所有任课老师和所有同学在学习生涯给自己的指导和帮助，是你们陪伴我度过美好的时光，教会了我专业知识，见证了我的成长。祝愿我的母校明天更加美好、未来更加辉煌。

感谢各位老师的批评指导！

答辩委员签名的答辩决议书

IV - 2答辩委员会对论文的评定意见

黎俊男同学的硕士论文“基于 AES 与 ECC 的游戏数据混合加密的研究与实现”，选题结合了工作内容和专业知识，有较好的实际意义和应用价值。

论文首先分析了目前热门的网络游戏通信构架、存在的安全问题以及游戏对性能的要求，并阅读了加密算法相关的文献，整理了几种常用加密算法体制的特点。在此基础上，论文提出了一种兼顾安全性能和运算性能的基于改进 ECC 和 AES 的混合加密体制。并将该加密体制实现、应用到一款游戏《深海游击队》中。根据论文给出的测试结果，该安全体制较好的保障了游戏数据传输的安全，同时也没有对游戏的运算效率造成过大的影响。但测试主要基于仿真平台进行，无法完全反映真实系统的情况。

作者对文献的调研、数据的收集较充分，论文资料丰富，论点正确，结论合理，实验数据真实可信。反映作者具有一定的理论基础、一定的科研和工程能力。论文结构清晰，图文表达规范，达到硕士学位论文水平。

学位申请人答辩过程讲述清楚，对评阅意见中提出的问题或质疑已作出明确的回复，答辩委员判定学位申请人的回复已达到评阅专家的要求。经答辩委员会无记名投票，同意该同学通过硕士论文答辩，同意授予硕士学位。

论文答辩日期：2018年11月26日

答辩委员会委员共5人，到会委员5人

表决票数：优秀（0）票；良好（2）票；及格（3）票；不及格（0）票

表决结果（打“√”）：优秀（ ）；良好（ ）；及格（√）；不及格（ ）

决议：同意授予硕士学位（√）　不同意授予硕士学位（ ）

答辩委员会成员签名			
	刘强（主席）	左伟勤	成飞磊
		彭绍武	