文章编号：1005-8451（2010）03-0017-04

基于IPSec VPN数据安全性的混合加密算法研究

陈 娟[1]，魏义亮[2]

（1.山西大学 商务学院，太原 030000；2.中铁太原勘察设计咨询院有限公司，太原 030013）

摘 要：提出结合高级加密算法（AES）和椭圆曲线加密算法（ECC）两种加密算法组合而成的混合加密算法，研究讨论混合加密算法的实现机制，在C++平台下实现混合加密算法的仿真系统。研究结果表明：在IPSec VPN的数据通信中，混合加密算法具有更高的安全性和可执行性，有效地增强VPN数据的安全性。

关键词：VPN；高级加密算法；椭圆曲线加密算法；混合加密算法

中图分类号：TP309 文献标识码：A

Research on mixed encryption algorithm based on IPSec VPN data security

CHEN Juan[1], WEI Yi-liang[2]

(1.Business College of Shanxi University,Taiyuan 030000, China;

2.Taiyuan Prospect & Design & Consultation Institute Co. Ltd of China Railway, Taiyuan 030013, China)

Abstract: In this paper, it was proposed two kinds of combination encryption algorithm based of AES and ECC, researched and discussed the implementation mechanism of hybrid encryption algorithm in C++ platform, achieved a Mixed-encryption Algorithm Simulation System. The research results showed that hybrid encryption algorithm with higher security and enforceable enhanced VPN data security effectively in the IPSec VPN data communication.

Key words: Virtual Private Network; Advanced Encryption Standard; Elliptic Curve Cryptography; Mixed Encryption Algorithm

VPN技术利用Internet等公用通信设施，通过隧道和加密技术建立了一个安全的、虚拟的专用通道，从而确保局域网络内部数据的保密性。VPN技术不仅能提供用户数据传输的安全性，且节约成本。IPSec是VPN结构中应用最多的协议族，但其强制要求的加密算法不能满足需求。本文提出基于IPSec VPN数据安全性的混合加密算法。该算法是由对称算法中的高级加密算法（AES）和非对称算法中的椭圆曲线加密算法（ECC）结合而成。AES算法简洁、高效、安全性高且具有良好的代数结构。ECC算法速度快、密钥短、所占资源空间少。

1 混合加密算法的提出

在混合加密算法提出前，可以通过表1对2种算法的优缺点进行分析比较。

对称加密算法和非对称加密算法都有局限性，而彼此的局限性正好可以互相弥补。将二者结合，形成一种新的加密算法即混合加密算法。

表1 对称与非对称加密算法性能对比

特性	对称加密算法	非对称加密算法
加密速度	非常快	慢
密钥关系	加密解密密钥相同	加密解密密钥不相同
密钥管理	困难	容易
密钥传递	需要	不需要
数字签名	无法实现	可以实现
主要用途	应用于大量数据的加密	小文件加密、数字签名及身份验证

2 混合加密算法的实现

为满足系统对数据快速高效加解密处理的要求，需要传输的数据采用AES加密，其中AES加密采用一次一密的模式，每次密钥均不同，数据通过VPN传输时，发送方先以随机生成的密钥加密，再用ECC加密AES算法的密钥，简化对密钥的交换与管理，并实现数字签名。最后，将经过加密处理的数据通过VPN传送给接收方。

2.1 混合密码算法的组成部分

收稿日期：2009-06-10

作者简介：陈 娟，助理讲师，魏义亮，工程师。

2.1.1　生成密钥

在椭圆曲线 $Ep\ (a, b)$ 上选一点 $G\ (x, y)$，G 的阶数为 n（n 为一个大素数），G 公开。在[1，$n-1$]之间随机地确定一个整数 K_s，计算 $K_p=K_sG$，且 K_p 为椭圆曲线 $E_p\ (a, b)$ 上的一点，由此就确定了密钥对 (K_s, K_p)。K_s 私钥，K_p 公钥。

加密AES密钥：设 K_A 为AES算法密钥，发送方取随机数 r，$r \in \{1, 2, \cdots, n-1\}$，计算 $u=rK_{BP}$（K_{BP} 为B的公钥），$R_1=rG=(x_1, y_1)$，$v=x_1K_A$。由此产生二元组 (u, v) 传送给接收方B。

解密AES密钥：用 K_{BS}（K_{BS} 为B的私钥）计算 $(x_1, y_1)=K_{BS}^{-1}u$，从而得 $KA=x_1^{-1}v$。

2.1.2　签名及认证

（1）公开消息摘要函数（md5函数），计算消息明文的摘要H（m）。

（2）签名生成：发送方A取随机数 s，$s \in \{1, 2, \cdots, n-1\}$，计算 $R_2=sG=(x_2, y_2)$，$e=x_2H\ (m)$，$k=s+eK_{AS}$，$w=KG$，由此产生二元组 (w, e) 作为发送方A对消息的签名。

（3）身份认证：计算 $R=w-eK_{AP}=(x_r, y_r)$，如 $e=x_rH\ (m)$ 成立则签名有效，否则无效。

2.2　系统仿真实现

2.2.1　硬件及网络环境

（1）服务器端：CPU频率Intel P4 2.7 GHz，Windows 2003 Server操作系统，网卡带宽100 Mbit/s。

（2）客户端：CPU频率Intel P4 2.4 GHz，Windows XP Professional操作系统，网卡带宽100 Mbit/s。

（3）支持TCP/IP协议。

（4）服务器端有真实的IP地址。

（5）服务器所在网络的防火墙设置特定监听端口。

（6）在该系统中是客户端向服务器端发起连接请求信号，所以服务器端要与Internet保持畅通。保证服务器端与客户端之间加密安全通道建立成功。

2.2.2　服务器端和客户端流程

该系统的服务器端有通信握手和数据传输2个部分。通信握手需要建立与客户端的TCP连接，与客户端同步AES密钥和建立数据安全传输通道；数据传输从客户端接收数据包、解密系统数据包、判断数据包有效性、处理数据包，并向客户端发送确认数据包和系统控制信息。服务器端是一对多的模式，服务器处理多个客户端的连接请求和数据传输，所以服务器端需要一个单独的线程来执行数据传输，而主线程可以继续接收下一个客户端发来的请求，直到接收完数据包，关闭服务器端口，如图1。

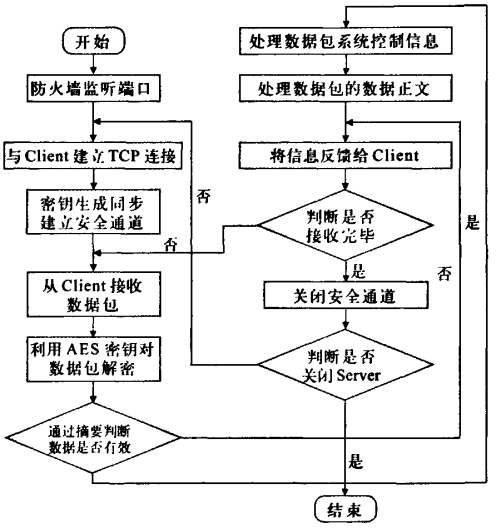

图1　服务器端流程图

同样，客户端的处理流程和服务器端很相似，也分为通信握手和数据传输2部分。服务器端解密数据包，发现错误信息并反馈给客户端后，客户端要重发数据包，保证系统的完整性，如图2。

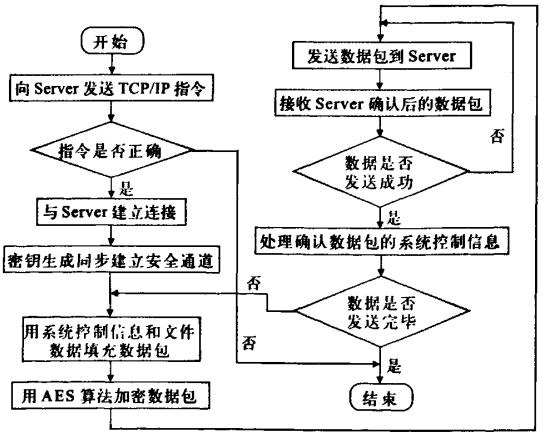

图2　客户端流程图

服务器测试运行时可接收多个客户的多次请求，也可以接收多个客户的同时请求，直到测试结束。

系统客户端程序在运行时必须输入两个参数，服务器端的IP地址和需要加密的文件传输路径。根据不同的测试请求，可单一客户端运行，也可多个客户端运行。

2.3 系统性能测试

2.3.1 单个客户端用户性能检测

通过检测6个数据文件，得到系统传输时间和数据大小的关系，如图3。

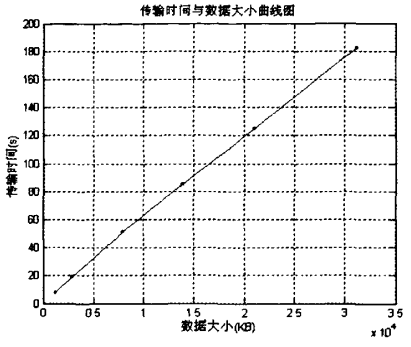

图3　单个客户端数据大小与传输时间的曲线图

从图3可知，文件在混合加密系统中的传输时间与数据文件的大小呈近似线形增长。

单客户端数据大小与传输速率的关系如图4。

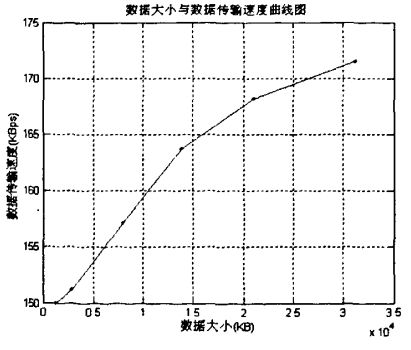

图4　单个客户端数据大小与传输速率的曲线图

从图4可知，数据传输的速度随着文件的增大而增长，但并不是线性增长。随着数据的增大，传输速率保持在170 kbit/s左右。

2.3.2 多个客户端性能检测

在系统测试中，混合加密系统的服务器接收多个客户端的连接请求和数据传输。通过对测试的6个文件得出6组数据，描绘出在多用户状态下，数据大小与传输速度之间的关系，如图5。

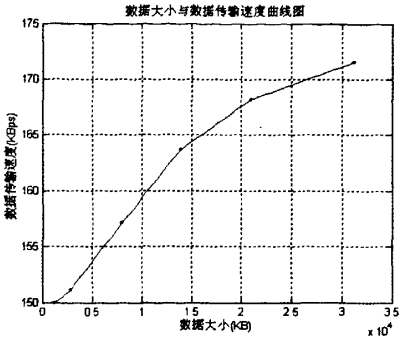

图5　多个客户端数据大小与传输速度的曲线图

通过图5，可以发现，随着客户端增多，每个客户端的传输速率要比单个传输时的速率有所下降，但是系统总速率要比单客户有较大增长。在本系统中，服务器端从安全通道中接收数据，在数据传输过程中，服务器端主要将时间消耗在对加密数据进行解密。而Borzio算法库中AES算法的加密时间比解密时间长很多。

对系统的总速率与客户端个数的分析如图6。

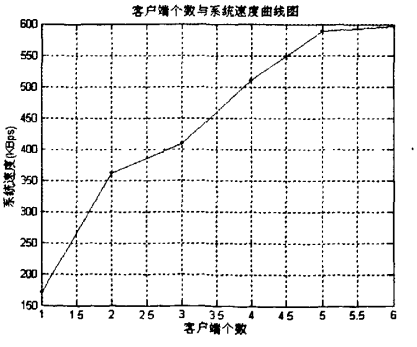

图6　客户端个数与系统速度的曲线图

由图6可知，随着客户端个数的增加，系统的速率也逐渐增加，并且速率稳定在600 kbit/s。

3 结束语

本文在C++平台下实现了混合加密算法的仿真系统。研究结果表明：在IPSec VPN的数据通信中，混合加密算法具有更高的安全性和可执行性，有效地增强了VPN的数据安全性。

文章编号：1005-8451（2010）03-0020-04

风力发电励磁系统研究

陆 野[1]，韩竺秦[2]，王 晶[2]
（1.中铁十四局 隧道处，南京 210000；2.兰州交通大学 机电技术研究所，兰州 730070）

摘 要：采用具有优良输入、输出特性的双脉宽调制（PWM）控制的交-直-交变频器作为交流励磁发电机的励磁电源。仿真实验表明：基于动态同步坐标轴系的双通道解耦励磁控制策略能够实现交流励磁发电机有功、无功和转速的独立调节。双PWM变换器具有功率双向流动，输入和输出谐波电流小，动态性能优良，功率因数可调等优点，是交流励磁发电机的理想励磁电源。

关键词：风力发电；励磁电源；脉宽调制；变速恒频
中图分类号：TM61 文献标识码：A

Study on Wind Power Excitation System

LU Ye[1], HAN Zhu-qin[2], WANG Jing[2]
(1. Tunnel Department, China Railway 14 Group Corporation, Nanjing 210000, China;
2.Mechatronic and Electronic Technology Institute, Lanzhou Jiaotong University, Lanzhou 730070, China)

Abstract: This article applied dual pulse width modulation (PWM) with the excellent input and the output feature to control AC-DC-AC inverters as the excitation power supply for AC excited generator. Through the simulation experiment, it was proved that dual-channel excitation controlling strategy based on dynamic synchronous shaft decoupling could implement the independent regulation of the AC excited generator active power, reactive power and rotating speed. The dual PWM converter had many advantages such as bidirectional power flow, low harmonics input and output currents, excellent dynamic response and adjustable power factor, it was the ideal excitation power of AC excited generator.

Key words: wind power; excitation power supply; pulse width modulation; variable speed constant frequency

利用可再生能源风能，对于缓解能源匮乏具有非同寻常的意义。和常规风力发电系统相比，变速恒频交流励磁双馈风力发电系统配置的变频器在转子回路，仅处理双向流动的转差功率，具有变频器体积小、重量轻、成本低的特点，实现了机电系统的柔性连接。目前，通常采用双脉宽调制（PWM）控制的交-直-交电压型变频器作为交流励磁发电机的变频励磁电源，该变频器由电网网侧变换器和转子侧变换器所构成，因此也常称为“背靠背”变换器或双PWM变换器。

收稿日期：2009-06-29
作者简介：陆 野，助理工程师；韩竺秦，在读硕士研究生。

1 双PWM变换器的工作原理

图1为双PWM变换器励磁的交流励磁发电机系统总体结构图，双PWM变换器由电网侧变换器

目前，本文提出的混合加密算法的仿真系统还不够完善，对它的研究、分析、测试和应用尚处于初级阶段，有待进一步提高。

参考文献：

[1] 董 尼. 基于AES与ECC的混合密码[D]. 合肥：合肥工业大学，2006，4.
[2] 涂志强. VPN技术研究及在油田的应用[D]. 北京：中国地质大学，2006，4.
[3] 邝献涛. IPSec协议分析研究[D]. 长沙：湖南师范大学，2004，4.
[4] 冯娟娟. 加速ECC算法的相关算法研究[D]. 北京：信息工程大学，2006，4.
[5] 杨成威. 基于AES和ECC的混合密码系统研究[J/OL]. 河南科学，2006，24(2).
[6] 侯整风，李 岚. 椭圆曲线密码系统(ECC)整体算法设计及优化研究[J/OL]. 电子学报，2004 (11)：145-147.
[7] 潘 茜. 基于IPSec VPN的安全策略研究[D]. 西安：西安电子科技大学，2007，1.