基于 BlowFish 算法的物联网网络安全算法设计

陈伟[1]，何丽萍[2]
1. 安庆职业技术学院信息技术学院，安徽 安庆 246000
2. 安庆职业技术学院现代商务学院，安徽 安庆 246000
DOI: 10.61369/TACS.2026010034

摘　　要： 物联网的发展，特别在片上系统的 Blowfish 算法自提出以后便得到了广泛应用，对它的攻击也越来越多。针对 WSN 节点内存空间小和运行执行能力相对弱，电池供电有限的情况下，提高网络的安全可靠性，对 Blowfish 算法进行研究，在 ZigBee 网络节点与节点之间通信过程中如何进行数据加密和数字签名，从这两个方面对算法进行优化，提高整个网络的通信效率，保证数据的完整性。提出基于椭圆曲线加密 BlowFish 密码（EECB）算法。

关 键 词： ZigBee 网络；Blowfish 算法；椭圆曲线；EECB 算法

Design of ZigBee Network Security Algorithm Based on BlowFish Algorithm

Chen Wei[1], He LiPing[2]
1.School of Information Technology Anqing Vocational&Technical College, Anqing, Anhui 246000
2.Modern Business College Anqing Vocational&Technical College, Anqing, Anhui 246000

Abstract: With the development of ZigBee network, especially the Blowfish algorithm of on-chip system has been widely used since it was put forward. For the WSN node memory space is small and the execution ability is relatively weak, the situation of battery power is limited, to improve the safety and reliability of the network, research on the Blowfish algorithm, data encryption and digital signature in network communication between ZigBee node and node, we can optimize the algorithm from the two aspects, to improve the communication efficiency of the whole the network, to ensure the integrity of the data. An algorithm based on elliptic curve cryptography for BlowFish encryption (EECB) is proposed.

Keywords: ZigBee network; Blowfish algorithm; elliptic curve; EECB algorithm

引言

随着计算机网络的普及和电子设备的发展，信息化已经成为社会发展的不懈动力，而网络已逐渐成为人们生活的必需品。通过网络的发展人们不断提出新观点，实现“存在即上网”。融合传感器技术、网络通信技术和信息处理技术的无线传感器网络技术的产生[1]。它的应用已经渗透到社会的各行各业，由多种无线通信技术，从红外到 ZigBee 网络的发展。而 ZigBee 无线传感网络是 ZigBee 联盟建立的标准，它是面向短距离、低功耗和低速率的网络，主要在自动控制、监控、电子消费和农业等领域，李永娜[2]采用非对称加密算法，对原始数据加密生成的密文比较简单，很难保护数据安全。采用公钥密码算法 (RSA) 和对称密码混合加密[3-4]的 方式保证个人隐私方面效果很好。

Blowfish 算法是在1993年由提出的一种对称分组加密算法，本文分析了 Blowfish 算法的加密、解密过程进行分析在 CC2530芯片上实现，它是基于8051CPU 的芯片设计出完全支持 ZigBee2007/Pro 协议栈的通信模块，它们封装成加密盒，有效地保护了 Zigbee 网络的通信，提高网络安全的可靠性。而在通信过程中通常采用数据加密、身份认证、数字签名等技术措施来防止外部的攻击。可以采用非对称加密机制替代原有的对称加密算法的方法。提高数据的安全性和数据通信的效率同时还要保证节点的功耗。我们采用 Blowfish 算法和非对称加密的算法相结合，在 ZigBee 网络中节点之间的通信用椭圆曲线加密算法，还可以利用数字签名来确保信息的完整性。

一、BlowFish 算法原理分析

BlowFish 算法是一种对称分组加密算法。在32位微处理器基础上实现的，而且能够在小于5K 存储器中运行。它的设计准则是快速、简单和可变安全性。每次加密输入64位明文信息，使用32位到448位的可变长度密钥，经过两个阶段：密钥扩展和数据加

项目信息：
安徽高校省级质量工程项目 (2020jyxm1124,2020qk125)；
安徽省高校自然科学研究项目（KJ2020A1024）；
安庆职业技术学院科研重点项目（2026AQZYSK01）。
作者简介：陈伟（1983—），男，安徽桐城人，硕士研究生，安庆职业技术学院，讲师，研究方向：网络信息安全、无线传感器网络。E-mail:hmsz8888@163.com

密，最终以64位密文信息输出[1]。该算法需要两个数组即P数组和S数组。

（一）数据加、解密

首先初始化信息，使用加密函数BlowFish_Encrypt（），加密所用的密钥的明文分成两个部分，即LE和RE各32位，加密过程是16层Feistel网，加密需要16次迭代，需要使用P数组密钥和S盒子密钥，最后输出64位密文。在计算机密钥过程中使用模2^{32}加运算和异或运算以及用S盒子密钥替代操作，所以实现加密的算法非常的快速[5]。

信息解密同样用BlowFish算法需要有两个过程为首先密钥扩展过程与加密过程相同；其次把加密过程的P数组逆序使用就可以得到。

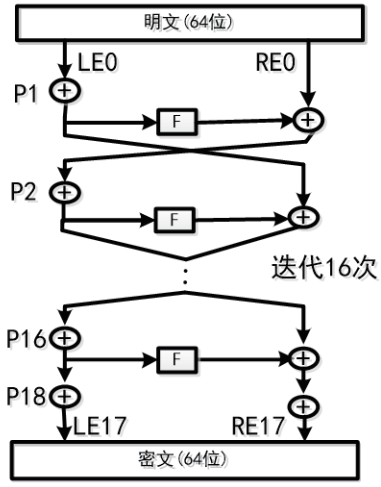

图1 BlowFish加密过程

文献[4]提出改进的的BlowFish算法以概率分布[6],F函数由异或运算、移位运算、模加法运算、S数组运算生成。异或运算，明文分组中左LE0（32位）与相应的密钥P1进行异或运算；经过F函数之后的结果与明文分组中右RE0（32位）进行异或运算；初始P数组与主密钥每32位循环异或；F函数中，S1、S2的32位加法输出与S3的32位输出进行异或运算；移位运算，子密钥产生过程中，初始化P数组，需要将主密钥循环移位，以产生新的P数组，每次向左或者向右移位1位；模加法运算，S1与S2的32位输出进行模2^{32}的运算；S1、S2、S3的32位输出与S4的32位输出进行模2^{32}的运算；S盒运算（查表运算），F函数中，每次进行8位输入32位输出的查表运算[1]。

二、BlowFish算法的优化

椭圆曲线有丰富的数学结构，这使得它在公钥密码系统中有广泛的应用。结合椭圆曲线密码算法的数学基础对椭圆曲线密码体制进行分析，然后利用椭圆曲线实现BlowFish密码体制。

（一）椭圆曲线的定义

椭圆曲线并不是椭圆，只是因为它通过三次方程来进行表征的，而该三次方程与计算椭圆的周长方程类似，因此把它称之为椭圆曲线。椭圆曲线的研究来源于椭圆积分。这里

$$\int \frac{dx}{\sqrt{E(x)}} \quad (1)$$

$E(x)$是x的三次次多项式表示。这样的积分不能用初等函数来表达，为此引入了所谓的椭圆函数。所椭圆曲线是指由韦尔斯特拉斯方程如下：

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6 \quad (2)$$

若F是已给域，其中$a_i \in F, i=1,2,\cdots,6$满足韦尔斯特拉斯方程的数（$x,y$）称为域$F$上椭圆曲线$E_p$（$a,b$）的点。椭圆曲线的基本性质：设$E_p$是一条$G$（$p$）上的椭圆曲线中的点及其上加法运算构成一个群，$E_p$群的阶（$E_p$的点的个数）为$\#E_p(a,b)=p+1-t, |t| \le 2\sqrt{p}$。

（二）椭圆曲线系统实现的建立

椭圆曲线密码体制是比较新的技术[7]，在椭圆曲线密码体制中，首要问题就是安全椭圆曲线的选取问题，如果选取的椭圆曲线本身是不安全的，那么基于该椭圆曲线的任何方案都是不安全的。如何选取基点也是构造椭圆曲线密码体制的关键要素。

有限域F_d和定义在有限域F_d上的曲线E（F_d），对于已知椭圆上的点P，求$Q=kp$。已知p和Q求出k的值过程是非常的困难。该问题被称为椭圆曲线上的离散对数问题。椭圆曲线密码系统主要选用安全可靠椭圆曲线。所谓的安全可靠的曲线是指能抵御各种已有攻击的曲线，目前对椭圆曲线攻击比较有效的方法有*MOV*攻击、*pollard*方法等

有限域F_d在椭圆曲线上E（F_d）需要满足：

（1）椭圆曲线的群的阶，E（F_d）大于2^{160}且大于$4\sqrt{q}$的素数因子。

（2）E（F_d）不是超奇曲线或反常曲线，这两种曲线在所有的椭圆曲线公钥密码的标准中都被指定禁止使用。

构成椭圆曲线密码系统的参数集称为椭圆曲线域参数，包括有限域F_d，椭圆曲线E，基点G（椭圆曲线上的随机选择的一个点），基点的阶n椭圆曲线群的阶E（F_d），相关因子h。椭圆曲线的域参数是公开信息。

（三）利用椭圆曲线加密BlowFish密码（EECB）体制

BlowFish密码算法的明文在ZigBee网络传输过程中的明文M。通过实体A和B的通信来说明加、解密的过程：

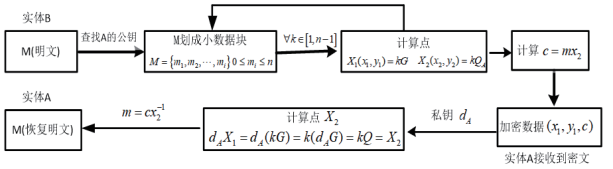

图1 椭圆曲线加密过程

数字签名过程：

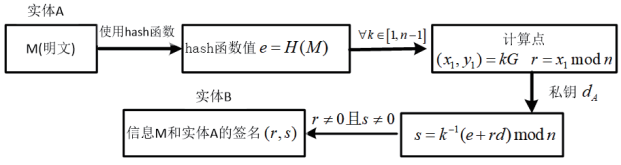

图2 数字签名过程

数字签名的验证过程

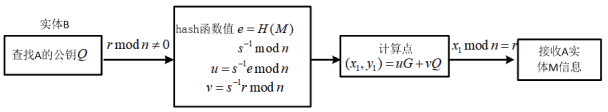

图3 数字签名验证过程

三、网络安全模型算法实现

常见的加密第一种采用重叠深度学习算法用于网络通信数据的混合加密[8]，第二种粒子群优化 (PSO) 算法用于提高 RSA 的加解密速度[9]，本文通过 Blowfish 算法和椭圆曲线系统，克服了常规技术中加密算法的安全问题。在 ZigBee 网络中在感知层使用的芯片是 CC2530，使用 EECB 算法提供版权保护和加密功能。单片机芯片中存储加密算法和程序，使用软件时可将加密盒插入 PC 的串口或 USB 等 I/O 接口中，对软件进行保护。在无线节点进行通信时使用 EECB 算法，同时不断的变换密钥设计，增强了软件的安全性。

四、总结

黑客通过攻击手段，数据在传输过程中的安全性很难保证，会造成核心信息泄露，特别对企业造成极大损失[10-11]，通过 Blowfish 算法不仅安全可靠，而且加解密速度快，使用于不同的平台，因此在软件版权保护和嵌入式应用系统中有很大的发展潜力。通过椭圆曲线加密算法和 Blowfish 算法相结合，提出 EECB 算法，提高网络通信的安全性同时加强单片机芯片的保密通信。提高整个网络的可靠性。

参考文献

[1] 李根等 . 基于超混沌序列改进分组密码算法的无线传感网络通信数据加密方法 [J]. 电气自动化 ,2023,45(5):78-80

[2] 李永娜. 农业网络云储存信息非对称加密方法研究 [J]. 农机化研究 ,2024,46(11):224-228.

[3] 陈靖，汪烈军，钟劲松，等 . 改进型 AES 加密算法在无线传感器网络中的研究与实现 [J]. 现代电子技术 ,2021,44(12):44-48.

[4] 皇甫大双 . 基于 Logistic 映射的视频敏感信息加密技术设计 [J]. 河南工程学院学报 (自然科学版),2023,35(1):71-74.

[5] 张晓敏 . 计算机网络信息安全中数据加密技术研究 [J]. 信息技术 ,2021,45(6):68-72.

[6] 叶清等 . 基于 Blowfish 的 HEVC 高效选择性加密方案 [J]. 海军工程大学学报，2022,34(1):7-12+19.

[7] 李荣，夏天勇，张琪，等 . 论数据加密技术在计算机网络安全中的应用 [J]. 网络安全技术与应用，2024 (01)：24-25.

[8] 秦武韬，王鹏，李王峰，基于周期耦合处理的 CAN 总线数据组合加密方法 [J7. 通信学报，2023，44(1):29-38

[9] 张志红 . 基于改进 Blowfish 算法的网络安全隐私数据加密方法 []. 宁夏师范学院学报，2024，45(10):95-104.

[10] 张育梅 . 基于数据消冗技术的大数据属性加密数学建模 [J]. 计算机仿真 ,2021,38 (5):418-422.

[11] 李宏伟等 . 一种基于双勾函数的数据加密算法研究 [J]. 计算机技术与发展 ,2022，32 (6):120-125.

