

基于置换移位的单字节分组保密方法

陈 帅¹, 朱士永¹, 石军锋², 王 丽¹, 李 营¹

(1. 淮南师范学院 计算机与信息工程系, 安徽 淮南 232001;

2. 西南大学 工程学院, 重庆 400715)

摘 要:为减少无线传感器网络编码的冗余字节, 提高基于 Feistel 结构的无线传感器网络分组加密的安全性, 提出了一种新的单字节分组密码保密方法。采用生成单位矩阵的幂次和密钥变换矩阵生成密钥, 明文通过单字节的置换和循环移位得到加密密文。首先介绍无线传感器网络 Feistel 结构分组加密算法, 然后给出了置换和移位操作编码原理, 并给出了设计的加密解密算法, 最后进行了分析和实验。提出的方法既可以实现加密, 也可以实现解密。分析结果表明, 密钥具有较高的安全性能, 可以增强基于 Feistel 结构的无线传感器网络分组加密安全性。

关键词:单字节; 分组密码; 无线传感器网络; 置换; 循环移位

中图分类号:TP393; TP309; TN918

文献标识码:A

文章编号:1673-629X(2010)10-0176-04

Confidential Algorithm Based on Permutation and Shifter for Single Byte Cipher

CHEN Shuai¹, ZHU Shi-yong¹, SHI Jun-feng², WANG Li¹, LI Ying¹

(1. Computer and Information Engineering Department, Huainan Normal University, Huainan 232001, China;

2. Engineering College, Southwest University, Chongqing 400715, China)

Abstract: In order to reduce redundancy byte and enforce safety for confidential communication in wireless sensor networks based on Feistel structure, a new single byte block cipher algorithm was brought forward. The keys are produced through the times of unit matrix and the cipher transforming matrix. Byte permutation and loop shifter was used to encrypt plain texts into cipher texts in the algorithm. First, the cipher block algorithm in Feistel structure for wireless sensor networks was introduced. Then the encoding principle of the permutation and shifter operation was given, and the algorithm was introduced. In the end, the algorithm was analyzed and the experiment was completed. The algorithm may be used both for encryption and decryption. Encoding principle was given and algorithm was designed. The result from analyzing is that the group keys are more secure, and the algorithm may improve security for wireless sensor networks block cipher based on Feistel structure.

Key words: single byte block; block cipher; wireless sensor networks; permutation; loop shifter

0 引 言

无线传感器网络^[1~3] (wireless sensor networks, WSN), 由于网络节点资源有限、处理能力有限, 监测少量字节的数据, 如果采用多字节分组包加解密, 必然会引入冗余字节数据。采用单个字节的分组数据包进行处理, 就可以做到不引入冗余数据, 从而可以达到编码的最大有效利用率。DES^[4~6]算法和 AES^[5~7]对于

只需要 8bit 信息的传输引起多余冗余字节。文献[8, 9]对 WSN 的安全进行了分析。文献[10~12]对于 WSN 的单字节分组保密通信, 提出了 Feistel 结构的密码编解码。

在 Feistel 结构的机密体系中, 例如 DES 和基于 Feistel 结构的 WSN 分组加密结构中, 在轮 Feistel 处理的前后都用到了置换操作。而这些算法的机密性在于多轮 Feistel 结构处理而不在于置换操作。如果在这些算法中将置换引入机密机制, 必将增强算法的安全性。

1 无线传感器网络 Feistel 结构分组加密算法简介

基于 Feistel 结构的 WSN 分组算法结构如图 1^[8,9]

收稿日期: 2010-02-18; 修回日期: 2010-05-24

基金项目: 重庆市自然科学基金项目(2005BB2198); 安徽省自然科学基金研究重点项目(KJ2010A310); 淮南师范学院科研基金资助计划项目(2009LK02)

作者简介: 陈 帅(1969-), 男, 副教授, 博士, CCF 会员, 研究方向为无线传感器网络、嵌入式系统等。

所示。结构采用了置换和多轮的 Feistel 结构。输入的 8bit 明文分组首先被进行单字节位的置换变换;然后被分成两个 4bit 的 R_i, L_i (其中 i 为 Feistel 加密的轮次, $i = 1, 2, 3, 4, \dots, n$), 再进行 n 轮的 Feistel 结构加密, 其中每轮的 Feistel 加密结构如图 2 所示。

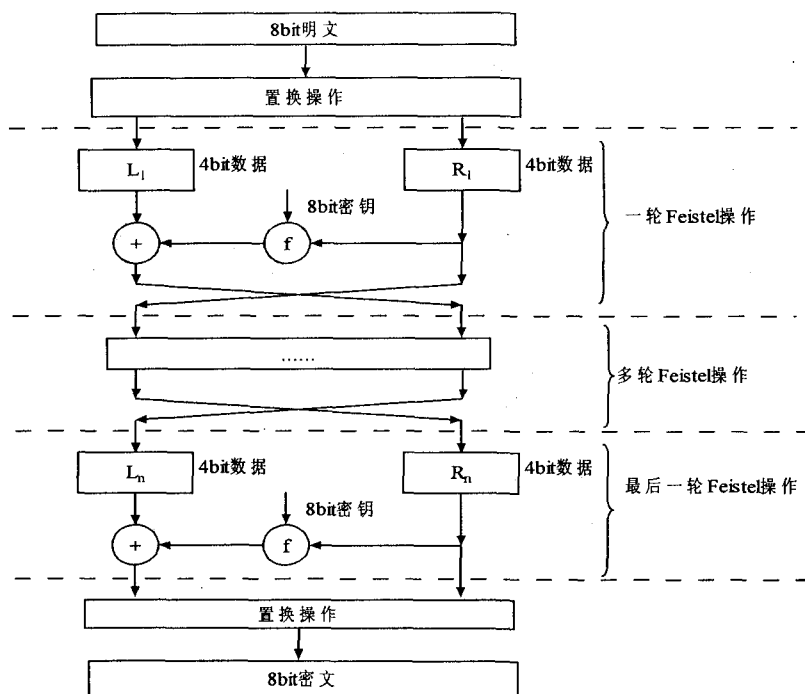


图 1 基于 Feistel 结构的 WSN 分组加密结构

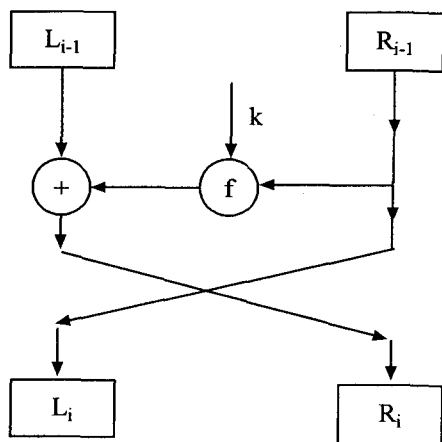


图 2 单字节分组的 Feistel 结构

八比特分组的 Feistel 结构的处理过程表示^[8]为:

$$\begin{cases} R_i = L_{i-1} \oplus T \\ L_i = R_{i-1} \end{cases} \quad (1)$$

其中 $R_i, R_{i-1}, L_i, L_{i-1}, T$ 都为 4bit, k 为密钥, f 为加密函数。其中 Feistel 加密的最后一轮不进行高低半字节交换;最后再进行一次单字节的置换变换。

2 置换操作

考察单字节的置换变化。从字节数据 A 变换到

字节 B 的置换变换, 可以看做是 A 数据的二进制位的重新排列, 例如, 设字节 $A = (abcdefgh)^T, B = (dhcfeagb)^T$, 其中 a, b, c, d, e, f, g, h 都取 0 或 1, 变换前后 A 和 B 字节中位值为 1 和 0 的总数不变, T 表示矩阵转置操作。则这种变换可以表示为:

$$B = (dhcfeagb)^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$(abcdefgh)^T = PA \quad (2)$$

其中 T 表示矩阵转置。可见通过变换矩阵 P 完成了从 A 到 B 的置换变换:

$$A \rightarrow B \quad (3)$$

观察矩阵 P , 可见有以下规律:

(a) P 是由 1 和 0 组成的矩阵, 是由以下 8 个向量 $a_1 \sim a_8$ 构成的矩阵:

$$\begin{aligned} a_1 &= (10000000) \\ a_2 &= (01000000) \\ a_3 &= (00100000) \\ a_4 &= (00010000) \\ a_5 &= (00001000) \\ a_6 &= (00000100) \\ a_7 &= (00000010) \\ a_8 &= (00000001) \end{aligned} \quad (4)$$

(b) P 的秩为 8, 即:

$$\text{rank}(P) = 8 \quad (5)$$

(c) P 的 n (n 为整数) 次幂矩阵仍然是由 1 和 0 组成的矩阵, 且 n 次幂矩阵的秩也为 8:

$$\text{rank}(P^n) = 8 \quad (6)$$

(d) P 的 m (m 为整数) 次幂矩阵可以得到单位矩阵, 即:

$$P^m = E = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (7)$$

m 称为矩阵 P 的生成单位阵次数, E 为单位阵。在上面的例子中 $m = 8$ 。

还可以继续进行类似(2)式的变换操作,例如:

$$C = (fagcbhd)^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$(dhefgcba)^T = PB \quad (8)$$

将(2)式代入,则:

$$C = (fagcbhd)^T = PB = PPA = P^2A \quad (9)$$

通过变换矩阵 P^2 完成了从 A 到 C 的置换变换:

$$A \rightarrow C \quad (10)$$

进而可以继续操作,即进行变换:

$$A \rightarrow P^n A \quad (11)$$

这样,如果将 $n(1 \sim m)$ 和 P 做为密钥,则得到一种单字节数据的密码编码方案。

3 移位操作

移位可以改变数据的位置,但数据的相邻关系不变。为保持移位后数据位的不损失,这里的移位操作指循环移位,包括循环右移位和循环左移位。

设:

$$A = (abcdefgh)^T \quad (12)$$

另设密钥为 K ,移位操作为 $S(K)$,其中 $S(K)$ 为 $0-1$ 矩阵,移位后为 B ,则:

$$B = S(K)A \quad (13)$$

从字节数据 A 变换到字节 B 的循环移位变换,可以看做是将 A 数据的二进制位重新排列,例如,设字节 $A = (abcdefgh)^T$, $B = (defghabc)^T$,其中 a, b, c, d, e, f, g, h 都取 0 或 1,变换前后 A 和 B 字节中位值为 1 和 0 的总数不变。则这种变换可以表示为:

$$B = (defghabc)^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$(abcdefgh)^T = QA \quad (14)$$

可见 Q 矩阵与 P 矩阵具有相同的性质,也是(4)式向量的一种排列。

同样可以继续下列变换操作:

$$A \rightarrow Q^s A \quad (15)$$

其中 s 取 $1 \sim 8$ 的整数。这样,如果将 s 和 Q 做为密钥,则也得到一种单字节数据的密码编码方案。

4 算法设计

4.1 加密方案

由于 P 和 Q 性质相同,将 P 和 Q 矩阵操作合并,就得到:

$$A \rightarrow P^n Q^s A \rightarrow W^k A \quad (16)$$

其中 k 为密钥, W 为变换密钥矩阵, W 是(4)式向量的一种排列矩阵,与矩阵 P 和 Q 性质相同。

设单字节密文数据为 A ,单字节密文数据为 B ,则加密过程表示为:

$$B = e_{k,W}(A) = W^k A \quad (17)$$

4.2 解密方案

解密是利用(7)式的特性。已知道密文 B ,密钥 k 和 W ,则解密操作为:

$$d_{k,W}(B) = W^{m-k} B = W^{m-k} W^k A = W^m A \quad (18)$$

根据(7)式,如果:

$$W^m = E \quad (19)$$

则(18)式变为:

$$d_{k,W}(B) = W^{m-k} B = W^{m-k} W^k A = W^m A = EA = A \quad (20)$$

从而正确得到明文。

5 密钥分析

密钥有 k, W 。变换密钥矩阵 W 是从(4)式的 8 个向量排列得到的矩阵,这 8 个向量排列有: $8! = 40320$ 种,故 W 矩阵有 40320 个。密钥 k 是与生成单位阵次数 m 有关,其取值为 $k = 1 \sim m$ 。

通过统计,得到 W 矩阵的生成单位阵次数 m 有 11 种可能取值: $1 \sim 8, 10, 12, 15$,其得到的变换矩阵 W 数量如表 1 所示。

表 1 生成单位阵次数 m 和 W 矩阵数目

m	k 的取值	W 矩阵数目
1	1	4
2	1 ~ 2	1518
3	1 ~ 3	1846
4	1 ~ 4	6451
5	1 ~ 5	2685
6	1 ~ 6	11399
7	1 ~ 7	5228
8	1 ~ 8	2786
10	1 ~ 10	4031
12	1 ~ 12	3010
15	1 ~ 15	1362

每当取定一个 m ,则密钥取值为 $k = 1 \sim m$,而变

换矩阵 W 就有多种可选。例如取 $m = 8$, 则 k 可以取 $1 \sim 8$ 其中之一, 对应的 W 矩阵有 2786 种可供选择。于是, 密钥组合是 k 和 W 可能取值数目的乘积。通过计算可以得到总共的密钥数目为: 3.866×10^{43} 。若采用穷举法破解, 以每秒列举 10^{20} 个密钥, 则需要 1.23×10^{16} 年才能穷举完所有密钥组合。可见密钥的安全性比较高。

6 实验

取密钥 $k = 9$, 变换密钥矩阵 W 为:

$$W = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (21)$$

计算可知: $\text{rank}(W) = 8$ 。在 MATLAB 下进行加密解密计算, 设明文 $A = [1 \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0]^T$, 结果如图 3、图 4 所示。

$$\begin{aligned} A' &= \\ 1 & \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \\ B' &= (W^{\wedge} 9 * A)' = \\ 1 & \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \\ C' &= (W^{\wedge} 3 * B)' = \\ 1 & \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \end{aligned}$$

图 3 密文 B 通过正确密钥解密得到正确明文 C

$$\begin{aligned} A' &= \\ 1 & \ 1 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \\ B' &= (W^{\wedge} 9 * A)' = \\ 1 & \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 1 \\ D' &= (W^{\wedge} 5 * B)' = \\ 1 & \ 0 \ 1 \ 0 \ 0 \ 1 \ 1 \ 1 \end{aligned}$$

图 4 密文 B 通过错误密钥解密得到错误明文 D

图 3 中明文 A 先被加密成密文 B , 然后通过正确密钥解密得到正确的明文 C 。图 4 中明文 A 先被加密成密文 B , 然后通过错误密钥解密得到错误的明文 D 。可见, 算法能够完成保密。

7 结束语

针对无线传感器网络等的少量数据字节的密码编码, 为增强基于 Feistel 结构的 WSN 分组加密的安全性, 提出了一种新的单字节密码编码算法。算法采用单字节的置换和循环移位, 既可以实现加密, 也可以实现解密。分析结果表明, 密钥具有较高的安全性能, 并在实验中验证了算法。

参考文献:

- [1] Asada G, Bhatti I, Lin T H, et al. Wireless Integrated Network Sensors (WINS)[J]. Proceedings of SPIE - The International Society for Optical Engineering, 1999, 3673: 11 - 18.
- [2] 陈 帅, 钟先信, 刘积学, 等. 无线传感器网络的新进展与应用[J]. 压电与声光, 2006, 28(3): 297 - 299.
- [3] 任丰原, 黄海宁, 林 闯. 无线传感器网络[J]. 软件学报, 2003, 14(7): 1282 - 1291.
- [4] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644 - 654.
- [5] 张晓丰, 樊启华, 程红斌. 密码算法研究[J]. 计算机技术与发展, 2006, 16(2): 179 - 180.
- [6] 范 红, 冯登国. 安全协议理论与方法[M]. 北京: 科学出版社, 2003.
- [7] Danmen J, Rijmen V. AES Proposal: rijndael. AES algorithm submission. AES home page [EB/OL]. 1999 - 09 - 03. <http://www.nist.gov/aes>.
- [8] 郎为民, 杨宗凯, 吴世忠, 等. 无线传感器网络安全研究[J]. 计算机科学, 2005, 32(5): 54 - 58.
- [9] 贾玉福, 董天临, 石 坚. 无线传感器网络安全问题分析[J]. 网络安全技术与应用, 2005(1): 48 - 51.
- [10] Chen Shuai, Zhong Xianxin, Wu Zhengzhong. Chaos block cipher for wireless sensor network[J]. Science in China Series F: Information Sciences, 2008, 51(8): 1055 - 1063.
- [11] Chen Shuai, Zhong Xianxin. Confidential Communication through Chaos Encryption in Wireless Sensor Network[J]. Journal of China University of Mining & Technology, 2007, 17(2): 258 - 261.
- [12] Stinson D R, Feng Dengguo. Cryptography theory and practice[M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2003.

中国计算机学会会刊、中国科技核心期刊
《计算机技术与发展》欢迎投稿, 欢迎订阅!