

一种基于动态思想的 SMS4 算法改进与实现

周术洋, 彭蔓蔓, 肖小欢

(湖南大学 计算机与通信学院, 湖南 长沙 410082)

摘 要: SMS4 算法是国家商用密码管理办公室于 2006 年 1 月公布的用于无线局域网产品的分组对称密码算法。文中介绍了 SMS4 算法的原理, 在原算法的基础上基于动态思想对其进行了改进, 并实现了改进后的算法。同时针对改进后的算法的安全性和效率与原算法进行了对比分析。

关键词: 密码学; 动态思想; SMS4 密码算法; 安全性

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)09-0086-03

An Improvement of SMS4 Algorithm Based on Dynamic

ZHOU Shu-yang, PENG Man-man, XIAO Xiao-huan

(Institute of Computer and Communications, Hunan University, Changsha 410082, China)

Abstract: SMS4 algorithm is the domestic encryption standard for WLAN use, released of The State Password Administration Offices in January 2006. This paper simply introduces the principle of SMS4 algorithm, improves the SMS4 algorithm based on dynamic thinking, also implements it and compare analysis the improved algorithm with SMS4 aiming at the security and efficiency.

Key words: cryptography; dynamic; SMS4; security

1 引言

SMS4 算法是国家商用密码管理办公室于 2006 年 1 月公布的用于无线局域网产品的分组对称密码算法。SMS4 算法是我国第一个公开的、针对无线局域网产品的密码算法^[1], 作为公众信息安全建设的基石, 应具有相当高的安全性, 但国内外相关研究表明其存在安全隐患。文中基于动态思想对原算法进行改进, 提高其安全性能。

2 SMS4 概述

SMS4 算法是一个分组算法。算法的分组长度为 128 比特, 密钥长度为 128 比特。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同, 只是轮密钥的使用顺序相反, 解密轮密钥是加密轮密钥的逆序。

2.1 加/解密算法

明文输入为 (X_0, X_1, X_2, X_3) , 密文输出为 (Y_0, Y_1, Y_2, Y_3) , 轮密钥为 $rk_i, i = 0, 1, \dots, 31$ 。则 SMS4 算法的加密变换为:

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \\ (Y_0, Y_1, Y_2, Y_3) &= R(X_{32}, X_{33}, X_{34}, X_{35}) \\ &= (X_{35}, X_{34}, X_{33}, X_{32}) \end{aligned}$$

本算法的解密变换与加密变换结构相同, 不同的仅是轮密钥的使用顺序。加密时轮密钥的使用顺序为: $(rk_0, rk_1, \dots, rk_{31})$, 解密时轮密钥的使用顺序为: $(rk_{31}, rk_{30}, \dots, rk_0)$ 。

其中 F 函数称为轮函数, F 定义:

$$F(X_0, X_1, X_2, X_3, rk) = X_0 \oplus T(X_1 \oplus X_2 \oplus X_3 \oplus rk)$$

T 函数是合成置换, 它是一个 $Z_2^{32} \rightarrow Z_2^{32}$ 的可逆

收稿日期: 2010-12-21; 修回日期: 2011-01-30

基金项目: 国家“八六三”计划项目(754209009)

变换,由非线性变换 τ 和线性变换 L 复合而成,即 $T(.) = L(\tau(.))$.

τ 由 4 个并行的 S 盒变换构成. 设输入为 $A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4$, 输出为 $B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$, 则:

$$(b_0, b_1, b_2, b_3) = \tau(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3))$$

非线性变换 τ 的输出是线性变换 L 的输入. 设输入为 $B \in Z_2^{32}$, 输出为 $C \in Z_2^{32}$, 则:

$$C = L(B) = B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B \ll 24)$$

$Sbox(.)$ 为 S 盒变换,是一个固定的 8 比特输入 8 比特输出的置换.

R 函数为反序变换:

$$R(A_0, A_1, A_2, A_3) = (A_3, A_2, A_1, A_0).$$

2.2 密钥扩展算法

加密算法的轮密钥由加密密钥通过密钥扩展算法生成. 加密密钥 $MK = (MK_0, MK_1, MK_2, MK_3), i = 0, 1, 2, 3$; 定义一个 32 位的 $K_i, i = 0, 1, \dots, 35$, 轮密钥为 $rk_i, i = 0, 1, \dots, 31$, 则轮密钥生成方法为:

$$\text{首先, } (K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$$

$$\text{然后, 对 } i = 0, 1, \dots, 31; rk_i = K_{i+4} = K_i \oplus T'(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$$

其中:

(1) T' 变换与加密算法轮函数中的 T 基本相同,只将其中的线性变换 L 修改为:

$$L(B) = B \oplus (B \ll 13) \oplus (B \ll 23)$$

(2) 系统参数 FK 的取值,采用 16 进制表示:

$$FK_0 = (A3B1BAC6), FK_1 = (56AA3350)$$

$$FK_2 = (677D9197), FK_3 = (B27022DC)$$

(3) 固定参数 CK 的取值方法为:设 $ck_{i,j}$ 为 CK_i 的第 j 字节 ($i = 0, 1, \dots, 31; j = 0, 1, 2, 3$), 即: $CK_i = (ck_{i,0}, ck_{i,1}, ck_{i,2}, ck_{i,3})$, 则 $ck_{i,j} = (4i + j) \times 7 \pmod{256}$.

3 基于动态思想对 SMS4 算法的改进

3.1 分组对称密码算法中的动态思想

密码算法设计的任务是对分组明文进行打乱、扩散处理,而攻击者试图破解密码是试图从大量的密文中获取某些隐含的明文的相关信息^[2-4]. 针对 SMS4 加密电路,采用差分功耗分析攻击方式进行密钥破解,其理论基础为集成电路中门电路在实现

加密算法时的物理特征、功耗模型及数据功耗相关性^[5]. 因此,要提高加密算法的抗攻击能力,就必需使解密者尽可能少地从加密过程中获得相关信息.

动态对称算法是基于对称加密算法架构,通过变化对称加密编制中的表、函数等要素,使其变化具有随机性,来实现动态对称加密编制^[6].

SMS4 密码算法中加密编制的要素包括:迭代的轮函数 F 、系统参数 CK 、固定参数 FK 等. 基于动态思想可将这些加密要素在保证正确合理的基础上,与随机函数相结合,从而使得原来固定公开的加密要素变成随机动态生成,与其他组件组成一套一次一变的加密编制. 随机函数的结果是生成临时加密编制中加密要素的依据,只要将这个结果与密钥一起通过其他安全通道发送给密文接受方,接收方根据解密算法就能正确解密.

3.2 对 SMS4 算法的改进

文中对 SMS4 的改进之处主要体现在以下两点:

(1) 将 32 个固定参数 CK 由“固定公开”修改为“动态随机生成”.

将 32 个固定参数表扩展为一个 16×16 的 CK 盒, CK 盒中共 256 个 CK 元素,每个元素 4 字节,以时间为种子,随机生成 32 个 2 字节的随机数,通过 $CKbox(.)$ 产生 32 个 4 字节的 CK 参数,将这 32 个 CK 参数作为 SMS4 算法中某一个临时编制的 32 个固定参数表. 其中 $CKbox(.)$ 类似于原算法中的 $Sbox(.)$,是一个固定的 16 位数据输入,32 位数据输出的置换.

将 32 个参数通过非对称加密算法构成的安全通道发送给接受方,从而达到动态 SMS4 编制一次一变. 同时,由于变化参数受到保密,则将已知编制转化成未知编制,增强了密文的安全性.

(2) 将 32 迭代所用轮函数由“固定函数”改为“动态选择”.

研究表明^[7] 将原轮函数:

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \end{aligned}$$

改为:

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus T(X_{i+1} + X_{i+2} + X_{i+3} \oplus rk_i) \end{aligned}$$

即把原算法中 $X_{i+1}, X_{i+2}, X_{i+3}$ 的异或运算替换有进位的加法是可行的、正确的,通过有进位的加法使 $X_{i+1}, X_{i+2}, X_{i+3}$ 的每一个比特都会影响到相加和的每一个比特,打破 data 数据中各比特位之间的独

立关系,增加安全性.但无论是原算法轮函数的“ $\oplus$ ”还是替换后的“ $+$ ”,32 轮迭代都是使用相同的轮函数,对密文的安全性留下隐患.根据动态算法的思想,将 32 迭代所用轮函数由“固定函数”改为“动态选择”,对每轮使用的轮函数在使用“ $\oplus$ ”还是“ $+$ ”运算时进行动态随机选择.在对密码进行迭代之前以时间为随机种子,使用随机函数 $K(\text{time})$ 生成一个 4 字节 32 位的随机数 G , G 的每一位作为每一轮迭代时选择“ $\oplus$ ”还是“ $+$ ”运算的轮函数,为 0 选择使用“ $\oplus$ ”的轮函数,为 1 选择使用“ $+$ ”的轮函数.

定义函数 G' :

$$G' = H(a_0, a_1, a_2, \cdots a_{31}) = (a_{31}, a_{30}, \cdots a_0)$$

其中, $a_i (i = 0, 1, 2 \cdots 31)$ 为 1bit 数据.将 $G' = H(G)$ 通过非对称加密算法构成的安全通道发送给接受方,作为解密时每一轮迭代选择轮函数的根据.

改进后算法的轮函数如图 1 所示.

4 改进后的 SMS4 算法的实现与评价

在 VC 环境下采用 C 语言实现了 SMS4 算法和改进后的算法,并选取算法的效率和和密文安全性

两项指标进行对比分析.从占用的时间资源来评价算法的效率.

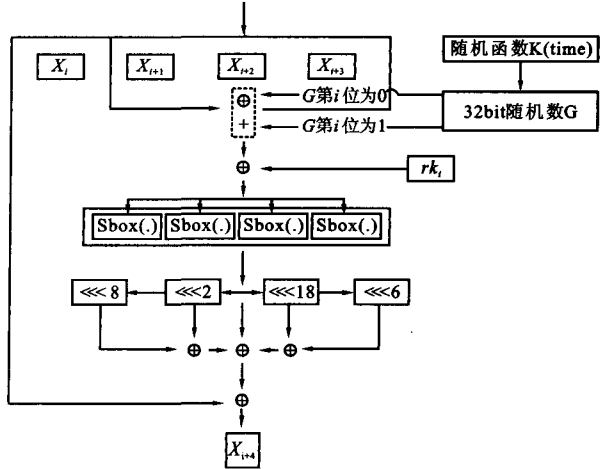


图 1 改进算法轮函数示意图

在同一台 PC 机上对同 10 组明文加密 10^4 次进行实验测试.设总运行时间为 t 秒,则加密一组 128 bit 明文所需时间为 $t/10^4$.使用同一组密钥测试 5 次,再取其平均值作为占用时间资源这个指标进行评价.算法效率指标的对比实验数据如表 1 所示.

表 1 算法效率对比分析

算法	加密时间 / μs					平均时间 / μs
	第一次	第二次	第三次	第四次	第五次	
原算法	35.67	35.73	35.61	35.71	35.65	35.67
改进后的算法	35.79	35.81	35.76	35.86	35.80	35.80

算法加密的密文安全性,主要从扩散性的角度对改进后的算法进行安全性分析.

扩散性是指所设计的密码体制使明文的每一位数字影像密文的许多位数字,以便隐蔽明文数字的统计特性.密码的雪崩效应是指明文的一点微小的变化会使得密文发生一个很大的变化.当改变明文的任何一个比特时,对应密文改变的比特个数是一个随机变量,如果其平均长度是分组长度的一半,则称该密码体制实现了“雪崩性”^[7].

根据扩散性概念,取 100 组明文数据,对每组明文改变任一比特时测试其密文比特改变个数,取其均值测试改进算法的扩散性.算法安全性指标的对比实验数据如表 2 所示.

表 2 算法安全性对比分析

算法	密文改变比特个数的均值
原算法	63.21
改进后的算法	66.09

5 结束语

文中基于动态思想对 SMS4 算法进行了改进,随机生成 32 个固定参数 CK、动态选择 32 轮迭代所用轮函数.改进后的算法用极少量的时间代价换取了可观的安全性能的提升,有广泛的应用价值.

参考文献:

[1] 国家密码管理局.无线局域网产品使用的 SMS4 密码算法[EB/OL]. [2006-01-06]. <http://www.oscca.gov.cn/>.

[2] 刘文华,杜现朝,耿乔科.改进的 SMS4 算法差分故障与暴力联合攻击[J].计算机工程与设计,2009,30(18): 4204-4206.

[3] 张鹏,邓高明,邹程,等.差分功率分析攻击中的信号处理与分析[J].微电子学与计算机,2009,26(11):1-4.

[4] 陈财森,王韬,陈建泗,等.基于 Cache Missing 的 RSA

(下转第 92 页)

Q_3 对因素 A_1, A_2, A_3 的变权值及综合评估值和文献 [3] 以基础权重为权值的“常权综合评估值”, 结果如表 2 所示.

表 2 综合评估值

方案	A_1	A_2	A_3	综合值	常权综合值
Q_1	0.717	0.179	0.104	34.46	49.29
Q_2	0.522	0.391	0.087	42.95	46.96
Q_3	0.413	0.405	0.182	66.16	70.22

由表 2 可知, 由文中提出的变权法综合评估值, 三个方案的排序为 $Q_3 > Q_2 > Q_1$, 在这三个方案中, 优选 Q_3 , 依据 Q_3 的综合值隶属于 $u_T(A) \in [50, 75]$, 于是对实体的评估结果为“很信任”; 而按常权综合值排序为 $Q_3 > Q_2 > Q_1$. 由于 Q_1 关于 A_1 的评估值很低, 为了保证 A_1 不被剔除, 突出了 A_1 的权值, 故 Q_1 排在最后是必然的, 所以按照常权综合值的方法是不理想的.

4 结束语

文中引入模糊决策理论中的隶属度的概念来描述信任的模糊性, 并定义了信任等级和综合评估机制^[7]. 此外, 依据评估值动态变化, 利用变权法实现了主观信任评估权值的动态分配, 突出了权值较小因素在评估中的作用. 同时对信任的程度进行了等级划分, 最后利用基于综合评估得到的可信值, 评估信任模型的信任等级.

参考文献:

- [1] 林闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751-757.
- [2] Abdul-Rahman A, Hailes S. A distributed trust model [C]//Proceedings of the 1997 New Security Paradigms Workshop. Golumbria, UK: ACM Press, 1998: 48-60.
- [3] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401-1408.
- [4] Beth T, Borchherding M, Klein B. Valuation of trust in open network[C]//Proceedings of the European Symposium on Research in Security (ESORICS). Brighton: Springer-Verlag, 1994: 3-18.
- [5] 陈书义, 闻英友, 赵宏. 基于模糊集合的可信计算信任模型评估[J]. 计算机科学, 2008, 35(11): 39-42.
- [6] 黎梨苗, 陈志刚, 邓晓衡, 等. 基于模糊理论的主观信任综合评价模型研究[J]. 计算机应用研究, 2010, 27(5): 1860-1862.
- [7] 张景安, 赵慧勤. P2P 网络中模糊信任模型研究[J]. 微电子学与计算机, 2009, 26(8): 158-162.

作者简介:

左双勇 男, (1985-), 硕士研究生. 研究方向为信息安全、可信计算.

陈光喜 男(1971-), 博士, 教授. 研究方向为信息安全、智能软件与算法.

丁勇 男(1975-), 博士, 教授. 研究方向为密码学与信息安全.

王祥玲 女(1986-), 硕士研究生. 研究方向为控制与决策理论.

(上接第 88 页)

计时攻击[J]. 微电子学与计算机, 2009, 26(5): 180-182.

[5] 李浪, 李仁发, 李静, 等. 一种 SMS4 加密算法差分功耗攻击[J]. 计算机科学, 2010, 37(7): 39-41.

[6] 胡样义, 刘彤. 动态对称密码算法的研究与探讨[J]. 网络安全技术与应用, 2006(3): 69-71.

[7] 郑秀林, 李敏. SMS 算法的一种改进[J]. 北京电子科技学院学报, 2007, 15(4): 16-18.

作者简介:

周术洋 男, (1983-), 硕士研究生. 研究方向为嵌入式计算.

彭蔓蔓 女, (1964-), 教授. 研究方向为计算机体系结构.

肖小欢 男, (1985-), 硕士研究生. 研究方向为嵌入式计算.