基于双伪随机变换和Feistel结构的轻量级分组密码VHF

代学俊 黄玉划 刘宁钟
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 针对资源受限的移动终端对轻量级密码的需求,提出了一种基于双伪随机变换和Feistel结构的新的轻量级分组密码算法VHF。类似于许多其他轻量级分组密码,VHF的分组长度为128bit,密钥长度为80bit和128bit。VHF的安全评估结果表明,其可以对已知的攻击实现足够的安全性,如差分分析、线性分析和不可能差分分析等。在安全的基础上测试软件效率及硬件实现,与现有的轻量级分组密码进行的对比表明,VHF的软硬件效率都高于同为面向8位平台的国际标准CLEFIA算法。

关键词 轻量级分组密码,硬件实现,安全分析
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.02.030

VHF: A Lightweight Block Cipher Based on Dual Pseudo-random Transformation and Feistel Structure

DAI Xue-jun HUANG Yu-hua LIU Ning-zhong
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract A new lightweight block cipher based on double pseudo random transform and Feistel structure called VHF was proposed for the demand of the resource constrained mobile terminal for the lightweight cipher. Similar to many other lightweight block ciphers, the block size of VHF is 128bit and the key size is 80bit and 128bit. Security evaluation of VHF shows that VHF can achieve enough security margin against known attacks, such as differential cryptanalysis, linear cryptanalysis, and impossible differential cryptanalysis etc. Furthermore, VHF can be implemented efficiently not only in hardware environments but also in software platforms such as 8bit microcontroller. The implementation efficiency of both software and hardware based on VHF is higher than CLEFIA algorithm, which is the international standard also oriented to 8bit platform.

Keywords Lightweight block cipher, Hardware efficiency, Cryptanalysis

1 介绍

近年来,大量安全和高性能的分组密码设计推动了密码学的发展,例如AES[1],Camellia和SHACAL等。然而,随着无线网络技术的发展,普通的分组密码算法难以满足资源受限的移动终端,需要轻量级密码算法来满足软硬件、计算能力和能耗等资源受限终端的需求。CLEFIA[2]和PRESENT[3]作为轻量级分组密码的杰出代表,为基于当前最先进的技术设计适用于资源受限的移动终端提供了良好的时机。分组密码[4]是这样一个数学变换:它首先将明文消息用二进制数字序列$x_1, x_2 \cdots$编码表示,并划分成长为m的分组$x=(x_1, x_2, \cdots, x_m)$,然后在密钥$k=(k_1, k_2, \cdots, k_t)$的作用下,将各分组信息分别变换成等长的数字序列$y=(y_1, y_2, \cdots, y_n)$后输出,这个过程可以用如图1所示的数学模型表示。

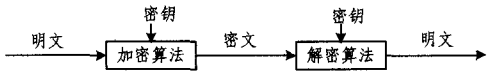

图1 分组密码的数学模型

本文提出了一种新的轻量级分组密码VHF,即Vertical Horizontal Feistel(纵横),整体采用Feistel结构,轮函数采用行伪随机变换和对角线伪随机变换。VHF是将128bit明文分为长度为64bit的左右两个分支,轮函数采用双伪随机变换进行扩散和混淆,支持长度为80bit和128bit的密钥。VHF新颖的设计方法之一是采用伪随机变换构造256bit的加密变换表,简化了S盒的设计,充分体现了轻量级分组密码的实现占用空间小的特点。此外,VHF经过P置换后,对已置换过的对角线数据进行伪随机变换,提高了它的安全性。VHF对当前已知的攻击方法达到了足够的免疫力并且在硬件实现和软件消耗上呈现高效性。VHF的硬件实现需要1632个GE数,软件效率为50.82Mb/s。而CLEFIA的硬件实现达到了5979个GE数,软件效率为33.90Mb/s。我们认为VHF算法的软硬件效率都高于同为面向8位平台的国际标准CLEFIA算法,VHF在安全和性能上取得了优越的平衡性,在满足安全性的基础上提高了软件效率,并且兼顾了硬件效率,这使得其更加实用。

到稿日期:2015-11-18 返修日期:2016-03-01 本文受江苏省科技支撑计划项目(BE2013879),南京航空航天大学青年科技创新基金项目(NS2010097)资助。

代学俊(1991—),女,硕士生,主要研究方向为信息安全,E-mail:daixuemai@163.com;黄玉划(1975—),男,博士后,副教授,主要研究方向为信息安全与保密等;刘宁钟(1975—),男,博士,教授,博士生导师,主要研究方向为嵌入式系统等。

2 VHF 算法

2.1 符号及术语说明

本文采用的符号及说明如表 1 所列。

表 1　VHF 算法采用的符号说明

符号	说明
F	轮函数
K_0	初始密钥
L_0	左支初始数据
R_0	右支初始数据
$S[256]$	加密变换表
$\|$	连接运算
$\oplus$	异或运算
&	与运算

2.2 VHF 算法描述

本文所述的轻量级分组密码算法 VHF 采用 Feistel[4] 结构，如图 2 所示，其分组长度为 128bit，并且分为长度为 64bit 的两个分支 L_0 和 R_0，支持长度为 80bit 和 128bit 的密钥，相应的迭代轮数分别为 $r=14,16$。轮函数 F 采用行伪随机变换、对角线随机变换。一轮 Feistel 通过如下计算输出 $L_1 \| R_1$：$L_1=R_0$，$R1=L_0\oplus F(R_0,K_0)$，经过 r 轮迭代后得到最后的加密结果 $L_r \| R_r$。

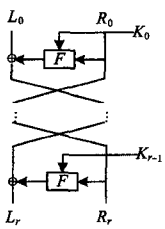

图 2　Feistel 结构

2.2.1 轮函数

VHF 算法的分组长度为 128bit，并且支持 80bit 和 128bit 长度的密钥，迭代伦数为 $r=14,16$。该算法采用 Feistel 结构，将 128bit 的分组分为 64bit 的左右两个分支 L_i 和 R_i，然后进行 r 轮完全相同的运算。加密过程为：

$L_i=R_{i-1}$

$R_i=L_{i-1}\oplus F(R_{i-1},K_{i-1})$

其中轮函数 F 采用双伪随机变换的加密流程，轮函数 F 为：

SBoxLayer(R_{r-1})

SBoxLayer(PLayer(R_{r-1}))

• SBoxLayer()：它是一个关于字节的非线性变换，将加密过程中的每个字节非线性地变换为另外一个字节。S 盒采用伪随机变换的方法产生。先计算 $T(i)=\lceil|256\sin i|\rfloor$，其中 $\lceil\ \rfloor$ 表示向下取整运算；为了产生不重复的 256 个字节，i 的取值为 1 到 30000，遇到重复的则将其排除，直到产生全部不重复的 256 个字节为止。加密变换表 $S[256]$ 是 256 个字节的一个伪随机排列，由 T 中字节轮换得到：$S[T(j)]=T(j+1)$，$S[T(255)]=T(0)$，其中 $0\leqslant j\leqslant 254$。对数据进行行伪随机变换，即对数据的每个字节用加密 S 盒进行伪随机变换：$M_i(j)=S[C_{i-1}(j)]$；其中 i 从 1 到 r 取值，$M_i(j)$ 表示 M_i 的第 j 个字节，$0\leqslant j\leqslant 7$。

• SBoxLayer(PLayer(R_{r-1}))：它是将每一个字节进行对角线伪随机变换成另一个字节。把 64bit 数据排成 8 * 8 的方阵，如图 3 所示，对 M_i 的每个斜对角线用加密 S 盒进行伪随机变换：

$P_i(0)=S\{[M_i(0)\&128]|[M_i(1)\&64]|[M_i(2)\&32]|[M_i(3)\&16]|[M_i(4)\&8]|[M_i(5)\&4]|[M_i(6)\&2]|[M_i(7)\&1]\}$

$P_i(1)=S\{[M_i(1)\&128]|[M_i(2)\&64]|[M_i(3)\&32]|[M_i(4)\&16]|[M_i(5)\&8]|[M_i(6)\&4]|[M_i(7)\&2]|[M_i(8)\&1]\}$

$P_i(2)=S\{[M_i(2)\&128]|[M_i(3)\&64]|[M_i(4)\&32]|[M_i(5)\&16]|[M_i(6)\&8]|[M_i(7)\&4]|[M_i(0)\&2]|[M_i(1)\&1]\}$

$P_i(3)=S\{[M_i(3)\&128]|[M_i(4)\&64]|[M_i(5)\&32]|[M_i(6)\&16]|[M_i(7)\&8]|[M_i(0)\&84]|[M_i(1)\&2]|[M_i(2)\&1]\}$

$P_i(4)=S\{[M_i(4)\&128]|[M_i(5)\&64]|[M_i(6)\&32]|[M_i(7)\&16]|[M_i(0)\&8]|[M_i(1)\&84]|[M_i(2)\&2]|[M_i(3)\&1]\}$

$P_i(5)=S\{[M_i(5)\&128]|[M_i(6)\&64]|[M_i(7)\&32]|[M_i(0)\&16]|[M_i(1)\&8]|[M_i(2)\&84]|[M_i(3)\&2]|[M_i(4)\&1]\}$

$P_i(6)=S\{[M_i(6)\&128]|[M_i(7)\&64]|[M_i(0)\&32]|[M_i(1)\&16]|[M_i(2)\&8]|[M_i(3)\&84]|[M_i(4)\&2]|[M_i(5)\&1]\}$

$P_i(7)=S\{[M_i(7)\&128]|[M_i(0)\&64]|[M_i(1)\&32]|[M_i(2)\&16]|[M_i(3)\&8]|[M_i(4)\&84]|[M_i(5)\&2]|[M_i(6)\&1]\}$

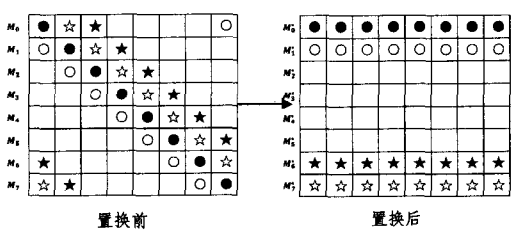

图 3　P 置换过程

2.2.2 密钥扩展

通过递推进行密钥扩展，将 L 字节的密钥 K 扩展成 $L*r$ 字节，其中 $L=10,16$；扩展密钥 $Key=K_0|K_1|\cdots|K_i|\cdots|K_{r-1}=k_0|k_1|\cdots|k_j|\cdots|k_{L*r-1}$，每个 K_i 为 L 字节，$0\leqslant i\leqslant r$；每个 k_j 为单元字节，$0\leqslant j\leqslant L*r-1$。对于 10bit 和 16bit 的密钥 K，相应的迭代轮数 $r=14,16$。扩展密钥 Key 的前 L 字节就是密钥 K：$K=k_0|k_1|\cdots|k_{L-1}$（$L\leqslant j\leqslant L*r-1$）时，扩展密钥 Key 中的 k_i 由 k_{i-L} 和 k_{i-1} 两个字节递推得到，即 $k_i=S[k_{i-1}]\oplus k_{i-L}$。

最后再将上述输出 P_i 与该轮的子密钥 K_i 进行异或得到该轮的 F_i，最终得到 $R_{i+1}=L_i\oplus F_i$。经过 r 轮加密后由 (L_r,R_r) 级联得到密文比特串。

3 VHF 算法的软硬件实现

由于轻量级分组密码的应用环境对能耗、成本及存储方

面有非常严格的限制，因此在保证一定安全性的情况下，设计轻量级分组密码要考虑的首要问题就是实现性能。轻量级分组密码有面向硬件的设计、面向软件的设计和兼顾硬件和软件目标平台的设计。每种轻量级分组密码都会受到实现性能的评估，分析硬件、软件实现所需资源和运行效率，进而为不同种类的受限设备采用何种轻量级分组密码提供参考。在评估轻量级分组密码的硬件和软件实现性能时是分开进行的，因为它们有不同甚至是相反的特性。对于软件实现，一般考虑它执行的时间以及效率；对于硬件实现，则用等效门电路数即 GE 数来衡量。

3.1 软件效率

在 Intel(R)、Core(TM)、CPU 为 i7-3610QM、主频 2.3 GHz、内存 8GB、C 语言编程环境下对 VHF-80 和 VHF-128 分别进行测试，循环次数为 $1\times10^6\sim6\times10^6$，经过测试，VHF 算法所需要的执行时间如图 4 所示，随着循环次数的增大，所需时间明显增大；随着密钥长度的增加，执行时间也有所增加。在循环次数为 10^6 时，VHF-80 和 VHF-128 所需时间分别为 2.308s 和 2.991s。

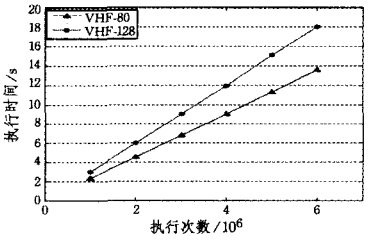

图 4 VHF 算法软件实现的执行时间

VHF 算法与其他轻量级分组密码算法的软件效率对比如图 5 所示，VHF-80 的软件效率大约为 50.82Mb/s，明显高于 PRESENT-80 算法的0.98Mb/s 和 MIBS-80 算法的33.26 Mb/s。VHF-128 的软件效率大约为 41.11Mb/s，与 CLEFIA-128 的 33.9Mb/s 比较可知，VHF-128 的软件实现优于同为面向 8 位平台的国际标准 CLEFIA。因此，VHF 算法的软件效率优于其他轻量级分组密码算法。

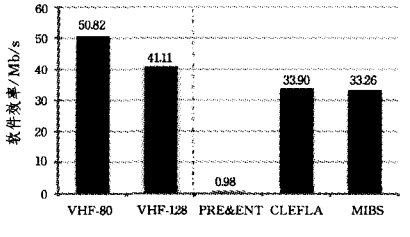

图 5 VHF 与其他轻量级分组密码的软件效率比较

3.2 硬件实现

硬件实现效率一般用等效 GE 数来衡量。文献[2]对 CLEFIA-128 算法硬件实现的 GE 数做了估算，作者认为忽略不同的 ASIC 库的影响，实现 CLEFIA-128 算法需要 5979 个 GE 数。文献[2]指出存储 1 个比特需要 6 个 GE 数，实现 1 次异或运算需要约 2.67 个 GE 数。

VHF 算法的硬件实现所需的 GE 数如表 2 所列，VHF-80 算法密钥扩展中字节的异或运算需要 1 个异或门，共 2.67 个 GE 数；每轮需存储长度为 80bit 的子密钥，共 480 个 GE 数。加密过程中，存储 128bit 的明文分组需要 768 个 GE 数；S 盒需要 200 个 GE 数；加密过程中采用 64 个与门，共 85.12 个 GE 数；采用 56 个或门，共 74.48 个 GE 数；每轮加密明文需要和子密钥进行异或运算，需要 8 个异或门，共21.36个 GE 数。VHF-80 和 VHF-128 硬件实现分别需要 1632 个 GE 数和 1920 个 GE 数，符合轻量级分组密码应用环境的硬件需求。

表 2 VHF 算法的硬件实现/GE

VHF	密钥扩展	加密过程	总共
VH-80	482.67	1148.96	1631.63
VH-128	770.67	1148.96	1919.63

VHF 算法与其他轻量级分组密码算法的硬件实现所需要的门电路数如图 6 所示，VHF-80 大约为 1632 个 GE 数，与同样采用 80bit 的 PRESENT 和 MIBS 的硬件实现相当。VHF-128 大约 1920 个 GE 数，与 CLEFIA-128 的硬件实现所需要的门电路数 5979 个 GE 数比较可知，VHF-128 的硬件实现优于同为面向 8 位平台的国际标准 CLEFIA。

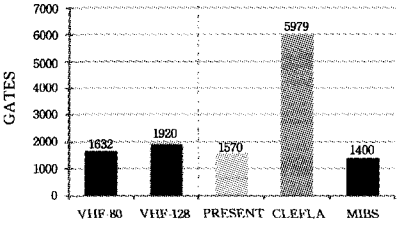

图 6 VHF 与其他轻量级分组密码的硬件实现比较

4 VHF 算法的安全性分析

4.1 差分分析和线性分析

差分分析[6]和线性分析[7]一直以来都是针对分组密码最有效的攻击手段，文献[6-7]详细论述了评估密码抗差分和线性分析能力的实际方法，即通过计算活动 S 盒的个数来计算最大差分和线性概率，文献[2]在对 CLEFIA 算法进行评估时运用了这种方法。

通过计算可得 VHF 算法的 S 盒的最大差分概率是 $2^{-4.415}$，通过程序计算得到 VHF 算法 14 轮的活动 S 盒的个数 DS，如表 3 所列。由此可得 VHF 算法的 6 轮最大差分概率 $DCP^{6r}_{max}\leqslant 2^{35\times(-4.415)}=2^{-154.525}\leqslant 2^{-128}$。当迭代轮数大于 6 时，找不到一个有效的差分特征进行分析，所以完整轮数的 VHF 算法可以抵抗差分分析。

表 3 VHF 算法的差分和线性活动 S 盒个数

轮数	DS	LS
1	0	0
2	7	8
3	14	16
4	21	24
5	28	32
6	35	40
7	42	48
8	49	56
9	56	64
10	63	72
11	70	80
12	77	88
13	84	96
14	91	104

（下转第 201 页）

Fundamentals of Electronics Communications & Computer Sciences, 1996, 79(9): 1338-1354.

[9] ATENIESE G, BURNS R C, CURTMOLA R, et al. Provable data possession at untrusted stores[C] // Proceedings of the 14th ACM Conference on Computer and Communications Security. 2007: 598-609.

[10] JUELS A, KALISKI JR B S. PORs: Proofs of retrievability for large files[C] // Proceedings of the 14th ACM Conference on Computer and Communications Security. ACM, 2007: 584-597.

[11] ATENIESE G, DI PIETRO R, MANCINI L V, et al. Scalable and efficient provable data possession[C] // Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks. ACM, 2008: 1-10.

[12] ERWAY C. Dynamic provable data possession[C] // Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, 2009: 213-222.

[13] WANG C, WANG Q, REN K. Ensuring data storage security in cloud computing[C] // 17th International Workshop on Quality of Service, 2009. IWQoS. 2009.

[14] WANG Q, WANG C, LI J, et al. Enabling public verifiability and data dynamics for storage security in cloud computing[M] // Computer Security (ESORICS 2009). Springer Berlin Heidelberg, 2009: 355-370.

[15] WANG C, WANG Q, REN K, et al. Privacy-preserving public auditing for data storage security in cloud computing[C] // 2010 Proceedings IEEE INFOCOM. 2010: 1-9.

[16] WANG Q, WANG C, REN K, et al. Enabling public auditability and data dynamics for storage security in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(5): 847-859.

[17] KIM S, PARK S, WON D. Proxy signatures, Revisited [J]. Information and Communications Security, 1997: 223-232.

[18] http://wiki.apache.org/hadoop/#MapReduce.

[19] GUO Peng. Cassandra in Action. China Machine Press.

(上接第 194 页)

通过计算可得 VHF 算法的 S 盒的最大线性概率是 $2^{-2.83}$，通过程序计算得到 VHF 算法 14 轮活动 S 盒的个数 LS，如表 3 所列。由此可得 VHF 的 7 轮最大线性概率为 $LCP_{\max}^{7r} \leqslant 2^{48\times(-2.83)} = 2^{-135.84} \leqslant 2^{-128}$。当迭代轮数大于 7 时，找不到一个有效的线性特征进行分析，所以完整轮数的 VHF 算法可以抵抗线性分析。

4.2 不可能差分分析

不可能差分分析[8]对 VHF 算法来说是一种非常有效的攻击手段。J. Kim 等[9]发明了一种矩算法 μ-method 用来对分组密码的结构进行不可能差分分析，该方法能够找到不同的不可能差分路径。采用此方法对 VHF 算法进行不可能差分分析得到的最大轮数为 6，找到了 8 条不可差分路径。

$$(0,0,0,\alpha,0,\alpha,\alpha,\alpha) \xrightarrow{6r} \not\rightarrow (0,0,0,0,\alpha,\alpha,\alpha,\alpha), p=1$$

$$(0,0,\alpha,0,\alpha,\alpha,\alpha,0) \xrightarrow{6r} \not\rightarrow (0,0,0,0,\alpha,\alpha,\alpha,\alpha), p=1$$

$$(0,\alpha,0,\alpha,\alpha,\alpha,0,0) \xrightarrow{6r} \not\rightarrow (0,0,0,\alpha,\alpha,\alpha,\alpha,0), p=1$$

$$(0,\alpha,\alpha,\alpha,0,0,0,\alpha) \xrightarrow{6r} \not\rightarrow (0,\alpha,\alpha,\alpha,\alpha,0,0,0), p=1$$

$$(\alpha,0,0,0,\alpha,0,\alpha,\alpha) \xrightarrow{6r} \not\rightarrow (\alpha,\alpha,0,0,0,0,\alpha,\alpha), p=1$$

$$(\alpha,0,\alpha,\alpha,\alpha,0,0,0) \xrightarrow{6r} \not\rightarrow (0,0,\alpha,\alpha,0,0,0,0), p=1$$

$$(\alpha,\alpha,0,0,0,\alpha,0,\alpha) \xrightarrow{6r} \not\rightarrow (\alpha,\alpha,\alpha,0,0,0,0,\alpha), p=1$$

$$(\alpha,\alpha,\alpha,0,0,0,\alpha,0) \xrightarrow{6r} \not\rightarrow (\alpha,\alpha,\alpha,\alpha,0,0,0,0), p=1$$

其中，$\alpha \in GF(2^8)$，表示非零差分。由此可知，不可能差分分析对 VHF 算法攻击无效。

结束语　本文提出了一种基于双伪随机变换和 Feistel 结构的轻量级分组密码算法 VHF，并将其应用于无线通信中低成本嵌入式移动终端。通过产生加密变换表 S[256]进行行伪随机变换和对角线伪随机变换，实现混淆和扩散。通过软件效率测试与 MIBS, CLEFIA, PRESENT 等轻量级分组密码算法进行比较得出，VHF 算法的软件实现性能优异；通过硬件实现与其他轻量级分组密码算法进行比较，得到的 1632 个 GE 数高于国际标准算法 CLEFIA 得到的 5979 个 GE 数；总体来说，VHF 算法的软件效率和硬件实现都高于同为面向 8 位平台的国际标准 CLEFIA 算法。对 VHF 算法采用差分、线性分析和不可能差分分析方法进行安全分析，验证了 VHF 算法的安全性。

参 考 文 献

[1] DAEMEN J, RIJMEN V. The design of Rijndael: AES-the advanced encryption standard [M]. Berlin Heidelberg: Springer, 2002: 10-18.

[2] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128-bit Blockcipher CLEFIA, 2007[C] // Proceedings of the 14th International Conference on Fast Software Encryption. Berlin Heidelberg: Springer, 2007: 181-195.

[3] BOGDANOV A, KNUDSEN L R, LEADER G, et al. PRESENT: An ultra-lightweight block cipher[J]. Lecture Notes in Computer Science, 2007: 450-466.

[4] WU W L, FENG D G, ZHANG W T. Design and analysis of Block cipher [M]. Beijing: TsingHua University Press, 2009: 5-20. (in Chinese)
吴文玲，冯登国，张文涛. 分组密码的设计与分析[M]. 北京：清华大学出版社，2009：5-20.

[5] IZADI M, SADGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C] // International Conference on Cryptology and Network Security Berlin Heidelberg: Springer, 2009: 334-348.

[6] BIHAM E, SHAMIR A. Differential cryptanalysis of the data encryption standard [M]. New York: Springer-Verlag, 1993.

[7] MATSUI M. Linear Cryptanalysis Method for DES Cipher, 2007 [M]. Berlin Heidelberg: Springer, 1994: 386-397.

[8] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, 1999 [M]. Berlin Heidelberg: Springer, 1999: 12-23.

[9] KIM J, HONG S, SUNG J, et al. Impossible Differential Cryptanalysis for Block Cipher Structures[J]. Lecture Notes in Computer Science, 2003, 2904: 82-96.