一种新的密码算法设计方法

杨宏志 韩文报 斯雪明
(信息工程大学信息工程学院 郑州 450002)

摘 要 将可重构的概念引入密码算法设计中,创造性地提出密码算法簇的概念,通过密钥控制密码算法结构变化,不但提高了密码算法的灵活性,同时也适应了多层次不同用户的安全需求。分析了密码算法簇的安全性和实现效率,并结合AES算法给出了一个密码算法簇的例子。

关键词 密码算法簇,可重构,一次一密
中图法分类号 TP309 **文献标识码** A

New Design Method for Cipher Algorithms for Block Cipher

YANG Hong-zhi HAN Wen-bao SI Xue-ming
(Institute of Information Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract The reconfiguration idea was introduced into the design of cryptography algorithms, and the concept of cipher cluster was creatively proposed. Variation of cipher architecture was controlled by keys, which could not only enhance flexibility of algorithms but also suite to security needs of different users at variety levels. Security and performance of cipher cluster were analyzed, and a paradigm was given using AES cipher.

Keywords Cipher cluster, Reconfigurable, One-time-pad

1 引言

从工程实现和安全性的角度出发,密码学者一直致力于寻找实现简单而且密码结构好的组件设计分组密码算法,比如AES的扩散层,它采用最优分支数的线性变换,同时其对应矩阵选取合理,便于硬件快速实现;AES的S盒基于有限域上乘法求逆运算,差分均匀性和线性偏差都达到了最佳,同时8×8的S盒硬件实现代价很小。但是随着密码理论研究的深入,新的密码分析技术层出不穷,比如代数攻击、旁路攻击等等,现阶段认为安全的密码算法无法保证不被未来的密码分析方法所攻击。

另一方面,专用密码芯片的核心部件都是确定且不可更改的,一旦该算法被攻破,将会存在极大的安全隐患;安全机制往往要求硬件电路能够支持多种密码算法,以便满足不同用户安全需求和密码算法升级换代的需要。如何在算法硬件实现中提供足够的灵活性是密码算法设计者需要考虑的问题。

本文将可重构的概念引入密码算法设计中,创作性地提出密码算法簇的概念,以在保证算法安全性的同时,提高密码算法的灵活性,进而满足多层次的用户安全需求。

本文的研究对象限定为分组密码。

2 密码算法簇

2.1 背景

随着集成电路和微电子技术的发展,可重构技术目前已经成为学术界和工业界的研究热点。在信息安全领域应用中,一方面,可重构技术灵活性大、开发成本小、周期短等方面的优点使得它很适合实现密码算法;另一方面,不同密码用户多层次的安全性能需求和密码算法不断升级换代的需求,使得密码芯片必须支持多种密码算法。

目前在密码学中可重构技术相关的研究主要集中在现有密码算法的可重构实现方面,通过利用可重用的硬件资源,将密码算法运算单元细化,实现可重构,在保证效率的同时一定程度上提高逻辑电路应用的灵活性。主要的研究内容有可重构体系结构研究、可重组密码逻辑设计等,研究成果参见文献[1-3]。但这种实现方式,由于密码算法结构固定,不同的密码算法相似的运算颗粒度很小,导致最终的逻辑电路效率大大折扣。

我们将工程实现中可重构的思想引入密码算法设计中,在密码算法安全性保证的前提下,不但可以使密码算法设计更加贴近工程实现,降低硬件电路的资源消耗,提高密码算法的实现效率,而且由于密码算法运算单元参数化,使得硬件电路支持密码算法变化,在应用中提高密码算法的使用灵活度,增强密码算法的应用安全性,可以满足多层次不同用户的安全需求。

2.2 概念

从密码安全性的角度,一次一密是绝对安全的,但是这种加密方式由于其生产、存储的高成本制约,应用场合仅限于高

到稿日期:2009-08-19 返修日期:2009-10-26 本文受国家863计划(2006AA01Z425),国家自然科学基金重大研究计划(90104035)资助。
杨宏志(1978—),男,博士生,主要研究方向为密码理论,E-mail:hz_yang@sohu.com;韩文报(1963—),男,博士生导师,主要研究方向为密码理论、网络安全;斯雪明(1966—),男,副研究员,主要研究方向为密码理论、网络安全。

度机密的低带宽信道[4]。

一次一密的加密映射由密钥唯一决定，也就是说 $\forall K_1, K_2 \in \kappa$，当 $K_1 \neq K_2$ 时，加密映射 $E_1 \neq E_2$，而现有绝大多数加密算法的加密映射与密钥无关。很自然地，我们会问：能否在密钥发生变化时部分地更改加密算法？这样设计密码算法的好处在于不但有效降低了一次一密密钥维护的成本，而且很大程度上可以提高密码算法的灵活性，进而满足多层次用户的安全需求。

我们剖分密钥空间 $\kappa=(\kappa_f,\kappa_d)$，使得加密映射 E 由密钥空间 κ 的子空间 κ_f 决定。由此，给出分组密码簇的概念。

定义 1[5] n 比特分组密码是指函数 $E:V_n\times\kappa\to V_n$ 对于每个密钥 $K\in\kappa$，$E(P,K)$ 是一个从 V_n 到 V_n 的可逆映射（密钥为 K 时的加密函数）。它的逆映射为解密函数，记为 $D(C,K)$。

假设函数 $E:V_n\times\kappa\to V_n$ 对于每个密钥 $(K_f,K_d)\in\kappa'$，$E(P,K_f,K_d)$ 是一个从 V_n 到 V_n 的可逆映射（密钥为 K 时的加密函数）。它的逆映射为解密函数，记为 $D(C,K_f,K_d)$。

定义 2 n 比特分组密码簇是指集合 $\{(E,K_f)\mid E:V_n\times\kappa'\to V_n,(K_f,*)\in\kappa'\}$。

显然，定义 1 中的分组密码 E 为映射，与 P,K 取值无关，定义 2 中的分组密码簇为映射集合，具体的映射 E 由 K_f 取值唯一决定。

GOST 算法是前苏联设计的分组密码算法，它已经具备了密码算法簇的雏形。可以认为 GOST 具有 610 比特左右的有效密钥[6]，其中 256 比特用于代表加密过程的密钥，即 K_d，其余的密钥用于 8 个 S 盒的编码，即 K_f，每个 S 盒是[0，1，…，15]整数的置换。在实际应用中，设计者生成一个相对较小的 S 盒选择集合，通过密钥 K_f 从选择集合中指定 S 盒。

在实际的密码算法设计中，从安全性和实现效率等多方面考虑，密码算法簇中若干算法的整体框架应该一致，在密钥 K_f 的作用下，算法单元和参数可灵活变化，而算法安全性和实现效率应当基本一致。

3 安全性与效率

分组密码的密码设计需要考虑安全性和实现效率两个方面。

3.1 概念

差分密码分析和线性密码分析是分组密码安全性分析中最重要、最基本的两种方法。估计密码抵抗这两种攻击的能力，是分组密码设计者必须考虑的问题。通常我们在评估密码算法的安全性时[7]，先计算密码算法小模块的密码参数，然后通过整个密码最大差分概率平均值和最大线性概率平均值与小模块的密码参数之间的关系，从可证明安全性的角度评估整个密码的安全性。

以图 1 中的 SPS 函数为例[8,9]，它的最大差分概率平均值由 S 盒的最大差分特征概率和扩散层的差分分支数给出上界，最大线性概率平均值由 S 盒的最大线性逼近概率中的最大值及扩散层的线性分支数给出上界。

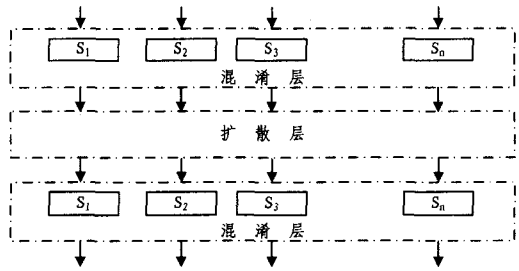

图 1 SPS 函数

对于密码算法簇而言，在变换算法密钥时，实现算法单元和参数可变，这种算法可变是可控的，相应的小模块的密码参数也是可计算的，从而证明密码算法簇的安全性也是可行的。

稍后，结合例子给出具体的安全性分析过程。

3.2 实现效率

密码算法实现可以分硬件和软件两种方式，本文基于可重构硬件平台讨论算法实现。

现有的密码算法可重构实现，多根据密码算法的特点，提取密码算法的基本运算，将不同的密码算法共同的运算设计为可重构处理单元，通过将这些可重构处理单元为不同的密码算法共用，实现密码算法的可重构实现。这样可重构实现密码算法虽然增强了安全性和灵活性，但往往会大大降低处理速度。

我们通过对密码算法的整体框架研究，给出密码算法簇的概念，提高密码算法可重构实现的颗粒度，降低可重构处理单元的复杂度，减少它的时延，从而有效提高密码算法硬件的实现效率。

密码算法簇基于一个整体框架实现，在该框架下，通过算法密钥部分，选取不同的算法模块。在保证密码算法簇整体实现效率的同时，同一个算法模块在不同参数下实现效率应该大致相当。

例如针对分组密码算法的 S 盒模块，如果采用基于 LUT 的方式实现，将算法涉及的 S 盒变换结果预先计算，得到置换表，再采用查表法对每个状态进行变换，实现方式与 S 盒的内容无关。对于 Feistel 网络结构的分组密码，当更换 f 变换时，要求不同的 f 变换，对应的硬件资源消耗和速度差别不大。

4 例子

4.1 算法描述

参照 AES 算法，下面给出一个密码算法簇的例子，密码算法簇增加算法密钥部分 K_f，算法细节仅对 AES 算法的 S 盒组件进行改动，密钥扩展、行变换、列变换等操作保持不变。

我们知道，AES 算法的 S 盒映射为 $f(g(x))$，逆 S 盒映射为 $g(f^{-1}(x))$，其中 g 为有限域上的逆映射，$f:x\to y=Ax\oplus b$，$A=\begin{bmatrix}1&1&1&1&1&0&0&0\\0&1&1&1&1&1&0&0\\0&0&1&1&1&1&1&0\\0&0&0&1&1&1&1&1\\1&0&0&0&1&1&1&1\\1&1&0&0&0&1&1&1\\1&1&1&0&0&0&1&1\\1&1&1&1&0&0&0&1\end{bmatrix}$，$b=\begin{bmatrix}0\\1\\1\\0\\0\\0\\1\\1\end{bmatrix}$，逆运算

中，

$$A=\begin{bmatrix}0&1&0&1&0&0&1&0\\0&0&1&0&1&0&0&1\\1&0&0&1&0&1&0&0\\0&1&0&0&1&0&1&0\\0&0&1&0&0&1&0&1\\1&0&0&1&0&0&1&0\\0&1&0&0&1&0&0&1\\1&0&1&0&0&1&0&0\end{bmatrix},b=\begin{bmatrix}0\\0\\0\\0\\0\\1\\0\\1\end{bmatrix}$$。密码算法簇的新S盒映射设定为 $f_1(g(f_2(x)))$，逆S盒映射为 $f_2^{-1}(g(f_1^{-1}(x)))$，其中 g 为有限域上的逆映射，f_1，f_2 为仿射变换。

为方便讨论，取定 $f_1=f$，$f_2:x\to y=x\oplus b$，其中 b 由密钥 K_f 唯一指定，这里设定每轮的 f 相同，显然 $|K_f|=2^{128}$，当 b 取全零时，密码算法簇中的该映射即为AES算法。

4.2 安全性分析

新S盒的非线性度由有限域上的乘法求逆变换决定，增加一次仿射变换只会掩盖乘法求逆变换的代数结构，而不会改变其非线性度。新S盒的代数次数在取定 f_2 变换的情况下，可以通过lagrange插值公式求得。通过选取合适的仿射变换，可以使得合成后的S盒有较高的代数次数。

仿照AES算法，遵循宽轨迹策略，可以得到算法的最大差分特征概率和最大线性特征概率，从而可以分析算法簇抵抗差分密码分析和线性密码分析的能力。

4.3 实现效率分析

该算法簇的设计是，在密钥不同的情况下，S盒的运算不同，如果采用LUT方式实现S盒，可采用分解运算的方式，构造一个有限域乘法求逆运算的查找表，其余的矩阵乘法和异或运算采用逻辑门实现，其电路规模与基于LUT方式实现的AES算法相比，只增加了少许基本门运算；如果基于有限域运算实现S盒，不同的 f_2 在变换相似的情况下，电路规模与同样方法实现的AES算法几乎相同，而新增的线性变化带来的电路时延也不大。

该实例除了S盒部件外，其他部件的硬件实现都可参照AES算法，根据上面的分析，整个算法簇的硬件实现资源消耗和电路性能大致与AES算法相当。

结束语 密码设计一直是工程多于科学[10]的一项工作，从算法的应用中发现问题，进而改进密码算法设计是密码学者必须进行的研究工作。我们给出可重构密码算法簇的概念，提供了密码算法一种新的设计思路，相关研究包括密码算法整体框架研究、算法模块的密码参数研究、密码算法的硬件实现效率等多方面内容，涉及密码算法设计的各个方面，通过对其进行深入探讨，可加深对密码算法设计的认识。

参考文献

[1] 高娜娜. 密码算法可重构性分析及高速可重构密码芯片研究[D]. 北京：北京科技大学，2005，12

[2] 姜晶菲. 可重构密码处理结构的研究与设计[D]. 长沙：国防科技大学，2004

[3] 曲英杰. 可重组密码逻辑的研究与设计[D]. 北京：北京科技大学，2001

[4] Schneier B. 应用密码学[M]. 吴世忠，等译. 北京：机械工业出版社，2000

[5] Menezes A J, van Oorschot P C, Vanstone S A. 应用密码学手册[M]. 胡磊，等译. 北京：电子工业出版社，2005

[6] Charnes C, O'Connor L, Pieprzyk J, et al. Comments on Soviet encryption algorithm[C]// Advances in Cryptology-EUROCRYPT'94 (LNCS 950). 1995：433-438

[7] 张文涛. 分组密码的分析与设计[D]. 北京：中国科学院，2004

[8] Hong S, Lee S, Lim J, et al. Provable Security against Differential and Linear Cryptanalysis for the SPN Structure[C]// Bruce Schneier, ed. Fast Software Encryption' 2000, LNCS 1978. Springer-Verlag, 2000：273-283

[9] Kang J S, Hong S, Lee S. Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks[J]. ETRI journal, 2001, 23(4)：158-167

[10] Daemen J, Rijmen V. 高级加密标准(AES)算法-Rijndael的设计[M]. 谷大武，等译. 北京：清华大学出版社，2003

(上接第65页)

[9] Cordeiro C, Challapali K, Ghosh M. Cognitive PHY and MAC layers for dynamic spectrum access and sharing of TV bands[C]// Proceedings of the First International Workshop on Technology and Policy for Accessing Spectrum. Boston, Massachusetts: ACM, 2006

[10] Cheng G, Liu W, Li Y, et al. Spectrum Aware On-Demand Routing in Cognitive Radio Networks[C]// New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium. 2007：571-574

[11] Feng Z, Yang Y. Joint transport, routing and spectrum sharing optimization for wireless networks with frequency-agile radios [C]// INFOCOM 2009. The 28th Conference on Computer Communications. IEEE, 2009

[12] Ren W, Zhao Q, Swami A. Connectivity of cognitive radio networks: proximity vs. opportunity[C]// Proceedings of the 2009 ACM Workshop on Cognitive Radio Networks. Beijing, China: ACM, 2009

[13] Xing F, Wang W. On the critical phase transition time of wireless multi-hop networks with random failures[C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. San Francisco, California, USA: ACM, 2008

[14] Penrose M. Random Geometric Graphs[M]. Oxford University Press, 2003

[15] Meester R, Roy R. Continuum percolation[M]. Cambridge University Press, 1996