信息战中的信息加密技术*

徐政五** 龚耀寰

(电子科技大学电子工程学院 成都 610054)

【摘要】 介绍了信息战的背景；描述了信息战的概念；概述了在信息战中，进攻方和防守方为保护信息使用的加密技术，并较全面的提供了数据加密标准、分组迭代快速数据加密算法、标准分组密码算法、非专用分组密码算法、密钥可变分组密码算法等20多种加密算法，这些算法反映了近年来加密技术的发展，并有可能为加密技术的成功实施提供一些新的思路。

关 键 词 信息战； 加密技术； 分组密码； 加密算法

中图分类号 TN918

1 信息战的由来

信息是事物的一种基本属性，而信息化则是人类发展的重要趋势。未来社会中的一切都受到信息化的影响，武器将成为信息化的武器，军队将成为信息化的军队，战争也将成为信息化的战争，即以信息为主导的信息战。

信息战是由美军首先提出的，接着原苏联和一些工业发达的国家也相继提出。信息战就是一种以信息为基础的战争，是作战安全，军事欺骗，心理战，电子战，实体破坏和精确打击等行动的综合应用，它依靠情报相互支援使敌人无法获取信息，并影响，降低和破坏敌方的指挥控制能力，同时还要有防止敌方信息探察和保持己方信息资源完整的能力，使自己的指挥控制系统免遭敌人的毁坏。

信息战是在信息领域内的作战，作战的目的是夺取信息领域的控制权。象其他的领域的作战一样，它也存在进攻和防御两种形式。进攻性信息战是指为使己方自由地利用信息和防止敌方自由地利用信息而进行的心理战，战术欺骗，直接攻击，公共事务和民事活动。防御性信息战有积极防御和消极防御两方面内容。积极防御是指直接防护行动，作战保密，通信保密，计算机保密，反情报，公共事务等。消极防御战是指加固信息系统和进行保密教育等传统活动。

随着信息战的兴起，必然激起人们加速研究新的信息攻击手段，这种手段主要包括以下三个方面：

1) 信息攻击：包括电子信息攻击和非电子信息攻击。电子信息攻击包括各种方式的窃听、截收、流量分析、破译以及主动的恶意宣传广播、冒充、欺骗、窜改和删除等。近年来，由于计算机的广泛应用，还出现了许多新型的信息攻击方式,如计算机病毒、蠕虫、特洛依木马、逻辑炸弹、陷阱门、易损芯片、纳米机器人和芯片细菌，它们直接对信息进行攻击，被攻击的信息可以是传递过程中的，也可以是存储于计算机中的。信息攻击直接、隐蔽、不易发现、危害大，甚至影响战争的最后命运。

2) 电磁攻击：通称电子战，它是通过电子侦察，有意释放强有力的电磁干扰信号、压制对方雷达和通信系统信号，使对方变瞎、致聋。过去，干扰机主要是人工操作进行定频的窄带干扰，现在各国正在针对抗干扰的通信体制，跳频、扩频及跳扩频进行宽频带干扰。

3) 火力攻击：以强大而准确的火力摧毁对方暴露于空间的电子信息系统的诸要素，雷达、通

2000年4月29日收稿
* 电子部预研基金资助项目
** 男 25岁 在职硕士生 助教

信设施、甚至管理和使用人员。在信息战中，电子信息系统的作用十分突出，已成为主战武器，自然也就成为火力攻击的首要目标。

随着信息战的兴起，电脑加密技术等新的信息攻击手段的随之出现，电脑空间加密技术显得更重要。它广泛用于各种通信网上，不仅用于话音，还用于信息存储以及信息系统本身的保护。为此，在网络系统脆弱性分析与评估基础上需要着重解决多级加密、多功能加密、系统加密及加密密钥自动化管理与分发，并与其他机制相结合形成一个具有完备体系结构的信息安全系统。在新形势下，还要面对新兴的通信电子战技术，充分利用其干扰频谱、功率、空间、时间受限及处于被动跟踪地位的弱点，不断提高跳频的速度，增加跳频数目，跳频图案也应不断变化使对方难于实现波形跟踪。在不断提高跳频速度，增加扩展频带及跳频集的前提下，要由单频技术和设备的对抗逐步过渡到系统的对抗和网络的对抗。

如果一个国家过于依赖于信息系统，其防御就会更加脆弱，因此要求它在研究信息进攻的同时必须加强信息的防御。也就是说，随着社会的发展，对安全技术的依赖性将会有增无减。所以，要保证传递信息的安全性，必须建立起完整的信息安全技术。下面就其中的信息加密作一介绍。

2 信息加密

信息加密是保障信息安全最基本、最核心的技术措施和理论基础，它用很小的代价为信息提供相当大的安全保护，是保证信息机密的唯一方法。信息加密已引起许多国家政府、技术部门和各大公司的日益重视。信息加密主要研究内容是密码学,其他安全措施，如口令字和控制非法访问网络的物理方法都不如密码学可靠。

事实上，密码技术是已知的唯一能保护经由电话线路、通信卫星和微波设备的通信网络传输的数据的实用方法；在某些情况下，密码技术可能是保护存储着的数据的实用方法；密码技术还可以用于消息的确认、数字签名以及对授权办理电子支付和信用卡业务的当事人进行识别等等。

70年代后期提出的数据加密标准 DES 等一些较重要的分组密码及算法，在信息加密中得到广泛应用和研究，下面进行简要介绍。

2.1 DES(数据加密标准)

DES 是由 IBM 公司提出的“魔王”算法发展而来，于1977年被美国国家标准局 NBS 定为联邦标准 FIPS 中的一项，被批准供机密机构通信使用，ISO 也已将 DES 作为数据加密标准。

DES 是典型的利用传统换位和置换等加密方法的传统密码体制,它假定信息为二进制的字符串，信息被分为64 bit 的块，使用密钥为64位明文块进行初始置换，然后分成左、右两部分经过16次迭代，进行循环移位与变换，最后再进行逆变换得出密文；解密和加密过程相似，只不过将密钥的顺序倒过来。

DES 的关键性在于变换函数 F 的复杂性，它是公开的。DES 的保密性仅取决对密钥的保密。DES 算法的优点是速度快，可用硬件芯片实现，很适合大量数据加密，但缺点是通信双方需要共享一组密钥并且要在网络中传输，为此若 n 个用户之间互相通信保存 $n(n-1)/2$组密钥，而保存这些密钥本身就极不安全。

DES 是世界上最早公认的实用密码算法标准，是一种最广泛采用的对称保密体制，即加密密钥和解密密钥必须完全相同。还有一类密码叫非对称密码，它们使用不同但相关的密钥实现加密和解密过程。

但是，DES 作为一个优秀的加密算法已走完了其辉煌的一生，随着近几年计算机技术的迅猛发展和新的有效攻击算法的提出，使破译 DES 成为可能。这样，自然就需要一个新的加解密算法来代替 DES，它既要能克服已知的 DES 弱点和能抵抗已知的密码攻击，还必须能在最近几年甚至十几年内在计算机速度大幅度提高的前提下不被攻破。1997年，NIST 向全世界招募将在下个世纪

替代 DES 成为 FIPS 标准的高级加密标准 AES，包括 MARS、RC6™、Rijndael、Serpent、TwoFish 在内的15种加密算法通过了第一次选拔。作为众多侯选算法中的佼佼者，这5种算法在接受了全世界将近一年时间的考察之后，通过了 NIST 的第二轮选拔。

下面先对通过NIST第二轮选拔出的5种算法进行简要介绍，然后介绍其他各种算法。

2.2 MARS 算法

MARS 算法是由 IBM 公司提出的，它分为前向混和、加密变换、后向混和3部分。前向混和与后向混和是互逆的过程,其目的是使明文不会直接参加加密变换，以保护加密变换不会直接受到来自已知明文的攻击。加密变换是 MARS 算法的核心，它运用了乘法、数据控制的循环移位、非线形 S-box 等多种技术隐匿明文信息。MARS 算法综合使用了多种加密手段，为密码分析者设置了许多障碍，有着较高的安全余量，初步看来，是5种算法中“最安全的”。

2.3 RC6™ 算法

RC6™算法是由 RSA 公司提出的，是5个算法中最“简单”的一种，所有的算法可以用不到20行算法描述语言表达清楚，实现的时间代价和空间代价也较其他算法有明显优势。如同 MD5和 RC6 的前身 RC5一样，RC6所有的加密能力都是基于数据控制的循环移位，该操作对隐匿数据有较好的特性，且在大多数 CPU 上都可以高速执行。由于 RC6™ 算法中数据长度、密钥长度、循环轮数都可作为参数配置算法，因而对速度、加密程度、数据分组长度等不同的需要都可以满足。

2.4 Rijndael 算法

Rijndael 算法是由 Joan Daemen 和 Vincent Rijnmen 提出的，是5种侯选算法中唯一明显依托于数学理论的加密算法。它依靠有限域/有限环的有关性质给加密、特别是为解密提供了良好的理论基础，使算法设计者可以既高强度地隐藏信息，又同时保证了算法可逆。又因为 Rijndael 算法在一些关键常数(如 $M(x)$)的选择上非常巧妙，使得该算法可以在整数指令和逻辑指令的支持下高速完成加/解密，从而得到了良好的效率。

2.5 Serpent 算法

Serpent 算法是由 Ross Anderson、Eli Biham 和 Lars Knudsen 提出的，从 Serpent 的循环轮数就能明显看出 Serpent 算法是一种“以安全为重”的加密算法。它几乎就是 DES 的翻版，但是在安全性上有了较大提高，着重体现在：

1) 子密钥生成算法强劲，其强度几乎可以与传统对称分组密码的加密核心相媲美。

2) 加密核心稳固，不象其他算法，Sperpent 的加密核心没有使用 Feistel 变换，而是仅使用了 S-box 和数据控制的循环移位这两种已经被证实为加密性能较好的操作；并且提高了循环轮数以获得较高的安全余量。

Serpent 算法的结构并不复杂，其加密核心仅仅使用了两种操作，因而分析其安全性较为容易。但是，Serpent 的缺点是速度慢。在多种环境下，其他侯选者分别比 Serpent 快1.5~6倍。

2.6 TwoFish 算法

TwoFish 算法是由 Bruce Schneier、John Kelsey 和 Doug Whiting 等人提出的，其核心是 Feistel 变换和“最大码距”理论。TwoFish 的这两个基本理论都是用来保证信息隐藏特性的。Feistel 变换主要完成与密钥相关的 F 函数，以使明文在密钥控制下变换形式。但这种变换相对简单，“最大码距”理论(maximum distance separable)主要完成对输入的离散变换，以使输入和输出达到最大的离散性。配和这两点，使该算法在获得较好安全性的同时也达到很高的效率，其在各种软硬件平台上的实现都明显快于其他算法。TwoFish 的另一个明显优点在于：在对时间代价和空间代价的取舍上，TwoFish 比其他算法好，向用户提供了较大的选择余地。TwoFish 提供的多种实现方案，分别对时间代价和空间代价有不同的偏重，有利于在各种应用环境中进行优化。

2.7 IDEA

1990年瑞士联邦技术学院来学嘉和 Massey 提出了建议标准算法 PES(Proposed Encryption Standard)，后改称为 IEDA。1992年进行了改进，强化了抗差值分析能力。这是近年来提出的各种分组密码中一个很成功的方案，已在 PGP 中采用。

2.8 SAFER-64

SAFER-64(Secure and Fast Encryption Routine)是 Massey 为 Cylink 公司设计的非专用分组密码算法[1] 。算法的明文密文数据分组为64 bit 面向字节运算，K-64的密钥为64 bit，用 r 轮迭代，适于软件实现，采用了非正则线形变换 PHT 可实现有效的混淆，采用了密钥编置来消弱密钥。

2.9 GOST

这是前苏联国家标准采用的一种标准分组密码算法标准，系列号为2814789[2]。不知其是否作为机密业务还是只作为商用加密，传闻曾用作机密军事通信。其消息分组为64 bit，密钥长为256 bit，此外还用了一些附加密钥。

2.10 Blowfish

这是由 Schneier B 设计的用于大型微处理器上实现的密钥可变分组密码算法[3, 4]。易于软件快速实现，所需存储不到5 K，在32 bit 微处理器上完成数据加密，每字节只需26个时钟，运算中只含加、异或和32 bit 操作，查表不易出错。安全性可以调整，密钥量可长达448 bit。适用于密钥不经常改变的加密，如通信链路或文件加密。

2.11 REDOC

REDOC Ⅰ是由 Wood M 为 Cryptech 公司设计的算法[5]。分组长为80 bit，密钥长为160 bit，易于软件实现。代换表可换，采用10轮迭代。分析表明其安全性高。

REDOC Ⅱ是 REDOC Ⅰ的流水线形式。80 bit 分组，密钥长度可变，可高达20 480 bit。没有置换和代换，仅用密钥异或运算，算法易于快速实现， 在33 MHz 的386 PC 机上的加密速度可达2.75 Mbit/s。但分析表明不够安全。

2.12 KHUFU 和 KHAFRE

KHUFU 和 KHAFRE 为 Merkle 在1990年提出的两种建议算法[6]，目的是克服 DES 的一些缺点。KHUFU 密钥量为512 bit，采用16轮8 bit 输入32 bit 输出的 S 盒，分析表明它较安全。KHAFRE 类似于 KHUFU，但不要求予计算，密钥为64 bit 或128 bit。每一轮较 KHUFU 更复杂些，总轮数可高于16。

2.13 MMB

MMB 密码是(Modular Multiplication—Based Bolok Cipher)由 Daemen 提出的算法[7]，分组长和密钥长均为128 bit，其基本理论类似于 IDEA，采用不同代数群的混和运算，由4个32 bit 非线形可迭代换盒实现。软件实现较有效，但硬件实现不如 DES。

2.14 CA.1.1

CA.1.1是由法国 Gutowitz 提出的利用胞元自动机(callular automata)设计的分组密码。分组长为384 bit，密钥由1 024 bit 和64 bit 长的两个密钥组成，故密钥总长为1 088 bit，以大量并行 IC 器件实现很有效。CA.1.1是一种新的算法，其安全性尚待检验。

2.15 SXAL8/MBAL

这是由日本伊藤(Ito)等人提出的64 bit 分组密码算法[8]。SXAL8是基本形式，MBAL 是其扩充，分组长度可变化。轮数较少就了提供足够安全性。一个分组长为1 024字节的 MBAL，其加密速度要比 DES 快70倍。但有人怀疑其抗差分攻击和抗线形攻击的能力。

2.16 SHARK

SHARK 是 Rijmen 等人提出的[9]，利用高度非线形代换盒和极大距离可分（MDS—Maximum

Distance Separable)码组合成的一种分组密码。经过很少几轮就可抗差分和线形攻击，利于用快速软件实现加、解密，在64 bit 结构下，用 C-语言编程实现较 SAFER 和 IDEA 快4倍。

2.17 BEAR 和 LION

BEAR 和 LION 由 Anderson R, Biham E 提出[10]，从流密码和杂凑函数构造可证明安全的分组密码是通过一个从流密码构造的密钥控制杂凑函数来实现。分组长度可以任意，而且当分组较长时，本方案可能优于以前的方案。

2.18 MacGuffin

这一分组密码是由 Blaze M、Schneier B 提出[11]，是最早提出利用非平衡 Feistel 网络(UFN)实现的分组密码。其明文分组长度，实现的轮结构，性能和应用等方面与 DES 相似。UFN 在密码杂凑函数中用得要早些，如 MD5和 SHA。

2.19 TEA

TEA 是由 Wheeler D J, Needham R M 设计的一种精巧的快速软件分组加密算法[12]。可运行于各类计算机。TEA 采用了32轮，密钥为128 bit，软件实现比 DES 快3倍。可以采用 DES 的所有模式运行。TEA 软件程序很易于存储和复制，而且安全，不受出口限制，是一种有效而有用的算法。

2.20 其他算法

在数据加密技术中已讨论的各种算法相当多，如 RSA 公司提出的 Rc1~5算法，CACB 算法，日本 NTT 公司提出的 FEAL-N 算法，MD5杂凑算法，澳大利亚提出的 LOKI-89算法，加拿大提出的 CAST 算法，美国提出的 SKIPJICK 算法，Madryga W E 提出的 MADRYGA 算法，比利时 Daemken 提出的3-way 算法，快速 RSA 算法，等等[13~15]。均与上述介绍的算法具有相同或类似之处，不再一一介绍。

3 结 束 语

未来的战争将是以信息为主导的高技术战争，赢得信息战胜利是克敌制胜的关键。在这里，也提醒我们在发动信息攻击战的同时，更需要加强信息安全的工作。而且，随着社会的进步和电信网络的发展，各国将会大力加强密码技术的研究和开发，以防止信息的泄露和窃取。本文介绍的20余种快速软、硬件实现的分组密码算法只是现有算法中的一部分，而且由于通信网，特别是 Internet 的迅猛发展，一些新的、更好的算法已设计出来。希望我们所介绍的资料对于我们了解分组密码算法的研究动向，掌握、运用和设计分组密码新算法能有点帮助。

参 考 文 献

1 Massey J L. SAFER K-64: a byte riented block-ciphering algorithm. Davics S W ed. Ist Fast Software Encryption, Cambridge Security Workshop Procee-dings, Berlin: Springer-Verlag, 1994: 1~47

2 Gost, Gosudarstvennyi Standard 28147-89. Cryptographic protection for data processing systems. Government Committee of USSR for Standard, 1989

3 Schneier B. Description of new wariable-length key, 64 bits block cipher(blowfish). Fast Software Encryption, Cambridge Security Workshop Proceeding, Springer-Verlag, 1994: 191~204

4 Schneier B. The blowfish encryption algorithm. Dr Dobb's Journal, 1994, 19(4): 38~40

5 Cusick T W, Wood M C. The REDOC-II cryptosystem. In: Menezes A J, Vanstone S A eds. Advance in Cryptology CRYPTO'90, Berlin: Springer-Verlag, 1991: 545~563

6 Merkle R C. Fast software encryption functions. In: Feigenbaum J ed. Advances In Cryptoly-CRYPTO'91 Proceedings, Berlin: Springer-Verlag, 1991: 476~501

7 Daemen J, Govaerts R, Vandewalle J. Block ciphers based on modular arithmetic. Proceedings of 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, 1993: 80~89

8 Ito K, Kondo S, Mitsuoka Y. SXAL8/MBAL algorithm. Technical Report, ISEC93-68, IEICE, Japan, 1993

9 Rijmen V, Daemen J, Prenecd B, *et al*. The cipher SHARK. In: Gollman D ed. 3rd Fast Softmanl Encryption, Springer-Verlag, 1996: 99~111

10 Biham E R. Two practial and provably secure block ciphers; BEAR and LION. In: Gollman D ed. 3rd Fast Software Encryption, Springer-Verlag, 1996: 113~120

11 Blaze M, Schneier B. The MacGaffin block cipher algorithm. In: Prenteel B ed. 2nd Fast Soft Encryption, Springer-Verlag, 1995: 97~110

12 Wheeler D J, Needham R. TEA, a ting encryption algorithm. In: Prenteel B ed. 2nd Fast Soft Encryption, Springer-Verlag, 1995: 363~366

13 陈 运. 一种组合RSA算法. 电子科技大学学报, 1996, 25(2): 116~119

14 陈 运. 基于乘同余对称特性的快速RSA算法的改进. 电子科技大学学报, 1997, 26(5): 477~482

15 陈 运, 龚耀寰. 基于二进制冗余数的递归余数和算法. 电子科技大学学报, 2000, 29(1): 1~4

Information Encryption Technology in Information Warfare

Xu Zhengwu Gong Yaohuan

(College of Electronic Eng., UEST of China Chengdu 610054)

Abstract In this paper, the concept and background of information warfare are introduced. The encryption techniques for protecting information both for offensive and defensive are described. More than twenty block cipher algorihtms are discussed. Especially emphases are given to those algorithms representing the current development of encryption technology in recent years, which might provide some new ideas to the techniques.

Key words information warfare; encryption technology; block ciper; encryption algorithms