第 36 卷 第 5 期 计 算 机 工 程 2010 年 3 月
Vol.36 No.5 Computer Engineering March 2010
·安全技术· 文章编号：1000—3428(2010)05—0134—03 文献标识码：A 中图分类号：TP309

磁盘加密模式分析

张 慧，郭翠芳，牛夏牧，吴春欢
(哈尔滨工业大学深圳研究生院，深圳 518055)

摘 要： 基于国内外磁盘加密产品的研究成果，通过跟踪 IEEE 存储安全工作组(SISWG)制定的块存储设备加密标准 P1619，分析磁盘加密的特定需求，指出其在国内研究的欠缺。选取目前主流的加密模式进行安全性分析，根据其在应用中的优缺点，给出相应建议，并总结磁盘加密算法研究的发展方向。

关键词： 磁盘加密；存储安全；加密模式

Analysis of Disk Encryption Mode

ZHANG Hui, GUO Cui-fang, NIU Xia-mu, WU Chun-huan
(Shenzhen Graduate School, Harbin Institute of Technology, Shenzhen 518055)

【Abstract】 The latest researches and products of disk encryption are outlined, and the special requirements are analyzed. The existing constraints of disk encryption developments and researches are proposed by discussing the standard P1619 developed by SISWG. Typical disk encryption cipher modes are analyzed and some practical advices are listed. The study focuses and development tendency of disk encryption are summarized.

【Key words】 disk encryption; storage security; encryption mode

磁盘丢失、被盗或未授权的使用而造成信息和数据的泄漏已经给国家、企业和个人带来了难以估量的损失。严峻的现实同时也揭示了巨大的社会需求和市场价值。磁盘加密技术作为解决磁盘信息安全问题最直接、最有效的技术之一，在社会和市场的推动下，近几年得到了长足的发展。在新的操作系统中，磁盘加密开始成为一个标准组件。目前致力于存储安全研究的机构主要有可信赖计算组织(TCG)、美国电气及电子工程师学会(IEEE)、美国国家标准学会(ANSI)等。他们在各自关于存储安全的规范中都已经开始包含关于磁盘加密的算法、模式和密钥管理等内容，其中具有代表性的是 IEEE 于 2008 年 4 月 18 日发布的 IEEE Std P1619™-2007[1]。我国关于磁盘加密的产品和理论研究还相对比较落后，需要跟踪并适应国际在这个方向上的最新研究成果。

1 国内外磁盘加密技术发展现状

1.1 磁盘加密产品

磁盘加密技术以密文的形式在磁盘上保存数据，以实时加解密的方式支持操作系统对数据的访问和使用，可以有效地解决磁盘在被盗或遗失情况下的数据保密问题。近几年，伴随着磁盘加密理论研究的进步和芯片处理能力的提高，磁盘加密产品在安全性、产品形式和数量上都有了很大的发展。磁盘加密的产品形式主要有基于 TPM 芯片的安全硬盘和磁盘加密软件 2 类。产品的安全性依赖于所选择的加密算法和模式。在加密算法上，典型产品如 Windows Vista 的磁盘加密组件 BitLocker，Linux 的磁盘加密系统 LUKS 采用的是 AES 算法；而免费开源磁盘加密软件 TrueCrypt 和 FreeOTFE 以及 SafeNet 公司的磁盘加密软件 ProtectDrive，除了支持传统的加密算法(如 DES, 3DES, TwoFish)之外，也支持 AES 算法。而模式上，Windows Vista BitLocker 采用微软自己研发的 AES-CBC+Elephant diffuser[2]；LUKS 采用 CBC；TrueCrypt 和 FreeOTFE 除了支持传统的加密模式 CBC 外，也支持专门针对磁盘加密的模式 XTS。

国内在磁盘加密产品的开发上，长春卓尔公司的 SQY07 磁盘加密系统填补了我国这个领域的空白，被列入 2001 年度国家重点新产品，之后相关密码产品不断涌现。直到 2008 年 6 月 1 日，通过国家商用密码管理办公室认证的 386 项商用密码通用产品中，有 19 项是磁盘加密系统或软件，有 35 项是可以应用于磁盘加密的 PCI 卡、密码卡等。

国内磁盘加密产品在安全性上与国外同行相比存在明显的差距。目前，只有为数不多的产品提供 AES 算法；而加密模式也大都只采用传统的 ECB 和 CBC 模式。究其原因，一方面，国内商用密码产品的生产受到《商用密码管理条例》的限制，任何单位或个人在商用中只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。新算法和新模式的研究只能由国家密码管理机构指定的单位承担，在一定程度上与市场需求脱节。另一方面，国内缺乏足够的市场细分，商用密码研究主要集中在分组密码本身，而缺乏针对磁盘加密特定需求的加密模式的研究。

1.2 磁盘加密理论和标准

1977 年，美国标准局(NBS)，即现在的国家标准与技术研究所(NIST)，公布了数据加密标准(DES)。1980 年又公布了 4 种 DES 的加密模式。1997 年，NIST 正式宣布 NIST 计划，发起了在全世界范围内征集新的加密标准算法，新的标

基金项目： 国家自然科学基金资助项目(60832010, 60671064, 60703011)；国家“863”计划基金资助项目(2007AA01Z458)
作者简介： 张 慧(1978－)，男，博士，主研方向：存储安全，感知哈希；郭翠芳，硕士；牛夏牧，教授、博士生导师；吴春欢，硕士
收稿日期： 2009-09-20 **E-mail：** zhanghui1978@gmail.com

准称为高级加密标准(AES)。在 AES 即将诞生之际，NIST 又为 AES 公开征集加密模式。这一系列举动在国际上再次掀起了分组密码算法的研究热潮，2000 年欧洲的 NESSIE 计划和日本的 CRYPTREC 规划，韩国和其他国际组织对分组算法的大量研究以及我国“863”计划中对制定密码的标准化问题列入议程，这些都为磁盘加密奠定了深厚的理论基础。

为弥补在静态存储数据安全标准上的空白，SISWG 致力于制定利用加密技术保护存储数据的相关标准。目前已完成了适用于磁盘的窄块定长加密标准的制定。于 2007 年 12 月提交给 IEEE 通过审核，并作为标准 IEEE Std P1619™-2007 在网站上对外公开；另一个标准 P1619.2 还在制定中，它将应用于 512 Byte 或 512 Byte 以上的宽块媒介定长加密。这些标准的制定希望能够为用户带来如下好处[3]：(1)不必自己去设计一个安全结构；(2)不必自己去做关于费用和时间消耗方面的安全分析，减少开发费用和时间；(3)提供一种早已被公众鉴定的安全结构；(4)提高对被推荐的安全结构的信任程度；(5)为原始设备制造商们提供一个具有类似安全结构的开发资源。

由于相关标准的制定，磁盘加密算法和模式的开发以及相应的安全性分析得到发展。到目前，一些规范组织和企业已经陆续根据自己的分析和测试，提出各自关于磁盘加密算法和模式的建议。跟踪和分析这些最新的研究成果，有助于明确磁盘加密算法及模式的研究方向，必将促进我国磁盘加密产品和理论研究的进步。

2 磁盘加密的要求

磁盘加密目的是保证保磁盘上的数据在任何时刻都以密文形式存在。而操作系统或程序对磁盘的使用是频繁且随机的，因此，磁盘加密功能往往部署在操作系统的内核态或者在对磁盘直接进行存取的硬件电路上。如图 1 所示，磁盘加密功能模块对存入磁盘的数据实时加密，对读出磁盘的数据实时解密，从而保证操作系统或程序对磁盘数据使用的需要。磁盘加密产品一般以整块物理硬盘或一个逻辑卷为操作对象，对保存在硬盘或者逻辑卷上的所有数据，甚至空白区域都进行同样的处理。

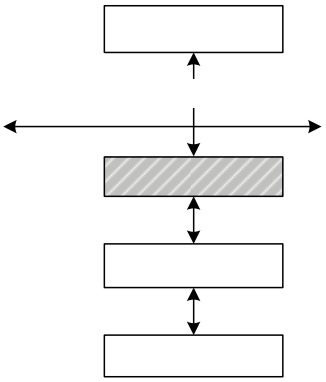

图 1 磁盘加密系统结构

磁盘数据读写的特点要求磁盘加密操作必须以扇区为单位进行，并且每个扇区的加密都是互相独立的。因此，磁盘加密的算法和模式必须满足如下 2 点要求：

(1)定长变换。磁盘加密的密文长度必须和明文长度相同。这意味着磁盘加密不能使用额外的空间来存储信息，如消息鉴别码(MAC)等认证或校验信息。

(2)适用于独立且无序的数据单元。计算机对磁盘数据的存取可以看作一个随机事件，每次存取事件之间是独立且无序的。因此，磁盘加密不能依赖于扇区之间的关系。这意味着，磁盘加密的算法只能以扇区为操作单位，加密模式也只能对一个扇区内的多个分组进行处理。

分组密码可以处理特定大小的明文分组，并产生相同大小的密文，满足磁盘加密的要求。但是一方面因为磁盘巨大的数据容量，相同的算法和相同的密钥使用太多次必将导致加密结果容易受到分析；另一方面，由于磁盘数据是高度规定化的，存在大量的规则数据和重复数据，如果相同的明文产生相同的密文，就会暴露磁盘的模式信息，容易受到攻击。为了解决这些问题，分组加密模式的研究成为磁盘加密算法研究的关键。

3 典型的磁盘加密模式分析和简评

按照加密粒度的大小，磁盘加密模式可分为窄块模式和宽块模式 2 类。窄块模式指分组长度小于扇区大小的分组，常用的有 ECB, CBC, CFB, CTR, XTS 等；宽块模式指分组长度等于扇区大小的分组，常用的有 EME, XCB, ABL4, AES-CBC+Elephant diffuser 等。本节选取目前研究和应用中典型和前沿的加密模式进行分析。

令 $E_k(P)$ 表示用密钥 K 加密明文 P；$D_k(C)$ 表示用密钥 K 解密密文 C；m 为加密算法对应数据块长度；$P=P_1|\cdots|P_i|\cdots|P_n$ 表示明文被划分为 n 个分组；C_i 表示 P_i 对应的密文，密文的 n 个分组为 $C=C_0|\cdots|C_i|\cdots|C_n$；$K=K_1|K_2$ 表示密钥 K 被拆分为 K_1 和 K_2 2 个部分；$|X|$ 表示数据块 X 的长度；$HEAD_u(Y)$ 表示 Y 的高 u 比特；$TAIL_u(Y)$ 表示 Y 的低 u 比特；α 为伽罗瓦域运算的基本元素。

3.1 ECB模式和CBC模式

ECB 和 CBC 是 1980 年 NBS(后为 NIST)为 DES 算法选定的加密模式，后来在 2001 年秋 NIST 公布的文件 800-38A 中再次入选为 AES 的保密工作模式。ECB 和 CBC 模式是当前国内磁盘加密产品使用的主要的加密模式。

ECB 模式工作原理为

$$\boldsymbol{C}_i = E_k(P_i),\quad i=1,2,\cdots,n$$

该模式的主要优点是：(1)操作简单；(2)可并行计算，速度快；(3)各个分组之间不受影响，即使加密时发生错误，也不会出现错误传递，并且解密时发生错误只影响当前明文，其他明文不会受到影响。然而其致命的缺点是：只要密钥相同，相同的明文无论出现在任何扇区、任何分组总是得到相同的密文，这样不但泄漏了数据模式，而且易受水印攻击。因此从安全性的角度来讲，ECB 不能满足磁盘加密的需要。

CBC 模式工作原理为

$$\boldsymbol{C}_i = E_k(\boldsymbol{C}_{i-1}\oplus \boldsymbol{P}_i),\quad i=1,2,\cdots,n$$

其中，$\boldsymbol{C}_0$ 称为初始向量(IV)。

该模式的主要优点是：克服了 ECB 的缺点，使用前一个密文块对当前明文“随机化”，相同明文将对应不同的密文，从而降低了信息的泄漏。主要缺点是：(1)由生日悖论可预知 $2^{M/2}$ 个分组后会出现完全相同的分组，M 为分组大小。对 64 位的分组，约为 34 G；(2)一个密文错误会影响整个明文分组以及下一个分组的相应位；(3)IV 的使用方法直接影响到其安全性。当固定扇区采用固定的 IV 时，会产生和 ECB 同样的问题。所以，应该采用瞬时 IV 来保证同一个密钥作用域下 IV 的唯一性。

磁盘加密中，普通的方法直接将扇区号作为 IV，这时 IV

是可以预测的，同样会遭受水印攻击。如果将扇区号和密钥的 Hash 值相结合生成 IV，这样 IV 就不可预测。推荐的 IV 计算方法如下：

$$\boldsymbol{IV}(sector) = E_s(sector)$$

其中，$s = Hash(K)$。

然而，这也并不意味着 CBC 模式就是安全的。假设攻击者可以读取部分文件且可以修改磁盘上的密文，它仍然可以获得很多的信息。

3.2 XTS模式

该模式被认为是目前最适合磁盘加密的窄块加密模式，标准 IEEE Std P1619™-2007 采纳的就是这种模式。由于模式有一定复杂性，本文通过伪代码介绍其工作原理。

(1)定义块加密函数

$$C \leftarrow blockEnc(K, P, t, j)$$

其中，i 是调柄，j 是当前块在明文内的编号。块加密函数伪代码如下：

```
//XTS 块加密函数
T ← E_k2(t) ⊗ α^j
PP ← P ⊗ T
CC ← E_k1(PP)
C ← CC ⊗ T
```

(2)定义明文加密函数

$$C \leftarrow Enc(Key, P, t)$$

其中，t 是调柄。明文加密函数伪代码如下：

```
//XTS 明文加密函数
P ← P_1 | ··· | P_i | ··· | P_n
 for  i ← 1  to n-2 do
     C_i ← blockEnc(K, P_i, t, i)
 end for
 u =| P_n |
 if u=0 then do
        C_n-1 ← blockEnc(K, P_n-1, t, n -1)
        C_n ← empty
 else do
        CC ← blockEnc(K, P_n-1, t, n -1)
        u ←| P_n |
        C_n ← HEAD_u(CC)
        CP ← TAIL_m-u(CC)
        PP ← P_n | CP
       C_n ← blockEnc(K, PP, t, n)
 end if
 C ← C_0 | ··· | C_i | ··· | C_n
```

该模式的主要优点是：(1)各分组之间可以并行运算；(2)由于和当前块在磁盘中的逻辑编号相结合，可以有效抵抗密文操作和复制粘贴攻击；(3)可以处理任意长度的数据；(4)不存在错误扩散，当前块发生错误，不会影响到其他块。

主要缺点是：(1)算法有一定的复杂性；(2)调柄的预处理是关键，需要有伽罗瓦域相关的数学知识的储备；(3)当调柄表现为非随机性(如高密度或低密度)时，密文随机性就会下降很多。可以通过加密、哈希或其他控制函数来改变调柄的随机性。

随着 IEEE Std P1619™-2007 得到厂商的广泛支持，XTS 模式的应用也将越来越广泛，已经有很多磁盘加密产品使用了这种模式。而且 SISWG 也表示经过验证的 XTS 将会为用户提供良好的数据保护。

3.3 AES-CBC+Elephant diffuser模式

该模式是由微软研发并在 Windows Vista BitLocker 中使用的磁盘加密方法。它采用了宽块加密模式，加密粒度是一个扇区。微软已经证明了使用扩散体(diffuser)后的 CBC 比原来的 CBC 更难攻击，但为了让密码学界来分析 diffuser 算法的安全性作用，微软已将此模式的设计报告对外公开。其工作原理如下：

(1) $K = K_1 \mid K_2$；

(2) $PP = P \oplus K_1$；

(3)PP 经过 2 个 diffuser 算法的作用后，使用 CBC 模式进行加密。其中，每个扇区的 $\boldsymbol{IV} = E_{k_2}(e(sector))$，其中，$sector$ 为扇区号；$e()$ 将扇区号映射为一个唯一的 16 Byte 的值。

从安全性角度考虑，加密粒度越大，攻击者需要的初始信息越多，因此，BitLocker 希望使用宽块加密模式，放弃了 XTS；CMC 和 EME 基本上可以满足需求，但从效率上考虑，BitLocker 希望由于加密造成速度的延迟在用户可以忍受的范围内，CMC 和 EME 却需要 2 次遍历数据，因此被 BitLocker 排除；而一个全新的加密模式需要很长时间被外界分析和认可。基于上述原因，微软在 CBC 的基础上设计了 AES-CBC+Elephant diffuser 模式，通过 diffuser 算法来确保在明文中很小的改动也将导致整个扇区密文的变化，从而弥补 CBC 在完整性上的遗憾。即使不考虑 diffuser 算法的安全性，AES-CBC+Elephant diffuser 模式也可以在随机性和抗攻击性上保证和 CBC 模式有相同的安全性。而且德国数据处理学会和慕尼黑技术大学最新的《关于磁盘加密模式的统计特性测试》[4]表明，AES-CBC+Elephant diffuser 模式随机特性很好，甚至优于窄块加密模式。

4 结束语

本文介绍并简评了国内外目前使用的各种主流加密模式和国外相关研究的发展动态。关于几种典型模式的安全性分析表明，窄块加密模式中的 XTS 模式代表了磁盘加密模式研究的发展方向，而宽块加密模式也将成为研究的一个新的方向。为开发我国具有自主知识产权的磁盘加密产品，业界应对国内目前广泛应用的磁盘加密模式的不足引起重视。

参考文献

[1] IEEE Storage Systems Standards Committee and Information Assurance Standards Committee. IEEE Std 1619-2007 IEEE Standard for Cryptographic Protection of Data on Block-oriented Storage Devices[S]. 2008.

[2] Ferguson N. AES-CBC+Elephant Diffuser: A Disk Encryption Algorithm for Windows Vista[EB/OL]. (2006-04-03). http://download.microsoft.com/download/0/2/3/0238acaf-d3bf-4a6d-b3d6-0a0be4bbb36e/ BitLockerCipher200608.pdf.

[3] Hars L, Research S. Discryption: Internal Hard-Disk Encryption for Secure Storage[J]. Computer, 2007, (6): 103-105.

[4] El-Fotouh M A, Diepold K. Statistical Testing for Disk Encryption Modes of Operations[EB/OL]. (2007-12-14). http://eprint.iacr.org/2007/362.

编辑　金胡考