第 38 卷 第 8 期
Vol.38 No.8
计 算 机 工 程
Computer Engineering
2012 年 4 月
April 2012

• 安全技术 •　　文章编号：1000—3428(2012)08—0101—04　　文献标识码：A　　中图分类号：TP309.2

Office 认证机制中密钥导出函数安全性分析

邹 梅，吴鸿伟，周 君，李晓潮，郭东辉
(厦门大学电子工程系，福建 厦门 361005)

摘 要：微软 Office2007 及其后续版本采用 ECMA-376 的文件加密格式，其安全性主要通过用户认证和文件加密实现，而密钥导出算法是整个安全机制的核心。为此，研究 ECMA-376 密钥导出算法的安全性，利用 Game-Playing 技术计算该密钥导出算法与随机函数的不可区分优势的上限。通过该理论和攻击实例对 Office 安全性进行分析，结果表明，当用户口令字符长度大于 6 时，Office 具有一定的安全性。

关键词：消息认证码；密钥导出函数；可证明安全性；ECMA-376 文件加密格式；随机预言机模型

Security Analysis of Key Derivation Function in Office Authentication Mechanism

ZOU Mei, WU Hong-wei, ZHOU Jun, LI Xiao-chao, GUO Dong-hui
(Department of Electronic Engineering, Xiamen University, Xiamen 361005, China)

【Abstract】Microsoft Office2007 and later version adopt ECMA-376 document encryption format. In this format, the file security is mainly protected by user authentication and files encryption, and Password Based Key Derivation Function(PBKDF) is the core of the Office security mechanism. In order to analyze the security of the PBKDF in ECMA-376 format, this paper proves the upper bound of the adversary's advantage between the Key Derivation Function(KDF) and ideal random function through the Game-Playing technology, and discusses the safety of the Office encrypted files based on that theoretical result and the actual attack experiment. Based on the analysis results, it obtains that Office is with a certain degree of security while the user password is longer than 6 characters.

【Key words】Message Authentication Code(MAC); Key Derivation Function(KDF); provable security; ECMA-376 document encryption format; random oracle model

DOI: 10.3969/j.issn.1000-3428.2012.08.033

1 概述

在加密文件中，为了防止文件在传输或存储过程中未经授权而被访问和篡改，一般采用消息认证机制[1]。相比于其他物理和生物特征的认证方式，基于口令的认证机制被广泛使用，几乎所有的加密软件都支持口令认证机制，并将其作为主要的身份认证机制。由于口令通常是从一个相对较小的空间选取的，很容易受到穷尽口令搜索攻击与字典攻击，因此基于文件的口令认证机制往往需要对用户口令进行扩展处理以加强其安全性，即采用基于口令的密钥导出函数(Password Based Key Derivation Function, PBKDF)生成密钥。

文件口令认证机制中消息认证码(Message Authentication Code, MAC)的安全性定义是在密钥随机均匀分布的前提下给出的，不均匀分布的密钥空间不仅在一定程度上缩小了强力(brute force)攻击的密钥搜索空间，而且在很多密码系统中，如果密钥不均匀分布也是不安全的[2]。若 MAC 生成算法是安全的，则文件口令认证机制的安全性主要取决于 PBKDF 导出密钥的随机性。

通过在口令认证机制中的密钥导出算法中引入循环次数(c)与盐($salt$)以增加穷尽口令搜索攻击与字典攻击的代价，从而提高口令认证机制的安全性。虽然盐和循环次数很快在工业技术领域如 PKCS[3]中得到广泛的应用，但是其安全性在理论证明方面却进展缓慢。文献[4]给出了密钥导出算法——PBKDF1 的安全性定义，并界定了攻击者成功区分导出密钥与随机字符串的概率，从理论上证明其安全性，并给出循环次数与攻击算法可获得不可区分优势的数量关系。

Microsoft Office 软件是由微软公司开发的一套被广泛使用的办公软件。其安全性主要通过文件认证机制来保证。通过对 Office 各版本中认证过程的分析，Office97/2000 的加密密钥长度仅为 40 bit，在穷尽口令搜索攻击口令攻击下是不安全的[5]，虽然 Office2003 密钥长度提升为 128 bit，但是由于其密钥导出算法缺少迭代，攻击者进行口令猜测时速度很快[6]，从 Office2007 开始，微软采用 ECMA-376 的文件加密格式[7]，加密密钥长度至少为 128 bit，密钥导出算法的循环次数 c 至少为 50 000 次。

随着密码学中可证明安全性理论的不断丰富，特别是在随机预言机(random oracle)模型[2]提出之后，在该模型下出现了一种统一的证明方法：Game-Playing[8]。它最早是由 Rogaway 提出的，后来被广泛地应用于各种证明[9-10]。本文使用 Game-Playing 技术证明了 ECMA-376 中所使用的密钥导出算法的安全性，在底层所使用的基础散列算法(H)是在伪随机置换的假设下，量化了该密钥导出算法与随机函数之间的不可区分性。

基金项目：福建省高校产学合作科技基金资助重大项目(2010H6026)；厦门市科技计划基金资助项目(3502Z20093002)

作者简介：邹 梅(1987－)，女，硕士研究生，主研方向：嵌入式系统设计，信息安全；吴鸿伟，博士研究生；周 君，硕士研究生；李晓潮，副教授、博士后；郭东辉，教授

收稿日期：2011-02-20　**E-mail：**leexcjeffrey@xmu.edu.cn

2 加密文件认证机制与密钥导出算法

2.1 加密文件消息认证机制

基于口令的认证机制是用对称密码算法来实现数据完整性的密码方案，使得文件在传输或存储过程中不受未经授权的篡改和访问。它由密钥生成算法、MAC 生成算法和验证算法构成，即 $MAC=(K, T, V)$。其中，K 是密钥导出算法，用于生成 MAC 生成算法的密钥 key；MAC 生成算法 T 以密钥 key 和消息 M 作为输入，得到消息认证码 σ，即 $\sigma \leftarrow T_{Key}(M)$；验证算法 V 是一个确定算法，以密钥 key、消息 M 和消息认证码 σ 作为输入，输出是否符合确认信息，记为 $d \leftarrow V_{key}(M,\sigma)$ [2]。

基于口令的消息认证流程见图 1，为验证用户是否为合法和传输中未受到未授权的修改，要求 $V_{key}(M,T_{key}(M))=1$。因此，验证算法需要重新计算认证码，并和文件中内置的认证码进行比较，从而判断输入的用户口令是否正确。在文件认证机制中，MAC 生成算法 T 一般是确定的，并有 2 种主要方式：使用 Hash 函数或是使用分组密码。Office 系列采用的是 Hash 函数。

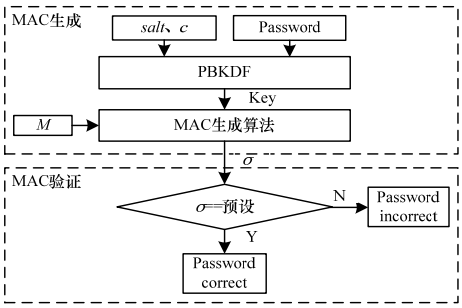

图 1 基于口令的认证机制流程

2.2 密钥导出算法

在 PKCS#5[3]基于口令的密码系统规范中详细定义了 2 个密钥导出函数：PBKDF1 和 PBKDF2。其中，PBKDF1 可表示为：

$$key=H^{(c)}(p\|s)$$

运算过程中通过对口令(p)和盐(s)的串联，并结合散列函数(H)，重复 c 次，然后导出密钥 key，散列函数可以为 MD2、MD5 和 SHA-1 等。导出密钥的长度受散列函数输出长度的限制，MD2 和 MD5 是 16 Byte，SHA-1 是 20 Byte。处理过程如下：

U0=p||s
For i=0 to c−1 Do
Ui+1=H(Ui)
END FOR
key=Uc<0,1,⋯,15>

其中，n 表示导出密钥的字节长度；U 表示中间变量。

Microsoft Office 采用 ECMA-376 文件格式，其密钥导出算法是 $key=H^{(c)}(i\|p\|s)$，其运算步骤和 PBKDF1 类似，唯一的不同之处仅在于将每次的迭代轮数也作为基本散列函数 H 的消息输入，主要将 1 Byte 的迭代轮数(i)、用户口令(p)以及 16 Byte 的盐(s)的串联，经过 c 轮的基本散列函数 H 循环迭代处理后取前 128 bit 作为 AES 解密算法的密钥 key。ECMA-376 文件加密中的密钥导出算法的伪代码如下：

U0=p||s
For i=0 to c−1 Do
Ui+1=H(i||Ui)
END FOR
key=Uc<0,1,⋯,15>

2.3 密钥导出函数的安全性定义

在可证明安全理论中，通常使用优势函数(advantage)[2]来度量一个算法和理想的算法之间的差别。如果这个差别可忽略，就认为该算法是安全的，通常密钥导出函数的安全性可通过它与随机函数之间的不可区分性来度量。

密钥导出函数可以视为是密钥扩展(key stretching)，因此，其安全性的关键在于导出函数的构成[4]。对于底层的 Hash 函数可以视为黑盒，这里用随机预言机来替换。

假设攻击者 A 的攻击过程为：首先 A 获得一个长为 n bit 的字符串 y_0，其中，y_0 可能是密钥导出函数 F 的导出密钥，也可能为一个随机字符串，然后 A 通过查询随机预言机 H 并获得回答后，判断 y_0 是导出密钥还是随机字符串，最后若 A 断定 y_0 为导出密钥则输出 1，否则输出 0。

对于随机函数 G：$\{0,1\}^n \rightarrow \{0,1\}^n$ 和密钥导出函数 F：$key=H^{(c)}(i\|p\|s)$，根据攻击者 A 的攻击过程，设计如代码 1 所示的攻击实验 F_A 与 G_A：

代码 1

1.salt,c 已知且固定
2.随机选择 p0，得到 u0=p0||salt
3. y0=H(c)(i||u0) **y0=Rand(n)**
4.s=0;
5.重复：
6 A 选择 Xi，询问 H 获得 H(Xi)
7. s=s+1
8.当 s 达到最大询问次数 t 时，重复结束
9.输出 0 或 1

其中，t 表示攻击者 A 可询问预言机的次数。代码 1 中步骤 3 处黑体部分 $Rand(n)$表示长度为 n bit 的随机数，F_A 不包括步骤 3 的黑体语句，将 $y_0=H^{(c)}(i\|u_0)$用黑体部分 $y_0=Rand(n)$代替后形成攻击实验 G_A。对于特定的 t，密钥导出算法 F 与随机函数 G 的差别用攻击优势表示：

$$Adv^{prf}_{F,G}(t)=|\Pr[F_A=1]-\Pr[G_A=1]| \quad (1)$$

其中，$\Pr[F_A=1]$ 表示攻击者 A 采用 F 预言机输出 1 的概率。因此，式(1)表示攻击者 A 经过 t 次询问预言机后，成功区分密钥导出函数与随机函数的概率。对于特定的询问次数 t，如果攻击者 A 获得的攻击优势是可忽略的，则称密钥导出函数 F 是安全的，即密钥导出函数 F 与随机函数 G 是不可区分的。

下文使用 Game-Playing 技术证明对于 ECMA-376 文件的密钥导出算法，若攻击者 A 只能查询随机预言机 H，其攻击优势 $Adv^{prf}_{\text{ECMA-376}}(t)<\lfloor t/c \rfloor/|PW|+t^2/2^n$，其中，$|PW|$表示密钥空间 PW 中密钥的个数；n 表示导出密钥的比特长度。

3 密钥导出算法的安全性证明

根据 2.3 节中的攻击实验 F_A 与 G_A 设计出 2 个游戏(Game)$R0$ 与 $R1$，其中，Game $R0$ 的具体实现过程如下：

代码 2

设定 salt,c
选择：p0←PW,y0=Rand(n),i=0,U0=p0||salt, Y={U0,y0}
第 s 次询问预言机 H(Xs):
4.1 y=Rand（n）
4.2 If y ∉ Y,then Y=Y ∩ {y}
4.3 else { bad=1}

4.4 If(t<c-1&& Xs ==i||Ui)i=i+1, Ui =y

4.5 elseif(i==c-1&& Xs ==i||Ui){bad=1,**y=y0**}

4.6 H(Xs)=y,返回 y

将 $y=y_0$ 删除后形成 Game $R1$，Y 表示包含所有的攻击者 A 询问 x_s 后获得的返回值 $H(x_s)$ 以及初始值 u_0、y_0 的集合，$p0\leftarrow PW$ 表示从口令集中随机选择一个密钥赋值给 $p0$。

对比代码 1 和代码 2 可以看到，在攻击实验 F_A 的 y_0 在实验开始前就随机选择，并设置 $H^{(c)}(i\|u_0)$，由于 H 是随机预言机，且 u_0 是随机选取的，因此和 Game $R0$ 在游戏开始前随机选取 y_0 从攻击者 A 的角度看来并没有区别。此外，从 Game $R0$ 中的步骤 4.5 看到，当攻击者 A 的询问值 x_s 为 $(c-1\|u_{c-1})$ 时，Game $R0$ 中会修改预言机 H 的返回值为 y_0。因此，存在关系 $y_0=H(c-1\|u_{c-1})=H^{(c)}(i\|u_0)$。对于其他任意的询问值，均返回一个随机值，和攻击实验 F_A 中的随机预言机 H 等效。所以，攻击实验 F_A 与 Game $R0$ 等效，于是 A 输出 1 的概率是相等的，即有 $\Pr[F_A=1]=\Pr_{R0}[A=1]$，其中，$\Pr_{R0}[A=1]$ 表示 A 在游戏 $R0$ 中输出 1 的概率。

在 Game $R1$ 中的预言机 H 对于任意的询问值，均返回一个随机值，因此，和攻击实验 G_A 中的随机预言机 H 等效，从 A 的角度攻击实验 G_A 与 Game $R1$ 并没有区别。所以，在实验 G_A 与 Game $R1$ 中 A 输出 1 的概率相等，即 $\Pr[G_A=1]=\Pr_{R1}[A=1]$，其中，$\Pr_{R1}[A=1]$ 表示 A 在游戏 $R1$ 中输出 1 的概率。因此，ECMA-376 密钥导出算法的不可区分优势 $Adv^{prf}_{\text{ECMA-376}}(t)$ 可等效为：

$$Adv^{prf}_{\text{ECMA-376}}(t)=|\Pr_{R0}[A=1]-\Pr_{R1}[A=1]| \tag{2}$$

在游戏 $R0/1$ 中增加了模拟预言机 H 对攻击者询问的回答(代码 2 中的步骤 4.1~步骤 4.6)，但这些计算从攻击者 A 的角度是不可见的，A 只能看到 H 返回的值。在游戏中，步骤 4.3 和步骤 4.5 如果检测到碰撞(collision)发生，则将标志 bad 置 1。在步骤 4.3 检测散列函数内部的碰撞，在步骤 4.5 检测 $H^{(c)}(i\|u_0)$ 的碰撞。对比 Game $R0$ 和 $R1$，它们只在 bad 置 1 之后的操作有所不同，符合 Identical-until-bad-is-set 条件，所以，根据文献[8]中的引理 5 可得：

$$Adv^{prf}_{\text{ECMA-376}}(t)\leqslant \Pr_{R0}[BAD]=\Pr_{R1}[BAD] \tag{3}$$

其中，$\Pr_{R0}[BAD]$ 与 $\Pr_{R1}[BAD]$ 分别表示在 Game $R0$ 与 $R1$ 中 bad 标志置 1 发生的概率，两者是相等的。由于 Game $R1$ 比较简单，因此选用 $\Pr_{R1}[BAD]$ 作为攻击优势的上界并进行求解。

在游戏 $R1$ 中，用 BAD_1 表示代码 2 中步骤 4.3 处 bad 置 1，BAD_2 表示步骤 4.5 处 bad 置 1。BAD 表示 BAD_1 与 BAD_1 至少有一个发生，满足 $BAD=BAD_1\cup BAD_2$，“$\cup$”表示 2 个事件的和事件。根据一致限(union bound)命题[1]，则有：

$$\Pr_{R1}[BAD]=\Pr_{R1}[BAD_1\cup BAD_2]\leqslant \Pr_{R1}[BAD_1]+\Pr_{R1}[BAD_2] \tag{4}$$

对于步骤 4.3 处 bad 置 1 的情况，相当于每次随机地选择一个长度为 n 位的字符串 y，然后测试其是否在集合 Y 中。这个集合起始时有 2 个元素 u_0、y_0(代码 2 中步骤 3)，如果 y 不在其中，则添加到 Y，直到 t 次查询结束，那么 BAD_1 发生的概率分成 2 个部分：(1)等同于从 2^n 个数的集合中，随机均匀地选择 t 个数，其中至少有 2 个数相等的概率(或碰撞的概率)。这个问题和生日问题类似，所以根据“生日”问题可知这个概率的上界为 $t^2/2^{n+1}$ [1]。(2)这 t 个数与集合初始化时存在的 $\{u_0,y_0\}$ 碰撞的概率。对于任意 2 个数，它们的碰撞概率为 $\Pr(col_{i,j})=1/2^n$，$i\neq j$，因此，和 u_0、y_0 中任意一个发生碰撞的概率为 $2t/2^n$，于是有：

$$\Pr_{R1}[BAD_1]\leqslant (t^2/2+2t)/2^n \tag{5}$$

若 $t\geqslant 4$，则 $(t^2/2+2t)/2^n\leqslant t^2/2^n$，$\Pr_{R1}[BAD_1]\leqslant t^2/2^n$。

将 Game $R1$ 中的步骤 4.3 删去，得到游戏 $R2$，由于仅删除一处，可得 $\Pr_{R2}[BAD]=\Pr_{R1}[BAD_2]$，因此有：

代码 3

设定 salt,c

选择：p0←PW,y0=Rand(n),i=0,U0=p0||salt

第 s 次询问预言机 H(Xs):

4.1 y=Rand（n）

4.4 If(t<c−1&& Xs ==i||Ui)i=i+1, Ui =y

4.5 elseif(i==c−1&& Xs ==i||Ui){bad=1}

4.6 H(Xs)=y,返回 y

在 Game $R2$ 中预言机 H 的返回值 y 是随机选择的，并且它的值不影响 bad 的设置，即 bad 变量和 y 是独立的，所以 Game $R2$ 具有 oblivious 性质；可将 $R2$ 中与 y 相关的部分删除而不影响代码 3 中步骤 4.5 处 bad 置 1 的概率。根据 Coin fixing 定理[8]，Game $R2$ 中的随机预言机询问可以用一个 for-循环模拟，改为如下所示：

代码 4

设定 salt,c

选择：p0←PW,y0=Rand(n),i=0,U0=p0||salt

For s=0 to t−1Do

4.4 If(t<c−1&& Xs ==i||Ui)i=i+1, Ui = Rand(n)

4.5 elseif(i==c−1&& Xs ==i||Ui){bad=1}

End For

在 $R3$ 中假设查询序列 $x_0,x_1,\cdots,x_{t-1}$ 为最大化 $\Pr_{R3}[BAD]$ 的查询序列，则有 $\Pr_{R2}[BAD]\leqslant\Pr_{R3}[BAD]$。

注意到代码 4 中步骤 4.4 处的 $U_1,U_2\cdots,U_s,\cdots,U_{c-1}$ 是在游戏过程中随机生成的，即攻击者 A 不能越过中间 $c-1$ 次 H 计算直接得到导出密钥或者猜测到中间状态 i，所以，最好的攻击方式是从口令空间随机选择一个口令 p，生成消息 $0\|p\|salt$，并依次循环迭代计算 c 次，得到导出密钥，再随机选择另一个口令，直到 t 次计算结束。所以，在 Game $R3$ 中最多可以计算 $\lfloor t/c\rfloor$ 个口令 p 的导出密钥，每个 p 等于 p_0 的概率为 $1/|PW|$，所以，t 次询问中 x_s 与 $c-1\|u_{c-1}$ 相等的概率最多为 $\lfloor t/c\rfloor/|PW|$，最后可得 $\Pr_{R3}[BAD]\leqslant\lfloor t/c\rfloor/|PW|$。

综上可证得 ECMA-376 文件加密格式中的密钥导出算法的安全性定理：$Adv^{prf}_{\text{ECMA-376}}(t)<\lfloor t/c\rfloor/|PW|+t^2/2^n$，其中，当 $n\geqslant 128$ 时，上边界值的第 2 项为可忽略的。

4 数据和分析

应用 ECMA-376 密钥导出算法的安全性定理，Office 2007 及其后续版本中的密钥导出算法所使用的散列函数为 160 bit 的 SHA-1，经过至少 50 000 次的循环迭代计算，生成长 128 bit 的加密密钥。若用 l 表示口令的比特长度，即口令空间大小 $|PW|=2^l$，则攻击者 A 经过 t(假设 t 取 c 的整数倍)次随机预言机询问过后，获得不可区分优势满足如下条件：

$$Adv^{prf}_{\text{Office}}(t)<t/2^{l+1\text{bc}}+t^2/2^{128} \tag{6}$$

可以得出如下 4 个结论：

(1)当询问次数 $t\ll c|PW|$ 时，对于 Office 中的密钥导出

算法，A 获得的不可区分优势是可忽略的，说明此时 Office 中口令认证机制的密钥导出算法是安全的。

(2)由于循环次数 c 的引入使得穷尽口令搜索攻击 Office 口令认证机制的工作量增加了近 c 倍，相当于将用户口令的有效长度从原来的 l bit 扩展到了 $(l+1\text{b}c)$ bit。

(3)根据前文对口令认证机制的研究，对口令认证机制的攻击，可分为对口令空间进行穷尽搜索攻击以及直接对密钥空间进行攻击。当 $(l+1\text{b}c)>n$ 时，穷尽口令搜索攻击的代价比直接攻击密钥空间的代价更大。在 Office2007 版本的密钥导出算法中 c=50 004，n=128，所以，当口令长度 $l \geqslant 113$ bit 时应该选择攻击密钥空间。

(4)说明 Office 密钥导出算法中 "$i\|$" 的引入，并没有使其安全性有所改进，其不可区分优势和 PBKDF1 的一致[4]。

由上文的前 2 个结论得出对于 Office2007 及其后续版本加密文件的安全性取决于攻击者的计算能力以及用户口令空间大小，攻击者除了依次进行 c 次循环迭代计算基本散列函数外并没有其他捷径，所以，目前对 Office 加密文件的最有效攻击方法为强力攻击和字典攻击。目前 GPU(图形处理单元)以其强大的并行计算能力被广泛应用于密码运算中[11]，通过测试得出的单张目前主流的通用计算 GPU-ATI HD5970 与 nVidia GTX260 在 1 s 分别可计算 2 300M 次与 175M 的 SHA-1 运算，其中，1M= 2^{20}，则进行一次 SHA-1 计算所需时间分别为 $2^{-31.2}$ s 与 $2^{-27.5}$ s。假设用户口令的字符集为 a~z、A~Z、0~9 以及空格和问号共 64 个常用字符，则字符长度为 4 的口令空间集个数为 $64^4=2^{24}$。由第 3 个结论可知当字符长度不大于 18 时，应攻击用户口令空间，不同口令长度的穷尽搜索攻击时间代价如表 1 所示。

表 1 Office2007 及其后续版本加密文件口令穷尽搜索的时间代价

口令空间字符长度	Office2007 攻击时间		Office2010 攻击时间	
	HD5970	GTX260	HD5970	GTX260
4	5.7 min	1.2 h	11.5 min	2.4 h
5	6.0 h	19.6 d	12.1 h	39.5 d
6	96.7 d	3.5 y	193.5 d	7.0 y
7	17.2 y	223.5 y	34.5 y	447.0 y
8	1 100 y	14 303 y	2 200 y	28 606 y

通过表 1 的数据可知，Office2007 加密文件的口令认证机制在口令长度较小时存在安全隐患，当用户口令字符长度大于 6 时，使用 GPU 进行并行口令穷尽搜索由于巨大的时间代价而失效，此时 Office2007 加密文件的口令认证机制是安全的。Office2010 的安全性在各版本中最强，它的 KDF 里循环次数是 Office2007 的 2 倍，所以，对其进行穷尽口令攻击的时间是 2007 版的 2 倍。

5 结束语

本文使用 Game-Playing 技术证明了 ECMA-376 密钥导出算法与随机函数的不可区分优势，从而证明 Office 密钥导出算法是安全的。根据安全性定理，可以看到 Office2007 及其以后版本加密文件的口令认证机制安全性取决于攻击者的计算能力和用户口令空间大小。同时，针对基于 GPU 进行的穷尽口令搜索攻击的最新进展，通过实验得出当用户口令字符长度大于 6 时，Office2007 及其后续版本的加密文件具有一定的安全性。

参考文献

[1] 乔纳森·卡茨, 耶胡达·林德尔. 现代密码学——原理与协议[M]. 任 伟, 译. 北京: 国防工业出版社, 2011.

[2] 吴文玲, 冯国登, 张文涛. 分组密码的设计与分析[M]. 2 版. 北京: 清华大学出版社, 2009.

[3] RSA Laboratories. PKCS #5 v2.1: Password-based Cryptography Standard[EB/OL]. (2006-01-05). ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2_1.pdf.

[4] Yao F F, Yin Y L. Design and Analysis of Password-based Key Derivation Functions[C]//Proc. of CT-RSA'05. San Francisco, USA: [s. n.], 2005: 245-261.

[5] 何克晶. RC4 流密码与微软 Office 文档安全分析[J]. 计算机工程, 2009, 35(23): 130-132.

[6] 李小波, 管海兵, 李小勇, 等. Office 文件加密机制的安全性[J]. 计算机应用, 2010, 30(z1): 126-129.

[7] Microsoft Corporation. Office Document Cryptography Structure Specification[EB/OL]. (2012-02-20). http://msdn.microsoft.com/en-us/library/cc313071(v=office.12).aspx.

[8] Bellare M, Rogaway P. The Game-playing Technique[EB/OL]. (2004-06-06). http://eprint.iacr.org/.

[9] 徐 津, 温巧燕, 王大印. 一种新的一阶段加密认证模式[J]. 电子学报, 2009, 37(10): 2187-2191.

[10] Bellare M, Rogaway P. Code-based Game-playing Proofs and the Security of Triple Encryption[C]//Proc. of EUROCRYPT'06. St. Petersburg, Russia: Springer-Verlag, 2006: 409-426.

[11] 李昌新. 存储加密系统中加密和认证机制研究[D]. 厦门: 厦门大学, 2010.

编辑 任吉慧

(上接第 100 页)

参考文献

[1] Boneh D, Hamburg M. Generalized Identity-based and Broadcast Encryption Schemes[C]//Proc. of the 14th International Conference on the Theory and Application of Cryptology and Information Security. Melbourne, Australia: [s. n.], 2008.

[2] 陈昭智, 郑建德. 一种基于身份分层结构加密算法的广播加密方案[J]. 厦门大学学报, 2009, 45(3): 342-346.

[3] 吕锡香, 张卫东, 杨文峰. 基于双线性映射的非对称公钥叛逆者追踪[J]. 计算机工程, 2009, 35(3): 4-6, 44.

[4] Wang Jin, Bi Jingguo. Lattice-based Identity-based Broadcast Encryption[EB/OL]. [2010-12-11]. http://www.techrepublic.com/whitepapers/lattice-based-identity-based-broadcast-encryption-scheme/2868805.

[5] Regev O. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography[J]. Journal of the ACM, 2009, 56(6): 318-345.

[6] Cash D, Hofheinz D, Kiltz E. How to Delegate a Lattice Basis[C]//Proc. of the 29th Annual International Conference on Theory and Applications of Cryptographic Techniques. [S. l.]: Springer-Verlag, 2009.

[7] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for Hard Lattices and New Cryptographic Constructions[C]//Proc. of the 14th Annual ACM International Symposium on Theory of Computing. Victoria, Canada: [s. n.], 2008.

[8] Gentry C, Silverberg A. Hierarchical ID-based Cryptography[C]//Proc. of the 8th International Conference on the Theory and Application of Cryptology and Information Security. Queenstown, New Zealand: [s. n.], 2002.

[9] 祝跃飞, 张亚娟. 公钥密码学设计原理与可证安全[M]. 北京: 高等教育出版社, 2009.

[10] Canetti R, Halevi S, Katz J. A Forward-secure Public Key Encryption Scheme[J]. Journal of Cryptology, 2007, 20(3): 255-271.

编辑 张 帆