DOI:10.13229/j.cnki.jdxbgxb2011.02.037

基于身份的商品双重防伪机制

胡 亮,林海群,初剑峰,袁 巍,李宏图,赵 阔

(吉林大学 计算机科学与技术学院,长春 130012)

摘 要:提出了一种基于身份的商品双重防伪机制,其思想是通过对每一个最小销售单元赋予一个唯一的并隐藏有产品信息的身份标识作为产品查询号,同时采用基于身份的加密系统中由身份生成对应私钥的一种改进方法,获得一个产品身份对应的私钥(即防伪码),供用户比对。该方案生成的所有产品查询号唯一,且具有防伪成本低、易实现和可伪造性低等优点。最后,给出了该方案的算法安全性分析。

关键词:计算机应用;商品防伪;基于身份;双重防伪机制

中图分类号:TP309 **文献标志码**:A **文章编号**:1671-5497(2011)02-0447-05

Identity-based dual anti-counterfeit mechanism for products

HU Liang, LIN Hai-qun, CHU Jian-feng, YUAN Wei, LI Hong-tu, ZHAO Kuo

(*College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*)

Abstract: An identity-based dual anti-counterfeit mechanism is proposed. The basic idea of this mechanism is to give each minimum sale unit a unique identity as a product query number with hidden product information, while using the improved EXTRACT algorithm of identity-based encryption to get the private key corresponding to the product ID as the anti-counterfeit code, which is for user to compare. This scheme generates unique query numbers for all products with the advantages of low cost, hard to forge, easy for implementation and so on. Security analysis of the algorithm of the scheme is presented.

Key words: computer application; product anti-counterfeit; identity-based; dual anti-counterfeit mechanism

由于商品包装防伪[1]成本造价高,易被伪造,而目前市场上采用的数码防伪技术又几乎全部都是建立数据库,依靠数据检索核对随机组合生成的产品查询号码。当产品数据库的容量达到一定程度时,检索数据量极其庞大,产品的查询效率将受到严重影响。同时这些网络查询通常无法为用户提供鉴别产品真伪的其他辅助手段,如产品特性、使用方法等众多信息。

针对以上问题,本文提出一种基于身份的商品双重防伪机制,其思想是通过对每一个最小销售单元赋予一个唯一的并隐藏有产品信息的身份标识作为产品查询号,同时采用基于身份的加密

收稿日期:2009-07-10.

基金项目:国家自然科学基金项目(60873235,60473099);教育部新世纪优秀人才支持计划项目(NCET-06-0300);吉林省重点项目(20080318);吉林大学研究生创新项目(20080244);"973"国家重点基础研究发展规划项目(2009CB320706).

作者简介:胡亮(1968-),男,教授,博士生导师. 研究方向:网格计算与网络安全. E-mail:hul@mail.jlu.edu.cn

通信作者:初剑峰(1978-),男,博士研究生,讲师. 研究方向:计算机系统结构. E-mail:aa11@21cn.com

系统[2]中由身份生成对应私钥的一种改进方法，获得一个产品身份对应的私钥即防伪码，供用户比对。在用户查询产品真伪的同时，为用户提供了具体的产品信息，并提供假冒商品的追踪。

1 基于身份的双重防伪原理

1.1 符号定义

定义1 流水号 L 是根据每个最小销售单元的信息生成的一段固定长度的字符串，这些信息包括生产日期、产品编号、产品名称、批次、件号、盒号。根据该字符串即可获取对应的产品信息。

定义2 查询号 C 是为用户提供辨别产品真伪的查询编码，它是由流水号 L 经过变换生成的，与 L 一一对应，并且是唯一的，因此可以作为产品的一个身份标识。

定义3 防伪码 F 是为产品提供第二层防伪查询的编码，每个查询号 C 都有与它相对应的一个防伪码 F 。

1.2 对称密码

对称密码是一种加解密使用相同密钥的密码体制，也称为传统密码算法[3]。对称算法的加密和解密表示为

$$E_K(M)=C;D_K(C)=M$$

式中：K 为对称密钥；M 为明文；C 为密文；E 为加密算法；D 为解密算法。

对称密码加密/解密速度快[4]，并且加密解密所使用的密钥是相同的，这样系统就无需保存过多的密钥对，并且能够提高系统的效率。

1.3 BF-IBE加密方案

在BF-IBE(Identity-based encryption)加密方案[2]中，每个用户的公钥就是用户的ID，或者由ID导出，它的核心是使用了超奇异的椭圆曲线[5]的双线性映射。该方案具体的执行算法[6-7]如下：

(1)SETUP(系统参数建立)

①选择一个k-bit并且满足 $p=2 \bmod 3$，$p=6q-1$ 的素数(q 为一个大于3的素数)。设 E 是定义在 Fp 上的椭圆曲线 $y^2=x^3+1$。选择一个任意的具有 q 阶的点 $P\in E/(Fp)$。

②找到一个随机数 $s\in Zq^*$，设置 $P_{\text{pub}}=sP$。主密钥 s 通过 sP 方式秘密共享。

③选择4个哈希函数 $H:F_{p^2}\rightarrow\{0,1\}^n$，$G:\{0,1\}^*\rightarrow F_p$，$H_1:\{0,1\}^n\times\{0,1\}^n\rightarrow F_q$，$G_1:\{0,1\}^n\rightarrow\{0,1\}^n$。明文空间为 $M=\{0,1\}^n$。密文空间为 $C=E/F_p\times\{0,1\}^n$。系统参数为 $params=\langle p,n,P,P_{\text{pub}},G,H,G_1,H_1\rangle$。主密钥为 $s\in Z_q$。

(2)EXTRACT(用户私钥提取)

①用MapToPoint算法将ID映射到一个具有 q 阶的点 Q_{ID}。

②设置私钥 $d_{\text{ID}}=sQ_{\text{ID}}$。

(3)ENCRYPT(加密)

①用MapToPoint算法将ID映射到一个 q 阶的点 Q_{ID}。

②选择一个随机串 σ，设置 $r=H_1(\sigma,M)$。

③计算密文 $C=\langle rP,\sigma\oplus H(g_{\text{ID}}^r),M\oplus G_1(\sigma)\rangle$，其中 $g_{\text{ID}}=e(Q_{\text{ID}},P_{\text{pub}})\in F_{p^2}$。

(4)DECRYPT(解密)

设加密算法形式为 $C=\langle U,V,W\rangle\in C$

①计算 $V\oplus H[e(d_{\text{ID}},U)]=\sigma$。

②计算 $W\oplus G_1(\sigma)=M$。

③ $r=H_1(\sigma,M)$，测试 $U=rP$。如不成功，则退出。

④输出明文 M。

1.4 防伪原理

基于身份的双重防伪方案采用了对称加密技术以及基于身份的加密体系中根据用户身份得到对应私钥的生成算法的一个变型。它的防伪原理为：①商品制造商将要出厂的一批产品参数提交给管理员，获得该批次的所有最小销售单元的防伪标签码 (C,F) 的列表；由商品制造商负责为每个最小销售单元附上相应的防伪标签。②管理员负责审核商品制造商提交的产品参数并提交给防伪标识生成模块；获取已生成的防伪标识列表并提交给商品制造商，同时将合法的、已经生成防伪标识的同一批次产品信息(包括生成日期、产品编号、产品名称、总件数、总盒数等)录入到后台数据库中，提供合法产品验证。③防伪标识生成模块根据管理员提交的产品信息为每个最小销售单元生成流水号 L，采用对称加密技术加密流水号 L，生成与流水号 L 一一对应的产品查询号 C。当密钥取定后，每一个明文分组都有唯一的密文与之对应，因此产品查询号可以作为产品的唯一身份，产品防伪码根据该唯一身份生成。④防伪查询模块负责用户查询数据的管理和提交后台数据管理模块；由后台数据管理模块处理查询数据并返回查询结果。

基于上述说明，本文提出的基于身份的商品

双重防伪机制具有以下功能：

①为每一件产品赋予一个唯一的身份码，且无任何规律。②产品信息的编码中包含了产品编号、生产日期、批次、件号、盒号这些具有产品个性化的信息。③消费者可以通过网络查询方式自主地对产品的真伪进行查询和辨别。④对上万件产品的防伪标识只需要在数据库中保存一条相应记录即可判断产品的真伪。解决了目前检索数据量庞大的问题，节约空间，同时提高海量数据的查询效率。⑤为每一件产品提供双重防伪机制，只有在用户获取到产品的详细信息，同时保证防伪码一致的情况下才可以确认产品的真伪。

2　新的基于身份的商品防伪方案

新的基于身份的商品防伪方案包括：①初始化；②产品编码；③产品查询号的生成；④产品防伪码的生成；⑤商品验证。其中，初始化过程包括对称密钥的生成以及 BF-IBE 系统的 Setup 过程[2]。

由流水号 L 的定义可知，不同的产品对应的流水号不同，流水号又与查询号一一对应，因此任何一个产品查询号是唯一的。一个产品查询号以及防伪码的生成包括以下几个步骤：根据产品信息编码为产品流水号、将产品流水号对称加密生成产品查询号、产品查询号根据私钥生成算法形成产品防伪码。

2.1　产品信息编码为产品流水号

所谓编码就是将产品信息编码为一段有序的字符串，即产品流水号。该产品流水号是一个 16 进制编码，每一个产品信息以 16 进制形式占据一定的位数。图 1 是产品信息编码的一种格式。

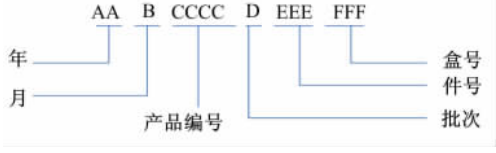

图 1　流水号格式

Fig. 1　Pattern of Serial Number

设以图 1 为例的一个产品流水号编码为 0ACEE3A500014C5，那么其对应的产品信息为：2010 年 12 月生产，产品编号为 EE3A 的第 5 批次第 1 件的第 4C5 盒。在实际生产过程中，可以根据实际情况进行分配。为了便于理解，以下的算法说明都是按照该分配方案进行。

2.2　产品查询号生成

为了保证产品查询号的位数，采用 36 进制（大写字母 A～Z，0～9）形式来表示。它的生成过程如下：

$$C = Z_{36}[E_K(L)]$$

首先对产品流水号 L 用系统初始化过程中选取的对称密钥 K 进行加密，再将得到的密文转换为 36 进制形式。

2.3　产品防伪码生成

采用基于身份的加密系统中身份的概念，每一个产品流水号都对应了一个唯一的产品查询号，因此该产品查询号就可以作为一个产品的唯一身份标识，并根据该身份标识生成对应私钥。这里采用 BF-IBE 系统[2]中 EXTRACT 步骤中的生成私钥方案的一个变型，过程如下：

(1) $Q_{\mathrm{ID}} = H_1(C)$；

(2)生成私钥 $d_{\mathrm{ID}} = (s+L)Q_{\mathrm{ID}}$。

由于主密钥 s 与流水号 L 由不同的实体进行保管，这样可以解决 IBE 系统中主密钥由单个实体托管的问题。

d_{ID} 就是一个由初始化过程中生成的主密钥 s 和已经验证合法的流水号 L 计算得到的私钥。设 d_{ID} 在椭圆曲线上的横纵坐标分别为 x、y。同样，需要将该点变换成一个用户可读的防伪码，变换过程如下：

$$F = Z_{36}[CRC_{32}(x) \parallel CRC_{32}(y)]$$

或　$F = Z_{36}[HASH_{64}(x \parallel y)]$

式中：$CRC_{32}(m)$ 是指对 m 进行 32 bit 的 CRC 校验后得到的值；$HASH_{64}$ 为 64 bit 的压缩函数；符号“$\parallel$”表示字的有结构的联结，即从联结后的字 $x \parallel y$ 总可以准确恢复出原来的字 x 和字 y。

2.4　验证过程

消费者购买的产品上的标签附有查询号和防伪码 2 个号码。用户只要在登录该产品查询网站，输入所需要查询的产品查询号即可进行产品的真伪验证，具体过程如下：

(1)用户登录防伪查询模块，输入该产品标签上的查询号，假设为 C'；该模块提交用户输入的查询号，后台数据处理模块首先将该查询号转换为二进制编码，再由对称解密模块用对称密钥进行解密，得到该产品对应的产品流水号 L'，即

$$L' = D_K[Z_2(C')]$$

(2)根据产品流水号 L' 通过解码即可获得对应该 L' 的产品信息，即生产日期 MFD、产品编号

No.、批次BN、件号PN、盒号BoxN。

(3)将产品的生产日期MFD、产品编号No.以及批次BN与数据库记录进行比对,若存在对应记录,再依次查看产品件号PN和盒号BoxN是否在对应记录中的总件数SUMPN和总盒数SUMBoxN的范围之内,即:

```
IF Exist(MFD,No.,BN) THEN
  IF PN <= SUMPN AND BoxN <= SUMBoxN THEN
    RETURN TRUE
  ELSE
    RETURN FALSE
ELSE
  RETURN FALSE
```

如果比对成功,后台数据管理模块为用户提供该查询号对应商品的具体信息,同时为该商品提供一个防伪码与标签上的F进行比对,为产品提供第二层防伪标识,否则,直接告知用户该产品一定是假冒商品。

用户在查询防伪码时,后台数据管理模块通过计算自动得出产品的相关信息,所以,该标签不需要数据检索,不受数据容量、查询次数、时效的限制,查询效率极高。

3 算法安全性分析

对该方案的安全性分析主要从算法的安全性分析角度考虑。由于本方案采用的是对称加密算法与基于身份的加密系统中EXTRACT算法的改进,一个敌手如果能够根据若干个合法查询号推出其余产品查询号以及相应的防伪码,就赢得胜利,而产品流水号的获取取决于对称算法的安全性,产品防伪码的获取取决于改进的EXTRACT算法的安全性。因此,以下就结合本方案从对称算法以及EXTRACT算法的角度进行方案的安全性分析。

3.1 对称算法的安全性分析

相邻的产品流水号对应的产品查询号是无任何规律的,攻击者A只有在已知产品流水号以及对称算法的私钥后才可以获取相应的产品查询号。假设攻击者A通过有限个合法的查询号$C_1,\cdots,C_n$送入系统进行查询后,获得相应的产品信息$M_1,\cdots,M_n$,再假设攻击者A可以根据这些产品信息组合成为流水号$L_1,\cdots,L_n$,即相当于明文,这就等价于已知明文攻击[3]。

事实上,对现有的对称密码算法,攻击者欲得到一些明、密文对并不困难,一般来说,现有的对称密码算法经得起已知明文的攻击[8]。并且,在本方案中,攻击者A必须提供合法的查询号进行查询,否则防伪查询模块无法提供一个正确的产品信息。那么攻击者所伪造出的一个非法查询号以及防伪码对该方案的攻击没有任何意义。

3.2 EXTRACT改进算法的安全性分析

由查询号生成对应防伪码的过程相当于基于身份加密系统中的以下情况,即敌手具有有限个身份ID以及对应ID的私钥。以下就该攻击方法给出相应的安全性说明。

针对本文提出的设计方案,一个敌手如果能够根据多个产品查询号及防伪码获得系统采用的主密钥,那么就赢得胜利。

这里假设敌手已知有限个查询号$C_1,\cdots,C_n$以及由$C_1,\cdots,C_n$生成的相应的私钥$d_1,\cdots,d_n$。其中$d_1=(s+L_1)H(C_1),\cdots,d_n=(s+L_n)H(C_n)$。即使在$L_1,\cdots,L_n$已知的情况下对该方案攻击(相当于IBE方案中的合谋攻击),即允许攻击者A访问oracle-EXTRACT(s,.)[9],安全的IBE方案是能够抵抗此类攻击的。

另外,在本方案中,防伪码是由私钥d_1上横纵坐标的64 bit压缩。假设采用的是512 bit的安全级别,那么由已知的防伪码恢复到真实的私钥d_1的概率为$1/(2^{16}*64)$。

采用本方案的优势在于,即使密钥泄露敌手也无法通过修改数据库伪造出自己要求的产品信息对应的数据记录;并且根据认证日志[10],一旦密钥泄露可及时追踪。

4 结束语

本文结合了对称加密算法并给出了一种基于身份的加密系统中EXTRACT算法的改进方案,提出了一种基于身份的双重防伪机制,通过结合密码学技术实现了自动化的防伪标签生成、验证及全程电子监管。该方案具有以下特点:

(1)批量生成。对于一批商品,管理员只需要提交该批商品的特征信息,防伪标识生成模块就会自动为该批商品中的每一个最小销售单元分别编号并生成相应的查询号及防伪码。

(2)海量数据查询。设一批货物中共有M件产品,每一件产品中包含N盒最小销售单元。在现有的产品防伪技术中,$M\times N$个单元需要在数

据库中保存 $M \times N$ 个数据记录，而在该方案中，$M \times N$ 个单元对应一条数据库记录，相对于目前已有的方案节省了海量数据查询时间。

(3)双重防伪机制。由于产品查询号本身就可以提供一层产品防伪功能，并且由对称密码算法可以推出，产品查询号具有唯一性，这样就不存在两个产品防伪标签 (C_1, F_1)、(C_2, F_2) 使得 $C_1 = C_2$ 且 $F_1 = F_2$。防伪码作为一个对查询号的第二重验证标识，即使在生成防伪码时使用了压缩算法也不会影响用户对产品查询号的防伪验证。

参考文献：

[1] 张逸新，吴梅. 包装的材料防伪技术[J]. 包装工程，2003，24(5)：86-89.
Zhang Yi-xin，Wu Mei. Security technology of packaging materials[J]. Packaging Engineering，2003，24(5)：86-89.

[2] Boneh D，Franklin M. Identity-based encryption from the weil pairing[J]. Lecture Notes in Computer Science，2001，2139：213-229.

[3] Stallings W. Cryptography and Network Security Principles and Practices[M]. New Jersey，USA：Prentice Hall，2005.

[4] 胡亮，袁巍，于孟涛，等. 单向性策略与 AES 密钥生成算法的改进[J]. 吉林大学学报：工学版，2009，39(1)：137-142.
Hu Liang，Yuan Wei，Yu Meng-tao，et al. One-way property strategy and improvement of key generation algorithm of Rijndael[J]. Journal of Jilin University (Engineering and Technology Edition)，2009，39(1)：137-142.

[5] Hankerson D，Menezes A，Vanstone S. Guide to Elliptic Curve Cryptography[M]. New York：Springer-Verlag，2004.

[6] 胡亮，初剑峰，林海群，等. IBE 体系的密钥管理机制[J]. 计算机学报，2009，32(3)：543-551.
Hu Liang，Chu Jian-feng，Lin Hai-qun，et al. The key management mechanism of IBE system[J]. Chinese Journal of Computers，2009，32(3)：543-551.

[7] 胡亮，初剑峰，林宇，等. 基于信任服务的 IBE 系统[J]. 吉林大学学报：工学版，2009，39(3)：737-742.
Hu Liang，Chu Jian-feng，Lin Yu，et al. IBE system based on trust service[J]. Journal of Jilin University (Engineering and Technology Edition)，2009，39(3)：737-742.

[8] 冯登国. 可证明安全性理论和方法研究[J]. 软件学报，2005，16(10)：1743-1756.
Feng Deng-guo. Research on theory and approach of provable security[J]. Journal of Software，2005，16(10)：1743-1756.

[9] Canetti R，Golreich O，Halevi S. The random oracle methodology，revisited[J]. Journal of the ACM，2004，51(4)：557-594.

[10] 马兆丰，冯博琴，宋擒豹，等. 面向认证的传统商品数字化防伪机制研究[J]. 计算机工程，2003，29(3)：14-16.
Ma Zhao-feng，Feng Bo-qin，Song Qin-bao，et al. Research on authentication-oriented digital countfeit mechanism for traditional merchandise[J]. Computer Engineering，2003，29(3)：14-16.