(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103117857 A
(43)申请公布日 2013.05.22

(21)申请号 201310014539.8
(22)申请日 2013.01.16
(71)申请人 深圳市怡化电脑有限公司
地址 518000 广东省深圳市福田区金田路4018号安联大厦27楼A02
申请人 深圳市怡化时代科技有限公司
深圳市怡化金融智能研究院
(72)发明人 赵玉民 韦静
(74)专利代理机构 深圳市兴科达知识产权代理有限公司 44260
代理人 王翀
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)
G06Q 20/18(2012.01)

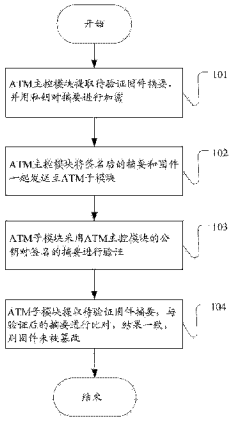
权利要求书1页 说明书4页 附图2页

(54)发明名称

基于硬件加密算法的ATM机信息安全检测方法及系统

(57)摘要

本发明提供了一种基于硬件加密算法的ATM机信息安全检测方法及系统，该方法包括步骤：a：ATM主控模块提取待验证固件摘要，并用私钥对摘要进行加密；b：ATM主控模块将签名后的摘要和固件一起发送至ATM子模块；c：ATM子模块采用ATM主控模块的公钥对签名的摘要进行验证；d：ATM子模块提取待验证固件摘要，与验证后的摘要进行比对，结果一致，则固件未被篡改。本发明提供的基于硬件加密算法的ATM机信息安全检测方法及系统，通过对ATM机各模块固件代码进行身份验证，使通过认证的模块得以工作，以杜绝产品被攻击者伪造、盗用；从而保证ATM机生产商和用户的财产安全。



CN 103117857 A

1. 一种基于硬件加密算法的 ATM 机信息安全检测方法，其特征在于，包括步骤：

a :ATM 主控模块提取待验证固件摘要，并用私钥对摘要进行签名；

b :ATM 主控模块将签名后的摘要和固件一起发送至 ATM 子模块；

c :ATM 子模块采用 ATM 主控模块的公钥对签名的摘要进行验证；

d :ATM 子模块提取待验证固件摘要，与验证后的摘要进行比对，结果一致，则固件未被篡改。

2. 如权利要求 1 所述的基于硬件加密算法的 ATM 机信息安全检测方法，其特征在于，步骤 a 中所述用私钥对摘要进行签名包括：

密钥生成

（1）任意选取两个不同的大质数 p 和 q；

（2）计算乘积 n=p*q，φ（n）=（p-1）（q-1），φ（n）为 n 的欧拉函数；

（3）随机选择整数 e（1<e<φ（n）），要求满足 gcd（e，φ（n））=1，即 e 与 φ（n）互质；

（4）用扩展的 Euclidean 算法计算私钥 d，以满足 $d*e \equiv 1 \bmod (\varphi(n))$，即 $d \equiv e^{-1} \bmod (\varphi(n))$；

得到：公钥为 e 和 n，d 是私钥；

加密过程

明文先转换为比特串分组，使每个分组对应的十进制数小于 n，即分组长度小于 $\log_2 n$，然后对每个明文分组 m_i 作加密运算，具体过程如下：

（s1）获得接收公钥（e，n）；

（s2）把信息 M 分组长度为 L（$L<\log_2 n$）的消息分组 $M=m_1m_2\cdots m_t$；

（s3）使用加密算法 $c_i = m_i^e \bmod n$（$1 \leqslant i \leqslant t$），计算出密文 $C = c_1c_2\cdots c_t$；

签名：$H=\mathrm{Hash}(M)$，$S \equiv H^d \bmod n$。

3. 如权利要求 2 所述的基于硬件加密算法的 ATM 机信息安全检测方法，其特征在于，所述步骤 c 具体包括：

（A）将密文 C 按长度 L 分组得 $C = c_1c_2\cdots c_t$；

（B）使用私钥 d 和解密算法 $m_i = c_i^d \bmod n$（$1 \leqslant i \leqslant t$）计算得 m_i；

（C）得到明文 $M=m_1m_2\cdots m_t$；

验证：$H \equiv S^e \bmod n$ 和 Hash(M) 是否相等。

4. 一种 ATM 机信息安全检测系统，其特征在于，包括：

ATM 主控模块、ATM 子模块，ATM 主控模块通过网线或 CAN 总线与 ATM 子模块建立通信；

ATM 主控模块包括：提取单元、签名单元；

提取单元用于提取待验证固件摘要；

签名单元用于通过私钥对摘要进行加密；

ATM 子模块包括：验证单元、提取单元、比较单元；

验证单元用于采用公钥对签名的摘要进行验证；

提取单元用于提取待验证固件摘要；

比较单元用于与验证后的摘要进行比对，结果一致，则固件未被篡改。

基于硬件加密算法的ATM机信息安全检测方法及系统

技术领域

[0001] 本发明涉及ATM机信息安全技术领域，尤其涉及一种基于硬件加密算法的ATM机信息安全检测方法及系统。

背景技术

[0002] 目前，随着我国银行ATM机的不断增加，在方便百姓、提高了银行自身服务效率、活跃金融市场的同时，随之而来的利用ATM机盗取客户存款的犯罪手段也日渐增多，如何进行防范成为银行比较头痛的问题。常见的犯罪手段有以下几种：1. 安装针孔摄像头窃取用户信息；2. 堵塞ATM机的出钞口；3. 更换ATM机子模块、固件代码等方式窃取用户信息，如：在ATM机的插卡口加装假读卡器；在ATM机的键盘上加装假键盘等。

[0003] 通常银行、公安对上述犯罪手段只能做到事后取证调查，即当有客户发生存款丢失后客户报案，相关部门在到案发现场调查、同时提取录像资料(有部分ATM机上装备了摄像机)等等，从中查找线索、证据，这种方式不及时、也很被动，已经远远落后于我们经济建设的步伐。

发明内容

[0004] 本发明的目的在于提供一种基于硬件加密算法的ATM机信息安全检测方法及系统，通过对ATM机各模块固件代码进行身份验证，使通过认证的模块得以工作，以杜绝产品被攻击者伪造、盗用。

[0005] 本发明的目的是通过以下技术方案实现的。

[0006] 一种基于硬件加密算法的ATM机信息安全检测方法，包括步骤：

[0007] a：ATM主控模块提取待验证固件摘要，并用私钥对摘要进行签名；

[0008] b：ATM主控模块将签名后的摘要和固件一起发送至ATM子模块；

[0009] c：ATM子模块采用ATM主控模块的公钥对签名的摘要进行验证；

[0010] d：ATM子模块提取待验证固件摘要，与验证后的摘要进行比对，结果一致，则固件未被篡改。

[0011] 优选的，步骤a中所述用私钥对摘要进行签名包括：

[0012] 密钥生成

[0013] (1) 任意选取两个不同的大质数p和q；

[0014] (2) 计算乘积n=p*q，φ(n)=(p-1)(q-1)，φ(n)为n的欧拉函数；

[0015] (3) 随机选择整数e(1<e<φ(n))，要求满足gcd(e，φ(n))=1，即e与φ(n)互质；

[0016] (4) 用扩展的Euclidean算法计算私钥d，以满足d*e ≡ 1mod(φ(n))，即 $d \equiv e^{-1} \bmod (\phi(n))$；

[0017] 得到：公钥为e和n，d是私钥；

[0018] 加密过程

[0019] 明文先转换为比特串分组，使每个分组对应的十进制数小于 n，即分组长度小于 $\log_2 n$，然后对每个明文分组 m_i 作加密运算，具体过程如下：

[0020] （s1）获得接收公钥（e，n）；

[0021] （s2）把信息 M 分组长度为 L（$L<\log_2 n$）的消息分组 $M=m_1m_2\cdots m_t$；

[0022] （s3）使用加密算法 $c_i = m_i^e \bmod n$（$1 \leqslant i \leqslant t$），计算出密文 $C = c_1c_2\cdots c_t$；

[0023] 签名：$H=Hash(M)$，$S \equiv H^d \bmod n$。

[0024] 优选的，所述步骤 c 具体包括：

[0025] （A）将密文 C 按长度 L 分组得 $C = c_1c_2\cdots c_t$；

[0026] （B）使用私钥 d 和解密算法 $m_i = c_i^d \bmod n$（$1 \leqslant i \leqslant t$）计算得 m_i；

[0027] （C）得到明文 $M=m_1m_2\cdots m_t$；

[0028] 验证：$H \equiv S^e \bmod n$ 和 Hash(M) 是否相等。

[0029] 一种 ATM 机信息安全检测系统，包括：

[0030] ATM 主控模块、ATM 子模块，ATM 主控模块通过网线或 CAN 总线与 ATM 子模块建立通信；

[0031] ATM 主控模块包括：提取单元、签名单元；

[0032] 提取单元用于提取待验证固件摘要；

[0033] 签名单元用于通过私钥对摘要进行加密；

[0034] ATM 子模块包括：验证单元、提取单元、比较单元；

[0035] 验证单元用于采用公钥对签名的摘要进行验证；

[0036] 提取单元用于提取待验证固件摘要；

[0037] 比较单元用于与验证后的摘要进行比对，结果一致，则固件未被篡改。

[0038] 本发明实施例与现有技术相比，本发明提供的基于硬件加密算法的 ATM 机信息安全检测方法及系统，通过对 ATM 机各模块固件代码进行身份验证，使通过认证的模块得以工作，以杜绝产品被攻击者伪造、盗用；从而保证 ATM 机生产商和用户的财产安全。

附图说明

[0039] 图 1 是本发明 ATM 机信息安全检测方法流程图；

[0040] 图 2 是本发明实施例使用的非对称密钥进行安全认证示意图。

图 3 是本发明 ATM 机信息安全检测系统原理框图。

具体实施方式

[0041] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0042] 请参阅图 1 所示，本发明 ATM 机信息安全检测方法，包括：

[0043] 步骤 101：ATM 主控模块提取待验证固件摘要，并用私钥对摘要进行加密；

[0044] 提取固件摘要用于检测固件的完整性，判断固件是否被篡改；用私钥对摘要进行加密即签名，用于子模块对固件来源的鉴定，只有私钥拥有方才能生成相应的签名，如果不是私钥拥有方签名的固件，子模块不予以升级和运行。

[0045] 生成摘要的算法有 MD5、HASH 算法如 SHA-256、SHA-512 等，签名的算法有 RSA 等。RSA 算法既能用于数据加密也能用于数字签名，算法描述如下：

[0046] 1. 密钥生成

[0047] （1）任意选取两个不同的大质数 p 和 q，(例如长度都接近 512Bit)；

[0048] （2）计算乘积 n=p*q，φ（n）=（p-1）（q-1），φ（n）为 n 的欧拉函数；

[0049] （3）随机选择整数 e（1<e<φ（n)),要求满足 gcd（e，φ（n))=1,即 e 与 φ（n）互质。

[0050] （4）用扩展的 Euclidean 算法计算私钥 d，以满足 d*e ≡ 1mod（φ（n)),即 $d \equiv e^{-1} \bmod (\varphi(n))$。

[0051] 得到：公钥为 e 和 n，d 是私钥(两个素数 p 和 q，可销毁，不能泄露)。

[0052] 2. 加密过程

[0053] 明文先转换为比特串分组，使每个分组对应的十进制数小于 n，即分组长度 小于 $\log_2 n$，然后对每个明文分组 m_i 作加密运算，具体过程如下：

[0054] （1）获得接收公钥(e，n)；

[0055] （2）把信息 M 分组长度为 L（L<$\log_2 n$）的消息分组 $M=m_1m_2\cdots m_t$；

[0056] （3）使用加密算法 $c_i = m_i^e \bmod n$（$1 \leqslant i \leqslant t$），计算出密文 $C = c_1c_2\cdots c_t$；

[0057] 3. 签名：H=Hash(M)，$S \equiv H^d \bmod n$

[0058] 步骤 102：ATM 主控模块将签名后的摘要和固件一起发送至 ATM 子模块；

[0059] 步骤 103：ATM 子模块采用 ATM 主控模块的公钥对签名的摘要进行验证；具体如下：

[0060] 4. 解密过程

[0061] （1）将密文 C 按长度 L 分组得 $C = c_1c_2\cdots c_t$；

[0062] （2）使用私钥 d 和解密算法 $m_i = c_i^d \bmod n$（$1 \leqslant i \leqslant t$）计算得 m_i；

[0063] （3）得到明文 $M=m_1m_2\cdots m_t$。

[0064] 5. 验证：$H \equiv S^e \bmod n$ 和 Hash(M) 是否相等。

[0065] 步骤 104：ATM 子模块提取待验证固件摘要，与验证后的摘要进行比对，结果一致，则固件未被篡改，且确实是拥有私钥的 ATM 主控模块发来的信息，ATM 子模块可以使用和运行该固件。

[0066] 数字签名是一串二进制数，应与被签名的信息“绑定”在一起。它提供一种鉴别方法，以解决伪造、抵赖、冒充等问题。数字签名在信息安全中，包括身份认证、数据完整性、不可否认性等方面的重要应用，特别是在大型网络安全通信中的密钥分配、认证以及电子商务系统中具有重要作用。

[0067] RSA 签名方案是目前使用较多的一个签名方案，也是已经提出的数字签名方案中最容易理解和实现的签名方案，其安全性基于大整数因子分解的困难性。

[0068] 图 2 所示实施例中，使用的是非对称密钥加密算法，同样，基于对称密钥 加密算法的验证方式也适用。对称加密算法所用的加密密钥和解密密钥通常是相同的，即使不同也可以很容易地由其中的任意一个推导出另一个。在此算法中，加、解密双方所用的密钥都要保守秘密。由于计算速度快而广泛应用于对大量数据如文件的加密过程中，如 RD4 和 DES。

[0069] 图 2 所示实施例，重点说明了 ATM 子模块验证主控模块发来的固件等数据的合法性，同样，使用所述方法也适用于 ATM 主控模块验证子模块发来的数据的合法性，非授权的子模块发来的数据不予以响应并发出错误警告。

[0070] 请参阅图 3 所示，本发明 ATM 机信息安全检测系统，包括 ：

[0071] ATM 主控模块、ATM 子模块，ATM 主控模块通过网线或 CAN 总线等串行总线与 ATM 子模块建立通信 ；

[0072] ATM 主控模块包括 ：提取单元、签名单元 ；

[0073] 提取单元用于提取待验证固件摘要 ；

[0074] 签名单元用于通过私钥对摘要进行加密 ；

[0075] ATM 子模块包括 ：验证单元、提取单元、比较单元 ；

[0076] 验证单元用于采用公钥对签名的摘要进行验证 ；

[0077] 提取单元用于提取待验证固件摘要 ；

[0078] 比较单元用于与验证后的摘要进行比对，结果一致，则固件未被篡改。

[0079] 综上，本发明提供的基于硬件加密算法的 ATM 机信息安全检测方法及系统，通过对 ATM 机各模块固件代码进行身份验证，使通过认证的模块得以工作，以杜绝产品被攻击者伪造、盗用 ；从而保证 ATM 机生产商和用户的财产安全。

[0080] 以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

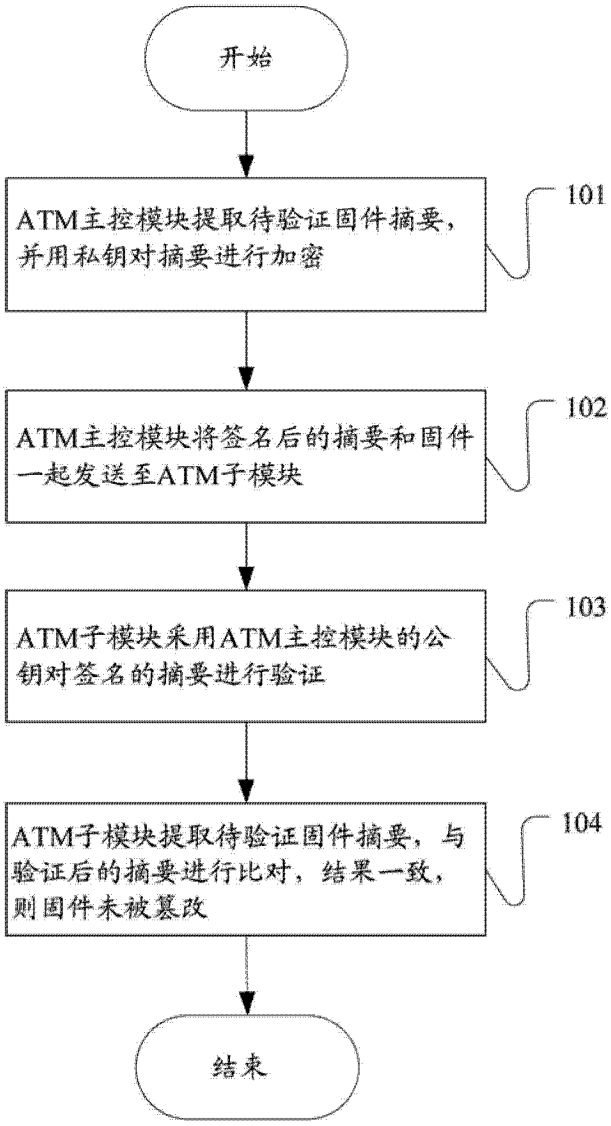

开始
ATM主控模块提取待验证固件摘要，并用私钥对摘要进行加密
101
ATM主控模块将签名后的摘要和固件一起发送至ATM子模块
102
ATM子模块采用ATM主控模块的公钥对签名的摘要进行验证
103
ATM子模块提取待验证固件摘要，与验证后的摘要进行比对，结果一致，则固件未被篡改
104
结束

图 1

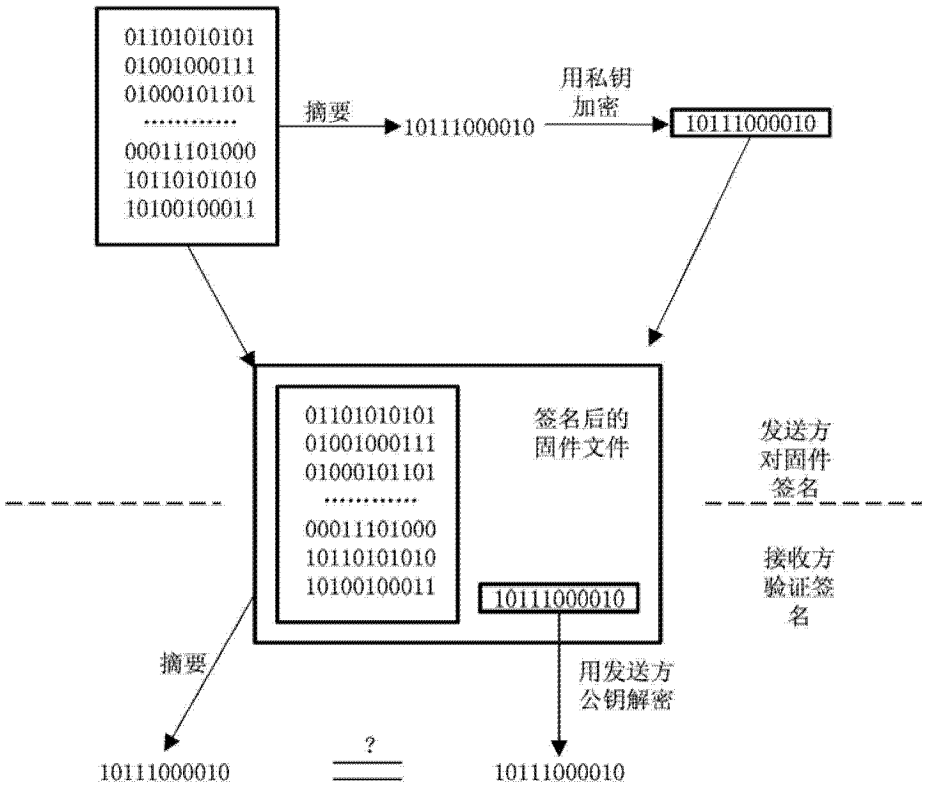

01101010101
01001000111
01000101101
.....
00011101000
10110101010
10100100011
摘要
10111000010
用私钥
加密
10111000010
01101010101
01001000111
01000101101
.....
00011101000
10110101010
10100100011
签名后的
固件文件
10111000010
发送方
对固件
签名
接收方
验证签
名
摘要
用发送方
公钥解密
10111000010
?
10111000010

图 2

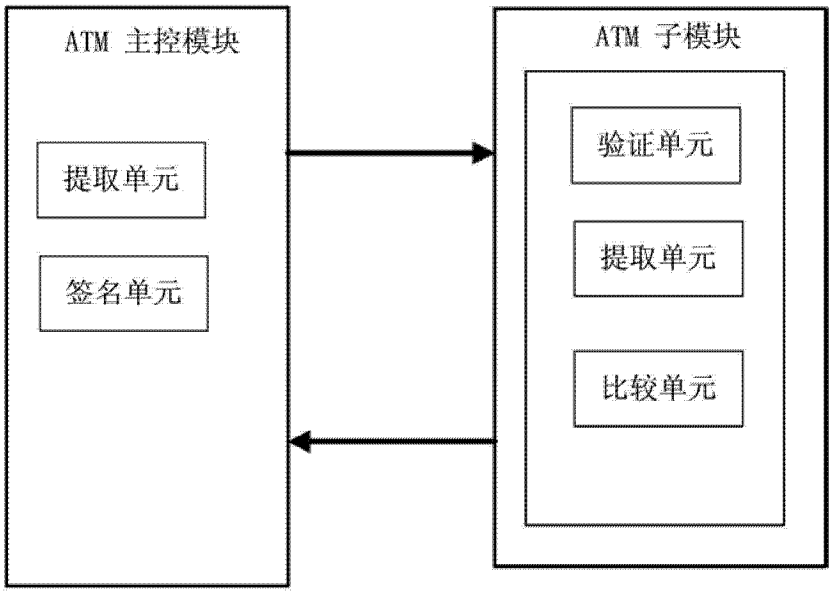

ATM 主控模块
提取单元
签名单元
ATM 子模块
验证单元
提取单元
比较单元

图 3