基于身份认证加密的私钥共享方案及其应用*

封化民[1,2]，孙轶茹[1]，孙 莹[2]
(1. 西安电子科技大学 通信工程学院，西安 710000；2. 北京电子科技学院，北京 100070)

摘 要：为了解决基于身份的认证加密方案中私钥共享的问题，结合可验证的(t,n)门限秘密共享方案，提出了一种新的私钥共享方案，并与已有私钥共享方案进行了对比分析，分析表明该方案在效率方面有较大的优势且安全性也较高。结合基于身份的认证加密方案，提出了一个在政府内网的电子公文安全交换模型，为实现电子公文的快速交换提供了安全保证。通过分析可知，该方案效率较高且安全。

关键词：基于身份的加密方案；PKI；BDH 问题；电子公文；秘密共享
中图分类号：TP309.7 **文献标志码**：A **文章编号**：1001-3695(2014)05-1507-04
doi:10.3969/j.issn.1001-3695.2014.05.054

Authenticated identity-based private key sharing scheme and its application

FENG Hua-min[1,2], SUN Yi-ru[1], SUN Ying[2]
(1. *Institute of Communication Engineering, Xi'an Electronic & Science University, Xi'an* 710000, *China*; 2. *Beijing Electronic Science & Technology Institute, Beijing* 100070, *China*)

Abstract: In order to solve the private sharing problem in the authenticated identity-based scheme, combined with (t,n) threshold verifiable secret sharing scheme, this paper proposed a new private key sharing scheme, and with the existing private key sharing scheme, made a comparative analysis. Analysis showed that this scheme had a greater advantage in terms of efficiency and it's also safety. It also combined with authentication identity-based encryption scheme, and provided a security electronic document interchange model in the government network, to achieve the rapid exchange of electronic documents and to provide the security guarantee. Analysis shows that the scheme is safe and high efficiency.

Key words: identity-based encryption; PKI; BDH problem; electronic official document; secret sharing

0 引言

我国电子政务在近些年得到了快速的发展，由于电子公文传送中的涉密问题的要求和网络安全问题[1~3]，影响了电子政务的发展。因此要加快电子政务的发展，先解决一个重要的问题是如何安全高效地交换电子公文。在文献[4~9]中给出了PKI 在电子政务中的应用，这些方案都较好地解决了身份认证、电子公文安全传递等问题，但是由于 PKI 自身的不足，影响了电子公文传输的效率，传输的成本也较高。因此，本文引入基于身份的认证加密方案[10]，在一定程度上解决了 PKI 方案的不足，保证了电子公文安全交换的同时也提高了运转效率。

但是基于身份的加密方案[11~16]需要一个 PKG 集中式管理系统私钥，这就存在着泄密的风险和权利过度集中在 PKG 的问题。所以本文利用可验证的(t,n)门限秘密共享方案[17]，提出了一种新的私钥共享方案，降低了基于身份的加密方案中秘密泄露的风险，避免了权利过度集中的问题。

下面简单对比了一下 PKI 和 IBE，结论[18~21]如表 1 所示。

可以看出，应用 PKI 时需要为用户发放公钥证书，需要保存和更新公钥证书列表，并且建立 CA 认证机构的成本和复杂性也较高。这些不足就影响了 PKI 在电子政务中的应用。所以本文引入了基于身份的认证加密方案[10]，并结合一种新的私钥共享方案，将 IBE 更好地应用在电子政务系统中。

表 1 PKI 和 IBE 的对比

比较次	PKI	IBE
私钥生成	分散式(由用户或 CA 生成)	集中式(由 PKG 生成)
密钥证书	有	无
密钥分发	公钥保存在证书中，证书采用静态分发、动态管理	密钥采用动态分发、动态管理
公钥获取方式	依赖证书，从公共目录或密钥持有者中获取，证书库在线运行	不需要证书，基于持有者的身份动态获取
私钥保存方式	不需要由 CA 保管(除非由 CA 生成的)，由用户自己的载体保存	由 PKG 保存
公钥保存方式	包含用户公钥的证书存放在公共的、在线运行的一个目录中	密钥托管中心
公钥的产生	公钥和私钥同时产生，由 CA 或用户自己产生	公钥先于私钥产生，由系统的任何用户生成
用户身份信息的获取方式	用户的身份信息要和证书绑定，在验证了签名之后才能确认用户的身份	表示用户身份的信息是公开的，可以直接得到

收稿日期：2013-06-13；**修回日期**：2013-07-26 **基金项目**：国家自然科学基金资助项目(60972139)

作者简介：封化民(1963-)，男，陕西富平人，教授，博士，主要研究方向为信息安全、多媒体智能信息处理；孙轶茹(1987-)，女，内蒙古人，硕士研究生，主要研究方向为基于身份的加密方案及其应用(xiaoxiaoqq_1987@126.com)；孙莹(1982-)，女，中级助理研究员，博士，主要研究方向为密码科研.

1 基于身份的认证加密方案

定义 1[11~16] 给出两个素数 q 阶的加法循环点群 G 和乘法循环点群 G_1。然后称一个映射 $e: G \times G \to G_1$ 为双线性的，如果对于所有的 $g, h \in G$ 和 $a, b \in F_q$，有 $e(g^a, h^b) = e(g,h)^{ab}$，$e(ag, h) = e(g,h)^a = e(g, ah)$。

定义 2 BDH 问题[11~16]。对于一个双线性映射 $e: G \times G \to G_1$，$|G| = |G_1| = q$ 是素数。定义如下：给出 $g, g^a, g^b, g^c \in G$，计算 $e(g,g)^{abc}$，g 是生成元，a、b、c 是从 F_q 中随机选取的。若一个算法以 ε 的优势解决了 BDH 问题，如果有

$$\Pr[A(g, g^a, g^b, g^c) = e(g,g)^{abc}] \geqslant \varepsilon$$

一个基于身份的加密方案[11~16]是由以下四个算法组成，即 setup、extract、encrypt 和 decrypt。总的来说，setup 产生公开分布式系统参数和一个主密钥，extract 产生一个对应于给定原始 ID 的私钥，encrypt 用这个给定的 ID 加密一个消息，而 decrypt 用私钥解密这个密文。

本文把消息空间定义为 $M = \{0,1\}^*$，除非另有说明。需要这些算法满足标准的一致性约束，定义当给定 ID 时 d 是由算法 extract 产生的私钥，A 是公钥，然后

$$\forall M \in M: \text{decrypt}(\text{param}, A, C, d) = M$$

这里，$C = \text{encrypt}(\text{param}, A, M)$。

带认证—加密：输入一个消息，一个（发送者的）私钥，一个（接收者的）ID，输出一个密文。

带认证—解密：输入一个密文，一个（发送者的）ID，一个（接收者的）私钥，输出对应的明文。

要求这两个算法满足标准的一致性约束条件。另外，对于所有的消息 M 和两个 ID_A 和 ID_B 对应的私钥 d_A、d_B，要求

$$\text{authenticated} - \text{encrypt}(M, d_A, \text{ID}_B) = \text{authenticaated-decrypt}(M, \text{ID}_A, d_B)$$

具体方案如下：由 setup、extract、authenticated-encrypt 和 authenticated-decrypt 四部分组成。

1）Setup 输入 $k \in Z$。运行 BDH 参数生成器，在 k 多项式时间内输出两个群 G、G_1 和双线性映射 $e: G \times G \to G_1$ 的说明，$|G| = |G_1| = q$ 是素数。选择一个随机的 $a \in F_q$ 和一个随机的 $g \in G$。挑选加密哈希函数（对于某些 n）：

$$H_1: F_q \times G_1 \to \{0,1\}^n, H_2: \{0,1\}^* \to G$$

$$H_3: \{0,1\}^* \times \{0,1\}^* \to F_q, H_4: \{0,1\}^n \to \{0,1\}^n$$

对于安全性证明，本文将哈希函数看做是随机预言模型。

输出：主密钥 a 和参数

$$\text{param} = \langle e, G, G_1, g, g^a, H_1, H_2, H_3, H_4 \rangle$$

2）Extract 输入一个 ID_A，输出 $d_A = H_2(\text{ID}_A)^a$。

假设有一个语义安全的对称密码体制。用 E_k、D_k 来表示密钥 K 的加密和解密函数，并假设密钥空间 $k \in \{0,1\}^*$。

3）Authenticated-encrypt 输入一个消息 $M \in \{0,1\}^*$，一个私钥 d_A，一个 ID_B 和系统参数 params。选择一个随机 $\sigma \leftarrow \{0,1\}^n$，计算 $r = H_3(\sigma, M)$ 和 $s = e(d_A, H_2(\text{ID}_B))$ 然后输出密文

$$C = \langle r, \sigma \oplus H_1(r,s), E_{H_4(\sigma)}(M) \rangle$$

4）Authenticated-decrypt 输入一个密文 $\langle U, V, W \rangle$，一个 ID_A，一个私钥 d_B。计算

$$s = e(H_2(\text{ID}_A), d_B), \sigma = V \oplus H_1(U,s), M = D_{H_4(\sigma)}(W)$$

检查 $U = H_3(\sigma, M)$ 是否相等。如果不相等，拒绝密文，否则输出明文 M。

一致性是明确的，因为 $e(d_A, H_2(\text{ID}_B)) = e(H_2(\text{ID}_A), H_2(\text{ID}_B))^a = e(H_2(\text{ID}_A), d_B)$ 的双线性。

基于身份的认证加密方案在加密时因为少了一个幂次且没有点乘，所以加密的速度比普通的加密要快，但是同样存在密钥托管问题，也有泄密的风险，因此本文利用可验证的 (t,n) 门限秘密共享方案[17]，提出了一种新的私钥共享方案，降低了基于身份的加密方案中秘密泄露的风险，避免了权利过度集中的问题。下面介绍这种新的私钥共享方案。

2 私钥共享方案

2.1 私钥分发

将私钥 d_A 按如下步骤分发给 $\{K_1, K_2, \cdots, K_n\}$ 这 n 个可信中心：

a）用户 A 随机选取一个数 $S_{\text{ID}} \in Z_q^*$，计算 $P = g^{S_{\text{ID}}}$，$Q = H_2(\text{ID}_A)^{S_{\text{ID}}} \cdot d_A$。并广播 $\langle P, Q \rangle$。

b）n 个可信中心可以验证等式 $e(H_2(\text{ID}_A), P_{\text{PKG}} \cdot P) = e(Q, g)$ 是否成立。

因为

$$e(H_2(\text{ID}_A), P_{\text{PKG}} \cdot P) = e(H_2(\text{ID}_A), g^a \cdot g^{S_{\text{ID}}}) =$$

$$e(H_2(\text{ID}_A), g^{a + S_{\text{ID}}}) = e(H_2(\text{ID}_A)^{a + S_{\text{ID}}}, g) =$$

$$e(H_2(\text{ID}_A)^a \cdot H_2(\text{ID}_A)^{S_{\text{ID}}}, g) =$$

$$e(H_2(\text{ID}_A)^{S_{\text{ID}}} \cdot d_A, g) = e(Q, g)$$

若等式成立，则 P、Q 是合法的。

c）用户 A 用可验证的 (t,n) 门限秘密共享方案[17]来共享 $S_{\text{ID}} \in Z_q^*$ 给 n 个可信中心。

（a）选取一个随机的 $t-1$ 次多项式 $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$，使得 $a_0 = S_{\text{ID}}$。其他的系数 $a_1, a_2, \cdots, a_{t-1}$ 是在 Z_q^* 中随机选取的。接着广播 $\langle g^{a0}, g^{a1}, \cdots, g^{a_{t-1}} \rangle$，其中 $g^{a0} = g^{S_{\text{ID}}} = P$。

（b）用户 A 为每一个可信中心秘密地发送其部分私钥 $S_{\text{ID}_i} = f(i) \bmod q$，每个私钥都可以通过等式 $g^{S_{\text{ID}_i}} = g_j^{\sum_{j=0}^{t-1} a_j \cdot ij}$ 进行验证。

例如，取 $i = h, 0 \leqslant h \leqslant t-1$：

$$S_{\text{ID}_h} = f(h) \bmod q = a_0 + a_1 h + a_2 h^2 + \cdots + a_{t-1} h^{t-1} \bmod q$$

$$g^{S_{\text{ID}_h}} =$$

$$g^{a_0 + a_1 h + a_2 h^2 + \cdots + a_{t-1} h^{t-1}} = g_{j=0}^{\sum_{j=0}^{t-1} a_j \cdot hj}$$

d）任何 t 个部分私钥 $S_{\text{ID}_{i_1}}, S_{\text{ID}_{i_2}}, \cdots, S_{\text{ID}_{i_t}}$ 可按如下步骤恢复私钥 d_A。

（a）利用拉格朗日公式恢复临时私钥 S_{ID}：

$$S_{\text{ID}} = \sum_{j=1}^{t} \frac{\prod_{k \neq j, k=1}^{t} i_k}{\prod_{k \neq j, k=1}^{t} (i_k - i_j)} \cdot f(i_j) \bmod q$$

（b）再计算 $d_A = H_2(\text{ID}_A)^{-S_{\text{ID}}} \cdot Q$，恢复私钥 d_A。

结合基于身份的加密方案和门限密码体制，可以有效地解决基于身份加密方案中的密钥托管问题。但是现有的解决方案都借助双线性对，把秘密共享方案应用到基于身份的门限秘密共享方案中，就使得在基于身份的门限秘密共享方案的各个环节中出现大量的双线性对的计算。目前没有快捷有效的计算双线性对的方法，所以基于身份的门限秘密共享方案的效率

相对于基于 PKI 的门限密码方案没有提高。

本文的私钥共享方案结合了可验证的(t,n)门限秘密共享方案[17],将用户私钥的共享问题转换为整数的秘密共享问题,减少了很多的双线对计算。

2.2　私钥共享

私钥共享方案思路总结如下:

a)先由用户随机产生一个随机数作为临时私钥 S_{ID};

b)再将 S_{ID}用可验证的(t,n)门限秘密共享方案分发给 n 个可信中心;

c)需要恢复用户私钥 d_A 时,仅需恢复临时私钥 S_{ID},通过计算 $S_{\mathrm{ID}}=\sum_{j=1}^{t}\frac{\prod_{k\neq j,k=1}^{t} i_k}{\prod_{k\neq j,k=1}^{t}(i_k-i_j)}\cdot f(i_j)\bmod q$ 可得;

d)进而通过计算 $H_2(\mathrm{ID}_A)^{-S_{\mathrm{ID}}}\cdot Q$,可得私钥 d_A。

在文献[17]中给出了整数秘密共享方案的安全性证明,显然可以得出本文私钥共享方案的安全性。

下面对该私钥共享方案计算量进行分析,结果如表 2 所示。

表 2　本文私钥共享方案计算量分析

操作	私钥分发	部分私钥验证	私钥恢复
双线性对 e 运算	0	2	0
hash 运算	1	1	1
Lagrange 插值	0	0	1
模指数运算	t	t	t

将本文的私钥共享方案与已有的一些方案进行了对比,从私钥分发阶段、部分私钥验证阶段、私钥恢复阶段几个主要方面进行了比较分析。比较的运算包括双线性对运算 E、模指数运算 S 和 Lagrange 插值 L,其他运算由于运算量较小,在此不予考虑。结果如表 3 所示。

表 3　本文私钥共享方案与已有几个方案的比较

方案	私钥分发阶段	部分私钥验证阶段	私钥恢复阶段
Yu-Kong 方案[22]	$(4n+2t+1)S$	$(2n+t+2)S$	$2nS+1L$
文献[23]方案	$(3n+t)E$	$2E+(t+1)S$	$tE+(t-1)S+1L$
Dehkordi-MH 方案[24]	$3nS$	tS	$(n-t)S+1L$
本文方案	tS	$2E+tS$	$tS+1L$

3　基于身份认证加密电子公文安全快速交换模型

基于身份的认证加密方案在加密的时候少了一个幂次且没有点乘,所以加密的速度比普通的加密要快,同时本文的私钥共享方案结合了可验证的(t,n)门限秘密共享方案,提出了一种新的私钥共享方案,将用户私钥的共享问题转换为整数的秘密共享问题,减少了很多的双线性对计算。

下面将基于身份的认证加密方案应用在电子公文安全交换中,如图 1 所示。

PKG 运行基于身份加密方案初始化算法,随机的 $a\in F_q$ 为主密钥,公开

$$\mathrm{params}=\langle e,G,G_1,g,g^a,H_1,H_2,H_3,H_4\rangle$$

发送者 A 的身份为 ID_A,先向管理模块提交发送申请,发送者从电子公文信息交换中心得到接收者 B 的身份 ID_B,用随机生成的 $\sigma\leftarrow\{0,1\}^n$ 和对称加密函数 E_k 加密要发送的电子公文 $M\rightarrow E_{H_4(\sigma)}(M)$;然后用公钥加密对称密钥,组合成密文 $C=\langle r,\sigma\oplus H_1(r,s),E_{H_4(\sigma)}(M)\rangle$ 发送文件,保证了文件内容的安全性。

发送者 A 将要发送的加密文件和发送申请一起发给所属内部系统的管理模块,得到许可后,由所属内部系统在加密文件中加入该系统的数据签名。通过数字签名和管理模块的过程控制,保证了发送者 A 身份的认证和发送的不可抵赖性;

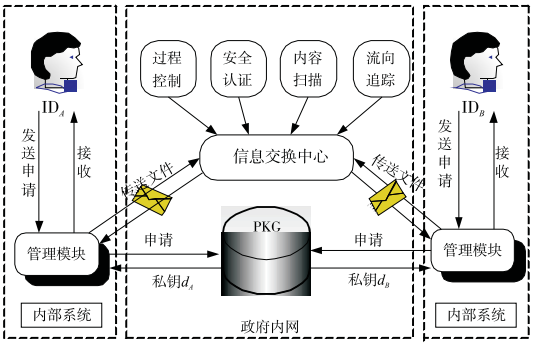

图1　基于身份的认证加密的电子公文安全快速交换模型

加密的电子公文 C 传送至信息交换中心,然后通过 PKG 对该签名进行确认,同时根据 C 和私钥 d_A,对电子公文传送过程进行流向跟踪,并根据实际需要对要传送的电子公文内容进行扫描,在确定无误之后传送到接收者 B 方面。

电子公文接收者 B 所在内部系统接收到加密的文件之后,通过数字签名对发送者 A 所在的系统进行身份认证,认证后可记录该加密文件的基本信息,转发给接收者 B,同时发送回执给信息交换中心。接收者 B 用身份 ID_B 向 PKG 申请私钥 d_B,通过计算 $s=e(H_2(\mathrm{ID}_A),d_B)$,$\sigma=V\oplus H_1(U,s)$,$M=D_{H_4(\sigma)}(W)$,检查 $U=H_3(\sigma,M)$。如果不相等,拒绝密文,否则输出明文 M。然后进入所在内部系统开始办理电子公文的相关业务。

在内部系统中,用户 A 和 B 的私钥应用本文提出的私钥共享方案分享给 n 个可信中心进行托管,有效地解决了密钥托管的问题,最重要的是托管的只是临时私钥,真正的私钥是不易被 n 个可信中心中的多个共谋攻击得到的,所以安全性是有保证的。

4　安全性分析

该模型建立在政府内网和相关内部系统中,与外网之间有一定的物理隔离,使得该模型运行环境的安全性比较高。所应用的基于身份的认证加密方案中,用于生成发送者和接收者的私钥的 PKG 设立在信息交换中心上,更易于管理和监控。

在文献[10]中,已经给出基于身份的认证加密方案完整性和安全性的证明。结论如下:

定理 1　假设 A 是一个多项式时间有界的攻击者能够以 ε 的优势伪造密文并且最多可进行 QH_2 查询和 Q_D 解密查询。然后存在一个多项式时间有界的算法 B 以至少 $\varepsilon/Q_D\binom{Q}{2}^2$ 的优势解决 BDH 问题。

定理 2　假设 A 是一个多项式时间有界的 AID-CCA 攻击者,优势是 ε。H_2 查询的数量是由 Q 界定的,H_1 查询的数量是由 Q_1 界定。而且,假设本文方案是密文不可伪造的。然后存在一个多项式时间有界的算法 B 以至少 $\frac{\varepsilon}{Q_1}\binom{Q}{2}^2$ 的优势解决 BDH 问题。

所以该 IBE 方案的安全性和身份认证仅用到了 BDH 假设和随机预言模型,在随机预言机模型下可以抵抗适应性选择密文攻击。

5 结束语

根据以上的分析可知,基于身份的认证加密方案是安全的,所以该政府内网中的电子公文交换模型在发送者加密、接收者解密、私钥分发等方面均保证了完整性和安全性。并且该 IBE 方案的加密速度比一般的 IBE 加密要快,就保证了电子公文传送的效率。同时提出了一种新的私钥共享方案,解决了 IBE 方案的密钥托管问题。通过对比分析可知,该私钥共享方案效率和安全性都较高,使得该系统应用更方便。

参考文献:

[1] 官盱玲. 电子公文应用的不安全因素及对策[J]. 江西行政学院学报,2004,6(4):84-86.

[2] 陈晓辉. 电子公文:能走多远——我国电子公文档案管理五大问题剖析[J]. 档案与建设,2012(8):10-13.

[3] 张晓芳. 电子公文系统的安全性研究[J]. 数字技术与应用,2013(2):175.

[4] 丁惠春. PKI 及其在电子政务中的应用研究[D]. 西安:西北工业大学,2005.

[5] 苏锐丹. 电子政务安全工程若干关键技术研究[D]. 西安: 西安电子科技大学,2010.

[6] 姜岚, 王宏滨. PKI/CA 技术在电子政务中的应用[J]. 黑龙江科技信息,2010(12):68- 69.

[7] 蔡谊, 沈昌祥. PKI 技术在电子政务中的应用[J]. 计算机应用研究,2002,19(10):11-13,16.

[8] 程程. PKI 技术在电子政务中的应用研究[D]. 重庆:重庆大学,2004.

[9] 杨硕,周乐,陈茂兴. PKI 技术及其在电子政务中的应用[J]. 电子科技大学学报:社科版,2007,9(4):35-54.

[10] LYNN B. Authenticated ID-based encryption cryptology, ePrint Archive Report 2002/072[R]. 2002.

[11] 徐丽娟. 基于身份密码体制的研究及应用[D]. 济南:山东大学,2007.

[12] 王璐. 身份密码的密钥管理研究[D]. 武汉:华中科技大学,2011.

[13] 胡亮,刘哲理,孙涛,等. 基于身份密码学的安全性研究综述[J]. 计算机研究与发展,2009,46(9):1537-1548.

[14] 王皓. 基于身份密码体制的研究[D]. 济南:山东大学,2012.

[15] 刘学. 基于身份的密码体制密钥管理研究[D]. 济南:山东大学,2012.

[16] 龙宇, 徐贤, 陈克非. 两个降低 PKG 信任级的基于身份的门限密码体制[J]. 计算机研究与发展,2012,49(5):932-938.

[17] FELDMAN P. A practical scheme for non-interactive verifiable secret sharing[C]//Proc of FOCS'87. New York:ACM Press, 1987.

[18] 侍伟敏. PKI_IBE 关键技术的研究及应用[D]. 北京:北京邮电大学,2006.

[19] 滕曰, 王首道, 林宇, 等. PKI、IBE 、CPK 对比分析[J]. 科技信息:科学教研,2008(18):402- 403.

[20] 石艳荣,贺永强. PKI 和基于身份加密的比较[J]. 微计算机信息,2008(3):16-18.

[21] 杨斌. IBC 和 PKI 组合应用研究[D]. 郑州:解放军信息工程大学,2009.

[22] YU Jia, KONG Fan-yu, HAO Rong. Publicly verifiable secret sharing with enrollment ability[C]//Proc of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing. Washington DC: IEEE Computer Society,2007:194-199.

[23] 李大伟. 基于身份加密的秘密共享及其应用研究[D]. 南京:南京邮电大学, 2011.

[24] DEHKORDI M H, MASHHADI S. New efficient and practical verifiable multi-secret sharing schemes [J]. Information Sciences: an International Journal, 2008,178(9):2262-2274.

(上接第 1506 页)

[3] 沈昌祥,张焕国,王怀民,等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2):139-166.

[4] 虚拟化与云计算小组. 虚拟化与云计算[M]. 北京:电子工业出版社,2009.

[5] 武少杰. 云计算下虚拟环境安全的关键技术研究[D]. 郑州:解放军信息工程大学,2012.

[6] 程川. 一种基于 Xen 的信任虚拟机安全访问设计与实现[J]. 计算机与数字工程,2010,38(3):109-113.

[7] BERGER S, CACERES R, GOLDMAN K A ,*et al*. vTPM: virtualizing the trusted platform module[C]//Proc of the 15th USENIX Security Symposium. Berkeley:USENIX Association,2006.

[8] OPPILGER R,RYTZ R. Does trusted computing remedy computer security problems? [J]. IEEE Security & Privacy,2005,3(2):16-19.

[9] 张兴,黄强,沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.

[10] ZHANG Xin-wen, COVINGTON M J, CHEN Song-qing. *et al*. SecureBus:towards application-transparent trusted computing with mandatory access control[C]// Proc of the 2nd ACM Symposium on Information, Computer and Communications Security. New York: ACM Press,2007:117-126.

[11] 张兴,陈幼雷,沈昌祥. 基于进程的无干扰可信模型[J]. 通信学报, 2009, 30(3): 6-11.

[12] 赵佳,沈昌祥,刘吉强,等. 基于无干扰理论的可信链模型[J]. 计算机研究与发展, 2008, 45(6): 974-980.

[13] 张兴,黄强,沈昌祥. 一种基于无干扰模型的信任链传递分析方法[J]. 计算机学报, 2010, 33(1): 74-81.

[14] 张帆, 陈曙, 桑永宣,等. 完整性条件下无干扰模型[J]. 通信学报, 2011,32(10):78-85.

[15] RUSHBY J. Noninterference, transitivity, and channel-control security policies,CSL-92-02[R]. [S. l.]:Computer Science Laboratory, SRI International, 1992.