抗合谋攻击的无可信中心门限签名方案①

王玲玲

(安徽工商职业学院 电子信息系, 合肥 230041)

摘 要: 现有的门限签名方案中, 合谋攻击一直是一个难以解决的问题. 针对王斌等人及王鑫等人所控方案的安全缺陷, 提出一种新方案. 为抗合谋攻击, 该方案综合使用三种方法: 采用无可信中心的模型, 从而彻底地消除可信中心“权威欺骗”的安全隐患, 使得安全级别更高; 采用添加随机数和时间戳的方法, 避免攻击者恢复签名成员的秘密参数, 同时防止中断协议攻击; 采用零知识证明的验证方法, 确认签名成员拥有正确的秘密参数, 避免攻击者直接伪造签名. 结果表明, 该方案是正确的, 能够抗伪造攻击和合谋攻击, 并具有匿名性和可追查性.

关键词: 合谋攻击; 伪造攻击; 无可信中心; 零知识证明; 可追查性

Threshold Signature Scheme Without a Trusted Party Resisting Conspiracy Attack

WANG Ling-Ling

(Electronic Information Department, Anhui Business Vocational College, Hefei 230041, China)

Abstract: In the existing threshold signature schemes, conspiracy attack is still a difficult problem to solved. To overcome the security weaknesses of Wang Bin’s work and Wang Xin’s work, a new scheme was proposed. In order to resist conspiracy attack, it utilized three ways: using model without a trusted part, it can eliminate authority cheating thoroughly and the security level was higher; adding random number and time stamp, it can prevent the attacker to recover the signer member’s secret parameters and also to prevent the attack of disrupting protocol; using zero-knowledge proof verifiable method to confirm that the signer member had right secret parameters, so it can prevent the attacker to forge signature directly. The results show that this scheme is correct, and it can not only resist forgery attack and conspiracy attack, but also provide anonymity and traceability simultaneously.

Key words: conspiracy attack; forgery attack; without a trusted party; zero-knowledge proof; traceability

门限签名是一种特殊的数字签名, 自提出以来得到广泛地发展, 它在保证电子数据的完整性、私有性和不可抵赖性等方面发挥着极其重要的作用. 但由于现有的门限签名都是基于 Shamir 门限体制设计的, 因此, 不能防止合谋攻击问题.

而实现抗合谋攻击, 意味着即使超过门限值的恶意成员合谋, 也不能恢复群私钥或伪造其它成员的签名. 因此, 不仅群私钥可以反复使用、不必担心泄露, 伪造签名也变得更加困难. 这对门限系统的效率和安全性都是有效地提高.

为此, 大量方案从抗合谋攻击的角度进行了研究[1-8], 按照秘密份额分发方式的不同, 可分为有可信中心[2,3,6,7]和无可信中心[1,4,5,8]两大类. 而能被所有成员认可的可信中心在现实中很难成立, 且可信中心可能会有权威欺骗行为, 使得成员无法完成门限签名, 因此无可信中心的方案更有吸引力. 但伴随着每种抗合谋攻击方案[1,2,6]的出现, 都会产生相应的攻击方法[3,4,7], 使得这些方案失去抗合谋攻击的作用. 因此, 尚未出现一个能为公共认可的抗合谋攻击方案.

本文重点对文献[5]和[8]的方案进行分析, 针对它们的安全缺陷, 给出相对应的伪造攻击方法, 并提出一个新的无可信中心方案, 能够抗合谋攻击, 分析表明其总体性能优于前两者.

① 收稿时间:2012-06-18;收到修改稿时间:2012-08-16

1 文献[5]和[8]方案的安全缺陷

1.1 共同的安全问题

(1) 在初始化阶段秘密发送参数, 存在信息被截获的安全隐患, 增加使用安全信道的费用.

(2) 在部分签名的生成阶段, 仅采用添加随机数的方法易受中断协议攻击[9].

1.2 文献[5]方案的安全缺陷

(1) 超过门限值的成员合谋, 能够恢复秘密多项式, 从而直接恢复群私钥, 因此不能抗合谋攻击.

(2) 哈希函数 H 仅包含消息 m, 不能抗文献[4]提出的内部和外部伪造攻击.

1.3 文献[8]方案的安全缺陷

(1) 在初始化阶段未提供对的验证功能, 无法防止恶意成员的欺骗.

(2) 不能抗合谋攻击. 假设超过门限值的恶意成员与被动签名合成者(DC)合谋, 则可成功地进行内部伪造攻击, 产生对违法消息的合法签名并通过验证, 且不需要负责. 具体步骤如下:

① 由于 U_i 的公钥仅对群 S 和 DC 公开, 且随着签名集合 S_t 变化, 需要在签名时重新发送给 DC, 因此可另选一个秘密随机数 k_i', 计算 $r_i'=g^{k_i'} \bmod p$ 并发送给 S_t 中其它成员, 将 $y_i'=g^{C_i\lambda_i+k_i'} \bmod p$ 作为公钥. 其余参数选择方法不变, 计算 $T_i=g^{t_i} \bmod p$, $T=\prod T_i \bmod p$, $r'=\prod r_i' \bmod p$, $s_i'=[(C_i\lambda_i+k_i')h(m',r')-t_iT] \bmod q$, 将 (m',s_i',y_i',T_i) 发送给 DC.

② 显然验证等式 $g^{s_i'}(T_i)^T=(y_i')^{h(m',r')} \bmod p$ 成立.

③ DC 计算 $s'=\sum s_i'$, 群签名 (m',s',r',T) 产生, 显然验证等式 $g^{s'}(T)^T=(y\times R^{-1}\times r')^{h(m',r')} \bmod p$ 成立.

$$\because s'=\sum s_i'=\sum[C_i\lambda_i h(m',r')+k_i'h(m',r')-t_iT] \bmod q$$
$$=[\sum F(0)h(m',r')+\sum k_i'h(m',r')-\sum t_iT] \bmod q$$
$$\therefore g^{s'}(T)^T=(y\times R^{-1})^{h(m',r')}(g^{\sum k_i'})^{h(m',r')} \bmod p$$
$$=(y\times R^{-1}\times r')^{h(m',r')} \bmod p$$

④ 当发生争议时, S_t 外的任何人都不能追查签名成员的身份, 因为在群内公布的任意 t 个成员的 r_i 乘积都不等于 r'.

2 新方案

2.1 初始化阶段

由所有成员选定公共参数: $N=pq$, p 和 q 是大素数, q 是 p-1 的素因子; g 和 h 是乘法群 Z_p^* 上阶为 q 的子群的生成元; $H(*)$ 是一个安全的单向哈希函数. $P=\{P_1,P_2,\cdots,P_n\}$ 是所有成员的集合, t 是门限值, $P_i\in P$ 有一个私钥 x_i 和对应的公钥 $y_i=g^{x_i} \bmod p$, 须满足条件: 任意 t 个成员的 y_i 之积 $y=\prod_{i\in w\wedge|w|=t,w\subset\{1,2,\cdots,n\}} y_i \bmod p$ 均不相等, 有一对整数 (e_i,d_i) 满足条件: $e_id_i=1 \bmod \phi(N)$, ϕ 是欧拉函数, 公布 y_i、e_i 和身份标志 ID_i.

成员通信模型: P 中每个成员都和一个公共信道连接, 该公共信道可以使得发送到它上的信息瞬时到达与其连接的每一方.

(1) $P_i\in P$ 首先选择 Z_q 中 t 个随机数, 定义 t-1 次多项式 $f_i(x)=a_{i0}+a_{i1}x+a_{i2}x^2+\cdots+a_{i,t-1}x^{t-1} \bmod q$. 然后计算 $A_{im}=h^{a_{im}} \bmod p, m\in\{0,1,\cdots,t-1\}$ 和 $\lambda_{ij}=f_i(ID_j) \bmod q$, 并用其它 n-1 个成员 P_j 的 e_j 加密 $E_{ij}=(\lambda_{ij})^{e_j} \bmod N$. 广播信息 $(ID_i,\{A_{im}\}_{m\in\{0,1,\cdots,t-1\}},\{E_{ij}\}_{j\in\{1,2,\cdots,n\}\setminus\{i\}})$.

(2) $P_i\in P$ 接收到信息后用 d_i 解密得 $E_{ji}^{d_i}=(\lambda_{ji})^{e_id_i} \bmod N=\lambda_{ji}$, 然后按照定理 1 进行验证. 计算秘密份额 $\lambda_i=\sum_{j=1}^{n}\lambda_{ji} \bmod q$, 并广播 $g^{\lambda_i} \bmod p$ 和 $h^{\lambda_i} \bmod p$.

(3) 定义 $F(x)=\sum_{i=1}^{n}[f_i(x)+x_i] \bmod q$. 当所有成员完成上述步骤后, 计算群公钥并广播: $Y=g^{F(0)} \bmod p$
$=\prod_{i=1}^{t}g^{\lambda_iL_i}\cdot\prod_{i=1}^{n}y_i \bmod p, L_i=\prod_{j=1,j\neq i}^{t}\frac{ID_j}{ID_j-ID_i}$.

2.2 部分签名的生成与验证阶段

假设成员集合 $U=\{P_1,P_2,\cdots,P_t\}\subset P$ 想对消息 m 签名, t_i 为当前系统时间.

(1) 签名成员 $P_i\in U$ 首先选择随机数 $b_i\in Z_p^*$, 计算并广播 $B_i=g^{b_i\|t_i} \bmod p$ 和 $D_i=h^{b_i\|t_i} \bmod p$. 然后计算 $T_i=H(g^{yx_i},h^{yx_i},m)$, $R_i=[yx_i-y\lambda_iL_i-(b_i\|t_i)T_i] \bmod q$, 其中 $y=\prod_{P_i\in U}y_i \bmod p$, $L_i=\prod_{P_j\in U,j\neq i}\frac{ID_j}{ID_j-ID_i}$. 将部分签名 (m,T_i,R_i,t_i,ID_i) 发送给 DC.

(2) DC 接收到 t 个部分签名后计算 $S_i=g^{\lambda_iL_i} \bmod p$ 和 $G_i=h^{\lambda_iL_i}$, 然后按照定理 3 和定理 4 进行验证.

2.3 门限签名的生成与验证阶段

当 t 个部分签名都通过验证后, DC 计算门限签名: $R=\sum_{P_i\in U}R_i \bmod q$, $T=\prod_{P_i\in U}B_i^{T_i} \bmod p$, $S=\prod_{P_i\in U}S_i \bmod p$, $y'=\prod_{P_i\notin U,P_i\in P}y_i \bmod p$.

任何签名接收者都可以按照定理 5 进行验证.

2.4 签名成员身份追查

当发生纠纷时, 群体要对一项失误的决策追究责任, 则群中任何成员都可以通过如下方法追查出生成某签名的 t 个成员的身份, 而群外的用户则无法知道签名的具体成员.

若某 t 个成员的公钥 y_i 满足如下跟踪方程(见 2.1 节):

$$y=\prod_{i\in w,|w|=t,w\subset\{1,2,\cdots,n\}} y_i \bmod p$$

则参加签名的成员即为这 t 个人.

3 方案分析

3.1 正确性分析

定理1. 若成员按照2.1节步骤产生参数, 则接收者能够验证方程 $h^{\lambda_{ji}}=\prod_{m=0}^{t-1}A_{jm}^{(ID_i)^m} \bmod p$ 成立.

证明: $h^{\lambda_{ji}}=h^{f_j(ID_i)\bmod q} \bmod p$

$$=h^{a_{j0}}\cdot(h^{a_{j1}})^{(ID_i)^2}\cdot\cdots\cdot(h^{a_{jt-1}})^{(ID_i)^{t-1}} \bmod p$$

$$=\prod_{m=0}^{t-1}A_{jm}^{(ID_i)^m} \bmod p$$

定理 2. 群公钥的计算是正确的.

证明: $Y=g^{F(0)} \bmod p=g^{\sum_{i=1}^{n}[f_i(0)+x_i]\bmod q} \bmod p$

$$\because \lambda_i=\sum_{j=1}^{n}f_j(ID_i)\bmod q=\sum_{j=1}^{n}\lambda_{ji}\bmod q$$

$$\therefore \sum_{i=1}^{n}f_i(0)\bmod q=\sum_{i=1}^{t}\lambda_i L_i \bmod q$$

$$\Rightarrow Y=g^{\sum_{i=1}^{t}\lambda_i L_i \bmod q}\cdot g^{\sum_{i=1}^{n}x_i \bmod q} \bmod p$$

$$=\prod_{i=1}^{t}g^{\lambda_i L_i}\cdot\prod_{i=1}^{n}y_i \bmod p, L_i=\prod_{j=1,j\neq i}^{t}\frac{ID_j}{ID_j-ID_i}$$

定理3. 若签名成员按照2.2节步骤产生部分签名, 则 DC 能够验证方程 $T_i=H(g^{R_i}S_i^y B_i^{T_i},h^{R_i}G_i^y D_i^{T_i},m)$ 成立.

证明: $\because R_i=[yx_i-y\lambda_i L_i-(b_i\|t_i)T_i]\bmod q$

$$\therefore yx_i=[R_i+y\lambda_i L_i+(b_i\|t_i)T_i]\bmod q$$

$$T_i=H(g^{yx_i},h^{yx_i},m)$$

$$=H(g^{R_i+y\lambda_i L_i+(b_i\|t_i)T_i},h^{R_i+y\lambda_i L_i+(b_i\|t_i)T_i},m)$$

$$=H(g^{R_i}S_i^y B_i^{T_i},h^{R_i}G_i^y D_i^{T_i},m)$$

定理 4. 若定理 3 成立, 则使用的零知识证明[10]是正确的, 签名成员向 DC 证明了它拥有正确的秘密份额、私钥和随机数, 同时不会泄露该信息.

证明: 假设签名成员在已知 α,g,β,h 且 $\alpha=g^s$ 的条件下, 向 DC 证明它知道 s, 其中 g 和 h 是生成元, 且以 g 为底 α 的离散对数等于以 h 为底 β 的离散对数, 即 $\beta=h^s$. 令 $T_i=H(g^r,h^r,m)$, $R_i=r-sT_i$.

(1) 若 (T_i,R_i) 有效, 显然有 $T_i=H(g^{R_i}\alpha^{T_i},h^{R_i}\beta^{T_i},m)$.

(2) 反之, 若 $T_i=H(g^{R_i}\alpha^{T_i},h^{R_i}\beta^{T_i},m)$, 令 $\chi=g^{R_i}\alpha^{T_i}$, $\delta=h^{R_i}\beta^{T_i}$, 由2.1节可知 Z_p^* 中任何一个元素可用生成元 g 的幂表示, 设整数 a,b,c,d 使得 $h=g^a$, $\beta=g^b$, $\chi=g^c$, $\delta=g^d$. 根据 χ,δ 的定义, 可得 $g^{R_i+sT_i}=g^c$, $g^{aR_i+bT_i}=g^d\Rightarrow R_i+sT_i=c\bmod q$, $aR_i+bT_i=d\bmod q\Rightarrow(as-b)T_i=(ac-d)\bmod q$, 又由于 T_i 是哈希函数得到的随机值, 所以 $(as-b)=0\bmod q$, 故 $\beta=g^b=g^{as}=h^s$, 由已知 $\alpha=g^s$, 说明 α 和 β 相对于底数 g 和 h 有共同的离散对数.

定理 5. 若 DC 按照 2.3 节步骤合成门限签名, 则签名接收者能够验证方程 $g^R(y')^y ST=Y^y \bmod p$ 成立.

证明: $R=[y(\sum_{P_i\in U}x_i-\sum_{P_i\in U}\lambda_i L_i)-\sum_{P_i\in U}(b_i\|t_i)T_i]=[y(\sum_{P_i\in U}x_i$

$$+\sum_{P_i\in U}\lambda_i L_i+\sum_{P_i\notin U,P_i\in P}x_i-\sum_{P_i\notin U,P_i\in P}x_i-2\sum_{P_i\in U}\lambda_i L_i)-\sum_{P_i\in U}(b_i\|t_i)T_i]$$

$$=[y(\sum_{P_i\in P}x_i+\sum_{P_i\in P}f_i(0)-\sum_{P_i\notin U,P_i\in P}x_i-2\sum_{P_i\in U}\lambda_i L_i)-\sum_{P_i\in U}(b_i\|t_i)T_i]$$

$$=[yF(0)-y\sum_{P_i\notin U,P_i\in P}x_i-2y\sum_{P_i\in U}\lambda_i L_i-\sum_{P_i\in U}(b_i\|t_i)T_i]\bmod q$$

$$\Rightarrow g^R(y')^y S^{2y}T=Y^y \bmod p$$

3.2 安全性分析

定理 6. 新方案抗中断协议攻击.

证明: Michels 和 Horster 已证实[9], 仅用添加随机数的方法易受中断协议攻击, 提出的改进思想是使用同步广播信道或对随机数进行零知识证明. 假设在 2.2 节, 攻击者执行中断协议攻击. 由于签名成员 P_i 计算的 B_i、D_i 和 R_i 中都添加了时间戳 t_i, 并进行了零知识证明(见定理 4), 使得签名具有时间性, 则已签名成员可以宣布: 在 t_i 时刻的签名作废失效, 从而使攻击者已拥有的签名失去利用的价值. 因此, 攻击者利用已有的签名进行伪造签名将变得更加困难, 中断协议攻击对新方案无效.

定理 7. 新方案抗内部和外部伪造攻击.

证明: 由于 $H(*)$是一个安全的单向哈希函数, g 和 h 是两个不同的生成元, 试图通过找到 $(g^{r'},h^{r'},m')$ 得到 $H(g^{r'},h^{r'},m')=H(g^r,h^r,m)$ 是不行的. 因此, 新方案抗文献[4]提出的内部和外部伪造攻击.

定理 8. 新方案抗篡改攻击.

证明: 假设在 2.2 节, 攻击者篡改签名成员 P_i 的广播参数 A_{im}、$g^{\lambda_i} \bmod p$ 、$h^{\lambda_i} \bmod p$ 、B_i 或 D_i, 试图阻止 DC 合成正确的门限签名. 由于使用了两个不同的生成元 g 和 h, 则 P_i 首先用 λ_i 判断 $g^{\lambda_i} \bmod p$ 和 $h^{\lambda_i} \bmod p$ 是否被篡改; 若 $g^{\lambda_i} \bmod p$ 和 $h^{\lambda_i} \bmod p$ 正确, 接着用定理 1 判断 A_{im} 是否被篡改, 若定理 1 不成立, 则认为 A_{im} 已被篡改; 若定理 1 成立, 接着用定理 3 和定理 4 判断 B_i 或 D_i 是否被篡改, 若不能通过零知识证明的验证, 则认为 B_i 或 D_i 已被篡改. 然后发送信息通知 DC 哪些参数被篡改, 那么在更正参数后, DC 就可以合成正确的门限签名. 因此, 篡改攻击对新方案无效.

定理 9. 新方案抗合谋攻击.

证明: 假设在 2.3 节, t 个以上恶意成员合谋, 试图伪造群 $U \subset P$ 对违法消息 m' 的门限签名. 它们首先利用 *Lagrange* 插值公式合作重构多项式 $\sum_{P_i \in P} f_i(x)$, 可得 $\sum_{P_i \in U} \lambda_i L_i$.然后选择随机数 b_i' 构造 $\sum_{P_i \in U} (b_i' \| t_i) T_i'$, 由定理 7 可知试图计算 $T_i' = T_i$ 是不行的, 由定理 6 可知添加时间戳 t_i 使伪造签名变得更加困难. 又由于不知道所有成员的私钥, 无法计算出 $\sum_{P_i \in P} x_i \bmod q$, 因此无法根据 $F(0) = \sum_{P_i \in P} [f_i(0) + x_i] \bmod q$ 恢复 $F(0)$. 由定理 5 可推出, 不知道 $F(0)$、$\sum_{P_i \notin U, P_i \in P} x_i \bmod q$ 和 T_i, 攻击者无法构造出合法的门限签名使其通过验证. 另外, 试图通过 $y' = \prod_{P_i \notin U, P_i \in P} y_i \bmod p = g^{\sum_{P_i \notin U, P_i \in P} x_i \bmod q} \bmod p$ 求出 $\sum_{P_i \notin U, P_i \in P} x_i \bmod q$ 必须面对离散对数问题. 因此, 即使有 t 个以上恶意成员合谋攻击, 对新方案仍然无效.

定理 10 新方案在保证匿名性的同时, 实现了签名成员身份的可追查性.

证明: 由于 2.4 节的跟踪方程是利用门限签名的必要参数 y 设计的, y 是参与门限签名的 t 个成员的公钥之积, 而群中任意 t 个成员的公钥之积均不相等(见 2.1 节), 因此每个门限签名都能唯一确定出 t 个成员的身份. 此外, 由于各成员的公钥仅在群内公开, 因此群外的用户(包括签名接收者)都不能从 y 中获得有关签名成员身份的任何信息.

3.3 性能分析

3 种方案的计算量比较详见表 1, 其中 T_{exp} 是模指数运算时间, T_{mul} 是模乘运算时间, T_{inv} 是模逆运算时间, T_h 是单向哈希函数运算时间, k 是门限签名次数, 模加/减运算的时间复杂度相当小, 可以忽略.

(1) 在初始化阶段, 新方案和文献[5]方案提供了对 λ_{ij} 的验证功能, 虽然增加了 $3t(n\text{-}1)T_{exp}+(t\text{-}1)(n\text{-}1)T_{mul}$ 运算量, 但由于可验证秘密共享是门限签名方案中最基本和十分重要的安全特性, 且不影响之后签名的效率, 因此增加相应的运算是值得的. 另外, 这两者较文献[8]方案减少了在每次签名时重新计算私钥和公钥的 $1T_{exp}+(t\text{-}2)T_{mul}+(t\text{-}1)T_{inv}$ 运算量.

(2) 在初始化阶段, 新方案提供了对 λ_{ij} 的加解密功能, 虽然增加了 $2(n\text{-}1)T_{exp}$ 运算量, 但能克服文献[5]和[8]方案中信息被截获的安全隐患, 减少使用安全信道的费用, 因此增加相应的运算是值得的.

(3) 在签名过程中, 虽然新方案使用的哈希函数运算加长（涉及的模指数和模乘运算单独计算）, 但可与部分签名的产生同步进行, 不会影响最终签名的效率, 且由于它能够有效克服前两者的安全缺陷, 安全性更高, 能够真正抗合谋攻击、伪造攻击和中断协议攻击, 因此增加相应的运算是值得的.

表 1

计算量	初始化阶段	部分签名生成与验证阶段	门限签名生成与验证阶段
文献[5]方案	$(3tn\text{-}3t+2)T_{exp}+(tn\text{-}t)T_{mul}$	$5T_{exp}+(6t\text{-}1)T_{mul}+(2t\text{-}2)T_{inv}+2T_h$	$3T_{exp}+3T_{mul}+T_h$
文献[8]方案	$(2+k)T_{exp}+[2t^2+(k\text{-}2)t+n+1\text{-}2k]T_{mul}+[t^2+(k\text{-}1)t\text{-}k]T_{inv}$	$4T_{exp}+(4t\text{-}1)T_{mul}+2T_h$	$3T_{exp}+3T_{mul}+T_{inv}+T_h$
本方案	$(3tn\text{-}2t+2n)T_{exp}+(tn)T_{mul}+(t\text{-}1)T_{inv}$	$12T_{exp}+(4t+2)T_{mul}+(2t\text{-}2)T_{inv}+2T_h$	$4T_{exp}+(n+t)T_{mul}$

因此, 新方案在安全性增强的前提下, 效率接近于文献[5]和[8]的方案, 其性能总体上优于这两者, 具有更好的应用前景.

4 结语

抗合谋攻击的门限签名是数字签名研究的热点, 有着广泛的应用前景. 本文在对文献[5]和[8]方案的安

(下转第 184 页)

减少，通过大量采用技术先进、结构简单、稳定可靠和免维护的系统设备，达到减少维修量、工作量和降低维修成本的目标；四是节能环保，通过采用远程异地存储的方式，减少了使用本地磁盘及移动存储设备的存储量；五是提升系统运营管理效率和水平，按照系统运营管理模式的改革目标配备先进可靠的技术设备，为实现新的系统实现方式及设备维修模式创造了良好条件.

通过一段时间的实际使用，本容灾备份方案很好地保证了数据的完整性和量传业务的连续性，并且具有很高的性价比和可扩充性，可以满足同类系统的容灾要求及业务要求.

参考文献

1 刘羿彤,李丽,张明.计量管理软件系统建设及其安全性分析.中国计量,2011,(3):103−104.

2 JL 002-2012, 计量院信息化总体建设技术规范——软件部分,2012.

3 Sysmantec .Sysmantec NetBackup 7.0 备份、存档和还原入门指南 http://entsupport.symantec.com 2011.

4 Sysmantec .Sysmantec NetBackup 7.0 SAN 客户端和光纤传输指南 http://entsupport.symantec.com 2011.

5 Sysmantec. Sysmantec NetBackup 7.0 故障排除指南. http://entsupport.symantec.com 2011.

6 GB/T 20988.2007, 信息安全技术信息系统灾难恢复规范 2007.

7 HP. HP D2D4106 Backup System Capacity Upgrade Kit. http://h10010.www1.hp.com/wwpc/uk/en/sm/WF06c/A1-329290-3320517-3329763-3329763-3741179-4350671.html,March 2010.

8 康剑斌,汪海山,贾惠波.基于磁带库的磁盘缓存策略.仪器仪表学报,2009,30(6):1281−1284.

9 王德军,王丽娜.容灾系统研究.计算机工程,2005,31(6):43−45.

10 张磊.虚拟磁带库在灾备系统中的应用研究.小型微型计算机系统,2007,28(6):1149−1152.

11 IBM. IBM International Techincal Support Organization. Disaster Recovery Strategies with Tivoli Storage Management www. redbooks.ibm.com/redbooks/pdfs/sg 246844.pdf 2002.

(上接第 207 页)

全缺陷的分析基础上，提出一个新方案. 该方案无可信中心，具有更高的安全性；既可以有效避免中断协议攻击、篡改攻击、伪造攻击、合谋攻击等多种攻击，又可以在保证匿名性的同时，实现可追查性.

参考文献

1 王斌,李建华.无可信中心的(t,n)门限签名方案.计算机学报,2003,26(11):1581−1584.

2 Gan YJ. Verifiable threshold signature schemes against conspiracy attack. Journal of Zhejiang University Science, 2004, 5(1):50−54.

3 Xie Q. Cryptanalysis and improvement of two threshold signature schemes. Journal on Communications, 2005,26(7):123−128.

4 郭丽峰,程相国.一个无可信中心的(t,n)门限签名方案的安全性分析.计算机学报,2006,29(11):2013−2016.

5 张文芳,何大可,王宏霞,等.具有可追查性的抗合谋攻击(t,n)门限签名方案.西南交通大学学报,2007,42(4):461−467.

6 张有谊,乜国雷,郑东.一种可防止合谋攻击的门限签名方案.计算机应用与软件,2008,25(12):51−52.

7 徐光宝,姜东焕.抗合谋攻击的门限签名方案分析与改进.计算机工程,2010,36(20):155−156.

8 王鑫,张少武.无可信中心的门限签名方案的分析和改进.计算机工程与应用,2011,47(29):93−95.

9 Michels M, Horster P. On the risk of disruption in several multiparty signature schemes. Proceeding of Advances in Cryptology-ASIACrypt'96. Berlin: Springer, 1996:334−345.

10 Fouque PA, Poupard G, Stern J. Sharing decryption in the context of voting or lotteries. Proceeding of Financial Cryptography 2000.Berlin:Springer,2000:90−104.