文章编号:1001 - 9081(2011)01 - 0127 - 02 doi:10.3724/SP. J. 1087. 2011. 00127

基于身份的双向门限代理重签名方案

张玉磊,杨小东,王彩芬
(西北师范大学 数学与信息科学学院, 兰州 730070)
(zylei79@163.com)

摘 要:基于 Shao 等人提出的基于身份的代理重签名方案,构造了一种标准模型下可证安全的基于身份的双向门限代理重签名方案,避免了传统公钥证书所带来的存储和管理开销问题,解决了代理重签名方案中代理者权利过大的难题。方案能容忍 $t < n/2$ 个代理者被恶意攻击者攻陷,在计算 Diffie-Hellman(CDH)问题假设下,方案是健壮的,对适应性选择身份和消息攻击是不可伪造的。

关键词:门限代理重签名;基于身份;可证安全;标准模型
中图分类号: TP393 **文献标志码**:A

ID-based bidirectional threshold proxy re-signature

ZHANG Yu-lei, YANG Xiao-dong, WANG Cai-fen
(*College of Mathematics and Information Science, Northwest Normal University, Lanzhou Gansu* 730070, *China*)

Abstract: Based on Shao et al' s ID-based proxy re-signature, an ID-based bidirectional threshold proxy re-signature scheme in the standard model was presented in this paper. The scheme eliminated the cost of restoring and managing certificates, and solved the difficult problem of excessive rights of the proxy in the proxy re-signature scheme. The scheme can tolerate $t < n/2$ malicious proxies. This scheme proves to be robust and secure against the existential forgery under the adaptive chosen identity and message attacks, under the computation Diffie-Hellman assumption.

Key words: threshold proxy re-signature; identity-based; provably secure; standard model

0 引言

代理重签名中[1],一个拥有重签名密钥的半可信代理者可以把受托者的签名转换为委托者对同一消息的签名(即重签名),但代理者不能单独生成受托者或委托者的签名。代理重签名在简化证书管理、管理群签名、提供遍历的路径证明、构造数字版权管理系统等方面有广泛的应用前景[2]。然而,一旦重签名密钥泄露,代理重签名的安全性便遭到破坏。

门限代理重签名[3]不仅能防止代理者签名权利过分集中而被滥用,还可保证重签名密钥的安全性和完整性。一个 (t, n) 门限代理重签名可将重签名密钥分成个 n 个子密钥,然后分发给 n 个代理者持有,至少需要 t 个诚实的代理者合作才能产生正确的重签名。即使 $t-1$ 个(或更少)重签名子密钥被泄露,门限代理重签名方案仍是安全的。

Canetti 等人[4]指出,在随机预言模型下可证安全的密码体制,当具体的哈希函数取代随机预言机时,所得方案不一定是安全的。所以,研究标准模型下可证安全的门限代理重签名显得更有吸引力。基于 Shao 等人[5]提出的基于身份的代理重签名方案 $S_{id\text{-}mb}$ 基础上,提出了一个标准模型下可证安全的基于身份的双向门限代理重签名方案,并在标准模型下证明方案是健壮的,能容忍 $t < n/2$ 个代理者被恶意攻击者攻陷,对适应性选择身份和消息攻击是不可伪造的。

1 预备知识

1.1 双线性对

设 G_1 和 G_2 是两个阶为素数 p 的循环群,g 是 G_1 的生成元,定义两个群 G_1 和 G_2 上的双线性映射 $e: G_1 \times G_1 \to G_2$,且满足以下性质。

1)双线性:对任意的 $a, b \in Z_p$,有 $e(g^a, g^b) = e(g, g)^{ab}$。

2)非退化性:$e(g, g)$ 不等于 G_2 的单位元。

3)可计算性:对任意的 $g_1, g_2 \in G_1$,存在一个高效的算法计算 $e(g_1, g_2)$。

1.2 复杂性假设

计算性 Diffie-Hellman(CDH)问题:设 G 是阶为素数 p 的循环群,g 是 G 的生成元,则群 G 上的 CDH 问题是:已知 $g, g^a, g^b \in G$,其中 a, b 是从 Z_p 中随机选取的,计算 g^{ab}。

如果没有一个概率多项式时间算法在时间 t 内以至少 ε 的概率解决群 G 上的 CDH 问题,则称群 G 上的 (t, ε) -CDH 假设成立[6]。

2 基于身份的双向门限代理重签名方案

方案涉及到四方:受托者、委托者、n 个半可信的代理者组成的签名者集合 $P = \{P_1, P_2, \cdots, P_n\}$ 和密钥生成中心 PKG。该方案是双向、透明、多用和密钥最优的。为了使方案更加灵活,对于不同长度的用户身份和签名消息比特串,利用两个抗碰撞的哈希函数 $H_1: \{0,1\}^* \to \{0,1\}^{n_{id}}$ 和 $H_2: \{0,1\}^* \to \{0,1\}^{n_m}$ 分别进行处理,将所有的用户身份和签名消息的长度映射到方案所要求的 n_{id} 和 n_m 比特长。

方案由以下 7 个算法组成。

1)Setup:输入一个安全参数 1^k,选择两个阶为素数 p 的循环群 G_1 和 G_2,g 和 h 是 G_1 的生成元,定义 $e: G_1 \times G_1 \to G_2$ 是一个双线性映射。在 G_1 中随机选取 $n_{id}+1$ 个元素 $(v, v_1, \cdots,$

收稿日期:2010 - 07 - 12;**修回日期**:2010 - 09 - 16。 **基金项目**:教育部科学技术研究重点项目(208148);甘肃省教育厅重点项目(0801-01);甘肃省自然科学基金资助项目(096RJZA124);西北师范大学青年教师科研基金资助项目(NWNU-LKQN-09-5)。

作者简介:张玉磊(1979 -),男,讲师,硕士,CCF 会员,主要研究方向:信息安全; 杨小东(1981 -),男,甘肃甘谷人,讲师,博士,主要研究方向:密码学、信息安全; 王彩芬(1963 -),女,河北安国人,教授,博士生导师,博士,主要研究方向:密码学、电子商务协议的设计与分析。

$v_{n_{id}}$) 和 n_m+1 个元素 $(u,u_1,\cdots,u_{n_m})$。另外,任选一个随机数 $\alpha\in Z_p^*$,计算密钥生成中心 PKG 的公钥 $g_1=g^\alpha$,公开系统参数 $params=(G_1,G_2,p,e,g,h,g_1,v,v_1,\cdots,v_{n_{id}},u,u_1,\cdots,u_{n_m})$,保密 PKG 的主密钥 $mk=\alpha$。

2)Extract:输入一个 n_{id} 比特长的身份 $ID=(ID_1,ID_2,\cdots,ID_{n_{id}})\in\{0,1\}^{n_{id}}$,PKG 选取 $s_{ID}\in_R Z_p^*$,计算 $J(ID)=v\prod_{i=1}^{n_{id}}v_i^{ID_i}$,输出对应的私钥 $sk_{ID}=(sk_{ID}^{(1)},sk_{ID}^{(2)})=(h^\alpha J(ID)^{s_{ID}},g^{s_{ID}})$。

3)ShareRekey:输入两个私钥 $sk_A=(h^\alpha J(ID_A)^{s_A},g^{s_A})$ 和 $sk_B=(h^\alpha J(ID_B)^{s_B},g^{s_B})$,PKG 操作如下:

① 在 Z_p^* 中选取 $t-1$ 个随机数 $a_1,a_2,\cdots,a_{t-1}$,构造一个 $t-1$ 次秘密多项式 $f(x)=\sum_{i=0}^{t-1}a_ix^i$,使得 $a_0=\alpha$。计算 $\alpha_i=f(i)\pmod p$,$i=1,2,\cdots,n$。

② 在 Z_p^* 中选取 $t-1$ 个随机数 $b_1,b_2,\cdots,b_{t-1}$,构造一个 $t-1$ 次秘密多项式 $g(x)=\sum_{i=0}^{t-1}b_ix^i$,使得 $b_0=s_B$。计算 $s_i=g(i)\pmod p$,$i=1,2,\cdots,n$。

③ 计算重签名子密钥 $rk_{A\to B}^i=(rk_{A\to B}^{i,1},rk_{A\to B}^{i,2})=\left(\frac{h^{\alpha_i}J(ID_B)^{s_i}}{h^\alpha J(ID_A)^{s_A}},g^{s_i}\right)$ 和验证公钥 $vk_i=g^{\alpha_i}$,通过一个秘密渠道将 $(i,rk_{A\to B}^i)$ 分发给代理者 P_i,$i=1,2,\cdots,n$。

④ 广播 g^{s_A} 和 $A_j=g^{b_j}$,$j=0,1,\cdots,t-1$,其中 $A_0=g^{s_B}$。公开验证公钥 $vk_1,vk_2,\cdots,vk_n$。

⑤ 每个代理者 $P_i(1\leqslant i\leqslant n)$ 收到重签名子密钥 $rk_{A\to B}^i=(rk_{A\to B}^{i,1},rk_{A\to B}^{i,2})$ 后,通过下式验证合法性:

$$\begin{cases}rk_{A\to B}^{i,2}=\prod_{j=0}^{t-1}(A_j)^{ij}\\ e(rk_{A\to B}^{i,1},g)=e(h,vk_i)e(h,g_1)^{-1}\\ \qquad\qquad e(J(ID_A),g^{s_A})^{-1}e(J(ID_B),rk_{A\to B}^{i,2})\end{cases}$$

如果等式都成立,说明 $rk_{A\to B}^i$ 是合法有效的。

4)Sign:输入一个 n_m 比特长的消息 $m=(m_1,m_2,\cdots,m_{n_m})\in\{0,1\}^{n_m}$ 和一个私钥 $sk_{ID}=(sk_{ID}^{(1)},sk_{ID}^{(2)})$,选取 $r_m\in_R Z_p^*$,计算 $\varpi=u\prod_{i=1}^{n_m}u_i^{m_i}$,输出签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)=(sk_{ID}^{(1)}\varpi^{r_m},sk_{ID}^{(2)},g^{r_m})$。可用对应的 ID 来验证签名 σ 的合法性。

5)ShareResign:输入一个重签名子密钥 $rk_{A\to B}^i=(rk_{A\to B}^{i,1},rk_{A\to B}^{i,2})$,一个 n_{id} 比特长的身份 ID_A,一个 n_m 比特长的消息 m 和一个签名 $\sigma_A=(\sigma_{A,1},\sigma_{A,2},\sigma_{A,3})$,如果 Verify $(ID_A,m,\sigma_A)=0$,输出 $\perp$;否则,选取一个随机数 $r_i\in Z_p$,计算一个对应于身份 ID_B 的消息 m 的部分重签名:

$$\sigma_{B,i}=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})=(\sigma_{A,1}\cdot rk_{A\to B}^{i,1}\cdot\varpi^{r_i},rk_{A\to B}^{i,2},\sigma_{A,3}\cdot g^{r_i})$$

6)Combine:假定 D 是一个指定的部分重签名的合成者(可以是任意一个代理者)。D 收到部分重签名 $\sigma_{B,i}=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})$ 后,通过下式验证其合法性:

$$e(\sigma_{i,1},g)=e(h,vk_i)e(J(ID_B),\sigma_{i,2})e(\varpi,\sigma_{i,3})$$

其中 vk_i 是代理者 P_i 的验证公钥。为了不失一般性,假定 D 收到 t 个合法的部分重签名 $\sigma_{B,i}=(\sigma_{i,1},\sigma_{i,2},\sigma_{i,3})$,$i=1,\cdots,t$,则消息 m 的门限重签名为:

$$\sigma_B=(\sigma_{B,1},\sigma_{B,2},\sigma_{B,3})=\left(\prod_{i=1}^{t}(\sigma_{i,1})^{\lambda_{0,i}},\prod_{i=1}^{t}(\sigma_{i,2})^{\lambda_{0,i}},\prod_{i=1}^{t}(\sigma_{i,3})^{\lambda_{0,i}}\right)$$

其中 $\lambda_{0,i}$ 是 Lagrange 插值多项式的系数。

7)Verify:输入一个 n_m 比特长的消息 m,一个 n_{id} 比特长的身份 ID 和一个签名 $\sigma=(\sigma_1,\sigma_2,\sigma_3)$,如果 $e(\sigma_1,g)=e(h,g_1)e(J(ID),\sigma_2)e(\varpi,\sigma_3)$,则输出 1;否则,输出 0。

3 正确性分析

方案的正确性可以通过以下方程得到验证。

1)重签名子密钥的正确性验证:

$$rk_{A\to B}^{i,2}=g^{s_i}=g^{s_B+b_1i+\cdots+b_{t-1}i^{t-1}}=g^{\sum_{j=0}^{t-1}b_ji^j}=\prod_{j=0}^{t-1}(g^{b_j})^{i^j}=\prod_{j=0}^{t-1}(A_j)^{i^j}$$

$$e(rk_{A\to B}^{i,1},g)=e\left(\frac{h^{\alpha_i}J(ID_B)^{s_i}}{h^\alpha J(ID_A)^{s_A}},g\right)=e(h^{\alpha_i}h^{-\alpha}J(ID_B)^{s_i}J(ID_A)^{-s_A},g)=e(h^{\alpha_i},g)e(h^{-\alpha},g)e(J(ID_B)^{s_i},g)e(J(ID_A)^{-s_A},g)=e(h,vk_i)e(h,g_1)^{-1}e(J(ID_A),g^{s_A})^{-1}e(J(ID_B),rk_{A\to B}^{i,2})$$

2)部分重签名的正确性验证:

$$e(\sigma_{i,1},g)=e(\sigma_{A,1}\cdot rk_{A\to B}^{i,1}\cdot\varpi^{r_i},g)=e\left(h^\alpha J(ID_A)^{s_A}\varpi^{r_m}\frac{h^{\alpha_i}J(ID_B)^{s_i}}{h^\alpha J(ID_A)^{s_A}}\cdot\varpi^{r_i},g\right)=e(h^{\alpha_i}J(ID_B)^{s_i}\varpi^{r_m+r_i},g)=e(h^{\alpha_i},g)e(J(ID_B)^{s_i},g)e(\varpi^{r_m+r_i},g)=e(h,vk_i)e(J(ID_B),\sigma_{i,2})e(\varpi,\sigma_{i,3})$$

3)门限重签名的正确性验证:

$$\sigma_{B,2}=\prod_{i=1}^{t}(\sigma_{i,2})^{\lambda_{0,i}}=\prod_{i=1}^{t}(rk_{A\to B}^{i,2})^{\lambda_{0,i}}=\prod_{i=1}^{t}(g^{s_i})^{\lambda_{0,i}}=g^{\sum_{i=1}^{t}s_i\lambda_{0,i}}=g^{s_B}$$

$$\sigma_{B,3}=\prod_{i=1}^{t}(\sigma_{i,3})^{\lambda_{0,i}}=\prod_{i=1}^{t}(\sigma_{A,3}\cdot g^{r_i})^{\lambda_{0,i}}=\prod_{i=1}^{t}(g^{r_m}\cdot g^{r_i})^{\lambda_{0,i}}=\prod_{i=1}^{t}(g^{r_m+r_i})^{\lambda_{0,i}}=g^{\sum_{i=1}^{t}(r_m+r_i)\lambda_{0,i}}$$

$$e(\sigma_{B,1},g)=e\left(\prod_{i=1}^{t}(\sigma_{i,1})^{\lambda_{0,i}},g\right)=e\left(\prod_{i=1}^{t}(h^{\alpha_i})^{\lambda_{0,i}}J(ID_B)^{s_i\lambda_{0,i}}\varpi^{(r_m+r_i)\lambda_{0,i}},g\right)=e\left(h^{\sum_{i=1}^{t}\alpha_i\lambda_{0,i}},g\right)e(J(ID_B),g^{\sum_{i=1}^{t}s_i\lambda_{0,i}})e\left(\varpi,g^{\sum_{i=1}^{t}(r_m+r_i)\lambda_{0,i}}\right)=e(h,g^\alpha)e(J(ID_B),g^{s_B})e\left(\varpi,g^{\sum_{i=1}^{t}(r_m+r_i)\lambda_{0,i}}\right)=e(h,g_1)e(J(ID_B),\sigma_{B,2})e(\varpi,\sigma_{B,3})$$

4 安全性分析

定理 1 若代理重签名是一个不可伪造的签名方案,且相应的门限签名方案是可模拟的,则基于代理重签名方案的门限代理重签名方案是不可伪造的[3]。

很容易验证,当 $n\geqslant 2t-1$ 时,本文提出的基于身份的双向门限代理重签名方案是强壮的。本文方案是基于 $S_{id\text{-}mb}$ 方案的,而 $S_{id\text{-}mb}$ 方案已证明在标准模型下在适应性选择身份和消息攻击下是存在不可伪造的[5]。因此,只需证明本文方案是可模拟的。

定理 2 本文方案是可模拟的。

证明 为了不失一般性,假定代理者 $P_1,P_2,\cdots,P_t$ 已被攻击者攻陷。给定两个身份 (ID_A,ID_B),构造一个门限重签名生成算法 ShareRekey 的模拟器 $SIM_{\text{ShareRekey}}$。$SIM_{\text{ShareRekey}}$ 知道已被攻陷代理者的重签名子密钥 $rk_{A\to B}^i=(rk_{A\to B}^{i,1},rk_{A\to B}^{i,2})$ 和验

(下转第 142 页)

叠加曲线图,由于是参照同一坐标系,因此可以看出DFCTrust信任模型对于善意节点与其他各种恶意节点的信任值具有明显的区分效果。

从以上实验结果可以看出,由于引入了时间衰减因子和波动惩罚因子,DFCTrust模糊综合信任模型对于抵御震荡欺骗和大交易欺骗具有明显的效果,同时对于懒惰节点等不活跃节点,DFCTrust模糊综合信任模型也具有明显的遏制效果。

4 结语

本文提出了一种基于P2P网络的动态模糊综合信任模型——DFCTrust,通过模糊综合评价的方法从本身服务满意度及交易上下文两方面来计算节点信任度以反映节点每次交易的差异性;然后,在静态评价的基础上引入时间衰减因子及波动惩罚因子以反映出节点可信度是随着时间及节点行为的改变而改变的特性。分析和仿真实验说明,该模型在抵御恶意节点的选择性欺骗及周期性振荡欺骗行为方面具有很好的优势,而且可以有效地抵制节点的懒惰行为,较大地提高了P2P系统的交易成功率。

参考文献:

[1] 代战锋, 温巧燕, 李小标. P2P网络环境下的推荐信任模型方案[J]. 北京邮电大学学报, 2009, 32(3): 69 - 72.

[2] Gnutella[EB/OL]. [2010 - 03 - 15]. http://www.gnutella.com.

[3] Kazaa[EB/OL]. [2010 - 03 - 10]. http://www.kazaa.com/

[4] LIANG J, KUMAR R, XI Y, *et al*. Pollution in P2P file sharing systems[C]// Proceedings of the IEEE INFOCOM 2005. Washington, DC: IEEE Computer Society, 2005: 1174 - 1185.

[5] 杨天路, 刘宇宏, 张文, 等. P2P网络技术原理与系统开发案例[M]. 北京: 人民邮电大学出版社, 2007.

[6] STEPHEN M. Formalising trust as a computational concept [D]. Stirling, Scotland: University of Stirling, 1994 .

[7] 唐文, 陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报, 2003, 14(8): 1401 - 1408.

[8] WANG Y, VASSILEVA J. Trust and teputation model in peer-to-peer networks[C]// Proceedings of the 3th International Conference on Peer-to-Peer Computing. Washington, DC: IEEE Computer Society, 2003: 150 - 157.

[9] 石志国, 刘冀伟, 王志良. 基于时间窗反馈机制的动态P2P信任模型[J]. 通信学报, 2010, 31(2): 120 - 129.

[10] 常俊胜, 王怀民, 尹刚. DyTrust: 一种P2P系统中基于时间帧的动态信任模型[J]. 计算机学报, 2006, 29(8): 1301 - 1307.

[11] LI XIONG, LIU LING. PeerTrust: Supporting reputaion-based trust for peer-to-peer electronic connmunities[J]. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843 - 857.

[12] 李景涛, 荆一楠, 肖晓春等. 基于相似度加权推荐的P2P环境下的信任模型[J]. 软件学报, 2007, 18(1): 157 - 167.

[13] 赵灵犀, 田园, 邓鲁耀. P2P环境下引入激励机制的动态信任模型[J]. 计算机应用研究, 2010, 27(1): 251 - 254.

[14] 姜守旭, 李建中. 一种P2P电子商务系统中基于声誉的信任机制[J]. 软件学报, 2007, 18(10): 2551 - 2563.

(上接第128页)

证公钥 $vk_i = g^{\alpha_i}(1 \leqslant i \leqslant t-1)$,于是 $SIM_{\text{ShareRekey}}$ 可计算未被攻陷代理者的验证公钥 $vk_j = g_1^{\lambda_{j,0}} \prod_{i=1}^{t-1} vk_i^{\lambda_{j,i}}(j = t, t+1, \cdots, n)$,其中 $\lambda_{j,i}$ 是Lagrange插值多项式的系数。由于 $rk_{A\to B}^{i,2} = \prod_{j=0}^{t-1}(A_j)^{ij}$ 且 $A_0 = g^{sB}$,从而可计算出 $A_i(i = 1, \cdots, t-1)$。从攻击者的角度来看,模拟器 $SIM_{\text{ShareRekey}}$ 模拟的过程与ShareRekey算法执行的过程是不可区分的,所以ShareRekey算法是可模拟的。

给定两个身份 (ID_A, ID_B),一个消息 m,一个原始签名 $\sigma_A = (\sigma_{A,1}, \sigma_{A,2}, \sigma_{A,3})$ 和一个重签名 $\sigma_B = (\sigma_{B,1}, \sigma_{B,2}, \sigma_{B,3})$,以及 $t-1$ 个已被攻陷的重签名子密钥 $rk_{A\to B}^i = (rk_{A\to B}^{i,1}, rk_{A\to B}^{i,2})$,构造一个部分重签名生成算法的模拟器 $SIM_{\text{ShareResign}}$。$SIM_{\text{ShareResign}}$ 在 Z_p^* 中任意选取 $t-1$ 个随机数 $r_1, \cdots, r_{t-1}$,代表 $t-1$ 个已被攻陷的代理者计算相应的部分重签名:

$$\sigma_{B,i} = (\sigma_{i,1}, \sigma_{i,2}, \sigma_{i,3}) = (\sigma_{A,1} \cdot rk_{A\to B}^{i,1} \cdot \varpi^{r_i}, rk_{A\to B}^{i,2}, \sigma_{A,3} \cdot g^{r_i});\quad i = 1, 2, \cdots, t-1$$

然后,$SIM_{\text{ShareResign}}$ 计算未被攻陷的代理者的部分重签名:

$$\sigma_j = (\sigma_{j,1}, \sigma_{j,2}, \sigma_{j,3}) = \left((\sigma_{B,1})^{\lambda_{j,0}} \prod_{i=1}^{t-1}(\sigma_{i,1})^{\lambda_{j,i}}, (\sigma_{B,2})^{\lambda_{j,0}} \prod_{i=1}^{t-1}(\sigma_{i,2})^{\lambda_{j,i}}, (\sigma_{B,3})^{\lambda_{j,0}} \prod_{i=1}^{t-1}(\sigma_{i,3})^{\lambda_{j,i}}\right);\quad j = t, t+1, \cdots, n$$

其中 $\lambda_{j,i}$ 是Lagrange插值多项式的系数。因此,$SIM_{\text{ShareResign}}$ 能模拟攻击者在算法ShareResign中输出消息的部分重签名的视图,即本文基于身份的双向门限代理重签名方案是可模拟的。

结合定理1、定理2和基于身份的门限代理重签名方案的强壮性,可得如下定理。

定理3 在标准模型下,本文所提的基于身份的双向门限代理重签名方案在CDH假设下是安全的;在允许恶意攻击者攻陷 $t-1$ 个代理者的情况下,本文方案也是强壮的,并且 $n \geqslant 2t-1$。

5 结语

将基于身份的密码思想引入到门限代理重签名中,有效解决了管理公钥证书的复杂度问题。提出了一个基于身份的双向门限代理重签名方案,并在标准模型下证明了该方案的安全性。基于身份的门限代理重签名的研究,目前还处于初级阶段,仍有很多问题急需解决,比如设计高效的标准模型下可证安全的基于身份的单向门限代理重签名方案,以及寻找构造基于身份的门限代理重签名方案的一般性方法等。

参考文献:

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]// Proceedings of EUROCRYPT 1998. Berlin: Springer, 1998: 127 - 144.

[2] ATENIESE S, HOHENLERGER S. Proxy re-signatures: New definitions, algorithms and applications[C]// Proceedings of the ACM Conference on Computer and Communications Security. New York: ACM, 2005: 310 - 319.

[3] YANG PIYI, CAO ZHENFU, DONG XIAOLE. Threshold proxy re-signature[C]// Computing and Communications Conference. New York: IEEE, 2008: 450 - 455.

[4] CANETTI R, GOLDREICH O, HALEVI S. The random oracle methodology[J]. Journal of the ACM, 2004, 51(4): 577 - 594.

[5] SHAO JUN, CAO ZHENFU, WANG LICHENG, *et al*. Proxy re-signature schemes without random oracles[C]// Proceedings of the cryptology 8th International Conference on Progress in Cryptology. Berlin: Springer, 2007: 197 - 209.

[6] 毛文波. 现代密码学理论与实践[M]. 北京: 电子工业出版社, 2006.