代理重签名研究进展*

陈 亮, 陈性元, 孙 奕, 杜学绘
(解放军信息工程大学 河南省信息安全重点实验室, 郑州 450004)

摘 要: 综述了代理重签名理论及其发展状况、应用背景、一般模型和安全性定义;通过对现有经典代理重签名方案的系统研究,详细分析比较了其性能特性、执行效率和安全性。提出了代理重签名方案在数据安全交换中的应用,解决了现有电子政务中数据交换存在的效率低、密钥管理复杂、交换服务器权限过大等问题。最后概括了所取得的研究成果, 并讨论了目前研究中所遇到的关键问题。

关键词: 代理重签名; 双线性对; BLS 短签名方案; 安全性分析; 安全交换
中图分类号: TP393 **文献标志码**: A **文章编号**: 1001-3695(2014)01-0023-05
doi:10.3969/j.issn.1001-3695.2014.01.004

Survey of proxy re-signature technology

CHEN Liang, CHEN Xing-yuan, SUN Yi, DU Xue-hui
(*Henan Provincial Key Laboratory of Information Security*, *PLA Information Engineering University*, *Zhengzhou* 450004, *China*)

Abstract: This paper first introduced a proxy re-signature theory and its development, and then discussed the background of the application of the proxy re-signature scheme, the general model and security definition. Through a systematic study of the existing classic proxy re-signature scheme, it analysed and compared their performance features, implementation efficiency and safety in detail. It proposed a proxy re-signature scheme application on security data exchange and solved the existing e-government data exchange in the presence of low efficiency, complex key management, too large exchange server permissions. Finally, it summaried the achievement of the research and discussed the challenging problems of the research.

Key words: proxy re-signature; bilinear pairings; BLS short signature scheme; security analysis; security exchange

0 引言

代理重签名的概念最早由 Blaze 等人[1] 于 1998 年提出(下文称做 BBS 方案)。在代理重签名方案中,一个半可信的代理着 Alice 和 Bob 之间签名的转换者,他可以将 Alice 在消息 m 上的签名转换为 Bob 在同一个消息 m 上的签名。为了实现这种转换,代理必须拥有一个由 Alice 和 Bob 的私钥生成的重签名密钥,但是代理并不能代理 Alice 或者 Bob 在任一消息上进行签名。代理重签名的概念虽然很早就被提出来了,但由于 Blaze 等人没有给出代理重签名的形式化定义,使得人们不能很好地认识其优点,并且容易与其他签名类型相混淆(如代理签名[2]、传递签名[3]、群签名[4]、多重签名[5]、聚合签名[6]等)。

2005 年,Ateniese 等人[7] 首先指出了 BBS 方案的缺陷,即攻击者在获得一对签名/重签名时,就能够计算出此次代理重签名过程的重签名密钥,并形式化定义了代理重签名和它的安全模型。此外,在 BBS 方案代理者和被委托者能够合谋获得委托者的私钥。为了解决上述问题,Boneh 等人提出了基于双线性配对[8,9] 的解决方案。第一种是在短签名方案——BLS[6,8] 上扩展的复用、双向代理重签名方案。第二种是单用、单向的代理重签名方案,其中包括两种不同的签名算法,第一层签名(first-level)能够被代理者转换,第二层签名(由第一层签名转换得到的签名称为第二层签名 second-level)则不能。两种方案都是在随机预言模型下被证明是安全的。

2007 年,Shao 等人[10] 提出了两个在标准模型下可证安全的代理重签名方案。其中一种是多用、双向的代理重签名方案,另一种是多用、双向的基于身份的代理重签名方案。这两种方案均在标准模型下基于 Waters[11] 的方法证明是安全的。随后 Kim 等人[12] 发现第一个方案并非是安全的,并通过重新随机化重签名算法修正了存在的问题。

2008 年 Libert 等人[13] 提出了第一个多用、单向的代理重签名方案,并解决了 Ateniese 等人遗留的问题。尽管文中说明能够以一种有效的方式来提高代理者拥有的重签名密钥的安全性,但是随着传输次数的增加,签名的长度将成直线增加。随后对代理重签名方案的研究开始逐渐兴起,不仅围绕代理重签名算法本身,还包括与其他签名算法的结合。文献[14]提出了一种盲代理签名方案;文献[15]中一种前向安全的门限代理重签名方案被证明是安全的。文献[11]提出了一种复用、双向的基于身份的代理重签名方案;文献[16]提出了一种基于公钥证书 PKI 签名向基于身份 IDB 签名的转换方案。

代理重签名在减小公共密钥的管理开支、形成弱的群签名、节省空间的特定路径遍历证明、简化密钥管理[1] 和构造 DRM 的跨域操作系统[17] 等方面有很好的应用前景。本文将

收稿日期: 2013-05-13; **修回日期**: 2013-06-23 **基金项目**: 国家“973”计划资助项目(2011CB311801);国家“863”计划资助项目(2012AA012704);河南省科技创新人才计划资助项目(114200510001)

作者简介:陈亮(1991-),男,河南浚县人,硕士研究生,主要研究方向为网络与信息安全(yixiu199151@sina.com);陈性元(1963-),男,安徽无为人,教授,博导,博士,主要研究方向为网络与信息安全;孙奕(1979-),女,河南郑州人,讲师,博士研究生,主要研究方向为网络与信息安全;杜学绘(1968-),女,河南辉县人,教授,硕导,博士,主要研究方向为网络与信息安全.

综述代理重签名方案的定义、一般模型及相关特性,并对现有的代理重签名方案的效率和安全性进行分析比较。

1 代理重签名

1.1 代理重签名的一般模型

代理重签名体制依靠一个半可信赖的代理充当 Alice 和 Bob 之间的转换者,它可以使用自己的重签名密钥将 Alice 在一个消息 m 上的签名转换为 Bob 在 m 上的签名,但是此代理并不知道签名密钥的信息并且不能代替 Alice 或者 Bob 在任一消息上签名。一个代理重签名方案由五个多项式时间算法(keyGen,reKey,sign,reSign,verify)组成。其中:

a)$\text{keyGen}(1^k)\rightarrow(pk,sk)$,输入安全参数 1^k,密钥生成算法 keyGen 生成一对公私钥对(pk,sk)。

b)$\text{reKey}(sk_a,sk_b)\rightarrow(rk_{a\leftrightarrow b})$,输入用户 A 和 B 的 sk_a,sk_b,再签名密钥生成算法 reKey 生成 A 和 B 之间的再签名密钥 $rk_{a\leftrightarrow b}$。

c)$\text{sign}(sk,m)\rightarrow\sigma$,输入私钥 sk、消息 m,签名算法 sign 输出消息 m 的签名 σ,该签名可以用 sk 对应的公钥 pk 验证,这种形式的签名称为原始签名。

d)$\text{reSign}(rk_{a\leftrightarrow b},pk_a,m,\sigma)\rightarrow\sigma'$,输入再签名密钥 $rk_{a\leftrightarrow b}$、消息 m、用户 A 的公钥 pk_a 以及用 pk_a 可验证 m 的签名 σ,再签名算法 reSign 输出消息 m 的新签名 σ'。该签名可以用用户 B 的公钥 pk_b 验证,称这种形式的签名为再签名。

e)$\text{verify}(pk,m,\sigma)=1$,$\text{verify}(pk_b,m,\sigma')=1$。当由签名算法和重签名算法合法产生的签名能通过签名验证时,即算法结果输出为 1 时,证明重签名方案正确。

在代理重签名体制中,代理可以将 Alice 在消息 m 上合法、可验证的签名 $\sigma_A(m)$ 转换为 Bob 在消息 m 上的签名 $\sigma_B(m)$。Alice 的签名和通过代理产生的签名能够同时存在并且可以验证是不同的两个人在同一消息上的签名。

1.2 代理重签名的特性

自 1998 年提出 BBS 方案以后,一直没有被给予足够的重视,原因是 BBS 原型和之后所提出的为数不多的代理签名方案均存在一系列的缺陷导致不适合大多数应用。为了使代理重签名更好地得到应用,Ateniese 等人[7]列举了方案要满足的一些特性:

a)单向性(unidirectional)。代理用重签名密钥 $rk_{A\rightarrow B}$ 只能将 Alice 的签名转换成 Bob 的签名,但是不能将 Bob 的转换为 Alice 的。不满足此特性的方案称为双向的(bidirectional)。一般来说,单向代理重签名比双向代理重签名更具有优越性,因为前者可以通过两个不同的方向来构成后者。

b)复用(multi-use)。一个消息可以被重签名多次,即由 sign 和 resign 算法产生的签名均能作为 resign 算法的输入。反之,非复用(single-use) 的代理重签名方案中只有 sign 产生的签名才能作为 resign 的输入。

c)秘密代理(private proxy)。在一个秘密代理者代理重签名方案中,代理者所拥有的额外信息是可以被代理者保密的,即攻击者不能从代理者执行转换过程中获得额外信息。相应地,在公开代理者的代理重签名方案中,攻击者能够通过观察代理的输入输出计算出重签名密钥。

d)透明(transparent)。代理是透明的,即 Alice 在消息 m 上由 sign 生成的签名和代理 reSign 生成的签名在计算性上是难以区分的。

e)密钥优化(key optimal)。在密钥最优的代理方案中,用户所要保存的秘密数据的量要小,并保证代理的安全,不论其有多少委托者和被委托者。

f)不可交互(non-interactive)。Bob(委托者)能通过自己的私钥和 Alice 的公钥产生重签名密钥 $rk_{A\rightarrow B}$,即被委托者不参与委托过程。

g)非传递(non-transitive)。签名的转换功能不能由代理者自己产生。

h)暂时性(temporary)。在暂时性特性中,委托者可以收回分配出去的签名权。

2 代理重签名方案分析

本章主要分析现有的代理重签名方案所满足的特性及算法效率等,其中包括基于公钥证书的签名机制、基于身份证书的签名机制以及混合签名机制。

2.1 现有典型代理重签名方案

2.1.1 BBS 方案

BBS 代理重签名方案。全局参数(g,p,q,H),其中 g 是阶为 $q=\Theta(2^k)$ 的、Z_p^* 的子群的生成元,且 H 是将$\{0,1\}^*$上的字符串转移到 Z_q 中元素的 hash 函数。

a)密钥生成(keyGen)。输入安全参数 1^k,选择随机的 $a\in Z_q$,并输出公私钥对 $pk=g^a$ 和 $sk=a$。

b)重签名密钥生成(reKey)。输入两个私钥 $sk_A=a$,$sk_B=b$(算法中不需要委托双方的公钥),输出重签名密钥 $rk_{A\rightarrow B}=a/b(\bmod q)$。

c)签名(sign)。输入私钥 $sk=a$ 和消息 m,选择随机元素 $x_1,\cdots,x_k\in Z_q$。然后,计算 $r=(g^{x_1},\cdots,g^{x_k})(\bmod p)$ 并从输出 $H(r)$ 中抽取 k 个伪随机比特 $b_1,\cdots,b_k$。最后输出签名 $\sigma=(r,s)$,其中 $s=(s_1,\cdots,s_k)$,每个 $s_i=(x_i-mb_i)/a(\bmod q)$。

d)重签名(reSign)。输入重签名密钥 $rk_{A\rightarrow B}$、公钥 pk_A、签名 σ 和消息 m,检查 $\text{verify}(pk_A,m,\sigma)=1$。如果 σ 通过验证,令 $r'=r$ 和 $s_i'=s_irk_{A\rightarrow B}(\bmod q)$,并输出签名 $\sigma_B=(r',s')$,其中 $s'=(s_1',\cdots,s_k')$,否则输出出错信息 $\perp$。

e)验证(verify)。输入公钥 pk_A,消息 m 和签名 $\sigma=(r,s)$,计算 $H(r)$,并从中抽取伪随机比特 $b_1,\cdots,b_k$。对于每个 $g^{x_i}\in r$ 和 $s_i\in s$,检查$(pk_A)^{s_i}=g^{x_i}/g^{mb_i}(\bmod p)$。如果所有的检查通过输出 1,否则输出 0。

在 BBS 方案中,重签名密钥是公开的,攻击者通过观察一个合法的签名及其对应的代理重签名就足以推算出重签名密钥成为恶意的代理者,并由此计算出对方的私钥。

2.1.2 AH 方案

2005 年,Ateniese 等人[7]首先指出了 BBS 方案的缺陷,并基于双线性对提出了第一个单向的代理重签名方案 AH 方案。此方案需要一个双线性映射 $e:G_1\times G_1\rightarrow G_2$,其中 G_1 和 G_2 都是阶为素数 $q=\Theta(2^k)$ 的循环乘法群。全局参数(e,q,G_1,G_2,g,H),其中,g 是 G_1 的生成元,H 是公开的、抗碰撞的单向哈希函数,$H:\{0,1\}^*\rightarrow G_1$。

a)密钥生成(keyGen)。输入安全参数 1^k,选择随机的 $a\in Z_q$,并输出公私钥对 $pk=g^a$ 和 $sk=a$。

b)重签名密钥生成(reKey)。输入两个私钥 $sk_A=a, sk_B=b$(算法中不需要委托双方的公钥),输出重签名密钥 $rk_{A\to B}=b/a(\mathrm{mod}\ q)$。

c)签名(sign)。输入私钥 $sk=a$ 和消息 m,输出 $\sigma=H(m)^a$。

d)重签名(reSign)。输入重签名密钥 $rk_{A\to B}$,公钥 pk_A,签名 σ 和消息 m,检查 verify$(pk_A,m,\sigma)=1$。如果 σ 通过验证,$\sigma'=\sigma^{rk_{A\to B}}$,否则输出 $\perp$。

e)验证(verify)。输入公钥 pk_A、消息 m 和待验证的签名 σ,如果 $e(\sigma,g)=e(H(m),pk_A)$ 成立输出 1,否则输出 0。

其中 AH_b 为双向、复用的 AH 方案,AH_u 为单向、单用的 AH 方案。在 AH_u 方案中每个签名者都有一对强密钥、弱密钥与公钥相对应,使用重签名密钥可以把 Alice 在强密钥下的签名转换为 Bob 在弱密钥下的签名。因为在弱密钥下的签名不能转换,所以方案是单用的。

2.1.3　SCW 方案

2007 年,Shao 等人[10]第一次提出了两个在标准模型下可证安全的代理重签名方案(SCW 方案)假设所有被签名的消息均可能表示成 n_m 长的比特字符串,n_m 与双线性群的阶 p 无关,选取抗碰撞的哈希函数 $H:\{0,1\}^*\to\{0,1\}^{n_m}$。选择两个阶为素数 $q=\Theta(2^k)$ 有限循环群 G_1 和 G_2 且 $e:G_1\times G_1\to G_2$,设 g 是 G_1 的生成元。从 Z_p^* 中任选一个数 a,从 G_1 中任选 n_m+2 个随机数 $(g_2,u',u_1,\cdots,u_{n_m})$,公开参数 $(G_1,G_2,e,g_2,u',u_1,\cdots,u_{n_m})$。

a)密钥生成(keyGen)。输入安全参数 1^k,输出公私钥对 $pk=g_1=g^a$ 和 $sk=a$。

b)重签名密钥生成(reKey)。输入两个私钥 $sk_A=a, sk_B=b$(算法中不需要委托双方的公钥),输出重签名密钥 $rk_{A\to B}=b/a(\mathrm{mod}\ q)$。

c)签名(sign)。输入私钥 $sk=a$ 和 n_m 比特长的消息 m,输出 $\sigma=(\Im,\Re)=(g_2^a\cdot w^r,g^r)$,$r$ 是从 Z_p^* 中选取的一个数。$w=u'\cdot\prod_{i\in u}u_i$,$u\subset\{1,\cdots,n_m\}$ 是 $m[i]=1$ 的索引 i 的集合,$m[i]$ 是消息 m 的第 i 个比特的值。

d)重签名(reSign)。输入重签名密钥 $rk_{A\to B}$、公钥 pk_A、签名 σ 和 n_m 比特长的消息 m,检查 verify$(pk_A,m,\sigma)=1$。如果 σ 通过验证,$\sigma'=\sigma^{rk_{A\to B}}=(g_2^b\cdot w^{rb/a},g^{rb/a})=(g_2^b\cdot w^{r'},g^{r'})$,其中 $r'=rb/a(\mathrm{mod}\ p)$,否则输出 $\perp$。

e)验证(verify)。输入公钥 pk_A,n_m 比特长的消息 m 和待验证的签名 σ,如果 $e(pk,g_2)e(\Re,w)=e(\Im,g)$,输出 1,否则,输出 0。

其中 SCW 方案是复用、双向的;SCW_i 方案是在 SCW 方案的基础之上扩展的基于身份的复用、双向代理重签名方案。

2.1.4　LV 方案

2008 年 Libert 等人[13]提出了第一个复用、单向的代理重签名方案(LV 方案),并解决了 Ateniese 等人遗留的代理传输的单向性及可能存在的签名重放问题。

全局建立(global-setup):给定秘密参数 λ、n,算法选取阶为 $p>2^\lambda$ 的双线性群 (G,G_T),生成 $g,h\xleftarrow{R}G$ 和一个随机的 $(n+1)$ 矢量 $u=(u',u_1,\cdots,u_n)\xleftarrow{R}G^{n+1}$,然后定义一个函数 $F:\{0,1\}^n\to G$ 匹配 n 比特的字符串 $m=m_1\cdots m_n$(对于所有的 $i\in\{0,1\}$,$m_i\in\{0,1\}$)到 $F(m)=u'\cdot\prod_{i=1}^n u_i^{m_i}$。公共参数为 $cp:\{G,G_T,g,h,u\}$。

a)密钥生成 keyGen(λ)。用户 i 为每一个随机数 $x_i\xleftarrow{R}Z_p^*$,设置其公钥 $X_i=g^{x_i}$。

b)重签名密钥生成 reKeygen(x_j,X_i)。给定用户 j 的私钥 x_j 和用户 i 的公钥 X_i,生成单向重签名密钥 $R_{ij}=X_i^{1/x_j}=g^{x_i/x_j}$(此重签名密钥可以将用户 i 的签名转换为用户 j 的签名)。

c)签名 sign$(1,m,x_i)$。对消息 $m=m_1\cdots m_n\in\{0,1\}^n$ 进行第一层的签名,随机选取 $r\xleftarrow{R}Z_p^*$,然后计算:

$$\sigma^{(1)}=(\sigma_0,\sigma_1)=(h^{x_i}\cdot F(m)^r,g^r)$$

d)签名 sign$(2,m,x_i)$。为了生成 $m=m_1\cdots m_n\in\{0,1\}^n$ 的第二层签名,选取 $r,t\xleftarrow{R}Z_p^*$,并计算:

$$\sigma^{(2)}=(\sigma_0,\sigma_1,\sigma_2,\sigma_3)=(h^{tx_i}\cdot F(m)^r,g^r)$$

e)重签名 reSign$(1,m,\sigma^{(1)},R_{ij},X_i,X_j)$。输入消息 $m\in\{0,1\}^n$,重签名密钥 $R_{ij}=g^{x_i/x_j}$,签名 $\sigma^{(1)}=(\sigma_0,\sigma_1)$ 和公钥 X_i,X_j,检查签名者 i 的签名 $\sigma^{(1)}$ 的有效性:

$$e(\sigma_0,g)=e(X_i,h)\cdot e(F(m),\sigma_1)\tag{1}$$

如果 $\sigma^{(1)}$ 有效,就能够通过选取 $r',t\xleftarrow{R}Z_p^*$ 并计算:

$$\sigma^{(2)}=(\sigma_0',\sigma_1',\sigma_2',\sigma_3')=(\sigma_0^t\cdot F(m)^{r'},\sigma_1^t\cdot g^{r'},X_i^t,R_{ij}^t)=(h^{tx_i}\cdot F(m)^{r''},g^{r''},X_i^t,g^{tx_i/x_j})$$

从而转换为 j 的签名。这里 $r''=tr+r'$,如果令 $\tilde{t}=tx_i/x_j$,则

$$\sigma^{(2)}=(\sigma_0',\sigma_1',\sigma_2',\sigma_3')=(h^{\tilde{t}x_j}\cdot F(m)^{r''},g^{r''},X_j^{\tilde{t}},g^{\tilde{t}})\tag{2}$$

f)验证 verify$(1,m,\sigma^{(1)},X_i)$。第一层签名 $\sigma^{(1)}=(\sigma_0,\sigma_1)$ 的正确性由(1)式验证。

g)验证 verify$(2,m,\sigma^{(2)},X_i)$。如果下列条件成立:

$$e(\sigma_0,g)=e(\sigma_2,h)\cdot e(F(m),\sigma_1')$$
$$e(\sigma_2,g)=e(X_i,\sigma_3)$$

则第二层签名 $\sigma^{(2)}=(\sigma_0,\sigma_1,\sigma_2,\sigma_3)$ 成立。

虽然 LV 方案满足了大部分代理重签名的特性,解决了一系列的问题,并且是第一个复用、单向的代理重签名方案。但是,由于其计算量比较大,占用较大的存储空间,难以应用于实际环境。

2.2　方案分析

2.2.1　特性分析

本节将从代理重签名算法的特性分析现有的代理重签名方案。目前为止还没有任何一个满足 1.2 节中提出的所有特性。表 1 列出了当前已有的被证明安全的代理重签名方案[18~20]。

表 1　证明安全的代理重签名方案的特性分析

Pro	BBS	AH_b	AH_u	SCW	SCW_i	LV_s	LV_m
1	No	No	Yes	No	No	Yes	Yes
2	Yes	Yes	No	Yes	Yes	Yes	Yes
3	No	Yes	No	Yes	Yes	No	No
4	Yes	Yes	Yes	Yes	Yes	Yes	Yes
5	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6	No	No	Yes	No	No	Yes	Yes
7	No	No	Yes	No	No	Yes	Yes
8	No	No	Yes	Yes	Yes	No	No

注:AH_b 是双向、复用的 AH 方案;AH_u 是单向、单用的 AH 方案;SCW_i 是基于身份的 SCW 方案;LV_s 是复用、单向 single-hop 方案;LV_u 是复用、单向 multi-hop 方案

从表中可以看出随着代理重签名技术的不断发展研究,代理重签名方案满足的特性越来越多。BBS、AH_b、SCW 和 SCW_i

都是双向、多用的代理重签名方案，AH_u 方案虽然实现了单向功能但是并不是多用的。LV 方案虽然保证了单向、多用的特性，但是由于其代理者并不能秘密地保存重签名密钥，因此也存在相应的安全隐患并且计算代价偏高。

2.2.2 性能及安全性分析

本节从验证和重签名算法的处理时间、方案基于的安全性问题及重签名密钥是否需要保存等方面分析现有代理重签名方案的性能及安全性。具体分析结果如表2所示[21~24]。

表2 证明安全的代理重签名方案性能及安全性分析

scheme	key-pro	check	re-sign	security
BBS	Yes	$(3k)$e	(k)me	Under ROM, if CDH is difficult, it is EF-CMA security.
AH_b	Yes	2p	1e	Under ROM, if CDH and 2-DL is difficult, it is EF-CMA security.
AH_u	No	2p	1e	Under ROM, if CDH is difficult, it is EF-CMA security.
SCW	Yes	3p	2e	Under SM, if CDH is difficult, it is EF-CMA security.
SCW_i	Yes	4p	2e	Under SM, if CDH is difficult, it is EF-CMA security.
LV_s	No	2p∪4p	3e∪1e	Under SM, if L-Flex and m-CDH is difficult, it is EF-CMA security.
LV_m	No	$(2l+2)$p	$(2l+3)$e	Under ROM, if L-Flex and m-CDH is difficult, it is EF-CMA security.

注：key-pro 表示重签名密钥是否需要秘密保存；p 代表一次对数运算；e 代表一次一次幂运算；me 代表多重幂运算；ROM 为随机预言模型；SM 为标准模型；EF-CMA 为适应性选择消息下抵抗存在性伪造攻击[25]。

从表中可以看出 BBS、AH_b、SCW 和 SCW_i 方案的重签名密钥虽然需要秘密地保存，但其在算法的执行上相对比较高效。AH_u、LV_s 和 LV_m 方案的重签名密钥不需要秘密地保存，但其在算法的执行上时间开销比较大。因此，强安全性模型和提高算法效率是重签名算法下一步的研究重点。

3 应用场景

3.1 代理重签名的应用

3.1.1 特定路径的遍历证明

利用代理重签名可以证明图中的特定路径被遍历。如图1所示。

签名者 A 生成消息 m 的第一个签名 $\sigma_A(m)$，中间的代理者通过特定的变换顺序将其转换为最终的签名 $\sigma_E(m)$，通过这样的构造，可以保证图中的某一特定路径被遍历，而没有走其他的路径。例如，为了保证外国游客合法地进入本国，并通过了一系列相应的检查，美国海关只需保留一个公钥（用于验证护照上的原始签名是否是由移民局签名的），在这种情况下，复用的代理重签名将能得到更好的应用。

3.1.2 数字证书的共享和转换

BBS 方案中指出代理重签名方案可以用来在系统中添加新的公钥对或者更新公钥对而不用获取新的证书，从而减小公钥的管理开支。因为生成新公钥的证书花费是比较大的，使用代理重签名方案可以共享已经存在的证书。新密钥下的签名通过签名转换可以转换为已经认证过的公钥下的签名。

3.1.3 管理群组签名

代理重签名方案可以通过对签名的管理，隐藏公司内部组织成员的信息。例如公司的内部文件一般是由公司内部某一特定成员签名的。在这些文件离开公司内部之时，代理可以把包含了个人信息的公司成员签名转换为能用公司公钥验证的签名。从而隐藏了原始签名者的身份信息和公司内部的组织结构。

3.1.4 透明认证

代理重签名方案可以转换来自不同认证中心（CAs）的公钥证书。假设 A 和 B 之间要建立一条秘密的安全信道，并且 A 只能验证来自认证中心 CA1 的证书，B 只能验证来自认证中心 CA2 的证书，这两个认证中心可以通过建立一个半可信的代理人来转换它们之间的证书。如图2所示。

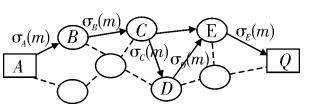

图1 特定路径遍历示意图

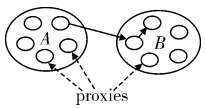

图2 透明认证

当证书由一个网络发送到另一个网络时，首先证书需要被目标网络中的代理者转换，然后再发送至目标节点；或者目标节点首先收集来自其他网络的所有不兼容的证书，然后再发送到本网络中的代理者进行转换。在此场景中使用代理重签名可以使两个网络之间以类似于对内部节点透明的方式进行通信。

3.2 数据安全交换中的应用举例

下面举一个代理重签名在数据安全交换中的应用，如图3所示。

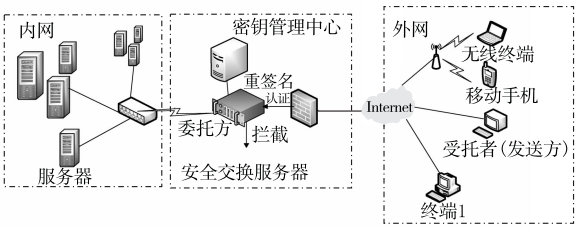

图3 数据安全交换背景

电子政务内、外网在涉密性要求，具体职能，业务范围以及服务对象等存在着差异，政务外网 CA 认证服务通过向外网接入单位发放证书提供统一用户管理、身份认证、授权管理等功能，同时加强服务公众、社会管理等的应用，充分发挥政务外网的服务功能，外网证书发放的终端服务对象为公众、企业和政府部门相关人员。而内网 CA 认证应用仅限于向内网接入单位发放，用于保护内网应用安全，因此内网证书发放的终端服务对象为政府部门及重要企事业单位工作人员。这些差异的存在决定了内、外网用户位于不同的证书域中[26]。当内外网之间的用户需要进行文件交换时，现有的解决方案主要是通过采用交换服务器再签名的方式，在一定程度上满足了内外网用户的文件交换需要。但是这种方式存在以下问题及安全隐患：

a）效率低。交换服务器需要将发送的数据进行签名验证，然后再签名，发送给接收方，即交换服务器需要进行一次验证和签名操作才能将数据转发出去，计算量大，效率低。

b）密钥管理复杂。交换服务器为了验证签名，需要保存所有用户的公钥，密钥存储量大。并且发送方的公钥需扩散至接收方的证书域中才能使接收方对其签名进行验证，即公钥需跨域传输，操作复杂，不便于密钥的更新和维护。

c）交换服务器的权限大。采取现有的再签名方式，交换数据的转发都需由交换服务器完成一次验证和签名操作。此时交换服务器可以伪造发送者向接收者发送任何信息，权限过大，一旦交换服务器被攻破，整个交换过程就将不可信。

正因为代理重签名方案独特的签名转换功能，因此可以很

好地解决数据安全交换中存在的上述问题。假定交换服务器是半可信的,安全交换服务器拥有交换双方单向的重签名密钥。以外网向内网发送数据为例,安全交换代理重签名过程如图 4 所示。

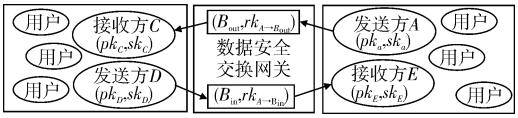

图 4　安全交换代理重签名过程

a)A 首先产生对消息 m 的签名 $\sigma_A = \mathrm{sign}(sk_a, m)$,并将消息 m 及签名信息 σ_A 发送给安全交换服务器 B;

b)B 收到 A 发送的信息后,对消息 m 的签名进行验证 $\mathrm{verify}(pk_a, m, \sigma_A)$,输出 1,继续执行步骤 c),输出 0,结束;

c)B 执行重签名算法 $\sigma_{B_{in}} = \mathrm{reSign}(rk_{A\to B_{\mathrm{in}}}, \sigma_A)$,并将消息 m 及重签名信息 σ_{Bi} 发送给接收方 C;

d)C 接收到信息后,对消息 m 的重签名进行验证 $\mathrm{verify}(pk_{B_{\mathrm{in}}}, m, \mathrm{reSign}(rk_{A\to B_{\mathrm{in}}}, \sigma_A))$,输出 1,验证成功,输出 0,结束。

4　研究热点及发展前景

由于代理重签名可以应用于许多场合,越来越受到了国内外学者的关注,特别是 2005 年,Ateniese 对代理重签名进行了新的解释和定义之后。然而现有的代理重签名方案还存在许多缺陷,还有很多问题亟需解决,导致其发展和应用并不广泛。为了使代理重签名能有进一步的发展和应用,以后的研究主要需解决以下几个关键问题:

a)现有的代理重签名方案在应用过程中,除了需要满足已有的特性之外,还需根据不同的应用场景增加新特性。例如在一些证书与身份或者属性信息绑定的系统中,还需要满足消息绑定的特性。

b)即使对于已提出的特性,现有的代理重签名方案也只能满足其中一部分的特性,并且当满足的特性比较多,计算量也随之增加。例如复用、单向的代理重签名方案在解决网络路径证明方面有着很好的应用,但是目前存在的复用、单向代理重签名方案都是有签名扩展的。每经过一次重签名,那么重签名后的长度会增加一个原始签名的长度,极大地增加了数据的传输量和计算量。

c)代理重签名理论和技术提出的时间还比较短,可以与现有成熟的签名方案结合,使之能够更好地解决实际问题,发挥潜在的优势。例如,代理重签名与流认证的结合,可用于解决实时、动态的流签名转换;代理重签名与属性信息的结合,可用于解决云计算环境下云存储服务的数据共享问题。

5　结束语

本文概述了代理重签名技术的研究进展及应用场景,重点分析和比较了现有的代理重签名方案的特性、执行效率和安全性。在对代理重签名技术深入理解的基础上,举例说明了代理重签名在数据安全交换中的应用,解决了电子政务中数据安全交换存在的内外网证书体系结构差异性问题。目前针对代理重签名的研究还主要集中在技术本身的安全性、执行效率、特性功能及与其他签名技术的结合方面。随着对代理重签名技术的进一步研究发展,代理重签名方的应用领域会进一步扩展,应用前景会更加广阔。

参考文献:

[1] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Advances in Cryptology. Berlin: Springer-Verlag, 1998: 127-144.

[2] BOLDYREVA A, PALACIO A, WARINSCH B. Secure proxy signature schemes for delegation of signing rights[J]. Journal of Cryptology, 2012, 25(1): 57-115.

[3] MICALI S, RIVEST R L. Transitive signature schemes[M]//Topics in Cryptology. Berlin: Springer-Verlag, 2002: 236-243.

[4] CHEN Xi-hui, LENZINI G, MAUW S, *et al*. A group signature based electronic toll pricing system[C]//Proc of the 7th International Conference on Availability, Reliability and Security. Washington DC: IEEE Computer Society, 2012: 85-93.

[5] SEVERENS M, FARQUHAR J, DUYSENS J, *et al*. A multi-signature brain-computer interface: use of transient and steady-state responses[J]. Journal of Neural Engineering, 2013, 10(2): 026005.

[6] BONEH D, GENTRY C, LYNN B, *et al*. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Advances in Cryptology. Berlin: Springer-Verlag, 2003: 416-432.

[7] ATENIESE G, HOHENBERGER S. Proxy re-signatures: new definitions, algorithms, and applications[C]//Proc of the 12th ACM Conference on Computer and Communications Security. New York: ACM Press, 2005: 310-319.

[8] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319.

[9] MENEZES A J, OKAMOTO T, VANSTONE S A. Reducing elliptic curve logarithms to logarithms in a finite field[J]. IEEE Trans on Information Theory, 1993, 39(5): 1639-1646.

[10] SHAO Jun, CAO Zhen-fu, WANG Li-cheng, *et al*. Proxy re-signature schemes without random oracles[C]//Progress in Cryptology. Berlin: Springer-Verlag, 2007: 197-209.

[11] WATERS B. Efficient identity-based encryption without random Oracles[C]//Advances in Cryptology. Berlin: Springer-Verlag, 2005: 114-127.

[12] KIM K, YIE I, LIM S. Remark on Shao *et al*'s bidirectional proxy re-signature scheme in Indocrypt 2007[J]. International Journal of Network Security, 2009, 8(3): 308-311.

[13] LIBERT B, VERGNAUD D. Multi-use unidirectional proxy re-signatures[C]//Proc of the 15th ACM Conference on Computer and Communications Security. New York: ACM Press, 2008: 511-520.

[14] DENG Yu-qiao. A blind proxy re-signatures scheme based on random Oracle[J]. Advanced Materials Research, 2011, 204-210: 1062-1065.

[15] YANG Xiao-dong, WANG Cai-fen, ZHANG Yu-lei, *et al*. A new forward-secure threshold proxy re-signature scheme[C]//Proc of IEEE International Conference on Network Infrastructure and Digital Content. 2009: 566-569.

[16] VIVEK S S, SELVI S S D, RANGAN C P, *et al*. A special purpose proxy re-signature scheme[C]//Proc of International Conference on Innovations in Information Technology. 2012: 261-266.

[17] BISHR M, WYTZISK A, MORALES J. GeoDRM: towards digital management of intellectual property rights for spatial data infrastructures[EB/OL]. (2006-11-10). http://www.gsdicocs.org/gsdiconf/GSDI-9/paper/TS8.4paper.pdf.

[18] SUNITHA N R, AMBERKER B B. Proxy re-signature schemes: multi-use, unidirectional & translations[J]. Journal of Advances in Information Technology, 2011, 2(3): 165-176.

(下转第 32 页)

国大百科全书出版社,2010: 417.
[2] SHANNON M. The expansion of international organizations[C]// Proc of Annual Meeting of the American Political Science Association. 2004.
[3] SAVAGE I R, DEUTSCH K W. A statistical model of the gross analysis of transaction flows [J]. Econometrica, 1960, 28(3): 55-72.
[4] BRAMS S J. Transaction flows in the international system [J]. American Political Science Review, 1966, 60 (4): 880-898.
[5] SKJELSBAEK K. Peace and the structure of the international organization network [J]. Journal of Peace Research, 1972, 9(4): 315-330.
[6] SNYDER D, KICK E L. Structural position in the world system and economic growth, 1955-1970: a multiple network analysis of transnational interactions [J]. American Journal of Sociology, 1979, 84 (5): 1096-1126.
[7] FABER J. Measuring cooperation, conflict, and the social network of nations [J]. Journal of Conflict Resolution, 1987, 31(3): 438-464.
[8] SACKS M A, VENTRESCA M J, UZZI B. Global institutions and networks: contingent change in the structure of world trade advantage [J]. American Behavioral Scientist, 2001, 44(10): 1579-1601.
[9] HAFNER-BURTON E M, MONTGOMERY A H. Power positions: international organizations, social networks, and conflict [J]. Journal of Conflict Resolution, 2006, 50(1): 33-43.
[10] MAOZ Z, KUPERMAN R D, TERRIS L, *et al*. Structural equivalence and international conflict : a social network analysis [J]. Journal of Conflict Resolution, 2006, 50(3): 664-669.
[11] HAFNER-BURTON E M, KAHLER M, MONTGOMERY A H. Network analysis for international relations [J]. International Organization, 2009, 63(5): 559-592.
[12] OLIVEIRA M, GAMA J. An overview of social network analysis [J]. Wires Data Mining Knowledge Discovery, 2012, 30 (2): 99-115.
[13] MORENO J L. Who shall survive? [M]. [S. l.]: Beacon House, 1953: 98-112.
[14] WASSERMAN S, FAUST K. Social network analysis: methods and applications [M]. Cambridge: Cambridge University Press, 1994: 26-29.
[15] FREEMAN L C. Centrality in social networks [J]. Social Networks, 1979, 16(1): 215-239.
[16] ALTMANN M. Reinterpreting networks measures for models of disease transmission [J]. Social Networks, 1993, 15(1): 1-17.
[17] POULIN R, BOILY M C, MASSE B R. Dynamical systems to define centrality in social networks [J]. Social Networks, 2000, 22(3): 187-220.
[18] 薄辉. 社区发现技术的研究与实现[D]. 北京:北京交通大学, 2009.
[19] 朱明. 数据挖掘[M]. 合肥:中国科学技术大学出版社, 2008: 222-223.
[20] BONACICH P. Power and centrality: a family of measures [J]. American Journal of Sociology, 1987, 92(5): 1170-82.
[21] STEPHENSON K, ZELEN M. Rethinking centrality: methods and examples [J]. Social Networks, 1989, 11(1): 1-37.
[22] FREEMAN L C, BORGATTI S P, WHITE D R. Centrality in valued graphs: a measure of betweenness based on network flow [J]. Social Networks, 1991, 13(2): 141-54.
[23] JOHNSON S C. Hierarchical clustering schemes [J]. Psychometrika, 1967, 38(4): 241-254.
[24] BREIGER R, ENNIS J. Personae and social roles: the network structure of personality types in small groups [J]. Social Psychology Quarterly, 1979, 42(3): 262-270.
[25] KRUSKAL W, WISH M. Multidimensional scaling: quantitative applications in the social sciences [M]. [S. l.]: SAGE Publication, 1978: 232-250.
[26] HAMER C. Cluster analyzing profile data confounded with interrater differences: a comparison of profile association measures [J]. Applied Psychological Measurement, 1981, 42(5): 63-72.
[27] EVERITT B S. Unresolved prolems in cluster analysis [J]. Biometrics, 1980, 35(3): 169-181.
[28] BECKFIELD J. Inequality in the world polity: the structure of international organization [J]. American Sociological Review, 2003, 68(3): 401-24.
[29] KIM J H, BARNETT G A. A structural analysis of international conflict: from a communication perspective [J]. International Interactions, 2007, 33(2): 135-165.
[30] MANGER M S, PICKUP M A, SNIJDERS T A B. When country interdependence is more than a nuisance: the longitudinal network approach [C]//Proc of the 104th Annual Meeting of the American Political Science Association. 2008.
[31] FREEMAN W. Using galois lattices to represent network data [J]. Sociological Methodology, 1993, 15(2): 127-146.
[32] FAUST W. Correlation and association models for studying measurements on ordinal relations [J]. Sociological Methodology, 1993, 14(2): 177-216

(上接第27页)

[19] SUNITHA N R, AMBERKER B B. Multi-use unidirectional forward-secure proxy re-signature scheme [C]//Proc of IEEE International Conference on Internet Multimedia Services Architecture and Applications. Piscataway: IEEE Press, 2009: 223-228.
[20] CAMENISCH J, STADLER M, CAMNENISCH J, *et al*. Proof systems for general statements about discrete logarithms [R]. [S. l.]: Institut für Theoretische Informatik, ETH Zurich, 1997.
[21] WANG Xu-an, YANG Xiao-yuan. On DDos attack against proxy in proxy re-encryption and proxy re-signature[C]//Proc of the 9th IEEE International Conference on Computer and Information Technology. Washington DC: IEEE Computer Society, 2009: 213-218.
[22] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology. Berlin: Springer-Verlag, 1985: 47-53.
[23] HONG Xuan, LONG Yu. A novel unidirectional proxy re-signature scheme and its application for MANETs[J]. Journal of Computers, 2012, 7(7): 1796-1800.
[24] LIN IS. Multi-agent designated proxy re-signature scheme[EB/OL]. (2012-08-28). http://etd.lib.nsysu.edu.tw/ETD-db/ETD-search/view_etd?URN=etd-0828112-101715.
[25] GOLDWASSER S, MICALI S, RIVEST R L. A digital signature scheme secure against adaptive chosen-message attacks [J]. SIAM Journal on Computing, 1988, 17(2): 281-308.
[26] 唐鹏. 浅析我国电子政务内、外网 CA 认证架构体系[EB/OL]. (2012-08-14). http://www.stateca.gov.cn/NewsInfo.aspx.