新型可授权的秘密双向认证协议

温雅敏[1] 龚 征[2]
(广东商学院数学与计算科学学院 广州 510320)[1] (华南师范大学计算机学院 广州 510631)[2]

摘 要 秘密双向认证协议(又被称为秘密握手)允许同一组织内群成员间进行匿名的相互认证和通信,但允许群成员把认证能力临时授权给一个可信代理者的功能实现并没有深入研究。为了实现更有效的可授权功能,提出了一个新型可授权的秘密双向认证协议。在该协议中,允许组织外一个被授权且可信的代理者和组织内的成员完成一次成功的秘密认证和通信。基于新的 $k+1$ 平方根和离散对数表示问题的困难性假设,新型可授权的秘密双向认证协议在随机预言机模型下证明是安全的,并且在计算开销上具备一定的优势。

关键词 授权,隐私保护,双向认证,代理,不可关联性
中图法分类号 TP309.7 **文献标识码** A

New Delegatable Private Mutual Authentication Protocol

WEN Ya-min[1] GONG Zheng[2]
(School of Mathematics and Computational Science, Guangdong University of Business Studies, Guangzhou 510320, China)[1]
(School of Computer Science, South China Normal University, Guangzhou 510631, China)[2]

Abstract Private mutual authentication (or Secret handshake scheme) was proposed for anonymous bi-directional authentication among group members from the same organizations. However, the delegation functionality is not deeply studied which allows a group member to delegate his authentication rights to temporary proxies. For solving this problem more efficiently, a new delegatable private mutual authentication protocol was presented. A temporary proxy can act on behalf of his delegator and accomplish a successful secret handshake with the other member. Based on the difficulty assumptions of the $k+1$ square roots and discrete logarithm representation problems, our proposal is proven secure under the random oracle model. Compared with the related schemes, the performance of our new scheme is competitive.

Keywords Delegation, Privacy preserving, Mutual authentication, Proxy, Unlinkability

1 引言

考虑这样一个应用场景,假设一个大型的拍卖公司(如北京保利)的一个拍卖代理 Alice 试图通过公开网络与在该公司注册的拍卖客户(例如,Bob)进行秘密通信。在这个通信过程中,Alice 必须确认与她通信的另一方 Bob 确实是该拍卖公司的注册客户才能向 Bob 暴露她从属于拍卖公司的信息。也就是说,当且仅当 Bob 是该拍卖公司的合法客户时,而 Bob 也确认 Alice 是其注册的拍卖公司的合法的拍卖代理时,Alice 才能和 Bob 相互秘密认证成功。拍卖公司的代理和客户之间的双向通信是秘密进行的,他们组织身份(拍卖公司)的暴露在实际应用中有时是无法接受的。因此,对于这类隐私保护要求更强的敏感应用来说,需要能实现组织隐藏的秘密双向认证协议。

秘密握手(Secret handshakes)正是为了解决上述秘密双向认证问题而提出的新技术,最早是由 Balfanz[1] 等人于 2003 年第一次提出,并给出了简单的方案实现,它的基本功能是允许从属于同一个组织的不同成员间能秘密地进行相互认证及通信。随后,有许多基于不同密码学技术实现的两方秘密握手方案被陆续提出,如基于"CA-不经意公钥加密"[2]、基于 ElGamal 签名和数字签名算法(DSA)构建的方案[3]以及基于 RSA 的方案[4]等。如果同一个用户所执行的多次双向认证实例是不能关联的,则实现的是秘密握手方案的不可关联性。上述方案都是通过伪名证书的一次性使用实现了秘密握手方案的不可关联性。基于可重用证书实现不可关联秘密握手方案则能够减少一次性伪名证书带来的存储和计算开销,Xu 和 Yung[5] 尝试构建了第一个基于可重用的证书,实现了不可关联的秘密握手方案,但他们的方案实现的是更弱的匿名定义。结合 Balfanz 等人的方案[1]和盲化技术,陆续有一些基于可重用证书的不可关联方案被提出[6-9]。上述这些方案都是在随机预言机模型下实现可证安全的。第一个在标准模型下证明安全的基于可重用证书实现的秘密握手方案是由 Ateniese 等人提出的动态和模糊的秘密握手方案[10],该方案推广了秘密握手的功能,实现了更加灵活的秘密双向认证策略。继文

到稿日期:2012-08-20 返修日期:2012-11-12 本文受国家自然科学基金项目(61100201,11101096),广东省自然科学基金(S2012040006711,S2012010010376),广东省教育厅育苗工程(LYM11053,LYM11068),广东商学院校级科研项目(11BS41301)资助。
温雅敏(1981-),女,博士,讲师,主要研究方向为密码学与信息安全,E-mail:yamin.wen@gmail.com;龚 征(1981-),男,博士,副教授,主要研究方向为信息系统安全。

献[10]之后，Jarecki 和 Liu 基于公钥广播加密构造了实现撤销功能的不可关联方案[11]。此外，在 Ateniese 等人方案的基础上，Sorniotti 和 Molva 也陆续提出了类似功能的双向认证方案[12-14]。借助消息恢复的群签名方案，Kawai 等人[15]设计了支持强匿名性的秘密握手方案。在 2009 美密会上，Jarecki 和 Liu[16]基于条件不经意传输的思想，构造了可同时支持撤销和追踪功能的秘密双向认证协议(Private mutual authentication)。在这两篇文献[15,16]核心思想的启发下，Wen 和 Zhang 构造了支持后向不可关联的可撤销的秘密握手方案[17]。

在实际应用中，很多密码学系统要求能提供用户的临时授权功能。例如，代理签名[18]，允许一个代理者能够代表他的授权者进行签名；群签名[19]，可以看作一个群管理中心把群的签名权利授权给群成员的签名。支持授权功能的匿名证书系统[20,21]也被陆续提出。在现有关于秘密握手方案的文献中，大多数都是围绕两方秘密双向认证的基本功能进行设计和完善的，对于可授权的功能实现没有深入的研究，而在秘密双向认证的应用中，用户的临时授权也是非常有用的。例如，对于本文开头介绍的应用场景，拍卖代理 Alice 与她的客户 Bob 采用基本的秘密双向认证协议处理拍卖业务，如果 Alice 临时有急事或者需要出差，而她正好有紧急业务需要与 Bob 进行协商处理，这时她可以委托一个可信的第三方 Peter 作为她的临时代理人与 Bob 通信来处理紧急业务。为了保证拍卖机构组织的隐私性，代理人 Peter 和 Bob 之间的通信认证也需要执行秘密双向认证协议。为了实现秘密握手的授权功能，最直接的方法是让一个授权者直接寻找与他同属于一个组织的成员作为他的临时代理。但是这个直接的方法违反了秘密握手的安全要求，因为一个组织的不同成员之间彼此都是匿名的。一般情形下，授权人 Alice 和代理人 Peter 从属于不同的机构，Alice 运用自己的群证书把群成员的握手权利临时授权给 Peter。显然，Peter 和 Bob 之间执行的秘密握手协议也必须达到秘密双向认证的安全要求。Wen 和 Zhang 在文献[22]中首次实现了具有可授权功能的秘密握手方案，但其双线性对的计算开销相对较大。本文在文献[22]的基础上，基于新的 $k+1$ 平方根困难性假设构造了一个新型的可授权秘密双向认证协议，其通过减少在线双线性对的计算量提高了协议的计算性能。

2 预备知识

2.1 双线性对

令 G 是素数阶 p 的椭圆曲线循环加法群，其中 P 是 G 的生成元。如果以下 3 个条件都满足，则一个单向映射 $e:G\times G\rightarrow G_T$ 被称为一个双线性对。

a)双线性性：任意 $P\in G$ 是 G 的生成元，且 $a,b\in Z_p^*$，都满足 $e(aP,bP)=e(P,P)^{ab}$。

b)非退化性：即 $e(P,P)\neq 1$。换言之，如果 P 生成 G，则 $e(P,P)$生成 G_T。

c)可计算性：对所有 $u,v\in G$，总存在一个算法能有效计算单向映射 $e(u,v)$。

2.2 复杂性假设

接下来介绍本文方案所涉及的困难性问题和复杂性假设。

$k+1$ 平方根问题($k+1$-Square Roots Problem，$k+1$-SRP)[23]：令(G,G_T)是两个素数阶为 p 的循环群，对于任意一个整数 k 和 $x\in_R Z_p^*$，$P\in G$，给定以下信息，

$$\{P,Q=xP,h_1,\cdots,h_k\in Z_p^*,(h_1+x)^{\frac{1}{2}}P,\cdots,(h_k+x)^{\frac{1}{2}}P\}$$

对某个 $h\notin\{h_1,\cdots,h_k\}$，需要计算输出某个$(h+x)^{\frac{1}{2}}P$。

$k+1$-SR 假设：如果不存在多项式时间算法能以不可忽略的概率解出 $k+1$ 平方根问题，我们认为这是一个 $k+1$ 平方根假设。

离散对数表示问题(Discrete Logarithm Representation Problem，DLRP)[24]：令 G_T 是素数阶为 p 的循环群，$g_1,\cdots,g_k\in G_T$ 是 G_T 的 $k\geqslant 2$ 个生成元。把$(g_1,\cdots,g_k)$和 $h\in G_T$ 作为均匀分布的输入，输出唯一的一个 k 元组$(a_1,\cdots,a_k)$，称之为 h 关于生成元$(g_1,\cdots,g_k)$的表示，满足等式 $h=\prod_{i=1}^{k}g_i^{a_i}$。

DLR 假设：如果不存在多项式时间算法能以不可忽略的概率解出离散对数表示问题(DLRP)，我们认为这是一个 DLR 假设。正如文献[24]的描述，离散对数表示问题在计算复杂度上等价于离散对数问题。

2.3 定义与安全要求

秘密握手最初的定义是允许同一组织的不同群成员的秘密认证，由于可授权功能的加入，原先秘密握手方案的核心握手算法(Handshake)的功能将随之改变，代理人和群成员之间的认证可更准确地定义为代理双向认证(Proxy Mutual Authentication)。结合基本的秘密握手定义[1,10]以及可授权秘密握手[22]的定义，本文对可授权的秘密双向认证协议的定义和安全要求给出重新总结和回顾：

(1)系统建立(Setup)：该算法选择一个安全参数 κ 输入后，输出公开的参数 *params*，系统参数可以被接下来创建的群组织所共用。

(2)组织创建(CreateGroup)：该算法由群管理中心(Group Authority，GA)运行密钥生成算法，以建立一个组织，输入公开参数 *params*，群组织创建算法输出群的公私钥对(gpk,gsk)。

(3)成员加入(AddMember)：该算法是由 GA 和一个用户(如 U)共同交互完成的两方协议。由 GA 对用户真实身份进行检查和验证。如果用户符合加入组织 G_U 的条件并通过验证，GA 将利用群密钥对(gpk_U,gsk_U)为用户颁发群证书 $cred_U$，使用户成为该组织的合法成员。

(4)授权(Delegation)：该算法完成一个群成员 U 作为授权者向一个可信任的临时代理者 TP 实施授权的功能。算法输入授权者 U 的群证书 $cred_U$ 以及授权书 ω(包含代理者公钥及对代理者权限的相关信息)，U 首先向 TP 零知识证明他持有一个合法的群证书 $cred_U$，以证明他是组织 G_U 的合法成员。TP 使用组织 G_U 的群公钥 gpk_U 对这个零知识证明进行验证，在不知道授权者 U 真实身份的情况下，确认 U 是组织 G_U 的合法成员。与此同时，TP 从这个非交互式零知识证明中获得 U 对 ω 签发的授权证书 Del-Cred。作为可公开验证的授权书，ω 不应该泄漏关于 U 和 TP 的任何隐私信息，因而可以是公开的。另外，由于 TP 并不是合法的群组织成员而仅是临时的代理者，基于安全性考虑，TP 行使代理认证的能力应该是受到一定限制的。因此，在本文的方案中，我们限定

一个授权证书仅能使用一次。如果授权者 U 允许代理者代理多次，则需要为代理者签发多个授权证书。

(5)代理双向认证(Proxy Mutual Authentication)：该算法是由一个被授权的临时代理者 TP 和另一个群成员 V 执行的具有代理功能的秘密双向认证协议。假设代理者 TP 作为协议的发起方，而 V 作为响应方。算法输入除了包括一些公开参数以及当前状态的公开信息之外，协议参与方需要输入各自的秘密信息。如果 TP 的授权者与 V 来自于同一个组织，则算法参与方各自输出为"1"，表明认证成功；否则，算法输出为"0"。

基于增加的授权和代理双向认证算法，本节进一步总结一个安全的可授权秘密双向认证协议必须达到的几个基本的安全要求：a)完全性：对于授权 Delegation 算法，如果临时代理者 TP 充分可信且授权者 U 确实是其宣称组织的合法群成员，那么 TP 总能获得一个有效的授权证书。进而，在代理双向认证算法中，如果 TP 的授权者与另一个参与方法属于同一个组织时，则代理双向认证协议总能执行成功。b)防伪造性：对于 Delegation 算法，任何攻击者都不能伪造成一个合法的群成员向代理者进行有效的授权。此外，任一攻击者也不能伪造成一个有效的代理者执行代理双向认证算法。这个安全要求还蕴含着，即使作为代理者真正的授权者 U 也不能伪造出他的临时代理者 TP 执行代理双向认证过程的副本，从而可以保护代理者不被恶意的授权者诬陷。c)防侦测性：任一攻击者试图作为参与方执行秘密双向认证协议来侦测出对方的秘密信息是不能成功的。虽然在代理双向认证算法中 TP 作为代理者的身份是公开的，但任一攻击者都不能识别出 TP 的授权者(U)的组织信息。另外，没有得到合法授权的攻击者不能成为一个合法的代理者，因而也不能通过参与代理认证算法成功地识别出另一个群成员(V)的组织信息。对于授权 Delegation 算法，临时代理者除了知道授权者的组织信息外，不能侦测出其他身份信息。d)不可关联性：攻击者不能成功地识别出两次秘密认证实例的关联性。我们限制一份授权证书仅能使用一次，以确保授权者的不可关联性，而同一个临时代理者所执行的多次代理服务很容易被攻击者关联。但是，代理者常常是为不同组织群成员提供代理服务的第三方服务机构，因而，攻击者只能关联到同一个代理者的多次代理服务，并不能从中推导和关联出其他任何信息，包括某一个代理者是否为同一个授权者服务等信息。

3 新型可授权的秘密双向认证协议

为了实现可授权代理的秘密双向认证协议，一个临时代理者首先需要从他的授权者那里获得一个合法的授权证书。假设由一个可信的第三方代理服务中心推荐一个代理实体来临时完成授权者的任务，但这个代理必须能验证授权者的合法群成员身份。因此这个授权证书对于代理者而言是一个可公开验证的签名，本质上是由授权者向代理者执行匿名群认证的过程。在此，假设授权者和代理者通过一个秘密通道进行通信。然后，代理者再运用持有的授权证书与另一个群成员执行代理双向认证协议。在代理认证过程中，代理者需证明其拥有合法的授权证书，而另一个群成员也需证明其拥有合法的群证书。类似地，本文提出的方案将借鉴文献[9,22]中使用的可消息恢复但不能公开验证的"签名"来实现双方的证书零知识证明。当且仅当协议参与方所代表的组织是同一个时，消息才能正确地恢复并且通过验证。基于新的 $k+1$-SR 困难性假设，本文构造了一个新型的可授权的秘密双向认证协议(Delegatable Private Mutual Authentication，DPMA)。DPMA 方案的一个具体实现描述如下：

(1)系统建立(Setup)：给定一个安全参数 κ，执行 $Setup(1^\kappa)\rightarrow params=(p,G,G_T,P,e,H,F,F^{-1})$。其中，$G$ 是素数阶为 p 的椭圆曲线加法循环群，P 是群 G 的一个生成元。$e:G\times G\rightarrow G_T$ 是双线性对。$H:\{0,1\}^*\rightarrow Z_p^*$ 是密码学哈希函数。$F:G\rightarrow Z_p^*$ 是从 G 映射到 Z_p^* 的一一映射函数。而 $F^{-1}:Z_p^*\rightarrow G$ 是 F 的逆映射。

(2)组织创建(CreateGroup)：GA 随机选取 $gsk=s\leftarrow_R Z_p^*$ 作为该群组织的群私钥，然后输出群公钥 $gpk=sP$。

(3)成员加入(AddMember)：为了把用户 U 加入到组织使之成为组织的合法成员，同时又保证用户参与的秘密性和隐私性，本文将利用文献[21]中的安全两方计算协议使得用户 U 的群证书由 GA 和 U 共同参与生成，而不是采用让 GA 直接颁发的方式。用户 U 首先生成自己的私钥 $x_U\in_R Z_p^*$ 并作为两方计算协议的一个秘密输入，然后 GA 把自己的群私钥 $s\in_R Z_p^*$ 作为两方计算协议的另一个秘密输入，基于加法同态加密方案的特性，经过 3 轮的两方交互和验证过程，用户在最后一轮可以去盲计算出秘密的群证书 $cred_U=(x_U+s)^{\frac{1}{2}}P$(详细的两方安全计算协议可以参考文献[21])，这类似于由 GA 和用户 U 共同产生的短签名[23]。用户 U 通过验证等式 $e(cred_U,cred_U)\stackrel{?}{=}e(P,P)^{x_U}e(P,sP)$ 来确认群证书的正确性。

(4)授权(Delegation)：如果 TP 被可信的第三方代理服务中心选择成为群成员 U 的临时代理，U 将执行 Delegation 算法为 TP 签发一个授权证书。TP 的可信性会由 U 进行预先验证。不失一般性，代理 TP 并不是其授权者 U 所在组织 G_U 的群成员，TP 仅仅临时代表 G_U 的群成员 U 来参与握手认证。为了明确代理的职能与权限，U 需要为 TP 定义一个可撤销的授权书(标记为 ω)。授权书 ω 通常有固定的格式，包含授权代理的相关信息，例如代理者 TP 的公钥、代理序列号和有效期限等。为了保证匿名性，ω 不能包含任何关于 U 的身份和群组织信息，也不包含代理者的其他信息。在此，详细描述 U 执行以下几个步骤为 TP 签发一个授权证书 Del-Cred。

• U 首先验证 TP 的身份，TP 持有一个公私钥对($x_{TP}\in_R Z_p^*$，$y_{TP}=x_{TP}P$)以及对应的公钥证书。如果 TP 经验证是可信的，U 将签发授权证书给 TP，与此同时也向 TP 证明他是组织 G_U 的合法群成员身份。

a)U 选择一个随机数 $k_U\in_R Z_p^*$，然后计算 $\rho=k_U cred_U$，$\theta=e(P,P)^{k_U^2}$。

b)U 接着随机选取 $l_1,l_2\in_R Z_p^*$，并计算 $L_1=e(P,P)^{l_1}e(P,gpk_U)^{l_2}$，$L_2=e(P,P)^{l_2}$。

c)U 计算 $s_1=f(L_1)k_U^2x_U+H(\omega)l_1$ 以及 $s_2=f(L_1)k_U^2+H(\omega)l_2$。

d)U 最后把 Del-Cred=$(\omega,\rho,\theta,L_1,L_2,s_1,s_2)$ 发送给 TP。

• 接收到 Del-Cred 之后，TP 使用 G_U 的群公钥 gpk_U 验证下面两个等式，以确认授权证书的有效性，同时也验证了 U

的群成员身份。

$e(P,P)^{s_1}e(P,gpk_U)^{s_2}\stackrel{?}{=}e(\rho,\rho)^{f(L_1)}L_1^{H(\omega)}$ 和 $e(P,P)^{s_2}\stackrel{?}{=}\theta^{f(L_1)}L_2^{H(\omega)}$，一旦代理者 TP 接受了授权证书之后，他将计算代理认证密钥 $D_1=s_1+x_{TP}H(\omega)$ 和 $D_2=s_2+x_{TP}H(\omega)$。

(5)代理双向认证(Proxy Mutual Authentication)：假设临时代理者 TP 需要代表他的授权者 U 与另一个群成员 V 进行秘密通信，TP 和 V 在不泄漏双方所代表的组织的前提下，将执行以下 3 轮步骤进行秘密的双向认证，进而协商一个会话密钥进行后续的通信。协议的详细描述如下：

I. $TP\rightarrow V$: $\{\omega,L_1,L_2,\rho,\theta,R_{P1},R_{P2},C_P\}$

a)TP 随机选择 $t_{P1},t_{P2}\in_R Z_p^*$，然后计算 $T_{P1}=e(P,P)^{t_{P1}}e(P,gpk_U)^{t_{P2}}$，$T_{P2}=e(P,P)^{t_{P2}}$。

b)TP 选取 $\lambda_P\in_R Z_p^*$ 并计算 $m_P=\lambda_P P$，接着生成 $C_P=H(params\parallel gpk_U\parallel T_{P1}\parallel T_{P2})\oplus F(m_P)$。

c)TP 计算 $R_{P1}=t_{P1}-D_1C_P$ 以及 $R2=t_{P2}-D_2C_P$，最后把 $\{\omega,L_1,L_2,\rho,\theta,R_{P1},R_{P2},C_P\}$ 发送给 V。注意，这是对代理密钥 (D_1,D_2) 的一种知识证明，也可以看作是基于 DLRP 构造的不能公开验证可消息恢复的签名。TP 作为签名者向接收者证明他知道代理密钥 (D_1,D_2)，且满足等式 $e(P,P)^{D_1}e(P,gpk_U)^{D_2}=e(\rho,\rho)^{f(L_1)}\cdot L_1^{H(\omega)}\cdot(e(y_{TP},P)\cdot e(y_{TP},gpk_U))^{H(\omega)}$。

同时也证明了 $s_2\neq 0(D_2\neq x_{TP}H(\omega))$，即证明 D_2 满足等式 $e(P,P)^{D_2}=\theta^{f(L_1)}L_2^{H(\omega)}e(P,y_{TP})^{H(\omega)}$。因此，只有持有合法的授权证书的用户才能够提供这样的知识证明。

II. $V\rightarrow TP$: $\{\rho_V,R_{V1},R_{V2},C_V,resp_V\}$

a)接收到 $\{\omega,L_1,L_2,\rho,\theta,R_{P1},R_{P2},C_P\}$ 之后，V 使用他自己组织的群公钥 gpk_V 以及 ω 中所包含的 TP 的公钥，按照下面的等式恢复出一个消息 $\widetilde{m}_P$。

$\widetilde{T}_{P1}=e(P,P)^{R_{P1}}e(P,gpk_V)^{R_{P2}}\cdot(e(\rho,\rho)^{f(L_1)}(L_1\cdot e(y_{TP},P)\cdot e(y_{TP},gpk_U))^{H(\omega)})^{C_P}$

$\widetilde{T}_{P2}=e(P,P)^{R_{P2}}\cdot(\theta^{f(L_1)}\cdot(L_2\cdot e(P,y_{TP}))^{H(\omega)})^{C_P}$

$\widetilde{m}_P=F^{-1}(H(params\parallel gpk_V\parallel\widetilde{T}_{P1}\parallel\widetilde{T}_{P2})\oplus C_P)$

b)V 接着随机选取 $k_V\in_R Z_p^*$，计算 $\rho_V=k_V cred_V$，$\theta_V=e(P,P)^{k_V^2}$。

c)然后随机选取 $t_{V1},t_{V2}\in_R Z_p^*$，计算出 $T_{V1}=e(P,P)^{t_{V1}}e(P,gpk_V)^{t_{V2}}$，$T_{V2}=e(P,P)^{t_{V2}}$。

d)接着类似地选择 $\lambda_V\in_R Z_p^*$，产生随机消息 $m_V=\lambda_V P$ 并生成 $C_V=H(params\parallel gpk_V\parallel T_{V1}\parallel T_{V2})\oplus F(m_V)$。

e)V 计算生成 $R_{V1}=t_{V1}-k_V^2x_VC_V$ 和 $R_{V2}=t_{V2}-k_V^2C_V$。

f)V 需要验证授权书 ω 的有效性，例如序列号是否被撤销以及是否过有效期。如果 ω 已经失效了，则 V 将随机生成上述元素并且返回一个随机的验证响应值 $resp_V\leftarrow_R Z_p^*$；否则，V 将计算响应值 $resp_V=H(\lambda_V(\widetilde{m}_P)\parallel m_V\parallel 0)$。最后，$V$ 把 $\{\rho_V,\theta_V,R_{V1},R_{V2},C_V,resp_V\}$ 发送给 TP。

III. $TP\rightarrow V$: $\{resp_P\}$

a)从 V 处接收到 $\{\rho_V,R_{V1},R_{V2},C_V,resp_V\}$ 之后，TP 可以使用他的授权者的群公钥 gpk_U 通过下面的等式恢复出一个消息 $\widetilde{m}_V$。

$\widetilde{T}_{V1}=e(P,P)^{R_{V1}}e(P,gpk_U)^{R_{V2}}e(\rho_V,\rho_V)^{C_V}$

$\widetilde{T}_{V2}=e(P,P)^{R_{V2}}\theta^{C_V}$

$\widetilde{m}_V=F^{-1}(H(params\parallel gpk_U\parallel\widetilde{T}_{V1}\parallel\widetilde{T}_{V2})\oplus C_V)$

b)TP 接着可以通过下面的等式验证响应值 $resp_V$，$resp_V\stackrel{?}{=}H(\lambda_P(\widetilde{m}_V)\parallel\widetilde{m}_V\parallel 0)$，如果等式验证成立，则 TP 将输出“1”并计算 $resp_P=H(\lambda_P(\widetilde{m}_V)\parallel m_P\parallel 1)$ 发送给 V；否则，TP 输出“0”且并返回一个随机数 $resp_P\leftarrow_R Z_p^*$ 给 V。

c)最后，V 类似地通过下面的等式验证 TP 的响应值 $resp_P\stackrel{?}{=}H(\lambda_V(\widetilde{m}_P)\parallel\widetilde{m}_P\parallel 1)$。如果等式成立，$V$ 输出“1”表明完成了一次成功的代理双向认证协议；否则，V 将输出“0”。

4 安全与性能分析

本节将对提出的新型可授权的秘密双向认证协议进行安全和性能分析。密码学协议的安全性证明一般通过可证明安全的方法，将攻击者成功的概率转换为针对某一困难问题(通常是 NP 或 NPC 问题)的求解。目前常用的可证明安全模型有随机预言机和标准模型两大类。本文通过采用随机预言机模型，将攻击者的成功概率归约为对 $k+1$-SR 和 DLR 困难问题的求解。

4.1 安全分析

引理 1 DPMA 方案的授权 Delegation 算法能实现完全性。

证明：在 DPMA 方案的授权阶段，如果临时代理者 TP 和授权者 U 都是诚实可信的，则 TP 能以概率趋近于 1 获得一个有效的关于授权 ω 的授权证书 Del-Cred。即使代理者 TP 不知道授权者 U 的确切身份，TP 也能确认 U 是所宣称的组织 G_U 的合法成员。详细的证明可以通过下面的等式加以验证。

$$\begin{aligned}
&e(P,P)^{s_1}e(P,gpk_U)^{s_2}\\
&=e(P,P)^{f(L_1)k_U^2x_U+H(\omega)l_1}e(P,gpk_U)^{f(L_1)k_U^2+H(\omega)l_2}\\
&=e(P,P)^{f(L_1)k_U^2x_U}e(P,P)^{H(\omega)l_1}\cdot e(P,sP)^{f(L_1)k_U^2}e(P,gpk_U)^{H(\omega)l_2}\\
&=e(P,P)^{f(L_1)k_U^2(x_U+s)}(e(P,P)^{l_1}e(P,gpk_U)^{l_2})^{H(\omega)}\\
&=e(k_U(x_U+s)^{\frac{1}{2}}P,k_U(x_U+s)^{\frac{1}{2}}P)^{f(L_1)}L_1^{H(\omega)}\\
&=e(\rho,\rho)^{f(L_1)}L_1^{H(\omega)}\\
&e(P,P)^{s_2}=e(P,P)^{f(L_1)k_U^2+H(\omega)l_2}\\
&\quad=(e(P,P)^{k_U^2})^{f(L_1)}(e(P,P)^{l_2})^{H(\omega)}\\
&\quad=\theta^{f(L_1)}L_2^{H(\omega)}
\end{aligned}$$

定理 1 DPMA 方案代理双向认证协议能实现完全性。

证明：如果临时代理者 TP 的授权人 U 和 V 属于同一个组织，则意味着他们的群公钥是相等的，即 $gpk_U=gpk_V=sP$。这使得 TP 和 V 都可以使用正确的群公钥从修正的消息恢复签名中恢复出对方的原始消息。从而，通信双方计算生成的对应的响应值都能够通过验证，使得秘密双向认证成功。结合引理 1 的推导，详细的证明可以通过下面的等式加以验证。

$$\begin{aligned}
\widetilde{T}_{P1}&=e(P,P)^{R_{P1}}e(P,gpk_V)^{R_{P2}}\cdot(e(\rho,\rho)^{f(L_1)}\cdot(L_1\cdot e(y_{TP},P)\cdot e(y_{TP},gpk_U))^{H(\omega)})^{C_P}\\
&=e(P,P)^{t_{P1}-D_1C_P}e(P,sP)^{t_{P2}-D_2C_P}\cdot(e(\rho,\rho)^{f(L_1)}L_1^{H(\omega)}(e(y_{TP},P)e(y_{TP},gpk_U))^{H(\omega)})^{C_P}\\
&=e(P,P)^{t_{P1}}e(P,sP)^{t_{P2}}e(P,P)^{-(s_1+x_{TP}H(\omega))C_P}\cdot e(P,sP)^{-(s_2+x_{TP}H(\omega))C_P}\cdot(e(\rho,\rho)^{f(L_1)}L_1^{H(\omega)})^{C_P}\cdot(e(y_{TP},P)e(y_{TP},gpk_U))^{H(\omega)})^{C_P}
\end{aligned}$$

$$=e(P,P)^{t_{P1}}e(P,sP)^{t_{P2}}e(P,P)^{-s_1C_P}e(P,sP)^{-s_2C_P}\cdot(e(\rho,\rho)^{f(L_1)}L_1^{H(\omega)})^{C_P}e(P,P)^{-x_{TP}H(\omega)C_P}e(P,sP)^{-x_{TP}H(\omega)C_P}\cdot(e(y_{TP},P)e(y_{TP},gpk_U))^{H(\omega)})^{C_P}$$

$$=e(P,P)^{t_{P1}}e(P,sP)^{t_{P2}}=T_{P1}$$

$$\tilde{T}_{P2}=e(P,P)^{R_{P2}}\cdot(\theta^{f(L_1)}\cdot(L_2\cdot e(P,y_{TP}))^{H(\omega)})^{C_P}$$

$$=e(P,P)^{t_{P2}-D_2C_P}\cdot(\theta^{f(L_1)}\cdot L_2^{H(\omega)})^{C_P}\cdot e(P,y_{TP})^{H(\omega)C_P}$$

$$=e(P,P)^{t_{P2}}e(P,P)^{-s_2C_P}e(P,P)^{-x_{TP}H(\omega)C_P}\cdot(\theta^{f(L_1)}\cdot L_2^{H(\omega)})^{C_P}\cdot e(P,y_{TP})^{H(\omega)C_P}$$

$$=e(P,P)^{t_{P2}}=T_{P2}$$

定理 2 基于 k+1-SR 和 DLR 假设，DPMA 方案在随机预言机模型下证明满足防伪造性。

证明：如果一个攻击者 A 在多项式时间 t 内以不可忽略的概率 ε 成功地攻破了 DPMA 方案的防伪造性，则我们可以利用 A 衍生出一个算法 B 能在多项式时间内以不可忽略的概率求解出 k+1-SR 和 DLR 问题。假设 B 面对一个 k+1-SR 问题，B 可以模拟 DPMA 方案的组织创建、成员加入、授权和代理双向认证算法以及作为随机预言机的哈希函数。A 将适应性地访问上述算法预言机，预言机根据不同的请求模拟对应的算法。为了充分发挥 A 的攻击能力，B 在模拟上述预言机行为时，返回的值和真正的算法产生的回答是不可区分的。因为，本方案颁发的群证书是在张等人提出的短签名[23]基础上修改生成的，详细的模拟方法可以参考文献[23]的证明过程。

经过上述预言机的训练之后，攻击者 A 试图伪造为组织 G^* 中的合法群成员参与到秘密双向认证协议中。为了成功地完成伪造，攻击者 A 在上述算法的执行过程中不得不伪造关于正确群证书 $cred_A$ 的非交互式知识证明。这也意味着，A 在没有获得秘密的群证书 $cred_A$ 的前提下伪造出有效的不具有公开验证但可消息恢复的“签名”，而这类“签名”能在交互式双向认证阶段通过验证。因为这类签名是基于离散对数表示问题(DLRP)进行构造的，攻击者 A 要证明持有秘密值 $(k_A^2x_A,k_A^2)$ 且满足等式：

$$e(\rho_A,\rho_A)=e(P,P)^{k_A^2x_A}e(P,sP)^{k_A^2}$$

式中，$\rho_A=k_Acred_A$，而 sP 是组织 G^* 的群公钥。根据分叉归约引理[25]，成功的伪造者 A 可以被 B 归约为一个提取器以不可忽略的概率获得 $(k_A^2x_A,k_A^2)$ 解决 DLR 问题。进而，B 也就可以计算得出签名 $cred_A=k_A^{-1}\rho_A$，以不可忽略的概率解决了 k+1-SR 问题。

另一方面，攻击者会试图伪造为一个合法的授权者或者是有效的代理者。在 DPMA 方案的 Delegation 算法中，一个合法的群成员 U 通过为其代理者签发授权证书 Del-Cred 以证明 U 持有组织 G^* 的 GA 所签发的有效群证书。类似地，Del-Cred 是关于正确群证书 $cred_U$ 的非交互式知识证明，本质上是基于 DLR 问题生成的对授权书 ω 的可验证签名。因此，如果攻击者 A 想要成功伪造成一个合法群成员实现授权功能，则 A 不得不伪造关于正确群证书 $cred_A$ 的可验证签名。这样，B 也将类似地利用 A 作为提取器解决 DLR 和 $(k+1)$-SR 问题。同时，如果没有有效的授权证书 Del-Cred，攻击者 A 要生成正确的代理认证密钥也是不可行的，从而也就不能伪造为一个有效的代理者执行代理双向认证协议。综上所述，基于 k+1-SR 和 DLR 假设，可以推导出这与攻击者能成功伪造的假设是相互矛盾的。定理得证。

定理 3 基于 k+1-SR 和 DLR 假设，DPMA 方案在随机预言机模型下证明满足防侦测性和不可关联性。

证明：假设存在一个攻击者 A 能以不可忽略的概率 $\frac{1}{2}+\varepsilon$ 攻破 DPMA 方案的防侦测性，则 A 可用于构造一个算法 B 以不可忽略的概率解决 DLR 和 k+1-SR 问题。

我们首先假设存在一个模拟器 R 可以模拟输出双向认证的协议副本。如果 A 想要攻破防侦测性，则他必须能够以不可忽略的概率优势 ε 辨别出一个握手实例是由模拟器 R 所产生的还是由一个真实的群成员产生的。因为攻击者 A 至少有 $\frac{1}{2}$ 的概率可以猜对，则 A 能猜对的概率为 $\frac{1}{2}+\varepsilon$。在一个双向认证实例中，一个诚实群成员参与认证的副本包含有这个群成员群证书完全盲化后的随机信息以及关于群证书的部分知识证明。模拟器 R 随机产生的协议副本和一个诚实的群成员(V)生成的真正的协议副本是不可区分的。因此，攻击者 A 必须能辨别出由 R 产生的随机值 $resp_V=\mathrm{SIM}(params)$ 以及由 V 实际计算的值 $resp_V=H((\tilde{m}_A)^{\lambda_V}\|m_V\|0)$。但是，这只能依赖于 A 参与双向认证协议时能够伪造出正确的对消息 m_A 的可消息恢复的签名，并使得 V 在收到该签名后能正确地恢复出原始消息 $\tilde{m}_A=m_A$。除此之外，A 也应该能够恢复出正确的 m_V，验证 $resp_V$ 并返回正确的响应值 $resp_A=H((\tilde{m}_V)^{\lambda_A}\|m_A\|1)$。因此，我们可以按照类似于定理 2 的方式利用 A 作为提取器以不可忽略的概率优势解决 DLR 和 k+1-SR 问题。另一方面，假设存在一个模拟器 R 可以产生授权书 ω 并模拟一个代理生成代理双向认证协议副本。尽管 ω 暴露了代理的事实，但它不会泄露其他任何秘密信息。因此，基于 DLR 和 k+1-SR 困难性假设，攻击者 A 参与代理双向认证协议时想要辨别出这个认证实例是由一个模拟器 R 产生的还是一个真实的代理者产生的也是不可行的。

不可关联性的安全证明和防侦测性有些类似的地方，可以看作是攻击者对两次试图攻破防侦测性所执行的握手实例进行辨别，让攻击者确定这两次握手实例是否为同一个群成员所为。一般情况下，仅为攻击者提供两个握手实例的副本，让攻击者对这两个握手实例的关联性进行判断。根据上一段对防侦测性的证明描述，不可关联性的证明只需要让攻击者在攻击游戏中执行两次握手实例后再进行辨别。因此，我们不再详细推导不可关联性的证明过程，仅在此简要分析 DPMA 方案的不可关联性。因为群成员每次参与双向认证协议时，都是选用不同的随机数对其可重用的群证书实施完全的盲化，甚至于这个群成员所在组织的 GA 也都无法通过监听同一个群成员产生的多个握手实例对群成员的身份进行关联。另外，在 DPMA 方案中，每一个授权证书 Del-Cred 只允许使用一次。尽管存在不同的授权书包含有同一个代理者的公钥，即同一个代理者被多个授权者授权，以实现代理服务，但是同一个代理在执行不同的握手实例时所传递的其他信息仍然是完全随机的。在方案描述中我们也提到代理者来自于一个可信的代理服务中心，同一个代理者可以为不同的授权者提供服务，可能是为同一个组织的多个群成员代理，可能是为不同的群组织中不同的群成员代理，也可能是为同一个群成员代理多次。那么，从同一个代理者的多个握手实例中猜测出对应的授权者之间的关联性是比较困难的，对不同代理

者执行的握手实例进行关联就更不可行了。定理得证。

4.2 性能分析

本节将对所提可授权的秘密双向认证方案的性能进行简要分析，并给出 DPMA 方案与其他相关方案的性能比较。为了简明起见，针对秘密双向认证方案的不同阶段分别给出计算开销，主要考虑双线性对、点乘和模幂计算的开销，详细如表 1 所列。

表 1 相关方案的性能比较

方案 \ 阶段	系统建立	组织创建	成员加入	双向认证	授权
文献[10]	$2(n+2)T_m$	—	$2T_m$	$4T_p+6T_e$	不支持
文献[22]	0	T_m	T_m	$7T_p+11T_e+5T_m$	支持
DPMA	0	T_m	T_m	$3T_p+16T_e+5T_m$	支持

表 1 中 T_p 表示椭圆曲线群上的一个双线性对运算的时间，T_m 表示椭圆曲线群上的点乘运算的时间，T_e 表示一个有限域的模幂运算的时间。令 n 表示文献[10]中的群组织名称所需的比特长度。

对于能提供授权代理功能的方案的双向认证阶段，我们给出的是代理双向认证的计算开销。从表 1 可以看出，与第一个有效的基于可重用证书的不可关联秘密握手方案[10]相比，文献[22]和 DPMA 方案在功能上具备一定的优势，可以支持授权算法和代理双向认证的功能。另外，由于Ateniese等人的方案[10]是通过名称来区分不同的群组织的，其中假设每个群组织的名称统一用 n 比特的字符串表示，因此在方案的 Setup 阶段需要 $2(n+2)$次椭圆曲线的点乘运算，并且在 CreateGroup 阶段需要每个群组织知道并保存$(n+2)$个点乘值作为群私钥为群成员签发群证书。从而，Ateniese 等人的方案[10]的应用局限于同一个大组织内不同的部门间的秘密双向认证，而不是独立的群成员之间的秘密认证。虽然 Ateniese 等人的方案[10]描述为两轮的实现，但他们的方案如果要完成真正意义的秘密认证而不是简单的密钥协商，实际上也需要通过 3 轮的交互才能实现。

相对于同样可支持授权功能的方案[22]，DPMA 方案减少了比较耗时的在线双线对运算，提高了一定的计算性能。此外，DPMA 方案多耗费的模幂运算的开销可以通过多个模幂相乘的优化算法进行优化。这样，本文的代理双向认证协议在线的计算开销可以缩减大概 $5T_e$ 的模幂运算时间。因此，基于新的困难性假设，本文提出的新型可授权秘密双向认证协议在性能上仍具有一定的优势。

结束语 本文主要提出了一个新型可授权的秘密双向认证协议，其允许群成员把他的认证通信权利临时授权给一个可信的代理者。基于对可重用证书的随机化，该方案实现了抵抗恶意 GA 的强的完全不可关联性。同时，基于 DLR 和 k +1-SR 困难性假设，DPMA 方案在随机预言机模型下是可证安全的，满足秘密双向认证协议的基本安全要求。

参 考 文 献

[1] Balfanz D, Durfee G, Shankar N, et al. Secret handshakes from pairing-based key agreements[C]// Berkeley, California, USA. Proceeding of IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2003: 180-196

[2] Castelluccia C, Jarecki S, Tsudik G. Secret handshakes from ca-oblivious encryption[C]// Jeju Island, Korea. Proceedings of ASIACRYPT 2004. Berlin/Heidelberg: Springer, 2004: 293-307

[3] Zhou Lan, Susilo W, Mu Y. Three-round secret handshakes based on elgamal and dsa[C]// Hangzhou, China. Proceedings of ISPEC 2006. Berlin/Heidelberg: Springer, 2006: 332-342

[4] Vergnaud D. RSA-based secret handshakes[C]// Bergen, Norway. Proceedings of International Workshop of Coding and Cryptography (WCC 2005). Berlin/Heidelberg: Springer, 2005: 252-274

[5] Xu Shou-huai, Yung M. K-anonymous secret handshakes with reusable credentials[C]// Washington, DC, USA. Proceedings of ACM Conference on Computer and Communications Security (CCS 2004). New York, NY, USA: ACM Press, 2004: 158-167

[6] Huang Hai, Cao Zhen-fu. A novel and efficient unlinkable secret handshake scheme[J]. IEEE Communications Letters, 2009, 13(5): 363-365

[7] Su Ren-wang. On the security of a novel and efficient unlinkable secret handshakes scheme[J]. IEEE Communications Letters, 2009, 13(9): 712-713

[8] Gu Jie, Xue Zhi. An improved efficient secret handshakes scheme with unlinkability[J]. IEEE Communication Letters, 2011, 15(2): 259-261

[9] Wen Ya-min, Zhang Fang-guo, Xu Ling-ling. Unlinkable secret handshakes from message recovery signature[J]. Chinese Journal of Electronics: 2010, 19(4): 705-709

[10] Ateniese G, Blanton M, Kirsch J. Secret handshakes with dynamic and fuzzy matching[C]// San Diego, California, USA. Proceedings of Network and Distributed System Security Symposium(NDSS 2007). The Internet Society, 2007: 159-177

[11] Jarecki S, Liu Xiao-ming. Unlinkable secret handshakes and key-private group key management schemes[C]// Zhuhai, China. Proceedings of ACNS 2007. Berlin/Heidelberg: Springer, 2007: 270-287

[12] Sorniotti A, Molva R. Secret handshakes with revocation Support[C]// Seoul, Korea. Proceedings of ICISC 2009. Berlin/Heidelberg: Springer, 2009: 274-299

[13] Sorniotti A, Molva R. A provably secure secret handshake with dynamic controlled matching [J]. Computers & Security, 2010, 29(5): 619-627

[14] Sorniotti A, Molva R. Federated secret handshakes with support for revocation [C] // Barcelona, Spain. Proceedings of ICICS 2010. Berlin/Heidelberg: Springer, 2010: 218-234

[15] Kawai Y, Yoneyama K, Ohta K. Secret handshake: strong anonymity definition and construction[C]// Xi'an, China. Proceedings of ISPEC 2009. Berlin/Heidelberg: Springer, 2009: 219-229

[16] Jarecki S, Liu Xiao-ming. Private mutual authentication and conditional oblivious transfer[C]// Santa Barbara, California, USA. Proceedings of CRYPTO 2009. Berlin/Heidelberg: Springer, 2009: 90-107

[17] Wen Ya-min, Zhang Fang-guo. A new revocable secret handshake scheme with backward unlinkability [C] // Athens, Greece. Proceedings of EUROPKI 2010. Berlin/Heidelberg: Sprin-ger, 2011: 17-30

[18] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]// Proceedings of ACM Conference on Computer and Communications Security (CCS 1996). New York, NY, USA: ACM Press, 1996: 48-57

(下转第 123 页)

3.3 文本串的搜索

文本串的搜索过程如下：

1. 将两个文本串右对齐；

2. 将模式串集中最短串与文本串右端对齐；

3. 从模式树的根节点开始，从左往右进行模式匹配操作。这步通过调用构造的 2-目标多模式树自动机来完成。

4. 根据移位函数计算出的移动位数序列，分别对文本串向右移动。当某个文本串长度不够时，在文本串左端添加空字符 null；当两个文本串的字符都是 null 时，匹配搜索结束。

4 系统测试

根据上面的工作，我们使用 VC6.0 对 Snort 里面的 Importkey()函数、MakeMr()函数和 PatternMatch()函数进行相应的修改。测试环境为：Snort2.0 默认值规则集，测试机 CPU 为 AMD5200+，内存 2G，操作系统为 WinXP。测试数据采用 1999 年美国高级研究计划局(DARPA)做 IDS 评估时所使用的数据集。分别对 AC-BM 算法、双向 AC-BM 算法、2-目标 AC-BM 算法和 3-目标 AC-BM 算法进行测试。我们主要是考虑算法的时间效能。测试结果如表 1 所列。

表 1 测试结果(单位 s)

时间	测试数据	AC-BM	双向 AC-BM	2-目标 AC-BM	3-目标 AC-BM
周一	inside. tcpdump(325M)	208.9967	169.4463	170.5543	137.4578
	outside. tcpdump(308M)	196.1908	152.2133	149.4321	101.4376
周二	inside. tcpdump(325M)	141.0486	100.2637	110.2477	85.6512
	outside. tcpdump(310M)	131.4404	92.2342	98.8960	77.9874
周三	inside. tcpdump(367M)	285.5676	213.2512	200.4333	169.0012
	outside. tcpdump(351M)	272.8887	201.1235	189.7216	145.5622
周四	inside. tcpdump(527M)	219.8750	175.1251	164.3234	137.2345
	outside. tcpdump(493M)	203.2156	167.4234	174.6643	140.6775
周五	inside. tcpdump(294M)	144.3443	102.2134	98.4311	80.4499
	outside. tcpdump(271M)	131.0623	98.1234	102.4452	82.4457

改进的算法在 2-目标下，时间性能和双向 AC-BM 算法差不多，但它只运行一个模式树自动机，系统开销和 AC-BM 算法差不多。当目标增加到 3 时，可以看到时间性能有了很大的提高。随着目标的增多，相应的模式树自动机的构造会越复杂，但不会带来严重的影响：(1)模式树自动机需要提前构造；(2)规则不会太频繁变化。

参 考 文 献

[1] Navaro G R M. Flexible Pattern Matching in Strings[M]. Cambridge University Press, 2002

[2] Roesch M, Green C. Snort users manual [OL]. https://www.Snort.org

[3] Boyer R S, Moor J S. A fast string searching algorithm[J]. Communications of the ACM, 1977, 20(10): 762-772

[4] Fan Jang-jong, Su K. An Efficient Algorithm for Matching Multiple Patterns[J]. IEEE Transactions on Knowledge and Data Engineering, 1993, 5(2): 339-351

[5] 周四伟，蔡勇. AC-BM 算法的改进及其在入侵检测中的应用[J]. 微计算机应用，2007，28(1)：27-31

[6] 万国根，秦志光. 改进的 AC-BM 字符串匹配算法[J]. 电子科技大学学报，2006，35(4)：531-534

[7] 姚亚锋，蒋毅. 模式匹配算法及其优化[J]. 南通职业大学学报，2011，25(4)：98-100

[8] Hou Zheng-feng, Zhang Xiao-le. Research and improvement of AC-BM algorithm[J]. Chinese Journal of Scientific Instrument, 2011, 3(2): 216-221

[9] Wu Pei-fei. The research and amelioration of pattern-matching algorithm in intrusion detection system[C]// Proceedings of the 14th IEEE International Conference on High Performance Computing and Communications(HPCC-2012). 2012: 1712-1715

[10] 杨超. 双向 AC 算法及其在入侵检测系统中应用[J]. 计算机应用，2011，20(3)：222-225

[11] 黄海. 字符串匹配算法通用并行技术研究[D]. 西安：西安建筑科技大学，2010

[12] Miao Chang-sheng, Chang Gui-ran, Wang Xing-wei. Filtering Based Multiple String Matching Algorithm Combining q-Grams and BNDM[C]// Proceedings of the 2010 Fourth International Conference on Genetic and Evolutionary Computing. ACM, 2010: 582-585

[13] Zhang Wei-zhe, Zhang Yuan-jing, Zhang Hong-li, et al. A Memory-Efficient Multi-pattern Matching Algorithm Based on the Bitmap[C]// Proceedings of the 2009 Fourth International Conference on Internet Computing for Science and Engineering. ACM, 2009: 1-5

[14] Chen Xin-ming, Ge Kai-lin, Chen Zhen. AC-Suffix-Tree: Buffer Free String Matching on Out-of-Sequence Packets[C]// Proceedings of the 2011 ACM/IEEE Seventh Symposium on Architectures for Networking and Communications Systems, 2011: 36-44

(上接第 99 页)

[19] Chaum D, Van Heijst E. Group signatures[C]// Brighton, UK. Proceedings of EUROCRYPT 1991. Berlin/Heidelberg: Springer, 1991: 257-265

[20] Chase M, Lysyanskaya A. On signatures of knowledge [C]// Santa Barbara, California, USA. Proceedings of CRYPTO 2006. Berlin/Heidelberg: Sprin-ger, 2006: 78-96

[21] Belenkiy M, Camenisch J, Chase M, et al. Randomizable proofs and anonymous credentials [C] // Santa Barbara, California, USA. Proceedings of CRYPTO 2009. Berlin/Heidelberg: Springer, 2009: 108-125

[22] Wen Ya-min, Zhang Fang-guo. Delegatable secret handshake scheme[J]. Journal of Systems and Software, 2011, 84(12): 2284-2292

[23] Zhang Fang-guo, Chen Xiao-feng, Susio W, et al. A new signature scheme without random oracles from bilinear pairings [C]// Hanoi, Vietnam. Proceedings of VIETCRYPT 2006. Berlin/Heidelberg: Springer, 2006: 67-80

[24] Brands S. An efficient off-line electronic cash system based on the representation problem [R]. CS-R9323. CWI (Centre for Mathematics and Computer Science) Amesterdam, The Newthelands, Apr. 1993

[25] Pointcheval D, Stern J. Security proofs for signature schemes[C]// Saragossa, Spain. Proceedings of EUROCRYPT 1996. Berlin/Heidelberg: Springer, 1996: 387-398