一种适合大群组的高效群签名方案*)

崔国华　李　俊

(华中科技大学计算机学院信息安全系　武汉 430074)

摘　要　提出了一种安全高效的不使用知识签名的群签名方案，方案具有固定长度的群公钥和群签名，加入新成员时也无需更新群公钥，而且群签名的生成和验证操作远远低于 ACJT 方案。提出的方案能有效抵制联合攻击，打开群签名的效率与群规模无关，因此非常适合于大群体。

关键词　数字签名，群签名，抵制合谋，大群体

An Efficient Group Signature Scheme for Large Groups

CUI Guo-Hua　LI Jun

(College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074)

Abstract　A secure and efficient group signature scheme without using of signature of knowledge is proposed. The scheme has constant size of group public key and group signature, and the group public key need not to be updated when receiving the registration of a group member. The operation cost of sign and verify algorithm is less than ACJT scheme, which stands for the state of the art. The proposed scheme can effectively resist coalition attacks, and the efficiency is also independent with the group size, which results that the scheme is fit for large groups.

Keywords　Digital signature, Group signature, Coalition-resistant, Large groups

1　引言

群签名(group signature)由 Chaum 和 van Heyst[1] 在 1991 年提出之后便在不同的领域得到了广泛的应用，如电子支付、电子投票等。群签名允许任何群成员代表群进行匿名地签名，当发生纠纷时，群管理员能够揭示签名者的真实身份；同时，区分任意两个不同的群签名是否来自于同一个签名者是不可行的。另外，群签名还须满足抵制伪造攻击、陷害攻击和合谋攻击等安全特性。

群签名的效率是其从理论走向实用的一个关键因素[3]。在群签名的发展初期提出的一些方案中[1,2]，群公钥的长度和(或)签名的长度与成员数成线性关系；当增加新的成员时，至少要修改群公钥。如何将普通数字签名用来构造群签名方案是这个时期的一个公开问题。早期 Fiat 和 Shamir 建议了一种将验证者诚实的完全 ZK 协议转化为数字签名方案的一般方法[7](称为"F-S 启发式")。受 F-S 启发式的影响，利用知识签名[8]技术提出的 CS97 方案[4]是第一个具有固定长度的群公钥和群签名的方案。此后，知识签名技术成为群签名方案设计[4~9]的必不可少的基本工具。Ateniese 等人提出的 ACJT 方案[6]代表了当前群签名的技术发展水平，它不仅具有高效性，而且满足可证明抵制合谋的安全性。然而，相比于普通数字签名而言，使用知识证明的签名方案的效率要低得多。最近，张键红等人[15]提出了一种高效的群答名，其方案仅在群成员加入时采用知识签名，算法效率较高。但其方案在设计上存在缺陷，因此该文所声称的安全性无法满足。本文提出了一种安全高效的群签名方案，并且方案不需要使用知识签名。新方案不仅仅具有固定长度的群公钥和群签名，加入新成员时也无需更新群公钥，而且群签名的生成和验证操作远远低于 ACJT 方案。同时，方案能有效抵制合谋，打开群签名的效率与群规模无关，非常适合于大群体。

本文第 2 节对群签名的模型和实现方法进行了描述，然后给出方案所依赖的数论假设。新的适合于大群体的群签名方案在第 4 节进行描述，第 5 节对方案的安全性和效率进行了分析，最后给出结论。

2　模型和实现方法

本节将给出群签名体制的概念，并给出我们实现群签名体制的一些基本思想。

2.1　模型

一个群签名方案由以下算法组成：

系统设置(Setup)：一个指定群管理员和群成员之间的交互协议，其结果包括群公钥 Y 和群管理员的秘密管理密钥 x_M。

成员加入(Join)：群成员与群管理员之间的一个概率交互协议，注册新成员的身份 ID，为新成员产生成员私钥 x_G。

生成签名(Sign)：一个签名生成算法，输入待签名的消息 m、某个合法群成员的私钥 x_G 和群公钥 Y，输出签名 s。

验证签名(Verify)：一个签名验证算法，输入消息 m、群签名 s 和群公钥 Y，当且仅当签名 s 是由群成员使用 Sign 算法完成的。

打开签名(Open)：一个追踪算法，输入群签名 s、消息 m 和群管理密钥 x_M，返回签名者的真实身份 ID。

2.2　群签名的安全性和效率

一个群签名方案必须满足以下安全性要求：

*)本课题得到国家自然科学基金(60403027)、国家"八六三"高科技研究发展计划基金(301-1-3)资助。崔国华　教授，博士生导师，主要研究方向为信息安全，计算机算法；李　俊　博士研究生，主要研究方向为密码理论与数字签名技术。

①正确性：一个合法的群成员按照签名算法产生的群签名一定能够通过验证算法。

②不可伪造性：非群成员要产生一个通过验证算法的群签名在计算上是不可行的。

③匿名性：对于一个有效的群签名，除了群管理员之外，决定签名者的真实身份在计算上是不可行的。

④不可关联性：决定两个不同的群签名是否来自于同一个群成员在计算上是不可行的。

⑤抗陷害性：不管是群成员还是群管理员都不能代表其它群成员进行签名。

⑥可追踪性：对于有效的签名，签名者的真实身份可以被群管理员揭开。

⑦抵制合谋：任意多个群成员联合起来也不能伪造一个无法追踪的群签名。

群签名体制的有效性由如下几个因素决定：①群公钥 Y 的长度。②签名 s 的长度。③签名与验证算法的效率。④新成员加入和群签名打开算法的效率。

2.3 实现方法

近年来提出的具有固定群公钥和签名长度的群签名方案中，大部分[3~9]都使用知识签名作为其基本构件，实现这些方案的核心思想大体如下。群管理员计算普通数字签名方案的密钥对(sig_M, ver_M)和公钥概率加密体制的密钥对($encr_M$, $decr_M$)，然后公开两个密钥对中的公钥作为群公钥 Y，即(ver_M, $encr_M$)。若 Alice 要加入群，她随机选择一个秘密密钥 x 并计算成员密钥 $z=f(x)$，其中 f 是一个单向函数，它委托 z 来代表自己，例如对 z 进行签名。Alice 将 z 发送给群管理员，群管理员返回给 Alice 一个群成员证书 $v=sig_M(z)$，那么 Alice 的群秘密密钥为(x,z,v)。当群成员 Alice 代表群对消息 m 签名时，Alice 用群管理员的加密密钥加密对(m,z)，即 $d=encr_M(r,(m,z))$，其中 r 是足够大的随机串。Alice 再计算一个非交互的最小泄漏证明 p，以证明她知道(x',v',r')满足下列等式：

$$d=encr_M(r',(m,f(x')))$$

$$ver_M(v',f(x'))=true$$

那么得到消息 m 的签名为(d,p)，验证 p 的正确性即可验证签名的有效性。若出现纠纷要打开这个签名，群管理员解密 d 获得群成员密钥 z，从而揭示 Alice 的真实身份。

根据上述思想设计的群签名方案实质上是由两个非群签名方案组成，一个用来颁发成员证书，另一个用于产生实际的群签名。前一个签名方案的安全性不仅影响到群签名的安全性，而且它关系到群签名方案是否满足抵制合谋的性质。因为在加入协议中，每一个群成员都得到由群管理员颁发的唯一的证书，该证书实际上是 GM 对每个成员选取的随机秘密消息的签名。对于合谋而言，它即是将所有群成员看作一个能发起适应性选择消息攻击(adaptive chosen message attack)的敌手，加入协议的每一次运行实例即获得一次签名预言(Oracle)服务。因此，设计一个实际群签名方案的主要挑战就是寻找一个合适的签名方案用于颁发成员资格证书，并且允许使用证书来有效进行后一个签名，即产生实际的群签名。现有的群签名方案中[3~9]，后一个签名方案一般由成员证书的知识证明获得(使用 F-S 启发式[7])，但是寻找一个颁发成员资格的签名方案并且使知识签名得到高效的实现一般是比较困难的。为此，我们尝试折回到群签名的发展初期，不采用知识签名技术，而是寻找一个普通的签名方案直接使用成员资格证书来完成实际的群签名。在第 4 节可以看到，这样的签名方案不仅存在，而且方案的效率比采用知识签名的方案要高得多。

3 数论假设

定义 1(DL 问题)：设 G 为一给定的有限循环群，g 为 G 的一个生成元。离散对数(DL)问题可以描述为：给定 $a\in G$，求解 x 使满足 $a=g^x$。

定义 2(RSA 问题)：设 $n=pq$，其中 p 和 q 是素数，e 是一个整数且满足 $gcd(e,(p-1)(q-1))=1$，RSA 问题可以描述为：给定 $c\in Z_n^*$，求解唯一的整数 m 使满足 $m^e\equiv c(\mathrm{mod}\ n)$。

假设 1(DL 假设)：存在概率多项式时间算法 $\mathscr{A}$，对于输入的安全参数 l_G 来说，算法 $\mathscr{A}$ 输出的二元组(G,g)满足：对于所有的概率多项式时间算法 $\mathscr{K}$ 来说，解 DL 问题的概率是可忽略的。

假设 2(RSA 假设)：存在概率多项式时间算法 $\mathscr{A}$，对于输入的安全参数 l_G 来说，算法 $\mathscr{A}$ 输出的二元组(n,e)满足：对于所有的概率多项式时间算法 $\mathscr{K}$ 来说，解 RSA 问题的概率是可忽略的。

4 一种适合大群组的高效群签名方案

4.1 系统参数的建立

群签名方案由群管理员(GM)和群成员组成，系统参数的设置由 GM 完成。GM 选取三个素数 p,q,f（三个素数的选取方法参考注记 1)和 RSA 模数 $n=pq$，同时选取 e 和 d 满足 $ed\equiv 1(\mathrm{mod}\ \varphi(n))$。令 g 是 Z_n^* 中的一个 f 阶元素，$H(\cdot)$是 Hash 函数：$\{0,1\}^*\mapsto\{0,1\}^k$，$(k=160)$。GM 选取随机数 $x\in_U Z_f^*$，计算 $y=g^x(\mathrm{mod}\ n)$。

GM 保留群管理员私钥为(d,x)，然后公开(n,e,f,g,y)为群公钥。

注记 1：选取 Z_n^* 中的一个 f 阶元素 g 可以按下面方法进行。随机选取 5 个素数 p,q,f,p',q' 使满足 $p=2fp'+1$，$q=2fq'+1$，$|f|=160$。令 $g=h^{\varphi(n)/f}(\mathrm{mod}\ n)$，其中 $h\in_U Z_n^*$，若 $g>1$，则 g 的阶为 f。因此，存在有效的算法寻找 Z_n^* 中的一个 f 阶元素 g。

4.2 成员加入协议

如果 Alice 要加入群，首先 Alice 选择私钥 $k\in_U Z_f^*$，通过计算 $z=g^k(\mathrm{mod}\ n)$对 k 进行承诺，同时计算离散对数 $\log_g z$ 的知识证明 p(参考 Schnorr 协议[13])，然后将申请信息连同(z,p)提交给 GM。

GM 验证离散对数知识证明的正确性之后，按下面步骤为 Alice 生成成员证书：

(1)选择随机数 $l\in_U Z_f^*$，计算 $r=g^l(\mathrm{mod}\ n)$；

(2)计算 $s=l+xH(z\|r)(\mathrm{mod}\ f)$；

(3)计算 $w=(H(g^z))^{-d}(\mathrm{mod}\ n)$

GM 将(r,s,w)发送给 Alice，同时保存(w,z)用于打开群签名。

Alice 收到(r,s,w)后验证 $r\overset{?}{\equiv}g^s y^{H(z\|r)}(\mathrm{mod}\ n)$ 且 $H(g^z)\overset{?}{\equiv}w^{-e}(\mathrm{mod}\ n)$是否同时成立，若验证通过，Alice 接受$(s,w)$为成员证书 $cert_A$。

4.3 群签名的生成

成员 Alice 利用成员证书 $cert_A$ 和私钥 k 来生成群签名。

Alice 选择随机数 $l\in_U Z_f^*$，$h\in_U Z_n^*$，计算

$$\begin{cases} t=g^{l} \pmod n \\ r=t\cdot h^{r} \pmod n \\ u=H(r\parallel m) \\ s_1=l+u(s+k) \pmod f \\ s_2=h\cdot w^{u} \pmod n \end{cases}$$

得到的群签名为(u,t,s_1,s_2)。

4.4 群签名的验证

当验证者得到签名(u,t,s_1,s_2)后：

step1. 计算 $\eta=u^{-1} \pmod f$；

step2. 计算 $r'=ts_2^{e}(H((t^{-1}g^{s_1})^{\eta}))^{u} \pmod n$；

然后判断是否满足 $u\overset{?}{=}H(r'\parallel m)$，若等式满足则通过验证。

4.5 打开群签名

当产生纠纷时，可以由GM来打开群签名。由于GM保存有每个成员的身份信息(w,z)，对于任意有效的群签名(u,t,s_1,s_2)，GM按如下方法揭示签名者的真实身份：

step1. 计算 $\eta=u^{-1} \pmod f$

step2. 计算 $v=s_2^{e}(H((t^{-1}g^{s_1})^{\eta}))^{u} \pmod n$

step3. 计算 $w=(s_2v^{-d})^{\eta} \pmod n$

由于w与成员身份一一对应，因此计算出w便可揭示出签名者的真实身份。

5 安全性与性能分析

在本节，我们对上述的群签名方案进行安全性与性能分析。

5.1 方案的正确性证明

定理1 如果群签名(u,t,s_1,s_2)是由一个合法的群成员按照签名算法产生，那么该签名一定能够通过验证。

证明：若群签名(u,t,s_1,s_2)是由某个群成员使用成员证书(s,w)和成员密钥k生成，那么验证者计算

$$\begin{aligned} r' &= ts_2^{e}(H((t^{-1}g^{s_1})^{\eta}))^{u} \pmod n \\ &= ts_2^{e}(H((g^{s_1-l})^{\eta}))^{u} \pmod n \\ &= ts_2^{e}(H((g^{u(s+k)})^{\eta}))^{u} \pmod n \\ &= ts_2^{e}(H(g^{s+k}))^{u} \pmod n = ts_2^{e}(w^{-e})^{u} \pmod n \\ &= t(s_2w^{-u})^{e} \pmod n = th^{e} \pmod n = r \end{aligned}$$

因此，验证等式$u=H(r'\parallel m)$成立。 □

5.2 方案能抵制的恶意攻击

这一部分我们将分析方案所能满足的安全性质以及所能抵制的适应性攻击。首先我们给出方案的一个性质。

定理2 与成员的身份承诺z对应的成员证书(s,w)只能由群管理员GM生成。

证明：假设敌手adv不知道(d,x)，随机选取$k\in_U Z_f^*$并计算身份承诺$z=g^{k} \pmod n$，他的目标是伪造一个二元组(s,w)使满足$H(g^{s}z)\equiv w^{-e} \pmod n$。我们假设函数$H$满足随机预言机[9](ROM)的性质，其输出服从均匀分布。那么伪造二元组(s,w)等价于求解RSA问题，由RSA假设知道实际上是不可行的。另外，若敌手不知道(d,x)，伪造部分信息r和s也是不可行的。因为(r,s)满足$r\equiv g^{s}y^{H(z\parallel r)} \pmod n$，实质上是关于$z$的Schnorr签名[13]。文[11]在随机预言机模型和离散对数(DL)假设下给出了Schnorr签名在适应性选择消息攻击下的不可伪造性证明，这意味着在群成员总数目为多项式有界的条件下，即使所有的群成员合谋也无法获取交互过程中的部分信息(r,s)。因此，有效的成员证书只能由拥有群管理密钥(d,x)的群管理员GM生成。进一步，成员加入的交互协议本质上由Schnorr身份识别协议[13]完成，那么交互协议便是关于GM的验证者诚实的完备零知识。在DL假设下，GM拥有的秘密密钥(d,x)是不会被泄漏的。因此，伪造一个有效的成员证书(s,w)是不可行的。 □

下面分析方案满足的安全性质。

(1)恶意攻击者无法伪造群签名。假设攻击者是合法的群成员，要伪造一个不可追踪的群签名，从打开签名算法可知，他必须能伪造(s',w')使满足$H(g^{s'}z)\equiv(w')^{-e} \pmod n$，从定理2的分析可知等价于解RSA问题的困难性。下面我们假设存在更一般的恶意攻击者，他的目标是伪造能满足验证等式的四元组(u,t,s_1,s_2)。根据验证等式$r'=ts_2^{e}(H((t^{-1}g^{s_1})^{\eta}))^{u} \pmod n$和$u=H(r'\parallel m)$，假设$H$满足随机预言机性质，那么当攻击者随机选择$t,s_1$和$u$后，计算$s_2$等价于解密一个随机选择的RSA密文，在RSA假设下这是不可行的。因此，方案可以抵制伪造攻击和陷害攻击。

(2)任意多个群成员的合谋都无法伪造有效的群签名。群成员合谋伪造一个不可追踪的群签名可以通过两种方法完成，一是合谋伪造一个新的成员证书，由定理2知其困难性等价于Schnorr签名在适应性选择消息攻击下的存在性伪造和RSA方案的选择明文攻击，这在DL假设和RSA假设下是不可行的。再就是联合伪造满足验证等式的四元组(u,t,s_1,s_2)，根据前面的分析，在随机预言机模型下，其困难性等价于RSA的选择明文攻击。因此，多个群成员伪造群签名是不可行的。

(3)群签名的匿名性、不可关联性和可追踪性。根据群签名的打开算法，要计算与成员身份一一对应的w值，必须先恢复签名生成算法中选取的随机数h。$v=h^{e} \pmod n$是可以根据签名(u,t,s_1,s_2)直接计算得到的，但是解密v得到随机数h只有群管理员GM才能完成。那么撤销群签名的匿名性依赖于求解一个随机选择的RSA密文，这实质上是求解RSA问题。另外，若给定任意的两个签名(u,t,s_1,s_2)和(u',t',s'_1,s'_2)，判定这两个签名是否来自于同一个群成员，需要判断这两个签名所使用的证书是否有关联。从签名过程可以看出，签名结果实际上将证书信息s和w进行了概率加密，得到的密文s_1和s_2与对应的明文信息s和w是不可关联的。除了制定的群管理员外，其不可关联性无法揭开。由此可知，群签名方案满足匿名性、不可关联性和可追踪性。

5.3 群签名的效率分析

就方案的效率而言，我们主要考虑签名、验证和打开群签名的执行效率。算法的运算代价主要依赖于模幂运算和求逆运算，我们用exp表示模幂运算，用inv表示求逆运算，将方案的效率与ACJT方案进行比较如下：

	签名	验证	打开
ACJT方案	10exp	12exp	5exp+1inv
我们的方案	3exp	4exp+2inv	6exp+3inv

从表中我们可以发现，我们的方案具有较好的效率，适合于大群体的群签名。

结论 提出了一种高效的群签名方案，该方案没有使用知识签名。新方案不仅仅具有固定长度的群公钥和群签名，加入新成员时也无需更新群公钥，而且群签名的生成和验证操作远远低于ACJT方案。同时，方案能有效抵制合谋，打开群签名的效率与群规模无关，非常适合于大群体。

(下转第118页)

策略描述的是WS的一般特性而不是专属于某个过程的特性，所以可以将策略描述与Profile结合在一起。利用SWS提供的丰富的语义注释，通过提供具有语义意义的、说明性的、计算机可处理的策略描述和相关的算法和工具来实现服务请求者与服务提供者之间的策略匹配，从而解决SWS面临的安全问题。

将策略集成到SWS描述中可以提供多层次的安全性。策略可以限制谁能够在何种条件下使用一项服务，相关信息应当如何提交给服务以及服务要如何使用所提供的信息。策略说明就是对请求者、服务和内容不同属性所实施的约束。例如，授权策略，定义了一组限制访问服务的规则，只有特定的用户在特定的环境下才能访问服务；隐私策略，描述了什么样的信息能够被交换，信息的合法使用以及信息交换应当处于什么样的条件下；机密性策略，描述了一个服务的输入和输出参数的密码特征。

为了实现在服务的安全需求中包含策略说明，只须增加一个新的特性作为securityRequirement的子特性，用来描述为正确执行服务所必须实施的各种策略。

为了实现一个SWS应用安全框架，除了提供可部署的、具有明确形式定义OWL-S接口的安全服务外，还需要部署各种会话、鉴别或交互协议以支持密钥或策略的建立和交换及协约的协商。而且，框架中的服务和协议都需要进行语义注释以为那些执行服务分析和组合的语义工具所使用。

结束语 在SW技术的推动下，SWS近年来受到了学术界的广泛关注。SWS是在WS中加入了语义的支持，使得计算机之间能够理解互相通信的内容，从而实现WS的自动发现、调用和组合。SWS是为解决WS的语义描述问题而提出的，面临着与WS一样的安全、隐私和信任等问题。因此，营造一个SWS应用安全环境，既是为了满足下一代WWW应用的发展需要，也为复杂的SWS应用实现安全可信的在线交易提供了必要保证。

提出并建立一个灵活的、自适应的SWS应用安全框架是我们的最终研究目标。当前，DAML Project下的DAML-S安全工作小组已经开发了一些与安全有关的本体，比如凭证本体、安全机制本体、服务安全扩展本体、Agent安全扩展本体及隐私本体等。在安全本体研究的基础上，安全服务的语义描述、实现和部署是实现这个目标所需要完成的第一步。本文提出了采用OWL-S安全本体和策略注释的方法来解决安全服务的语义描述问题。下一步的工作就是考虑如何实现和部署安全服务。如何实现安全推理器中的安全匹配算法，采用哪一种策略表示语言，选用微软的.Net平台还是Sun的J2EE标准，采用两层还是三层部署结构等一些问题还有待进一步解决。

参 考 文 献

1 Kearney P. Message Level Security for Web Services. Information Security Technical Report, 2005,10:41～50
2 Lee TB, Hendler J, Lassila O. The Semantic Web. Scientific American, 2001,5:34～43
3 Denker G, Kagal L, Finin T. Security in the Semantic Web Using OWL. Information Security Technical Report, 2005,10:51～58
4 MacVittie L. Web Services Security. NetworkComputing. http://www.networkcomputing.com/showArticle.jhtml?articleID=21400998&pgno=3, 2004
5 Atkinson B, Della-Libera G, Hada S, et al. Web services security(WS-Security). Http://www-128.ibm.com/developerworks/Webservices/library/ws-secure/, 2002
6 Anderson S, Bohren J, Boubez T, et al. Web Services Trust Language(WS-Trust). ftp://www6.software.ibm.com/software/developer/library/ws-trust.pdf, 2005
7 Bajaj S, Box D, Chappell D, et al. Web Services Policy Framework(WS-Policy). http://download.boulder.ibm.com/ibmdl/pub/software/dw/specs/ws-polfram/ws-policy-2006-03-01.pdf, 2006
8 SAML. Assertions and Protocols for the OASIS Security Assertion Markup Language(SAML) V2.0. http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf, 2005
9 Denker G, Kagal L, Finin T. Security for DAML Web Services: Annotation and Matchmaking. In:Proceedings of the 2nd International Semantic Web Conference (ISWC2003), LNCS2870, Springer-Verlag, 2003.335～350
10 Web Ontology Working Group. OWL. Http://www.w3.org/2001/sw/WebOnt/
11 DAML Services - Security and Privacy. Http://www.daml.org/services/owl-s/security.html
12 http://www.daml.org/services/owl-s/security/security.owl
13 DAML Services. Http://www.daml.org/services/owl-s

(上接第81页)

参 考 文 献

1 Chaum D, Heyst V E. Group Signatures[C]. In:Proc. of EUROCRYPT'91. Lecture Notes in Computer Science, 1991, 547:257～265
2 Chen L, Pedersen T. New group signature schemes[A]. In:Proceedings of EUROCRYPT'94, Lecture Notes in Computer Science. Springer-Verlag, 1995, 950: 171～1811
3 Camenish J, Stadler M. Efficient group signatures for large groups[C]. In:Proc. of CRYPTO'97. Lecture Notes in Computer Science, 1997, 1296: 410～424
4 Camenisch J. Group signature schemes and payment systems based on the discrete logarithm problem:[PhD thesis]. vol. 2 of ETH Series in Information Security and Cryptography, ISBN 3-89649-286-1. Hartung-Gorre Verlag, Konstanz, 1998
5 Ateniese G, Tsudik G. Some open issues and new directions in group signatures[C]. In: Franklin M, ed. Financial Cryptography Conf. LNCS 1648, Berlin: Springer-Verlag, 1999. 196～211
6 Ateniese G, Camenish J, Joye M, et al. A practical and provably secure coalition-resistant group signature scheme [A]. In: M. Bellare, ed. Advances in Crypto'2000, Berlin: Springer-Verlag, 2000. 255～270
7 Ateniese G, Medeiros B. Efficient Group Signatures without Trapdoors. In: Advances in Cryptology - ASIACRYPT'2003, LNCS2894, 2003. 246～268
8 Boneh D, Boyen X, Shacham H. Short group signatures. In: CRYPTO'2004, LNCS. Springer Verlag, 2004
9 Camenisch J, Groth J. Group Signatures: Better Efficiency and New Theoretical Aspects. In: SCN 2004, LNCS 3352, 2005. 120～133
10 Fiat A, Shamir A. How to prove yourself: practical solutions to identification and signature problems. In: Advances in Cryptology - CRYPTO'86, Springer-Verlag, LNCS263, 1987. 186～194
11 Camenisch J, Stadler M. Proof systems for general statements about discrete logarithms:[Technical Report]. TR 260, Institute for Theoretical Computer Science, ETH Zurich, Mar. 1997
12 Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols. In: First ACM Conf. on Computer and Communications Security, New York: ACM Press, 1993. 62～73
13 Schnorr C P. Efficient identification and signature generation for smart cards. In: CRYPT'89, LNCS435, Springer-Verlag, 1990. 239～252
14 Pointcheval D, Stern J. Security proofs for signature schemes. In:Cryptology-Proceedings of EUROCRYPT'96, Lecture Notes in Computer Science 1070, Springer-Verlag, 1996. 387～398
15 张键红，伍前红，邹建成，王育民. 一种高效的群签名，2005,33(6):1113～1115