基于 ID 的群向签名方案

马春波[①②] 敖 珺[③] 何大可[④]
[①](西南交通大学计算机与通信工程学院 成都 610031)
[②](上海交通大学信息安全工程学院 上海 200030)
[③](西安电子科技大学电子所 西安 710071)
[④](西南交通大学信息安全与国家计算网格实验室 成都 610031)

摘 要 该文首先提出了一种新的签字模型，并由此设计了一种新的群向签名方案，其具有如下特点：基于 ID 的密码概念；不具有密钥托管功能，也就是只有成员自己知道自己的私钥，而其他成员，包括 PKG 也不知道；指定签名验证群中的每一个成员都可以独立地完成对签名的验证。此签名不是基于秘密共享技术的，因此，他不需要多名成员来共同完成对签名的验证。这样，既减少了对系统资源的占用，又提高了系统的效率。

关键词 公钥密码，群向签名，密钥托管
中图分类号: TP309.2 **文献标识码**：A **文章编号**：1009-5896(2006)06-1145-05

ID Based Group Oriented Signature

Ma Chun-bo[①②] Ao Jun[③] He Da-ke[④]
[①](*School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu* 610031, *China*)
[②](*School of Information Security Engineering, Shanghai Jiaotong University, Shanghai* 200030, *China*)
[③](*Laboratory for Radar Signal Processing, Xidian University, Xi'an* 710071, *China*)
[④](*Lab. of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu* 610031, *China*)

Abstract A new kind of group-oriented signature is presented with a new signature model in this paper. The signature has the following properties: it is based on ID cryptography concept; does not have the function of key escrow, that is, no one, other than the member himself, knows the secret key, even the PKG does not know; the member in the designated group can verify the signature independently. The secret sharing is not used in the signature, so the cooperation among the members is not needed. Comparing to other group-oriented signature, the new one uses less system resources, and improves the system efficiency.

Key words Public key cryptography, Group oriented signature, Key escrow

1 引言

到目前为止，具有定向性质的签名可以分为两类，一类是定向群的，也就是群向签名；另一类是定向于某一个特定的接收者的。群向密码最早由Desmedt在 1987 年提出[1]，其要解决的问题是：当给一群人发送加密的消息时，只有某一个授权子集内的成员可以通过合作解密得到明文。群向密码的关键的技术就是秘密共享技术，也就是在解密阶段，密钥需要几个成员的合作才能重构，从而完成解密过程。将此技术应用到签字上，就形成了群向签名。我们可以这样来理解：群向签名是指在授权集合内的成员，通过共同合作来完成签名或对签名进行验证。通常来说，群向签名的基本技术也是基于 (t,n) 门限的秘密共享技术。对于群向签名的研究有文献[2 – 6]。

定向于某一个特定接收者的签名是指只有指定的接收者才能对签名进行验证，如卡梅隆签名。此签名是Krawczyk和Rabin在 2000 年提出的一种签名算法[7]，此算法与一般的签名算法不同之处在于它的Hash函数。卡梅隆Hash函数是一种有陷门的单向函数，基于此类单向函数构造的签名算法，是一种指定确认人的签名。

到目前为止，对构建基于公钥密码的安全系统来说，选择或应用适当的安全算法已经不是什么问题，而问题的关键是 PKI 的构建和管理。从目前的情况看，基于 ID 的公钥系统可以成为基于证书系统的替代，特别是对那些对需要有效的秘钥管理同时对安全性要求不是很高的系统。总的来说，基于 ID 的密码系统比起传统的秘钥系统更容易管理。在传统的密码系统中，用户 A 的身份跟他的公钥是没有什么关系

2004-11-15 收到，2005-03-28 改回
西南交通大学博士生创新基金资助课题

的，其公钥仅仅是一串随机的字符串。当用户 B 想给 A 发送信息，那么 B 首先要获得 A 的经过认证的公钥。为了解决这个问题，在典型的公钥密码系统中要建立一张目录，以备查询使用。基于 ID 的公钥系统的优点在于，它的任何用户的公钥可以由此用户的某一身份特征来推导得出，比如说他的邮箱地址。对于公钥系统本身来说，这使得公钥的维护和认证变得简单。

Shamir在 1984 年首先提出了基于ID的密码的概念[1]，并在此文章中描述了第一个基于ID的签名。然而，真正实用的第一个基于ID的密码机制直到 2001 年Boneh和Franklin的工作发表之后才得以实现[2]。Boneh-Franklin体制的安全性建立在双线性Diffie-Hellman问题上。

对于一个公钥体制，如果其密钥分配依赖于一个可信赖的密钥分配中心，那么就不可避免地存在一个密钥托管的问题。对于密钥托管本身而言，它不会给用户带来任何好处。用户不得不相信托管机构的安全性程序，以及参与人的诚实。他不得不相信托管机构没有改变他们的策略，政府没有改变他的法律，那些得到密钥的执法机构和托管机构会合法地和负责地做事[8]。因为成员的所有的密钥都由密钥分配中心来分配，因此，密钥分配中心就可以生成任意成员的有效签名，比如文献[3－7]都存在这种问题。对于这个问题，以前有两种解决方案，如引入多个密钥分配中心或采用无可信赖密钥分配中心的方式，如文献[2]。但是这两种解决方案都是引入了秘密共享技术，从而增大了系统的通信流量和系统的复杂性。值得注意的是，文献[9]提出了一种新的密钥分配形式，通过此方案生成的成员密钥仅为成员自己所知，其余任何人，包括密钥分配中心都不知道。

现在让我们考虑以下问题：假设在网络上有两个独立的群体 A 和 B，群体 B 的成员将要把对消息 m 的签名发给群体 A，并且使得群体 A 内的任何成员都可以独立的对签名进行验证，而其他群内的成员则无法完成验证过程。这个问题与以上提到的群向签名不同的是，群体 A 内的成员对签名的验证是独立进行的，而不是通过成员之间的合作来完成。考虑到基于 ID 的密码体制的优点以及密钥托管等问题，在对文献[8]提出的密钥分配方法进行适当的修改后，本文提出了一种新的群向签名方案，其具有如下特点：基于 ID 的密码概念；不具有密钥托管功能，也就是只有成员自己知道自己的私钥，而其他成员，包括 PKG 也不知道；指定签名验证群中的每一个成员都可以独立地完成对签名的验证。此签名不是基于秘密共享技术的，因此，他不需要多名成员来共同完成对签名的验证。这样，既减少了对系统资源的占用，又提高了系统的效率。

2 背景知识

2.1 双线性对

设 G_1， G_2 分别是同为 q 阶的加群和乘群，并假设 P 为 G_1 的生成子。假设在群 G_1，G_2 中，离散对数问题是难解的。可定义双线性映射对为 e： $G_1\times G_1\to G_2$，并满足以下特性：

(1)双映射性： $e(aP,bP')=e(P,P')^{ab}$，对所有的 P，$P'\in G_1$，所有的 $a,b\in Z_q$ 成立。

(2)非退化性(Non-degenerate)：如果 $e(P,P')=1$，存在 $P'\in G_1$，则有 $P=\mathrm{O}$。

(3)可计算性：存在有效的算法，对于 P， $P'\in G_1$，可计算 $e(P,P')$。

映射 e 可以由在有限域椭圆曲线上的 Weil 或 Tate 对推导得来。

2.2 GDH 群

设 G_1， P 和 q 如上面所定义。假设 G_1 的逆和乘法存在有效的计算方法。我们首先介绍在 G_1 中的下列问题：

(1)离散对数问题(DLP)：给定 G_1 中的两个元素 P 和 Q，寻找整数 $n\in Z_q^*$，使得 $Q=nP$ 成立。

(2)可计算 Diffie-Hellman 问题(CDHP):给定 P,aP,bP，$a,b\in Z_q^*$，计算 abP。

(3) 可判定 Diffie-Hellman 问题(DDHP)：给定 P,aP,bP,cP， $a,b,c\in Z_q^*$，判定是否存在 $c=ab\bmod q$。

定义 1 一个算法 Λ 在群 G_1 中解决 CDHP 问题的**盈余**可定义为概率：

$$P_r[\Lambda(P,aP,bP)=abP:a,\mathrm{b}\overset{R}{\leftarrow}Z_q^*]$$

如果没有一种算法可以在多项式时间内以不可忽略的概率解决 CDHP 问题但是有算法可以解决 DDHP 问题，我们把满足此种要求的群 G 叫做 GDH 群。这样的群可以在超椭圆曲线或超奇椭圆曲线上构建，文献[10]中有关于这方面的具体论述。

2.3 在椭圆曲线上的 GDH 群

基于椭圆曲线的GDH群的构建是构造基于GDH问题的签名方案的基础。下面我们来对 GDH 群做一下说明。

定义 2 设 E 是域 F_k^n 上的具有 l 个点的椭圆曲线，k 是一个素数，n 是一个正指数。设 P 是 E 上的阶为 q 的点，其中 q 为素数，并且 q^2 不能整除 l。对某一个整数 $\alpha>0$，对于任何 $t=1,2,\cdots,\alpha-1$，如果 $a\,|\,k^{n\alpha}-1$ 和 q 不能被 $k^{nt}-1$ 整除。也就是说，在域 F_q^* 上的 k^n 的阶为 α，那么我们就说子群 $<P>$ 就有一个安全乘子 α。

要计算椭圆曲线上的离散对数，通常是将椭圆曲线上的离散对数问题映射到域 F_k^n 的某个扩展域上，比如 F_k^{nt}。要使得 $<P>$ 上的 CDHP 难解同时保证 DDHP 易解，就要选择合适的安全系数 α。就像我们在文献[10]中看到的那样，在超椭圆曲线上选择 $\alpha=6$，可以获得用于构造短签名的 $<P>$，其安全性与 F_k^{6n} 上的离散对数问题相当。为了保证 F_k^{6n} 上的离散对数的难解性，要求 k^n 要足够的大。当然，我们也可以选择别的椭圆曲线或者是超椭圆曲线来构造这样的群以获

得更高的安全性。

3　群向签名

不失一般性，我们来讨论在网络上两个群的群向签名问题，并设两个群分别为群 A 和群 B。设有群 $A=\{p_{A1},p_{A2},\cdots,p_{An}\}$，$B=\{p_{B1},p_{B2},\cdots,p_{Bn}\}$，其成员分布在网络的不同位置，并通过网络来相互联系。设群 B 中的成员 p_{Bi} 将要对消息 m 签名，并通过网络将此签名发送给群 A。

3.1　初始化

设要签名的消息为 m。G_1 是阶为 q 的 GDH 群，其中，q 为大素数。可定义双线性映射为 e：$G_1\times G_1\to G_2$。并假设 P 为 G_1 的生成子。

设有单向函数　H_0：$\{0,1\}^*\to G_1$，H_1：$\{0,1\}^*\to Z_q^*$。此签名方案中有一个 PKG(Public Key Generator)。它的功能是为网络中的独立的群体提供群公钥及相应群成员的部分私钥。

3.2　密钥的产生

PKG 首先选择随机数 $t,s\in Z_q^*$，并以 $P_A=\{tsP,tP\}$ 作为群 A 的公钥，表示为 $P_A=\{P_A^1,P_A^2\}$。PKG 将 $sH_0(\mathrm{ID}_{Ai})$，$tH_0(ID_{Ai})$ 通过安全信道传递给群 A 的成员 p_{Ai}。以同样的方法，PKG 随机选择 $s'\in Z_q^*$，并以同样的方法生成群 B 的公钥 $P_B=\{P_B^1,P_B^2\}=\{ts'P,tP)$，将 $s'H_0(\mathrm{ID}_{Bi})$，$tH_0(\mathrm{ID}_{Bi})$ 通过安全信道传递给群 B 的成员 p_{Bi}。我们分别把 $\{sH_0(\mathrm{ID}_{Ai}),tH_0(\mathrm{ID}_{Ai})\}$，$\{s'H_0(\mathrm{ID}_{Bi}),tH_0(\mathrm{ID}_{Bi})\}$ 叫做 p_{Ai} 和 p_{Bi} 的部分私钥。由密钥的生成过程我们看到，部分私钥是由 PKG 生成的。

p_{Ai} 随机选择 $x_{Ai}\in Z_q^*$，那么 p_{Ai} 的私钥为：$S_{Ai}=\{x_{Ai}sH_0(\mathrm{ID}_{Ai}),x_{Ai}tH_0(\mathrm{ID}_{Ai})\}$，可表示为：$S_{Ai}=\{S_{Ai}^1,S_{Ai}^2\}$，其公钥为 $P_{Ai}=x_{Ai}H_0(\mathrm{ID}_{Ai})$。

同样的方法，群 B 的成员 p_{Bi} 随机选择 $x_{Bi}\in Z_q^*$，那么 p_{Bi} 的私钥为：$S_{Bi}=\{x_{Bi}s'H_0(\mathrm{ID}_{Bi}),x_{Bi}tH_0(\mathrm{ID}_{Bi})\}$，并表示成：$S_{Bi}=\{S_{Bi}^1,S_{Bi}^2\}$。其公钥为 $P_{Bi}=x_{Bi}H_0(\mathrm{ID}_{Bi})$。

在此签名方案中，私钥由成员生成并保存，PKG 生成的仅仅是成员的部分私钥。

3.3　签名的生成

设群 B 的成员 p_{Bi} 将对消息 m 进行签名，并通过网络进行广播，最终由群 A 的成员对签名进行验证。p_{Bi} 按照如下步骤生成签名：

(1)随机选择 $k\in Z_q^*$，并公布 $U=kP_{Bi}$ 及 kP_A^2，设 $V=kP_A^2$。

(2)计算 $h=H_1(m,U)$，则 p_{Bi} 对 m 的签字为：$\sigma=(h+k)(S_{Bi}^2+P_A^1)$。

此签字 (m,U,V,h,σ) 在网络上以广播的形式进行传播，群 A 的每一个成员都可以对签名进行验证。在密钥分配初期，PKG 为网络上的每一个群都可选择一个群标志，并将此群标志嵌入相应的成员私钥当中，在群 A 中，其标志是 s，在群 B 中，其标志是 s'。包含此标志的分别是群 A 的成员的私钥 $x_{Ai}sH_0(\mathrm{ID}_{Ai})$ 和群 B 的成员的私钥 $x_{Bi}s'H_0(\mathrm{ID}_{Bi})$。

3.4　签名的验证

正是因为本签名体制在群成员的私钥中嵌入了群标志，才使得签名能被指定接收群的所有成员独立验证。下面是验证的过程及方法:

设有群 A 中的成员 p_{Aj} 将要对签名进行验证，其步骤是：

(1)取得 p_{Bi} 公布的值 $U=kP_{Bi}$，$V=kP_A^2$，并计算 $h=H_1(m,U)$。

(2)验证下列等式是否成立：

$$e((h+k)(S_{Bi}^2+P_A^1),P_{Aj})\stackrel{?}{=}e(hP_{Bi}+U,S_{Aj}^2)e(hP_A^2+V,S_{Aj}^1)\quad(1)$$

如果判别式(1)成立，则可判断该签名正确有效。

4　安全性分析

对于此签名，我们从如下几个方面对其安全性进行分析，并且着重讨论它的不可伪造性。

(1)可验证性　如果给定一个正确的签名，那么指定群内的成员一定可以正确地完成验证过程。

定理 1　对于给定签字 σ，指定群中的成员用判别式(1)一定能够验证签字的有效性和正确性。

证明　不失一般性，我们设群 B 中的成员 p_{Bi} 对 m 生成的签字为 $\sigma=(h+k)(S_{Bi}^2+P_A^1)$，并指定由群 A 中的成员进行验证。各参数的定义与文中所给出的一致，那么我们设群 A 的成员 p_{Aj} 将根据判别式(1)对签字进行验证，有

$$\begin{aligned}&e(\sigma,x_{Aj}H_0(\mathrm{ID}_{Aj}))\\&=e((h+k)(x_{Bi}tH_0(\mathrm{ID}_{Bi})+tsP),x_{Aj}H_0(\mathrm{ID}_{Aj}))\\&=e((h+k)x_{Bi}H_0(\mathrm{ID}_{Bi}),x_{Aj}tH_0(\mathrm{ID}_{Aj}))e((h+k)tP,x_{Aj}sH_0(\mathrm{ID}_{Aj}))\\&=e(hP_{Bi}+U,S_{Aj}^2)e(hP_B^2+V,S_{Aj}^1)。\end{aligned}$$

因此，如果 p_{Bi} 的签名正确有效，那么，签字的指定接收群 A 中的 p_{Aj} 就能够验证该签字。　　证毕

(2)本方案的安全性基于 Diffie-Hellman 问题给定 tsP、tP，各参数的意义同本文的定义，那么求解 sP 在计算上是不可行的。同样，在知道 $x_{Ai}H_0(\mathrm{ID}_{Ai})$，$H_0(\mathrm{ID}_{Ai})$ 的情况下，求解 x_{Ai} 在计算上也是不可行的。

(3)不可伪造性　应用文献[11]中的攻击模型和经过改进了的文献中的若干引理和定理来说明本文所阐述的签名的不可伪造性，在这里也就是证明对签名 σ 的不可伪造性。我们假设攻击者可以获得任意他想得到的由 PKG 发给成员的部分秘钥，即便如此，攻击者采用基于自适应选择明文的存在伪造攻击在计算上也是不可行的。现对模型描述如下：ϖ 是一个多项式时间算法，在本体制中用来模仿攻击者；多项式时间算法 θ 用来模仿签字者和 PKG。各参数的定义与上文给出的定义相同。

(A) θ 建立签名体制，并公布系统参数。

(B) ϖ 进行如下问询：

(a)Hash 函数问询：θ 将 ϖ 的问询作为输入，然后计算 Hash 值并输出给 ϖ 。

(b)私钥问询：给出公钥 P_{Bi} ，θ 将相应的私钥 S_{Bi} 返回给 ϖ 。

(c)签字问询：给出公钥 P_{Bi} 和消息 m ，θ 通过签字过程得到一个关于消息 m 的签字。

(C) 对于一个没有问询过的 (P_{Bi},m)，ϖ 输出 (P_{Bi},m,σ)。如果 σ 是对应与某一个组成员的消息 m 的签名，那么我们就说 ϖ 攻击成功了。

引理 1 如果有一个算法 ϖ_0，对签名 σ 在 t_0 时间段内进行自适应明文攻击和成员身份攻击，具有盈余 ε_0，那么，存在一个算法 ϖ_1，对签名 σ 在时间 $t_1 \le t_0$ 内进行自适应明文攻击和针对某个成员的身份攻击，具有盈余 $\varepsilon_1 \ge \varepsilon_0/q-1$，其中，$q$ 是 Z_q^* 的阶。

证明 不失一般性，我们可以假设对任意成员的公钥，ϖ_0 最多只对相应的私钥和签名询问一次。对于 ϖ_0 输出的签名 $(P_{\text{out}},m,\sigma)$ 有 $\Pr[(P_{\text{out}},m,\sigma)\text{有效}]\ge\varepsilon_0$。假设 ϖ_1 攻击某个组成员 P_{Bi}，那么有 $\Pr[P_{\text{out}}=P_{Bi}\,|\,(P_{\text{out}},m,\sigma)\text{有效}]\ge 1/q-1$，因此就有 $\Pr[P_{\text{out}}=P_{Bi}\cap(P_{\text{out}},m,\sigma)\text{有效}]\ge\varepsilon_0/q-1$，也就是 $\varepsilon_1\ge\varepsilon_0/q-1$，很明显 $t_1\le t_0$。

引理 2 如果有算法 ϖ_1，对签名 σ 进行自适应明文攻击和确定成员 P_{Bi} 的身份攻击，设它做 Hash 函数问询、签字问询、私钥问询的次数至多分别是 q_H,q_S 和 q_k，在时间 t_1 内具有盈余 $\varepsilon_1\ge 10(q_S+1)(q_S+q_H)/(q-1)$，则 CDHP 问题可以在 $t_2\le 120686q_Ht_1/\varepsilon_1$ 得到解决，这里 q 是 Z_q^* 的阶。

证明 我们用文献[12]中的定理 3 来证明此引理。下面是定理 3 的描述：

设 ϖ 是一个输入仅为公共参数的概率多项式时间图灵机。我们以 Q 表示 ϖ 可以问询随机 Oracle 的次数，以 R 表示 ϖ 可以问询签名的次数。假设在时间 T 内，ϖ 以概率 $\varepsilon\ge 10(R+1)(Q+R)/2^k$ 产生一个正确的签名 (m,σ_1,h,σ_2)。如果三元组 (σ_1,h,σ_2) 能在不知道秘钥的情况下，以不可区别的概率分布被模拟，那么存在另外一个可控制 ϖ 的图灵机 ϖ'，它模拟 ϖ 与签字者的交互过程，在 $T'\le 120686QT/\varepsilon$ 的时间内生成两个正确的签名 (m,σ_1,h,σ_2) 和 $(m,\sigma_1,h',\sigma_2')$，这里 $h\ne h'$，k 是安全参数。

现在我们来证明引理 2，设 L 为 GDH 群 G_1 的生成子。给定 (L,aL,bL)，我们将证明我们可以计算得到 abL。从文献[12]的定理 3 的描述我们看到，如果一个算法 ϖ_1 可以以盈余 $\varepsilon_1\ge 10(q_S+1)(q_S+q_H)/(q-1)$ 来伪造签名 (P_{Bi},U,V,h,σ)，那么就有另一个算法 ϖ_2，在时间 $t_2\le 120686q_Ht_1/\varepsilon_1$ 内，通过选择不同的 h，得到另外一个正确的签名 (P_{Bi},U,V,h',σ')。对于本文所设计的签名系统，设攻击者可以获得他想得到的任意成员的部分秘钥，并设 $P_{Bi}=aL=x_{Bi}H_0(\text{ID}_{Bi})$，$tH_0(\text{ID}_{Bi})=bL$，$q\ge 2^k+1$。由两个正确的签字 (P_{Bi},U,h,σ)，(P_{Bi},U,h',σ') 可以得到 $\sigma=h(abL+P_A^1)+k(abL+P_A^1)$ 和 $\sigma'=h'(abL+P_A^1)+k(abL+P_A^1)$。整理两个等式我们得到 $\sigma-\sigma'=(h-h')(abL+P_A^1)$，因此可以解得 $abL=((\sigma-\sigma')/(h-h'))-P_A^1$。$\varpi_2$ 的运行时间为 $t_2\le 120686q_Ht_1/\varepsilon_1$。由此得到下面定理。

定理 2 如果有算法 ϖ_0 对签名 σ 进行自适应明文攻击和成员身份攻击，设它做 Hash 函数问询、签字问询、私钥问询的次数至多分别是 q_H,q_S 和 q_k，在时间 t_1 内具有盈余 $\varepsilon_1\ge 10(q_S+1)(q_S+q_H)$，则 CDHP 问题可以在 $t_2\le 120686q_Ht_0(q-1)/\varepsilon_0$ 得到解决，这里 q 是 Z_q^* 的阶。

在文章中，我们都假定 CDHP 问题是难解的，这与以上结果相矛盾，因此我们说签字 σ 是不可伪造的。

(4)密钥托管的问题 在以往的群向签名方案中，如果有可信赖的 PKG，则存在密钥托管问题，即 PKG 可用任意成员的私钥对任何信息进行签名。在本方案中，PKG 生成群 A，B 的群公钥 $P_A=\{tsP,tP\}$ 和 $P_B=\{P_B^1,P_B^2\}$ 及成员的部分私钥。但是，成员的私钥由成员自己生成。这样，除成员本人外，其他人，包括 PKG 都不知道成员的私钥。

5 结束语

结合应用环境，考虑到基于 ID 的密码体制的优点以及密钥托管等问题，在对文献[9]提出的密钥分配方法进行适当的修改后，本文提出了一种新的群向签名方案，其具有如下特点：基于 ID 的密码概念；不具有密钥托管功能，也就是只有成员自己知道自己的私钥，而其他成员，包括 PKG 也不知道；指定签名验证群中的每一个成员都可以独立的完成对签名的验证。与以往的群向签名体制不同，本签名体制不是基于秘密共享技术的，因此，他不需要多名成员来共同完成对签名的验证。本签名体制在网络中具有定向广播的功能，即签字者只进行一次签名，就可以让所有处在指定接收群的接收者接收并独立地完成验证，这样既减少了对系统资源的占用，又提高了系统的效率。本文最后对签字的安全性进行了讨论，并着重讨论了它的不可伪造性。

参 考 文 献

[1] Desmedt Y. Society and group oriented cryptography: A new concept[A]. Proceedings of CRYPTO 87[C], New York, Lecture Notes in Computer Science, 1988: 120−127.

[2] Pedersen T P. A threshold cryptosystem without a trusted party[A]. Proceedings of EUROCRYPT'91[C], New York, Lecture Notes in Computer Science, 1992: 522−526.

[3] Shoup V. Practical threshold signatures[A]. Advance in Cryptology-Eurocrypt'00[C], New York, Lecture Notes in Computer Science, 1807, 2000: 207−220.

[4] Damgard I, Koprowski M. Practical threshold RSA signature without a trusted dealer[A]. Advances in Cryptology-Eurocrypt'01[C], New York, Lecture Notes in Computer Science, 2045, 2001: 152−165.

[5] Fouque P A, Stern J. Fully distributed threshold RSA under standard assumptions[A]. Proceedings of Asiacrypt'01[C], Gold Coast, Australia, Lecture Notes in Computer Science, 2248, 2001: 310−330

[6] Boldyreva A. Threshold signatures, multisignatures and blind signatures based on the Gap-Diffie-Hellman-Group signatures scheme[A].Proceedings of PKC'2003[C], Miami, FL, USA, Lecture Notes in Computer Science, 2567, 2003：31−64.

[7] Krawczyk H, Rabin T. Chameleon signatures[A]. In Proceedings of NDSS2000[C], San Diego, California, USA, 2000: 143 − 154.

[8] Schneier B 著, 吴世忠, 等译. 应用密码学[M]. 北京：机械工业出版社，2000: 68−70.

[9] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[A]. http://eprint.iacr.org/2003/126/

[10] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[A]. Advances in Cryptology ——Asiacrypt'2001, Gold Coast, Australia, Lecture Notes in Computer Science, [C] 2248, Springer-Verlag, 2001: 514−532.

[11] Jae Choon Cha, Jung Hee Cheon. An identity-based signature from gap Diffie-Hellman groups[A]. Proc. of PKC 2003[C], Miami, FL, USA, Lecture Notes in Computer Science, 2567, 2002: 18−30.

[12] Proincheval D, Stern J. Security aguments for digital signatures and blind signatures[A]. *J. of Cryptology*[J], 2000, 13(3): 361−396.

马春波：　男，1975 年生，博士生，从事密码学、移动通信系统安全、信息系统安全工程的研究.

敖　珺：　女，1977 年生，博士生，从事编码、通信信号处理的研究.

何大可：　男，1944 年生，教授，博士生导师，从事密码学、移动通信系统安全、信息系统安全工程、并行计算、应用数学的研究.