基于身份的可快速撤销代理权的代理签密方案

禹 勇[①] 杨 波[②] 李发根[③] 孙 颖[②]
[①](西安电子科技大学 ISN 国家重点实验室 西安 710071)
[②](华南农业大学信息学院 广州 510642)
[③](电子科技大学计算机科学与工程学院 成都 610054)

摘 要：在代理签密方案中，一个被指定的代理签密人可以代表原始签密人生成有效的代理签密。然而，现有的代理签密方案都没有解决代理撤销问题，即如何收回代理签密人的签密权利。本文基于双线性对，提出了一个新的基于身份的代理签密方案，所提方案引入一个安全中介 SEM，其作用是：帮助合法的代理签密人生成有效的代理签密；监督代理签密人是否按照授权证书的规定签名；检查代理签密人的签密权利是否被撤销。新方案不仅满足代理签密方案的所有安全要求，而且代理签密人只有与 SEM 合作才能生成有效的代理签密，使得方案具有快速撤销的功能。

关键词：数字签名；代理签密；基于身份
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2008)03-0672-04

An ID-based Proxy Signcryption Scheme with Fast Revocation

Yu Yong[①] Yang Bo[②] Li Fa-gen[③] Sun Ying[②]
[①](*National Key Lab. of ISN*, *Xidian University*, *Xi'an* 710071, *China*)
[②](*College of Information*, *South China Agricultural University*, *Guangzhou* 510642, *China*)
[③](*School of Computer Science and Engineering*, *University of Electronic Science and Technology of China*, *Chengdu* 610054, *China*)

Abstract: Proxy signcryption schemes allow an original signcrypter to delegate his signcryption rights to a proxy signcrypter. However, the existing proxy signcryption schemes have the defect that can not solve the proxy revocation problem, that is, how to revoke the delegated signcryption rights of a proxy signcrypter. Based on the bilinear pairings, a new identity-based proxy signcryption scheme is proposed in this paper. A SEcurity Mediator (SEM) is introduced in the scheme to help a proxy signcrypter to generate valid proxy signcryptions, to examine whether a proxy signcrypter signcrypts messages according to the warrant, and to check the revocation of a proxy signcrypter. It is shown that the proposed scheme satisfies all the security requirements of a secure proxy signcryption scheme. Moreover, a proxy signcrypter must cooperate with the SEM to generate a valid proxy signcryption, which makes the new scheme has an effective and fast proxy revocation.

Key words: Digital signature; Proxy signcryption; Identity based

1 引言

代理签名的概念由 Mambo 等[1]于 1996 年提出，在代理签名方案中，原始签名人可以将其签名权利授权给代理签名人，之后代理签名人就可以代表原始签名人进行签名。当验证者验证一个代理签名时，需要同时验证签名和原始签名人的授权协议，代理签名广泛应用于我们的现实生活中，如经理不在的时候，授权其签名权利给他的秘书。1999 年，Lee 和 Kim[2]首次引入了强代理签名的概念。

使消息既保密又认证地传输是信息安全研究的主要目标之一，实现这一目标的传统方法是“先签名后加密”，它所需的代价是签名和加密所需的代价之和，因而效率较低。为了提高效率，Zheng[3]于 1997 年提出了签密的概念。签密能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能，而其计算量和通信成本都要低于传统的“先签名后加密”，因而它是实现既保密又认证地传输消息的较为理想的方法。签密技术已经得到了广泛的应用，如防火墙[4]和密钥分配[5]等。

近几年来，基于身份的密码体制成为密码学界的一个研究热点，该体制最初是由 Shamir[6]于 1984 年提出，其目的是为了简化密钥管理。在基于身份的密码体制中，用户的公钥直接从其身份信息(如姓名、身份证号、E-mail 地址等)得到，而私钥则是由私钥生成中心(PKG)生成。自 1984 年来，相继提出了许多实用的基于身份的签名方案，但一个满意的基于身份的加密方案直到 2001 年才被提出，该方案是由

2006-09-14 收到，2007-05-15 改回
国家自然科学基金(60372046, 60573043)资助课题

Boneh 和 Franklin[7]利用椭圆曲线上的双线性对设计的。

代理签密的概念由 Gamage 等[8]首次提出并给出了一个具体方案，该方案是代理签名方案和签密方案的有机结合，它允许一个原始签密人授权他的签密权利给一个代理签密人，代理签密人可以代表原始签密人对授权消息生成有效的代理签密。2004 年，Li 和 Chen 提出了一个基于身份的代理签密方案[9]；随后，Wang 等人[10] 也提出了两个代理签密方案。代理签密的授权方式与代理签名相同，也分为 3 种：完全授权, 部分授权和基于委任状的授权。在完全授权的代理签密中，原始签密人直接把自己的私钥通过安全信道发送给代理人，由于代理签密人和原始签密人产生的签密是不可区分的，因此，有可能存在陷害；部分授权方式因没有限制代理签密人的签密消息范围而使得代理人可能滥用代理权利;在基于委任状的授权方式中(委任状中包含授权签密消息的范围、有效期等)，原始签密人首先对委任状签名，生成一个代理授权, 发给代理人，这样代理人只能在规定的有效期内代表原始签密人签密。一旦把代理授权发送给代理人以后，随之的问题是如何撤销这个代理授权，自然的答案是，等代理期限到了以后，代理授权自动收回。可是在有些紧急情况下, 比如：(1)发现代理人把代理密钥用于代理签密之外的其他目的，此时需要及时撤销他的代理权。(2)公司的经理原计划出差 3 个月，把签密权力授权给了他的秘书，可是经理提前一个月回来了，此时需要提前收回代理权。现有的代理签密方案都没有解决代理授权快速撤销的问题，本文借鉴 Boneh 等人在文献[11]中的思想，结合 Libert 等提出的基于身份的签密方案[12]，提出了一个具备快速撤销功能的代理签密方案，引入了一个安全中介 SEM，其作用是：(1)帮助合法的代理人生成有效的代理签密; (2)监督代理人是否按照授权证书的规定签密; (3)检查代理人的代理权利是否被撤销。提出的方案基于双线性对，计算有效且密文长度短。

2　预备知识

2.1 双线性对

令 G_1 是由 P 生成的阶为 q 的加法循环群， G_2 是阶为 q 的乘法循环群， q 是一个大素数。若两个群之间的双线性映射 $e: G_1 \times G_1 \to G_2$ 满足以下条件：

(1) 双线性　若 $a,b \in Z_q$，则 $e(aP,bQ)=e(P,Q)^{ab}$；

(2) 非退化性　存在 $P,Q \in G_1$，使得 $e(P,Q) \neq 1$；

(3) 可计算性　存在一个有效的算法计算 $e(P,Q)$，$P,Q \in G_1$；

则称 e 为双线性对。利用椭圆曲线上的 Weil 对或者 Tate 对可以构造满足以上条件的双线性映射，详见文献[7]。相关的数学困难问题：

计算性双线性 Diffie-Hellman 问题(CBDHP)：给定 $(G_1, G_2, e, aP, bP, cP)$，计算 $e(P,P)^{abc}$。

判定性双线性 Diffie-Hellman 问题(DBDHP)：给定 $(G_1, G_2, e, aP, bP, cP, h)$，判断是否 $h=e(P,P)^{abc}$。

2.2 代理签密方案的安全要求

一个安全的代理签密方案需要满足以下性质[2, 3]：

(1)可区分性　任何人都能够区分普通签密和代理签密。

(2)可验证性　从代理签密密文中，验证者能够相信原始签密人认同了这份消息；

(3)强不可伪造性　只有指定的代理人能够产生有效的代理签密，原始签密人和没有被指定为代理人的第三方都不能产生有效的代理签密；

(4)强可识别性　任何人都能从代理签密密文中确定代理人的身份；

(5)强不可否认性　一旦代理人代表原始签密人生成了有效的代理签密，他就不能否认该签密；

(6)防止代理权利的滥用　应该确保代理密钥不能被用于除进行代理签密以外的其它目的。

(7)消息机密性　从一个签密密文中，除指定接收方外，任何人企图获得签密消息的任何信息是计算上不可行的。

3　本文提出的方案

在本文提出的方案中，除了签密接收方 Bob 外，还包含三方：原始签密人 Alice，代理签密人 Carl 和安全中介 SEM，他们的身份分别记为 ID_B, ID_A, ID_C 和 ID_S。SEM 是一个半可信在线第三方，负责验证代理授权和计算部分代理签密。在验证代理授权时，SEM 检查代理期限是否有效，代理人是否在撤销列表中。如果都有效，SEM 给代理人发送部分代理签密，没有 SEM 的帮助，代理人无法生成一个有效的代理签密。因此，如果某个代理签密是在代理期限时间外生成的，那么代理人无法声称该签密是在代理期限时间内生成的，从而弥补了引言中提到的第 1 个缺陷。并且，提出的方案具有快速撤销的功能，如果原始签密人要提前撤销某个代理人的签密权利，他只需通知 SEM 停止给该代理人提供帮助，因此，提出的方案也弥补了第 2 个缺陷。方案描述如下：

系统建立　PKG 选择 (G_1, G_2, P, e) 如上所述，选择安全的 Hash 函数：$H_1: \{0,1\}^* \to G_1^*$，$H_2: G_2 \to \{0,1\}^n$，$H_3: \{0,1\}^* \times G_2 \to Z_q^*$ 和 $H_4: \{0,1\}^* \times G_1 \to Z_q^*$，然后随机选择 $s \in Z_q^*$ 作为主密钥并计算 $P_{\mathrm{pub}}=sP$，PKG 还要选择安全的对称密码算法 (E,D)。最后，PKG 公布系统参数 $(G_1, G_2, P, e, n, P_{\mathrm{pub}}, H_1, H_2, H_3, H_4, E, D)$ 并秘密保存 s。

密钥提取　给定身份 ID, PKG 分别计算 $Q_{\mathrm{ID}}=H_1(\mathrm{ID})$ 和 $D_{\mathrm{ID}}=sQ_{\mathrm{ID}}$ 作为与 ID 对应的公钥和私钥，PKG 通过安全信道把 D_{ID} 发送给 ID。

代理密钥生成　(1)代理生成　原始签密人 A 生成授权证书 ω，在 ω 中包含原始签密人、指定的代理签密人和 SEM 的身份，授权的有效期限，需要签密的消息范围以及其它授权信息。然后 A 随机选择 $x_1, x_2 \in Z_q^*$，计算 $x=x_1+x_2$，$U=xP$ 和 $h=H_4(\omega \,||\, U)$。然后，A 随机选择 $S_r \in G_1^*$，并计算 $S_{\omega p}=hS_r+x_1P_{\mathrm{pub}}$ 和 $S_{\omega s}=h(D_A-S_r)+x_2P_{\mathrm{pub}}$。

(2)代理发送　原始签密人 A 分别发送 $(\omega, U, S_{\omega p})$ 和 $(\omega, U, S_{\omega s})$ 给代理人 Carl 和 SEM，SEM 把 (ω, U) 存储到自

己的存储列表。

(3)代理密钥生成 首先 Carl 和 SEM 验证代理的有效性，Carl 计算 $R_C = e(P, S_{\omega p})$ 并发送 (ω, R_C) 给 SEM; SEM 计算 $R_S = e(P, S_{\omega s})$ 并发送 R_S 给 Carl。他们各自计算 $h = H_4(\omega \,||\, U)$ 并验证是否 $R_C R_S = e(P_{\text{pub}}, hQ_A + U)$ 成立。若该式不成立，他们要求 A 重新发送；否则，B 和 SEM 计算各自的代理密钥：$S_{AC} = S_{\omega p} + hD_C$ 和 $S_{AS} = S_{\omega s} + hD_S$ 。

代理签密生成 (1)代理有效性检查 为了给接收方 Bob 生成消息 m 的有效代理签密，代理人 Carl 必须和 SEM 合作。Carl 发送 (ω, U, R_C, m) 给 SEM，SEM 检查接收到的 (ω, U) 是否与在代理密钥生成阶段接收到的数据相同。如果两者不相同，SEM 不给 Carl 提供签名帮助；如果相同，SEM 检查以下条件：授权证书 ω 中的代理期限是否有效；(ω, U) 是否在自己的撤销列表中。如果 (ω, U) 在 SEM 的撤销列表中，表明该代理人的签密权力已被撤销。若代理期限有效且 (ω, U) 不在 SEM 的撤销列表中，SEM 给代理签名人提供签名帮助，他们合作生成有效的代理签密。

(2)代理签密生成 (a)Carl 和 SEM 各自计算 $Q_B = H_1(\text{ID}_B)$ 。

(b) Carl 随机选择 $r_c \in Z_q^*$ 并计算 $k_{1c} = e(P, P_{\text{pub}})^{r_c}$ 和 $k_{2c} = e(P_{\text{pub}}, Q_B)^{r_c}$ ，然后，Carl 把 (k_{1c}, k_{2c}) 发送给 SEM。

(c) SEM 收到 (k_{1c}, k_{2c}) 后，随机选择 $r_s \in Z_q^*$ 并计算 $k_{1s} = e(P, P_{\text{pub}})^{r_s}$ 和 $k_{2s} = e(P_{\text{pub}}, Q_B)^{r_s}$ ，然后计算 $k_1 = k_{1c} k_{1s}$ ， $k_2 = k_{2c} k_{2s}$ ， $k_3 = H_2(k_2)$ ， $c = E_{k_3}(m)$ ， $r = H_3(\text{ID}_C \,||\, \text{ID}_S, c, k_1)$ 和 $S_{\text{sem}} = r_s P_{\text{pub}} - r S_{AS}$ ，最后，SEM 发送 $(k_1, c, r, S_{\text{sem}})$ 给 Carl。

(d)Carl 收到 $(k_1, c, r, S_{\text{sem}})$ 后，首先计算 $k_{1s}' = e(P, S_{\text{sem}})(R_s \cdot e(P_{\text{pub}}, Q_s)^h)^r$ 并验证是否 $r = H_3(\text{ID}_C \,||\, \text{ID}_S, c, k_{1s}' \cdot k_{1c})$ ，若该式不成立，Carl 要求 SEM 重新发送一次信息；否则，Carl 计算 $S_{\text{pro}} = r_c P_{\text{pub}} - r S_{AC}$ 和 $S = S_{\text{pro}} + S_{\text{sem}}$ ，最终的代理签密被设置为 $\sigma = (\omega, U, c, r, S)$ ，发送给接收方 Bob。

解签密 当 Bob 收到 $\sigma = (\omega, U, c, r, S)$ 后，

(a)计算 $Q_A = H_1(\text{ID}_A), Q_C = H_1(\text{ID}_C)$ 和 $Q_S = H_1(\text{ID}_S)$ ；

(b)计算 $h = H_4(\omega \,||\, U)$ ；

(c)计算 $k_1' = e(P, S)(e(\text{P}_{\text{pub}}, Q_A + Q_C + Q_S)^h e(P_{\text{pub}}, U))^r$ ；

(d) 计 算 $k_3' = H_2(e(S, Q_B)(e(Q_A + Q_C + Q_S, D_B)^h e(U, D_B))^r)$ ；

(e)恢复 $m = D_{k_3'}(c)$ ，如果 $r = H_3(\text{ID}_C \,||\, \text{ID}_S, c, k_1')$ 成立，Bob 接受 σ ；否则，拒绝。

授权撤销 如果由于某些原因如发现代理人 Carl 滥用代理权利，Alice 可以提前撤销 Carl 的代理权利，此时，Alice 只需通知 SEM 把相应的 (ω, U) 加入撤销列表中。当 Carl 请求 SEM 帮助他生成代理签密时，SEM 检查代理授权日期是否过期以及在撤销列表中是否包含 (ω, U) ，只要有一个条件成立，SEM 都不会为 Carl 提供签密帮助。一旦 SEM 发现某个代理授权已经过期，他就从撤销列表中删除对应的 (ω, U) 项，以免撤销列表长度无限增加。

4 安全性分析

提出的基于身份的代理签密方案满足代理签密的所有安全性质。

(1)可区分性 在一个有效的代理签密密文中包含授权 ω ，并且在签密验证时，需要用到授权 ω 、原始签密人和代理签密人的公钥，因此，一个有效的代理签密与代理人的普通签密是可以区分的。

(2)可验证性 在提出的方案中，消息 m 的代理签密由 (ω, U, c, r, S) 组成。签密的验证人从授权 ω 中可以得知原始签密人、代理人和 SEM 的身份，并且，由于在代理签密验证中使用到原始签密人的公钥 Q_A ，签密验证人可以相信对该消息的签密是经过原始签密人同意的。

(3)强不可伪造性 考虑两种形式的攻击，外部攻击和内部攻击。内部攻击是指 SEM 企图伪造某个消息 m 的代理签密；外部攻击是指除 SEM 之外的第三方企图伪造某个消息 m 的代理签密。我们首先证明 Carl 和 SEM 的部分代理签密与 Libert 和 Quisquater 的签密[12]等价，然后再证明提出的方案可以抵抗外部攻击和内部攻击。

定理 1 假设 Hash 函数 H_3 是安全的，那么 Carl 和 SEM 的部分代理签密与 Libert 和 Quisquater 的签密[12]等价。

证明 在 Libert 和 Quisquater 的签密方案中，消息 m 的一个有效的签密为 (c, r, S) ，其验证方程可表示为

$$r = H_3(c, e(P, S) e(P_{\text{pub}}, Q_A)^r) \tag{1}$$

在本文的方案中，SEM 对消息 m 的部分代理签密为 $(k_1, c, r, S_{\text{sem}})$ ，其验证式可以表示为

$$r = H_3(\text{ID}_C \,||\, \text{ID}_S, c, e(P, S_{\text{sem}})(R_s \cdot e(P_{\text{pub}}, Q_s)^h)^r \cdot k_{1c}) \tag{2}$$

提前固定 k_{1c} 后，可以看出式(1)和式(2)是等价的，这就意味着，找到满足式(2)的 $(k_1, c, r, S_{\text{sem}})$ 与找到满足式(1)的 (c, r, S) 是同等困难的。另一方面，在式(2)中，已知 r 求 $(c, S_{\text{sem}}, k_{1c})$ 是困难的，因为 H_3 是安全的 Hash 函数。在 DBDH 问题是困难的假设下，Libert 和 Quisquater 的签密方案[12]已被证明是安全的，故 SEM 对消息 m 的部分代理签密是不可伪造的。同理，Carl 的部分代理签密与 Libert 和 Quisquater 的签密[12]等价。 证毕

定理 2 本文提出的方案抗外部攻击。

证明 对于一个外部敌手 A，他企图伪造消息 m 的代理签密，即敌手 A 在获得原始签密人、代理签密人和 SEM 的公钥后，企图伪造 $\sigma = (\omega, U, c, r, S)$ 满足代理签密验证式。验证式可以表示为：

$$r = H_3(\text{ID}_C \,||\, \text{ID}_S, c, e(P, S) \cdot (e(P_{\text{pub}}, Q_A + Q_C + Q_S)^h e(P_{\text{pub}}, U))^r) \tag{3}$$

在式(3)中，令 $Q = Q_A + Q_C + Q_S$ ，伪造满足式(3)的 (c, r, S) 与伪造 Libert 和 Quisquater 的签密等价，而 Libert 和

Quisquater 的签密方案[12]已被证明是安全的，故提出的方案抗外部攻击。即使是原始签密人，由于不能获得代理人的代理私钥，也无法伪造消息 m 的代理签密。　　证毕

定理 3　本文提出的方案抗内部攻击，即，SEM 也无法伪造消息 m 的代理签密。

证明　SEM 在获得原始签密人、代理签密人和 SEM 的公钥、SEM 的私钥以及 SEM 的代理签密密钥后，他企图伪造 $\sigma=(\omega,U,c,r,S)$ 满足代理签密验证式。设 SEM 对消息 m 的部分代理签密为 (k_1,c,r,S_{sem})，假如 SEM 能够成功伪造消息 m 的代理签密 $\sigma=(\omega,U,c,r,S)$，则 $(k_1,c,r,S-S_{\text{sem}})$ 是代理人对消息 m 的部分代理签密，由定理 1 可知，伪造代理人对消息 m 的部分代理签密与伪造 Libert 和 Quisquater 的签密等价，故 SEM 无法伪造消息 m 的代理签密，本文提出的方案抗内部攻击。　　证毕

由以上分析可知，本文提出的方案具有强不可伪造性。从另一个角度，本文提出的代理签密方案可以看成 Libert 和 Quisquater 签密方案[12]的 (2,2) 门限版本，故只有代理人与 SEM 合作才能生成有效的代理签密。

(4)强可识别性　在本文提出的方案中，代理人的身份信息包含在授权 ω 中，并且在签密验证中需要代理人的公钥，因此，验证人可以从代理签密密文中确定代理人的身份。

(5)强不可否认性　由于离散对数问题的困难性，只有代理人 Carl 自己知道他的私钥 D_C，因此，一旦 Carl 生成了一个有效的代理签密，他就无法否认，因为该签密是用他的私钥生成的。

(6)防止签名权利滥用　由代理签密生成过程可知，只有代理人 Carl 与 SEM 合作才能代表原始签密人生成有效的代理签密，因此，他要对代理签密负责。一经发现 Carl 滥用代理权利，原始签密人立即通知 SEM 停止给 Carl 提供签密帮助，这样因 Carl 得不到 SEM 的部分代理签密而无法生成有效的代理签密，达到了即时撤销的目的。除代理人之外的其他人都无法滥用代理权，因为他们不能生成有效的代理签密。

(7)消息机密性　对于消息机密性，我们得到以下定理。

定理 4 本文提出方案的消息机密性与Libert和Quisquater签密方案的消息机密性等价。

证明　在 Libert 和 Quisquater 签密方案中，消息 m 的有效的密文是 $c=E_{k_2}(m)$，其中

$$k_2=H_2(e(S,Q_B)e(Q_A,D_B)^r) \tag{4}$$

在本文提出的方案中，消息 m 的一个有效的密文是 $c=E_{k_3}(m)$，其中

$$k_3=H_2(e(S,Q_B)(e(Q_A+Q_C+Q_S,D_B)^h e(U,D_B))^r) \tag{5}$$

在式(5)中，令 $Q=Q_A+Q_C+Q_S$，则式(4)与式(5)等价，也就是说，计算满足式(5)的 k_3 与计算满足式(4)的 k_2 同样困难，故提出方案的消息机密性与 Libert 和 Quisquater 签密方案的消息机密性等价。　　证毕

5　结束语

代理权的撤销是代理签密中的一个重要问题，如果解决不好，代理签密无法走向实用，本文提出了一个具备快速撤销功能的代理签密方案，SEM 的引入较好地解决了代理快速撤销问题。最后，分析了提出的方案满足代理签密方案的所有性质。

参 考 文 献

[1] Mambo M, Usuda K, and Okamoto E. Proxy signature: Delegation of the power to sign message[J]. *IEICE Tran. on Fundam*, 1996, E79-A(9): 1338–1353.

[2] Lee B, Kim H, and Kim K. Strong proxy signature and its applications[C]. Proc of SCIS'01, Oiso, Japan, 2001: 603–608.

[3] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption<< cost (signature)+cost (encryption)[C]. Proc of CRYPTO'97, Berlin: Springer-Verlag, 1997, LNCS 1294.: 165–179.

[4] Gamage C, Leiwo J, and Zheng Y. Encrypted message authentication by firewalls[C]. Proc of PKC'99, Berlin: Springer-Verlag, 1999, LNCS 1560: 69–81.

[5] 陈伟东，冯登国. 签密方案在分布式协议中的应用[J]. 计算机学报, 2005, 28(9): 1421–1430.
Chen W D and Feng D G. Some applications of signcryption schemes to distributed protocols[J]. *Chinese Journal of Computers*, 2005, 28(9): 1421–1430.

[6] Shamir A. Identity-based cryptosystems and signature schemes[C]. Proc of CRYPTO'84, Berlin: Springer-Verlag, 1984, LNCS 196: 47–53.

[7] Boneh D and Franklin M. Identity-based encryption from the weil pairing[C]. Proc of CRYPTO 2001, Berlin: Springer-Verlag, 2001, LNCS 2139: 213–229.

[8] Gamage C, Leiwo J, and Zheng Y. An efficient scheme for secure message transmission using proxy signcryption [C]. Proc of 22nd Australasian computer science conference, Berlin: Springer-Verlag, 1999: 420–431.

[9] Li X and Chen K. Identity based proxy signcryption sheme from pairings[C]. Proc of the 2004 IEEE International conference on services computing, Shanghai, 2004: 494–497.

[10] Wang Q and Cao Z F. Two proxy signcryption schemes from bilinear pairings[C]. Proc of CANS 2005, Berlin: Springer-Verlag, 2005, LNCS 3810: 161–171.

[11] Boneh D, Ding X, and Tsudik G, *et al.*. A method for fast revocation of public key certificates and security capabilities[C]. Proc of the 10th USENIX Security Symposium, Washington D. C, 2001: 297–308.

[12] Libert B and Quisquater J J. A new identity based signcryption schemes from pairings[C]. Proc of IEEE information theory workshop, Paris, France, 2003: 155–158.

禹　勇：　男，1980 年生，博士生，研究方向为信息安全、密码学.
杨　波：　男，1963 年生，教授，博士生导师，研究方向为信息安全密码学.
李发根：　男，1979 年生，博士，讲师，研究方向为密码学.
孙　颖：　女，1980 年生，硕士，助教，研究方向为信息安全.