具有代理解签密功能的无证书签密方案

于 刚 韩文报
(解放军信息工程大学信息工程学院 郑州 450002)

摘 要 首先,提出具有代理解签密功能的签密概念.此模型中,原始解签密者把消息分为不同的主题,按照主题把解密权力授予不同的代理人;代理人可以代替原始解签密者解密其授权主题下的密文.其次,给出安全模型并基于无证书公钥密码体制提出一个具体方案.最后,基于 Weak-BDH 难题证明该方案的安全性.

关键词 无证书公钥密码体制;签密;可证安全;代理解签密
中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2011.01291

Certificateless Signcryption Scheme with Proxy Unsigncryption

YU Gang HAN Wen-Bao
(*Institute of Information Engineering, People's Liberation Army Information Engineering University, Zhengzhou* 450002)

Abstract Firstly, this paper gives a new signcryption model, named signcryption with proxy unsigncryption. In this model, the original unsigncrypter divides messages into several subjects and delegates his unsigncryption powers to different proxies. The authorized proxies can directly unsigncrypt ciphertexts for the original unsigncrypter. Secondly, this paper gives the security model and based on certificateless public key cryptography give a concrete scheme. At last, this paper proves its security based on Weak-BDH problem.

Keywords certificateless public key cryptography; signcryption; provable secure; proxy unsigncryption

1 引 言

2003 年,Al-Riyami 和 Paterson[1] 提出无证书公钥密码系统(CL-PKC).CL-PKC 是传统公钥密码系统和基于身份密码系统的折中.在 CL-PKC 中,密钥生成中心(KGC)根据系统主密钥和用户的身份生成用户部分私钥,而用户选择秘密值,利用秘密值与 KGC 分发的部分私钥一起生成完全私钥,完全私钥作为用户密钥进行签名或者解密.CL-PKC 既避免了传统公钥密码系统中 PKI 证书管理负担(包括证书的颁发、传输、存储、验证及撤销等),又解决了基于身份公钥密码系统的密钥托管问题——私钥生成中心 PKG 为每一个用户生成私钥,恶意 PKG 可以伪造任意用户的私钥.

使消息既保密又认证地传输是信息安全研究的重要目标之一.实现这一目标的传统方法是"先签名后加密".具体做法是先将消息签名,然后将消息及签名一起加密生成密文,其代价是签名代价与加密代价之和,因此效率较低.为了提高效率,1997 年,Zheng[2] 提出签密的概念.签密能够在同一个逻辑步骤内同时完成签名和加密两项功能,是实现既保密又认证消息传输的理想方法.2008 年,Barbosa 与 Farshim[3] 首次将签密思想引入到无证书公钥密码体制,提出基于无证书公钥密码体制的签密概念,并给出一个有效的方案.此后,许多无证书签密方案被

收稿日期:2010-11-11;最终修改稿收到日期:2011-04-01.本课题得到国家自然科学基金(61003291)和国家"八六三"高技术研究发展计划项目基金(2009AA01Z417)资助.于 刚,男,1984 年生,博士研究生,主要研究方向为信息安全.E-mail: gyu1010@126.com.韩文报,男,1963 年生,教授,博士生导师,主要研究领域为密码学.

提出，例如文献[4-6]等.

代理密码体制的概念由 Mambo 等人[7]在 1996 年提出，主要指的是签名权力授权与代理. 随着信息化的迅速发展，代理业务需求越来越大，相应的许多拓展概念及方案被提出，如门限代理签名[8]、代理解密[9]、代理签密[10]、多代理多签密[11]、无证书多代理签密[12]等.

本文从解签密角度出发，基于无证书公钥密码体制提出具有代理解签密功能的签密概念. 不妨考虑以下场景：假设 Bob 是一个业务繁忙的公司经理，他需要经常出差. 而每天他又需要处理一大堆经过签密的密文文件. 为了把他自己从繁忙的工作中解放出来也为了避免因其不在公司而导致重要业务流失，他把消息分成几类，像 E-mail 的主题一样为每一类消息命名一个主题. 然后，他就可以安排不同的助理代替自己处理不同主题下的业务.

正是基于此类需求，本文提出具有代理解签密功能的无证书签密，原始解签密者把消息划分为不同主题，并把解签密的权力按照主题分别授权给不同代理解签密者. 代理解签密者能解密其授权主题下的签密密文. 此外，基于公告牌提出一个拓展方案，实现了原始解签密者通过公告牌随时终止某主题下代理解签密者解签密授权的功能.

2 基础知识

2.1 双线性对

设 G_1 为大素数 q 阶的加法循环群；G_2 为 q 阶的乘法循环群，双线性对是满足以下性质的映射 $\hat{e}:G_1\times G_1\rightarrow G_2$：

(1) 双线性性. 对于任意的 $P,Q\in G_1$ 和所有的 $a,b\in Z_q^*$，有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$.

(2) 非退化性. 存在 $P,Q\in G_1$，使得 $\hat{e}(P,Q)\neq 1$.

(3) 可计算性. 对所有的 $P,Q\in G_1$，$\hat{e}(P,Q)$ 可以在多项式时间内有效计算出来.

本文方案的安全性基于 CDH 问题及弱双线性 Diffie-Hellman 问题(Weak-BDH 问题).

定义 1. CDH 问题. 设 P 是 G_1 的生成元，群 G_1 中的 CDH 问题是：给定 (P,aP,bP)，其中 $a,b\in Z_q^*$，求解 abP.

定义 2. Weak-BDH 问题. 设 $(G_1,G_2,q,\hat{e})$ 是双线性对系统，P 是 G_1 的生成元，Weak-BDH 问题是：给定 $(P,aP,bP,cP,cw_1,\cdots,cw_l)$，其中 $a,b,c,l\in Z_q^*$，$w_i\in G_1$，求解 $\hat{e}(P,P)^{abc}$.

2.2 具有代理解签密功能无证书签密的形式化定义

具有代理解签密功能的无证书签密，记为 PUCLSC，由以下 7 个算法组成：

(1) 系统初始化(Setup). 给定安全参数 1^k，该算法生成系统的公开参数 $Params$ 和主密钥 s. 记为 $(Params,s)\leftarrow Setup(1^k)$.

(2) 部分私钥生成(Partial Secret Key Generate). 给定身份 ID_U，KGC 为用户生成部分私钥 PSK_U. 记为 $PSK_U\leftarrow PSKG(ID_U,s,Params)$.

(3) 公钥生成(Public Key Generate). 用户 ID_U 选取秘密值 x_U，结合 $Params$ 以及身份生成对应公钥 P_U. 记为 $P_U\leftarrow PKG(ID_U,x_U,Params)$.

(4) 完全私钥生成(Full Secret Key Generate). ID_U 利用秘密值 x_U 及部分私钥 PSK_U 生成完全私钥 FSK_U. 记为 $FSK_U\leftarrow FSKG(ID_U,x_U,PSK_U,Params)$.

(5) 代理私钥生成(Proxy Secret Key Generate). 原始解签密者，Alice，要把解签密权力分别授权给 l 个代理解签密者 $P_1,\cdots,P_l$，首先他把消息分成 l 类，并为每一类定义主题 $sub_i,i=1,2,\cdots,l$. 然后，Alice 利用完全私钥 FSK_A 为主题 sub_i 生成代理私钥 S^{sub_i}，并把代理私钥 S^{sub_i} 秘密发送给代理者 P_i. 记为 $S^{sub_i}\leftarrow PRSKG(sub_i,FSK_A,Params)$.

(6) 签密(Signcrypt). 发送消息 $m\in sub_i$ 给原始解签密者 ID_A，发送者 ID_B 利用 ID_A 的公钥 P_A 及自己的完全私钥 FSK_B 生成密文 δ. 记为 $\delta\leftarrow SC(ID_B,FSK_B,ID_A,P_A,sub_i,m)$.

(7) 解签密(Unsigncrypt). 收到密文 δ，原始解签密者 Alice 以及该主题的代理解签密者分别利用完全私钥 FSK_A 或代理私钥 S^{sub_i} 恢复消息 $m\in sub_i$，或输出“$\perp$”表示解签密失败. 记为 $m\leftarrow USC(ID_B,P_B,ID_A,FSK_A(S^{sub_i}),sub_i,\delta)$.

2.3 具有代理解签密功能的无证书签密的安全模型

我们的安全模型基于 Barbosa 和 Farshim[3]提出的无证书签密的安全模型. 对于无证书公钥密码体制，存在两种类型攻击，I 型攻击和 II 型攻击，对应着两种敌手，A_{I} 和 A_{II}. A_{I} 代表着第三方攻击，A_{I} 不能得到 KGC 的主密钥但是可以随意替换用户的公钥；A_{II} 代表着恶意的 KGC 攻击，A_{II} 知道主密钥但是不允许替换任何公钥.

定义 3. 机密性. PUCLSC 称作是适应性选择密文攻击安全(IND-PUCLSC-CCA2)，如果不存在任何多项式有界的攻击者(包括 A_{I} 和 A_{II})以不可

忽略的概率赢得下面的游戏：

IND-PUCLSC-CCA2-x.

$(s,Params)\leftarrow Setup(1^k)$

$(ID_S^*,ID_R^*,(m_0^{\beta_1},m_1^{\beta_1}),\cdots,(m_0^{\beta_k},m_1^{\beta_k}))\leftarrow$

$A_{Phase_1}^{O_1}(Params,aux)$,

$1\leq i\leq k\leq l, m_0^{\beta_i},m_1^{\beta_i}\in\{sub_i\}$,

$\gamma\leftarrow\{0,1\}$,

$\delta_i^*\leftarrow SC(ID_S^*,FSK_S^*,ID_R^*,P_R^*,sub_i,m_\gamma^{\beta_i})$,

$i=1,2,\cdots,k$,

$\gamma'\leftarrow A_{Phase_2}^{O_2}(\delta_1^*,\cdots,\delta_k^*)$,

$Adv(A_{\text{IND-PUCLSC-CCA2-x}})=|2P[\gamma'=\gamma]-1|$,

其中，$m_0^{\beta_i}$ 和 $m_1^{\beta_i}$ $(1\leq i\leq k)$ 是相同长度的消息；ID_S^* 和 ID_R^* 是不同身份；当 $x=\text{I}$ 时，aux 为空，当 $x=\text{II}$ 时，$aux=s$.

在上述游戏的阶段 1 和阶段 2 中，敌手可以向挑战者 C 进行以下询问：

(1) 部分私钥询问. 敌手询问用户 ID_U 的部分私钥 PSK_U，C 返回对应的部分私钥 PSK_U.

(2) 公钥询问. 敌手询问用户 ID_U 的公钥，C 返回对应的公钥 P_U.

(3) 完全私钥询问. 敌手询问用户 ID_U 的完全私钥 FSK_U，如果 ID_U 的公钥没有被敌手替换，C 返回对应的完全私钥 FSK_U.

(4) 公钥替换. 敌手可以向挑战者要求把用户 ID_U 的公钥 P_U 替换为 P_U'.

(5) 代理私钥询问. 敌手可以询问主题 sub_i 下的代理私钥，C 返回对应的代理私钥 S^{sub_i}. 这里敌手至多询问 $l-1$ 个代理私钥.

(6) 签密询问. 敌手给定发送者身份 ID_S、接收者身份 ID_R、公钥 P_R 和消息 $m\in sub_i$，C 返回密文 δ.

(7) 解签密询问. 敌手给定密文 δ、发送者身份 ID_S、公钥 P_S、接收者身份 ID_R、C 返回消息 m 或者 $\perp$.

此外，在上述游戏中，A_I 需要遵守以下限制：

(1) A_I 不能询问 ID_R^* 的完全私钥以及挑战主题 sub_{i^*} 对应的代理私钥 $S^{sub_{i^*}}$.

(2) 敌手 A_I 不能询问公钥被替换用户的完全私钥.

(3) 敌手 A_I 不能同时在挑战阶段结束前替换 ID_R^* 的公钥和在某一阶段询问 ID_R^* 的部分私钥.

(4) 敌手不能对挑战密文 $\delta_1^*,\cdots,\delta_k^*$ 执行解签密询问除非发送者或者接收者的公钥被替换.

A_II 需要遵守以下限制：

(1) 敌手 A_II 不能替换任何公钥.

(2) 敌手 A_II 不能询问 ID_R^* 的完全私钥以及挑战主题 sub_{i^*} 对应的代理私钥 $S^{sub_{i^*}}$.

(3) 敌手 A_II 不能对挑战密文 $\delta_1^*,\cdots,\delta_k^*$ 进行解签密询问.

定义 4. 不可伪造性. PUCLSC 称作是适应性选择消息攻击下存在性不可伪造(EUF-PUCLSC- ACMA)的，如果不存在任何多项式有界的攻击者以不可忽略的概率赢得如下定义的游戏：

EUF-PUCLSC-ACMA-x

$(s,Params)\leftarrow Setup(1^k)$,

$(ID_S^*,ID_R^*,\delta^*,sub_{i^*})\leftarrow A^O(Params,aux)$,

$Adv(A_{\text{EUF-PUCLSC-ACMA-x}})=$

$Pr\{A_{\text{EUF-PUCLSC-ACMA-x}}\text{成功}\}$,

其中，当 $x=\text{I}$ 时，aux 为空，当 $x=\text{II}$ 时，$aux=s$. 如果密文 ID_S^*、ID_R^*、δ^*、sub_{i^*} 不是签密询问产生的，也没询问 ID_S^* 的完全私钥，那么敌手成功当且仅当对密文解签密的结果不是 $\perp$.

同游戏 IND-PUCLSC-CCA2-x，敌手可以获得 C 的预言服务. 此外，在上述游戏中，A_I 需要遵守以下限制：

(1) 敌手 A_I 不能询问 ID_S^* 的完全私钥；敌手 A_I 不能询问公钥被替换的用户的完全私钥.

(2) 敌手 A_I 不能同时在挑战阶段结束前替换 ID_S^* 的公钥和在某一阶段询问 ID_S^* 的部分私钥.

A_II 需要遵守以下限制：

(1) 敌手 A_II 不能替换任何公钥.

(2) 敌手 A_II 不能询问 ID_S^* 的完全私钥.

3　PUCLSC 方案

本节，首先基于无证书公钥密码体制给出一个基础方案：B-PUCLSC；然后，基于公告牌提出一个拓展方案：F-PUCLSC. F-PUCLSC 中原始解签密者可以通过公告牌随时终止代理解签密者的解签密授权，即使代理解签密者仍处在合法授权期内.

3.1　基础方案 B-PUCLSC

系统初始化. 设 G_1 为大素数 q 阶的加法循环群，生成元为 P；G_2 为 q 阶的乘法循环群；$\hat{e}:G_1\times G_1\rightarrow G_2$ 为双线性对；定义 4 个安全的 Hash 函数：$H_0:\{0,1\}^{n_1}\rightarrow G_1^*$，$H_1:\{0,1\}^{n_2}\rightarrow G_1^*$，$H_2:G_1\times G_1\times\{0,1\}^{n_3}\times\{0,1\}^{n_1}\times G_1\times\{0,1\}^{n_1}\times G_1\rightarrow Z_q^*$，$H_3:G_2\rightarrow G_1^*\times\{0,1\}^{n_3}\times\{0,1\}^{n_1}$，$n_1,n_2,n_3$ 分别表示身份、主题和消息的比特长度；KGC 随机选择主密钥 $s\in Z_q^*$，计算系统公钥 $P_{Pub}=sP$. 最后，KGC 秘密保

存 s,公开系统参数 $Params=\{G_1,G_2,q,\hat{e},P,P_{Pub},H_0,H_1,H_2,H_3\}$.

部分私钥生成. 用户将身份 ID_U 提交给 KGC,KGC 计算对应的部分私钥 $PSK_U=sQ_U$,其中 $Q_U=H_0(ID_U)$,并将 PSK_U 秘密发送给 ID_U.

公钥生成. 用户 ID_U,生成其公钥 $P_U=(X_U,Y_U)$ 如下:

①随机选择 $x_U\in Z_q^*$.

②计算 $X_U=x_UP$,$Y_U=x_UP_{Pub}$,并公开 $P_U=(X_U,Y_U)$.

任何人可以通过等式:$\hat{e}(X_U,P_{Pub})=\hat{e}(Y_U,P)$ 验证其形式上的正确性.

完全私钥生成. 用户 ID_U 的完全私钥为 $FSK_U=x_UPSK_U=x_U\cdot s\cdot Q_U$.

代理私钥生成. 假设用户,Alice(原始解签密者),其身份 ID_A、公钥 P_A、完全私钥 FSK_A,要把解签密权力分别授权给 $l\in Z_q$ 个代理解签密者 $P_1,\cdots,P_l$,执行以下步骤:

1. 将所有消息 $m\in\{0,1\}^{n_3}$ 划分为 l 类,对每一类定义主题 $sub_i\in\{0,1\}^{n_2}$,$i=1,2,\cdots,l$,公布 sub_i.

2. 对于主题 $sub_i\in\{sub_1,\cdots,sub_l\}$,Alice 生成该主题下的代理解签密密钥:

2.1. 随机选择 $d_i\in Z_q^*$.

2.2. 计算 $S^{sub_i}=(S_1^{sub_i},S_2^{sub_i})=(d_iw_i+FSK_A,d_iP)$,其中 $w_i=H_1(sub_i)$.

3. Alice 将 S^{sub_i} 通过安全方式秘密分发给相应的代理解签密者 P_i.

签密. 发送者 Bob(身份 ID_B、完全私钥 FSK_B),执行以下步骤:

1. 随机选择 $r\in Z_q^*$,计算 $U=rP$ 和 $W=rw_i$,其中 $w_i=H_1(sub_i)$.

2. 计算 $h=H_2(U,W,m,ID_A,X_A,ID_B,X_B)$.

3. 计算 $V=rQ_B+h\cdot FSK_B$.

4. 计算 $k_t=H_3(\hat{e}(Y_A,Q_A)^r)$ 和 $z=V\parallel m\parallel ID_B\oplus k_t$.

5. 密文为 $\langle sub_i,U,W,z\rangle$.

解签密. Alice 收到密文 $\langle sub_i,U,W,z\rangle$ 后,

1. 计算会话密钥 k_t:

1.1. 原始解签密者,Alice,计算:$k_t=H_3(\hat{e}(U,FSK_A))$.

1.2. 代理解签密者,P_i,计算:$w_i=H_1(sub_i)$,$k_t=H_3\left(\dfrac{\hat{e}(S_1^{sub_i},U)}{\hat{e}(S_2^{sub_i},W)}\right)$.

2. 恢复明文消息 $V\parallel m\parallel ID_B=z\oplus k_t$.

3. 验证 Bob 对消息的签名. $\hat{e}(V,P)=\hat{e}(U+hY_B,Q_B)$,其中 $h=H_2(U,W,m,ID_A,X_A,ID_B,X_B)$.

注. 如果 Bob 希望该消息由 Alice 本人恢复消息,可以设置 $W=0$. 基础方案中,如果发送者正常签密,原始解签密者不能终止代理解签密者在合法授权下恢复消息.

3.2 拓展方案 F-PUCLSC

系统初始化. 除 Hash 函数 H_2 略微改变,变为 $H_2:G_1^3\times\{0,1\}^{n_3}\times\{0,1\}^{n_1}\times G_1\times\{0,1\}^{n_1}\times G_1\to Z_q^*$ 外,其它参数同基础方案一样.

部分私钥生成、公钥生成、完全私钥生成,同基础方案.

代理私钥生成.

1. 代理私钥生成:

1.1. 将消息 $m\in\{0,1\}^{n_3}$ 划分为 l 类,对每一类定义主题 $sub_i\in\{0,1\}^{n_2}$,$i=1,2,\cdots,l$,公布 sub_i.

1.2. 对于主题 $sub_i\in\{sub_1,\cdots,sub_l\}$,Alice 如下生成代理解签密密钥 S^{sub_i}:

1.2.1. 随机选择 $b_0,b_1,d_i\in Z_q^*$,其中 $b_0+b_1=1\bmod q$.

1.2.2. 计算 $S^{sub_i}=(S_1^{sub_i},S_2^{sub_i})=(d_iw_i+b_0-FSK_A,d_iP)$,其中 $w_i=H_1(sub_i)\in G_1$.

1.3. Alice 将 S^{sub_i} 通过安全方式秘密分发给代理解签密者 P_i.

2. 公告牌参数更新:

2.1. 对某一时段 $\tau_j\in\{\tau_1,\tau_2,\cdots\}$,$\tau_j\in\{0,1\}^{n_1}$,选择 $d_i^{\tau_j}\in Z_q^*$.

2.2. 计算 $P(\tau_{j_i})=(x(\tau_{j_i}),y(\tau_{j_i}))=(b_1\cdot FSK_A+d_i^{\tau_j}\Gamma_j,d_i^{\tau_j}P)$,其中 $\Gamma_j=H_0(\tau_j)$.

2.3. Bob 在公告牌上为其代理解签密者更新 $P(\tau_{j_i})$.

签密. 发送者 Bob(身份 ID_B、完全私钥 FSK_B),执行以下步骤:

1. 随机选择 $r\in Z_q^*$,计算 $U=rP$、$W=rw_i$ 和 $T=r\Gamma_j$,其中 $w_i=H_1(sub_i)$、$\Gamma_j=H_0(\tau_j)$.

2. 计算 $h=H_2(U,W,T,m,ID_A,X_A,ID_B,X_B)$.

3. 计算 $V=rQ_B+h\cdot FSK_B$.

4. 计算 $k_t=H_3(\hat{e}(Y_A,Q_A)^r)$ 和 $z=V\parallel m\parallel ID_B\oplus k_t$.

5. 密文为 $\langle sub_i,U,W,T,z\rangle$.

解签密. Alice 收到密文 $\langle sub_i,U,W,T,z\rangle$ 后,

1. 计算会话密钥 k_t:

1.1. 原始解签密者 Alice 计算 $k_t=H_3(\hat{e}(U,FSK_A))$.

1.2. 代理解签密者,P_i,计算:$w_i=H_1(sub_i)$,$k_t=H_3\left(\dfrac{\hat{e}(S_1^{sub_i}+x(\tau_{j_i}),U)}{\hat{e}(S_2^{sub_i},W)\hat{e}(y(\tau_{j_i}),T)}\right)$.

2. 恢复明文消息 $V\parallel m\parallel ID_B=z\oplus k_t$.

3. 验证 Bob 对消息的签名:$\hat{e}(V,P)=\hat{e}(U+hY_B,Q_B)$,其中 $h=H_2(U,W,T,m,ID_A,X_A,ID_B,X_B)$.

注. 如果发送者希望该消息由原始解签密者本人恢复消息,可以设置 $W=0$ 和 $T=0$. 拓展方案中,

如果主题 sub_i 下的代理解签密者被腐化，原始解签密者把原来的 $b_0, b_1, d_i, d_i^{\tau_j} \in Z_q^*$ 改为 b_0'，b_1'，$d_i' d_i^{\tau_j\prime} \in Z_q^*$，其中 $b_i \neq b_i'$，$i=0,1$，$d_i \neq d_i'$，$d_i^{\tau_j} \neq d_i^{\tau_j\prime}$，$b_0'+b_1'=1 \bmod q$. 然后在公告牌上更新 $P(\tau_{j_i})$，并把新的代理解密私钥秘密发送给新的代理者.

4　安全分析

本节对基础方案，B-PUCLSC 的安全性做简单分析，拓展方案安全分析类似. 假设敌手最多进行 q_i 次 H_i 询问（$i=0,1,2,3$），q_s 次签密询问、q_u 次解签密询问.

机密性. 在 Weak-BDH 难题假设下，B-PUCLSC 方案是适应性选择密文攻击安全的.

B-PUCLSC 的机密性可以由以下两个引理得到.

引理 1.　假设存在 I 类敌手 $A_{\text{IND-PUCLSC-CCA2-I}}$ 能够以优势 $Adv(A_{\text{IND-PUCLSC-CCA2-I}})$ 赢得游戏 IND-PUCLSC-CCA2-I，则存在挑战者 C 以优势 ε 解决 Weak-BDH 问题，其中：

$$\varepsilon \geq \left(1-\frac{q_s q_3}{q}\right) \cdot \left(1-\frac{q_s \cdot (q_2+q_3+2q_s)}{q}\right) \cdot \frac{1}{q_0} \cdot \frac{1}{q_3} \cdot Adv(A_{\text{IND-PUCLSC-CCA2-I}}).$$

证明见附录 1.

引理 2.　假设存在 II 类敌手 $A_{\text{IND-PUCLSC-CCA2-II}}$ 能够以优势 $Adv(A_{\text{IND-PUCLSC-CCA2-II}})$ 赢得游戏 IND-PUCLSC-CCA2-II，则存在挑战者 C 以优势 ε 解决 Weak-BDH 问题，其中：

$$\varepsilon \geq \frac{1}{q_0}\frac{1}{q_3} Adv(A_{\text{IND-CLSCPU-CCA2-II}}).$$

证明见附录 2.

不可伪造性. 在 CDH 难题假设下，B-PUCLSC 方案在适应性选择消息攻击下抗存在性伪造.

B-PUCLSC 方案中的签名本质上是 Hess 提出的基于身份签名[13]在无证书环境下的变体. 具体签名及验证算法如下：

首先 $H_2': G_1 \times \{0,1\}^{n_3} \times \{0,1\}^{n_1} \times G_1 \to Z_q^*$ 是一个安全的 Hash 函数.

签名. 签名者 Bob，其身份为 ID_B，公钥为 $P_B=(X_B, Y_B)$，完全私钥为 $FSK_B = x_B \cdot s \cdot Q_B$，给定消息 m 后，执行以下步骤生成签名 $\sigma=(U,V)$：随机选择 $r \in Z_q^*$，计算 $U=rP$，$h=H_2'(U, m, ID_B, X_B)$ 和 $V=rQ_B+h \cdot FSK_B$，消息 m 的签名为 $\sigma=(U,V)$.

验证. 任何人可以计算 $h=H_2'(U, m, ID_B, X_B)$，验证 $\hat{e}(V,P)=\hat{e}(U+hY_B, Q_B)$ 是否成立. 当且仅当等式成立时签名 $\sigma=(U,V)$ 有效.

上述签名在适应性选择消息攻击下抗存在性伪造性，证明见附录 3.

考虑到 B-PUCLSC 方案中恶意的代理解签密者也存在伪造签名的可能，附录 3 证明中额外地考虑了敌手对代理私钥的询问，模拟了恶意的代理解签密者伪造签名的攻击方式，从而 B-PUCLSC 方案抗存在性伪造.

5　结　论

本文首先提出一个新的密码模型——具有代理解签密功能的签密，并给出其安全模型. 然后基于无证书密码体制提出一个基础方案，又通过公告牌给出一个拓展方案，实现代理授权的任意终止. 最后，基于 Weak-BDH 和 CDH 难题分析了方案的安全性.

参　考　文　献

[1] Al-Riyami S S, Paterson K G. Certificateless public key cryptography//Laih C S. Cryptology-ASIACRYPT 2003. LNCS 2894. Berlin: Springer-Verlag, 2003: 452-473

[2] Zheng Y. Digital signcryption or how to achieve cost (Signature&Encryption)≤Cost (Signature)+Cost (Encryption)//Burton S, Kaliski J. CRYPTO'97. LNCS 1294. Berlin: Springer-Verlag, 1997: 165-179

[3] Barbosa M, Farshim P. Certificateless signcryption//Proceedings of the ACM Symposium on Information, Computer and Communications Security (ASIACCS). New York, USA, 2008: 369-372

[4] Xie W, Zhang Z. Efficient and provably secure certificateless signcryption from bilinear maps//Proceedings of the 2010 IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS). Beijing, China, 2010: 558-562

[5] Liu Z, Hu Y, Zhang X, Ma H. Certificateless signcryption scheme in the standard model. Information Sciences, 2010, 180(3): 452-464

[6] Kushwah P, Lal S. Efficient Generalized Signcryption Schemes. Cryptology ePrint Archive Report 2010/346. Http://eprint.iacr.org/2010/346

[7] Mambo M, Okamoto E. Proxy cryptosystem: Delegation of a power to decrypt ciphertexts. IEICE Transactions on Fundaments of Electronics Communications and Computer Science, 1997, E80-A(1): 54-63

[8] Tzeng S F, Yang C Y, Hwang M S. A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification. Future Generation Computer Systems, 2004, 20(5): 887-893

[9] Wang L, Okamoto L, Mambo M, Okamoto E. A subject-delegated decryption scheme with "tightly" limited authority//Proceedings of the CSS 2006. Japan, 2006: 107-112

[10] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy-signcryption//Proceedings of the 22nd Australasian Computer Science Conference. Auckland, 1999: 420-431

[11] Liu Jun-Bao, Xiao Guo-Zhen. Multi-Proxy Multi-Signcryption Scheme from Pairings. 2005, http://arxiv.org/abs/cs.CR/0509030

[12] Yu Hui-Fang, Wang Cai-Fen, Wang Zhi-Cang, Ye Cheng-Xu. Certificateless multi-proxy signcryption scheme. Computer Engineering and Design, 2010, 31(5): 973-975(in Chinese)
(俞惠芳, 王彩芬, 王之仓, 叶成绪. 无证书的多代理签密方案. 计算机工程与设计, 2010, 31(5): 973-975)

[13] Hess F. Efficient identity based signature scheme based on pairings//Proceedings of the SAC 2002. Newfoundland, Canada, 2002: 310-324

[14] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures. Journal of Cryptology, 2000, 13(3): 361-396

附录 1. 引理 1 证明.

证明. 把敌手的能力最大化,假设敌手可以询问挑战原始解签密者的 $l-1$ 个代理私钥. 不妨设敌手不询问代理私钥 S^{sub_i}. 记敌手 $A_{\text{IND-CLSCPU-CCA2-I}}$ 成功的优势为 $Adv(A_{\text{IND-CLSCPU-CCA2-I}})$,挑战者 C 可以利用敌手解决 Weak-BDH 问题. 令(P, aP, bP, cP, cw_i),其中 $w_i=H_1(sub_i)$,是一个 Weak-BDH 实例. 为了保持一致性,C 将维护 L_0、L_1、L_2、L_3、L_s、L_p、L_{ps} 7 张列表. L_0、L_1、L_2、L_3 分别用于记录敌手对预言机 H_0、H_1、H_2、H_3 的询问;L_s、L_p、L_{ps} 分别用于记录敌手对于完全私钥、公钥、代理私钥询问.

系统初始化. C 运行初始化算法,并将公开参数发送给 $A_{\text{IND-CLSCPU-CCA2-I}}$,秘密保存主密钥 s.

H_0(ID_U)询问. 假设敌手不做重复询问,C 首先从 $\{1,\cdots,q_0\}$ 中选取随机数 i_b. 对于第 i 次询问,

① 如果 $i=i_b$,设置 $ID_b=ID_U$,$Q_b=H_0(ID_U\}=bP$;计算 $PSK_b=sbP$,并将(ID_b, Q_b, PSK_b, $\perp$)添加到 L_0,返回 $Q_b=bP$.

② 否则,随机选取 $k_U\in Z_q^*$,计算 $Q_U=H_0(ID_U\}=k_UP$,$PSK_U=k_UP_{Pub}$,将(ID_U,Q_U,PSK_U,k_U)添加到 L_0,返回 Q_U.

H_1(sub_i)询问. 在 L_1 中查询记录(sub_i, w_i),如果存在,则返回 w_i;否则,随机选择 $w_i\in G_1^*$,将(sub_i, w_i)添加到 L_1,返回 w_i.

H_2(U,W,m,ID_A,X_A,ID_B,X_B)询问. 在 L_2 中查询记录$((U,W,m,ID_A,X_A,ID_B,X_B),h)$,如果存在,则返回 h;否则,随机选择 $h\in Z_q^*$,将$((U,W,m,ID_A,X_A,ID_B,X_B),h)$添加到 L_2,返回 h.

H_3($\hat{e}(Y_A,Q_A)^r$)询问. 在 L_3 中查询记录($\hat{e}(Y_A,Q_A)^r$, k_t),如果存在,则返回 k_t;否则,随机选择 $k_t\in G_1^*\times\{0,1\}^{n_3}\times\{0,1\}^{n_1}$,将($\hat{e}(Y_A,Q_A)^r$, k_t)添加到 L_3,返回 k_t.

部分私钥询问. 对 ID_U 执行部分私钥询问前,假设敌手已经执行过 $H_0(ID_U)$ 询问,在 L_0 中查询记录(ID_U, Q_U, PSK_U, $*$),如果存在,则返回 PSK_U.

公钥询问. 在 L_p 中查询记录(ID_U, $*$, P_U),如果存在,则返回 P_U;否则,随机选取 $x_U\in Z_q^*$,计算 $X_U=x_UP$,$Y_U=x_UP_{Pub}$,设置 $P_U=(X_U,Y_U)$,将(ID_U,x_U,P_U)添加到 L_p 中,返回 P_U.

公钥替换. 如果敌手要求将 ID_U 的公钥 P_U 替换为 P'_U. 如果(ID_U, $*$, P_U)在 L_p 中,设置 $P_U=P'_U$,添加(ID_U, $\perp$, P'_U)到 L_p 中;否则,直接添加(ID_U, $\perp$, P'_U)到 L_p 中.

完全私钥询问. 对 ID_U 执行完全私钥询问前,假设敌手已经做过部分私钥询问和公钥询问. 在 L_0 中查找(ID_U, Q_U, PSK_U, $*$),在 L_p 中查找(ID_U, $*$, P_U),如果(ID_U, x_U, P_U)在表 L_p 中,计算 $FSK_U=x_UPSK_U$,添加(ID_U, FSK_U)在 L_s 中,返回 FSK_U. 如果(ID_U, $\perp$, $*$)在表 L_p 中,添加(ID_U, $\perp$)在 L_s 中,返回 $\perp$.

代理私钥询问. 对 ID_U, sub_i 执行代理私钥询问前设敌手已经做过完全私钥和 H_1 询问. 如果(ID_U, FSK_U)在 L_s 中,随机选择 $d_i\in Z_q^*$,计算 $S^{sub_i}=(S_1^{sub_i},S_2^{sub_i})=(d_iw_i+FSK_U, d_iP)$,将($ID_U$, sub_i, d_i, S^{sub_i})添加到 L_{ps};如果(ID_U, $\perp$)在 L_s 中,将(ID_U, sub_i, $\perp$, $\perp$)添加到 L_{ps},返回 $\perp$.

签密询问. 假设敌手对发送者 ID_S 执行过完全私钥询问和对接收者 ID_R 执行过公钥询问. C 首先检查 ID_R 公钥在形式上的正确性.

情形 1. 发送者 ID_S 的公钥没被替换.

同正常签密算法一样,只是其中的 $H_i(i=0,1,2,3)$ 值从对应的 H_i 询问获得.

情形 2. 发送者 ID_S 的公钥被替换,接收者 ID_R 公钥未被替换.

① 随机选择 $r,h\in Z_q^*$,计算 $U=rP-hY_S$,$W=(r-x_Rs)w_i$ 和 $V=rQ_S$.

② 计算 $k_t=H_3(\hat{e}(U,FSK_R))$ 和 $z=V\parallel m\parallel ID_S\oplus k_t$,添加($\hat{e}(U,FSK_R)$, k_t)到 L_3 中.

③ 密文为$\langle sub_i,U,W,z\rangle$.

情形 3. 发送者 ID_S 的公钥以及接收者 ID_R 的公钥均被替换.

① 随机选择 $r,h\in Z_q^*$,计算 $U=rP-hY_S$,$W=(r-x_Rs)w_i$ 和 $V=rQ_S$.

② 随机选择 $k_t\in G_1^*\times\{0,1\}^{n_3}\times\{0,1\}^{n_1}$,计算 $z=V\parallel m\parallel ID_S\oplus k_t$.

③将$(ID_S, Y_S, ID_R, X_R, U, W, z, V, m, r, h, k_t)$添加到$L_s$中，密文为$\langle sub_i, U, W, z\rangle$.

解签密询问. 假设敌手对发送者ID_S执行过公钥询问和对接收者ID_R执行过完全私钥询问. C首先检查ID_S公钥在形式上的正确性.

情形 1. 接收者ID_R的公钥没被替换.

同正常解签密算法一样，只是其中的$H_i(i=0,1,2,3)$值从对应的H_i询问获得.

情形 2. 接收者ID_R的公钥被替换.

①如果$(ID_S, Y_S, ID_R, X_R, U, W, z, V, *, *, *, *)\in L_s$，返回$(ID_S, Y_S, U, W, V, m)$.

②否则将$(ID_S, Y_S, ID_R, X_R, U, W, z, V)$添加到$L_u$中，并按以下步骤遍历$L_3$中所有记录$(\hat{e}(Y_A, Q_A)^r, k_t)$：

i. 计算$V \| m \| ID_S = z \oplus k_t$，如果发送者$ID_S$的公钥被替换，移到$L_3$中下一条，重新开始；否则找到$ID_S$的完全私钥$FSK_S$.

ii. 如果$((U, W, m, ID_S, X_S, ID_R, X_R), h)\in L_2$，令$h = H_2(U, W, m, ID_S, X_S, ID_R, X_R)$；否则移到$L_3$中下一条，重新开始.

iii. 检查等式$\hat{e}(Y_R, Q_S)^r = \hat{e}(Y_R, V - hFSK_S)$是否成立，成立则返回$(ID_S, Y_S, U, W, V, m)$，否则移到$L_3$中下一条，重新开始.

③如果遍历完L_3中所有记录没有消息返回，则按如下步骤遍历L_s：

i. 如果L_s中当前记录形如$(ID_S, Y_S, ID_R, X_R, U', W, z, V, m', r, h', k_t)$，验证$U = U'$是否成立，成立则继续下一步；否则移到$L_s$中下一条，重新开始.

ii. 如果L_s当前记录形如$(ID_R, Y_R, ID_S, X_S, U', W, z, V, m', r, h', k_t)$，验证$\hat{e}(U, Q_R) = \hat{e}(U', Q_S)$是否成立，成立则继续下一步；否则移到$L_s$中下一条，重新开始.

iii. 计算$V \| m \| ID_S = z \oplus k_t$

如果$((U, W, m, ID_S, X_S, ID_R, X_R), h)\in L_2$，令$h = H_2(U, W, m, ID_S, X_S, ID_R, X_R)$；否则移到$L_s$中下一条，重新开始.

iv. 检查等式$\hat{e}(Y_R, Q_S)^r = \hat{e}(Y_R, V - hFSK_S)$是否成立，成立则返回$(ID_S, Y_S, U, W, V, m)$，否则移到$L_s$中下一条，重新开始.

④根据返回的(ID_S, Y_S, U, W, V, m)，验证$\hat{e}(P, V) = \hat{e}(U + Y_s, Q_S)$，成立则返回$m$

⑤若最终没有消息返回，则返回$\perp$.

阶段 1 结束，敌手输出身份ID_S^*, ID_R^*，其中$P_R^* = (aP, saP)$，消息$m_0, m_1 \in sub_i$. 如果$ID_R^* \neq ID_b$，C终止模拟；否则，C令$U^* = cP, W^* = cw_i$；随机选择$V^* \in G_1$和$k_t^* \in G_1^* \times \{0,1\}^{n_3} \times \{0,1\}^{n_1}$；计算$z^* = V^* \| m_\gamma \| ID_S^* \oplus k_t^*$. 返回$< sub_i, U^*, W^*, z^* >$.

在阶段 2，敌手继续作询问. 询问结束后，敌手返回对γ的猜测γ'，如果$\gamma' = \gamma$，C可以在表L_3中找到$(\hat{e}(P, P)^{sabc}, k_t)$，然后计算得到 W-BDH 问题的答案$\hat{e}(P, P)^{abc} = \{\hat{e}(P, P)^{sabc}\}^{\frac{1}{s}}$.

下面计算C成功的概率，C在回答签密询问时，可能会重新定义某些$H_3(\hat{e}(Y_A, Q_A)^r)$和$H_2(U, W, m, ID_A, X_A, ID_B, X_B)$的值，这样可能会导致回答不一致. 敌手共执行$q_s$次签密询问、$q_2$次$H_2$询问，$q_3$次$H_3$询问，此事件出现的概率至多是$q_s \cdot (q_2 + q_3 + 2q_s)/q$，$2q_s$来自每次签密询问都要定义一个$H_2$值和$H_3$值. 在挑战阶段，敌手必须选择$ID_b$作为挑战身份，此事件概率为$1/q_0$. 在阶段 2，如敌手执行$H_3(\hat{e}(P, P)^{sabc})$询问，$C$会失败. 但是此情况下$C$将以$1/q_3$概率在表$L_3$中得到 Weak-BDH 问题答案.

综上所述，C成功解决 Weak-BDH 问题的概率：

$$\varepsilon \geq \left(1 - \frac{q_s q_3}{q}\right) \cdot \left(1 - \frac{q_s \cdot (q_2 + q_3 + 2q_s)}{q}\right) \cdot \frac{1}{q_0} \cdot \frac{1}{q_3} \cdot Adv(A_{\text{IND-PUCLSC-CCA2-I}}).$$

证毕.

附录 2.　引理 2 证明.

证明.　假设敌手可以询问挑战原始解签密者的$l-1$个代理私钥，不妨设敌手不能询问代理私钥S^{sub_i}. 记$A_{\text{IND-CLSCPU-CCA2-II}}$成功的优势为$Adv(A_{\text{IND-CLSCPU-CCA2-II}})$，挑战者$C$可以利用敌手解决 Weak-BDH 问题. 令$(P, aP, bP, cP, cw_i)$，其中$w_i = H_1(sub_i)$，是一个 Weak-BDH 实例. 同引理 1 证明，C将维护L_0、L_1、L_2、L_3、L_s、L_p、L_{ps} 7 张列表.

系统初始化. C运行初始化算法，并将公开参数以及主密钥s发送给敌手.

H_0询问、H_1询问、H_2询问、H_3询问、公钥询问：与引理 1 证明中对应询问相同.

完全私钥询问. 对ID_U执行完全私钥询问前假设敌手已经做过部分私钥询问和公钥询问. 在L_0中查找$(ID_U, Q_U, PSK_U, *)$，在L_p中查找$(ID_U, *, P_U)$，在表L_p中查找(ID_U, x_U, P_U)，计算$FSK_U = x_U PSK_U$，添加(ID_U, FSK_U)在L_s中，返回FSK_U.

代理私钥询问. 对ID_U, sub_i执行代理私钥询问前假设敌手已经做过完全私钥询问和H_1询问. C在L_s中查找(ID_U, FSK_U)，随机选择$d_i \in Z_q^*$，计算$S^{sub_i} = (S_1^{sub_i}, S_2^{sub_i}) = (d_i w_i + FSK_U, d_i P)$，将$(ID_U, sub_i, d_i, S^{sub_i})$添加到$L_{ps}$中.

签密询问. 假设敌手对发送者ID_S执行过完全私钥询问和对接收者ID_R执行过公钥询问. 由于此游戏中敌手不能替换公钥，C可以得到FSK_S，因此C正常签密，只是其中的$H_i, i=0,1,2,3$值从对应的H_i询问获得.

解签密询问. 假设敌手对发送者ID_S执行过公钥询问和对接收者ID_R执行过完全私钥询问. C可以得到FSK_R，因此C正常解签密，只是其中的$H_i, i=0,1,2,3$值从对应的H_i询问获得.

阶段 1 结束，敌手输出身份ID_S^*, ID_R^*，其中$P_R^* = (aP,$

$saP)$，消息 $m_0, m_1 \in sub_i$. 如果 $ID_R^* \neq ID_b$，C 终止模拟；否则，C 设置 $U^* = cP, W^* = cw_i$；随机选择 $V^* \in G_1$ 和 $k_t^* \in G_1^* \times \{0,1\}^{n_3} \times \{0,1\}^{n_1}$；计算 $z^* = V^* \parallel m_\gamma \parallel ID_s^* \oplus k_t^*$. 返回 $\langle sub_i, U^*, W^*, z^* \rangle$.

在阶段 2，敌手继续询问. 询问结束后，敌手返回对 γ 的猜测 γ'，如果 $\gamma' = \gamma$，C 可以在表 L_2 中找到 $(\hat{e}(P,P)^{sabc}, k_t)$，然后计算 Weak-BDH 问题的答案 $\hat{e}(P,P)^{abc} = \{\hat{e}(P,P)^{sabc}\}^{1/s}$.

附录 3. 签名方案抗存在性伪造证明.

证明. 假设敌手最多进行 q_i 次 H_i 询问 $(i=0,1,2)$，q_s 次签名询问、q_p 次公钥询问. 如果存在攻击者 A（I 类或者 II 类）可以伪造签名，那么挑战者 C 可以利用敌手解决 CDH 问题. 令 (P, aP, bP) 是一个 CDH 实例. 为了保持一致性，C 将维护 L_0、L_1、L_2、L_s、L_p、L_{ps} 6 张列表.

系统初始化. C 运行初始化算法，如果是 I 类敌手，C 将公开参数发送给 A_1，秘密保存主密钥 s. 如果是 II 类敌手，C 将公开参数及主密钥 s 都发送给 A_{II}.

H_0（ID_U）询问. 假设敌手不做重复询问，C 首先从 $\{1,\cdots,q_0\}$ 中选取随机数 i_b. 对于第 i 次询问，

① 如果 $i=i_b$，设置 $ID_b = ID_U$，$Q_b = H_0(ID_U) = bP$；计算 $PSK_b = sbP$；并将 (ID_b, Q_b, PSK_b) 添加到 L_0，返回 $Q_b = bP$.

② 否则随机选取 $Q_U \in G_1^*$，计算 $PSK_U = sQ_U$，将 (ID_U, Q_U, PSK_U) 添加到 L_0，返回 Q_U.

H_1（sub_i）询问. 在 L_1 中查询记录 (sub_i, w_i)，如果存在，则返回 w_i；否则，随机选择 $w_i \in G_1^*$，将 (sub_i, w_i) 添加到 L_1，返回 w_i.

H_2'（U, m, ID_B, X_B）询问. 在表 L_2 中查询记录 $((U, m, ID_B, X_B), h)$，如果存在，则返回 h；否则，随机选择 $h \in Z_q^*$，将 $((U, m, ID_B, X_B), h)$ 添加到 L_2，返回 h.

部分私钥询问. 对 ID_U 执行部分私钥询问前假设敌手已经执行过 $H_0(ID_U)$ 询问，在 L_0 中查询记录 (ID_U, Q_U, PSK_U)，如果存在，则返回 PSK_U

公钥询问. 在 L_p 中查询记录 $(ID_U, *, P_U)$，如果存在，则返回 P_U；否则，随机选取 $x_U \in Z_q^*$，计算 $X_U = x_U P, Y_U = x_U P_{Pub}$，设置 $P_U = (X_U, Y_U)$，将 (ID_U, x_U, P_U) 添加到 L_p 中，返回 P_U.

公钥替换. II 类敌手不允许进行公钥替换. 假设 I 类敌手要求将 ID_U 的公钥 P_U 替换为 P_U'. 如果 $(ID_U, *, P_U)$ 在 L_p 中，则设置 $P_U = P_U'$，添加 $(ID_U, \perp, P_U')$ 到 L_p 中；否则，直接添加 $(ID_U, \perp, P_U')$ 到 L_p 中.

完全私钥询问. 对 ID_U 执行完全私钥询问前假设敌手已经做过部分私钥询问和公钥询问. 在 L_0 中查找 (ID_U, Q_U, PSK_U)，在 L_p 中查找 $(ID_U, *, P_U)$，如果 (ID_U, x_U, P_U) 在表 L_p 中，计算 $FSK_U = x_U PSK_U$，添加 (ID_U, FSK_U) 到 L_s 中，返回 FSK_U. 如果 $(ID_U, \perp, *)$ 在表 L_p 中，添加 $(ID_U, \perp)$ 在 L_s 中，返回 $\perp$.

代理私钥询问. 对 ID_U, sub_i 执行代理私钥询问前假设敌手已经做过完全私钥和 $H_1(sub_i)$ 询问. 如果 (ID_U, FSK_U) 在 L_s 中，随机选择 $d_i \in Z_q^*$，计算 $S^{sub_i} = (S_1^{sub_i}, S_2^{sub_i}) = (d_i w_i + FSK_U, d_i P)$，将 $(ID_U, sub_i, d_i, S^{sub_i})$ 添加到 L_{ps}；如果 $(ID_U, \perp)$ 在 L_s 中，将 $(ID_U, sub_i, \perp, \perp)$ 添加到 L_{ps}，返回 $\perp$.

签名询问. 假设敌手对发送者 ID_S 执行过完全私钥询问. 考虑两种情况：

情形 1. 发送者 ID_S 的公钥没被替换.

同正常签名算法一样，只是其中的 $H_i, i=0,1,2$ 值从对应的 H_i 询问获得.

情形 2. 发送者 ID_S 的公钥被替换.

① 随机选择 $r, h \in Z_q^*$，计算 $U = rP - hY_S$ 和 $V = rQ_S$.

② 签名为 $\sigma = (U, V)$.

在预言服务结束之后，敌手将生成伪造签名 $(ID_B^*, P_B^*, m^*, \sigma^* = (U^*, V^*))$. 如果挑战身份 $ID_B^* \neq ID_b$，或者公钥 $P_B^* = (X_B^*, Y_B^*) \neq (aP, aP_{Pub})$，$C$ 终止模拟.

简单分析一下 C 模拟成功的概率. 签名询问的第 2 种情形下，如果随机选取的（隐性定义的 $H_2'(U, m, ID_B, X_B))h \in Z_q^*$ 在 $H_2'(U, m, ID_B, X_B)$ 询问已经明确定义，可能产生回答不一致，导致模拟失败. 此事件发生的概率至多是 $\frac{q_s q_2}{q}$. 此外要求挑战身份 $ID_B^* = ID_b$，公钥 $P_B^* = (X_B^*, Y_B^*) = (aP, aP_{Pub})$，此事件的概率至少是 $\frac{1}{q_0 q_p}$.

把生成签名 σ^* 时用到的 $h^* = H_2'(U^*, m^*, ID_B^*, X_B^*)$ 询问称作关键询问. 游戏其间，敌手至多执行 $q_2 + q_s$ 次 H_2' 询问. 选取 $i_b \in \{1,\cdots,q_2+q_s\}$，第 i_b 次 H_2' 询问恰好是关键询问的概率为 $1/q_2+q_s$. 假设 R' 记录 H_2' 询问的答案，R'' 记录其它随机语言询问的答案. 将 R' 划分成两个阶段，R_1' 包含 $1,\cdots, i_b-1$ 次询问答案，R_2' 包含 $i_b,\cdots,q_2+q_s$ 次询问答案. C 重新进行一次模拟，其中 R_1'、R'' 不变，R_2' 不同. 应用“分叉引理”[14]，其中 $\Theta = R'' \cup R_1'$，$\gamma = R_2'$，那么敌手以概率 $\left(1-\frac{q_s q_2}{q}\right)^2 \left(\frac{1}{q_0 q_p}\right)^2 \frac{1}{4(q_2+q_s)^2} (Adv(A))^2$ 产生另一个签名 $(ID_B^*, P_B^*, m^*, \sigma^{*\prime} = (U^*, V^{*\prime}))$，其中 $h^{*\prime} \neq h^*$. $\sigma^*, \sigma^{*\prime}$ 满足下列等式：

$$V^* = rQ_b + h^* \cdot FSK_b \tag{1}$$

$$V^{*\prime} = rQ_b + h^{*\prime} \cdot FSK_b \tag{2}$$

由式(1)及式(2)可以得到 CDH 问题的答案：

$$abP = \frac{1}{s(h^* - h^{*\prime})} V^* - V^{*\prime}.$$

证毕.

下面计算 C 成功的概率. 在挑战阶段，敌手要选择 ID_b 作为挑战身份，此事件概率为 $1/q_0$. 在阶段 2，如敌手执行 $H_3(\hat{e}(P,P)^{sabc})$ 询问，C 会失败. 但是此情况下 C 将以 $1/q_3$ 概率在表 L_3 中得到问题答案.

综上所述，C 成功解决问题的概率为

$$\varepsilon \geq \frac{1}{q_0}\frac{1}{q_3} Adv(A_{\text{IND-CLSCPU-CCA2-II}}).$$

证毕.

YU Gang, born in 1984, Ph. D. candidate. His research interests include information security and protocol analysis.

HAN Wen-Bao, born in 1963, Ph. D., professor. His research interests include information security and cryptography analysis.

Background

This work is supported by the National High Technology Research and Development Program (863 Program) of China under grant No. 2009AA01Z417 which focuses on design of encryption and authentication key exchange protocol in next-generation wireless communication network, and the National Natural Science Foundation of China under grant No. 61003291 which focuses on studying software-oriented high-speed stream cipher drive components.

Certificateless public key cryptography, proposed in 2003, is an intermediate between traditional public key cryptography and identity based cryptography. Its main purpose is to solve the key escrow problem inherited from identity based cryptography (A third party generates private keys for all users) without the use of certificates as in traditional public key cryptography.

Signcryption, proposed in 1997, can fulfill both the functions of signature and encryption in a logical step. Compared with traditional "Sign-then-Encrypt" method, signcryption has less computation complexity, less communication complexity and less implementation complexity.

Proxy signature enables a proxy signer to sign messages on behalf of the original signer. And, proxy re-encryption is a cryptosystem which allow proxy to alter a ciphertext which has been encrypted for one party, so that it may be decrypted by another.

In this paper, we firstly introduce the concept of proxy unsigncryption into a signcryption scheme, and based on certificateless public key cryptography give a new signcryption model, named certificateless signcryption with proxy unsigncryption. We consider following scenario: A busy corporate manager, Bob, may need to out of town on business frequently. At the same time, there may be a large number of signcrypted messages needed to deal with every day. In order to release himself from heavy office work or prevent important business from being delayed during his absence, he may divide messages into several types and entitle each type a subject just as the subject lines in the e-mail system. Then he partially delegates his unsigncryption power to his assistants (proxies) according to different subjects. In the actual application, if, say Alice, wants to signcrypt messages under subject to Bob, he can signcrypt the message with Bob's public key and the subject. And, both Bob and his proxy corresponding to subject are able to unsigncrypt the ciphertext to get the message and verify Alice's signature on the message.