doi:10.11959/j.issn.1000-436x.2017072

标准模型下可证明安全的无证书广义签密

牛淑芬，牛灵，王彩芬，李亚红
（西北师范大学计算机科学与工程学院，甘肃 兰州 730070）

摘 要：Liu 等在 2010 年提出了一种在标准模型下可证明安全的无证书签密算法（简称 LHZ 算法），但后续的研究成果显示 LHZ 算法实际上是不安全的。为了克服 LHZ 算法的不足，首先改进 LHZ 签密算法，然后以此为基本的签密算法提出一种新的无证书广义签密算法。同时给出了抵抗有预谋的 KGC 被动攻击（malicious-but-passive KGC attack）的无证书广义签密算法的安全性模型，并在标准模型下证明了该算法在判定性双线性 Diffie-Hellman 困难问题和计算性 Diffie-Hellman 困难问题假设下是安全的。此外，数值实验结果表明所提方案是有效的。

关键词：无证书密码体制；广义签密；标准模型；有预谋的 KGC 被动攻击
中图分类号：TP309.7 **文献标识码**：A

Certificateless generalized signcryption scheme in the standard model

NIU Shu-fen, NIU Ling, WANG Cai-fen, LI Ya-hong
(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China)

Abstract: In 2010, Liu, et al. proposed a certificateless signcryption scheme in the standard model, but many analyses revealed that Liu's scheme was insecure in fact. To overcome the disadvantages, the scheme was improved and a certificateless generalized signcryption scheme was constructed. In addition, a formal security model for the proposed scheme against the malicious-but-passive KGC attacks was introduced. Furthermore, the proposed scheme was proven to be secure under the decisional bilinear Diffie-Hellman and the computational Diffie-Hellman intractability assumptions in the standard model. Numerical results illustrate that the proposed algorithm is efficient.

Key words: certificateless cryptography, generalized signcryption, standard model, malicious-but-passive KGC attacks

1 引言

无证书密码系统是为了克服基于身份的系统中的私钥托管问题而提出的，与基于 PKI 的传统公钥密码系统相比，无证书的公钥密码系统和基于身份的系统一样不需要公钥证书，同时，无证书密码系统消除了基于身份的系统中的私钥托管问题。而作为无证书密码系统的一个密码学原语，无证书签密（CLSC, certificateless signcryption）结合了无证书密码体制和签密的特点，对传输的消息实现了保密性和认证性。Barbosa 等[1]首次提出无证书签密的概念并给出了形式化定义，在随机预言模型下证明了其安全性。随后，许多 CLSC 方案[2~4]被提出，国内学者在这个领域也有相关研究[5,6]。Liu 等[7]在 2010 年提出了一个在标准模型下可证明安全的 CLSC 方案，但随后的文献[8,9]研究表明 Liu 等的算法在安全性上是有缺陷的。

韩益亮等[10]提出了广义签密的概念，它能在同一个逻辑步骤内单独实现签密、加密和签名 3 种功能。随着广义签密研究的深入，无证书广义签密的概念随即被提出，Ji 等[11]在 2010 年首次提出了一种无证书广义签密（CLGSC, certificateless generalized signcryption）算法，并给出了算法的形式化模型和安全性模型，但后续的研究成果[12,13]指出 Ji 等

收稿日期：2016-04-07；**修回日期**：2017-03-02
基金项目：国家自然科学基金资助项目（No.61562077, No.61462077, No.61662071）
Foundation Item: The National Natural Science Foundation of China (No.61562077, No.61462077, No.61662071)

的方案也存在安全缺陷。Zhou[14]针对抵抗有预谋的KGC被动攻击(malicious-but-passive KGC attack)的CLGSC方案定义了一个安全模型并且构造了一种具体的算法，此方案在随机预言模型下证明了其安全性依赖于GBDH问题和GDH问题。国内对无证书广义签密的研究成果比较少，目前可查到的报道有文献[15,16]。通过对国内外现有文献的分析可以看出：对无证书广义签密的研究成果比较少，还有许多新的算法和新的应用领域需要进一步探讨；其次，现有算法的安全性证明多是在随机预言模型下进行研究的，但一些在随机模型下可证安全的方案在实际应用过程中却存在一定的安全隐患。因此，研究标准模型下可证安全的CLGSC密码算法，具有十分重要的现实意义。

文献[8,9]的研究成果显示Liu等的算法不能抵抗2类公钥替换攻击，所以在安全性上存在缺陷。为了克服LHZ算法的不足，本文以LHZ算法为基本算法，提出了一种在标准模型下可证明安全的无证书广义签密算法。本文在签密阶段引入2个随机变量 $r',r''\in\mathbb{Z}_p$，对签密算法进行改进，得到一个六元签密组 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6)$。与文献[7]的签密算法相比，由于增加了一个任意的安全随机变量且密文由五元组 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5)$ 变为六元组 $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6)$，故本文算法能够抵抗公钥替换攻击，极大地提高了算法的安全性。同时，为了保证消息的机密性和签名的不可伪造性，本文在2类攻击者模型下证明了算法的安全性。安全性证明显示本算法的安全性依赖于DBDH问题和CDH问题的困难性。

2 基础知识

设 $\mathbb{G}$ 和 $\mathbb{G}_T$ 是2个阶为 q 的乘法群，表1为文中一些基本符号描述。

2.1 双线性映射

设 q 是一个大素数，$\mathbb{G}$ 和 $\mathbb{G}_T$ 是2个有着相同素数 q 阶的乘法循环群，g 是 $\mathbb{G}$ 的生成元。一个双线性映射 $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 满足下列性质。

1) 双线性：对任意的 $g,h\in\mathbb{G}$ 和 $a,b\in\mathbb{Z}_q^*$，存在 $e(g^a,h^b)=e(g,h)^{ab}$。

2) 非退化性：存在 $g,h\neq 1_G$，使 $e(g,h)\neq 1_{\mathbb{G}_T}$。

3) 可计算性：对所有的 $g,h\in\mathbb{G}$，存在有效算法计算 $e(g,h)$。

表1 符号描述

符号	描述
$\mathbb{G}$, $\mathbb{G}_T$	阶为 q 的双线性群
g,g_1,g_2	群中的元素
q	大素数
$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$	双线性映射
$\boldsymbol{U}$, $\boldsymbol{V}$	群 $\mathbb{G}$ 中的向量
u_S , u_R	发送者和接收者的身份
u_φ	身份为空
sk_u	相应于身份 u 的私钥

2.2 计算性 Diffie-Hellman(CDH)问题

设 $\mathbb{G}$ 是阶为素数 q 的循环群，g 为群 $\mathbb{G}$ 的生成元，对于给定的 $g,g^a,g^b\in\mathbb{G}$，计算 g^{ab}。

2.3 判定性双线性 Diffie-Hellman (DBDH)问题

$\mathbb{G}$ 和 $\mathbb{G}_T$ 为2个阶为素数 q 的循环乘法群，$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ 为一个双线性映射，g 为群 $\mathbb{G}$ 的生成元，给定五元组 (g,g^a,g^b,g^c,T)，判定性双线性问题定义为判断 $T=e(g,g)^{abc}$ 是否成立。

3 形式化定义

参照文献[7]中无证书签密算法的形式化定义，给出本文广义无证书签密算法(CLGSC)的形式化模型。

3.1 算法形式化定义

广义无证书签密方案有3个合法参与者：密钥生成中心(KGC)、发送者、接收者，由以下6个算法构成。

1) 系统建立 $(1^\lambda)\to(params,msk)$：输入安全参数 λ，返回系统公开参数 $params$ 和系统主密钥 msk。

2) 部分私钥生成 $(params,msk,u)\to(d_u)$：输入参数 $params$、msk 以及用户身份 $u\in\{0,1\}^*$，输出用户部分私钥 d_u。

3) 用户钥生成 $(params,u)\to(x_u,pk_u)$：输入给定用户身份 u 和系统公开参数 $params$，返回一个秘密值 x_u 和用户的公钥 pk_u。

4) 私钥生成 $(params,x_u,d_u)\to(sk_u)$：输入给定用户身份 u、系统参数 $params$、用户的部分私钥 d_u 和秘密值 x_u，返回用户私钥 sk_u。

5) 签密算法 $(m,u_S,u_R)\to(\sigma)$：用 u_φ 表示发送

者或接收者缺省，签密算法有以下 3 种情形。

①加密算法：输入 (m,u_φ,u_R)，输出 σ。

②签名算法：输入 (m,u_S,u_φ)，输出 σ。

③签密算法：输入 (m,u_S,u_R)，输出 σ。

6) 解签密算法(CLGUSC) $(\sigma,u_S,u_R)\rightarrow(m,\top,\perp)$。

①解密算法：输入 (σ,u_φ,u_R)，输出消息 m。

②验证算法：输入 (σ,u_φ,u_S)，检查签名 σ 是否有效，若 σ 有效，输出 $\top$；否则，输出 $\perp$。

③解签密算法：输入 (m,u_R,u_S)，检查签名 σ 是否有效，若 σ 有效，输出消息 m；否则，输出 $\perp$。

3.2 安全模型

在方案安全模型中，考虑 2 类攻击者：第 1 类攻击者 $\mathcal{A}_\text{I}$ 和第 2 类攻击者 $\mathcal{A}_\text{II}$。第 2 类攻击者 $\mathcal{A}_\text{II}$ 为恶意但被动 KGC 的情形，它可以自己生成系统参数和主密钥。2 类攻击者的具体攻击能力定义如下。

第 1 类攻击者($\mathcal{A}_\text{I}$)：攻击者 $\mathcal{A}_\text{I}$ 没有系统的主密钥。但是他可以进行公钥询问、公钥替换询问、部分私钥提取询问和私钥提取询问，可以进行加密和解密询问、签名和验证询问以及签密和解签密询问。

第 2 类攻击者($\mathcal{A}_\text{II}$)：攻击者 $\mathcal{A}_\text{II}$ 拥有系统的主密钥，因而无须进行部分私钥提取询问，也不能进行公钥替换询问，但可以进行私钥提取询问、加密和解密询问、签名和验证询问以及签密和解签密询问。

3.2.1 机密性

本文方案的机密性定义为适应性选择密文攻击下的不可区分性，具体定义通过以下 2 个攻击游戏予以刻画。

1) 游戏Ⅰ（挑战者 $\mathcal{C}$ 和攻击者 $\mathcal{A}_\text{I}$）

系统建立　挑战者 $\mathcal{C}$ 运行 $Setup(1^\lambda)$算法生成系统参数 *params* 和系统主密钥 *msk*，并把 *params* 发送给 $\mathcal{A}_\text{I}$，保留 *msk*。在此游戏中，攻击者 $\mathcal{A}_\text{I}$ 不知道系统的主密钥 *msk*。收到 *params* 后，$\mathcal{A}_\text{I}$ 与 $\mathcal{C}$ 进行如下交互。

阶段 1　攻击者 $\mathcal{A}_\text{I}$ 可以适应性地进行最多多项式有界次的以下询问。

①公钥询问：攻击者 $\mathcal{A}_\text{I}$ 给挑战者 $\mathcal{C}$ 一个身份 u，$\mathcal{C}$ 计算公钥 pk_u 发送给 $\mathcal{A}_\text{I}$。

②部分私钥提取询问：攻击者 $\mathcal{A}_\text{I}$ 发送一个身份 u 给挑战者请求身份 u 的部分私钥，$\mathcal{C}$ 生成部分私钥 d_u 返回给攻击者。

③公钥替换询问：攻击者 $\mathcal{A}_\text{I}$ 发送一个身份 u 和一个有效的新公钥 pk'_u，$\mathcal{C}$ 用新的公钥替换当前的公钥 pk_u。

④私钥提取询问：攻击者 $\mathcal{A}_\text{I}$ 请求身份 u 的私钥，挑战者 $\mathcal{C}$ 发送私钥 sk_u 给 $\mathcal{A}_\text{I}$。

⑤签密询问：攻击者 $\mathcal{A}_\text{I}$ 发送身份 u_S、u_R 和消息 M 给 $\mathcal{C}$，$\mathcal{C}$ 运行签密算法得到 σ，返回 σ 给 $\mathcal{A}_\text{I}$。

⑥解签密询问：攻击者 $\mathcal{A}_\text{I}$ 发送身份 u_S、u_R 和签密 σ 给 $\mathcal{C}$。如果 σ 是有效的，挑战者恢复消息 M 发送给 $\mathcal{A}_\text{I}$；否则，$\mathcal{C}$ 返回一个错误符号 $\perp$ 给 $\mathcal{A}_\text{I}$。

挑战　在阶段 1 询问结束后，攻击者发送其想要挑战的消息和身份 (M_0,M_1,u_S^*,u_R^*) 给挑战者 $\mathcal{C}$。$\mathcal{C}$ 随机选择一个数 $b\in\{0,1\}$，并计算 M_b^* 的密文 σ^* 后发送给攻击者 $\mathcal{A}_\text{I}$。

如果 $u_S^*=u_\varphi$，挑战是密文；否则是签密。

阶段 2　挑战者 $\mathcal{A}_\text{I}$ 继续进行同阶段 1 的询问。

猜测　$\mathcal{A}_\text{I}$ 输出对 b 的猜测，如果 $b=b'$，称 $\mathcal{A}_\text{I}$ 赢得游戏。整个过程中 $\mathcal{A}_\text{I}$ 满足以下限制。

① $\mathcal{A}_\text{I}$ 不能对 u_R^* 进行私钥提取询问。

② $\mathcal{A}_\text{I}$ 不能对公钥已被替换的用户进行私钥提取询问。

③ $\mathcal{A}_\text{I}$ 如果在挑战阶段之前已经替换了 u_R^* 的公钥，那么 $\mathcal{A}_\text{I}$ 不能对 u_R^* 进行部分私钥提取询问。

④在阶段 2，$\mathcal{A}_\text{I}$ 不能对挑战密文 σ^* 在身份 u_S^* 或 u_R^* 下进行解密询问，除非公钥 pk_S^* 或 pk_R^* 在挑战阶段之后被替换过。

2) 游戏Ⅱ（挑战者 $\mathcal{C}$ 和攻击者 $\mathcal{A}_\text{II}$）

系统生成　$\mathcal{C}$ 运行 $Setup(1^\lambda)$生成系统参数，并把它发送给 $\mathcal{A}_\text{II}$。在此类攻击下，$\mathcal{A}_\text{II}$ 自己能够生成 *params* 和 *msk*。

阶段 1　进行如同游戏Ⅰ中各种询问，唯一的限制是 $\mathcal{A}_\text{II}$ 不能进行公钥替换询问，但 $\mathcal{A}_\text{II}$ 可以进行任何身份的部分私钥提取询问。

挑战　如同游戏Ⅰ。

阶段 2　$\mathcal{A}_\text{II}$ 继续进行如同阶段 1 的询问。

猜测　猜测如同游戏Ⅰ，但 $\mathcal{A}_\text{II}$ 满足以下限制。

① $\mathcal{A}_\text{II}$ 不能对 u_R^* 进行私钥提取询问。

②在阶段 2，$\mathcal{A}_\text{II}$ 不能对挑战密文 σ^* 在身份 u_R^* 下进行解密询问。

3.2.2 不可伪造性

方案的不可伪造性定义为适应性选择消息攻击下的存在性不可伪造，具体通过以下定义的 2 个

攻击游戏予以刻画。

1) 游戏Ⅲ(挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{I}}$)

系统建立、询问 挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{I}}$进行如同游戏Ⅰ中的操作。

输出 $\mathcal{A}_{\mathrm{I}}$输出一个消息M^*的签密对(σ^*,u_S^*,u_R^*)，如果(σ^*,u_S^*,u_R^*)是有效的，则攻击者赢得了游戏。攻击者$\mathcal{A}_{\mathrm{I}}$需要满足以下限制。

① $\mathcal{A}_{\mathrm{I}}$不能对u_S^*进行任何私钥询问。

② $\mathcal{A}_{\mathrm{I}}$不能对公钥已被替换的用户进行私钥提取询问。

如果$u_R^*=u_\varphi$，伪造是签名；否则，此伪造是签密。

2) 游戏Ⅳ(挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{II}}$)

系统建立、询问 挑战者$\mathcal{C}$和攻击者$\mathcal{A}_{\mathrm{II}}$进行同游戏Ⅱ中的交互。

输出 同游戏Ⅲ。

如果$u_R^*=u_\varphi$，此伪造是签名；否则，此伪造是签密。

4 无证书广义签密算法(CLGSC)

本节给出一种在标准模型下可以抵抗恶意但被动的KGC攻击的无证书广义签密方案，这里假设所有的用户身份都是长度为n的比特串。

系统建立 设群$\mathbb{G}$和$\mathbb{G}_T$的阶为素数q，g是群$\mathbb{G}$的生成元。e是一个可计算的双线性映射，$H:\{0,1\}^*\to\{0,1\}^m$是一个免碰撞的散列函数。KGC：随机地选择$\alpha\in\mathbb{Z}_q$，计算$g_1=g^\alpha$。选择3个随机值$g_2,u',v'\in\mathbb{G}$以及2个长分别为n_u bit和n_m bit的向量$\boldsymbol{U}=(u_i)$和$\boldsymbol{V}=(v_j)$。系统参数为$params=(\mathbb{G},\mathbb{G}_T,e,g,g_1,g_2,u',v',\boldsymbol{U},\boldsymbol{V},H)$，主密钥是$g_2^\alpha$。

部分私钥提取 $u[i]$表示身份$u\in\{0,1\}^n$的第i个比特值，$\mathbb{U}=\{i\,|\,u[i]=1,i=1,2,\cdots,n\}$。KGC随机选择$t\in\mathbb{Z}_q$，并计算身份$u$部分私钥为

$$d_u=(d_{u,1},d_{u,2})=(g_2^\alpha(u'\prod_{i\in\mathbb{U}}u_i)^t,g^t)$$

用户密钥生成 发送者和接收者分别随机地选取$x_S,x_R\in\mathbb{Z}_q$，分别计算公钥$pk_S=e(g_1,g_2)^{x_S}$，$pk_R=e(g_1,g_2)^{x_R}$。

私钥提取 用户u随机选择$r\in\mathbb{Z}_q$，计算私钥

$$sk_u=(sk_{u,1},sk_{u,2})=(d_{u,1}^{x_u}(u'\prod_{i\in\mathbb{U}}u_i)^r,d_{u,2}^{x_u}g^r)$$
$$=(g_2^{\alpha x_u}(u'\prod_{i\in\mathbb{U}}u_i)^{t_u},g^{t_u})$$

其中，$t_u=tx_u+r$。

签密 给定消息M，发送者随机地选择$r',r''\in\mathbb{Z}_q$，执行以下算法。

计算$\sigma_1=Mpk_R^{r'}=Me(g_1,g_2)^{x_Rr'}$；

计算$\sigma_2=pk_R^{-r''}f(u_R)$；

计算$\sigma_3=g^{r'+r''}$；

计算$\sigma_4=(u'\prod_{i\in\mathbb{U}_R}u_i)^{r'+r''}f(u_R)$；

计算$\sigma_5=sk_{S,2}g^{r''}f(u_S)$；

计算$m=H(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,u_R,pk_R)\in\{0,1\}^m$，$\mathbb{M}=\{j\,|\,m[j]=1,j=1,2,\cdots,m\}$，其中，$m[j]$表示$m$的第$j$ bit；

计算$\sigma_6=sk_{S,1}(v'\prod_{i\in\mathbb{M}}v_i)^{r'+r''}f(u_S)(u'\prod_{i\in\mathbb{U}_S}u_i)^{r''}$；

发送者发送$\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6)$给接收者。根据广义签密算法的性质可得以下几点。

1) $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,0,0)$是密文。如果$u_S=u_\varphi$，即$f(u_S)=0$。

2) $\sigma=(\sigma_1,0,\sigma_3,0,\sigma_5,\sigma_6)$是签名。如果$u_R=u_\varphi$，即$f(u_R)=0$。

3) $\sigma=(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6)$是签密。如果$u_S\neq u_\varphi,u_R\neq u_\varphi$。

解签密 一旦收到σ，接收者执行以下算法。

1) 如果$\sigma_2=0,\sigma_4=0$，则σ是签名算法的签名，接收者计算$m=H(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,u_R,pk_R)$，如果$e(\sigma_6,g)=pk_Se(u'\prod_{i\in\mathbb{U}_S}u_i,\sigma_5)e(v'\prod_{i\in\mathbb{M}}v_i,\sigma_3)$，则接收签名。

2) 如果$\sigma_5=0,\sigma_6=0$，则σ是加密算法的密文，接收者恢复消息

$$M=\frac{\sigma_1e(\sigma_4,sk_{R,2})}{\sigma_2e(\sigma_3,sk_{R,1})}$$

3) 否则，σ是签密算法的密文，接收者计算$m=H(\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,u_R,pk_R)\in\{0,1\}^m$，并检查等式

$$(\sigma_6,g)=pk_Se(u'\prod_{i\in\mathbb{U}_S}u_i,\sigma_5)e(v'\prod_{i\in\mathbb{M}}v_i,\sigma_3)$$

是否成立。若等式成立，输出$M=\frac{\sigma_1e(\sigma_4,sk_{R,2})}{\sigma_2e(\sigma_3,sk_{R,1})}$；否则，输出$\perp$。

正确性证明如下。

签密验证等式为

$$(\sigma_6,g)=e(sk_{S,1}(v'\prod_{i\in\mathbb{M}}v_i)^{r'+r''}(u'\prod_{i\in\mathbb{U}_S}u_i)^{r''},g)$$
$$=e(g_2^{\alpha x},g)e(u'\prod_{i\in\mathbb{U}_S}u_i,g^{t_S+r''})e(v'\prod_{i\in\mathbb{M}}v_i,g^{r'+r''})$$
$$=pk_S e(u'\prod_{i\in\mathbb{U}_S}u_i,\sigma_5)e(v'\prod_{i\in\mathbb{M}}v_i,\sigma_3)$$

对解密算法，有

$$\frac{\sigma_1 e(\sigma_4,sk_{R,2})}{\sigma_2 e(\sigma_3,sk_{R,1})}$$
$$=\frac{Me(g_1,g_2)^{x_R r'}e(g^{r'+r''},(u'\prod_{i\in\mathbb{U}_R}u_i)^{t_R})}{e((g_1,g_2)^{-x_R r''}e(g_2^{\alpha x_R}(u'\prod_{i\in\mathbb{U}_R}u_i)^{t_R},g^{r'+r''})}$$
$$=\frac{Me(g_1,g_2)^{x_R(r'+r'')}e(g^{r'+r''},(u'\prod_{i\in\mathbb{U}_R}u_i)^{t_R})}{e(g_2^{\alpha x_R},g^{r'+r''})e((u'\prod_{i\in\mathbb{U}_R}u_i)^{t_R},g^{r'+r''})}=M$$

5　安全性分析

本节给出本文提出方案在 3.2 节安全模型下的安全性证明，本文的结论都是在标准模型下得到的。在以下证明过程中，假设攻击者可以进行至多 q 次公钥询问、q_r 次公钥替换询问（对 $\mathcal{A}_{\Pi}$，$q_r=0$）、q_{pp} 次部分私钥询问（对 $\mathcal{A}_{\Pi}$，$q_{pp}=0$）、q_p 次私钥询问、q_s 次签密询问和 q_u 次解签密询问。

定理 1　在 DBDH 假设下，本文提出的算法 CLGSC 在适应性选择密文攻击下是安全的，即 IND-CCA 安全的。

定理 1 的证明可由引理 1 和引理 2 得到。

引理 1　假设存在一个 IND-CCA 的第 1 类攻击者 $\mathcal{A}_{\mathrm{I}}$ 可以 ε 的优势赢得 3.2 节定义的游戏 I，则存在一个区分者 $\mathcal{C}$ 可以以 ε' 的优势解决 DBDH 问题。

对签密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left[1-\frac{1}{q_s(n_u+1)}\right]$$

对加密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证明　证明思路基于 Waters[17]的证明方法。假设一个挑战者 $\mathcal{C}$ 收到一个随机的 DBDH 问题实例 $(g,A=g^a,B=g^b,C=g^c,Z)$，他需要判定 $Z=e(g,g)^{abc}$ 是否成立。

系统建立　令 $l_u=2(q_{pp}+q_p)=2q_s$，$l_m=2q_u$。$\mathcal{C}$ 随机地选择以下元素。

1) 2 个整数 k_u、k_m，其中，$0\leqslant k_u\leqslant n,0\leqslant k_m\leqslant m$。对于给定的 n和m，有 $l_u(n+1)<p,l_m(m+1)<p$。

2) 整数 $x'\in\mathbb{Z}_{l_u}$ 和向量 $\boldsymbol{X}=(x_i)_n(x_i\in\mathbb{Z}_{l_u})$。

3) 整数 $z'\in\mathbb{Z}_{l_m}$ 和向量 $\boldsymbol{Z}=(z_i)_m(z_i\in\mathbb{Z}_{l_m})$。

4) 2 个整数 $y',w'\in\mathbb{Z}_q$，向量 $\boldsymbol{Y}=(y_i)_n(y_i\in\mathbb{Z}_q)$ 和 $\boldsymbol{W}=(w_j)_m(w_j\in\mathbb{Z}_q)$。

定义以下变量为二元串 u 和 m 的函数，$F(u)=x'-l_uk_u+\sum_{i\in\mathbb{U}}x_i,J(u)=y'+\sum_{i\in\mathbb{U}}y_i$，$K(m)=z'-l_mk_m+\sum_{j\in\mathbb{U}}z_j,L(m)=w'+\sum_{j\in\mathbb{U}}w_j$，其中，$m=H(\cdot)$。

挑战者公布以下公钥参数。

$g_1=g^a,g_2=g^b$。

$u'=g_2^{x'-l_uk_u},u_i=g_2^{x_i}g^{y_i}(0\leqslant i\leqslant n)$。

$v'=g_2^{z'-l_mk_m},v_j=g_2^{z_j}g^{w_j}(0\leqslant j\leqslant n)$。

由上可得 $g_2^{\alpha}=g^{ab}$，$u'\prod_{i\in\mathbb{U}}u_i=g_2^{F(u)}g^{J(u)}$，$v'\prod_{j\in\mathbb{M}}v_j=g_2^{K(m)}g^{L(m)}$。

阶段 1　在询问阶段，$\mathcal{C}$ 按照以下方式回答 $\mathcal{A}_{\mathrm{I}}$ 的所有询问。

部分私钥提取询问　输入一个身份 u，如果 $F(u)=0\bmod q$，$\mathcal{C}$ 放弃；否则，$\mathcal{C}$ 随机选择 $r_u\in\mathbb{Z}_q$，计算

$$d_u=(d_{u,1},d_{u,2})=(g_1^{-\frac{J(u)}{F(u)}}(u'\prod_{i\in\mathbb{U}_R}u_i)^{r_u},g_1^{-\frac{1}{F(u)}}g^{r_u})$$

令 $r_u^{\sim}=r_u-\frac{a}{F(u)}$。因为

$$d_{u1}=g_1^{-\frac{J(u)}{F(u)}}(u'\prod_{i\in\mathbb{U}_R}u_i)^{r_u}$$
$$=g_2^a(g_2^{F(u)}g^{J(u)})^{-\frac{a}{F(u)}}(g_2^{F(u)}g^{J(u)})^{r_u}$$
$$=g_2^a(g_2^{F(u)}g^{J(u)})^{r_u-\frac{a}{F(u)}}$$
$$=g_2^{\alpha}(u'\prod_{i\in\mathbb{U}_R}u_i)^{r_u}$$

以及

$$d_{u2}=g_1^{-\frac{1}{F(u)}}g^{r_u}=g^{r_u-\frac{a}{F(u)}}=g^{r_u^{\sim}}$$

所以可得 d_u 是身份 u 的有效部分私钥。

公钥询问　当攻击者 $\mathcal{A}_{\mathrm{I}}$ 要求询问身份 u 的公钥时，挑战者 $\mathcal{C}$ 运行用户密钥生成算法产生密钥对 (x_u,pk_u)，其中，$pk_u=e(g_1,g_2)^{x_u}$，然后发送公钥

pk_u 给 $\mathcal{A}_{\mathrm{I}}$。

私钥提取询问 当攻击者 $\mathcal{A}_{\mathrm{I}}$ 要求询问身份 u 的私钥时，挑战者 $\mathcal{C}$ 运行用户密钥生成算法产生密钥对 (x_u, pk_u)。如果 $F(u)=0 \bmod q$，$\mathcal{C}$ 放弃；否则，$\mathcal{C}$ 随机选择 $r_u \in \mathbb{Z}_q$，计算

$$\begin{aligned} sk_u &= (sk_{u,1}, sk_{u,2}) \\ &= ((g_1^{x_u})^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in \mathbb{U}} u_i)^{r_u}, (g_1^{x_u})^{-\frac{J(u)}{F(u)}} g^{r_u}) \\ &= (g_2^{\alpha x_u} (u' \prod_{i \in \mathbb{U}} u_i)^{t}, g^{t}) \end{aligned}$$

其中，$t = r_u - \dfrac{\alpha x_u}{F(u)}$，发送私钥 sk_u 给 $\mathcal{A}_{\mathrm{I}}$。

公钥替换询问 当挑战者 $\mathcal{A}_{\mathrm{I}}$ 请求替换身份 u 的公钥 pk_u 时，$\mathcal{C}$ 随机地选择一个有效的公钥 pk_u' 发送给攻击者。

签密询问 $\mathcal{A}_{\mathrm{I}}$ 给挑战者发送 (M, u_S, u_R)，请求签密询问，有以下 2 种情况。

1) 当 $u_R \neq u_\varphi$(签密)，存在 2 种情形。

如果 $F(u_S) \neq 0 \bmod l_u$，$\mathcal{A}_{\mathrm{I}}$ 请求私钥询问和公钥替换询问获得签名者 u_S 的私钥 sk_S 和公钥 pk_S，$\mathcal{C}$ 执行签密算法计算 σ。

如果 $F(u_S)=0 \bmod l_u$，$\mathcal{C}$ 计算 $m = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, u_R, pk_R) \in \{0,1\}^m$。如果 $K(m)=0 \bmod l_m$，$\mathcal{C}$ 放弃；如果 $K(m) \neq 0 \bmod l_m$，$\mathcal{C}$ 首先计算

$$\begin{aligned} sk_u &= (sk_{u,1}, sk_{u,2}) \\ &= ((g_1^{x_u})^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in \mathbb{U}} u_i)^{r_u}, (g_1^{x_u})^{-\frac{J(u)}{F(u)}} g^{r_u}) \\ &= (g_2^{\alpha x_u} (u' \prod_{i \in \mathbb{U}} u_i)^{t}, g^{t}) \end{aligned}$$

然后随机选择整数 $r', r'' \in \mathbb{Z}_q$，并计算

$$\sigma_3 = g^{r'+r''}, \sigma_5 = (g_1^{x_S})^{-\frac{1}{F(u_S)}} g^{t_S} g^{r''}$$

$$\sigma_6 = (g_1^{x_S})^{-\frac{J(u_S)}{F(u_S)}} (u' \prod_{i \in \mathbb{U}_S} u_i)^{t_S} (g^{L(m)})^{r'+r''} (g^{J(u_S)})^{r''}$$

如果 $F(u_R) \neq 0 \bmod l_u$，$\mathcal{C}$ 请求公钥询问、部分私钥询问和私钥询问获得 u_R 的私钥 sk_R 和公钥 pk_R，计算 $\sigma_1 = Me(g_1, g_2)^{x_R r'}$，$\sigma_2 = e(g_1, g_2)^{-x_R r''}$ 和 $\sigma_4 = (g^{J(u_R)})^{r'+r''}$。游戏结束，$\mathcal{C}$ 获得 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$，将 (u_S, u_R, σ) 记录在 L-列表里，然后发送 σ 给 $\mathcal{A}_{\mathrm{I}}$。

2) 当 $u_R = u_\varphi$(加密)，则 $\mathcal{C}$ 如情形 1)中的方法计算 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, 0, 0)$，发送 σ 给 $\mathcal{A}_{\mathrm{I}}$。

解签密询问 当攻击者 $\mathcal{A}_{\mathrm{I}}$ 发送 (u_S, u_φ, σ) 给 $\mathcal{C}$，有以下 2 种情况。

1) 当 $u_S \neq u_\varphi$(解签密)，$\mathcal{C}$ 首先检查 (u_S, u_φ, σ) 是否在 L-列表里。如果在，$\mathcal{C}$ 返回相应的签密值 σ 给挑战者；否则，$\mathcal{C}$ 执行签密算法获得签密 σ。

同时，$\mathcal{C}$ 解密 σ 得到消息 M，因为

$$g_2^{r'+r''} = \left(\frac{\sigma_6}{(\sigma_3)^{L(m)} \left(\dfrac{\sigma_4}{sk_{S,2}} \right)^{J(u_S)}} \right)^{\frac{1}{K(m)}}$$

所以

$$M = \frac{\dfrac{\sigma_1}{\sigma_2}}{e(g_1, g_2)^{x_R(r'+r'')}} = \frac{\dfrac{\sigma_1}{\sigma_2}}{e(g_1^{x_R}, g_2^{r'+r''})}$$

2) 当 $u_S = u_\varphi$(解密)，$\mathcal{C}$ 如情形 1)中的方法计算 M，发送 σ 给 $\mathcal{A}_{\mathrm{I}}$。

挑战 经过多项式时间有界次询问，$\mathcal{A}_{\mathrm{I}}$ 选择 2 个不同的挑战身份 u_S^*、u_R^*，发送 (M_0, M_1, u_S^*, u_R^*) 给 $\mathcal{C}$。$\mathcal{C}$ 随机选择 $b \in \{0,1\}$ 和一个想要签密的消息 M_b，有以下 2 种结果。

1) 当 $u_S^* \neq u_\varphi$ 且 $u_R^* \neq u_\varphi$，挑战的是签密。

如果 $F(u_S^*)=0 \bmod q$，$\mathcal{C}$ 放弃；否则，计算 u_S^* 的私钥 $sk_S^* = (sk_{S,1}^*, sk_{S,2}^*)$。

如果 $F(u_R^*)=0 \bmod q$ 且 $K(m_b^*)=0 \bmod q$，设 $pk_S^* = e(g_1, g_2)^{x_S^*}$ 和 $pk_R^* = e(g_1, g_2)^{x_R^*}$ 分别是身份 u_S^* 和 u_R^* 的公钥，$\mathcal{C}$ 获取秘密值 x_S^* 和 x_R^*，令签密为

$$\sigma_1^* = m_b^* Z^{x_R^*}, \sigma_2^* = Z^{-x_R^*}, \sigma_3^* = (g^c)^2, \sigma_4^* = (g^c)^{2J_{u_R^*}}$$

$$\sigma_5^* = (g_1^{x_S^*})^{-\frac{1}{F(u_S^*)}} g^{t_s^*} g^c$$

$$\sigma_6^* = (g_1^{x_S^*})^{-\frac{J(u_S^*)}{F(u_S^*)}} (u' \prod_{i \in \mathbb{U}_{S^*}} u_i)^{t_s^*} (g^c)^{2L(\mathrm{m}_b)(r'+r'')} (g^c)^{J(u_S^*)}$$

$\mathcal{C}$ 发送 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*)$ 给攻击者 $\mathcal{A}_{\mathrm{I}}$；否则，$\mathcal{C}$ 放弃。

2) 当 $u_S^* = u_\varphi$ 且 $u_R^* \neq u_\varphi$，挑战的是密文。

$\sigma_1^* = m_b^* Z^{x_R^*}, \sigma_2^* = Z^{-x_R^*}, \sigma_3^* = (g^c)^2, \sigma_4^* = (g^c)^{2J_{u_R^*}}$，$\sigma_5^* = 0, \sigma_6^* = 0$。

$\mathcal{C}$ 发送密文 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*)$ 给 $\mathcal{A}_{\mathrm{I}}$；否则，$\mathcal{C}$ 放弃。

阶段 2 $\mathcal{A}_{\mathrm{I}}$ 继续进行同阶段 1 的询问，但不允许对 u_S^* 和 u_R^* 的签密进行询问。最终，$\mathcal{A}_{\mathrm{I}}$ 输出对

b 的猜测。如果 $b'=b$，攻击者 $\mathcal{A}_{\mathrm{I}}$ 赢得了游戏， 输出对 DBDH 的作答 $Z=e(g,g)^{abc}$。

下面分析 $\mathcal{C}$ 攻击成功的概率。如果模拟过程不终止，则有以下 6 个事件。

E_1：在所有对身份 u 的部分私钥提取和私钥提取询问中， $F(u)=0 \bmod q$ 不可能发生。

E_2：在签密询问中， $F(u_S)=0 \bmod l_u$ 不可能发生。

E_3：在解签密询问中，事件 $F(u_R)=0 \bmod l_u \wedge K(m)=0 \bmod l_m$ 不可能发生。

E_4： $F(u_S^*)=0 \bmod q$ （仅对 $u_S^* \neq u_\varphi$）。

E_5： $F(u_R^*)=0 \bmod q$。

E_6： $K(m^*)=0 \bmod l_m$。

事件 E_1、E_2、E_3、E_4、E_5 和 E_6 是相互独立的。假设 $l_u\left(n_u+1\right)<q$，可由 $F(u)=0 \bmod q$ 推导出 $F(u)=0 \bmod l_u$，因此

$$\begin{aligned}\Pr\left[\mathrm{E}_5\right] &= \Pr[F(u_R^*)=0 \bmod q \wedge F(u_R^*)=0 \bmod l_u] \\ &= \Pr[F(u_R^*)=0 \bmod l_u] \\ &\quad \Pr[F(u_R^*)=0 \bmod q \mid F(u_R^*)=0 \bmod l_u] \\ &= \frac{1}{l_u}\cdot\frac{1}{n_u+1}\end{aligned}$$

同理，$\Pr[\mathrm{E}_4]=1-\frac{1}{l_u}\cdot\frac{1}{n_u+1}$，$\Pr[\mathrm{E}_6]=\frac{1}{l_{\mathrm{m}}}\cdot\frac{1}{n_m+1}$。

对不同的身份 u_1 和 u_2，事件 $F(u_1)=0 \bmod l_u$ 和 $F(u_2)=0 \bmod l_u$ 是相互独立的，因此可得 $\Pr\left[\overline{\mathrm{E}_1}\right]=\frac{1}{l_u}$。因为 $\mathcal{A}_{\mathrm{I}}$ 可以进行至多 q_{pp} 次部分私钥询问和 q_p 次私钥询问，可得 $\Pr[\mathrm{E}_1]\geqslant\frac{q_{pp}+q_p}{l_u}$。另外， $\mathcal{A}_{\mathrm{I}}$ 可以进行至多 q_s 次签密询问，所以有 $\Pr[\mathrm{E}_2]\geqslant 1-\frac{q_s}{l_u}$。其次，函数 F 和 K 是相互独立的，可推导出 $\Pr\left[\overline{\mathrm{E}_3}\right]=\Pr[F(u_R=0 \bmod l_u \wedge K(m)=0 \bmod l_m]=\frac{1}{l_u l_m}$。$\mathcal{A}_{\mathrm{I}}$ 还可以进行至多 q_u 次解签密询问，可推导出： $\Pr[\mathrm{E}_3]\geqslant 1-\frac{q_u}{l_u l_m}$。

由上可以计算出 $\mathcal{C}$ 不放弃的概率。

对签密算法，有

$$\begin{aligned}\Pr\left[\overline{\text{abort}}\right] &\geqslant \Pr\left[\mathrm{E}_1 \wedge \mathrm{E}_2 \wedge \mathrm{E}_3 \wedge \mathrm{E}_4 \wedge \mathrm{E}_5 \wedge \mathrm{E}_6\right] \\ &= \Pr\left[\mathrm{E}_1\right]\Pr\left[\mathrm{E}_2\right]\Pr\left[\mathrm{E}_3\right]\Pr\left[\mathrm{E}_4\right]\Pr\left[\mathrm{E}_5\right]\Pr\left[\mathrm{E}_6\right] \\ &= \frac{1}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)\end{aligned}$$

对加密算法，有

$$\begin{aligned}\Pr\left[\overline{\text{abort}}\right] &\geqslant \Pr\left[\mathrm{E}_1 \wedge \mathrm{E}_2 \wedge \mathrm{E}_3 \wedge \mathrm{E}_4 \wedge \mathrm{E}_5\right] \\ &= \Pr\left[\mathrm{E}_1\right]\Pr\left[\mathrm{E}_2\right]\Pr\left[\mathrm{E}_3\right]\Pr\left[\mathrm{E}_4\right]\Pr\left[\mathrm{E}_5\right] \\ &= \frac{1}{16(q_{pp}+q_p)(n_u+1)}\left(1-\frac{1}{2q_s}\right)\end{aligned}$$

如果模拟过程不终止，$\mathcal{A}_{\mathrm{I}}$ 若能以 ε 的概率攻破本文的算法，则能够以 ε' 的概率解决 DBDH 问题。

对签密算法，有

$$\varepsilon' \geqslant \frac{\varepsilon}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)$$

对加密算法，有

$$\varepsilon' \geqslant \frac{\varepsilon}{16(q_{pp}+q_p)(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证毕。

引理 2　假设存在一个 IND-CCA 的第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 可以 ε 的优势赢得第 3.2 节定义的游戏 II，则存在一个区分者 $\mathcal{C}$ 可以以 ε' 的优势解决 DBDH 问题。其中，对签密算法，有

$$\varepsilon' \geqslant \frac{\varepsilon}{16q_p q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)$$

对加密算法，有

$$\varepsilon' \geqslant \frac{\varepsilon}{16q_p(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证明　假设存在一个第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 攻击该算法，攻击者 $\mathcal{A}_{\mathrm{II}}$ 可以进行至多 q 次公钥询问，q_p 私钥询问，q_s 次签密询问和 q_u 次解签密询问。假设有一个挑战者 $\mathcal{C}$ 收到了一个随机的 DBDH 问题实例 $(g,A=g^a,B=g^b,C=g^c,Z)$， 判定 $Z=e(g,g)^{abc}$ 是否成立。

系统建立　令 $l_u=2q_p=2q_s, l_m=2q_u$。$\mathcal{A}_{\mathrm{II}}$ 随机的选择一个整数 $\alpha\in\mathbb{Z}_q$ 作为系统的主密钥，$g_1=g^\alpha$。其余的参数定义如同引理 1 中所示。$\mathcal{A}_{\mathrm{II}}$ 发送所有的公开参数和主密钥 α 给 $\mathcal{C}$。

阶段 1　$\mathcal{A}_{\mathrm{II}}$ 首先计算所有身份的部分私钥，然

后执行以下的询问。

公钥询问 当攻击者 $\mathcal{A}_{\Pi}$ 要求询问身份 u 的公钥时，挑战者 $\mathcal{C}$ 运行用户密钥生成算法产生密钥对 (x_u, pk_u)，其中，$pk_u = e(g_1, g_2)^{x_u}$，然后发送公钥 pk_u 给 $\mathcal{A}_{\Pi}$。

私钥提取询问 当攻击者 $\mathcal{A}_{\Pi}$ 要求询问身份 u 的私钥时，$\mathcal{C}$ 首先执行公钥生成算法产生公私钥对 (x_u, pk_u)。如果 $F(u) = 0 \bmod q$，$\mathcal{C}$ 随机选择 $r_u \in \mathbb{Z}_q$，计算

$$\begin{aligned} sk_u &= (sk_{u,1}, sk_{u,2}) \\ &= ((A^{\alpha x_u})^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in \mathbb{U}} u_i)^{r_u}, (A^{\alpha x_u})^{-\frac{1}{F(u)}} g^{r_u}) \\ &= (g_2^{\alpha x_u} (u' \prod_{i \in \mathbb{U}} u_i)^{t}, g^{t}) \end{aligned}$$

其中，$t = r_u - \dfrac{\alpha x_u}{F(u)}$，发送 sk_u 给攻击者 $\mathcal{A}_{\Pi}$；如果 $F(u) = 0 \bmod q$，$\mathcal{C}$ 放弃。

签密询问 $\mathcal{A}_{\Pi}$ 给挑战者发送请求 (M, u_S, u_R) 给挑战者，有以下 2 种情况。

1) 当 $u_R \neq u_{\varphi}$(签密)，存在 2 种情形。

如果 $F(u_S) \neq 0 \bmod l_u$，$\mathcal{A}_{\Pi}$ 请求私钥询问和公钥替换询问获得签名者 u_S 的私钥 sk_S 和公钥 pk_S，$\mathcal{C}$ 执行签密算法计算 σ。如果 $F(u_S) = 0 \bmod l_u$，$\mathcal{C}$ 计算 $m = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, u_R, pk_R) \in \{0,1\}^m$。如果 $K(m) = 0 \bmod l_m$，$\mathcal{C}$ 放弃；如果 $K(m) \neq 0 \bmod l_m$，$\mathcal{C}$ 首先计算

$$\begin{aligned} sk_u &= (sk_{u,1}, sk_{u,2}) \\ &= ((A^{\alpha x_u})^{-\frac{J(u)}{F(u)}} (u' \prod_{i \in \mathbb{U}} u_i)^{r_u}, (A^{x_u})^{-\frac{1}{F(u)}} g^{r_u}) \\ &= (g_2^{\alpha x_u} (u' \prod_{i \in \mathbb{U}} u_i)^{t}, g^{t}) \end{aligned}$$

然后随机选择整数 $r', r'' \in \mathbb{Z}_q$，并计算

$$\sigma_3 = g^{r'+r''}, \sigma_5 = (A^{\alpha x_S})^{-\frac{1}{F(u_S)}} g^{t_S} g^{r''}$$

$$\sigma_6 = (A^{\alpha x_S})^{-\frac{J(u_S)}{F(u_S)}} (u' \prod_{i \in \mathbb{U}_S} u_i)^{t_S} (g^{L(m)})^{r'+r''} (g^{J(u_S)})^{r''}$$

如果 $F(u_R) \neq 0 \bmod l_u$，$\mathcal{C}$ 请求公钥询问和私钥询问获得 u_R 的私钥 sk_R 和公钥 pk_R，计算 $\sigma_1 = Me(B, A^{\alpha})^{x_R r'}, \sigma_2 = e(B, A^{\alpha})^{-x_R r''}, \sigma_4 = (g^{J(u_R)})^{r'+r''}$，游戏结束，$\mathcal{C}$ 获得签密 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6)$，将 (u_S, u_R, σ)，记录在 L-列表里，然后发送签密值 σ 给 $\mathcal{A}_{\Pi}$。

2) 当 $u_R = u_{\varphi}$(加密)，$\mathcal{C}$ 如情形 1)中的方法计算 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, 0, 0)$，发送 σ 给 $\mathcal{A}_{\Pi}$。

解签密询问 当攻击者 $\mathcal{A}_{\Pi}$ 发送 $(u_S, u_{\varphi}, \sigma)$ 给 $\mathcal{C}$，有以下 2 种情况。

1) 当 $u_S \neq u_{\varphi}$(解签密)，$\mathcal{C}$ 首先检查 $(u_S, u_{\varphi}, \sigma)$ 是否在 L-列表里。如果在，$\mathcal{C}$ 返回相应的签密值 σ 给挑战者；否则，$\mathcal{C}$ 执行签密算法获得签密 σ。

同时，$\mathcal{C}$ 解密 σ 得到消息 M，因为

$$g_2^{r'+r''} = \left(\frac{\sigma_6}{(\sigma_3)^{L(m)} \left(\dfrac{\sigma_4}{sk_{S,2}} \right)^{J(u_S)}} \right)^{\frac{1}{K(m)}}$$

所以

$$M = \frac{\dfrac{\sigma_1}{\sigma_2}}{e(B, A^{\alpha})^{x_R(r'+r'')}} = \frac{\dfrac{\sigma_1}{\sigma_2}}{e(A^{\alpha x_R}, g_2^{r'+r''})}$$

2) 当 $u_S = u_{\varphi}$(解签密)，$\mathcal{C}$ 如上述方法计算 M，发送 σ 给 $\mathcal{A}_{\Pi}$。

挑战 经过多项式时间有界次询问，$\mathcal{A}_{\Pi}$ 选择 2 个不同的想要挑战的身份 u_S^*, u_R^*。因为在阶段 1 中 $\mathcal{A}_{\Pi}$ 没有对 u_R^* 进行私钥提取询问，他发送 (M_0, M_1, u_S^*, u_R^*) 给 $\mathcal{C}$。$\mathcal{C}$ 随机选择 $b \in \{0,1\}$ 和一个想要签密的消息 M_b，有以下 2 种结果。

1) 当 $u_S^* \neq u_{\varphi}$ 且 $u_R^* \neq u_{\varphi}$，挑战的是签密。

如果 $F(u_S) = 0 \bmod q$，$\mathcal{C}$ 放弃；否则，计算 u_S 的私钥 $sk_S^* = (sk_{S,1}^*, sk_{S,2}^*)$。

如果 $F(u_R) = 0 \bmod q$ 且 $K(m_b^*) = 0 \bmod q$，令 $pk_S^* = e(B, A^{\alpha})^{x_S^*}$ 和 $pk_R^* = e(B, A^{\alpha})^{x_R^*}$ 分别是身份 u_S^* 和 u_R^* 的公钥，$\mathcal{C}$ 获取秘密值 x_S^* 和 x_R^*，令签密为

$$\sigma_1^* = M_b^* Z^{x_R^*}, \sigma_2^* = Z^{-x_R^*}, \sigma_3^* = (g^c)^2, \sigma_4^* = (g^c)^{2J_{u_R^*}}$$

$$\sigma_5^* = (A^{\alpha x_S^*})^{-\frac{1}{F(u_S^*)}} g^{t_s^*} g^c$$

$$\sigma_6^* = (A^{\alpha x_S^*})^{-\frac{J(u_S^*)}{F(u_S^*)}} (u' \prod_{i \in \mathbb{U}_S^*} u_i)^{t_S^*} ((g^c)^{2L(m_b^*)(r'+r'')}) (g^c)^{J(u_S^*)}$$

$\mathcal{C}$ 发送 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_5^*, \sigma_6^*)$ 给攻击者 $\mathcal{A}_{\Pi}$；否则，$\mathcal{C}$ 放弃。

2) 当 $u_S^* = u_{\varphi}$ 且 $u_R^* \neq u_{\varphi}$，挑战的是签名。

$\sigma_1^* = M_b^* Z^{x_R^*}, \sigma_2^* = Z^{-x_R^*}, \sigma_3^* = (g^c)^2$，$\sigma_4^* = (g^c)^{2J_{u_R^*}}$，

$\sigma_5^*=0$，$\sigma_6^*=0$。

$\mathcal{C}$ 发送密文 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,\sigma_6^*)$ 给 $\mathcal{A}_{\text{II}}$；否则，$\mathcal{C}$ 放弃。

阶段 2　$\mathcal{A}_{\text{II}}$ 继续进行同阶段 1 的询问，但不允许对 u_S^* 和 u_R^* 的签密进行询问。最终，$\mathcal{A}_{\text{II}}$ 输出对 b 的猜测。如果 $b'=b$，攻击者 $\mathcal{A}_{\text{II}}$ 赢得了游戏，输出对 DBDH 的作答 $Z=e(g,g)^{abc}$。

下面分析 $\mathcal{C}$ 攻击成功的概率，分析过程同引理 1。

对签密算法，有

$$\Pr\left[\overline{\text{abort}}\right]\geqslant\Pr\left[\text{E}_1\wedge\text{E}_2\wedge\text{E}_3\wedge\text{E}_4\wedge\text{E}_5\wedge\text{E}_6\right]$$

$$=\frac{1}{16q_pq_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)$$

对加密算法，有

$$\Pr\left[\overline{\text{abort}}\right]\geqslant\Pr\left[\text{E}_1\wedge\text{E}_2\wedge\text{E}_3\wedge\text{E}_4\wedge\text{E}_5\right]$$

$$=\frac{1}{16q_p(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

如果模拟过程不终止，$\mathcal{A}_{\text{II}}$ 若能以 ε 的概率攻破该算法，则能够以 ε' 的概率解决 DBDH 问题。

对签密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16q_pq_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)$$

对加密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16q_p(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证毕。

定理 2　在 CDH 假设下，CLGSC 方案在签名模式下是存在性不可伪造的，即 EUF-CMA 安全的。

定理 2 的证明可由引理 3 和引理 4 得到。

引理 3　假设存在一个 EUF-CMA 的第 1 类攻击者 $\mathcal{A}_{\text{I}}$ 可以以 ε 的优势赢得 3.2 节定义的游戏 III，则存在一个区分者 $\mathcal{C}$ 可以以 ε' 的优势解决 CDH 问题。

对签密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left(1-\frac{1}{q_s(n_u+1)}\right)$$

对签名算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证明　假设第 1 类攻击者 $\mathcal{A}_{\text{I}}$ 能够以不可忽略的概率攻破本文的算法，则存在一个算法 $\mathcal{C}$ 能够解决 CDH 问题，即给定一个随机实例 (g,g^a,g^b)，计算 g^{ab}。

系统建立　系统建立如同定理 1。需要注意的是，$\mathcal{C}$ 设定 $g_1=g^a$，$g_2=g^b$。

阶段 1　阶段 1 的各种询问也如同定理 1。

伪造　$\mathcal{A}_{\text{I}}$ 对消息 M^* 和身份 u_S^* 和 u_R^* 产生一个有效的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,\sigma_6^*)$，攻击者 $\mathcal{A}_{\text{I}}$ 在签密阶段不能对 (M^*,u_S^*,u_R^*) 进行询问，也不能对 u_S^* 进行私钥询问。身份 u_S^* 的公钥是 $pk_S^*=e(\text{g}^a,\text{g}^b)^x$，$u_R^*$ 的当前公钥 pk_R^*。

1) 当 $u_S^*\neq u_\varphi$ 和 $u_R^*\neq u_\varphi$，是签密伪造。

$F(u_S^*)\neq 0\bmod q, K(m^*)=0\bmod q, F(u_R^*)\neq 0\bmod q$ 时，$\mathcal{C}$ 可以获得 u_R^* 的私钥：$sk_R^*=(sk_{R,1}^*,sk_{R,2}^*)$，可计算 $m^*=H(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,u_R^*,pk_R^*)\in\{0,1\}^m$ 和 $M=\dfrac{\sigma_1^*e(\sigma_4^*,sk_{R,2}^*)}{\sigma_2^*e(\sigma_3^*,sk_{R,1}^*)}$。因此，$\mathcal{C}$ 可以计算出

$$\frac{\sigma_6^*}{(\sigma_5^*)^{J(u_S^*)}(\sigma_3^*)^{L(m^*)}}$$

$$=\frac{g_2^{ax}(u'\prod_{i\in U_{S^*}}u_i)^{t_S^*}(v'\prod_{i\in M}v_i)^{r'+r''}(u'\prod_{i\in U_{S^*}}u_i)^{r''}}{(g^{t_S^*}g^{r''})^{J(u_S^*)}(g^{r'+r''})^{L(m^*)}}$$

$$=g_2^{ax}=g^{abx}$$

挑战者 $\mathcal{C}$ 获得秘密值 x 使 $pk_S^*=e(g^a,g^b)^x$，因而输出 g^{ab}，相当于求解了 CDH 问题。

2) 当 $u_S^*\neq u_\varphi$ 和 $u_R^*=u_\varphi$，是签名伪造。

如果 $F(u_S^*)=0\bmod q$ 和 $K(m^*)=0\bmod q$，$\mathcal{C}$ 计算 $m^*=H(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,u_R^*,pk_R^*)\in\{0,1\}^m$。因此，$\mathcal{C}$ 可以计算出

$$\frac{\sigma_6^*}{(\sigma_5^*)^{J(u_S^*)}(\sigma_3^*)^{L(m^*)}}$$

$$=\frac{g_2^{ax}(u'\prod_{i\in U_{S^*}}u_i)^{t_S^*}(v'\prod_{i\in M}v_i)^{r'+r''}(u'\prod_{i\in U_{S^*}}u_i)^{r''}}{(g^{t_S^*}g^{r''})^{J(u_S^*)}(g^{r'+r''})^{L(m^*)}}$$

$$=g_2^{ax}=g^{abx}$$

下面分析 $\mathcal{C}$ 攻击成功的概率。如果模拟过程不终止，则有以下 6 个事件发生。

E_1、E_2、E_3：如同定理 1 的定义。

E_4：$F(u_S^*)=0 \bmod q$。

E_5：$F(u_R^*)\neq 0 \bmod q$ (仅对 $u_R^*\neq u_\varphi$)。

E_6：$K(m^*)=0 \bmod l_m$。

同定理 1 中的推理，可推导得

$$\Pr[\mathrm{E}_1]\geqslant\frac{q_{pp}+q_p}{l_u},\quad \Pr[\mathrm{E}_2]\geqslant 1-\frac{q_S}{l_u},$$

$$\Pr[\mathrm{E}_3]\geqslant 1-\frac{q_u}{l_u l_m},\quad \Pr[\mathrm{E}_4]=1-\frac{1}{l_u}\cdot\frac{1}{n_u+1}$$

$$\Pr[\mathrm{E}_5]=1-\frac{1}{l_u}\cdot\frac{1}{n_u+1},\quad \Pr[\mathrm{E}_6]=\frac{1}{l_m}\cdot\frac{1}{n_m+1}$$

攻击者 $\mathcal{C}$ 不放弃的概率如下。

对签密算法，有

$$\Pr[\overline{\text{abort}}]\geqslant\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3\wedge\mathrm{E}_4\wedge\mathrm{E}_5\wedge\mathrm{E}_6]$$

$$=\frac{1}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left[1-\frac{1}{q_s(n_u+1)}\right]$$

对签名算法，有

$$\Pr[\overline{\text{abort}}]\geqslant\Pr[\mathrm{E}_1\wedge\mathrm{E}_2\wedge\mathrm{E}_3\wedge\mathrm{E}_4\wedge\mathrm{E}_5]$$

$$=\frac{1}{16(q_{pp}+q_p)(n_u+1)}(1-\frac{1}{2q_s})$$

如果模拟过程不终止，$\mathcal{A}_{\mathrm{I}}$ 若能以 ε 的概率攻破算法，则 $\mathcal{C}$ 能够以 ε' 的概率解决 CDH 问题。

对签密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)q_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left[1-\frac{1}{q_s(n_u+1)}\right]$$

对签名算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16(q_{pp}+q_p)(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证毕。

引理 4 假设存在一个 IND-CCA 的 t 时间的第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 可以 ε 的优势赢得 3.2 节定义的游戏 IV，则存在一个区分者 $\mathcal{C}$ 可以以 ε' 的优势解决 CDH 问题。

对签密算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16q_pq_u(n_u+1)(n_m+1)}\left(1-\frac{1}{2q_s}\right)\left[1-\frac{1}{q_s(n_u+1)}\right]$$

对签名算法，有

$$\varepsilon'\geqslant\frac{\varepsilon}{16q_p(n_u+1)}\left(1-\frac{1}{2q_s}\right)$$

证明 假设第 2 类攻击者 $\mathcal{A}_{\mathrm{II}}$ 能够以不可忽略的概率攻破本文的算法，则存在一个算法 $\mathcal{C}$ 能够解决 CDH 问题，即给定一个随机实例 (g,g^a,g^b)，计算 g^{ab}。

系统参数的设置如同引理 2，攻击者把系统的主密钥 α 发送给 $\mathcal{C}$。$\mathcal{A}_{\mathrm{II}}$ 可以进行多项式有界次的公钥询问、私钥提取询问、签密询问和解签密询问。如果 $\mathcal{C}$ 不放弃，$\mathcal{A}_{\mathrm{II}}$ 对消息 M^* 及身份 u_S^* 和 u_R^* 生成有效的签名 $\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,\sigma_6^*)$，身份 u_S^* 的公钥是 $pk_S^*=e(B,A^\alpha)^x$，u_R^* 的公钥是 pk_R^*。

1) 当 $u_S^*\neq u_\varphi$ 和 $u_R^*\neq u_\varphi$，是签密伪造。

$F(u_S^*)\neq 0 \bmod q, K(m^*)=0 \bmod q, F(u_R^*)\neq 0 \bmod q$ 时，$\mathcal{C}$ 可以获得 u_R^* 的私钥：$sk_R^*=(sk_{R,1}^*,sk_{R,2}^*)$，可计算 $m^*=H(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,u_R^*,pk_R^*)\in\{0,1\}^m$ 和 $M=\dfrac{\sigma_1^*e(\sigma_4^*,sk_{R,2}^*)}{\sigma_2^*e(\sigma_3^*,sk_{R,1}^*)}$。因此，$\mathcal{C}$ 可以计算出

$$\frac{\sigma_6^*}{(\sigma_5^*)^{J(u_S^*)}(\sigma_3^*)^{L(m^*)}}$$

$$=\frac{g_2^{a\alpha x}(u'\prod_{i\in\mathbb{U}_{S^*}}u_i)^{t_S^*}(v'\prod_{i\in\mathbb{M}}v_i)^{r'+r''}(u'\prod_{i\in\mathbb{U}_{S^*}}u_i)^{r''}}{(g^{t_S^*}g^{r''})^{J(u_S^*)}(g^{r'+r''})^{L(m^*)}}$$

$$=(g_2^{ax})^\alpha=(g^{ab})^{x\alpha}$$

挑战者 $\mathcal{C}$ 获得秘密值 x 和主密钥 α，因而输出 g^{ab}，相当于求解了 CDH 问题。

2) 当 $u_S^*\neq u_\varphi$ 和 $u_R^*=u_\varphi$，是签名伪造。

若 $F(u_S^*)=0 \bmod q$ 和 $K(m^*)=0 \bmod q$，$\mathcal{C}$ 计算 $m^*=H(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\sigma_5^*,u_R^*,pk_R^*)\in\{0,1\}^m$。$\mathcal{C}$ 可以计算

$$\frac{\sigma_6^*}{(\sigma_5^*)^{J(u_S^*)}(\sigma_3^*)^{L(m^*)}}$$

$$=\frac{g_2^{a\alpha x}(u'\prod_{i\in\mathbb{U}_{S^*}}u_i)^{t_S^*}(v'\prod_{i\in\mathbb{M}}v_i)^{r'+r''}(u'\prod_{i\in\mathbb{U}_{S^*}}u_i)^{r''}}{(g^{t_S^*}g^{r''})^{J(u_S^*)}(g^{r'+r''})^{L(m^*)}}$$

$$=(g_2^{ax})^\alpha=(g^{ab})^{x\alpha}$$

证毕。

6 数值实验

本节主要给出所提方案在签密、验证、解密阶段以及整个算法总的运行时间。本文在 Linux 操作系统下利用双线性对包（pairing-based cryptography library），用

C 语言编程，在 2.9 GHz CPU，4 GB RAM PC 机上运行。表 2 说明双线性对包参数类型为 *a* 和 *e* 的性质。

表 2　　对参数的主要性质

参数类型	基域/bit	Dlog 安全/bit	椭圆曲线次数
a	512	1 024	2
e	1 024	1 024	1

在本文的数值实验中，对参数类型 *a* 和类型 *e* 对应的椭圆曲线安全参数分别为|*p*|=512 bit 和|*p*|=1 024 bit。

表 3 为本文算法运行 100 次各个阶段的平均运行时间。由表 3 可以看出，当参数类型选为 *a* 时，总的运行时间为 0.116 3 s，而当参数类型选为 *e* 时，总的运行时间为 0.305 2 s，这是因为类型 *e* 的安全参数更高一些。另外，由签密、验证和解密各个阶段的运行时间可以看出本文提出的算法是有效的。

表 3　签密、验证和解密阶段以及算法总运行时间

参数类型	签密阶段/s	验证阶段/s	解密阶段/s	总运行时间/s
a	0.025 4	0.010 4	0.005 4	0.116 3
e	0.085 6	0.035 8	0.024 8	0.305 2

7　结束语

本文提出了一个新的无证书广义签密方案，并在标准模型下证明了算法的安全性，在 Linux 操作系统下利用双线性对包对算法做了数值测试，分析了算法的有效性。本文的侧重点在于提高算法的安全性，所以在算法效率的分析上未与现有的其他算法做比较。下一步的研究目标是在提高算法安全性的基础上，研究高效率的广义签密算法。

参考文献：

[1] BARBOSA M, FARSHIM P. Certificateless signcryption[C]//ACM Symposium on Information, Computer and Communications Security. ACM, 2008:369-372.

[2] ARANHA D, CASTRO R, LÓPEZ J, et al. Efficient certificateless signcryption[C]//8th Brazilian Symposium on Information and Computer Systems Security (SBSEG 2008). 2008.

[3] WU C, CHEN Z. A new efficient certificateless signcryption scheme[C]//2012 Fourth International Symposium on Information Science and Engineering, 2008, 1(1):661-664.

[4] XIE W, ZHANG Z. Efficient and provably secure certificateless signcryption from bilinear maps[C]//IEEE International Conference on Wireless Communications, Networking and Information Security. IEEE, 2010: 558-562.

[5] 蔡伟艺, 杨晓元, 韩益亮, 等. 可公开验证的高效无证书签密方案[J]. 计算机工程, 2011, 37(17):108-110.
CAI W Y, YANG X Y, HAN Y L, et al. Efficient certificateless signcryption scheme with public verifiability[J]. Computer Engineering, 2011, 37(17):108-110.

[6] 刘文浩, 许春香. 无双线性配对的无证书签密方案[J]. 软件学报, 2011, 22(8):1918-1926.
LIU W H, XU C X. Certificateless signcryption scheme without bilinear pairing[J]. Journal of Software, 2011, 22(8): 1918-1926.

[7] LIU Z, HU Y, ZHANG X, et al. Certificateless signcryption scheme in the standard model[J]. Information Sciences, 2010, 180(3):452-464.

[8] MIAO S, ZHANG F, LI S, et al. On security of a certificateless signcryption scheme[J]. Information Sciences, 2013, 232(5):475-481.

[9] WENG J, YAO G, DENG R H, et al. Cryptanalysis of a certificateless signcryption scheme in the standard model[J]. Information Sciences, 2011, 181(3):661-667.

[10] HAN Y, YANG X, WEI P, et al. ECGSC: elliptic curve based generalized signcryption[C]//International Conference on Ubiquitous Intelligence and Computing. Springer-Verlag, 2006:956-965.

[11] JI H, HAN W, ZHAO L. Certificateless generalized signcryption[J]. Physics Procedia, 2012, 33(6):962-967.

[12] KUSHWAH P, LAL S. Efficient generalized signcryption schemes[R]. Cryptology ePrint Archive Report 2010/346.

[13] SELVI S S D, VIVEK S S, RANGAN C P. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[C]//International Conference on Information Security and Cryptology. Springer-Verlag, 2009:75-92.

[14] ZHOU C, ZHOU W, DONG X. Provable certificateless generalized signcryption scheme[J]. Designs Codes & Cryptography, 2014, 71(2):331-346.

[15] 冀会芳, 韩文报, 刘连东. 高效的无证书广义签密方案[J]. 四川大学学报：工程科学版, 2011, 43(5):133-139.
JI H F, HAN W B, LIU L D. Efficient certificateless generalized signcryption[J]. Journal of Sichuan University, 2011, 43(5):133-139.

[16] 刘连东, 冀会芳, 韩文报, 等. 一种无随机预言机的无证书广义签密方案[J]. 软件学报, 2012, 23(2):394-410.
LIU L D, JI H F, HAN W B, et al. Certificateless generalized signcryption scheme without random oracles[J]. Journal of Software, 2012, 23(2):394-410.

[17] WATERS B. efficient identity-based encryption without random oracles[M]. Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005:114-127.

作者简介：

牛淑芬（1976-），女，甘肃通渭人，西北师范大学副教授、硕士生导师，主要研究方向为密码学、云计算和大数据网络的隐私保护。

牛灵（1991-），女，甘肃通渭人，西北师范大学硕士生，主要研究方向为密码学。

王彩芬（1963-），女，河北安国人，西北师范大学教授、博士生导师，主要研究方向为信息安全、密码学。

李亚红（1984-），女，甘肃定西人，西北师范大学博士生，主要研究方向为密码学。