doi:10.11959/j.issn.1000-436x.2017267

抗密钥泄露的无证书签密方案

秦艳琳，吴晓平，胡卫
（海军工程大学信息安全系，湖北 武汉 430033）

摘 要：传统无证书签密方案在实际应用环境中容易遭受边信道攻击，带来密钥泄露问题。为抵制此类攻击，基于椭圆曲线密码体制及双线性对提出一种抗密钥泄露的无证书签密方案，并在随机预言机模型下证明方案的安全性建立在判定 Diffie-Hellman 问题的困难性之上，且能抵制适应性选择密文及密钥泄露攻击，满足选择消息及密钥泄露攻击下的存在不可伪造性。该方案没有使用构造复杂的非交互式零知识证明系统（NIZK），在签密阶段不含双线性对运算，与同类方案相比，能抵制密钥泄露攻击且具有较高的运算效率。
关键词：无证书签密；抗密钥泄露；判定 Diffie-Hellman 问题；椭圆曲线密码；随机预言机
中图分类号：TP309 **文献标识码**：A

Leakage-resilient certificateless signcryption scheme

QIN Yan-lin, WU Xiao-ping, HU Wei
（Department of Information Security, Naval University of Engineering, Wuhan 430033, China）

Abstract: In practical applications, the potential adversary may exploit partial information about the secret keys by side-channel attacks , traditional certificateless signcryption schemes can't resist these key-leakage attacks. A leakage-resilient certificateless signcryption scheme based on Elliptic Curve Cryptography and bilinear pairing was presented. In the random oracle, proved that the security of the scheme is based on the decisional Diffie-Hellman assumption. The scheme is also proved semantically secure against adaptive posterior chosen-ciphertext key-leakage attacks (KL-CCA2), and existentially unforgeable against chosen-message key-leakage attacks(KL-CMA). The proposed scheme was free from non-interactive zero knowledge proof system and needs no bilinear paring operation in signcryption phase. Compared with other schemes of the same kind, the proposed scheme can resist key-leakage attacks and maintains high efficiency.
Key words: certificateless signcryption, leakage-resilient, decisional Diffie-Hellman assumption, elliptic curve cryptography, random oracle

1 引言

签密方案[1]可以通过执行一个算法步骤同时实现签名和加密，较“先签名，后加密”的传统密码应用方案在通信和计算消耗上有较明显的优势。目前已有的签密方案主要分为三大类：一类是基于传统 PKI 机制的签密方案，需要证书管理中心(CA)为用户签发公钥证书，以确保系统中用户公钥的真实性，公钥证书库的管理和维护给系统运行带来巨大的负担；第二类是采用基于身份的公钥密码构造的签密方案[2,3]，该类方案虽避免了公钥证书的使用和维护，但用户私钥完全由第三方 KGC 产生，故存在私钥托管问题；第三类是基于无证书公钥密码[4]提出的无证书签密方案[5~9]，该类方案既不需要证书管理中心，同时也避免了密钥托管问题。以上三大类签密方案的一个共同点是其安全性都建立在敌手无法得到算法秘密信息（主密钥及用户私钥等）的理想情况下，而在现实环境中，攻击者可以通过边信道攻击等手段获取有关系统私钥的部分信息，由此导致方案无法满足原有的安全需求。

收稿日期：2017-10-09
基金项目：国家自然科学基金面上基金资助项目（No.61672531）；海军工程大学自主立项基金资助项目（No.20161607）
Foundation Items: The National Natural Science Foundation of China (No.61672531), The Natural Science Found of Naval University of Engineering (No.20161607)

为了解决现实应用中的密钥泄露问题，抗泄露密码方案被陆续提出。首个抗泄露公钥加密方案的安全模型由 Akavia 等[10]提出，在此类安全模型中，攻击者被允许以任意的函数 f 询问泄露预言机，并得到输出 $f(SK)$，SK 是系统的私钥。Naor 等[11]提出两个抗泄露公钥加密方案，并分别在适应性前向选择密文及密钥泄露攻击（KL-CCA1）和适应性后向选择密文攻击及密钥泄露攻击(KL-CCA2)下证明了方案的安全性。Li 等[12]在 Naor 等所提方案的基础上给出一个更为高效的抗泄露公钥加密方案，并给出方案在适应性后向选择密文攻击及密钥泄露攻击下的安全性。Xiong 等[13]提出第一个抗泄露无证书加密方案，该方案基于双线性对和非交互式零知识证明系统（NIZK）构造，但并未给出非交互式零知识证明的具体构造方法，导致方案的计算效率难以评估，并且方案仅在适应性选择明文攻击及密钥泄露攻击（KL-CPA）和 KL-CCA1 下被证明是安全的。Yu 等[14]在 Xiong 等所提方案的基础上构造了一个抗泄露证书基加密方案，并证明方案不仅能抵制解密密钥泄露还能抵制系统主密钥泄露攻击，但由于使用了大量双线性对运算和 NIZK，导致方案的运算效率较低。在抗泄露签密方案方面，Tang 等[15]基于传统 PKI 机制提出 2 个抗泄露签密方案，但仅证明了方案在适应性选择消息及密钥泄露攻击（KL-CMA）下的存在不可伪造性和 KL-CCA1 下的不可区分性。Zhou 等[16]提出一个不含双线性对的抗泄露无证书签密方案，并在 KL-CCA2 和 KL-CMA 下证明了方案的安全性，但方案中包含一个 NIZK，且未给出具体构造方法，导致方案的运算效率无法准确评估。本文将提出一个高效的抗泄露无证书签密方案，方案中没有使用 NIZK，仅在签名验证阶段使用了双线性对运算，并在随机预言机模型下证明了方案在 KL-CCA2 下的机密性和 KL-CMA 下的存在不可伪造性。

2 预备知识

定义 1 判定 Diffie-Hellman 问题（DDH）。设 G 是椭圆曲线加法循环群，阶为大素数 q，P 为 G 中的一个生成元，已知 $aP,bP,cP\in G$，$a,b,c\in Z_q^*$是未知的随机数，判定 $c=ab \bmod q$ 是否成立。

定义 2 统计距离。2 个随机变量的统计距离定义如下。

$$SD(X,Y)=\frac{1}{2}\sum_{z\in Z}\left|Pr[X=z]-Pr[Y=z]\right| \tag{1}$$

X、Y 为 2 个取值于有限域 Z 的随机变量。如果 $SD(X,Y)\leqslant\varepsilon$，则称随机变量 X 和 Y 是 ε-接近的。

定义 3 通用散列函数。如果一族散列函数 $\{H_k: X\to Y\}$ 满足

$$Pr_{k\leftarrow\mathcal{K}}[H_k(x_1)=H_k(x_2)]\leqslant\frac{1}{|\mathcal{Y}|} \tag{2}$$

其中，$x_1,x_2\in X$，且 $x_1\neq x_2$，则称其为通用散列函数族。

定义 4 最小熵随机变量 A 的最小熵定义如下。

$$H_\infty(X)=-\mathrm{lb}(\max_x Pr[X=x]) \tag{3}$$

定义 5 平均条件最小熵。平均条件最小熵表示在变量 Y 已知的情况下随机变量 X 保留的未知信息量。定义如下

$$\tilde{H}_\infty(X\mid Y)=-\mathrm{lb}(E_{y\leftarrow\mathcal{Y}}[2^{-H_\infty(X|Y=y)}]) \tag{4}$$

引理 1 对于任意随机变量 X、Y、Z，若 Y 有至多 2^δ 种可能值，则有式（5）成立。

$$\tilde{H}_\infty(X\mid Y,Z)\geqslant\tilde{H}_\infty(X\mid Z)-\delta \tag{5}$$

定义 6 随机提取器。对所有满足 $X\in\boldsymbol{X}$ 且 $\tilde{H}_\infty(X\mid Z)\geqslant k$ 的随机变量对（X,Z），若函数 Ext：$X\times\{0,1\}^t\to\{0,1\}^m$ 满足 $SD((Ext(X,S),S,Z),(U_m,S,Z))\leqslant\varepsilon$，其中，$S$ 是服从 $\{0,1\}^t$ 上均匀分布的随机种子，U_m 是服从 $\{0,1\}^m$ 上均匀分布的随机串，则称函数 Ext 是平均情形(k,ε)-顽健提取器。

引理 2 剩余散列引理 $\{H_k: X\to Y\}_{k\in\mathrm{K}}$ 是一族通用散列函数。U_Y 是集合 Y 上的均匀分布，对于任意的随机变量 $X\in\boldsymbol{X}$，$Z\in\boldsymbol{Z}$，$K\in\boldsymbol{K}$，满足

$$SD((H_k(X),K),(U_{\mathcal{Y}},K))\leqslant\frac{1}{2}\sqrt{2^{-H_\infty(X)}|\mathcal{Y}|} \tag{6}$$

并且 $SD((H_k(X),K,Z),(U_{\mathcal{Y}},K,Z))\leqslant\frac{1}{2}\sqrt{2^{-\tilde{H}_\infty(X|Z)}|\mathcal{Y}|}$。

引理 3 设 $\{H_k:X\to Y\}_{k\in\mathrm{K}}$ 是一族通用散列函数。对于任意的随机变量 $X\in\boldsymbol{X}$，$Z\in\boldsymbol{Z}$，$K\in\boldsymbol{K}$，若 $\tilde{H}_\infty(X\mid Z)\geqslant l$，$\mathrm{lb}\,|\mathcal{Y}|\leqslant l-2\mathrm{lb}\left(\frac{1}{\varepsilon}\right)+2$，则有 $SD((H_k(X),K,Z),(U_{\mathcal{Y}},K,Z))\leqslant\varepsilon$。

3 抗泄露无证书签密安全模型

Zhou 等[16]描述了抗泄露无证书签密的安全模型。首先，针对抗泄露无证书签密方案的攻击者包

括敌手 A_{I} 和敌手 A_{II}。前者能对系统用户的公钥进行替换，但不能接触系统主密钥；后者能获取主密钥，但无法替换用户公钥。将抗泄露无证书签密方案记作 Ψ，针对方案 Ψ 的攻击类型主要包括 2 种：适应性选择密文及密钥泄露攻击（KL-CCA2）和选择消息及密钥泄露攻击（KL-CMA）。Ψ 的安全模型可以通过敌手 A_{I}、A_{II} 以及挑战者 *Ch* 之间开展的 4 个游戏来定义。（δ 为固定的泄露参数）。

定义 7　A_{I} 敌手攻击下的机密性

假设 A_{I} 在概率多项式时间内在如下定义的游戏 1 中取胜的优势是可以忽略的，则称 Ψ 在 KL-CCA2 下满足机密性。

游戏 1

系统设置：*Ch* 选取系统 Ψ 中的公共参数 ρ 及主密钥，并将 ρ 发送给 A_{I}。A_{I} 收到后输出用户身份 *ID*，并向 *Ch* 提出以下类型的询问，询问次数为多项式次数泄露信息询问：A_{I} 输入用户的身份 *ID* 和一个概率多项式时间函数 $f_i: K \to \{0,1\}^*(i \geqslant 1)$，挑战者 *Ch* 回复 $f_i(SK_{ID})$，但满足 $\sum_i f_i(SK_{ID}) \leqslant \delta$。

散列询问：A_{I} 进行对任意散列值的询问。

提取私钥询问：A_{I} 对 *Ch* 提出针对私钥 SK_{ID} 的提取询问，*Ch* 产生 SK_{ID} 并将其发送给 A_{I}。

提取公钥询问：A_{I} 对 *Ch* 提出针对公钥 PK_{ID} 的提取询问，*Ch* 产生 PK_{ID} 并将其发送给 A_{I}。

公钥替换询问：A_{I} 可以重新选取公钥 PK'_{ID} 来对公钥 PK_{ID} 进行替换。

签密询问阶段：A_{I} 向 *Ch* 提出针对(m,ID_r,ID_s)的签密询问，其中，ID_r 和 ID_s 分别为接收者和签密者的身份，*Ch* 生成 PK_r 和 SK_s，并计算 σ=SC(ρ,*m*, PK_r, SK_s)(SC 为签密算法)，进而将 σ 发送给 A_{I}。

解签密询问阶段：*Ch* 接收到针对(σ,ID_r,ID_s)的解签密询问后，计算 SK_r 和 PK_s。并计算 USC(ρ,σ,PK_s, SK_r)(USC 为解签密算法)，进而将 *m* 或“签密为假”发送给 A_{I}。

挑战阶段：A_{I} 选定长度相等的消息 m_0 和 m_1，接收者身份 ID'_r 及签密者身份 ID'_s，随机选择 $z \in \{0,1\}$, 利用 SK'_s 和 PK'_r 计算 $\sigma' = SC(\rho, m_z, PK'_r, SK'_s)$，最后把 σ' 传送给 A_{I}。

猜测阶段：A_{I} 执行类似于询问阶段的一系列询问（不包括对 ID'_r 的提取私钥询问和针对 σ' 的解签密询问），进而输出猜测 $z' \in \{0,1\}$，若满足 $z' = z$，说明 A_{I} 赢得了游戏 1，获胜优势为 $Adv^{\Psi,A_I}_{\text{KL-CCA2}} = |Pr[z' = z] - \frac{1}{2}|$。

定义 8　A_{II} 敌手攻击下的机密性

假设 A_{II} 敌手在概率多项式时间内在如下定义的游戏 2 中取胜的优势是可以忽略的，则称 Ψ 在 KL-CCA2 下满足机密性。

游戏 2

系统设置：*Ch* 选取系统 Ψ 中的公共参数 ρ 及主密钥，并将 ρ 发送给 A_{II}。A_{II} 收到后输出用户身份 *ID*，并向 *Ch* 提出类似于定义 7 中的泄露信息询问、散列询问、部分私钥和秘密值询问、签密询问和解签密询问，注意在询问过程中不能执行“公钥替换”询问，但可以利用掌握的主密钥计算用户的部分私钥。询问阶段执行完毕后进行类似于定义 7 的挑战与猜测。若 A_{II} 赢得游戏 2，获胜优势为 $Adv^{\Psi,A_{\mathrm{II}}}_{\text{KL-CCA2}} = |Pr[z' = z] - \frac{1}{2}|$。

定义 9　如果 A_{I} 敌手在概率多项式时间内在如下定义的游戏 3 中取胜的优势是可以忽略的，则称 Ψ 在 KL-CMA 下满足存在不可伪造性。

游戏 3

系统设置：*Ch* 选取系统 Ψ 中的公共参数 ρ 及主密钥，并将 ρ 发送给 A_{I}。A_{I} 收到后输出用户身份 ID'_s。

具体询问同定义 7。

伪造阶段：在没有对 ID'_s 执行私钥提取询问的前提下，A_{I} 输出伪造的 (σ', ID'_s, ID'_r)，若 σ' 经过接收者的解密验证为真，则称 A_{I} 赢得了游戏 3，其优势为

$$Adv^{\Psi,A_I}_{\text{KL-CMA}} \leqslant \left| Pr[\sigma' \text{通过验证}] - \frac{1}{2} \right| \tag{7}$$

定义 10　如果 A_{II} 在概率多项式时间内在如下定义的游戏 4 中取胜的优势是可以忽略的，则称 Ψ 在 KL-CMA 下具有存在不可伪造性。

游戏 4

执行类似于定义 8 中的系统设置与询问。

伪造：在没有对 ID'_s 执行提取私钥询问的前提下，A_{II} 输出伪造的 (σ', ID'_s, ID'_r)，若 σ' 经过接收者的解密验证为真，则称 A_{II} 赢得了游戏 4，其优势为

$$Adv^{\Psi,A_{\mathrm{II}}}_{\text{KL-CMA}} \leqslant \left| \mathrm{Pr}[\sigma' \text{通过验证}] - \frac{1}{2} \right| \tag{8}$$

4 抗泄露无证书签密方案

本节对抗泄露无证书签密方案的算法细节进行描述。

1) 系统设置

密钥生成中心选定阶为大素数 q 的椭圆曲线加法循环群 G 和乘法循环群$(G_T,\cdot)$，随机选取 P_1、P_2 为加法群 G 的两个生成元；设定双线性映射 $\hat{e}$：$G\times G\to G_T$；定义 3 个安全散列函数

H_0：$\{0,1\}^*\times G\times G\to Z_q^*$

H_1：$G\times G\times G\times\{0,1\}^*\times G\to G$

H_2：$G\times G\times\{0,1\}^*\to Z_q^*$

选择随机提取函数 Ext：$G\times\{0,1\}^s\to\{0,1\}^m$，该函数是平均情形 $(\mathrm{lb}q-\delta,\vartheta)$—顽健的。$\delta(\gamma)$是固定的泄露参数($\gamma$ 为系统安全参数)，满足 $\delta\leqslant \mathrm{lb}q-L(m)-2\mathrm{lb}\left(\frac{1}{\vartheta}\right)$，其中，$L(m)$代表待签密消息长度。选择随机数 $t_1,t_2\in Z_q^*$作为系统主密钥，计算 $P_m=t_1P_1+t_2P_2$ 为对应的系统公钥，公开 $\rho=(G, G_T,q,P_m, P_1, P_2,H_0, H_1, H_2)$，对 t_1、t_2 进行保密处理。

2) 用户公/私钥设置

用户 ID_i 选择随机数 $u_{i1},u_{i2}\in Z_q^*$作为秘密值，计算 $U_i=u_{i1}P_1+u_{i2}P_2$，然后把 U_i 通过安全渠道发送给密钥生成中心；密钥生成中心在收到消息 U_i 以后，选择随机数 $k_{i1},k_{i2}\in Z_q^*$，接着计算

$$K_i=k_{i1}P_1+k_{i2}P_2,\ D_{i1}=k_{i1}+t_1H_0(ID_i,K_i,U_i),\ D_{i2}=k_{i2}+t_2H_0(ID_i,K_i,U_i) \tag{9}$$

将 $K_i\|D_{i1}\|D_{i2}$ 安全传递给用户 ID_i，ID_i 将$(u_{i1},u_{i2},D_{i1},D_{i2})$和$(U_i,K_i)$分别作为自己的完整私钥及公钥。用户通过验证 $K_i+H_0(ID_i,K_i,U_i)P_m=D_{i1}P_1+D_{i2}P_2$ 成立与否来确认密钥生成中心传递的部分私钥的合法性。

3) 签密算法

签密用户通过执行以下算法对(m,ID_A,ID_B)进行签密。

①选择随机数 $a\in Z_q^*$，种子 $S\in\{0,1\}^s$，计算 $T_1=aP_1$，$T_2=aP_2$，$h_A=H_0(ID_A, K_A,U_A)$, $h=H_1(T_1,T_2, U_A, ID_A, m,K_A)$，$w=H_2(T_1,T_2,S)$，$s_1=T_1+h(wD_{A1}+u_{A1}h_A)$，$s_2=T_2+h(wD_{A2}+u_{A2}h_A)$。

② 计算 $h_B=H_0(ID_B, K_B, U_B)$，$V_A=a(U_B+w(K_B+h_BP_m))$，$C=\mathrm{Ext}(V_A, S)\oplus(m\|ID_A)$。

③ 最后，签密用户将签密信息 $\sigma=(s_1,s_2, T_1,T_2, C,S)$传递给接收者。

4) 解签密算法

接收者收到签密信息 $\sigma=(s_1,s_2,T_1,T_2,C,S)$后，执行下列算法进行解签密验证。

①计算 $w=H_2(T_1,T_2,S)$,$V_B=(u_{B1}+wD_{B1})T_1+(u_{B2}+wD_{B2})T_2$, $\mathrm{Ext}(V_B, S)\oplus C=m\|ID_A$。

② 计算 $h=H_1(T_1,T_2,U_A,ID_A,m,K_A)$，验证等式 $\hat{e}(s_1,P_1)\ \hat{e}(s_2,P_2)=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,wK_A+h_A(wP_m+U_A))$ 成立与否，若成立，接受该签密密文为合法密文，若不成立，认为签密消息为假。

下面给出算法的正确性证明。

① 部分私钥验证算法的正确性

$$\begin{aligned}&D_{i1}P_1+D_{i2}P_2=(k_{i1}+t_1H_0(ID_i,K_i,U_i))P_1+(k_{i2}+t_2H_0(ID_i,K_i,U_i))P_2\\&=k_{i1}P_1+k_{i2}P_2+H_0(ID_i,K_i,U_i)(t_1P_1+t_2P_2)\\&=K_i+H_0(ID_i,K_i,U_i)P_m\end{aligned} \tag{10}$$

② 解密算法的正确性

$$\begin{aligned}V_B&=(u_{B1}+wD_{B1})T_1+(u_{B2}+wD_{B2})T_2,\\&=a(u_{B1}P_1+wD_{B1}P_1)+a(u_{B2}P_2+wD_{B2}P_2)\\&=a(u_{B1}P_1+u_{B2}P_2)+aw(D_{B1}P_1+D_{B2}P_2)\\&=a(U_B+w(K_B+h_BP_m))=V_A\end{aligned} \tag{11}$$

③验证算法的正确性

$$\begin{aligned}&\hat{e}(s_1,P_1)\ \hat{e}(s_2,P_2)\\&=\hat{e}(T_1+h(wD_{A1}+u_{A1}h_A),P_1)\hat{e}(T_2+h(wD_{A2}+u_{A2}h_A),P_2)\\&=\hat{e}(P_1,T_1)\ \hat{e}(h(wD_{A1}+u_{A1}h_A),P_1)\hat{e}(P_2,T_2)\ \hat{e}(h(wD_{A2}+u_{A2}h_A),P_2)\\&=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,(wD_{A1}+u_{A1}h_A)P_1)\ \hat{e}(h,(wD_{A2}+u_{A2}h_A)P_2)\\&=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,(wD_{A1}P_1+wD_{A2}P_2)+(u_{A1}h_AP_1+u_{A2}h_AP_2))\\&=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,w(K_A+h_AP_m)+h_AU_A)\\&=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,wK_A+h_A(wP_m+U_A))\end{aligned} \tag{12}$$

5 安全性分析

定理 1 敌手 A_I 攻击下的机密性

假设敌手 A_I 能够赢得游戏 1，则存在多项式时间算法 Ch 能够解决 DDH 问题。所提方案在适应性选择密文攻击及密钥泄露（密钥泄露参数满足 $\delta\leqslant \mathrm{lb}q-L(m)-2\mathrm{lb}\left(\frac{1}{\vartheta}\right)$）攻击下满足机密性。并且敌手赢得游戏的优势满足

$$Adv_{\text{KL-CCA2}}^{\Psi,A_I}\leqslant\frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}}+\frac{2^{\delta}q_D}{q-q_D+1} \tag{13}$$

证明　游戏开始时，算法 Ch 以（T_1,T_2,P_1,P_2）作为输入，选择随机整数 $t_1,t_2\in Z_q^*$作为系统主密钥（秘密保存），计算 $P_m= t_1P_1+t_2P_2$ 作为系统公钥，将公开参数$(G,G_T,q,P_m,P_1,P_2,H_0,H_1,H_2)$传递给 A_{I}。Ch 在游戏过程中需要维持 5 个列表：L_{H_0}、L_{H_1}、L_{H_2}、L_{PK}、L_{SK}，初始为空。

询问阶段：Ch 对 A_{I}的询问作如下回复。

H_0-散列询问：若 A_{I}执行对 ID_j的 H_0-散列询问，在 L_{H_0}查找（ID_j，K_j，U_j，h_j），若存在，返回 h_j的值；否则 Ch 随机选择 h_j，将（ID_j，K_j，U_j，h_j）加入 L_{H_0}，并将 h_j作为应答。

H_1-散列询问：若 A_{I}执行对（T_1,T_2,U_j,ID_j,m,K_j）的 H_1-散列询问，在 L_{H_1}中查找 $(T_1,T_2,U_j,ID_j,m,K_j,\theta_j)$，若存在，返回 θ_j的值；否则 Ch 随机选择 $\theta_j\in Z_q^*$，将 $(T_1,T_2,U_j,ID_j,m,K_j,\theta_j)$ 加入 L_{H_1}，并将 θ_j作为应答。

H_2-Hash 询问：若 A_{I}执行对(T_1,T_2,S)的 H_2-散列询问，在 L_{H_2}中查找 (T_1,T_2,S,τ)，若存在，返回 τ 的值。否则 Ch 随机选择整数 $\tau\in Z_q^*$，把 (T_1,T_2,S,τ) 加入 L_{H_2}，并将 τ 发送给 A_{I}。

提取公钥询问：Ch 接收到 A_{I}提出的公钥提取询问后，执行以下步骤：查找 L_{PK}，若（ID_j，U_j，K_j，c_j）存在，则将 $PK_j=(U_j,K_j)$发送给 A_{I}；否则，Ch 随机选择 $c_j\in\{0,1\}$,令 $\Pr[c_j=1]=\varsigma$。若 $c_j=0$，Ch 随机选择 u_{j1}，u_{j2}，D_{j1}，D_{j2}，$h_j\in Z_q^*$，计算 $U_j=u_{j1}P_1+u_{j2}P_2$，$K_j=D_{j1}P_1+D_{j2}P_2-h_jP_{sys}$，然后将（$ID_j$，$U_j$，$K_j$，$c_j$）加入 L_{PK}，将（ID_j，u_{j1}，u_{j2}，D_{j1}，D_{j2}）添加到 L_{SK}，将（ID_j，K_j，U_j，h_j）添加到 L_{H_0}，并将 $PK_j=(U_j,K_j)$发送给 A_{I}。若 $c_j=1$，Ch 选择随机数 u_{j1}，u_{j2}，k_{j1}，k_{j2}，$h_j\in Z_q^*$，计算 $U_j=u_{j1}P_1+u_{j2}P_2$，$K_j=k_{j1}P_1+k_{j2}P_2$，将（ID_j，U_j，K_j，c_j）添加到 L_{PK}，将（ID_j，K_j，U_j，h_j）添加到 L_{H_0}，并将 $PK_j=(U_j,K_j)$发送给 A_{I}。

提取私钥询问：查找 L_{SK}，若（ID_j，u_{j1}，u_{j2}，D_{j1}，D_{j2}）存在，返回 $SK_j=(u_{j1},u_{j2},D_{j1},D_{j2})$给 A_{I}；否则，Ch 对 ID_j 进行提取公钥询问，得到（ID_j，U_j，K_j，c_j）：①若 $c_j=0$，Ch 在 L_{SK}中搜索（ID_j，u_{j1}，u_{j2}，D_{j1}，D_{j2}），并将 $SK_j=(u_{j1},u_{j2},D_{j1},D_{j2})$返回给 A_{I}。②若 $c_j=1$，Ch 停止游戏并输出拒绝。

公钥替换询问：当 Ch 收到 A_{I}提供的公钥 (ID_j,U_j',K_j')，首先在 L_{PK}中搜索，然后用 (ID_j,U_j',K_j',c_j)替换（ID_j，U_j，K_j，c_j）。

签密询问：A_{I}执行对(m,ID_s,ID_r)的签密询问，Ch 在 L_{PK}中查询（ID_s，U_s，K_s，c_s），分 2 种情况进行回复：①$c_s=1$，Ch 停止游戏并输出拒绝；②$c_s=0$，Ch 分别查找 L_{SK}和 L_{PK}得到 SK_s及 PK_r，利用签密算法计算得到密文 $\sigma=(s_1,s_2,T_1,T_2,C,S)$。

解签密询问：A_{I}提出对(σ,ID_s,ID_r)的解签密询问，Ch 在 L_{PK}中搜索（ID_r，U_r，K_r，c_r），进而执行以下步骤：①若 L_{PK}中存在（ID_s，U_s，K_s，c_s）且 $c_r=1$，Ch 停止游戏并输出拒绝；②若 L_{PK}中存在（ID_s，U_s，K_s，c_s）且 $c_r=0$，Ch 在 L_{PK}中搜索 PK_s，在 L_{SK}中搜索 SK_r,计算 $w=H_2(T_1,T_2,S)$，$V_r=(u_{r1}+wD_{r1})T_1+(u_{r2}+wD_{r2})T_2$，$\mathrm{Ext}(V_r,S)\oplus C=m\|ID_s$；计算 $h=H_1(T_1,T_2,U_s,ID_s,m,K_s)$，验证以下等式是否成立：$\hat{e}(s_1,P_1)\ \hat{e}(s_2,P_2)=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,wK_s+h_s(wP_m+U_s))$，若成立，将 m 发送 A_{I}；否则回复“拒绝”；③若 L_{PK}中不存在（ID_s，U_s，K_s，c_s），Ch 在 L_{PK}中搜索 (ID_s,U_s',K_s',c_s)，进而在 L_{H_1}中搜索 $(T_1,T_2,U_s',ID_s,m,K_s',\theta_s)$，并将 m 传给 A_{I}。

挑战：A_{I}输出 2 个等长的消息 m_0和 m_1，签密用户的身份 ID_s和接收者的身份 ID_r，Ch 在 L_{PK}中搜索（ID_s，U_s，K_s，c_s）和（ID_r，U_r，K_r，c_r），随机选择种子 $S\in\{0,1\}^s$，$s_1,s_2\in G$，$z\in\{0,1\}$，计算 $w=H_2(T_1,T_2,S)$，$h=H_1(T_1,T_2,X_s,ID_s,m_z,K_s)$，使得 $\hat{e}(s_1,P_1)\ \hat{e}(s_2,P_2)=\hat{e}(P_1,T_1)\ \hat{e}(P_2,T_2)\ \hat{e}(h,wK_s+h_s(wP_m+U_s))$ 成立，选择 $V_s\in G$，$C=Ext(V_s,S)\oplus(m_z\|ID_s)$，将 $\sigma=(s_1,s_2,T_1,T_2,C,S)$ 返回给 A_{I}。

A_{I}经过执行类似于第一阶段中的询问后（但不能询问 ID_r 的私钥，也不能对 $\sigma=(s_1,s_2,T_1,T_2,C,S)$ 进行解签密询问，输出 z'作为对 z 的猜测，若 $z'=z$，Ch 输出 1，否则 Ch 输出 0。

下面对实例（T_1,T_2,P_1,P_2）进行分析。

1) 若 $\log_{P_1}T_1=\log_{P_2}T_2$，则有 $T_1=aP_1$，$T_2=aP_2$，显然有 $V_r=(u_{r1}+wD_{r1})T_1+(u_{r2}+wD_{r2})T_2=a(U_r+w(K_r+h_rP_m))=V_s$ 成立。由此可见 A_{I}在上述与 Ch 交互的游戏中没有获得有价值的信息。

$\log_{P_1}T_1\neq\log_{P_2}T_2$，则可以证明以下结论

$$P_r[z'=z]\leqslant\frac{1}{2}+\frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}}+\frac{2^{\delta}q_D}{q-q_D+1}\qquad(14)$$

首先给出以下定义。

定义 11　如果 $\log_{P_1}T_1'\neq\log_{P_2}T_2'$，则称 $\sigma'=(s_1',$

$s_2', T_1', T_2', C', S')$ 是一个无效的签密密文，否则为有效的签密密文。

结论 1 $P_r(accept) \leqslant \frac{2^\delta q_D}{q-q_D+1}$，其中，$P_r(accept)$ 是解密预言机在询问过程中接受所有无效签密密文的概率，q_D 是 A_I 执行解签密询问的次数。

证明 设 $\sigma' = (s_1', s_2', T_1', T_2', C', S') \neq (s_1, s_2, T_1, T_2, C, S)$ 是 A_I 向预言机提出的第一条无效密文，其中 $T_1' = a_1' P_1$，$T_2' = a_2' P_2$，$a_1' \neq a_2'$。对于攻击者 A_I 来说，若不考虑密钥泄露问题，掌握的信息仅包括 $(G, G_T, q, P_m, P_1, P_2, H_0, H_1, H_2, U_r, K_r)$，私钥 $(u_{r1}, u_{r2}, D_{r1}, D_{r2})$ 是未知的，考虑如下方程组

$$\begin{cases} \log_{P_1} U_r = u_{r1} + \beta u_{r2} \\ \log_{P_1}(K_r + h_r P_m) = D_{r1} + \beta D_{r2} \\ \log_{P_1}((u_{r1} + wD_{r1})T_1 + (u_{r2} + wD_{r2})T_2) \\ = a_1 u_{r1} + \beta a_2 u_{r2} + w a_1 D_{r1} + \beta w a_2 D_{r2} \\ \log_{P_1}((u_{r1} + w'D_{r1})T_1' + (u_{r2} + w'D_{r2})T_2') \\ = a_1' u_{r1} + \beta a_2' u_{r2} + w' a_1' D_{r1} + \beta w' a_2' D_{r2} \end{cases} \tag{15}$$

其中，$\log_{P_1} P_2 = \beta$。

式(15)的系数矩阵是

$$\begin{vmatrix} 1 & \beta & 0 & 0 \\ 0 & 0 & 1 & \beta \\ a_1 & \beta a_2 & w a_1 & \beta w a_2 \\ a_1' & \beta a_2' & w' a_1' & \beta w' a_2' \end{vmatrix} =$$

$$\beta^2 (a_1 - a_2)(a_1' - a_2')(w - w') \neq 0 \tag{16}$$

由此，A_I 可以利用式(15)计算私钥 $(u_{r1}, u_{r2}, D_{r1}, D_{r2})$ 的值。考虑到密钥泄露问题，敌手至多获得 δ 比特的密钥信息，泄露值 *leak* 至多有 2^δ 可能值，由引理 1 可得

$$\tilde{H}_\infty((u_{r1}, u_{r2}, D_{r1}, D_{r2}) | PK_r, leak) \geqslant$$
$$\tilde{H}_\infty((u_{r1}, u_{r2}, D_{r1}, D_{r2}) | PK_r) - \delta \geqslant \mathrm{lb}q - \delta \tag{17}$$

由平均最小熵的定义，可知 A_I 获得用户私钥 $(u_{r1}, u_{r2}, D_{r1}, D_{r2})$ 的概率至多为 $\frac{2^\delta}{q}$，由此 A_I 利用式(15)求得私钥 $(u_{r1}, u_{r2}, D_{r1}, D_{r2})$ 的概率至多为 $\frac{2^\delta}{q}$，也即解密预言机接受首个无效密文的概率至多为 $\frac{2^\delta}{q}$。以此类推，可知解密预言机接受第 i 条无效密文的概率是 $\frac{2^\delta}{q-(i-1)}$。因此，有

$$P_r(accept) \leqslant \frac{2^\delta}{q} + \frac{2^\delta}{q-1} + \cdots \frac{2^\delta}{q-q_D+1} \leqslant \frac{2^\delta q_D}{q-q_D+1} \tag{18}$$

结论 2 $\Pr[z' = z \,|\, reject] \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}}$，其中，*reject* 代表解密预言机拒绝无效密文的事件。

证明 假设 *Ch* 拒绝所有无效密文。由引理 1 可得

$$\begin{aligned} &\tilde{H}_\infty((u_{r1} + wD_{r1})T_1 + (u_{r2} + wD_{r2})T_2 | PK_r, \sigma, \rho, leak) \\ &\geqslant \tilde{H}_\infty((u_{r1} + wD_{r1})T_1 + (u_{r2} + wD_{r2})T_2 | PK_r, \sigma, \rho) - \delta \\ &\geqslant \mathrm{lb}q - \delta \end{aligned} \tag{19}$$

故有 $2^{-\tilde{H}_\infty((u_{r1}+wD_{r1})T_1 + (u_{r2}+wD_{r2})T_2 | PK_r, \sigma, \rho, leak)} \leqslant \frac{2^\delta}{q}$。

根据引理 2，在泄露信息的帮助下 A_I 输出 $m_{z'} \| ID_s = \mathrm{Ext}((u_{r1}+wD_{r1})T_1 + (u_{r2}+wD_{r2})T_2, S) \oplus C$ 的概率至多为 $\frac{1}{2}\sqrt{2^m \cdot \frac{2^\delta}{q}} = \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}}$，而在不考虑泄露信息的情况下，敌手 A_I 猜测出正确 $z'=z$ 的概率为 $\frac{1}{2}$，由此 $\Pr[z' = z \,|\, reject] \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}}$。

综合结论 1 和结论 2，得到 $\Pr[z' = z] \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}} + \frac{2^\delta q_D}{q-q_D+1}$，由此可得 $Adv^{\Psi, A_I}_{\text{KL-CCA2}} = |\Pr[z' = z] - \frac{1}{2}| \leqslant \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}} + \frac{2^\delta q_D}{q-q_D+1}$，定理 1 的结论成立。

定理 2 A_II 敌手攻击下的机密性

假设敌手 A_II 能够赢得游戏 2，则存在多项式时间算法 *Ch* 能够解决 DDH 问题。所提方案在适应性选择密文攻击及密钥泄露（密钥泄露参数满足 $\delta \leqslant \mathrm{lb}q - L(m) - 2\mathrm{lb}\left(\frac{1}{\vartheta}\right)$）攻击下满足机密性。并且敌手赢得游戏的优势满足

$$Adv^{\Psi, A_\mathrm{II}}_{\text{KL-CCA2}} \leqslant \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}} + \frac{2^\delta q_D}{q-q_D+1} \tag{20}$$

证明 A_II 执行除替换公钥询问之外的各种询问，且能获知 P_m，进而能得到用户的部分私钥。挑战阶段和猜测阶段与定理 1 类同。

通过类似于定理 1 中的分析，可以得到以下结论

$$Adv^{\Psi, A_\mathrm{II}}_{\text{KL-CCA2}} \leqslant \frac{1}{2}\sqrt{\frac{2^{m+\delta}}{q}} + \frac{2^\delta q_D}{q-q_D+1} \tag{21}$$

定理 3　A_{I}敌手攻击下的不可伪造性

假设 A_{I}能够赢得游戏 3，则存在多项式时间算法 *Ch* 能够解决 DDH 问题。所提方案在适应性选择消息攻击及密钥泄露（密钥泄露参数满足 $\delta \leqslant \log q - L(m) - 2\log\left(\frac{1}{\vartheta}\right)$）攻击下满足不可伪造性。并且敌手赢得游戏的优势满足

$$Adv_{\text{KL-CMA}}^{\Psi,A_I} \leqslant \left|\frac{(2^{\delta+1}+1)q_D - q - 1}{2(q-q_D+1)}\right| \tag{22}$$

证明　游戏开始时，算法 *Ch* 以（T_1,T_2,P_1,P_2）作为输入，参数设置及询问过程与定理 1 类似，继而通过以下步骤伪造 ID_s 对消息 m 的签密。

伪造：A_{I} 随机选取 $a',s_1,s_2 \in Z_q^*$，使 $a'P_1 = T_1$，$a'P_2 = T_2$，选择种子 $S \in \{0,1\}^s$，计算 $w=H_2(T_1,T_2,S)$，$V_s' = a'(U_r + w(K_r + h_r P_m))$，计算 C=Ext(V_s' , $S) \oplus (m||ID_s)$，输出签密密文 $\sigma = (s_1,s_2,T_1,T_2,C,S)$，若该签密能顺利通过验证，则 *Ch* 输出 1，否则输出 0。

定义 12　若签密密文 $\sigma' = (s_1',s_2',T_1',T_2',C',S')$ 满足签名验证等式 $\hat{e}(s_1',P_1)\ \hat{e}(s_2',P_2) = \hat{e}(P_1,T_1')\ \hat{e}(P_2,T_2')\ \hat{e}(h',w'K_s + h_s(w'P_m + U_s))$，则称 σ' 为有效签密密文，否则称为无效密文。

设 $\sigma' = (s_1',s_2',T_1',T_2',C',S') \neq (s_1,s_2,T_1,T_2,C,S)$ 是敌手 A_{I} 向解密预言机询问的第一条密文。对于攻击者 A_{I} 来说，若不考虑密钥泄露问题，掌握的信息仅包括($G,G_T,q,P_m,P_1,P_2,H_0,H_1,H_2,U_s,K_s$)，私钥($u_{s1},u_{s2},D_{s1},D_{s2}$)是未知的，考虑如下方程组

$$\begin{cases} \log_{P_1} U_s = u_{s1} + \beta u_{s2} \\ \log_{P_1}(K_s + h_s P_m) = D_{s1} + \beta D_{s2} \\ \log_{P_1} s_1 = a + \xi h_s u_{s1} + \xi w D_{s1} \\ \log_{P_1} s_2' = a' + \xi' h_s u_{s2} + \xi' w' D_{s2} \end{cases} \tag{23}$$

其中，$\log_{P_1} h = \xi$，$\log_{P_1} h' = \xi'$，$\log_{P_1} P_2 = \beta$。

式(23)的系数矩阵为

$$\begin{vmatrix} 1 & \beta & 0 & 0 \\ 0 & 0 & 1 & \beta \\ \xi h_s & 0 & \xi w & 0 \\ 0 & \xi' h_s & 0 & \xi' w' \end{vmatrix} = \beta\xi\xi' h_s (w' - w) \neq 0 \tag{24}$$

考虑密钥泄露问题，A_{I} 使用上述方程计算出($u_{s1},u_{s2},D_{s1},D_{s2}$)的可能性至多为 $\frac{2^\delta}{q}$，由此解签密算法接受第一条签密密文为有效密文的概率最多为 $\frac{2^\delta}{q}$。若解签密算法拒绝了首条签密密文，则攻击者会得到更多关于私钥 SK_s 的信息，进而 A_{I} 提供的第二条密文为有效密文的可能性增至 $\frac{2^\delta}{q-1}$。以此类推，解签密算法接受 A_{I} 提供的第 i 条密文为有效密文的概率至多为 $\frac{2^\delta}{q-i+1}$。因此，A_{I} 提供一条有效密文给 *Ch* 的概率至多为 $\frac{2^\delta q_D}{q-q_D+1}$，故 A_{I} 赢得游戏的优势满足

$$Adv_{KL-CMA}^{\Psi,A_I} \leqslant \left|\frac{2^\delta q_D}{q-q_D+1} - \frac{1}{2}\right| = \left|\frac{(2^{\delta+1}+1)q_D - q - 1}{2(q-q_D+1)}\right| \tag{25}$$

定理 3 得证。

定理 4　A_{II}敌手攻击下的不可伪造性

假设敌手 A_{II} 能够赢得游戏 4，则存在多项式时间算法 *Ch* 能够解决 DDH 问题。所提方案在适应性选择消息攻击及密钥泄露（密钥泄露参数满足 $\eta \leqslant \mathrm{lb}q - L(m) - 2\mathrm{lb}\left(\frac{1}{\vartheta}\right)$）攻击下满足不可伪造性。并且敌手赢得游戏的优势满足

$$Adv_{KL-CMA}^{\Psi,A_{II}} \leqslant \left|\frac{(2^{\delta+1}+1)q_D - q - 1}{2(q-q_D+1)}\right| \tag{26}$$

证明　证明过程与定理 3 类似，恕不赘述。

6　效率对比

本节将对构造的抗泄露无证书签密方案与同类方案的性能进行比较。为便于比较签密方案的计算效率，将椭圆曲线上的标量点乘运算记为 SM，有限乘法群上的指数运算记为 E（1 次指数运算约与 10 次点乘运算花费的时间相当）。双线性对运算记作 BP（512 bit 的 BP 运算时间约为 1 024 bit 的 E 运算时间的 10 倍以上）。散列函数及点加运算所花费的时间远少于 SM 和 E，不计入比较范围。如表 1 所示，可以看出本文方案在签密阶段没有使用双线性对（此阶段对运算效率的要求比解签密阶段要高），解签密阶段使用了 5 个双线性对运算，与文献[8]方案中使用的双线性对数相同，比文献[7,9]方案中使用的双线性对多一个，但本文方案具有抗密钥泄露的安全性能。文献[5,6]中的方案没有使用双线性对，具有较高的运算效率，但是不满足抗泄露性能且被证明存在其他安全问题[18]。文献[16]使用了 NIZK 系

统，且并未给出具体的构造方式，因此无法准确评估其计算效率，参照文献[19,20]中 NIZK 系统的构造方法，均包含多个双线性对运算，因此，本文方案与文献[16]相比具有运算效率方面的优势。

表 1　　计算效率比较

签密方案	签密阶段	解签密阶段	抗泄露性
文献[5]方案	3SM	4SM	No
文献[6]方案	3SM	4SM	No
文献[7]方案	1BP+6E	3BP+4E	No
文献[8]方案	1BP+1E+4SM	4BP+1E+1SM	No
文献[9]方案	2BP+3SM	2BP+2SM	No
文献[16]方案	2SM+C_{NIZK}	2SM+C_{NIZK}	Yes
本文方案	6SM	5BP+5SM	Yes

7　结束语

为抵制实际应用环境中的密钥泄露攻击，本文利用椭圆曲线密码及双线性对构造了一种新的抗泄露无证书签密方案，基于判定 Diffie-Hellman 问题的困难性假设，在随机预言机模型下证明该方案满足适应性选择密文及密钥泄露攻击下的机密性和选择消息及密钥泄露攻击下的存在不可伪造性。该方案没有使用抗泄露密码体制中常用的 NIZK 证明系统，在签密阶段不含双线性对运算，在同等安全强度下与同类方案相比具有较高的运算效率。

参考文献：

[1] ZHENG Y. Digital signcryption or how to achieve(signature & encryption) <<cost(signature)+cost(encryption)[C]//The Crypto'97, 1997: 291-312.

[2] SWAPNA G, REDDY V. An efficient id-based public verifiable signcryption scheme[J]. International Journal of Cryptography and Security, 2013, 3(1): 41-46.

[3] 刘振华, 李娟娟, 俎龙辉. 可撤销的基于身份的签密方案[J].四川大学学报(工程科学版), 2014, 46(2): 79-86.
LIU Z H,LI J J,ZU L H. Revocable ID-based signcryption scheme[J]. Journal of Sichuan University(Engineering Science Edition), 2014, 46(2): 79-86.

[4] ALRIYAMI S, PATERSON K. Certificateless public key cryptography[C]//ASIACRYPT 2003, 2003: 452-473.

[5] 刘文浩, 许春香. 无双线性配对的无证书签密机制[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.

[6] 何德彪. 无证书签密机制的安全性分析[J]. 软件学报, 2013, 24(3): 618-622.
HE D B. Security analysis of a certificateless signcryption scheme[J].Journal of Software, 2013, 24(3): 618-622.

[7] 孙华, 孟坤. 标准模型下可证安全的有效无证书签密方案[J]. 计算机应用, 2013, 33(7): 1846-1850.
SUN H, MENG K. Efficient provably secure certificateless signcryption scheme in standard model[J].Journal of Computer Applications, 2013, 33(7): 1846-1850.

[8] 马陵勇, 卓泽朋, 廉玉忠. 新的无证书签密方案[J]. 吉林师范大学学报(自然科学版), 2014, 3(8): 93-95.
MA L Y, ZHUO Z P, LIAN Y Z. New Certificateless signcryption scheme[J]. Jilin Normal University Journal (Natural Science Edition), 2014, 3(8): 93-95.

[9] 汤鹏志, 张庆兰, 杨俊芳. 一种改进的基于双线对的无证书签密方案[J]. 合肥工业大学学报(自然科学版), 2016, 39(7): 917-923.
TANG P Z, ZHANG Q L, YANG J F. An improved certificateless signcryption scheme based on bilinear pairing[J]. Journal of Hefei University of Technology(Natural Science), 2016, 39(7): 917-923.

[10] AKAVIA A, GOLDWASSER S, VAIKUNTANATHAN V. Simultaneous hardcore bits and cryptography against memory attacks[C]// The Theory of Cryptography Conference. 2009:474-495.

[11] NAOR M, SEGEV G. Public-key cryptosystems resilient to key leakage[J]. Society for Industrial and Applied Mathematics, 2012, 41 (4): 772-814.

[12] LI S J, ZHANG F T, SUN Y X, et al. Efficient leakage-resilient public key encryption from DDH assumption[J]. Cluster Comput, 2013, 16(4) :797-806.

[13] HAO X, YUEN T H, ZHANG C, et al. Leakage-resilient certificateless public key encryption[C]//The First ACM Workshop on Asia Public-key Cryptograph. 2013:13-22.

[14] YU Q H, LI J G, ZHANG Y C, et al. Certificate-based encryption resilient to key leakage[J]. Journal of Systems and Software, 2016, 116(1): 101-112

[15] TANG F, LI H. Joint signature and encryption in the presence of continual leakage[C]//Information Security Applications, LNCS8909, 2014: 269-280.

[16] ZHOU Y W, YANG B, ZHANG W Z. Provably secure and efficient leakage-resilient certificateless signcryption scheme without bilinear pairing[J]. Discrete Applied Mathematics,2016,204(3):185-202.

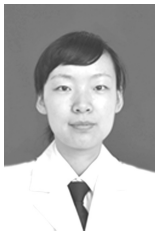
[17] FAONIO A, VENTURI D. Efficient public-key cryptography with bounded leakage and tamper resilience[C]//International Association for Cryptologic Research 2016. 2016: 877-907.

[18] 秦艳琳, 吴晓平. 对一种无证书签密方案的分析与改进[J].计算机应用研究, 2015, 32(11): 3426-3429.
QIN Y L, WU X P. Security analysis and improvement of certificateless signcryption scheme[J]. Application Research of Computers, 2015, 32(11): 3426-3429.

[19] GROTH J, OSTROVSKY R, SAHAI A. Perfect non-interactive zero knowledge for np[C]//EUROCRYPT 2006. 2006: 339-358.

[20] FAONIO A, VENTURI D. Efficient public-key cryptography with bounded leakage and tamper resilience[C]//International Association for Cryptologic research 2016. 2016: 877-907.

作者简介：



秦艳琳（1980-），女，河南安阳人，博士，海军工程大学讲师，主要研究方向为密码学及网络安全。

吴晓平（1961-），男，山西新绛人，海军工程大学教授、博士生导师，主要研究方向为信息安全及系统工程。

胡卫（1979-），男，湖北宜城人，海军工程大学副教授，主要研究方向为网络及信息安全。