签密方案的密文滥用性分析

陈 明* 王 霏

(宜春学院数学与计算机科学学院 宜春 336000)

摘 要：对签密密文的滥用是指恶意的接收者利用收到的密文伪造新的密文，使之具有不同的接收者，现有EUF-CMA(Existential UnForgeability against adaptive Chosen Messages Attack)模型不能有效模拟签密方案的密文滥用性，一些签密方案也不能抵抗对密文的滥用攻击。该文通过对EUF-CMA模型中敌手的能力进行增强，实现了模拟签密密文滥用攻击。以新近提出的几种异构签密方案为例，描述方案中存在的针对签密密文滥用的攻击实例，分析形成攻击的原因，并提出相应的改进方法。最后，以其中一种改进方案作为实例，演示采用增强的EUF-CMA模型分析签密方案密文滥用性的过程，表明该文中针对EUF-CMA模型的增强，以及对签密方案的改进方法是合理和有效的。

关键词：签密；机密性；不可伪造性；密文滥用性；EUF-CMA模型

中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2019)04-1010-07

DOI: 10.11999/JEIT180129

Resistance to Misuse Ciphertext of Signcryption Scheme

CHEN Ming WANG Fei

(*School of Mathematics and Computer Science*, *Yichun University*, *Yichun* 336000, *China*)

Abstract: The misuse of signcryption ciphertext means that the malicious recipient uses the received signcryption ciphertext to forge a new ciphertext that has a different recipient. It is found that the Existential UnForgeability against adaptive Chosen Message Attack (EUF-CMA) model can not simulate misuse attacks on signcryption schemes, and many of the existing signcryption schemes, claimed provable secure, can not resist the misuse attack. By enhancing the capabilities of adversaries in the EUF-CMA model, an extended EUF-CMA model is defined which captures the security associated with the resistance to misuse attacks on signcryption schemes. This paper describes the misuse attack instances in several newly proposed heterogeneous signcryption schemes, analyzes the reasons for the attacks and proposes improvement approaches. Finally, using the enhanced EUF-CMA model, the unforgeability of an improved heterogeneous signcryption scheme is analyzed, and the procedure of simulating the misuse attack is demonstrated. The results indicate that the enhanced EUF-CMA model and the improvement approaches for signcryption schemes are reasonable and effective.

Key words: Signcryption; Confidentiality; Unforgeability; Ciphertext misuse; Existential UnForgeability against adaptive Chosen Message Attack (EUF-CMA) model

1 引言

签密[1](signcryption)能同时实现消息传输的机密性和认证性，且计算开销小于加密加签名算法的总和，在网络传输中有着广泛的应用，成为近年来的研究热点。随着网络应用的飞速发展，许多网络系统采用不同的密码结构，例如传统的基于PKI的密码结构(Traditional Public Key Cryptography, TPKC)、基于身份的密码结构(IDentity-based Public Key Cryptography, IDPKC)、无证书的密码结构(CertificateLess Public Key Cryptography, CLPKC)等等。如何实现密码异构系统之间消息传输的机密性和不可伪造性，是一个值得研究的问题。

2010年，Sun等人[2]首次提出异构密码环境下的签密方案，构造了从TPKC到IDPKC的异构签

收稿日期：2018-01-30；改回日期：2019-01-28；网络出版：2019-02-20
*通信作者： 陈明 chenming9824@aliyun.com
基金项目：国家自然科学基金(61662083)，江西省教育厅科学技术研究项目(GJJ151040, GJJ161042, GJJ161677)

Foundation Items: The National Natural Science Foundation of China (61662083), The Science & Technology Research Project of Educational Commission of Jiangxi Province (GJJ151040, GJJ161042, GJJ161677)

密方案。随后，多种异构环境下的签密方案被分别提出来[3–11]，包括IDPKC→TPKC签密、IDKC→CLPKC签密以及TPKC-IDPKC双向签密方案等等。虽然已有多种异构签密方案被提出，但这一机制仍然是一种相对较新的密码原语，方案本身及其安全模型仍未得到充分研究，部分方案已被指出存在安全缺陷。

从签密的安全模型研究来看，目前主要的文献采用了IND-CCA2(INDistinguishability against adaptive Chosen Ciphertext Attack)模型和EUF-CMA(Existential UnForgeability against adaptive Chosen Messages Attack)模型分别模拟签密方案的机密性和不可伪造性[12]。但是，部分现有方案尽管在IND-CCA2模型和EUF-CMA模型下被证明满足安全性，仍然存在严重的安全缺陷。例如，本文分析发现，文献[5,9,11]中提出的几种异构签密方案就存在安全缺陷(虽然文献[5,9,11]中都分别采用上述安全模型证明了所提出的签密方案的安全性)，恶意的接收者能利用收到的签密密文伪造新的密文(具有不同的接收者)，本文把这一安全缺陷称为消息接收者对签密密文的滥用，详细分析见本文第3节和第4节。防止对签密密文的滥用在某些应用中非常重要，例如数字版权应用。假设这样一种场景：数字资源m的提供者Alice向其购买者Bob发送了一份对m的签密密文σ，其中，Alice对m的签名表明Alice对Bob的授权，但是注意，Alice仅授权Bob个人使用m，并未授权Bob向第三方传播，随后，Bob利用σ伪造新的密文σ'发送给Charley，并收取一定费用。在这一场景中，由于签密方案不能保证签密密文不被滥用，若出现版权纠纷，Charley可以向仲裁机构证明σ'是由Alice签名的合法签密密文而免于被惩处，从而导致Alice的利益受到了侵害。由以上分析可见，签密方案的安全模型还需要进一步研究，这是本文研究的出发点。

文献[12]重点讨论了签密方案的机密性，对IND-CCA2模型中敌手的攻击能力进行了泛化，建议在签密方案中采用泛化的gCCA2(generalized CCA2)攻击模型。本文则主要研究签密方案的不可伪造性。以文献[5,9,11]中提出的几种异构签密方案为例(详见本文第4节)，描述了恶意的接收者如何利用发送者所产生的签密密文构造对同一消息的新的签密密文，新的密文与原密文具有相同的发送者和不同的接收者。事实上，本文虽然以异构签密方案为例，但是一般签密方案也存在类似情形，例如文献[13]中提出的方案也存在相同攻击等等。根据这一攻击场景，本文定义了签密密文滥用性。进一步，本文对EUF-CMA模型进行了增强(详见本文第3节)，使之能模拟签密密文滥用性。最后，针对文献[5,9,11]中几种方案的安全缺陷，本文提出了改进方法，并采用增强的安全模型对改进方案的签密密文滥用性进行了分析。

2　困难问题及假设

这里简要描述与本文相关的数学困难问题及假设，详细内容请参考文献[14,15]。

双线性映射：给定素阶为q的加法循环群G_1和乘法循环群G_2，P是G_1的一个生成元，如果$e: G_1\times G_1\to G_2$是从G_1到G_2的一个有效的双线性映射，那么满足：

(1) 双线性：给定$U,\ V\in G_1$和任意$a,\ b\in\mathbb{Z}_q$，满足$e(aU,\ bV)=e(U,\ V)^{ab}$；

(2) 非退化性：$e(P,\ P)\neq 1$；

(3) 可计算性：任意的$U,\ V\in G_1$，存在多项式时间算法能成功计算$e(U,\ V)$。

CDH(Computational Diffie-Hellman)问题：对任意未知的$a,\ b\in\mathbb{Z}_q$，给定$(aP,\ bP)\in {G_1}^2$，计算abP。

CDH假设：不存在多项式时间算法能成功求解CDH问题。

BDH(Bilinear Diffie-Hellman)问题：对任意未知的$a,\ b,\ c\in\mathbb{Z}_q$，给定$(aP,\ bP,\ cP)\in {G_1}^3$，计算$e(P,\ P)^{abc}$。

BDH假设：不存在多项式时间算法能成功求解BDH问题。

***n*-SDH(Strong Diffie-Hellman)问题**：给定随机的$\alpha\in\mathbb{Z}_q$和$(P,\alpha P,\alpha^2 P,\cdots,\alpha^n P)\in G_1^{n+1}$，计算输出一对值$(w,\ (1/(w+\alpha))\ P)$。其中，$w\in\mathbb{Z}_q$。

***n*-SDH假设**：不存在多项式时间算法能成功求解n-SDH问题。

3　签密方案安全模型分析

签密方案(包括异构签密方案)实现的主要安全属性包括消息传输的机密性和不可伪造性。

目前，大量文献采用了标准签名的EUF-CMA模型分析签密方案的不可伪造性。但是，签密方案与标准签名方案存在明显不同：标准签名方案一般不指定消息及签名的接收者，而签密方案则明确地指定了消息及签名的接收者，而且可能有多个接收者，例如多接收者签密方案。因此，采用标准签名的EUF-CMA模型不能完全模拟签密方案的不可伪造性。对文献[5,9,11]的分析发现，尽管采用EUF-CMA模型证明了签密方案满足不可伪造性，仍然存在签密的接收者伪造发送者对同一消息的新的签

密密文(具有不同的接收者，详见第4节)，本文把这一安全缺陷称为接收者对签密密文的滥用，定义签密密文滥用性来刻画这一安全属性。为了模拟签密密文滥用性，以基于身份的EUF-CMA(记为ID-EUF-CMA)模型为例，本文对ID-EUF-CMA模型进行增强，记为eID-EUF-CMA模型，具体定义如下。

eID-EUF-CMA模型 eID-EUF-CMA模型定义为模拟器C和敌手A之间的游戏，分为初始化、询问和挑战3个阶段，具体定义如下。

初始化：C运行系统建立算法产生系统公开参数，并将参数发送给A。

询问：A自适应地发起多项式时间有界的如下询问，C模拟签密方案的相应算法对A的询问进行应答。

(1) 密钥询问：A提交用户身份ID_u, C输出ID_u的长期私钥。

(2) 签密询问：A输入$(\mathrm{ID}_s, \mathrm{ID}_r, m)$, C输出签密密文$\delta$。其中，$\mathrm{ID}_s$为发送者身份，$\mathrm{ID}_r$为接收者身份，$m$为待签密消息。

(3) 解签密询问：A输入$(\mathrm{ID}_s, \mathrm{ID}_r, \delta)$，如果验证签密密文有效，则输出明文$m$，否则返回$\perp$。

挑战：询问阶段结束以后，A输出关于发送者ID_s^*、接收者ID_r^*、以及明文m^*的一个签密密文δ^*。

如果验证δ^*为$(\mathrm{ID}_s^*, \mathrm{ID}_r^*, m^*)$的一个有效签密密文，且满足如下条件，那么A赢得游戏。

(1) A未提交ID_s^*的密钥询问；

(2) A未提交$(\mathrm{ID}_s^*, \mathrm{ID}_r^*, m^*)$的签密询问。

定义1 签密密文不可滥用性：如果A赢得游戏的优势$\mathrm{Adv}_{\mathrm{A}}$是可忽略的，那么签密方案满足签密密文不可滥用性。

与现有的一些用于分析签密方案的EUF-CMA模型(例如文献[9,11,12])比较，本文模型对敌手A的能力进行了增强：允许A提交消息$(\mathrm{ID}_s^*, \mathrm{ID}'_r, m^*)$的签密询问。其中，$\mathrm{ID}'_r$为任意不等于$\mathrm{ID}_r^*$的用户身份。

对敌手A的这一增强，能模拟恶意的接收者对签密密文滥用这一攻击场景。具体来说，A模拟恶意的接收者ID'_r，通过$(\mathrm{ID}_s^*, \mathrm{ID}'_r, m^*)$签密询问，获取$\mathrm{ID}_s^* \to \mathrm{ID}'_r$的密文$\delta'$，然后将$\delta'$转化为$\mathrm{ID}_s^* \to \mathrm{ID}_r^*$的密文$\delta^*$。

4 两种异构签密方案的密文滥用性分析与改进

4.1 ZYL异构签密方案滥用性分析与改进

4.1.1 ZYL异构签密方案

最近，张玉磊等人[9]提出一种IDPKC→CLPKC异构签密方案，记为ZYL异构签密方案，由：系统建立、密钥生成、密钥提取、签密和解签密5个算法组成，简要叙述如下。

(1) 系统建立算法：系统建立算法分为两个部分，在IDPKC和CLPKC环境下的密钥生成中心(Private Key Generator, PKG)分别运行系统建立算法为各自的密码系统生成公开参数以及PKG主密钥。

在IDPKC环境下，密钥生成中心PKG_1输入安全参数κ，输出系统公开参数$\mathrm{pa}_{\mathrm{ID}} = \{G_{1-1}, G_{1-2}, q_1, g, P_1, P_{\mathrm{pub}_1}, e_1, H_{1-1}, H_{1-2}\}$。其中，$G_{1\text{-}1}$为$q_1$阶循环加法群，$G_{1\text{-}2}$为$q_1$阶循环乘法群，$P_1 \in G_{1\text{-}1}$为$G_{1\text{-}1}$的一个生成元，$e_1$: $G_{1\text{-}1} \times G_{1\text{-}1} \to G_{1\text{-}2}$为满足本文第2节定义的双线性映射，$g = e_1(P_1, P_1)$，$P_{\mathrm{pub}_1} = s_1 P_1$为$\mathrm{PKG}_1$的公钥，$s_1 \in \mathbb{Z}_{q_1}$为$\mathrm{PKG}_1$的主密钥，$H_{1\text{-}1}$: $\{0,1\}^* \to \mathbb{Z}_{q_1}$和$H_{1\text{-}2}$: $\{0,1\}^* \times G_{1\text{-}2} \to \mathbb{Z}_{q_1}$为安全密码Hash函数。

在CLPKC环境下，PKG_2输入安全参数κ，输出公开参数$\mathrm{pa}_{\mathrm{CL}} = \{G_{2-1}, G_{2-2}, q_2, l_m, l_{\mathrm{ID}}, P_2, P_{\mathrm{pub}_2}, H_{2-1}, H_{2-2}\}$。其中，$G_{2\text{-}1}$为$q_2$阶循环加法群，$G_{2\text{-}2}$为同阶循环乘法群，$P_2 \in G_{2\text{-}1}$为$G_{2\text{-}1}$的一个生成元，$e_2$: $G_{2\text{-}1} \times G_{2\text{-}1} \to G_{2\text{-}2}$为双线性映射，$P_{\mathrm{pub}_2} = s_2 P_2$为$\mathrm{PKG}_2$公钥，$s_2 \in \mathbb{Z}_{q_2}$为$\mathrm{PKG}_2$的主密钥，$H_{2\text{-}1}$: $\{0,1\}^* \to G_{2\text{-}1}$和$H_{2\text{-}2}$: $\{0,1\}^* \to \{0,1\}^{l_{G_{2-1}}+l_{\mathrm{ID}}+l_m}$为安全密码Hash函数。其中，$l_m$为待加密消息长度，$l_{\mathrm{ID}}$为身份标识长度。

(2) 密钥生成算法：在IDPKC环境下，用户提交身份ID_{A}给PKG_1。PKG_1为ID_{A}生成私钥$S_{\mathrm{A}} = (1/(Q_{\mathrm{A}} + s_1))P_1$，通过安全信道将$S_{\mathrm{A}}$发回给$\mathrm{ID}_{\mathrm{A}}$。其中，$Q_{\mathrm{A}} = H_{1\text{-}1}(\mathrm{ID}_{\mathrm{A}})$。

(3) 密钥提取算法：在CLPKC环境下，用户提交身份ID_{B}给PKG_2。PKG_2为ID_{B}生成私钥$D_{\mathrm{B}} = s_2 Q_{\mathrm{B}}$，通过安全信道将$D_{\mathrm{B}}$发回给$\mathrm{ID}_{\mathrm{B}}$。其中，$Q_{\mathrm{B}} = H_{2\text{-}1}(\mathrm{ID}_{\mathrm{B}})$。$\mathrm{ID}_{\mathrm{B}}$随机选择$x_{\mathrm{B}} \in \mathbb{Z}_{q_2}$，计算无证书公钥$\mathrm{PK}_{\mathrm{B}} = x_{\mathrm{B}} P_2$，然后设置私钥$\mathrm{SK}_{\mathrm{B}} = (D_{\mathrm{B}}, x_{\mathrm{B}})$。

(4) 签密算法：发送者Alice(身份为ID_{A})发送消息m给Bob(身份为ID_{B})，执行以下步骤：

步骤 1 随机选择$r_1 \in \mathbb{Z}_{q_1}$, $r_2 \in \mathbb{Z}_{q_2}$，计算$R_1 = g^{r_1}$, $R_2 = r_2 P_2$；

步骤 2 计算$U = e_2(P_{\mathrm{pub}_2}, Q_{\mathrm{B}})^{r_2}$, $V = r_2 \mathrm{PK}_{\mathrm{B}}$；

步骤 3 计算$c = (m \| R_1 \| \mathrm{ID}_{\mathrm{A}}) \oplus H_{2-2}(U, V, R_2)$，其中，“$X \| Y$”表示消息$X$与消息$Y$联接；

步骤 4 计算$h = H_{1\text{-}2}(m, R_1)$, $W = (r_1 + h)S_{\mathrm{A}}$，则签密密文为$\delta = (c, R_2, W)$。

(5) 解签密算法：Bob收到密文(c, R_2, W)后，按以下步骤执行：

步骤 1 计算$U' = e_2(R_2, D_{\mathrm{B}})$, $V' = x_{\mathrm{B}} R_2$；

步骤 2　解密$(m\|R_1\|\mathrm{ID_A})=c\oplus H_{2-2}(U', V', R_2)$，然后计算$h=H_{1\text{-}2}(m, R_1)$, $Q_\mathrm{A}=H_{1\text{-}1}(\mathrm{ID_A})$；

步骤 3　验证等式$R_1=e_1(W, P_{\mathrm{pub}_1}+Q_\mathrm{A}P_1)g^{-h}$是否成立，若等式成立则接受签密并输出明文$m$，否则输出$\perp$。

上述签密方案的正确性验证请参考文献[9]，本文不再赘述。

4.1.2 ZYL方案密文滥用性分析

尽管张玉磊等人[9]分析并证明了ZYL异构签密方案具有消息传输的机密性和不可伪造性，但是本文分析发现，方案中的接收者Bob存在滥用签密消息的可能，形成新的攻击，具体描述如下。

假设恶意的Bob收到诚实的发送者Alice发送给他的签密密文(c, R_2, W), Bob首先按照本文4.1.1节中(5)解签密算法的步骤1和步骤2解密获得$(m||R_1||\mathrm{ID_A})$，然后任意选择CLPKC系统中的其它用户Charley(假设Charley的身份为$\mathrm{ID_C}$，无证书公钥为$\mathrm{PK_C}=x_\mathrm{C}P_2$)，接着按如下步骤生成新的签密：

步骤 1　随机选择$r_2^*\in\mathbb{Z}_{q_2}$，计算$R_2^*=r_2^*P_2$；

步骤 2　计算$Q_\mathrm{C}=H_{2\text{-}1}(\mathrm{ID_C})$, $U^*=e_2(P_{\mathrm{pub}_2}, Q_\mathrm{C})^{r_2^*}$, $V^*=r_2^*\mathrm{PK_C}$；

步骤 3　计算$c^*=(m\|R_1\|\mathrm{ID_A})\oplus H_{2-2}(U^*, V^*, R_2^*)$，并将新的签密密文$\delta^*=(c^*, R_2^*, W)$发送给Charley。

Charley收到(c^*, R_2^*, W)后，按照本文4.1.1节中(5)解签密算法的步骤1和步骤2解密获得$(m||R_1||\mathrm{ID_A})$，并且按照解签密算法的步骤3验证Alice的签名。由于(m, R_1, W)均由Alice产生，Bob并未修改其中的任何值，因此可以验证等式$R_1=e_1(W, P_{\mathrm{pub}_1}+Q_\mathrm{A}P_1)g^{-h}$成立。从Charley的视角来看，$(c^*, R_2^*, W)$是Alice发送给他的一个有效的签密密文，攻击成立。

4.1.3 ZYL方案改进

针对4.1.2节中描述的攻击场景，本文对ZYL方案进行改进。改进方案分为两步：第1步，在4.1.1节(1)系统建立算法中将Hash函数$H_{1\text{-}2}$扩展为$H_{1\text{-}2}{}^*$: $\{0,1\}^{l_\mathrm{ID}}\times\{0,1\}^{l_c}\times\{0,1\}^{l_m}\times G_{1\text{-}2}\to\mathbb{Z}_{q_1}$；第2步，在4.1.1节(4)签密算法步骤4中计算$h=H_{1\text{-}2}{}^*(\mathrm{ID_B}, c, m, R_1)$。其中，$l_\mathrm{ID}$和$l_m$与4.1.1节相同，$l_c$为密文$c$的长度。

通过上述改进，将Alice的签名与接收者身份$\mathrm{ID_B}$和发送的密文c进行绑定，对这两者的任意篡改都会影响签名结果，导致签名无效，从而防止上述攻击事件的发生。

4.2 LJW异构签密及其改进方案的滥用性分析与改进

在文献[5]中，刘景伟等人提出一种PKI-CLC异构系统下的双向签密方案，记为LJW异构签密方案。随后，张玉磊等人[11]指出LJW异构签密方案存在3种安全缺陷，并提出改进方案。但是，本文分析发现，LJW异构签密方案以及张玉磊等人提出的改进方案(记为ZYL-LJW改进方案)均存在接收者滥用签密密文的安全缺陷。由于论文篇幅有限，本文并不完整地论述LJW异构签密方案和ZYL-LJW改进方案及其安全性，仅以ZYL-LJW改进方案的PCHS(PKI-CLC Heterogeneous System)方案为例进行说明，LJW异构签密的PCHS和CPHS(CLC-PKI Heterogeneous System)方案以及ZYL-LJW改进方案的CPHS方案均存在相同的安全缺陷。

4.2.1 ZYL-LJW改进方案的PCHS签密方案

本文简要描述ZYL-LJW改进方案的PCHS签密方案，包括：系统建立、CLPKC用户密钥建立、TPKI用户密钥建立、PCHS签密和PCHS解签密5个算法，简要叙述如下。

(1) 系统建立算法：密钥生成中心PKG输入安全参数κ，输出系统公开参数$\mathrm{pa}_T=\{G_1, G_2, n, e, P, P_{\mathrm{pub}}, e_1, H_1, H_2, H_3, H_4, H_5, H_6, H_7\}$。其中，$G_1$, G_2分别为加法循环群和乘法循环群，$P\in G_1$为G_1的一个生成元，e: $G_1\times G_1\to G_2$为满足本文第2节定义的双线性映射，n表示签密消息长度，$P_{\mathrm{pub}}=sP$为PKG的公钥，$s\in\mathbb{Z}_q$为PKG的主密钥，H_1, H_2, H_3, H_4, H_5, H_6, H_7为安全密码Hash函数(具体定义参考文献[11])。

(2) CLPKC用户密钥建立：与本文4.1.1节(3)密钥提取算法类似，CLPKC环境下的用户$\mathrm{ID_B}$建立密钥$\mathrm{SK_B}=(D_\mathrm{B}=sQ_\mathrm{B}, x_\mathrm{B})$，对应的无证书公钥$\mathrm{PK_B}=x_\mathrm{B}P$。

(3) TPKI用户密钥建立：TPKI环境下的用户$\mathrm{ID_A}$随机选择$x_\mathrm{A}\in\mathbb{Z}_q$作为其私钥$\mathrm{SK_A}$，计算其公钥$\mathrm{PK_A}=x_\mathrm{A}P$。注意：文献[11]中省略了TPKI用户的公钥证书建立与发布过程，这里，本文的叙述也遵循上述文献。

(4) PCHS签密：假设待发送消息为m，发送者为TPKI环境下的用户$\mathrm{ID_A}$，接收者为CLPKC环境下的用户$\mathrm{ID_B}$。$\mathrm{ID_A}$执行以下步骤。

步骤 1　随机选择$k\in\{0, 1\}^n$，计算$r=H_2(k, m)$，$f=e(P_{\mathrm{pub}}, Q_\mathrm{B})^r$；

步骤 2　计算$U_1=rP$, $U_2=k\oplus H_3(f, r\mathrm{PK_B})$, $U_3=m\oplus H_4(k)$；

步骤 3　计算$S=(r+\mathrm{SK_A}H_5(m))\bmod n$，输出签密密文$\sigma=(S, U_1, U_2, U_3)$。

(5) PCHS解签密：$\mathrm{ID_B}$收到密文(S, U_1, U_2, U_3)后，执行以下步骤。

步骤 1 计算f=$e(D_{\mathrm{B}}, U_1)$, k=$U_2\oplus H_3(f, x_{\mathrm{B}}U_1)$;

步骤 2 计算$m = U_3\oplus H_4(k)$, r=$H_2(k, m)$, V=SP–$H_5(m)\mathrm{PK}_{\mathrm{A}}$;

步骤 3 验证V=U_1是否相等，若相等则接受签密并输出明文m，否则输出⊥。

4.2.2 PCHS签密算法密文滥用性分析

同样地，ZYL-LJW改进方案的PCHS签密算法也存在接收者滥用签密密文的安全缺陷，描述如下。

接收者ID_{B}收到ID_{A}发给他的签密密文(S, U_1, U_2, U_3)后，按照本文4.2.1节PCHS解签密算法计算(f, k, r, m)然后选择一个接收者ID_{C}，按照本文4.2.1节PCHS签密算法计算：f^*=$e(P_{\mathrm{pub}}, Q_{\mathrm{C}})^r$, $U_2^* = k\oplus H_3(f^*, r\mathrm{PK}_{\mathrm{C}})$，输出新的签密密文$\sigma^*$=$(S, U_1, U_2^*, U_3)$。其中，$Q_{\mathrm{C}}$=$H_1(\mathrm{ID}_{\mathrm{C}})$，$\mathrm{PK}_{\mathrm{C}}$是$\mathrm{ID}_{\mathrm{C}}$的公钥。由于$(S, U_1, r, k, U_3, m)$由$\mathrm{ID}_{\mathrm{A}}$直接产生，$\mathrm{ID}_{\mathrm{B}}$并未修改，且$(f^*, U_2^*)$仅用于恢复参数$k$，不影响签名验证，因此，可以验证$\sigma^*$是一个有效的$\mathrm{ID}_{\mathrm{A}}$→$\mathrm{ID}_{\mathrm{C}}$签密密文，并且$\mathrm{ID}_{\mathrm{C}}$能输出正确的消息$m$。可见，接收者滥用签密密文攻击成立。

4.2.3 ZYL-LJW改进方案的PCHS签密算法改进

对ZYL-LJW方案的PCHS签密算法的改进方法与本文4.1.3节的方法类似，具体分为两步。第1步，在系统建立算法中采用新的Hash函数H_5^*；第2步，在本文4.1.1节PCHS解签密算法步骤2中，将Hash运算$H_5(m)$扩展为$H_5^*(\mathrm{ID}_{\mathrm{B}}, U_1, U_2, U_3, m)$，以实现签名对接收者身份和签密密文进行绑定。

5 分析与比较

5.1 改进方案不可滥用性分析

以本文对ZYL方案[9]的改进方案(下文记为ZYL-G方案)为例，采用本文第3节定义的安全模型eID-EUF-CMA进行不可滥用性分析。对ZYL-LJW方案[11]的改进方案分析则类似，本文不再赘述。

定理1 如果n-SDH假设成立，则ZYL-G方案满足签密密文不可滥用性。

证明 本文将ZYL-G方案的签密密文不可滥用性规约到模拟器C利用敌手A求解n-SDH问题，即：假设A赢得本文第3节定义的安全游戏的优势为$\varepsilon(\kappa)$，那么C成功求解n-SDH问题的概率至少为$F(\varepsilon(\kappa))$。因此，如果n-SDH假设成立($F(\varepsilon(\kappa))$可忽略)，那么A赢得游戏的优势$\varepsilon(\kappa)$是可忽略的，因此根据本文第3节的定义1, ZYL-G方案满足签密密文不可滥用性。

给定n-SDH问题实例：$(P, \alpha P, \alpha^2 P, \cdots, \alpha^n P)\in G_1^{n+1}$, C构造算法$F$利用A输出一对值$(w^*, (1/(w^*+\alpha))P)$。下面模拟C和A之间的游戏。

初始化：C随机选择$w_1, w_2, \cdots, w_n\in\mathbb{Z}_{q_1}$和$G_{1\text{-}1}$的一个生成元$P$；令多项式$f(z)$=$\prod_{i=1}^{n-1}(z+w_i)$，展开可得$f(z)=\sum_{i=0}^{n-1}c_i z^i$；计算$P_1=\sum_{i=0}^{n-1}c_i(\alpha^i P)=f(\alpha)P$, $P_{\mathrm{pub}_1}=\sum_{i=1}^{n}c_{i-1}(\alpha^i P)=\alpha f(\alpha)P=\alpha P_1$, C创建系统参数$\mathrm{pa}_1=\{G_{1-1}, G_{1-2}, q_1, g, P_1, P_{\mathrm{pub}_1}, e_1, H_{1-1}, H_{1-2}\}$和$\mathrm{pa}_2=\{G_{2-1}, G_{2-2}, q_2, l_m, l_{\mathrm{ID}}, P_2, P_{\mathrm{pub}_2}, H_{2-1}, H_{2-2}\}$。其中，$P_1=f(\alpha)P$, $P_{\mathrm{pub}_1}=\alpha P_1$, α作为IDPKC系统主密钥(对C来说未知)，P_{pub_2}=s_2P_2, $s_2\in\mathbb{Z}_{q_2}$为CLPKC系统的主密钥，由C随机选择，$H_{1\text{-}1}$, $H_{1\text{-}2}$模拟为随机预言机，其它参数同4.1.1节系统建立算法。C维护初始为空的列表$\boldsymbol{L}_{\mathrm{ID}}$, $\boldsymbol{L}_{\mathrm{H}}$, $\boldsymbol{L}_{\mathrm{K}}$, $\boldsymbol{L}_{\mathrm{S}}$。这里要求$f(\alpha)\neq 0$，也就是$w_i\neq-\alpha, i\in\{1, 2, \cdots, n\}$。

询问：A自适应地执行多项式时间有界的询问，C模拟ZYL-G方案的相应算法做出应答。

(1) $H_{1\text{-}1}$询问：输入IDPKC环境下的用户身份$\mathrm{ID}_i(i\in\{1, 2, \cdots, n\})$，C查询$\boldsymbol{L}_{\mathrm{ID}}$，如果存在<$\mathrm{ID}_i$, Q_i>，则输出Q_i；否则，令Q_i=w_i，将<ID_i, Q_i>插入$\boldsymbol{L}_{\mathrm{ID}}$，输出$Q_i$。特定地，如果$\mathrm{ID}_i=\mathrm{ID}_s^*$，则令$Q_s^*=w^*$。

(2) $H_{1\text{-}2}$询问：输入$(\mathrm{ID}_r, c, m, R_1)$，C查询$\boldsymbol{L}_{\mathrm{H}}$，如果存在元组<$\mathrm{ID}_r$, c, m, R_1, h>，则输出h；否则，随机选择h←$\mathbb{Z}_{q_1}$，输出h，将<ID_r, c, m, R_1, h>插入$\boldsymbol{L}_{\mathrm{H}}$。

(3) 密钥询问：输入用户身份ID_u，如果$\mathrm{ID}_u=\mathrm{ID}_s^*$，则模拟失败(不允许A询问$\mathrm{ID}_s^*$的私钥)；否则如果$\mathrm{ID}_u$=$\mathrm{ID}_i(i\in\{1, 2, \cdots, n-1\})$属于IDPKC环境下的用户，那么令$f_i(\alpha)=f(\alpha)/(\alpha+w_i)=\prod_{j=1, j\neq i}^{n-1}(\alpha+w_j)$，扩展$f_i(\alpha)=\sum_{j=0}^{n-2}d_j\alpha^j$，然后计算$S_i$=$f_i(\alpha)P=\sum_{j=0}^{n-2}d_j(\alpha^j P)=(f(\alpha)/(\alpha+w_i))P=(1/(\alpha+w_i))P_1$，输出$S_i$；如果$\mathrm{ID}_u$属于CLPKC环境下的用户，那么C按照本文4.1.1节密钥提取算法计算ID_u的公私钥$(\mathrm{SK}_u, \mathrm{PK}_u)$，输出$\mathrm{SK}_u$。注意：为了保持用户身份和密钥的一致性，C在$\boldsymbol{L}_{\mathrm{K}}$中保存用户身份和密钥，对相同的询问给出相同的应答。

(4) 签密询问：输入$(\mathrm{ID}_s, \mathrm{ID}_r, m)$，如果$\mathrm{ID}_s=\mathrm{ID}_s^*\wedge\mathrm{ID}_r=\mathrm{ID}_r^*\wedge m=m^*$，则模拟失败(说明：根据本文第3节定义的安全模型，不允许A询问$(\mathrm{ID}_s^*, \mathrm{ID}_r^*, m^*)$的签密密文)；否则，如果$\mathrm{ID}_s\neq\mathrm{ID}_s^*$, C通过密钥询问取得$\mathrm{ID}_s$的私钥$S_s$，然后按照本文4.1.1节签密算法计算并输出签密密文δ=(c, R_2, W)；如果$\mathrm{ID}_s=\mathrm{ID}_s^*$, C随机选择$h$←$\mathbb{Z}_{q_1}$, r_2←$\mathbb{Z}_{q_2}$, W←$G_{1\text{-}1}$，计算$R_1=e_1(W, P_{\mathrm{pub}_1}+Q_sP_1)g^{-h}$, $R_2=r_2P_2$, $U=e_2(P_{\mathrm{pub}_2}, Q_r)^{r_2}$, $V=r_2\mathrm{PK}_r$,

$c=(m\|R_1\|\mathrm{ID}_s)\oplus H_{2-2}(U,V,R_2)$，输出签密密文$\delta=(c,\ R_2,\ W)$，并且将<ID$_r$, c, m, R_1, h>插入$\boldsymbol{L}_{\mathrm{H}}$。最后，将密文$\delta=(c,\ R_2,\ W)$插入$\boldsymbol{L}_{\mathrm{S}}$。其中，$Q_s$通过$H_{1\text{-}1}$询问取得，$Q_r=H_{2\text{-}1}(\mathrm{ID}_r)$，PK$_r$通过密钥询问取得。

(5) 解签密询问：输入(ID$_r$, c, R_2, W)，C通过密钥询问取得ID$_r$的私钥SK$_r$，然后按照4.1.1节解签密算法的步骤1、步骤2解密得到$(m||R_1||\ \mathrm{ID}_s)$，查询$\boldsymbol{L}_{\mathrm{H}}$和$\boldsymbol{L}_{\mathrm{ID}}$，如果存在元组<ID$_r$, c, m, R_1, h>和<ID$_s$, Q_s>，取得h和Q_s，并验证等式$R_1=e_1(W,P_{\mathrm{pub}_1}+Q_sP_1)g^{-h}$是否成立，若等式成立则输出明文$m$，并将密文$\delta=(c,\ R_2,\ W)$插入$\boldsymbol{L}_{\mathrm{S}}$；否则，相应的$h$和$Q_s$不存在或者等式不成立，则输出$\perp$。

挑战：询问阶段结束以后，A输出$(\mathrm{ID}_s^*,\mathrm{ID}_r^*,m^*)$的一个签密密文$\delta^*=(c^*,R_2^*,W^*)$。

如果验证δ^*为(ID$_s^*$, ID$_r^*$, m^*)的一个有效签密密文，那么根据双叉引理[16]，$\boldsymbol{L}_{\mathrm{S}}$中必然存在$\delta'=(c',R_2',W')$为一个有效签密密文，且与$\delta^*$拥有相同的$R_1$。C计算$S_s^*=\dfrac{W^*-W'}{h^*-h'}=\dfrac{(r_1+h^*)S_s^*-(r_1+h')S_s^*}{h^*-h'}$。其中，$h^*$和$h$'可从$\boldsymbol{L}_{\mathrm{H}}$中取得，因为要生成签密密文必须询问$H_{1\text{-}2}$预言机。

显然，$S_s^*=(1/(\alpha+w^*))\,P_1=(f(\alpha)/(\alpha+w^*))\,P$。根据多项式除法可展开$f(\alpha)=\gamma(\alpha)(\alpha+w^*)+\gamma_{-1}$，其中，$\gamma(\alpha)=\sum_{i=0}^{n-2}\gamma_i\alpha^i$, $\gamma_{-1}\in\mathbb{Z}_{q_1}$为一非零整数。则$f(\alpha)/(\alpha+w^*)=\dfrac{\gamma_{-1}}{\alpha+w^*}+\sum_{i=0}^{n-2}\gamma_i\alpha^i$，$S_s^*=\left(\dfrac{\gamma_{-1}}{\alpha+w^*}+\sum_{i=0}^{n-2}\gamma_i\alpha^i\right)P$，计算$\dfrac{1}{\alpha+w^*}P=\dfrac{1}{\gamma_{-1}}\left(S_s^*-\sum_{i=0}^{n-2}\gamma_i(\alpha^iP)\right)=\dfrac{1}{\gamma_{-1}}\left(\left(\dfrac{\gamma_{-1}}{\alpha+w^*}\sum_{i=0}^{n-2}\gamma_i\alpha^i\right)P-\sum_{i=0}^{n-2}\gamma_i(\alpha^iP)\right)$，输出$\left(w^*,\dfrac{1}{w^*+\alpha}P\right)$作为对$n$-SDH问题的回答。

证毕

5.2 对比分析

改进前后方案(ZYL-G和ZYL-LJW-G表示本文的改进方案)的安全性和计算开销对比见表1。表中，√表示签密方案实现了相关属性，×则表示没有，E表示乘法群上的模指数运算次数，M表示加法群上的点乘运算次数，P表示双线性对运算次数，H_i表示除$H_{1\text{-}2}$和H_5以外的其它哈希运算次数，$H_{1\text{-}2}$和H_5分别表示哈希运算$H_{1\text{-}2}$和H_5的次数，$H_{1\text{-}2}{}^*$和$H_5{}^*$则分别表示哈希运算$H_{1\text{-}2}{}^*$和$H_5{}^*$的次数。

表 1　改进前后方案的对比

签密方案	机密性	签名不可伪造性	签密不可滥用性	计算开销
ZYL方案	√	√	×	$2E+3M+1P+2H_i+1H_{1\text{-}2}/1E+2M+2P+2H_i+1H_{1\text{-}2}$
ZYL-G方案	√	√	√	$2E+3M+1P+2H_i+1H_{1\text{-}2}{}^*/1E+2M+2P+2H_i+1H_{1\text{-}2}{}^*$
ZYL-LJW方案	√	√	×	$2E+1M+1P+2H_i+1H_5/2E+1P+2H_i+1H_5$
ZYL-LJW-G方案	√	√	√	$2E+1M+1P+2H_i+1H_5{}^*/2E+1P+2H_i+1H_5{}^*$

从表1可以看出，本文提出的改进方案在增强原方案安全性的同时，几乎没有增加其计算开销。以ZYL-G方案为例，本文的改进方案与原方案唯一的不同是用$H_{1\text{-}2}{}^*$: $\{0,1\}^{l_{\mathrm{ID}}}\times\{0,1\}^{l_c}\times\{0,1\}^{l_m}\times G_{1\text{-}2}\to\mathbb{Z}_{q_1}$替换原方案中的$H_{1\text{-}2}$: $\{0,1\}^*\times G_{1\text{-}2}\to\mathbb{Z}_{q_1}$。也就是说，改进方案将哈希函数$H_{1\text{-}2}$的输入增加了$l_{\mathrm{ID}}+l_c$比特，这相对于整体计算开销来说，可忽略不计。ZYL-LJW-G方案则类似。

6　结束语

本文研究了签密方案的不可伪造性及其安全模型，主要研究内容和创新点包含以下几方面。第一，分析发现，文献[5,9,11]中提出的几种签密方案虽然在EUF-CMA模型下被证明满足不可伪造性，但是仍然存在签密密文被恶意的接收者滥用的安全缺陷，这是一种内部攻击事件，本文定义了密文不可滥用性以刻画这一安全缺陷。第二，本文对EUF-CMA模型进行扩展，增强了敌手的能力，使之能模拟密文不可滥用性。第三，针对文献[5,9,11]提出方案的安全缺陷，本文提出了改进方法，该方法能防范这一类型攻击。最后，本文以ZYL-G方案为例，演示了采用扩展的EUF-CMA模型分析签密方案的密文不可滥用性。

密文不可滥用性是签密方案的特有安全属性，对签密方案具有普遍意义。本文研究虽然以异构签密方案为例，对非异构环境下的签密方案也具有借鉴意义。但是，在非异构环境下，由于挑战用户ID*的私钥对模拟器来说未知，对敌手提交的(ID$_s$, ID*, σ)解签密询问无法做出正确的应答(此时，密文σ不是由模拟器生成，ID*为接收者；在异构环境下不存在这一情形，因为ID*不可能成为接收者)。因此，在非异构环境下，如何实现完备的安全游戏模拟过程还需要进一步研究。

参 考 文 献

[1] ZHENG Yuliang. Digital signcryption or how to achieve cost (signature & encryption)<<cost(signature)+cost(encryption)[C]. Proceedings of the 17th Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, USA, 1997: 165–179. doi: 10.1007/BFb0052234.

[2] SUN Yinxia and LI Hui. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. *Science China Information Sciences*, 2010, 53(3): 557–566. doi: 10.1007/s11432-010-0061-5.

[3] LI Fagen, ZHANG Hui, and TAKAGI T. Efficient signcryption for heterogeneous systems[J]. *IEEE Systems Journal*, 2013, 7(3): 420–429. doi: 10.1109/JSYST.2012.2221897.

[4] FU Xiaotong, LI Xiaowei, and LIU Wen. IDPKC-to-TPKC construction of multi-receiver signcryption[C]. Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an, China, 2013: 335–339. doi: 10.1109/INCoS.2013.62.

[5] 刘景伟, 张俐欢, 孙蓉. 异构系统下的双向签密方案[J]. 电子与信息学报, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

LIU Jingwei, ZHANG Lihuan, and SUN Rong. Mutual signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2948–2953. doi: 10.11999/JEIT160056.

[6] 张玉磊, 张灵刚, 张永洁, 等. 匿名CLPKC-TPKI异构签密方案[J]. 电子学报, 2016, 44(10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

ZHANG Yulei, ZHANG Linggang, ZHANG Yongjie, *et al*. CLPKC-to-TPKI heterogeneous signcryption scheme with anonymity[J]. *Acta Electronica Sinica*, 2016, 44(10): 2432–2439. doi: 10.3969/j.issn.0372-2112.2016.10.022.

[7] 路秀华, 温巧燕, 王励成. 格上的异构签密[J]. 电子科技大学学报, 2016, 45(3): 458–462. doi: 10.3969/j.issn.1001-0548.2016.02.025.

LU Xiuhua, WEN Qiaoyan, and WANG Licheng. A lattice-based heterogeneous signcryption[J]. *Journal of University of Electronic Science and Technology of China*, 2016, 45(3): 458–462. doi: 10.3969/j.issn.1001-0548.2016.02.025.

[8] 王彩芬, 李亚红, 张玉磊, 等. 标准模型下高效的异构签密方案[J]. 电子与信息学报, 2017, 39(4): 881–886. doi: 10.11999/JEIT160662.

WANG Caifen, LI Yahong, ZHANG Yulei, *et al*. Efficient heterogeneous signcryption scheme in the standard model[J]. *Journal of Electronics & Information Technology*, 2017, 39(4): 881–886. doi: 10.11999/JEIT160662.

[9] 张玉磊, 张灵刚, 王彩芬, 等. 可证安全的IDPKC-to-CLPKC异构签密方案[J]. 电子与信息学报, 2017, 39(9): 2127–2133. doi: 10.11999/JEIT170062.

ZHANG Yulei, ZHANG Linggang, WANG Caifen, *et al*. Provable secure IDPKC-to-CLPKC heterogeneous signcryption scheme[J]. *Journal of Electronics & Information Technology*, 2017, 39(9): 2127–2133. doi: 10.11999/JEIT170062.

[10] 王彩芬, 刘超, 李亚红, 等. 基于PKI和IBC的双向匿名异构签密方案[J]. 通信学报, 2017, 38(10): 10–17.

WANG Caifen, LIU Chao, LI Yahong, *et al*. Two-way and anonymous heterogeneous signcryption scheme between PKI and IBC[J]. *Journal on Communications*, 2017, 38(10): 10–17.

[11] 张玉磊, 王欢, 刘文静, 等. 异构双向签密方案的安全性分析和改进[J]. 电子与信息学报, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

ZHANG Yulei, WANG Huan, LIU Wenjing, *et al*. Security analysis and improvement of mutual signcryption schemes under heterogeneous systems[J]. *Journal of Electronics & Information Technology*, 2017, 39(12): 3045–3050. doi: 10.11999/JEIT170203.

[12] AN J H, DODIS Y, and RABIN T. On the security of joint signature and encryption[C]. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology, Amsterdam, Netherlands, 2002: 83–107. doi: 10.1007/3-540-46035-7_6.

[13] YU Yong, YANG Bo, SUN Ying, *et al*. Identity based signcryption scheme without random oracles[J]. *Computer Standards & Interfaces*, 2009, 31(1): 56–62. doi: 10.1016/j.csi.2007.10.014.

[14] GALBRAITH S D, PATERSON K G, and SMART N P. Pairings for cryptographers[J]. *Discrete Applied Mathematics*, 2008, 156(16): 3113–3121. doi: 10.1016/j.dam.2007.12.010.

[15] BONEH D and BOYEN X. Short signatures without random oracles[C]. Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 56–73. doi: 10.1007/978-3-540-24676-3_4.

[16] POINTCHEVAL D and STERN J. Security arguments for digital signatures and blind signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361–396. doi: 10.1007/s001450010003.

陈 明：男，1978年生，副教授，研究方向为信息安全，安全协议分析与设计.