一个基于身份的签密方案的分析与改进*

何俊杰，焦淑云，祁传达
（信阳师范学院 数学与信息科学学院，河南 信阳 464000）

摘　要：对肖鸿飞等人提出的基于身份的改进高效签密方案进行分析，指出方案不能抵抗不可区分性选择明文攻击和不诚实接收者的一般性伪造攻击。为此，提出了一个改进的签密方案。运用随机预言机模型，证明了新方案在适应性选择密文攻击下是不可区分的和在适应性选择消息及身份攻击下是存在性不可伪造的，安全性可以分别规约为判定双线性 Diffie-Hellman 问题和计算 Diffie-Hellman 问题。

关键词：签密；基于身份；公开验证性；前向安全性；语义安全性；不可伪造性
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2013)03-0913-04
doi:10.3969/j.issn.1001-3695.2013.03.070

Analysis and improvement of ID-based signcryption scheme

HE Jun-jie, JIAO Shu-yun, QI Chuan-da
(*College of Mathematics & Information Science*, *Xinyang Normal University*, *Xinyang Henan* 464000, *China*)

Abstract: Cryptanalysis of the improved efficient ID-based signcryption scheme which was proposed by Xiao, *et al.* shows that the scheme can't resist indistinguishability under chosen ciphertext attack and dishonest recipient's general forgery attack. This paper proposed an improved signcryption scheme to overcome these security problems. The new scheme had the indistinguishability against adaptive chosen ciphertext attacks property and was secure against an existential forgery for adaptive chosen messages and identity attacks in random oracle model, and the security was reduced to decisional bilinear Diffie-Hellman problem and computational Diffie-Hellman problem.

Key words: signcryption; ID-based; public verifiability; forward security; semantic security; unforgeability

1984 年，Shamir[1] 提出了基于身份公钥密码体制。与传统的基于证书的公钥密码体制相比，基于身份的密码体制简化了密钥管理的过程。其基本思想是将用户的公开身份信息如姓名、电话号码、IP 地址、电子邮件地址等直接作为用户公钥，或由用户身份信息通过公开算法计算出该用户的公钥，不再需要使用公钥证书；用户私钥则由一个可信第三方——私钥生成中心（private key generator，PKG）统一生成，并通过安全信道发送给用户。2001 年，Boneh 等人[2] 利用双线性对提出了第一个高效且可证安全的基于身份的加密方案，随后利用双线性对实现的基于身份的签名方案也被提出。

1997 年，Zheng[3] 提出了签密的概念。签密可以在一个逻辑步骤内同时完成对明文消息的加密和签名。与传统的先签名后加密的方案相比，签密方案的计算开销更小，传输的密文更短，效率更高，特别适用于计算资源和传输带宽受限的应用场合。结合基于身份密码体制和签密体制，Malone-Lee[4] 构造了第一个基于身份的签密方案。但 Libert 等人[5] 指出文献[4]中方案不具有语义安全性，并给出了一个新的基于身份的签密方案。李发根等人[6] 利用双线性对提出了一个新的基于身份的签密方案，具有较高效率。但张明武等人[7] 通过选择明文攻击，证明了文献[6]方案不具有语义安全性。李志敏等人[8] 也提出了一个基于身份的公开验证签密方案，但计算效率不高。张串绒等人[9] 提出了一种适合用于 Ad hoc 网络的密钥管理、安全路由等通信安全协议的基于身份的新签密算法。肖鸿飞等人[10] 指出文献[9]方案不满足前向安全性和公开验证性，并给出了一种改进方案。本文对文献[10]方案的安全性进行分析，指出方案不满足不可伪造性和不可否认性，并对其进行了改进。

1　双线性对及相关数学难题

1.1　双线性对

设$(G_1, +)$是一个阶为素数 q 的加法群，$(G_2, \cdot)$是一个阶为 q 的乘法群，假定在群 G_1 和 G_2 中的离散对数问题是难解的，称映射 $e: G_1 \times G_1 \to G_2$ 是一个双线性对，若满足如下性质：

a）双线性性。对于任何 $U, V \in G_1, a, b \in Z_q^*$，有 $e(aU, bV) = e(U, V)^{ab}$。

b）非退化性。存在 $U, V \in G_1$，使得 $e(U, V) \neq 1$。

c）可计算性。对于任何的 $U, V \in G_1$，存在一个高效的算法来计算 $e(U, V)$的值。

若群 G_1 取有限域上超奇异椭圆曲线或超椭圆曲线，双线性对就可以利用该曲线上的 Weil 配对或 Tate 配对构造。

1.2　相关数学难题

基于椭圆曲线上双线性对的签密算法一般基于以下的数学难题：

收稿日期：2012-07-14；**修回日期**：2012-08-27　　**基金项目**：国家自然科学基金资助项目(61272465)；河南省自然科学基金资助项目(102102210242,122400450189)；河南省教育厅科学技术研究重点项目(12A520034)

作者简介：何俊杰(1981-)，男，讲师，硕士，主要研究方向为信息安全(hejj99@163.com)；焦淑云(1979-)，女，讲师，博士研究生，主要研究方向为演化动力学；祁传达(1964-)，男，教授，博士，主要研究方向为密码理论.

a)离散对数问题(DLP)。任取 $P,Q\in G_1$,求 $x\in Z_q^*$,使得 $Q=xP$。

b)计算 Diffie-Hellman 问题(CDHP)。任给 $aP,bP\in G_1$($a,b\in Z_q^*$ 未知),计算 abP。

c)计算双线性 Diffie-Hellman 问题(CBDHP)。已知 $P,aP,bP,cP\in G_1$($a,b,c\in Z_q^*$ 未知),计算 $e(P,P)^{abc}\in G_2$。

d)判定双线性 Diffie-Hellman 问题(DBDHP)。任给 $P,aP,bP,cP\in G_1$($a,b,c\in Z_q^*$ 未知)和 $\xi\in G_2$,判断 $e(P,P)^{abc}=\xi$ 是否成立。

2 签密方案模型及安全性定义

2.1 签密模型[4]

基于身份的签密方案一般包括四个算法:

a)系统建立(setup)。给定系统安全参数 k,由 PKG 生成系统参数。

b)密钥提取(extract)。给定用户 U 的身份 ID_U,由 PKG 生成与之相对应的私钥 S_U,并通过秘密信道传送给用户 U。

c)签密(signcrypt)。发送者 Alice 输入自己的私钥 S_A、接收者 Bob 的身份 ID_B 以及消息 m,生成密文 σ。

d)解签密(unsigncrypt)。接收者 Bob 输入自己的私钥 S_B、发送者 Alice 的身份 ID_A 以及密文 σ,输出消息 m 或者“⊥”。输出“⊥”表明密文无效。

2.2 基于身份的签密方案的安全性

一个基于身份的签密方案要求满足:

a)保密性。攻击者从一个签密密文中获取任何明文信息在计算上是不可行的。

b)不可伪造性。攻击者产生一个合法的签密密文在计算上是不可行的。

c)不可否认性。发送者不能否认他已经签密过的消息。

d)公开验证性。任何第三方在获得密文后,在系统公开参数和签密方开钥的配合下,可以通过验证等式证明这个密文由签密者所签发,且验证者不能获得有关密文及签发者和接收者更多的信息。

e)前向安全性。如果某个用户的私钥被盗,第三方也不能恢复出他过去所签密消息的明文。

保密性和不可伪造性可以由下面的定义给出。

定义 1 保密性[5]。如果没有任何多项式有界的敌手以一个不可忽略的优势赢得以下的游戏 IND-IBSC-GAME,则称一个基于身份的签密方案在适应性选择密文和身份攻击下具有不可区分性(IND-IBSC-CCIA2)。

游戏 IND-IBSC-GAME 步骤如下:

a)系统设置。挑战者 C 输入安全参数 k,运行 setup 算法,并将系统参数 params 发送给敌手 $\mathcal{A}$。

b)询问 1。敌手 $\mathcal{A}$ 执行以下询问:

(a)Extract 询问。$\mathcal{A}$ 选择一个身份 ID_U,C 计算 $S_U=\text{extract}(ID_U)$,并将结果发送给 $\mathcal{A}$。

(b)Signcrypt 询问。$\mathcal{A}$ 选择两个身份 ID_A 和 ID_B,一个明文 m。C 计算 $\sigma=\text{signcrypt}(m,S_A,ID_B)$,并将结果 σ 发送给 $\mathcal{A}$。

(c)Unsigncrypt 询问。$\mathcal{A}$ 选择两个身份 ID_A 和 ID_B,一个密文 σ。C 计算私钥 $S_B=\text{extract}(ID_B)$ 和明文 $m=\text{unsigncrypt}(\sigma,ID_A,S_B)$,发送结果明文 m 或符号“⊥”给 $\mathcal{A}$。

c)挑战。$\mathcal{A}$ 生成两个相同长度的明文 m_0、m_1 和希望挑战的两个身份 ID_i 和 ID_j。ID_j 不能是已经执行过 extract 询问的身份。挑战者 C 随机选择 $u\in\{0,1\}$,计算 $\sigma=\text{signcrypt}(m_u,S_i,ID_j)$ 并将结果 σ 发送给 $\mathcal{A}$。

d)询问 2。敌手 $\mathcal{A}$ 像询问 1 那样执行多项式有界次询问。但是他不能对 ID_j 执行 extract 询问,也不能对密文 σ 执行 unsigncrypt 询问。

e)猜测。敌手 $\mathcal{A}$ 输出 u' 作为对 u 的猜测。如果 $u'=u$,敌手 $\mathcal{A}$ 赢得游戏。

定义 2 不可伪造性[5]。如果不存在任何多项式有界的攻击者以一个不可忽略的优势赢得以下的游戏 EUF-IBSC-GAME,则称一个基于身份的签密方案在适应性选择消息和身份攻击下是存在性不可伪造的(EUF-IBSC-CMIA)。

游戏 EUF-IBSC-GAME 步骤如下:

a)系统设置。挑战者 C 输入安全参数 k,运行 setup 算法,并将系统参数 params 发送给敌手 $\mathcal{A}$。

b)询问。敌手 $\mathcal{A}$ 执行多项式有界次类似游戏 1 中定义的询问。

c)伪造。最后,敌手 $\mathcal{A}$ 生成一个新的三元组(σ',ID_A,ID_B),即这个三元组不是寻找阶段 signcrypt 预言机输出的,且不是寻找阶段 extract 预言机输出的。如果 $\text{unsigncrypt}(\sigma',S_B,ID_A)\neq\perp$,则敌手 $\mathcal{A}$ 赢得游戏。

3 文献[10]方案的回顾

3.1 Setup

给定安全参数 k,PKG 选择椭圆曲线上的 q 阶加法循环群 G_1 和 q 阶乘法循环群 G_2,其中,G_1 的生成元为 P。由 G_1 和 G_2 上的 Weil 对或 Tate 对的变形得到双线性映射 $e:G_1\times G_1\to G_2$。PKG 选择系统的私钥 $\delta\in_R Z_q^*$,计算系统公钥 $P_{pub}=\delta P\in G_1$。PKG 选取安全的对称密码算法(E,D)和四个安全的散列函数 $H_1:\{0,1\}^{l_1}\to G_1$,$H_2:G_2\to Z_q^*$,$H_3:\{0,1\}^{l_2}\times\{0,1\}^{n'}\to Z_q^*$ 和 $H_4:\{0,1\}^n\to Z_q^*$。其中,l_1 是用户身份 ID 的比特长度;l_2 是 G_1 中元素的比特长度;n 是明文 m 的比特长度;n'是 H_4 输出的比特长度。系统参数 params 为$\{G_1,G_2,q,P,P_{pub},E,D,H_1,H_2,H_3,H_4\}$。

3.2 Extract

给出用户的身份 ID_U,PKG 计算相应的公钥 $Q_U=H_1(ID_U)$ 和私钥 $S_U=\delta Q_U$。本方案中发送者 Alice 和接收者 Bob 的私公钥对为(S_A,Q_A)和(S_B,Q_B)。

3.3 Signcrypt

用户 Alice 执行以下过程:

a)计算 $Q_B=H_1(ID_B)$。

b)选取 $x\in_R Z_q^*$,计算 $k_1=xQ_A$,$\omega=e(S_A,Q_B)^x$,$k_2=H_2(\omega)$。

c)计算 $t=E_{k_2}(m)$,$h=H_4(m)$,$r=H_3(k_1,h)$,$s=k_1/(r+Q_A)$。

用户 Alice 发送密文 $\sigma=(t,r,s)$给用户 Bob。

3.4 Unsigncrypt

用户 Bob 收到密文 $\sigma=(t,r,s)$后,执行以下解签密的操作:

a)计算 $Q_A=H_1(ID_A)$,$k_1=s(r+Q_A)$,$\omega=e(S_B,k_1)$。

b)计算 $k_2=H_2(\omega)$。

c)计算 $D_{k_2}(t)$得到 m 或⊥。

d)如果得到 m,则计算 $h=H_4(m)$,并验证 $r=H_3(k_1,h)$ 成立否。如果不成立则输出 $\perp$;如果成立则接受 m,并确信 $\sigma=(t,r,s)$ 来自用户 Alice。

4　对文献[10]方案的攻击

4.1　选择明文攻击

对文献[10]方案可以实施不可区分性选择明文攻击(indistinguishability under chosen ciphertext attack, IND-CPA)。

设敌手 $\mathcal{A}$ 选择两个明文 m_0、m_1。挑战者 C 随机选择一个明文,经签密预言机签密产生密文 $\sigma^*=(t^*,r^*,s^*)$。$\mathcal{A}$ 计算 $k_1^*=s^*(r^*+Q_A)$,$h^*=H_4(m_0)$,验证等式 $r^*=H_3(k_1^*,h^*)$ 是否成立,若等式成立则密文 σ^* 是 m_0 对应的签密密文,否则密文 σ^* 是 m_1 对应的签密密文。由于该方案采用消息明文直接在验证等式中,因此在选择明文攻击时利用上述攻击方案可以在不恢复明文的情况下取得对不可区分性游戏 IND-IBSC-GAME 的优势,而且这种优势是肯定的。因此该方案不具有语义安全性。

4.2　伪造攻击

不诚实的接收者 Bob 可以伪造用户 Alice 对任意消息的签密密文。对任意的消息 m',任取 $x'\in_R Z_q^*$,计算 $k'_1=x'Q_A$,$h'=H_4(m')$,$r'=H_3(k'_1,h')$,$s'=k'_1/(r'+Q_A)$,$\omega'=e(S_B,k'_1)$,$k'_2=H_2(\omega')$,$t'=E_{k'_2}(m')$,则 $\sigma'=(t',r',s')$ 是用户 Alice 对消息 m 的有效签密。所以,文献[10]方案不具有不可伪造性。

同时,由于接收者的可伪造性,使得对于公开的有效签密 $\sigma=(t,r,s)$,第三方无法区分是发送者 Alice 所为还是接收者 Bob 所为,方案失去了不可否认性。

5　文献[10]方案的改进

为了抵抗选择明文攻击和伪造攻击,本文对文献[10]方案进行了改进,提出了一个新的基于身份的签密方案。改进方案的 setup 和 extract 阶段与 3.1 和 3.2 节基本相同,只是修改了哈希函数 $H_3:G_1\times G_2\times\{0,1\}^n\rightarrow Z_q^*$,不需要哈希函数 H_4。下面是对 signcrypt 和 unsigncrypt 阶段描述。

5.1　Signcrypt

用户 Alice 执行以下过程:

a)计算 $Q_B=H_1(\mathrm{ID}_B)$。

b)任取 $x\in_R Z_q^*$,计算 $R=xQ_A$,$k_1=e(P,P)^x$,$\omega=e(S_A,Q_B)^x$,$k_2=H_2(\omega)$。

c)计算 $t=E_{k_2}(m)$,$r=H_3(R,k_1,t)$,$S=xP-rS_A$。

用户 Alice 发送密文 $\sigma=(t,r,R,S)$ 给用户 Bob。

5.2　Unsigncrypt

用户 Bob 收到密文 $\sigma=(t,r,R,S)$ 后,执行以下解签密的操作:

a)计算 $Q_A=H_1(\mathrm{ID}_A)$,$\omega=e(R,S_B)$。

b)计算 $k_1=e(S,P)e(Q_A,P_{\mathrm{pub}})^r$,$k_2=H_2(\omega)$。

c)计算 $D_{k_2}(t)$ 得到 m 或 $\perp$。

d)如果得到 m,则验证 $r=H_3(R,k_1,t)$ 是否成立,如果不成立则输出 $\perp$;如果成立则接受 m,并确信 $\sigma=(t,r,R,S)$ 来自用户 Alice。

算法的正确性可以由下面两式保证:

$$k_1=e(P,P)^x=e(xP,P)=e(S+rS_A,P)=$$
$$e(S,P)e(rS_A,P)=e(S,P)e(Q_A,P_{\mathrm{pub}})^r$$
$$\omega=e(S_A,Q_B)^x=e(\delta Q_A,Q_B)^x=e(xQ_A,\delta Q_B)=e(R,S_B)$$

6　改进方案的分析

6.1　安全性分析和证明

假设改进方案中所使用的散列函数 H_1、H_2、H_3 是随机预言机。用符号 $q_i(i=1,2,3)$ 表示攻击者至多询问 H_i 的次数,q_E、q_S 和 q_U 分别表示攻击者至多进行 extract 询问、signcrypt 询问和 unsigncrypt 询问的次数。

6.1.1　机密性

定理 1　在随机预言模型下,假设存在敌手 $\mathcal{A}$ 能够在 t 时间内以 ε 的优势赢得 IND-IBSC-GAME 游戏,那么就存在一个算法 $\mathcal{B}$,能够在 $t'\leqslant t+(2q_S+3q_U)t_e$ 时间内以 $\varepsilon'\geqslant\varepsilon e/q_1q_2$ 的优势解决 DBDHP。其中 t_e 表示计算一次双线性对运算所需要的时间。

证明　设 $\mathcal{B}$ 收到 G_1 中 DBDHP 实例(P,aP,bP,cP,ξ),其中随机数 $a,b,c\in Z_q^*$ 未知,算法 $\mathcal{B}$ 调用攻击者 $\mathcal{A}$ 为子程序去判断 $\xi=e(P,P)^{abc}$ 是否成立。

系统设置。算法 $\mathcal{B}$ 生成系统公共参数 params 发送给攻击者 $\mathcal{A}$,其中系统公钥设置为 $P_{\mathrm{pub}}=aP$,即用 a(未知)模拟系统主密钥。

询问 1。$\mathcal{B}$ 需要维护列表 L_1、L_2、L_3、L_S、L_U 响应 $\mathcal{A}$ 的 H_1 询问、H_2 询问、H_3 询问、signcrypt 询问和 unsigncrypt 询问,这些列表初始时是空的。具体交互过程如下:

a)H_1 询问。$\mathcal{B}$ 随机选取整数 $m(1\leqslant m\leqslant q_1)$。$\mathcal{A}$ 关于 ID_i $(1\leqslant i\leqslant q_1)$ 的每一次询问,$\mathcal{B}$ 首先检查列表 L_1。如果在列表 L_1 中已经存在项(ID_i,Q_i,a_i),$\mathcal{B}$ 将 Q_i 返回给 $\mathcal{A}$ 作为 ID_i 的 H_1 哈希值;否则,也就是 $\mathcal{A}$ 从来没做过 ID_i 的 H_1 询问。如果 $i=m$,置 $Q_m=bP$;如果 $i\neq m$,随机选取 $a_i\in_R Z_q^*$,计算 $Q_i=a_iP$。$\mathcal{B}$ 将(ID_i,Q_i,a_i) 添加到列表 L_1,并将 $H_1(\mathrm{ID}_i)=Q_i$ 返回给 $\mathcal{A}$。

b)H_2 询问。$\mathcal{A}$ 关于 $\omega_i(1\leqslant i\leqslant q_2)$ 的每一次询问,$\mathcal{B}$ 首先检查列表 L_2。如果在列表 L_2 中已经存在项(ω_i,k_{2i}),B 将 k_{2i} 返回给 $\mathcal{A}$ 作为 ω_i 的 H_2 哈希值;否则,随机选取 $k_{2i}\in_R Z_q^*$,将(ω_i,k_{2i}) 添加到列表 L_2,并将 $H_2(\omega_i)=k_{2i}$ 返回给 $\mathcal{A}$。

c)H_3 询问。$\mathcal{A}$ 关于(R_i,k_{1i},t_i) $(1\leqslant i\leqslant q_3)$ 的每一次询问,$\mathcal{B}$ 首先检查列表 L_3。如果在列表 L_3 中已经存在项(R_i,k_{1i},t_i,r_i),$\mathcal{B}$ 将 r_i 返回给 $\mathcal{A}$ 作为(R_i,k_{1i},t_i) 的 H_3 哈希值;否则,随机选取 $r_i\in_R Z_q^*$,将(R_i,k_{1i},t_i,r_i) 添加到列表 L_3,并将 $H_3(R_i,k_{1i},t_i)=r_i$ 返回给 $\mathcal{A}$。

d)Extract 询问。对 $\mathcal{A}$ 关于 $\mathrm{ID}_i(1\leqslant i\leqslant q_E)$ 的密钥提取询问(假设已经做过关于 ID_i 的 H_1 询问,否则先执行 H_1 询问),$\mathcal{B}$ 从列表 L_1 中找出项(ID_i,Q_i,a_i)。如果 $\mathrm{ID}_i=\mathrm{ID}_m$,$\mathcal{B}$ 宣告失败,算法终止;否则,$\mathcal{B}$ 计算 $S_i=aQ_i=a(a_iP)=a_i(aP)$,将 S_i 返回给 $\mathcal{A}$。

e)Signcrypt 询问。任何时候 $\mathcal{A}$ 可以选择消息 m 和两个身份 ID_A 和 ID_B,对$(m,\mathrm{ID}_A,\mathrm{ID}_B)$ 进行签密询问(假设已经做过关于 ID_A 和 ID_B 的 H_1 询问,否则先执行 H_1 询问)。如果 $\mathrm{ID}_A\neq\mathrm{ID}_m$,$\mathcal{B}$ 可通过 extract 算法获得 ID_A 的私钥 S_A,然后简单地运行 signcrypt 算法即可;如果 $\mathrm{ID}_A=\mathrm{ID}_m$,则 $\mathrm{ID}_B\neq\mathrm{ID}_m$。$\mathcal{B}$ 首先在 L_1 中找到(ID_A,Q_A,a_A) 和(ID_B,Q_B,a_B),其中 $Q_A=bP$,$Q_B=a_BP$,

计算 $S_B = a_B(aP)$。任意选取 $x' \in_R Z_q^*$，计算 $R = x'Q_A$，$\omega = e(S_B, R)$，查询 H_2 询问获得 $k_2 = H_2(\omega)$，计算 $t = E_{k_2}(m)$。任意选取 $r' \in_R Z_q^*$，计算 $k_1 = e(r'x'P + r'Q_A, P_{pub})$，如果 (R, k_1, t, r') 已经在列表 L_3 中，则重新选取 x' 和 r' 并计算 k_1；计算 $S = r'x'P_{pub}$ 并将 (R, k_1, t, r') 加到列表 L_3 中。$\mathcal{B}$ 将 $\sigma = (t, r', R, S)$ 返回给 $\mathcal{A}$。

$\mathcal{B}$ 对 $\mathcal{A}$ 的所有 signcrypt 询问的回答是有效的。事实上，$k_1 = e(r'x'P + r'Q_A, P_{pub}) = e(r'x'P, P_{pub})e(r'Q_A, P_{pub}) = e(r'x'P_{pub}, P)e(r'Q_A, P_{pub}) = e(S, P)e(Q_A, P_{pub})^{r'}$，即 $\sigma = (t, r', R, S)$ 是 (m, ID_A, ID_B) 的一个有效签密。

f) Unsigncrypt 询问。当 $\mathcal{B}$ 收到一个密文 $\sigma = (t, r, R, S)$ 和两个身份 ID_A 和 ID_B 的解签密询问时，若 $ID_B = ID_m$，则回答密文为非法密文；若 $ID_B \neq ID_m$，首先调用 H_1 预言机和 extract 预言机，可以获得 ID_A、ID_B 对应的公钥 Q_A、Q_B 和 ID_B 对应的私钥 S_B，然后计算 $\omega = e(S_B, R)$，查询 H_2 询问获得 $k_2 = H_2(\omega)$，计算 $m = D_{k_2}(t)$，$k_1 = e(S, P)e(Q_A, P_{pub})^r$。检查 (R, k_1, t, r) 是否在 L_3 中，如果不在，$\mathcal{B}$ 拒绝解签密该密文；否则，$\mathcal{B}$ 返回 m 给 $\mathcal{A}$。

挑战。在上述询问阶段结束后，敌手 $\mathcal{A}$ 输出两个希望挑战的身份 $\{ID_A, ID_B\}$ 和两个消息 $\{m_0, m_1\}$。如果 $ID_B \neq ID_m$，$\mathcal{B}$ 终止这个模拟；否则，$\mathcal{B}$ 随机选取 $u \in \{0, 1\}$，令 $\omega = \xi$，$Q_B = bP$，查询 H_1 询问获得 $Q_A = \alpha P(\alpha \in_R Z_q^*)$，计算 $S_A = aQ_A = a(\alpha P) = \alpha(aP)$，$R^* = \alpha^{-1}cQ_A = cP$，$k_1^* = e(\alpha^{-1}cP, P)$，$t^* = E_{H_2(\omega)}(m_u)$，$r^* = H_3(R^*, k_1^*, t^*)$，$S^* = \alpha^{-1}cP - r^*S_A$，将挑战密文 $\sigma_u^* = (t^*, r^*, R^*, S^*)$ 发送给 $\mathcal{A}$。

询问 2。敌手 $\mathcal{A}$ 继续执行多项式有界次的 hash 询问、extract 询问、signcrypt 询问和 unsigncrypt 询问。这时不能对 ID_B 执行 extract 询问，也不能对 σ_u^* 进行 unsigncrypt 询问。

猜测。询问结束后，若敌手得到猜测的 $u' = u$，则挑战者 $\mathcal{B}$ 能判断 $\xi = e(R^*, S_B) = e(cP, aQ_B) = e(cP, abP) = e(P, P)^{abc}$，即解决了 DBDHP。

分析。下面分析 $\mathcal{B}$ 成功的概率。

$\mathcal{A}$ 在一次 extract 询问时询问 ID_m 对应的私钥的概率为 $1/q_1$，则 $\mathcal{A}$ 没有执行过对 ID_m 的 extract 询问的概率 $p_1 \geqslant (1 - 1/q_1)^{q_E}$；$\mathcal{A}$ 选择 ID_m 作为挑战阶段的消息接收者身份的概率 $p_2 \geqslant 1/q_1$；$\mathcal{A}$ 没有执行过对 $\omega = \xi$ 的 H_2 询问的概率 $p_3 \geqslant 1/q_2$。$\mathcal{B}$ 成功的概率至少为

$$\varepsilon' = \varepsilon p_1 p_2 p_3 \geqslant \varepsilon(1 - 1/q_1)^{q_E}(1/q_1)(1/q_2) \approx \varepsilon e/(q_1 q_2)$$

在 $\mathcal{B}$ 的计算时间方面，每次 signcrypt 询问最多需要两次双线性对运算，每次 unsigncrypt 询问都是最多需要三次双线性对运算。所以 $t' \leqslant t + (2q_S + 3q_U)t_e$，其中 t_e 表示计算一次双线性对运算所需要的时间。

推论 1 在随机预言模型和 DBDHP 困难的假设下，改进的基于身份的签密方案在适应性选择密文攻击下具有不可区分性。

6.1.2 前向安全性

定理 2 改进的基于身份的签密方案是前向安全的。

证明 在定理 1 的证明过程中的挑战阶段，敌手 $\mathcal{A}$ 可以查询签密者身份 ID_A 对应的私钥 S_A。也就是说，即使签密者 Alice 的私钥被泄露了，该签密方案仍可保持明文的秘密性，因此方案是前向安全的。

6.1.3 不可伪造性

定理 3 在随机预言模型下，假设存在敌手 $\mathcal{A}$ 能够在 t 时间内，以 ε 的优势赢得 EUF-IBSC-GAME 游戏，那么，就存在一个算法 C，能够在 $t' \leqslant t + 2q_S t_e$ 时间内，以 $\varepsilon' \geqslant \varepsilon e/q_1$ 的优势解决 CDHP，其中 t_e 表示计算一次双线性对运算所需要的时间。

证明 设 C 收到 G_1 中 CDHP 实例 (P, aP, bP)，其中随机数 $a, b \in Z_q^*$ 未知，算法 C 调用攻击者 $\mathcal{A}$ 为子程序计算 abP。

系统设置。算法 C 生成系统公共参数 params 发送给攻击者 $\mathcal{A}$，其中系统公钥设置为 $P_{pub} = aP$，即用 a（未知）模拟系统主密钥。

询问。$\mathcal{A}$ 可以向 C 提出多项式有界次的 hash 询问、signcrypt 询问和 unsigncrypt 询问，具体过程同定理 1。

伪造。如果算法 C 没有终止，则 $\mathcal{A}$ 在没有做过 ID_m 的 extract 提取询问和 (m, ID_m, ID_B) 的 signcrypt 询问的条件下，以一个不可忽略的概率 ε 对一个输入消息 m 输出签密者身份 ID_m 和接收者身份 ID_B 对应的有效签密 $\sigma = (t, r, R, S)$。根据 Forking 引理[11]，通过对 $\mathcal{A}$ 哈希重放，C 可以获得关于消息 m 和身份 ID_m、ID_B 的两个有效签密 (t, r_1, R_1, S_1) 和 (t, r_2, R, S_2)，其中 $r_1 \neq r_2$。因为有效签密满足 $S = xP - rS_m$，所以

$$S_1 = xP - r_1 S_m, S_2 = xP - r_2 S_m$$

两式相减，得

$$S_1 - S_2 = (r_2 - r_1)S_m$$

所以

$$S_m = (r_2 - r_1)^{-1}(S_1 - S_2)$$

最终，C 可以输出 $S_m = aQ_m = abP$ 作为 CDH 问题的解。

分析。下面分析 C 成功的概率。

$\mathcal{A}$ 没有执行过对 ID_m 的 extract 询问的概率 $p_1 \geqslant (1 - 1/q_1)^{q_E}$；$\mathcal{A}$ 选择 ID_m 作为伪造阶段的签密者身份的概率 $p_2 \geqslant 1/q_1$，则 C 成功的概率至少为

$$\varepsilon' = \varepsilon p_1 p_2 \geqslant \varepsilon(1 - 1/q_1)^{q_E}(1/q_1) \approx \varepsilon e/q_1$$

在 $\mathcal{B}$ 的计算时间方面，每次 signcrypt 询问最多需要两次双线性对运算，所以 $t' \leqslant t + 2q_S t_e$，其中 t_e 表示计算一次双线性对运算所需要的时间。

推论 2 在随机预言模型和 CDHP 困难的假设下，改进的基于身份的签密方案在适应性选择消息和身份攻击下是存在性不可伪造的。

6.1.4 不可否认性

由定理 3 可知，只有拥有签密者 Alice 的私钥才能产生有效的签密密文，故签密者 Alice 不能否认他已经签密过的消息，即改进的基于身份的签密方案满足不可否认性。

6.1.5 公开验证性

改进方案的验证方程 $r = H_3(R, e(S, P)e(Q_A, P_{pub})^r, t)$ 中都是公开参数，可以由任何第三方直接验证，即改进的基于身份的签密方案满足公开验证性。

6.2 性能分析

将本文方案与已有基于身份的签密算法[4~10]进行计算效率和通信负载方面的比较。计算效率方面重点考虑计算消耗比较大的运算，主要有双线性对运算、群 G_1 中的标量乘运算和群 G_2 中的幂乘运算，分别用 P、M 和 E 表示；通信负载主要考虑传输密文的长度。具体比较数据如表 1 所示，其中 $x(+y)$ 表示需要 x 次对运算，y 次对预运算。可以看出，本文方案在增强安全性的同时，比文献[9,10]方案增加了运算量，但与文献[4~8]方案相比，计算量相差不大。

（下转第 920 页）

由表 2 可知,SVD-DWT 水印算法在没有受到攻击时,它的 PSNR 与 NC 都比较高,但受到攻击后,数值变化很大,抗攻击性很弱。SVD 与 DWT-SVD 算法的抗攻击性能比另外两种算法都要高,但 DWT-SVD 算法运算的时间更短。

DWT-SVD 算法被攻击后的提取水印图像如图 6 所示。

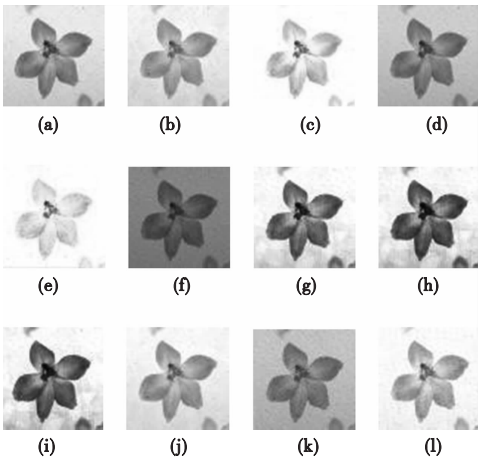

图6 攻击后的提取水印

由图 6 可知,DWT-SVD 算法在受到图 6(a) ~ (l)这 12 种攻击之后,其提取水印与原始水印仍有较高的峰值性噪比和相似度,验证了本算法的优点。

4 结束语

基于 DWT-SVD 的半盲彩色图像水印算法,对水印进行了双重保护:a) Arnold 图像置乱的系数 key;b) SVD 后的两个正交矩阵和原始水印的奇异值,使得水印的安全级别更高,很难被其他用户提取水印和更改水印,因此具有很高的实用价值。实验证明,本文算法对常见的攻击手段如压缩、剪切、常见的噪声干扰、几何变化等都具有良好的鲁棒性,抗攻击性能优越。

参考文献:

[1] 孙光民,于瑶,刘伟平,等. 基于小波变换的彩色图像多分量水印嵌入算法[J]. 北京工业大学学报, 2008, 34(5): 471-475.

[2] LIU Rui-zhen, TAN Tie-niu. An SVD-based watermarking scheme for protecting rightful ownership [J]. IEEE Trans on Multimedia, 2002, 4(1): 121-128.

[3] 周波,陈健. 基于奇异值分解的、抗几何失真的数字水印算法[J]. 中国图象图形学报, 2004, 9(4): 506-512.

[4] GANIC E, ESKICIOGLU A M. Robust embedding of visual watermarks using DWT-SVD[J]. IEEE Trans on Image Processing, 2004, 4(8): 1141-1146.

[5] SVERDLOV A, DEXTER S, ESKICIOGLU A M. Robust DCT-SVD domain image watermarking for copyright protection: embedding data in all frequencies[C]//Proc of the 13th European Signal Processing Conference. 2005: 4-8.

[6] BERGMAN C, DAVIDSON J. Unitary embedding for data hiding with the SVD[C]//Proc of IEEE Security, Steganography and Watermarking of Multimedia Contents VⅡ, SPIE 5681. 2005: 619-630.

[7] 许文丽,李磊,王育民. 抗噪声、几何失真和 JPEG 压缩攻击的鲁棒数字水印方案[J]. 电子与信息学报, 2008, 30(4): 933-936.

[8] 袁大洋,肖俊,王颖. 数字图像水印算法抗几何攻击鲁棒性研究[J]. 电子与信息学报, 2008, 30(5): 1251-1256.

[9] 王慧琴,崔福明,杜高峰. 利用 Arnold 变换和纠错编码实现盲数字水印[J]. 北京邮电大学学报, 2008, 31(1): 97-101.

[10] 刘挺,尤韦彦. 一种基于离散小波变换和 HVS 的彩色图像数字水印技术[J]. 计算机工程, 2003, 29(4): 115-117.

(上接第 916 页)

表 1 本文方案与其他方案的性能比较

方案	签密阶段			解签密阶段			密文长度
	P	M	E	P	M	E	
文献[4]	0(+1)	3	0	3(+1)	0	1	$2\|G_1\|+2\|m\|$
文献[5]	0(+2)	2	2	2(+2)	0	2	$\|G_1\|+\|m+\|q\|$
文献[6]	0(+1)	3	1	2(+2)	0	2	$2\|G_1\|+\|m\|$
文献[7]	0(+1)	3	1	3(+1)	0	1	$2\|G_1\|+\|m\|$
文献[8]	0(+1)	2	1	3(+1)	0	0	$2\|G_1\|+2\|m\|$
文献[9]	0(+1)	1	0	0(+1)	2	0	$\|m\|+2\|q\|$
文献[10]	0(+1)	1	1	1(+0)	1	0	$\|G_1\|+\|m\|+\|q\|$
本文方案	0(+2)	3	2	2(+1)	0	1	$2\|G_1\|+\|m\|+\|q\|$

7 结束语

本文对文献[10]提出的基于身份的改进高效签密方案进行了安全性分析,指出方案不能抵抗不可区分性选择明文攻击和不诚实接收者的一般性伪造攻击,并提出了一种改进方案。在随机预言模型下,证明了新方案在适应性选择密文攻击下具有不可区分性;在适应性选择消息和身份攻击下是存在性不可伪造的。

参考文献:

[1] SHAMIR A. Identity-based cryptosystems and signature schemes [C]//Advances in Cryptology-CRYPTO'84. Berlin: Springer-Verlag, 1984: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]//Advances in Cryptology- CRYPTO'01, LNCS, vol 2139. Berlin: Springer-Verlag, 2001: 213-229.

[3] ZHENG Yu-liang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [C]//Advances in Cryptology-CRYPTO'97, LNCS, vol 1294. Berlin: Springer-Verlag, 1997: 165-179.

[4] MALONE-LEE J. Identity-based signcryption [EB/OL]. (2002-07-09). http://eprint.iacr.org/2002/098.

[5] LIBERT B, QUISQUATER J. A new identity based signcryption schemes from pairings[C]//Proc of IEEE Information Theory Workshop. 2003: 155-158.

[6] 李发根,胡予濮,李刚. 一个高效的基于身份的签密方案[J]. 计算机学报, 2006, 29(9): 1641-1647.

[7] 张明武,杨波,周敏,等. 两种签密方案的安全性分析及改进[J]. 电子与信息学报, 2010, 32(7): 1731-1736.

[8] 李志敏,徐馨,李存华. 基于身份的公开验证签密方案[J]. 计算机应用, 2012, 32(1): 99-103.

[9] 张申绒,张玉清,李发根. 适于 Ad hoc 网络安全通信的新签密算法[J]. 通信学报, 2010, 31(3): 19-24.

[10] 肖鸿飞,刘长江. 一种基于身份的改进高效签密方案[J]. 计算机工程, 2011, 37(24): 126-128.

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