两种签密方案的安全性分析及改进

张明武[①] 杨 波[①] 周 敏[①] 张文政[②]
[①](华南农业大学信息学院 广州 510642)
[②](现代通信国家重点实验室 成都 610041)

摘 要：签密是能够在同一算法中提供认证性和机密性的密码方案，而所需要的计算量、通信成本和密文长度比“先签名后加密”的分开来实现要低，有较多的实际应用需求。多签密方案是多个签密者对同一明文执行签密操作。该文分析了两个签密方案：Li 等(2006)提出的签密方案和 Zhang 等(2008)提出的多签密方案，并通过选择明文攻击证明二者不能不具有语义安全性，并在此基础上提出了改进的方案，采用隐藏消息明文方法抵抗选择明文攻击，采用多签密成员签名认证的方法防止多成员签密密文被篡改，可抵抗选择明文攻击和选择身份攻击，达到语义安全性。

关键词：签密；选择明文攻击；语义安全性；不可伪造性
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2010)07-1731-06
DOI: 10.3724/SP.J.1146.2009.00911

Analysis and Improvement of Two Signcryption Schemes

Zhang Ming-wu[①] Yang Bo[①] Zhou Min[①] Zhang Wen-zheng[②]
[①](*College of Informatics*, *South China Agricultural University*, *Guangzhou* 510642, *China*)
[②](*National Laboratory for Modern Communications*, *Chengdu* 610041, *China*)

Abstract: Signcryption is a cryptographic primitive that simultaneously performs the functions of both digital signature and encryption in a way that is more efficient than signing and encrypting separately. Multi-signcryption is an extension of signcryption scheme for multi-signers performing together the signcryption operation on the same message. Two signcryption schemes, including signcryption proposed by Li et al.(2006), and multi-signcryption scheme by Zhang et al.(2008), are proved not to resist on chosen-plaintext attack and chosen-identity attack under the CPA adversary. Furthermore, the improved signcryption and multi-signcryption schemes are put forward that providing security properties including CPA, CCA2, and public verifiability, which deploy the message hidden method to resist on the chosen-plaintext attack, and multiple signer members authentication to protect the multi-signers' ciphertexts not be interpolated.

Key words: Signcryption; Chosen Plaintext Attack; Semantic Security; Unforgeability

1 引言

签密(Signcryption)最早由 Zheng 等人提出[1]，用于解决在同一个方案中既实现消息的保密又实现对消息的认证，但计算量、密文长度和通信成本等比传统的“先签名再加密”的分开实现方案要低。在 Boneh 等人提出基于椭圆曲线上的双线性对来实现一个实用的基于身份的签名方案后，基于身份的密码技术得到很大的发展。在 2002 年 Malone-Lee[2] 构造出第一个基于身份的签密方案后，陆续提出了多种的基于身份的签密方案，如短签密方案[3]、多签密方案[4,5]、多接收者签密方案[6]、基于策略的签密方案[7]、保护密钥隐私的签密方案[8,9]等。

Libert 和 Quisquator[10]指出文献[2]中方案不具有语义安全性，因为消息明文在密文中是可得到的，Barreto 等人[11]提出一种效率非常高的基于身份的签密方案，该方案基于 q 双线性 Diffie-Hellman 逆(q-BDHI)问题，文献[12]提出了一种具有较高效率的基于身份的签密方案，文献[13]提出公开验证和密文认证的签密方案。文献[13]对签密方案的形式化证明和安全性定义作了总体描述，并提出了签密方案的所要达到的机密性、不可伪造性、公开验证性等。

文献[12]中 Li 等人提出一个基于身份的签密方案，所提出的方案比现有方案的计算效率要高。本文通过选择明文攻击，证明该方案不具有语义安全性。文献[4]中 Zhang 和 Mao 提出一种基于身份的多

2009-06-23 收到，2010-02-15 改回
国家自然科学基金(60773175，60973134)，广东省自然科学基金(9151064201000058) 和现代通信国家重点实验室基金(9140c1108020906)资助课题
通信作者：张明武 csmwzhang@gmail.com

签密方案，多个用户可以共同签密一个消息给接收者。本文通过选择明文攻击和选择身份攻击，证明该方案的安全性存在缺陷，不具有语义安全性，也不能抵抗群广播消息的篡改。文献[5]针对文献[4]提出了改进方案，可抵抗选择身份攻击，但并没有解决选择明文攻击且该方案不具有公开验证性。本文针对文献[4,5,12]的不足，采用隐藏明文和签密成员认证的方法，提出了相应的改进方案达到语义安全性。

2 签密方案模型及安全性定义

2.1 签密模型

一个基于身份的签密方案由 4 个概率多项式 PPT 算法组成。

Setup. 系统初始化。系统输入安全参数 1^k，PKG 产生系统主密钥 s 并公开参数 params。

KeyExtract. 密钥提取生成。输入一用户的身份串 $\mathrm{ID}_U \in \{0,1\}^*$，PKG 计算并生成用户的秘密钥 D_U。

Signcrypt. 签密算法。输入系统参数 params，一个待签密的消息明文 m，发送者的秘密钥 D_S 和接收者的身份 ID_R，算法生成密文 $\sigma = \mathrm{Signcrypt}(m, D_S, \mathrm{ID}_R)$。

Unsigncrypt. 解密验证算法。在输入系统参数 params，发送者的身份 ID_S 和接收者的密钥 D_R，以及给定的密文 σ ,系统解密明文，若成功则输出明文 m，否则解签密失败输出 $\perp$。

2.2 多签密模型

一个多签密模型与一般签密模型不同之处在于，签密算法中是由多个用户 $\mathrm{ID}_1,\cdots,\mathrm{ID}_n$ 的秘密钥 $D_1,\cdots,D_n$ 进行签密的，在解签密时，需要使用接收者的秘密钥 D_R 和 n 个签密者身份进行解密。

2.3 安全性定义

签密方案要达到的安全性满足机密性(Confidentiality)、不可伪造性(Unforgeability)和公开验证性(Public verifiability)。

定义 1 签密机密性。一个基于身份的(多)签密方案在自适应性选择密文攻击下具有不可区分性(IND-mSC-CCA2)，则此方案机密性达到语义安全性。

多项式有界敌手 A 在下面游戏 IND-mSC-GAME 中没有一个不可忽略的优势赢得游戏，则此签密方案是不可区分的。

(1)Setup。挑战者 C 以参数 k 作输入执行 Setup 算法，并将系统的参数 params 发送给敌手 A。

(2)询问 1。敌手 A 自适应地执行下列询问：

-KeyExtract 询问。A 选择一个身份 ID_U，挑战者 C 计算其秘密钥 $D_U = \mathrm{KeyExtract}(\mathrm{ID}_U)$，并发送给 A。

-(Multi)Signcrypt 询问。敌手选择发送者身份 ID_S (签密选择多个发送身份 $\mathrm{ID}_{S1},\cdots,\mathrm{ID}_{Sn}$)和一接收者身份 ID_R，C 计算 $\sigma = \mathrm{Signcrypt}(m, D_S, \mathrm{ID}_R)$(多签密 $\sigma = \mathrm{MultiSigncrypt}(m, \{D_{S1},\cdots,D_{Sn}\}, \mathrm{ID}_R)$)，并将密文 σ 发送给 A。

-Unsigncrypt 询问。A 选择一密文 σ，以及发送者身份 ID_S (对多签密选择多个发送身份 $\mathrm{ID}_{S1},\cdots,\mathrm{ID}_{Sn}$)和接收者的秘密钥 D_R，挑战者 C 执行 $\mathrm{Unsigncrypt}(\sigma, \mathrm{ID}_S, D_R)$(对多签密执行 $\mathrm{Unsigncrypt}(\sigma, \{\mathrm{ID}_{S1},\cdots,\mathrm{ID}_{Sn}\}, D_R)$)，并将结果返回给 A。

(3)在 A 执行有界多项式的上述询问后，A 选择两个相同长度的明文 m_0, m_1，以及希望挑战的发送者身份 ID_{S^*} (对多签密是 $\mathrm{ID}_{S1^*},\cdots,\mathrm{ID}_{Sn^*}$)和接收者 ID_{R^*}，这时要求敌手 A 没有对 ID_{R^*} 已作 KeyExtract 询问。

(4)挑战。挑战者 C 随机选取 $b \in \{0,1\}$，计算 $\sigma^* = \mathrm{Signcrypt}(m_b, D_{S^*}, \mathrm{ID}_{R^*})$ (对多签密 $\sigma^* = \mathrm{Signcrypt}(m_b, \{D_{S1^*},\cdots,D_{Sn^*}\}, \mathrm{ID}_{R^*})$)，并将结果发送给 A。

(5)询问 2。敌手 A 像询问 1 阶段一样执行多项式有界次询问，这次限制是他不能对密文 σ^* 作解签密询问，也不能对 ID_{R^*} 作密钥提取询问。

(6)猜测。A 输出值 b'，若 $b' = b$ 则敌手赢得游戏。

A 的优势定义为 $\mathrm{Adv}^{\text{IND-mSC-GAME}}(A) = |2\Pr(b' = b) - 1|$

定义 2 不可伪造性。如果没有任何有界多项式的敌手 A 以不可忽略的优势赢得下面的游戏 EUF-mSC-GAME，则这个基于身份的签密方案在自适应选择消息攻击下是抗存在性伪造的(EUF-mSC-CMA2)。

(1)与 IND-mSC-GAME 初始化过程一样，挑战者产生系统参数 params 并发送给敌手 A。

(2) A 执行与 IND-mSC-GAME 询问 1 相同的多项式有界询问。

(3) A 生成三元组 $(\sigma^*, \mathrm{ID}_{S^*}, \mathrm{ID}_{R^*})$，且这个元组中的 σ^* 不是由签密预言机产生，也没有对 ID_{S^*} 执行过 KeyExtract 询问。如果 $\mathrm{Unsigncrypt}(\sigma^*, \mathrm{ID}_{S^*}, D_{R^*}) \neq \perp$ 则敌手赢得游戏。

定义 3 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公开钥的配合下，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，则此方案具有公开验证性。

3　Li-Hu-Li 签密方案攻击及改进

3.1 Li-Hu-Li 签密方案[12]

Li-Hu-Li 所提出的签密方案如下：

-Setup. G_1 是由 P 生成的阶为 q 的循环加法群，G_2 是具有相同阶 q 的循环乘法群，$\hat{e}: G_1 \times G_1 \to G_2$ 是一双线性映射。定义 4 个安全的 Hash 函数：$H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \to Z_q$，$H_3: G_1 \to Z_q$，$H_4: G_2 \to \{0,1\}^l$。PKG 随机选取一主密钥 $s \in Z_q^*$，计算 $P_{\text{pub}} = sP$。系统保存主密钥 s，公开参数 $\text{params} = \{G_1, G_2, l, \hat{e}, P, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$。

-KeyExtract. 输入用户身份 ID_U，PKG 计算 $Q_U = H_1(\text{ID}_U)$ 和 $D_U = sQ_U$。PKG 将用户秘密钥 D_U 通过秘密通道传送给 ID_U。

-Signcrypt.为把消息 m 秘密发送给 ID_R，发送方 ID_S 执行：(1)随机选取 $k \in Z_q^*$，计算 $R = kP$ 和 $S = k^{-1}(H_2(m) \cdot P_{\text{pub}} + H_3(R) \cdot D_S)$; (2)计算 $\omega = \hat{e}(P_{\text{pub}}, Q_R)^k$ 和 $c = H_4(\omega) \oplus m$; (3)产生的密文 $\sigma = (c, R, S)$。

-Unsigncrypt. 当收到密文 $\sigma = (c, R, S)$ 后，接收者 ID_R 执行：(1)计算 $\omega = \hat{e}(R, D_R)$，恢复消息明文 $m = c \oplus H_4(\omega)$;(2)验证等式 $\hat{e}(R,S) = \hat{e}(P, P_{\text{pub}})^{H_2(m)} \cdot \hat{e}(P_{\text{pub}}, Q_S)^{H_3(R)})$，如果成立则接收明文 m，否则输出 $\perp$ 认为密文不合法。

3.2 对 Li-Hu-Li 方案的攻击

现描述对该方案的选择明文攻击。设敌手 A 选择两明文 m_0, m_1 和消息的发送者 ID_S 和接收者 ID_R，经过签密预言机 Signcrypt 产生密文 $\sigma^* = (c^*, R^*, S^*)$。$A$ 直接用明文 m_0 去验证等式 $\hat{e}(R^*, S^*) = \hat{e}(P, P_{\text{pub}})^{H_2(m_0)} \cdot \hat{e}(P_{\text{pub}}, Q_S{}^*)^{H_3(R^*)})$，若等式成立则密文 σ^* 是明文 m_0 的签密密文，否则是 m_1 的签密密文。

由于该方案采用消息明文直接在验证等中，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-mSC-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。

3.3 改进方案

为保持 Li-Hu-Li 的高效性，在不降低现有方案的计算效率情况下，对该方案作改进，以抗击该方案对选择明文攻击。改进方案如下：

-Setup. 与 Li-Hu-Li 方案类似，改进该方案中的 Hash 函数 $H_2: \{0,1\}^n \to G_1$ (n 是密文长度)，同时防止攻击者获取收发双方的共享会话密钥 ω 的部分信息，加入一对称加密算法 (E, D)。

-KeyExtract. 与一般基于身份的密码方案的密钥提取算法相同，PKG 计算用户身份是 ID_U 的公开钥 $Q_U = H_1(\text{ID}_U)$ 和秘密钥 $D_U = sQ_U$。

-Signcrypt. ID_S 签密消息 m 给 ID_R 时执行：(1)随机选取 $k \in Z_q^*$，计算 $R = kP$ 和 $\omega = \hat{e}(P_{\text{pub}}, Q_R)^k$; (2)计算 $c = E_{H_4(w)}(m)$ 和 $S = k^{-1}(H_2(c) + H_3(R) \cdot D_S)$; (3)产生的密文 $\sigma = (c, R, S)$。

-Unsigncrypt.接收者 ID_R 收到密文 $\sigma = (c, R, S)$ 后执行：(1)计算 $\omega = \hat{e}(R, D_R)$，恢复明文 $m = D_{H_4(\omega)}(c)$;(2)验证等式 $\hat{e}(R,S) = \hat{e}(P, H_2(c)) \cdot \hat{e}(P_{\text{pub}}, Q_S)^{H_3(R)})$，如果成立则接收明文 m，否则拒绝接收并输出 $\perp$。

安全性分析。方案中 $\omega = \hat{e}(P_{\text{pub}}, Q_R)^k$ 值只能由拥有秘密钥 D_R 者才能恢复，由于值 k 的随机性使得 ω 在 G_2 上均匀分布，在已知明文 m 和密文 c 的情况下，$c = D_{H_4(\omega)}(m)$ 仍对明文消息 m 有保密能力，无法恢复加会话密钥 $H_4(\omega)$，敌手无法获得对选择明文的猜测攻击。同时在验证等式中没有直接用消息密文进行验证，可防止选择明文攻击。而原有方案中 $H_4(\omega) = c \oplus m$，敌手可获得解密钥的部分信息，采用对称加密算法后，有拥有 c, m 情况下仍无法获得 ω 的有关信息。本改进方案与 Li-Hu-Li 方案的签密和解密的算法过程类似，在随机预言机模型下对选择密文攻击和选择消息攻击的安全性是相同的。因此，本方案具有抗选择明文攻击、语义安全性、不可伪造性和公开验证性。

公开验证性。任何第三方通过对密文 $\sigma = (c, R, S)$ 和签密发送者公开钥 Q_S 进行验证等式 $\hat{e}(R,S) = \hat{e}(P, H_2(c)) \cdot \hat{e}(P_{\text{pub}}, Q_S)^{H_3(R)})$ 是否成立来判断消息的是否由 Q_S 签发。验证参数全为公开参数，在验证过程中第三方不能获得更多的密文安全有关的知识。

4　Zhang-Mao 多签密方案攻击及改进

4.1 Zhang-Mao 多签密方案[4]

-Setup. 系统初始化算法与 Li-Hu-Li 方案类似，不同之处在于该方案只选取 3 个 Hash 函数：$H_1: \{0,1\}^* \to G_1$，$H_2: G_2 \to \{0,1\}^l$，$H_3: \{0,1\}^* \to Z_q$。

-KeyExtract. 密钥提取算法与 Li-Hu-Li 方案相同。

-MultiSigncrypt.给定明文 m，n 个签密者 $\text{ID}_{S1}, \cdots, \text{ID}_{Sn}$ 和一个接收者 ID_R，每个签密者执行：(1)随机选取 $x_i \in Z_q$，计算 $R_i = x_i P$，$\omega_i = \hat{e}(P_{\text{pub}}, Q_R)^{x_i}$，将 (R_i, ω_i) 秘密发给下一位签密者；(2)当收到其他人发来的 (R_i, ω_i) 后，ID_{Si} 计算 $R = \sum_{j=1}^{n} R_j$，$\omega = \prod_{j=1}^{n} \omega_j$，$c = H_2(\omega) \oplus m$，$S_i = x_i H_1(m) + H_3(R)$

$\cdot D_{S_i}$， $S=\sum_{j=1}^{n}S_j$;(3)生成密文 $\sigma=(c,S,R)$。

-Unsigncrypt. 接收者 ID_R 收到密文 σ=(c,S,R) 后执行：(1)计算 ω=$\hat{e}(R,D_R)$， m=$H_2(\omega)\oplus c$；(2)验证等式 $\hat{e}(S,P)$=$\hat{e}(R,H_1(m))\cdot\hat{e}\left(P_{\mathrm{pub}},\sum_{j=1}^{n}Q_{\mathrm{ID}_j}\right)^{H_3(R)}$，如果成立则接收明文 m，否则认为密文不合法输出 $\perp$。

4.2 对 Zhang-Mao 方案的攻击

对该方案的攻击有两种方法:方案中 Hash 函数 H_1 一方面用于 KeyExtract 中生成用户的公开钥 $Q_U=H_1(\mathrm{ID}_U)$，另一方面对消息明文签名 $S_i=x_iH_1(m)+H_3(R)\cdot D_{S_i}$，可以采用选择身份对本方案进行攻击。攻击方法是：敌手 A 选取 ID_{U^*} 并作为签密的接收方，然后选择两明文 m_0,m_1 (其中 $m_0=\mathrm{ID}_{U^*}$)，经过签密预言机产生密文 $\sigma^*=(c^*,R^*,S^*)$，A 计算 $\omega=\hat{e}(R,D_U)$，验证等式 $\hat{e}(S^*,P)=\hat{e}(R^*,Q_{U^*})\cdot\hat{e}\left(P_{\mathrm{pub}},\sum_{j=1}^{n}Q_{\mathrm{ID}_j}\right)^{H_3(R^*)}$ 是否成立，若成立则 σ^* 是 m_0 对应的密文，否则是 m_1 对应的密文，攻击成功。

另一种攻击方法是，敌手 A 选择两明文 m_0,m_1 和消息的发送者 $\mathrm{ID}_{S1^*},\cdots,\mathrm{ID}_{Sn^*}$ 和接收者 ID_{R^*}，经过签密预言机 MultiSigncrypt 产生密文 $\sigma^*=(c^*,R^*,S^*)$。A 直接用明文 m_0 去验证等式 $\hat{e}(S^*,P)=\hat{e}(R^*,H_1(m_0))\cdot\hat{e}\left(P_{\mathrm{pub}},\sum_{j=1}^{n}Q_{\mathrm{ID}_j}\right)^{H_3(R^*)}$，若等式成立则密文 σ^* 是明文 m_0 对应密文，否则是 m_1 的签密密文，攻击成功。

此外，本方案无法抵抗敌手篡改攻击，要求签密者向该群广播(R_i,ω_i)是在秘密信道中完成的，这在实际上比较困难，一旦(R_i,ω_i)被篡改，系统却无法检测，最后产生的密文接收方是无法通过解密验证的。

4.3 文献[5]对方案的改进

文献[5]针对文献[4]方案的不足，提出一种改进的方案：增加定义 $H_4:\{0,1\}^*\to G_1$，修改 $H_3:\{0,1\}^*\times G_2\to Z_q$，在签密算法中 S_i 计算是 $S_i=x_iH_1(m)+H_3(R,\omega)\cdot D_{S_i}$，验证时等式是 $\hat{e}(S,P)=\hat{e}(R,H_4(m))\cdot\hat{e}\left(P_{\mathrm{pub}},\sum_{j=1}^{n}Q_{\mathrm{ID}_j}\right)^{H_3(R,\omega)}$。

该方案可以抵抗选择身份攻击，但在验证时需要用到秘密值 ω，不具有公开可验证性。而且改进的方案仍不具有语义安全性，利用 4.2 节所述选择明文攻击，仍可以获得对两明文消息猜测的肯定优势。

4.4 改进的多签密方案

本文改进方案在多签密群内成员收到其他的(R_i,T_i,ω_i)时先验证其完整性，保证每个成员的签名没有被篡改，同时在本方案中隐藏消息明文，可抵抗选择明文攻击和选择身份攻击。改进的方案如下：

-Setup.PKG 产生满足双线性映射的阶为 q 的循环加法群 G_1 和循环乘法群 G_2，$\hat{e}:G_1\times G_1\to G_2$。选取的 4 个 Hash 函数：$H_1:\{0,1\}^*\to G_1$，$H_2:G_2\to\{0,1\}^l$，$H_3:\{0,1\}^l\to G_1$，$H_4:G_1\to Z_q^*$，选取一对称加密算法 (E,D)。随机选取一主密钥 $s\in Z_q^*$，计算 $P_{\mathrm{pub}}=sP$。系统保存主密钥 s，公开参数 $\mathrm{params}=\{G_1,G_2,l,\hat{e},P,P_{\mathrm{pub}},H_1,H_2,H_3,H_4,E,D\}$。

-KeyExtract.与 Zhang-Mao 方案相同。

-MultiSigncrypt.给定明文 m，n 个签密者 $\mathrm{ID}_{S1},\cdots,\mathrm{ID}_{Sn}$ 和一个接收者 ID_R，每个签密者执行：(1)随机选取 $x_i\in_R Z_q^*$，计算 $R_i=x_iP$，$\omega_i=\hat{e}(P_{\mathrm{pub}},Q_R)^{x_i}$，$T_i=x_iP_{\mathrm{pub}}+D_i$，$k_i=H_2(\omega)$，将(Q_i,R_i,T_i,ω_i)发给其他签密者;(2)当收到其他人发来的(R_i,T_i,ω_i)后，ID_{Si} 验证 $\hat{e}(T_i,P)=\hat{e}(R_i,P_{\mathrm{pub}})\hat{e}(Q_i,P_{\mathrm{pub}})$；(3)若等式成立则计算 $R=\sum_{j=1}^{n}R_j$，$\omega=\prod_{j=1}^{n}\omega_j$，$k=H_2(\omega)$，$c=E_k(m)$，$S_i=x_iH_3(c)+H_4(R)D_{S_i}$，$S=\sum_{j=1}^{n}S_j$；(4)生成密文 $\sigma=(c,S,R)$。

-Unsigncrypt.收到密文 $\sigma=(c,S,R)$ 后 ID_R 执行：(1)计算 $k=H_2(\hat{e}(R,D_R))$，$m=D_k(c)$；(2)验证等式 $\hat{e}(S,P)=\hat{e}(R,H_3(c))\cdot\hat{e}\left(\sum_{j=1}^{n}Q_{\mathrm{ID}_j},P_{\mathrm{pub}}\right)^{H_4(R)}$，若等式成立则接收 m。

4.5 改进方案的安全性证明

定理 1 在随机预言模型下，假设存在敌手 A 以 $(q_{H1},q_{H2},q_{H3},q_{H4},q_S,q_U,\varepsilon)$ 的优势攻破本文方案，则存在算法 B，以 $\frac{e}{q_{H_1}q_U}\varepsilon$ (这里 e 是指数)的优势解决 DBDH 问题。

证明 设 B 收到 G_1 中 DBDH 实例 (P,aP,bP,cP,h)，算法 B 调用 A 为子程序去判断 $(P,aP,xe(P,P)^{abc}$ 是否成立。B 扮演 A 的挑战者并建立模拟 IND-CCA 环境如下：

(1)B 将 aP 作为系统公开钥 P_{pub}；

(2)B 维护 hash 预言机 $\mathrm{H_1}$，$\mathrm{H_2}$，$\mathrm{H_3}$，$\mathrm{H_4}$ 列表 $\mathrm{L_1}$，$\mathrm{L_2}$，$\mathrm{L_3}$ 和 $\mathrm{L_4}$。

$\mathrm{H_1}$ 询问。当 A 作 $H_1(\mathrm{ID}_j)$第 $j(j\in[1,q_{H1}])$ 次询问时，B 首先在 $\mathrm{L_1}$ 中查找该元组是否存在。若存在则返回 $\mathrm{H_1}$ 相应值，否则 B 随机选取 $b_j\in Z_q$，返回 b_jP 给 A，且将 b_jP 保存在 $\mathrm{L_1}$ 中。对于第 $i(i\neq j,1\le i\le q_{H1})$ 次询问时，B 应答 $\mathrm{H_1}(\mathrm{ID}_i)$=$bP$。

$\mathrm{H_2}$，$\mathrm{H_3}$，$\mathrm{H_4}$ 询问。对于 $\mathrm{H_2}$-$\mathrm{H_4}$ 的预言机询问，B 首先检查 $\mathrm{L_2}$，$\mathrm{L_3}$ 或 $\mathrm{L_4}$ 中是否已有询问过的元组，若有则返回相应值，否则于应用群中随机选取一元

素，返回该值并在对应表中添加该元组。

密钥提取询问。敌手 A 对 ID_j作密钥提取询问，若 $i=j$ 则询问失败并返回；否则随机选取 $b_j \in Z_q$，并返回 $b_j P_{\mathrm{pub}}$。

签密询问。对于身份列表 $(\mathrm{ID}_1,\cdots,\mathrm{ID}_n)$ 对消息 $m \in \{0,1\}^n$ 进行多签密询问，B 作如下应答: 若 $\mathrm{ID}_b = \mathrm{ID}_i$，随机取选 $w \in Z_q$，计算 $R = wP_{\mathrm{pub}}$，$c = E_{H_2(e(wP_{\mathrm{pub}},Q_{\mathrm{ID}_b}))}(m)$，检查 L_3 中是否存在对 c 的询问，若存在则失败并返回，否则随机选取 $u \in Z_q$，计算 $H_3(c) = uP - w^{-1}x\sum H_1(\mathrm{ID}_j)$，并置 $S = uwP_{\mathrm{pub}}$；若 $\mathrm{ID}_b \neq \mathrm{ID}_i$，则随机取选 $w \in Z_q$，计算 $R = w\sum H_1(Q_{\mathrm{ID}_j})$，检查 L_3 中是否存在对 c 的询问，若存在则失败并返回，否则随机选取 $u \in Z_q$，计算 $c = E_{H_2(e(R,S_{\mathrm{ID}_j}))}(m)$，$H_3(c) = uP - w^{-1}H_4(R)P_{\mathrm{pub}}$，$S = uwP$。

解签密询问。当 B 收到一个密文的解签密询问时，B 执行: 若 $\mathrm{ID}_b = \mathrm{ID}_i$ 则 B 回答密文为非法密文; 若 $\mathrm{ID}_b \neq \mathrm{ID}_i$，$B$ 首先调用密钥提取预言机获得 ID_b 密钥，然后计算 $\omega = e(R,S_{\mathrm{ID}_b})$，$m = D_{H_2(\omega)}(c)$，验证 $\hat{e}(S,P) = \hat{e}(R,H_3(c))\cdot\hat{e}\left(\sum_{j=1}^{n} Q_{\mathrm{ID}_j}, P_{\mathrm{pub}}\right)^{H_4(R)}$。

在有界的上述询问阶段结束后，A 输出长度相同的消息明文 $m_0, m_1 \in \{0,1\}^n$ 及发送者私钥 SK_A 和接收者公钥 PK_B，B 置 PK_B=bP，$R^* = cP$，随机选取 $b \in \{0,1\}$，将挑战密文 $\sigma_b^* = (c,S^*,R^*)$发送给 A。

猜测阶段。敌手 A 继续执行有界的 hash 询问、签密和解签密询问，这时不能对 σ_b^* 进行解签密询问。询问结束后，若敌手得到猜测的 $b' = b$，则 B 能输出 $h = e(R^*,S_{\mathrm{ID}_i}) = e(cP,abP) = e(P,P)^{abc}$ 解决 DBDH 的判定性问题。

B 成功的概率。要求在所有询问都成功的情形下敌手 A 能获得合法的猜测。敌手 A 在密钥提取询问中全部成功的概率 $P_1 \geq (1-1/q_{H_1})^{q_{H_1}}$，在签密阶段不失败的概率 $P_1 \geq 1/q_U$，解签密阶段密提取预言机不失败的概率 $P_3 \geq 1/q_{H_1}$ 则 B 成功的概率至少为

$$\varepsilon' \geq \varepsilon\frac{(1-1/q_{H_1})^{q_{H1}}}{q_{H_1}q_U} \approx \frac{e}{q_{H_1}q_U}\varepsilon$$

定理 2　任何第三方可以公开验证密文的签名身份。

任何第三方收到密文 $\sigma = (c,S,R)$ 后，检验等式 $\hat{e}(S,P) = \hat{e}(R,H_3(c))\cdot\hat{e}\left(\sum_{j=1}^{n} Q_{\mathrm{ID}_j}, P_{\mathrm{pub}}\right)^{H_4(R)}$ 是否成立，若成立则证明密文的签发者是 $Q_{\mathrm{ID}_j}(1 \leq j \leq n)$ 所共同签发，验证者不能获得其它有用信息，同时只有拥有密钥 D_R 的接收者才能解开明文 $m = D_{H_2(e(R,D_R))}(c)$。

5　结束语

本文在对分析基于身份的签密方案的基本安全模型的基础上，对两种基于身份的签密方案的安全性作了分析，并证明这两种方案不能抵抗选择明文和选择身份攻击，在此基础上，采用隐藏消息明文和多签密认证的方法提出改进的方案。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to archieve cost (signature & encryption) <<cost(signature) +cost (encryption)[C]. Advance in Cryptology- Crypto'97, 1997, LNCS 1294: 165–179.

[2] Malone-Lee J. Identity based signcryption[EB/OL]. Cryptology ePrint Archieve, Report 2002/098, IACR, 2002.

[3] Ma C. Efficient short signcryption with public verifiability[C]. Indoscrypt06, 2006, LNCS 4318: 118–129.

[4] Zhang J and Mao J. A novel identity-based multi-signcryption scheme[J]. *Computer Communications*, 2008, 32(6): 14–18.

[5] Zhang J, Yang Y, and Niu X. A novel identity-based multi-signcryption scheme[J]. *International Journal of Distributed Sensor Networks*, 2009, 5(1): 28.

[6] Duan S and Cao Z. Efficient and provably secure multi-receiver identity-based signcryption[C]. ACISP06, 2006, LNCS 4058: 195–206.

[7] 张明武, 杨波, 祝胜林, 张文政. 保护协商证书隐私的策略签名方案[J]. 电子与信息学报, 2009, 31(1): 224–227.
Zhang Ming-wu, Yang Bo, Zhu Sheng-lin, and Zhang Wen-zheng. Protect negotiation privacy policy signature scheme[J]. *Journal of Electronics & Information Technology*, 2009, 31(1): 224–227.

[8] Selvi S S D, Vivek S S, and Gopalakrishnan R. Cryptanalysis of Mu et al.'s and Li et al.'s schemes and a provably secure ID-based broadcast signcryption (IBBSC) scheme. WISA09, 2009, LNCS 5379: 115–129.

[9] Zhang J, Gao S, Chen H, and Geng Q. A novel ID-based anonymous signcryption scheme. APWeb/WAIM 09, 2009, LNCS 5446: 604–610.

[10] Libert B and Quisquater J. A new identity based signcryption schemes from pairings[C]. Proceeding of the 2003 IEEE Information Theory Workshop, Paris, France, 2003: 155–158.

[11] Barreto P S, Libert B, and McCullagh N, *et al*.. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]. AsiaCrypt2005, 2005, LNCS 3788: 515–532.

[12] 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, 26(9): 1641–1647.
Li Fa-gen, Hu Yu-pu, and Li Gang. An efficient identity-based signcryption scheme[J]. *Chinese Journal of Computers*, 2006, 29(9): 1641–1647.

[13] Baek J, Steinfeld R, and Zheng Y, *et al*.. Formal proofs for the security of signcryption[J]. *Journal of Cryptology*, 2007, 20(2): 203–235.

张明武： 男，1970 年生，博士，副教授，研究方向为分布式网络与信息安全、信任与隐私保护.

杨 波： 男，1963 年生，教授，博士生导师，研究方向为密码学与信息安全、可信计算.

周 敏： 女，1973 年生，博士生，研究方向为密码学与信息安全、安全多方计算.

张文政： 男，1966 年生，高级工程师，研究方向为密码技术、网络与信息安全.