# 对 2 种签密方案的分析与改进

卞洋洋，殷肖川，赵雪岩，谭　韧
(空军工程大学信息与导航学院,西安,710077)

**摘要**　针对 Zheng 签密方案和 SK 签密方案存在的不足,从安全性和效率 2 个方面出发,利用通过签密信息和一些公开信息可以恢复出解签密所需要的信息这一原理,分别提出改进方案。利用求解单向函数的困难性对 Zheng 签密方案进行改进,与原方案相比在不影响效率的情况下,在安全性上有了很大的提高,使其具有了前向安全性和公开验证性;采用椭圆曲线上的双线性对和基于身份的密码技术对 SK 签密方案进行改进,使改进后的方案在安全性和效率上都有了很大的提高,具有了公开验证性并降低了通信代价和计算代价。通过分别对改进后的方案进行分析及推导验证,改进后的方案不仅能够满足签密的基本要求,并且在安全性和效率上都得到了提高。

**关键词**　签密;前向安全性;公开验证性;单向函数;基于身份
**DOI**　10.3969/j.issn.1009-3516.2016.03.020
**中图分类号**　TP393　　**文献标志码**　A　　**文章编号**　1009-3516(2016)03-0106-06

## An Analysis and Improvement of Two Sign-cryptic Schemes

BIAN Yangyang, YIN Xiaochuan, ZHAO Xueyan, TAN Ren
(Information and Navigation College, Air Force Engineering University, Xi′an 710077,China)

**Abstract**: Aimed at the deficiencies of Zheng sign cryptic scheme and SK sign cryptic scheme, this paper proposes improved schemes respectively by utilizing the principle, i.e. sign cryptic information and open information for restoring the information needed by sign de-cryptic scheme to the needs of safety and efficiency. The difficulty of solving one-way function is utilized to improve Zheng sign cryptic scheme. The security has been greatly improved compared with the original scheme without affecting the efficiency of the case, and has forward security and public verifiability. The bilinear pairing of elliptic curve and identity-based cryptosystem are used to improve SK sign cryptic scheme, and the safety and the efficiency of the improved scheme both have been greatly improved with the public verifiability, and the communication cost and the computation cost are reduced. The results show that the safety and the efficiency of the improved schemes have been improved and meet the basic requirements of sign cryptic scheme.

**Key words**: sign cryptic; forward security; public verifiability; one-way function; identity-based

1997 年,Zheng[1]第 1 次提出签密,使签名和加密可以同时实现,且其效率和安全性明显超过传统的“先签名后加密”方案。在其之后,针对不同应用情景的各种签密方案相继被提出,比如群签密、盲签

**收稿日期**:2015-11-23
**基金项目**:陕西省自然科学基金(2015JM6340)
**作者简介**:卞洋洋(1991—),男,河南灵宝人,硕士生,主要从事网络安全与信息对抗研究.E-mail:byy902@163.com

*引用格式*:*卞洋洋,殷肖川,赵雪岩,等. 对 2 种签密方案的分析与改进[J]. 空军工程大学学报:自然科学版,2016,17(3):106-111. BIAN Yangyang, YIN Xiaochuan, ZHAO Xueyan, et al. An Analysis and Improvement of Two Sign-cryptic Schemes[J]. Journal of Air Force Engineering University: Natural Science Edition,2016,17(3):106-111.*

密、代理签密等等[2-5]。在众多方案中，有一种比较特殊的签密方案[6]：SK 签密方案。该方案最重要的一点就是可以将同一消息发送给不同人，但每个人只能解密出属于自己的那一小部分信息，而不能干涉其他人的信息。这一特点使得其在信息产业日益发达的今天，有着非常广阔的应用前景。

然而，通过对上述 2 个签密方案的分析，发现 Zheng 方案满足一般签名和加密所具有的特征，但不具有前向安全性和公开验证性；且 SK 方案也不满足可公开验证性的要求。针对 Zheng 方案不足，张串绒等人[7]给出了修改方案，该修改方案只具有前向安全性，不具有公开验证性[8-10]；对 SK 方案存在的安全缺陷，肖国镇[11]等人提出了一种改进方案，但该方案不具有公开验证性。

本文在对 Zheng 方案进行分析的基础上，利用求解单向函数问题的困难性方法对其进行改进，使得改进后的方案具有前向安全性和公开验证性；对 SK 方案进行深入分析，在基于身份的密码体制[12-14]基础上，结合椭圆曲线上的双线性对[15]给出了一种基于身份的并具有可公开验证性的改进方案。该改进方案特点是其可以使用任何公开信息作为用户公钥，例如用户的证件号码、姓名、E-mail 地址、IP 地址等等。并可以实现自动目录查询，而不需要代价昂贵、繁琐的认证和发布公钥的步骤。

# 1　预备知识

签密涉及到现代密码学和数学的许多知识，如公钥密码、数字签名、加密、单向函数、Hash 函数以及基于身份的密码体制等等。

## 1.1　数学基础知识

**定义 1**　单向函数：一个函数可以表示为：$f(x):D\to F$，则称其为单向函数，如果满足：对任意的 $x\in D$，可以高效地计算 $f(x)$；而对几乎所有的 $y\in F$，求解 $x$ 使得 $f(x)=y$ 是困难的。

**定义 2**　双线性对：设 $G_1$ 和 $G_2$ 对 $e:G_1\times G_1\to G_2$ 满足以下条件：

1)双线性：

对任意 $P,Q_1,Q_2\in G_1$ 有：$e(P,Q_1)\cdot e(P,Q_2)=e(P,Q_1+Q_2)$，对任意 $P_1,P_2,Q\in G_1$ 有：$e(P_1,Q)\cdot e(P_2,Q)=e(P_1+P_2,Q)$。

2)非退化性：

存在 $P\in G_1$，使：$e(P,P)\neq 1$。

3)可计算性：

对任何 $P,Q\in G_1$，存在有效的算法 $e(P,Q)$，就称 $e$ 是双线性对或双线性变换，即满足：$e(aP,Q)=e(P,aQ)=e(P,Q)^a$。

## 1.2　基于身份的密码体制

公钥密码体制是使用不同的密钥进行加密和解密，该密码体制的特点是不可能由加密密钥求解出解密密钥。但公钥密码体制最大的问题是对可信第 3 方（管理用户的身份以及所对应的公钥信息）的维护，当用户数量过多，频繁访问会使可信第 3 方的服务能力下降，对其存储能力也是一个巨大的挑战。

为了解决以上问题，Shamir[16]提出了一种新的密码技术——基于身份的密码体制，让用户的身份作为公钥，所谓身份，就是指跟用户相关的信息，比如身份证号、姓名、邮箱地址等等。这样加密者就不需要向可信第三方询问接收者的公钥，极大的方便了公钥信息的管理。例如，Bob 可将自己的邮箱地址 Bob@bob.space 作为他的身份信息，当 Alice 需要向 Bob 发送消息时，使用该身份信息 Bob@bob.space 作为公钥进行加密即可。

# 2　Zheng 方案及改进方案

## 2.1　Zheng 方案分析

传统实现通信消息保密和认证功能的方法，花费代价比较大。为了提高效率，Zheng 于 1997 年首次提出了签密方案，相比传统方案，签密有较小的计算复杂度，同时也具有较小的消息扩展等优势。

### 2.1.1　Zheng 签密方案

Zheng 的签密方案 SCS 公开的 3 个系统参数：① $p$：大素数；② $q$：$p-1$ 的一个素因子；③ $g$：$[1,2,\cdots,q-1]$ 中阶为 $q \bmod p$ 的整数。

hash 是一种单向散列算法，KH 是一个带有钥控的单向散列算法，$(E_k,D_k)$ 表示一种对称密码方案。这样 SCS 的全部公共参数为：$(p,q,g,\text{hash},\text{KH},E_k,D_k)$。

假定 Alice 的私钥为 $x_a$ 和公钥为 $y_a=g^{x_a}\bmod p$，Bob 的私钥为 $x_b$ 和公钥为 $y_b=g^{x_b}\bmod p$，他们执行如下算法。

签密算法：

1)从 $[1,2,\cdots,q-1]$ 中随机选取 $x$，令 $k=\text{hash}(y_b{}^x \bmod p)$，将 $k$ 有选择地分为 $k_1$ 和 $k_2$；

2) $\theta=E_{k_1}(m)$；

3) $r=\text{KH}\,k_2(m)$；

4) $s=x/(r+x_a)\bmod q$。

输出 $(\theta,r,s)$，并将其发送给 Bob。

解签密算法：

1)利用 $r$、$s$、$g$、$p$、$y_a$、$x_b$ 通过计算 $k=\text{hash}[(y_a\cdot g^r)^{s\cdot x_b}\bmod p]$ 恢复出 $k$；

2)将 $k$ 分成 $k_1$ 和 $k_2$。

3) $m=D_{k_1}(\theta)$。

4)当 $\mathrm{KH}_{k_2}(m)=r$ 时,说明 Alice 发出的消息是无误的,此时再输出 $m$,否则丢弃消息。

2.1.2 Zheng 方案性能分析

安全性分析:机密性和不可伪造性,是一般密码学最基本的特征,在此不再赘述。在验证消息时,Bob 利用自己的私钥 $x_b$ 解出 $k$,但在运算过程中会发现有以下等式成立:$k=\mathrm{hash}(y_a\cdot g^r)^{s\cdot x_b}\bmod p=\mathrm{hash}(y_b{}^{x_a+r})^s\bmod p$,假设 Alice 的私钥 $x_a$ 泄露,那获得 $x_a$ 的任何人都可以通过上式求解出 $k$,这样攻击者就能对签密消息进行解签密获得本次通信的秘密信息,进而获得双方的通讯密钥,即 Zheng 方案不具备前向安全性。此外,在求解 $k$ 时不可避免的用到了私钥 $x_b$,也就是说只有接收方 Bob 才能对签名进行验证,所以该方案不具备公开验证性。

效率分析:Zheng 方案操作所得密文 $(\theta,r,s)$ 的消息扩展为:$|H(\cdot)|+|q|$。在计算中,主要操作包括 3 次模运算,3 次哈希运算,2 次加/解密运算,比其他的先签名后加密方案所耗的代价低。

因此,该方案只具有不可伪造性和机密性,远远不能满足实际的应用需要。但在效率上与其它方法相比还是有了很大的提高。

### 2.2 针对 Zheng 的改进方案

文献[7]中,提出对 Zheng 签密方案的改进算法,但该算法只具备前向安全性,不具备公开验证性。本节在原方案的基础上,利用求解单向函数的困难性,提出一种对 Zheng 方案的改进算法,不仅使其具有前向安全性而且也具有公开验证性。

2.2.1 改进方案的签密算法

改进方案参数同 2.1.1 所述相同。原方案中,用于认证和加密的密钥 $k_1$ 和 $k_2$ 都源于密钥 $k$,一旦密钥 $k$ 泄露,那签密消息就会泄露。因此,在该方案中,分别独立求取 $k_1$ 和 $k_2$,但又相互结合使用,并且利用求单向函数的困难性引入参数 $S$,即使密文消息被黑客获取,其仍然无法求得密钥 $k_1$,进而无法求得密钥 $k_2$,提高了密文的机密性,同时也实现了认证功能。

签密算法:

1)从 $[1,2,\cdots,q-1]$ 中随机选取 $x$,计算:$k_1=g^x\bmod p$,$k_2=\mathrm{hash}(y_b{}^x\bmod p)$;

2)计算 $c=E_{k_2}(m)$;

3) $r=\mathrm{KH}_{k_1}(c)$;

4) $x=(s+x_a)\bmod q\Rightarrow s$,$S=g^s\bmod p$;

5)输出 $(c,r,S)$,并将其发送给 Bob。

解签密算法:

1)Bob 收到消息对 $(c,r,S)$ 后,计算:$k_1=(S\cdot y_a)\bmod p$,$k_2=\mathrm{hash}(k_1{}^{x_b}\bmod p)$;

2)解签密 $m=D_{k_2}(c)$;

3)当且仅当 $r=\mathrm{KH}_{k_1}(c)$ 成立时,接受 $m$;否则,丢弃。

Bob 接收到消息后,用已知公开信息求解 $k_1$,再进一步利用自己的私钥解出 $k_2$,当验证成功时,接受 $m$;否则,拒绝接受。

2.2.2 针对改进方案的分析

在改进方案中,发送的密文信息 $(c,r,S)$ 隐含了密钥 $k_1$ 和 $k_2$ 对消息的认证和加密功能,具备了签密最基本的特征。若利用签密消息和公开信息可以得出解签密所需要的信息,则可说明该改进方案算法正确。

在签密时用到的密钥为 $k_1$ 和 $k_2$,在解签密算法中,接收者利用已知信息和公开信息求得解签密密钥 $k'_1$ 和 $k'_2$,若 $k'_1=k_1$ 且 $k'_2=k_2$,则可以证明上述结论。

**第 1 步** 求得解出验证密钥的关键元素 $g^s$。

$$x=(s+x_a)\bmod q\Rightarrow$$
$$g^x=g^{(s+x_a)}\bmod p\Rightarrow$$
$$g^x=g^s\cdot g^{x_a}\bmod p\Rightarrow$$
$$g^s=g^{x-x_a}\bmod p \tag{1}$$

**第 2 步** 求得 $k'_1$,验证 $k'_1=k_1$ 是否成立。

$$k'_1=(S\cdot y_a)\bmod p=(g^s\cdot g^{x_a})\bmod p \tag{2}$$

将式(1)代入式(2),得到:

$$k'_1=g^x\bmod p=k_1$$

**第 3 步** 求得 $k'_2$,验证 $k'_2=k_2$ 是否成立。

$$k'_2=\mathrm{hash}(k_1{}^{x_b}\bmod p)=\mathrm{hash}[(S\cdot y_a)^{x_b}\bmod p]=\mathrm{hash}[(g^{s+x_a})^{x_b}\bmod p] \tag{3}$$

将式(1)代入式(3),可得:

$$k'_2=\mathrm{hash}(y_b{}^x\bmod p)=k_2$$

通过上述证明可以看出,得到预想要的结果。所以,该方案正确。

安全性分析:计算 $k_1=(S\cdot y_a)\bmod p$,其中所用信息都是公开的,即任何人均可求得,不需要用发送者或接受者的私钥,所以任何人都可以用公开信息和签密消息进行验证,且验证过程中不会泄露消息 $m$。因此,该方案具有公开验证性。假设 Alice 的私钥 $x_a$ 不小心被盗,黑客计算:$k_2=\mathrm{hash}(k_1{}^{x_b}\bmod p)=\mathrm{hash}(g^s\cdot g^{x_a})^{x_b}\bmod p=\mathrm{hash}(y_b{}^{(s+x_a)}\bmod p)$ 由于攻击者不知道 Bob 的私钥 $x_b$ 或者 $s$,也就不能解出加密密钥 $k_2$,无法对密文 $c$ 进行解密,所以该方案具有前向安全性。

效率分析:改进后的方案消息扩展为

$|H(\cdot)|+|p|$，比改之前的方案仅多了 $|p|-|q|$ 比特。在效率上比原方案主要多了一次模幂运算，少了一次模乘和一次模除，代价略有所加大，但比传统方案仍有很大优势，见下表 1。

**表 1　改进方案与其他方案效率比较**

Tab.1　Comparison of improved scheme with other schemes

| 方案 | 计算代价 | 消息扩展 |
|---|---|---|
| S 签+E 密 | $E=6,M=2$<br>$D=0,A=1$<br>$H=2,N=2$ | $\|H(\cdot)\|+\|p\|+\|q\|$ |
| D 签+ E 密 | $E=6,M=2$<br>$D=3,A=1$<br>$H=2,N=2$ | $2\|q\|+\|p\|$ |
| Zheng 签密 | $E=3,M=2$<br>$D=1,A=1$<br>$H=4,N=2$ | $\|H(\cdot)\|+\|q\|$ |
| 改进方案 | $E=4,M=1$<br>$D=0,A=1$<br>$H=4,N=2$ | $\|H(\cdot)\|+\|p\|$ |

表 1 中，S 签 + E 密表示 Schnorr 签名 + ElGamal 加密；D 签+E 密表示 DSS 签名+ElGamal 加密；$E$ 为模幂运算次数；$M$ 为模乘运算次数；$D$ 为模除运算次数；$A$ 为模加或模减运算次数；$H$ 为应用哈希次数；$N$ 为对称密码算法加解密次数。

通过以上分析，改进后的方案安全性有了明显提高，具有了不可否认性和前向安全性；效率上比其他方案仍有较大优势。

## 3　SK 签密方案及改进方案

### 3.1　SK 签密方案分析

SK 签密特点是可以将同一消息发送给不同人，但每个人只能解密出属于自己的一小部分信息，而不能干涉其他人的信息。这一特点使得其在信息产业日益发达的今天，有着非常广阔的应用前景。

#### 3.1.1　SK 签密方案

该方案中，$x_a$ 和 $y_a=g^{x_a} \bmod p$ 是发送者 Alice 的私钥和公钥，$x_{bi}$ 和 $y_{bi}$ 分别是接收者 $B_i$ 的私钥和公钥，其中 $i=1,2,\cdots,n$；$\|$ 表示级联，其余参数与 2.1.1 所述方案相同。

Alice 对 $m_i$ 签密，并将其发送给 $B_i(i=1,2,\cdots,n)$，并且，当 $i\neq j$ 时，不能解密出 $m_j$，其算法如下：

1）随机选取 $x\in Z_q^*$；

2）计算：

$k=\mathrm{hash}(g^x \bmod p)$，

$k_i=\mathrm{hash}(y_{bi}{}^x \bmod p)$，

$c_i=E_{k_i}(m_i)$，

$r_i=\mathrm{KH}_k(c_1\|c_2\|\cdots\|m_i\|\cdots\|c_n)$ $(i=1,2,\cdots,n)$，

$s=x/(r_1r_2\cdots r_n+x_a) \bmod p$；

3）Alice 将 $(c_1,c_2,\cdots,c_n,r_1,\cdots,r_n,s)$ 给 $B_i$。

解签密算法：$B_i$ 接收到 Alice 发来的消息后，作如下计算：

1）$t=(y_a g^{r_1\cdots r_n})^s \bmod p$，

$k=\mathrm{hash}(t)$，

$t_i=t^{x_{bi}} \bmod p$，

$k_i=\mathrm{hash}(t_i)$，

$m_i=D_{k_i}(c_i)$；

2）证 $r_i=\mathrm{KH}_k(c_1\|c_2\cdots\|m_i\|\cdots\|c_n)$ 是否成立；如果成立，$B_i$ 接收密文；否则，拒绝接收。根据需要，$B_i$ 还可将密文信息 $(c_1,c_2,\cdots,c_n,r_1,r_2,\cdots,r_n,s)$ 发送给 $B_j$，$B_j$ 用相同方法解密出 $m_j$，并验证密文的有效性。

#### 3.1.2　SK 签密方案的安全性分析

该方案的验证式是：$r_i=\mathrm{KH}_k(c_1\|c_2\cdots\|m_i\|\cdots\|c_n)$，当接收者必须解密出消息 $m_i$ 后，才能进行下一步的验证，这样就泄露了消息 $m_i$。因此，该方案不具有公开验证功能。文献[11]中，肖国镇等人提出了一种对 SK 方案的改进方案，使其具有前向安全性，但不具备公开验证性。本文结合基于身份的密码体制，针对其存在的缺陷提出了改进方案，使其具有公开验证性。

### 3.2　针对 SK 的改进方案

SK 签密方案在电子商务应用中具有重要的价值，但该方案是基于传统公钥密码体制的，在证书生成、管理等方面存在很多问题，且实施代价昂贵。

基于身份的密码体制[17]不用公钥证书，也不用可信第 3 方，避免了对证书的一系列复杂操作。而利用椭圆曲线上的双线性对[18]，可以使密钥长度更小，从而减少计算量和传输存储量。因此，将椭圆曲线上的双线性对和基于身份的签密方案相结合，将会使改进后的 SK 签密方案更加实用。

#### 3.2.1　改进的签密方案

所需参数由可信第 3 方 PKG[19]生成。首先，选取 2 个 $q$ 阶的循环群，加法循环群 $(G_1,+)$ 和乘法循环群 $(G_2,\cdot)$，$P$ 为 $G_1$ 的生成元，$G_1$ 和 $G_2$ 的双线性变换为：$e:G_1\times G_1\rightarrow G_2$。

$PKG$ 选取自己的私钥（主密钥）$\delta\in Z_q^*$，计算相应的公钥：$P_{\mathrm{pub}}=\delta P\in G_1$。还有安全密码算法 $(E,D)$ 和 Hash 函数 $H_0:\{0,1\}\rightarrow G_1$，$H:\{0,1\}\rightarrow Z_q$，以及带有钥控的单向散列算法 KH。该方案

的系统参数为：$(G_1,G_2,e,P,P_{pub},E,D,H_0,H,KH)$。结合其身份 $ID_u$，PKG 解出相对应的公钥和私钥：$p_u=H_0(ID_u)$ 和 $\delta_u=\delta p_u$。则相应的用户 Alice 的公钥和私钥分别为：$p_a=H_0(ID_a)$ 和 $\delta_a=\delta p_a$，$B_i$ 的公钥和私钥分别为：$p_i=H_0(ID_i)$；$\delta_i=\delta p_i(i=1,2,\cdots,n)$。$e$ 是椭圆曲线上的双性变换即 Weil 对或者改造的 Tate 对。

签密算法：

1)随机选取 $x\in Z_q^*$；

2)计算：

$k=e(P,P_{pub}{}^x)$，

$k'=H(e(P_i,P_{pub}{}^x))$，

$c_i=E_{k_i}(m_i)$，

$r=KH_k(c_1\|c_2\|\cdots\|c_n)$，

$s=P_{pub}{}^x-r\delta_a$；

3)Alice 发送 $(c_1,c_2,\cdots,c_n,r,s)$ 给 $B_i$，$(1\leqslant i\leqslant n)$。

解签密算法：

1)计算 Alice 的公钥：

$p_a=H_0(ID_a)\in G_1$，

$k=e(P,s)e(P_{pub},p_a)^r$，

$k_i=H(e(p_i,s)e(\delta_i,p_a)^r)$，；

2)验证 $r=KH_k(c_1\|c_2\|\cdots\|c_n)$，等式成立时接收 $m_i$；否则，拒绝接收。

当需要时，$B_i$ 可将 $(c_1,c_2,\cdots,c_n,r,s)$ 发送给 $B_j$。类似上述过程，$B_j$ 可获得属于他的信息 $m_j$。

3.2.2 针对改进方案的分析

改进后的方案，密钥 $k$ 和 $k_i$ 中隐含了接收者的公钥和发送者的私钥，使得签密密文 $(c_1,c_2,\cdots,c_n,r,s)$ 既包含了认证机制也包含了加密机制。所以，改进之后的方案具备签密最基本的特征。

签密算法的证明如下：如上所述，$P$ 为 $G_1$ 的生成元，$p_a$ 和 $\delta_a$ 分别为 Alice 的公钥和私钥，$p_i$ 和 $\delta_i$ 分别为接收者 $B_i$ 的公钥和私钥，$p_{pub}$ 为 PKG 的公钥，$k$ 和 $k_i$ 为签密密钥，$k'$ 和 $k'_i$ 为解签密密钥，若 $k=k'$ 且 $k_i=k'_i$，则可说明该算法正确可行，$s=P_{pub}{}^x-r\delta_a$ 为发送的消息扩展。证明如下：

$$\begin{aligned}k'&=e(P,s)e(P_{pub},p_a)^r=\\&e(P,s)e(P_{pub},rp_a)=\\&e(P,s)e(\delta P,rp_a)=\\&e(P,s)e(P,r\delta p_a)=\\&e(P,s)e(P,r\delta_a)=\\&e(P,s+r\delta_a)=\\&e(P,P_{pub}{}^x)\end{aligned}$$

可得 $k'=e(P,P_{pub}{}^x)=k$；

$$\begin{aligned}k'_i&=H(e(p_i,s)e(\delta_i,p_a)^r)=\\&H(e(p_i,s)e(\delta p_i,rp_a))=\\&H(e(p_i,s)e(p_i,r\delta p_a))=\\&H(e(p_i,s)e(p_i,r\delta_a))=\\&H(e(p_i,s+r\delta_a))=\\&H(e(P_i,P_{pub}{}^x))\end{aligned}$$

可得 $k'_i=H(e(P_i,P_{pub}{}^x))=k_i$。

综上所述，可得该方案正确。

安全性分析：该方案的特点没有影响 SK 方案独特性，每一个接收者只能解密属于自己的消息，并且可以验证该方案的有效性而不能解密其他人的消息。改进方案的验证式 $r=KH_k(c_1\|c_2\|\cdots\|c_n)$ 的参数不是公开信息，就是可以由已知信息求解出来的，因此，任何人都可以进行验证，不需要 $m_i$。因此，当出现纠纷时，可以由第 3 方进行验证，而且不会泄露私密信息。改进方案中的 $k_i$ 可由下式 $k_i=H(e(p_i,s+r\delta_a))$ 算出，若发送方的私钥 $\delta_a$ 泄露，则黑客就会依据上式算出加密密钥 $k_i$，从而解出 $m_i$。由于发送方私钥 $\delta_a$ 的丢失所引起的 Alice 与 $B_i$ 之间长期通信密钥的泄露，将会危机他们之前所有的会话消息，因为只要获得 Alice 发给 $B_i$ 的传输信息 $(c_1,c_2,\cdots,c_n,r,s)$（这对黑客是很容易的事情），就会获得此次通信的秘密信息。所以，改进后的方案目前只具有公开验证性。

效率分析：结合身份的公钥密码体制，不需要管理公钥，签密过程也不需要传递和验证证书，只需要双方的身份信息和一些系统参数，这样极大地降低了通信代价。

通过上述分析可以看出，将身份引入改进的签密方案，极大减少了计算和传输代价，提高了效率，同时改进后的方案还具备了公开验证性，但是还不具备前向安全性，这也是下一步需要努力的方向。就整体而言，改进方案在安全性和效率方面较原方案已有很大提高。

## 4 结语

本文提出了 2 个改进方案：一个是针对 Zheng 签密方案在安全上的缺陷，其不具有可公开验证性和前向安全性，运用签密消息和公开信息可以恢复出解签密所需的信息这一原理并结合求解单向函数的困难性，使得完善后的方案在安全性上有了很大的提高；另一个是对 SK 签密方案在公钥管理方面效率低下、代价大和安全性存在的问题，利用了椭圆曲线上的双线性对和基于身份的密码体制进行改进，改进后的方案在效率和安全性上都有很大的提高。但其还不具备前向安全性，这也是下一步工作

的重点，继续对基于身份的签密进行研究，并不断改进、优化，使其在效率和安全性上再有所突破。

**参考文献**(References)：


[1] ZHENG Yuliang. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption)[J]. Advances in Cryptology, 1997, 1294: 165-179.

[2] MOHANTY S, MAJHI B, DAS S. A Secure Electronic Cash Based on A Certificateless Group Signcryption Scheme[J]. Mathematical and Computer Modelling, 2013, 58(1): 186-195.

[3] ZHANG M, FU C, FU W. Two New Blind Signcryption Schemes with the Appointed Receiver Based on Elliptic Curve[J]. Journal of Convergence Information Technology, 2013, 8(7): 451.

[4] YEH J. The Insecurity of Two Proxy Signcryption Schemes: Proxy Credential Forgery Attack and How to Prevent It[J]. The Journal of Supercomputing, 2014, 70(3): 1100-1119.

[5] SHARMA G, BALA S, VERMA A K. An Identity-based Ring Signcryption Scheme[J]. IEIE Transactions on Smart Processing & Computing, 2012, 2(2): 57-66.

[6] SEO M, KIM K. Electronic Funds Transfer Protocol Using Domain-Verifiable Signcryption Scheme[C]// Information Security and Cryptology - ICISC'99. Springer-Verlag, 1999: 269-277.

[7] 张串绒，肖国镇. 签密方案的分析、设计和应用研究[D]. 西安：西安电子科技大学，2007.
ZHANG Chuanrong, XIAO Guozhen. Study on Analysis, Design and Applications of Signcryption Schemes[D]. Xi'an: Xidian University, 2007. (in Chinese)

[8] FEI F Y, CHEN W, CHEN K F, et al. Efficient Identity Based Signcryption Scheme with Public Verifiability and Forward Security[J]. Wuhan University Journal of Natural Sciences, 2005, 10(1): 248-250.

[9] 张串绒，张玉清. 基于身份的前向安全和可公开验证签密方案[J]. 空军工程大学学报：自然科学版，2009, 10(3): 78-81.
ZHANG Chuanrong, ZHANG Yuqing. Identity Based Signcryption Scheme with Both Forward Security and Public Verifiability[J]. Journal of Air Force Engineering University: Natural Science Edition, 2009, 10(3): 78-81. (in Chinese)

[10] 张建航，胡予濮，齐新社. 具有前向安全性和可公开验证性的签密方案[J]. 计算机应用研究，2011，28(2)：733-734.
ZHANG Jianhang, HU Yupu, QI Xinshe. Public Verifiable Signcryption Schemes with Forward Secrecy[J]. Application Research of Computers, 2011, 28(2): 733-734. (in Chinese)

[11] 张串绒，肖国镇. SK 签密方案的改进及应用[J]. 计算机研究与发展，2006，43(z2)：386-388.
ZHANG Chuanrong, XIAO Guozhen. Improvement and Applications of the SK Signcryption Scheme[J]. Journal of Computer Research and Development, 2006, 43(z2): 386-388. (in Chinese)

[12] BARRETO P S L M, LIBERT B, MCCULLAGH N, et al. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps[J]. Lecture Notes in Computer Science, 2005, 3788: 515-532.

[13] WU T Y, TSAI T T, TSENG Y M. A Revocable ID-based Signcryption Scheme[J]. Journal of Information Hiding and Multimedia Signal Processing, 2012, 3(3): 240-251.

[14] LI F, KHAN M K. A Biometric Identity-based Signcryption Scheme[J]. Future Generation Computer Systems, 2012, 28(1): 306-310.

[15] 胡磊. 椭圆曲线 Tate 对的压缩[J]. 软件学报，2007，18(7)：1799-1805.
HU Lei. Compression of Tate Pairings on Elliptic Curves[J]. Journal of Software, 2007, 18(7): 1799-1805. (in Chinese)

[16] SHAMIR A. Identity-Based Cryptosystems and Signature Schemes[C]//Advances in Cryptology. Berlin, Heidelberg: Springer, 1985: 47-53.

[17] 左黎明，陈仁群，郭红丽. 可证安全的基于身份的签密方案[J]. 计算机应用，2015，35(3)：712-716.
ZUO Liming, CHEN Renqun, GUO Hongli. Provable Identity-based Signcryption Scheme[J]. Journal of Computer Applications, 2015, 35(3): 712-716. (in Chinese)

[18] 黄振杰，郭亚峰. 一个双线性对下高效的基于证书签名方案[J]. 江苏大学学报：自然科学版，2013，34(3)：320-325.
HUANG Zhenjie, GUO Yafeng. An Efficient Certificate-based Signature Scheme with Bilinear Pairing[J]. Journal of Jiangsu University: Natural Science Edition, 2013, 34(3): 320-325. (in Chinese)

[19] 赵秀凤，徐秋亮. 一个有效的多 PKG 环境下基于身份签密方案[J]. 计算机学报，2012，35(4)：673-680.
ZHAO Xiufeng, XU Qiuliang. An Efficient Multi-PKG ID-Based Signcryption Scheme[J]. Chinese Journal of Computers, 2012, 35(4): 673-680. (in Chinese)


(编辑：徐楠楠)