基于身份的同时生效签密体制研究

刘文琦* 顾 宏 杨建华
(大连理工大学电信学部 大连 116023)

摘 要：签密体制能够在一个逻辑步骤内完成数字签名和加密两项功能。某些场合下，通信双方存在利益冲突，同时生效签名体制可以在不需要可信第三方的条件下提供签名交换的公平性。基于此，该文提出同时生效签密概念及其安全模型，并利用双线性对建立了一个基于身份的同时生效签密方案，证明了在 BDH 问题及 Co-CDH 是困难的假设下，方案是安全的。

关键词：签密；同时生效签名；双线性对；随机预言模型
中图分类号：TP309 **文献标识码**： A **文章编号**：1009-5896(2011)07-1582-07
DOI: 10.3724/SP.J.1146.2010.01346

Identity-based Concurrent Signcryption Scheme

Liu Wen-qi Gu Hong Yang Jian-hua
(*Faculty of Electronic Information and Electrical Engineering*, *Dalian University of Technology*, *Dalian* 116023, *China*)

Abstract: Signcryption is a cryptographic primitive that combines both the function of digital signature and encryption in a logical single step. However, in some occasion there are conflicts of interest between the two entities, so concurrent signature is proposed to ensure fair exchange of the signature without special trusted third party. The notion of concurrent signcryption is defined and the security model is proposed in this paper. And an identity-based concurrent signcryption scheme is established using bilinear based on the framework. The scheme is proved to be secure assuming Bilinear Diffie-Hellman problem and Computational Co-Diffie-Hellman problem are hard in the bilinear context.

Key words: Signcryption; Concurrent signature; Bilinear pairing; Random oracle model

1 引言

为在网络信息传输中同时满足机密性及认证性的要求，Zheng[1]于 1997 年首次提出一个签密方案，将签名和加密的功能结合，同时保证了机密性、认证性和不可伪造性。签密方法相对于传统“先签名后加密”的方法而言，计算时间和存储空间上的代价都大为降低。

早期许多签密方案大多采用基于证书的机制实现数字签名，因此存在着需要维护复杂的证书库、客户端的运算和存储开销较大的问题。基于身份的公钥密码体制以表明身份的字符串为公钥，不依赖于数字证书，减少了密钥管理带来的容量和开销问题。2002 年，Malonee-Lee[2]提出了基于身份签密方案的安全模型，利用双线性对构造了第 1 个基于身份的签密方案。之后，研究者提出了许多基于身份的签密方案，并且更加关注公开验证性、前向安全性等属性及签密在特殊场合中的应用[3−8]。其中，文献[3]提出的方案满足机密性、认证性、不可否认性和匿名性，而且具有较高的效率。

为保证有利益冲突的双方在交互过程中利益均不受损害，需实现签名的公平交换，Chen 等人[9]于 2004 年首次提出同时生效签名，签名双方在没有可信第三方的帮助下交换签名，发起协议的一方掌握一个关键数(keystone)，关键数释放之前，从任何第三方角度来看这两个签名是匿名的，可由签名的任何一方产生；关键数公开后，签名就与各自的签名者绑定。针对是否能实现真正的公平性，许多同时生效签名方案被提出[10−15]。Susilo 等人[10]指出文献[9]的方案中若签名者均是诚实参与者，任意第三方在关键数公布之前就可判断签名真正的签名人，因此提出了完美同时生效签名的概念，即使签名的双方均可信赖，关键数公开之前签名仍保持完全模糊，并提出了满足这个模型的两个方案。但 Wang 等人[11]指出这两个方案都不满足公平性，因此不是真正的同时生效签名。之后，文献[12]提出两个基于身份的完美同时生效签名方案。但 Huang 等人[13]指出文献[12]的方案中，两个关键数都由起始签名人产

2010-12-06 收到，2011-01-30 改回
*通信作者：刘文琦 wqliu@dlut.edu.cn

生，起始签名人可以欺骗匹配签名人，因而方案是不公平的，由此给出了含两个关键数的同时生效签名协议中公平性的形式化定义，并提出了两个完美同时生效签名方案。

基于签密和完美同时生效签名，本文提出了同时生效签密的概念，对其形式化概念及安全模型给出详细的描述，设计了一个可证明语义安全的基于身份的同时生效签密方案。同时生效签密体制可用于电子商务、电子政务协议的设计，在存在利益冲突的信息交互双方之间传递机密的信息时，这样的协议可以保证信息的机密性和双方的公平性。

2　先验知识

令 G_1 为由 P 生成的循环加法群，阶为素数 q，G_2 为具有相同阶 q 的循环乘法群，a,b 是 Z_q^* 中的元素。假设 G_1 和 G_2 这两个群中的离散对数问题都是困难问题。双线性对是指满足下列性质的一个映射 $\hat{e}: G_1 \times G_1 \to G_2$。

(1)双线性性　$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$ ($a,b \in Z_q^*$，$P,Q \in G_1$)；

(2)非退化性　存在 $P,Q \in G_1$，使得 $\hat{e}(P,Q) \neq 1$；

(3)可计算性　对所有的 $P,Q \in G_1$ 存在有效的算法计算 $\hat{e}(P,Q)$。

双线性映射 $\hat{e}$ 可以通过有限域上的超椭圆曲线上的 Tate 对或 Weil 对来构造。

定义 1　$<G_1,G_2,\hat{e}>$ 上的 BDH(Bilinear Diffie-Hellman)问题是：对于任意 $a,b,c \in Z_q^*$ 由 $<P,aP,bP,cP>$ 计算 $\hat{e}(P,P)^{abc}$。

定义 2　Co-CDH (Computational Co-Diffie-Hellman)问题是：对于任意 $<P_1,P_2,aP_1,bP_2>$，其中 $P_1,P_2 \in G_1$，$a,b \in Z_q^*$ 未知，计算 $abP_2 \in G_2$。

对于概率多项式算法，可以成功解决 BDH 问题和 Co-CDH 问题的概率均可忽略不计。

3　基于身份同时生效签密的形式化定义及安全模型

3.1 基于身份同时生效签密的形式化定义

定义 3　设置消息空间 $\mathcal{M}$，签名空间 $\mathcal{S}$，密文空间 $\mathcal{C}$，关键数对空间 $\mathcal{K}_I \times \mathcal{K}_M$，加密关键数空间 $\mathcal{K}'$ 和关键数确认值空间 $\mathcal{F}$，一个基于身份的同时生效签密方案由如下算法组成：

(1)初始化(Setup)　输入 PKG 私钥 k，输出系统参数 params 的概率算法。

(2)提取密钥(Extract)　输入用户 U_I 的身份 ID，输出私钥 S_{ID} 和公钥 Q_{ID} 的概率算法。

(3)签密(Signcrypt)　输入 $(m,S_{\mathrm{ID}_i},\mathrm{ID}_j)$，其中 ID_j 是 U_j 的身份，S_{ID_i} 是 U_i 的私钥，$m \in \mathcal{M}$；输出 U_i 发送给 U_j 对消息 m 的签密值 $c=\mathrm{Signcrypt}(m, S_{\mathrm{ID}_i},\mathrm{ID}_j)=\{X_i,y_i\}$ 的概率算法。

(4)初始关键数确认(Fix-initks)　输入初始关键数 $k_I \in \mathcal{K}_I$，输出确认值 $f_I \in \mathcal{F}$ 的确定算法。

(5)模糊签名生成(Amsign)　输入 $(\mathrm{ID}_i,\mathrm{ID}_j, S_{\mathrm{ID}_i},f,c)$，其中 $S_n \in \mathcal{S}$，$c \in \mathcal{C}$，$f \in \mathcal{F}$；输出对 c 的模糊签名 $\sigma=\{U_i,U_j,V\}$ 的概率算法。

(6)匹配关键数加密(Enc-matchingks)　输入匹配关键数 $k_M \in \mathcal{K}_M$，输出加密值 $K_M \in \mathcal{K}'$ 的确定算法。

(7)加密关键数确认(Fix-secks)　输入 (k_M,f_I)，输出加密关键数确认值 $f_S \in \mathcal{F}$ 的确定算法。

(8)模糊签名验证(Amverify)　输入 $(\mathrm{ID}_i,\mathrm{ID}_j, \sigma,c)$，其中 $\sigma=\{U_i,U_j,V\}$，输出 Yes 或 No 的确定算法。算法需满足对称性，即如果 $\sigma'=\{U_j,U_i,V\}$，则　$\mathrm{Amverify}(\mathrm{ID}_i,\mathrm{ID}_j,\sigma,c)=\mathrm{Amverify}(\mathrm{ID}_j,\mathrm{ID}_i,\sigma',c)$ 成立。

(9)关键数验证(Ver-ks)　输入 $(k_I,k_M,f_I,f_s, S_{\mathrm{ID}_i})$，验证 $f_I=\mathrm{Fix\text{-}initks}(k_I)$ 及 $f_s=\mathrm{Fix\text{-}secks}(\mathrm{Enc\text{-}matchingks}(k_M),S_{\mathrm{ID}_i})$ 是否成立，输出 Yes 或 No 的确定算法。

(10)关联验证(Ver-conn)　输入 $\{\sigma_i,\sigma_i',f_I,f_s\}$，验证 $U_j=f_i \otimes c$, $U_i'=U_j \otimes f_s$ 成立与否输出 Yes 或 No 的确定算法，其中 $\sigma_i=\{U_i,U_j,V\}$, $\sigma_i'=\{U_i',U_j', V'\}$ 为一对模糊签名，f_I 和 f_s 为一对关键数确认值，$\otimes$ 是群 $\mathcal{F}$ 上的运算。

(11)解签密(Unsign)　输入为 $(c,\mathrm{ID}_i,\mathrm{ID}_j)$，如能解密，输出 $m' \in \mathcal{M}$；否则返回 No。

(12)验证签名(Verify)　输入 (k_I,k_M,S',m')，其中 $(k_I,k_M) \in \mathcal{K}_I \times \mathcal{K}_M$, $S'=(\sigma_i,\sigma_j,\mathrm{ID}_i,\mathrm{ID}_j,c)$, m' 为解签密的输出，如 Ver-ks, Ver-conn 和 Amverify 算法输出均为 Yes，且 m' 被验证为有效，则输出 Yes，否则输出 No。

3.2 安全模型

安全的同时生效签密方案应满足：正确性、机密性、不可否认性、不可伪造性、模糊性以及公平性。

(1)正确性　给定系统参数 params、消息 $m \in \mathcal{M}$，由Signcrypt算法生成 m 的签密值 c、由Amsign算法生成的模糊签名 σ。Amverify算法会以绝对大概率输出“Yes”接受签名；关键数对 $(k_I,k_M) \in \mathcal{K}_I \times \mathcal{K}_M$ 公开后，Unsign 算法输出 $m' \in \mathcal{M}$，且Verify算法会以绝对大的概率输出“Yes”验证 m' 有效。

(2)机密性　任何攻击者试图从密文中获取相关明文信息的尝试在计算上不可行。若方案可以达

到适应性选择密文攻击下的不可区分安全性，则该方案满足机密性。可以采用挑战者 C 和敌手 $\mathcal{A}$ 之间进行游戏的方式定义此概念：

(a)初始化： C 执行Setup(1^k)，并将系统参数 params 发送给 $\mathcal{A}$，保存秘密 s。

(b)阶段 1：敌手 $\mathcal{A}$ 向挑战者 C 执行以下基于挑战/应答方式询问：

(i)Extract 询问： $\mathcal{A}$ 向 C 提交身份， C 以该身份的私钥值作为应答。

(ii)Hash 询问： $\mathcal{A}$ 可提出任意值， C 计算其 Hash 函数值作为应答。

(iii)Signcrypt 询问： $\mathcal{A}$ 选择发送者、接收者身份 ID_i , ID_j 及明文 m 提交给 C , C 计算 Signcrypt(m, S_{ID_i}, ID_j) 作为给 $\mathcal{A}$ 的应答。

(iv)Unsign 询问： $\mathcal{A}$ 选择 ID_i , ID_j 及密文 c 提交给 C ， C 使用接收者私钥 S_{ID_j} 解密密文并验证，将结果作为给 $\mathcal{A}$ 的应答。

阶段 1 结束时， $\mathcal{A}$ 输出两个信息 $\{m_0, m_1\}$ 和两个身份 $\{\mathrm{ID}_A, \mathrm{ID}_B\}$， $\mathcal{A}$ 须未进行过 ID_B 的 Extract 询问。

(c)挑战： C 随机选择 $b \in \{0,1\}$，生成 ID_A 给 ID_B 的消息 m_b 的签密值 c，并发送给 $\mathcal{A}$。

(d)阶段 2： $\mathcal{A}$ 与 C 继续采用阶段 1 中同样方式的询问，但不允许对 ID_B 签密的结果 c 进行 Unsign 询问，也不允许就接收者 ID_B 的私钥进行 Extract 询问。

(e)响应： $\mathcal{A}$ 如能返回 $b' \in \{0,1\}$ 满足 $b' = b$，则称 $\mathcal{A}$ 游戏获胜。

定义 4 如果完成上述游戏的敌手 $\mathcal{A}$ 的优势 $\mathrm{Adv}(\mathcal{A}) = \left|\Pr[b' = b] - 1/2\right|$ 可被忽略，则称方案满足适应性选择密文攻击下的不可区分性(IND-IBSC-CCA2)要求。

(3)不可否认性 双方的签名都具有模糊性，不诚实一方试图生成有效关键数的概率可忽略，即任何签名不能被包括对方在内的其他人伪造。此概念通过敌手 $\mathcal{A}$ 和挑战者 C 之间的游戏定义：

(a)初始化： C 执行 Setup(1^k)生成系统参数 params 发送给 $\mathcal{A}$, C 保存秘密 s。

(b)询问阶段：基于挑战/应答方式， $\mathcal{A}$ 向 C 进行“机密性”阶段 1 中的询问以及如下询问：

(i) F_I 询问： $\mathcal{A}$ 可以请求 C 选择也可自己选择任意关键数 $k_I \in \mathcal{K}_I$, C 计算关键数确定值 $f_I = F_I(k_I)$ 作为给 $\mathcal{A}$ 的应答。

(ii) F_M 询问： $\mathcal{A}$ 可以请求 C 选择也可自己选择匹配关键数 k_M , C 计算 $f_M = F_M(k_M, f_I)$ 并将该关键数确定值给 $\mathcal{A}$ 的应答。

(iii) F_I 公布询问： $\mathcal{A}$ 可以根据 F_I 询问中的情况，请求 C 或者自己公布生成 $f_I \in \mathcal{F}$ 的关键数 k_I。如果 f_I 是 F_I 询问的应答， C 输出满足 $f_I = F_I(k_I)$ 的 k_I； 否则 C 输出无效。

(iv) F_M 公布询问： $\mathcal{A}$ 可根据 F_M 询问中的情况，请求由 C 或自己公布生成 $f_M \in \mathcal{F}$ 的 k_M 和 f_I。如果 f_M 是 F_M 询问的应答， C 输出满足 $f_M = F_M(k_M, f_I)$ 的 k_M 和 f_I。否则 C 输出无效。

(v)Amsign 询问： $\mathcal{A}$ 可以请求任何形为 (ID_i, ID_j, S_{ID_i}, f, c) 的输入的模糊签名， C 以 σ={ U_i, U_j, V } 作为应答。

(c)伪造阶段： $\mathcal{A}$ 提交 $(m, \mathrm{ID}_A, \mathrm{ID}_B, c, \sigma)$，其中 ID_A 和 ID_B 为起始签名人和匹配签名人的身份， c 为密文， $\sigma = \{U_A, U_B, V\}$。如满足：

(i) $\mathrm{ID}_A \neq \mathrm{ID}_B$；

(ii) $\mathrm{Amverify}(\mathrm{ID}_A, \mathrm{ID}_B, \sigma, c) = \mathrm{Yes}$， $\mathrm{Unsign}(c, \mathrm{ID}_A, \mathrm{ID}_B) = m$；

(iii) c 不是使用发送者及接收者身份 ID_A 和 ID_B 经过 Signcrypt 询问得到的结果；

(iv) $\mathcal{A}$ 未进行过输入为多元组 $(\mathrm{ID}_A, \mathrm{ID}_B, S_{\mathrm{ID}_A}, f, c)$ 或 $(\mathrm{ID}_B, \mathrm{ID}_A, S_{\mathrm{ID}_B}, f, c)$ 的 ASign 询问；

(v)未对 ID_A 进行过 Extract 询问。

则称 $\mathcal{A}$ 赢得游戏。此时考虑内部安全性，敌手具有成功伪造密文签名的优势。

定义 5 令 $\mathcal{A}$ 表示完成上述游戏的敌手。如可忽略 $\mathcal{A}$ 的优势 $\mathrm{Adv}(\mathcal{A}) = \Pr[\mathcal{A}\ \mathrm{wins}]$，则称在内部选择信息攻击下方案存在性不可伪造。

(4)不可伪造性 任何攻击者企图生成合法的签名在计算上是不可行的。 $\mathcal{A}$ 在不掌握任何关于私钥 S_{ID} 知识的前提下，不会生成有效的签密值通过 Amverify 验证并被 Unsign 有效解签密。此概念通过 $\mathcal{A}$ 和 C 之间的游戏定义：

前面步骤与不可否认性完全相同，仅在判断 $\mathcal{A}$ 赢得游戏的条件上最后一个条件变为：

(vi)未对 ID_A 和 ID_B 进行过 Extract 询问。

定义 6 如果可以忽略完成上述游戏的敌手 $\mathcal{A}$ 的优势 $\mathrm{Adv}(\mathcal{A}) = \Pr[\mathcal{A}\ \mathrm{wins}]$，则称方案在外部选择消息攻击下满足存在性密文不可伪造性。

(5)模糊性 给定模糊签名对 (σ_1, σ_2)，关键数公开之前，从 $\mathcal{A}$ 看来， σ_1 和 σ_2 均由起始签名人产生或匹配签名人产生或分别由两个签名人产生的概率相同，因而不能区分谁是实际签名人。通过敌手 $\mathcal{A}$ 和挑战者 C 之间的游戏定义此概念：

(a)初始化及阶段 1：与不可否认性及不可伪造性定义中对应阶段相同。

(b)挑战： $\mathcal{A}$ 选择 $(\mathrm{ID}_i, \mathrm{ID}_j, c)$，其中 ID_i 和 $\mathrm{ID}_j \neq$

ID_i 是参与方身份，$c \in \mathcal{C}$。C 随机选择 $k_I \in \mathcal{K}_I$ 并计算其关键数确定值 $f = F_I(k_I)$ 或随机选择 $(k,k') \in \mathcal{K}_I \times \mathcal{K}_M$ 并计算 $f = F_M(k, F_I(k'))$（每种情况有 1/2 概率），然后随机选择 $b \in \{0,1\}$。如果 $b = 0$，C 计算 $\sigma = \mathrm{Amsign}(\mathrm{ID}_i, \mathrm{ID}_j, S_{\mathrm{ID}_i}, f, c)$；如 $b = 1$，C 计算 $\sigma = \mathrm{Amsign}(\mathrm{ID}_j, \mathrm{ID}_i, S_{\mathrm{ID}_j}, f, c)$，以模糊签名 $\{U_1, U_2, V\}$ 作为应答输出。

(c)阶段 2：$\mathcal{A}$ 与 C 继续进行一系列如阶段 1 相同方式的询问/应答。

(d)输出：如在 $\mathcal{A}$ 没有进行过任何关于 U_1、U_2 的 F_I、F_M 公布询问的条件下，$\mathcal{A}$ 输出 $b' \in \{0,1\}$ 满足 $b' = b$，则称 $\mathcal{A}$ 赢得游戏。

定义 7　如果可以忽略完成上述游戏的敌手 $\mathcal{A}$ 的优势 $\mathrm{Adv}(\mathcal{A}) = \Pr[A \text{ wins}]$，则称方案满足签名模糊性。

(6)公平性　模糊签名将会在关键数公开后对应其签名人。不会出现起始签名人的签名与其关键数能够对应而匹配签名人不可的情况，反之亦然。通过敌手 $\mathcal{A}$ 和挑战者 C 之间的游戏定义这个概念：

(a)初始化、询问：与不可否认性游戏中初始化及 Amsign 询问之外的询问相同。

(b)Amsign 询问：公平性游戏中包括两种询问，设 ID_i 和 $\mathrm{ID}_j \neq \mathrm{ID}_i$ 是参与方的身份，$c \in \mathcal{C}$：

(i)IAmsign 询问：$\mathcal{A}$ 请求任何形为 $(\mathrm{ID}_i, \mathrm{ID}_j, c)$ 输入的模糊签名。C 首先通过 F_I 询问获得一个关键数确定值 $f_I \in \mathcal{F}$，然后以模糊签名 $\sigma = \{U_i, U_j, V\}$ 应答。

(ii)MAmsign 询问：$\mathcal{A}$ 请求任何形为 $(\mathrm{ID}_i, \mathrm{ID}_j, c, f)$ 输入的模糊签名，$f \in \mathcal{F}$。C 计算模糊签名 $\sigma = \{U_i, U_j, V\}$ 作为应答。

(c)输出：$\mathcal{A}$ 任意选择身份 ID_A 和 ID_B，输出 $\sigma = \{f, U, V\}$ 和 $c \in \mathcal{C}$。如 $\mathrm{Amverify}(\mathrm{ID}_A, \mathrm{ID}_B, \sigma, c) = \mathrm{Yes}$ 成立，且

(i)σ 是 IAmsign 询问的结果。$\mathcal{A}$ 在没有进行过对 f 的 F_I 公布询问的条件下，能够生成满足 $f = F_I(k)$ 的关键数 k 或者满足 $f = F_M(k, F_I(k'))$ 的关键数对 (k,k')。

(ii)σ 是 MAmsign 询问的结果。$\mathcal{A}$ 生成满足 $f = F_I(k)$ 的关键数 k 或者生成满足 $F_M(k_1, F_I(k_2)) = F_M(k', f')$ 但 $f' \neq F_I(k_2)$ 的关键数 k_1、k_2 和 k'，签名 σ 的关键数确定值 f' 通过 MAmsign 询问中获得。

定义 8　如果任何多项式有界的敌手能够赢得公平性游戏的概率可以忽略，则称方案是公平的。

如一个基于身份的同时生效签密方案满足正确性、机密性、不可否认性、不可伪造性、模糊性及公平性，则称该方案是安全的。

4　一个基于身份同时生效签密方案

本文基于文献[3]和文献[13]提出一个具体的同时签密方案。

令 G_1 为由 P 生成的循环加法群，阶为 q，G_2 为具有相同阶 q 的循环乘法群，a,b 是 Z_q^* 中的元素。$\hat{e}: G_1 \times G_1 \to G_2$ 为双线性对映射。方案包括如下算法：

(1)初始化(Setup)

(a)选择大素数 q，G_1 是阶为 q、生成元为 P 的循环加法群，G_2 是 q 阶循环乘法群，$\hat{e}: G_1 \times G_1 \to G_2$ 为一个双线性映射；

(b)设置 $\mathcal{M} = \mathcal{C} = Z_q, \mathcal{K}_M = G_2, \mathcal{K}_I = \mathcal{S} = \mathcal{K}' = \mathcal{F} = G_1$；

(c)选择 4 个安全 Hash 函数：$H_0: \{0,1\}^{k_1} \to G_1$，$H_1: \{0,1\}^* \to Z_q^*$，$H_2: G_2 \to \{0,1\}^{k_0+n}$，$H_3: \{0,1\}^* \to Z_q^*$，其中，$k_0$、$k_1$ 和 n 分别表示 G_1 中元素的字节长度、用户身份的字节长度和消息长度；

(d)PKG 选择随机数 $s \in Z_q^*$，计算 $P_{\mathrm{pub}} = sP$，保密主密钥 s；

(e)输出系统公共参数 $\mathrm{params} = \{G_1, G_2, \hat{e}, n, P, P_{\mathrm{pub}} H_0, H_1, H_2, H_3\}$。

(2)提取密钥(Extract)

(a)用户 I 向 PKG 提交其身份 ID_i；

(b)PKG 确认 I 身份后，计算 $Q_{\mathrm{ID}_i} = H_0(\mathrm{ID}_i)$，$S_{\mathrm{ID}_i} = sQ_{\mathrm{ID}_i}$，并将 S_{ID_i} 从安全通道交给 I。

(3)签密(Signcrypt)

(a)输入 $(\mathrm{ID}_j, S_{\mathrm{ID}_i}, m)$，随机选取 $r \in Z_q^*$，并计算 $X \leftarrow rQ_{\mathrm{ID}_i}$；

(b)计算 $h_1 \leftarrow H_1(X \,||\, m)$ 和 $Z \leftarrow (r + h_1)S_{\mathrm{ID}_i}$，$\omega \leftarrow \hat{e}(rS_{\mathrm{ID}_i}, Q_{\mathrm{ID}_j})$；

(c)计算 $y \leftarrow H_2(\omega) \oplus (Z \,||\, m)$，密文 $c = (X, y)$。

(4)初始关键数确认(Fix-initks)　取 $k_i = X$ 作为起始签名人的关键数，计算确认值 $f_i = H_3(k_i)P + X \in \mathcal{F}$。

(5)模糊签名(Amsign)

(a)输入 $(\mathrm{ID}_i, \mathrm{ID}_j, S_{\mathrm{ID}_i}, f, c)$，设 $U_j = f \in G_1$，计算 $h_j = H_3(y \,||\, \mathrm{ID}_i \oplus \mathrm{ID}_j \,||\, U_j)$；

(b)随机选取 $r_i' \in Z_q^*$，计算 $U_i = r_i' Q_{\mathrm{ID}_i} - U_j - h_j Q_{\mathrm{ID}_j} \in G_1$；

(c)计算 $h_i = H_3(y \,||\, \mathrm{ID}_i \oplus \mathrm{ID}_j \,||\, U_i)$，$V = (h_i + r_i')S_{\mathrm{ID}_i} \in G_1$，输出 $\sigma = \{U_i, U_j, V\}$。

(6)匹配关键数加密(Enc-matchingks)　输入 $(\mathrm{ID}_i, \mathrm{ID}_j, S_{\mathrm{ID}_j}, c')$，$c' = (X', y')$ 为匹配签名人生成的消息签密值。取 $k = H_3(X') \in Z_q^*$，计算加密匹配关键数 $K_M = k \cdot P \in \mathcal{K}'$。

(7)秘密关键数确认(Fix-secks)

(a)计算匹配关键数 $k_M = \hat{e}(P_{\text{pub}}, Q_{\text{ID}_i})^k \in \mathcal{K}_M$；

(b)计算 $f_M = H_3(k_M)P + U_j + X' \in \mathcal{F}$，作为匹配关键数确认值。

(8)模糊签名验证(Amverify)

(a)输入为 $(\text{ID}_i, \text{ID}_j, \sigma, y)$ 计算 $h_i = H_3(y \,||\, (\text{ID}_i \oplus \text{ID}_j) \,||\, U_i)$, $h_j = H_3(y \,||\, (\text{ID}_i \oplus \text{ID}_j) \,||\, U_j)$；

(b)如 $\hat{e}(P_{\text{pub}}, U_i + h_i Q_{\text{ID}_i} + U_j + h_j Q_{\text{ID}_j}) = \hat{e}(P, V)$ 成立，接受该模糊签名，输出“Yes”；否则拒绝，输出“No”。

(9)关键数验证(Ver-ks)

(a)判断 $f_i = H_3(k_i)P + k_i$ 成立与否，如成立，输出“Yes”；否则拒绝，输出“No”；

(b)计算 $k_M^{'} = \hat{e}(K_M, S_{\text{ID}_i})$, $X' = f_M - H_3(k_M^{'}) - U_j$，判断 $K_M = H_3(X')P$ 成立与否，如成立，输出“Yes”；否则拒绝，输出“No”。

(10)解签密(Unsign) 输入 $(c, \text{ID}_i, \text{ID}_j)$，计算 $\omega \leftarrow \hat{e}(X, S_{\text{ID}_j})$，恢复消息 $Z \,||\, m \leftarrow y \oplus H_2(\omega)$ 并输出。

(11)验证(Verify) 输入 (k_I, k_M, S', m')，其中 $S' = (\sigma_i, \sigma_j, \text{ID}_i, \text{ID}_j, c)$。如方案可以经 Amverify 算法、Verify-ks 算法验证通过，则使用 Unsign 算法解密获得消息 m'，并计算 $h_1 \leftarrow H_1(X \,||\, m')$，如等式 $\hat{e}(Z, P) = \hat{e}(P_{\text{pub}}, X + h_1 Q_{\text{ID}_i})$ 成立，接受该消息，输出“Yes”；反之，输出 “No”表示拒绝。

5 安全性分析

在随机预言模型中进行安全性分析，假设敌手进行各种哈希函数 H_i 询问的次数分别为 $q_i (i = 0, 1, 2, 3)$, Signcrypt 询问、Amsign 询问和 Unsign 询问的次数分别为 q_s, q_{as} 和 q_u。

(1)正确性 在公布关键数之前，双方使用Amverify算法验证对方的模糊签名：

$$\hat{e}(P_{\text{pub}}, U_i + h_i Q_{\text{ID}_i} + U_j + h_j Q_{\text{ID}_j}) = \hat{e}(sP, h_i Q_{\text{ID}_i} + r_i^{'} Q_{\text{ID}_i}) = \hat{e}(P, (h_i + r_i^{'}) s Q_{\text{ID}_i}) = \hat{e}(P, V)$$

设 $\sigma = \{U_i, U_j, V\}$, $\sigma' = \{U_j, U_i, V\}$，则 $\text{Amverify}(\text{ID}_i, \text{ID}_j, \sigma, y_i) = \text{Amverify}(\text{ID}_j, \text{ID}_i, \sigma', y_i)$ 成立，对称性满足。

关键数公开后，双方解签密并使用Verify算法验证：

$$\hat{e}(Z, P) = \hat{e}((r + h_1) S_{\text{ID}_i}, P) = \hat{e}((r + h_1) s Q_{\text{ID}_i}, P) = \hat{e}(sP, (r + h_1) Q_{\text{ID}_i}) = \hat{e}(P_{\text{pub}}, X + h_1 Q_{\text{ID}_i})$$

(2)机密性 基于文献[3]方案的机密性，可以通过引理1给出本文方案的机密性。

引理1 随机预言模型中，若存在能够以概率 ϵ 赢得机密性游戏的IND-IBSC-CCA2敌手 $\mathcal{A}$，则存在 $\mathcal{B}$ 可以在多项式时间内以不小于 $\epsilon \cdot \left(1 - \frac{q_s(q_1 + q_s)}{q}\right) \cdot \frac{1}{q_0 q_2}$ 的概率解决BDH难题。

分析：$\mathcal{B}$ 接收任意随机的 BDH 问题实例 (P, aP, bP, cP)，他的目标是计算出 $\hat{e}(P, P)^{abc}$。$\mathcal{B}$ 以挑战者身份将 $\mathcal{A}$ 作为子程序运行，与之开始 IND-IBSC-CCA2 游戏。游戏初始阶段，设 b 为 PKG 的主密钥，$\mathcal{B}$ 并不知道 b。$\mathcal{B}$ 向 $\mathcal{A}$ 发送 $P_{\text{pub}} = bP$ 等系统参数。$\mathcal{B}$ 维护初始为空的列表 L_0, L_1, L_2, L_s 和 L_u, L_i $(i = 0, 1, 2)$用于跟踪随机预言对 H_i 询问的响应；L_s 和 L_u 分别用于模拟签密预言机及解签密预言机。

根据安全模型的机密性定义，在阶段 1 最后，敌手会输出两个身份 $\{\text{ID}_A, \text{ID}_B\}$ 和两个消息 $\{m_0, m_1\}$。如果 $\text{ID}_B \neq \text{ID}_\beta$, $\mathcal{B}$ 终止这个模拟。否则选取 $y^* \leftarrow \{0,1\}^{k_0 + n}$，并设置 $X^* \leftarrow cP$，并向敌手 $\mathcal{A}$ 返回挑战的密文 $\sigma^* \leftarrow (X^*, y^*)$。$\mathcal{A}$ 在阶段 2 进行与阶段 1 同样方式的询问/应答直至该阶段结束，然后输出一个 bit 值 b，$\mathcal{B}$ 忽略 b 并在 L_0 中查找 $(\text{ID}_A, Q_A, S_A, x_a)$，在 L_2 中随机选择 ω 后计算 $\omega^{x_a^{-1}}$ 作为对 (P, aP, bP, cP) 的 BDH 问题解的猜测。

$\mathcal{B}$ 执行 $\mathcal{A}$ 攻击阶段中，对 H_0 和 H_1 的模拟与真正的随机预言不可区分，H_2 仅在 $\mathcal{A}$ 或 $\mathcal{B}$ 调用 H_2 询问时会被定义，因此 H_0、H_1 和 H_2 是可靠的。唯一产生由 $\mathcal{B}$ 运行 $\mathcal{A}$ 和实际的攻击看起来不同而造成模拟失败的可能是重复定义 $H_1(X \,||\, m)$，由于 X 在 G_1 上均匀分布，所以整个模拟中出现模拟失败的概率最多为 $q_s(q_1 + q_s)/q$, q_s 为Signcrypt询问次数。

模拟Extract询问时，$\mathcal{B}$ 选择 $\mathcal{A}$ 执行的 H_0 询问，以其要解决的BDH实例的结果作为应答。为避免Extract模拟出现错误，$\mathcal{A}$ 不对 ID_β 执行Extract询问的概率至少为 $1/q_0$。因为敌手试图提取私钥，$\mathcal{B}$ 则终止模拟。当 $\mathcal{B}$ 执行 $\mathcal{A}$ 攻击阶段2的时候，$\mathcal{A}$ 不对 $\omega = \hat{e}(P, P)^{x_\alpha abc}$ 进行 H_2 询问的概率大于 $1/q_2$，并且可能发生上述任何错误。

综上所述，$\mathcal{B}$ 可以解决BDH问题的概率至少为 $\epsilon \cdot \left(1 - \frac{q_s(q_1 + q_s)}{q}\right) \cdot \frac{1}{q_0 q_2}$。

(3)不可否认性

引理2 随机预言模型下，本文方案基于Co-CDH问题和BDH问题困难的假设在内部适应性选择消息攻击下满足存在不可伪造性。

分析：文献[3]中证明基于BDH问题是困难的假设，其签密算法在选择消息攻击下是存在不可伪造的。文献[13]证明基于Co-CDH问题是困难的假设，其方案在适应性选择消息攻击下是存在不可伪造的。本文方案基于文献[13]中的同时签名方案及文献[3]中的签密方案，可以采用类似证明基于Co-CDH

问题和BDH问题是困难的假设，本文方案在内部适应性选择消息攻击下是存在不可伪造的。

(4)不可伪造性

引理3　随机预言模型下，基于Co-CDH问题和BDH问题困难的假设，本文方案在外部适应性选择消息攻击下满足存在不可伪造性。

分析：与引理2类似。

(5)模糊性

引理4　随机预言模型中，关键数公布之前，双方的签名是模糊的。

分析：

$$\xi=\left\{(U_i,U_j,V)\left|\begin{array}{l} f\in G_1,k\in G_1,r'\in Z_q^* \\ U_j=f,h_j=H_3(y\,||\,\mathrm{ID}_i\oplus\mathrm{ID}_j\,||\,U_j) \\ U_i=r_i'Q_{\mathrm{ID}_i}-U_j-h_jQ_{\mathrm{ID}_j}, \\ h_i=H_3(y\,||\,\mathrm{ID}_i\oplus\mathrm{ID}_j\,||\,U_i) \\ V=(h_i+r_i')S_{\mathrm{ID}_i} \end{array}\right.\right\}$$

$$\zeta=\left\{(U_j',U_i',V')\left|\begin{array}{l} f\in G_1,k\in G_1,r_j'\in Z_q^* \\ U_i'=f,h_i'=H_3(y'\,||\,\mathrm{ID}_i\oplus\mathrm{ID}_j\,||\,U_i') \\ U_j'=r_j'Q_{\mathrm{ID}_j}-U_i'-h_i'Q_{\mathrm{ID}_i}, \\ h_j'=H_3(y'\,||\,\mathrm{ID}_i\oplus\mathrm{ID}_j\,||\,U_j') \\ V'=(h_j'+r_j')S_{\mathrm{ID}_j} \end{array}\right.\right\}$$

随机预言模型中的单向哈希函数输出均匀分布，故上述两个分布相同。在关键数释放之前，H_3 输出随机，使得签名 V 可以是 G_1 中任意元素，因此敌手赢得模糊性游戏的概率，即确定 V 的签名者的概率为1/2，因此方案满足模糊性。

(6)公平性

引理5　随机预言模型中，本文方案满足公平性。

分析：假设敌手 $\mathcal{A}$ 赢得公平性游戏的概率为 ϵ。如 IAmsign 询问的输出为 σ ,F_I 询问的输出为 f。令 q_I、q_M、q_{IS} 和 q_{MS} 分别是 $\mathcal{A}$ 进行 F_I、F_M、IAmsign 和 MAmsign 询问的次数。则可能出现如下两种情况：

(a) $\mathcal{A}$ 在未执行输入为 f 的 F_I 公布询问的情况下，找到关键数 k 满足 $f=H_3(k)P+X$。在随机预言模型中，$\mathcal{A}$ 生成能够满足条件 k 的概率不超过 $q_{IS}q_I/q$。

(b) $\mathcal{A}$ 找到关键数对 (k,k') 满足 $f=H_3(k)P+H_3(k')P+X+X'$。在随机预言模型中，$\mathcal{A}$ 获得 (k,k') 能够通过 F_M 询问的概率最多达到 $q_{IS}q_M/q$，通过 F_I 询问的概率最多达到 $q_{IS}q_I(q_I+1)/2q$，则能够生成 (k,k') 的概率最多为 $q_{IS}(q_I(q_I+1)+2q_M)/2q$。

如果 f 是对 f' 进行 F_M 询问的输出，σ 是 MAmsign 询问的输出，$\mathcal{A}$ 可通过 F_M 公布询问获得 (k',f') 满足 $f=H_3(k')+f'+X'$。本方案中 $\mathcal{A}$ 无法通过设置 $f'=H_3(k)-H_3(k')-X'$ 找到关键数，因为 f' 先于 k' 选择。由于 q_I、q_M、q_{IS} 和 q_{MS} 多项式有界，故概率 ϵ 忽略不计。

基于 Co-CDH 问题和 BDH 问题是困难的假设，本文方案在随机预言模型中是安全的。

6　结论

本文提出了基于身份的同时生效签密概念，在其基础上给出了同时生效签密的形式化定义和安全模型。基于 Chen 和 Malone-Lee 基于身份的签密方案及 Huang 等人的同时生效签名方案，提出了一个具体的基于身份同时生效签密方案，并在随机预言模型中进行了安全性证明。在 BDH 问题和 Co-CDH 问题是困难的假设下，所提方案被证明是安全的，该方案可以用于构建电子商务、电子签章协议，以确保协议公平性、机密性等安全属性的实现。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature&encryption)<<cost (signature)+cost(encrytion) [C]. Advances in cryptology - CRYPTO '97, Santa Barbara, USA, Aug. 17–21, 1997, LNCS 1294: 165–179.

[2] Malone-Lee J. Identity based signcryption. http://eprint.iacr.org/2002/098.pdf.

[3] Chen L and Malone-Lee J. Improved identity-based signcryption [C]. Public Key Cryptography - PKC'05, Les Diablerets, Switzerland, Jan. 23–26, 2005, LNCS 3386: 362–379.

[4] Li Fagen, Xin Xiang-jun, and Hu Yu-pu. Indentity-based broadcast signcryption [J]. *Computer Standards & Interfaces*, 2008, 30(1–2): 89–94.

[5] Sharmila Deva Selvi S, Sree Vivek S, and Shriram J, *et al*.. Identity based aggregate signcryption schemes [C]. Indocrypt 2009, New Delhi, India, Dec. 13–16, 2009, LNCS 5922: 378–397.

[6] Yu Yong, Yang Bo, Sun Ying, and Zhu Sheng-lin. Identity based signcryption scheme without random oracles [J]. *Computer Standards & Interfaces*, 2009, 31(1): 56–62.

[7] Zhang J and Geng Q. Cryptoanalysis of two signcryption schemes [C]. Fifth International Conference on Information Assurance and Security, Xi'an, China, Aug. 18–20, 2009: 65–68.

[8] Hur Jun-beom, Park Cha-nil, and Yoon Hyun-soo. Chosen ciphertext secure authenticated group communication using identity-based signcryption [J]. *Computers and Mathematics with Applications*, 2010, 60(2): 362–375.

[9] Chen L, Kudla C, and Paterson K G. Concurrent signatures [C]. Advances in Cryptology-EUROCRYPT 2004, Interlaken, Switzerland, May 2004, LNCS 3027: 287–305.

[10] Susilo W, Mu Y, and Zhang F. Perfect concurrent signature schemes [C]. Information and communications security - ICICS 2004, Malaga, Spain, Oct. 2004, LNCS 3269: 14–26.

[11] Wang G, Bao F, and Zhou J. The fairness of perfect concurrent signatures [C]. Information and Communications Security - ICICS2006, Raleigh, USA, Dec. 2006, LNCS 4307: 435–451.

[12] Chow S and Susilo W. Generic construction of (identity-based) perfect concurrent signatures [C]. International Conference on Information and Communications Security 2005, Beijing, China, Dec. 10–13, 2005, LNCS 3783: 194–206.

[13] Huang Z, Chen K, and Lin X, *et al*.. Analysis and improvements of two identity-based perfect Concurrent signature schemes[J]. *Informatica*, 2007, 18(3): 375–394.

[14] Huang X and Wang L. A fair concurrent signature scheme based on identity [C]. High Performance Computing and Applications-HPCA2009, Shanghai, China, Aug. 2009: 198–205.

[15] Zhang J and Gao S. Efficient strong fair concurrent signature scheme [C]. International Conference on E-Business and E-Government, Guangzhou, China, May 2010: 1327–1330.

刘文琦： 女，1973 年生，副教授，研究方向为安全协议、电子商务.

顾 宏： 男，1961 年生，教授，研究方向为电子商务.

杨建华： 男，1958 年生，教授，研究方向为电子商务.