一个基于 CPK 的高效签密方案

陈永刚[①] 贾春福[①] 吕述望[②]
[①](南开大学信息技术科学学院 天津 300071)
[②](信息安全国家重点实验室 北京 100049)

摘 要：基于组合公钥原理，该文提出一个新的签密方案 CPK-SC，抛弃了传统基于身份签密方案中的配对运算，并通过使用对称密码算法解决了传统基于身份签密方案只能处理定长消息的限制。与已有的基于双线性对的签密方案相比，CPK-SC 方案计算量小、生成密文短，适用于计算和通信资源受限环境，具有广泛的应用前景。在判定性 Diffie-Hellman(DDH)假设下，论文通过随机预言模型证明了 CPK-SC 的安全性。

关键词：签密；组合公钥；随机预言模型；Decisional Diffie-Hellman(DDH)
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2009)07-1753-05

An Efficient Signcryption Scheme Based on CPK

Chen Yong-gang[①] Jia Chun-fu[①] Lü Shu-wang[②]
[①](*College of Information Technical Science*, *Nankai University*, *Tianjin* 300071, *China*)
[②](*State Key Laboratory of Information Security*, *Beijing* 100049, *China*)

Abstract: In this paper, a new signcryption scheme called CPK-SC is proposed based on Combined Public Key (CPK) to resolve the authentication and non-repudiation problem. CPK-SC discards the pairings and solves the restriction that the traditional identity-based signcryption schemes can only deal with fixed length messages by introduction symmetric cryptography algorithm. CPK-SC spends fewer computations and produces shorter ciphertext, which can be widely used in the environment of computation and communication resource constrained, such as mobile ad-hoc network. In the random oracle model, the security of CPK-SC is tightly related to the Decision Diffie-Hellman (DDH) assumption.

Key words: Signcryption; Combined Public Key (CPK); Random oracle model; Decisional Diffie-Hellman (DDH)

1 引言

在网络通信中，通常采用“先签名后加密”的方式保证消息的保密性、完整性和不可否认性。1997 年，Zheng 在文献[1]中首次提出了签密的概念，其思想就是在一个合理的逻辑步内实现加密和签名两项功能。签密需要较少的计算和通信资源，较适用于计算能力和通信资源受限的环境。2002 年，Malone-Lee 在文献[2]中给出了第一个基于身份的签密方案。

2003 年，南湘浩教授在文献[3]首次提出了组合公钥(Combined Public Key, CPK)体制，其构建于椭圆曲线之上，使用基于身份的密码思想，有效减少了密钥管理问题。现有的基于身份的签密方案(如文献[4–9]等)均是基于双线性对构建，并不适用于 CPK 体制，并且这些方案大多只能处理定长消息，对于长度不足的消息，或不能处理，或需要增加冗余消息，这不仅会增加签密方的计算负担，而且也消减了签密方案节省通信资源的优点。

本文提出了一个适用于 CPK 体制、基于身份的签密方案 CPK-SC，该方案不仅能处理任意长消息，而且具有计算量小、生成密文短等优点，非常适用与计算资源和带宽受限的环境(如 Ad-hoc 网络)。

2 基础知识

CPK 依据 ECDLP 构建公、私钥矩阵，密钥生成中心 KGC 采用组合算法实现用户密钥的生产、存储与分发。设 $a,b \in F_p$ (阶为 p 的有限域)且 $4a^3+27b^2 \neq 0$。$y^2 = x^3 + ax + b \mod p$ 的所有解加上无穷远点〇构成椭圆曲线群 $Ep(a,b)$。G 是 $Ep(a,b)$ 的 n 阶子群，基元是 P。根据 $T=(a,b,P,n,p)$，KGC 构建公私钥种子矩阵($m \times h$ 阵)PKM 和 SKM，PKM 中元素记为 $R_{i,j}$ $(0 \le i \le m-1, 0 \le j \le h-1)$，SKM 中元素记为 $r_{i,j}$ $(r_{i,j} \in Z_n^*)$，其中 $R_{i,j} = r_{i,j} \cdot P$。

用户密钥由 KGC 生产(公钥可根据公共参数自己生产)，通过对用户 ID 的 hash 和映射运算，ID 被映射为 PKM 和 SKM 中的坐标，选取对应的密钥种子组合生成密钥。设 ID 映射的坐标为 (i_1, j_1)，

2008-09-08 收到，2009-01-12 改回
天津市应用基础及前沿技术研究计划项目(09JCBJC00300)和天津市科技发展计划项目基金(05YFGZGX24200)资助课题

$\cdots,(i_t,j_t)$，则 SK=$(r_{i_1,j_1}+\cdots+r_{i_t,j_t})\bmod n$，PK=$R_{i_1,j_1}+\cdots+R_{i_t,j_t}$。文中$|n|$表示位长度(若$|n|=0$,则$n$用$\theta$表示)；$a\,||\,b$表示位串$a$和$b$的连接；$[m]_q$表示从$m$(二进制表示)的最低位往高位依次取$q$比特；$[m]_{\bar{q}}$表示执行$[m]_q$后余下的位串。

3 签密方案的形式化定义

3.1 签密方案的组成

基于身份的签密方案由以下 4 个算法组成。

Setup：系统初始化算法。KGC 保密 SKM，公布 Param = {T,PKM}。

Keygen：密钥生成算法。输入用户 ID，计算公私钥pk_{ID}和sk_{ID}，并安全返送用户。

Signcrypt：签密算法。输入$m,\mathrm{ID}_B,sk_{\mathrm{ID}_A}$，计算密文$\sigma$=Signcrypt($m,sk_{\mathrm{ID}_A},\mathrm{ID}_B$)。

Unsigncrypt：解签密算法。输入$\sigma,sk_{\mathrm{ID}_B},\mathrm{ID}_A$，输出$m$或符号“⊥”(解签密失败)。

注：此处若σ=Signcrypt($m,sk_{\mathrm{ID}_A},\mathrm{ID}_B$)，则$m$=Unsigncrypt($\sigma,\mathrm{ID}_A,sk_{\mathrm{ID}_B}$)。

3.2 DDH 难题及安全模型

定义 1(DDH 难题) $E(F_p)$是椭圆曲线，给定 P, aP, bP, cP$\in E(F_p)$，判定 cP=abP。

定义 2 如果没有任何多项式有界的敌手以不可忽略的优势赢得以下游戏，则称基于身份的签密方案在自适应选择密文和身份攻击下具有不可区分性(IND-IBSC-CCIA)。

(1)挑战者C运行 Setup 算法，并将 Param 发送给敌手A。A执行下列查询：

Keygen 查询：包括公私钥查询。A选择 ID，C计算pk_{ID}和sk_{ID}，并将结果返送A；

Signcrypt 查询：A选择$\mathrm{ID}_i,\mathrm{ID}_j$和明文$m$，$C$计算$\sigma$=Signcrypt($m,sk_{\mathrm{ID}_i},\mathrm{ID}_j$)并返送$A$；

Unsigncrypt 查询：A选择$\mathrm{ID}_i,\mathrm{ID}_j$和密文$\sigma$，$C$计算 Unsigncrypt($\sigma,\mathrm{ID}_i,sk_{\mathrm{ID}_j}$)，并将结果(可以是“⊥”)返送$A$；

(2)A选择明文$m_0,m_1(|m_0|=|m_1|)$，同时选择$\mathrm{ID}_A,\mathrm{ID}_B$，$A$没有查询过$H(\mathrm{ID}_A)$，也没有查询过$\mathrm{ID}_B$的私钥。$C$随机选择$b\in\{0,1\}$，计算$\sigma$=Signcrypt($m_b,sk_{\mathrm{ID}_A},\mathrm{ID}_B$)并返送$A$；

(3)A执行多项式有界次查询，但不能查询ID_B的私钥，也不能对σ执行 Unsigncrypt 查询；最后A输出b',如果$b'=b$，则A赢得游戏。定义A的优势为$Adv(A)=|2\Pr[b'=b]-1|$。

注：对签密方案的存在性不可伪造(EUF-IBSC-ACMIA)定义等同采用文献[4]的定义。

4 CPK-SC 方案

Setup: 根据参数T，KGC 生成 PKM 和 SKM。另外，KGC 还选取 Hash 函数：$H:\{0,1\}^*\to\{0,1\}^r$,$H_1:G\to\{0,1\}^l$,$H_2:\{0,1\}^*\to Z_n^*$,$F:\{0,1\}^*\to\{0,1\}^t$,对称密码算法(E,D)(密钥长度为l)。KGC 保密 SKM，公开系统参数 Param = {T,PKM,H,$H_1,H_2,F,(E,D)$}。

Keygen: 给 KGC 用户 ID，KGC 计算H(ID)，根据H(ID)和映射算法，从 PKM 和 SKM 中选取元素组合pk_{ID}和sk_{ID}，并将$(pk_{\mathrm{ID}},sk_{\mathrm{ID}})$返送用户。

Signcrypt: 设发送者 Alice 标识为ID_A；接收者 Bob 标识为ID_B；消息为m。

(1)随机选$\omega\in Z_n^*$，计算$r_1=\omega\cdot P$，$k_1=H_1(r_1)$；

(2)计算$r_2=\omega\cdot pk_{\mathrm{ID}_B}$，$k_2=H_1(r_2)$；

(3)计算$c_1\,||\,c_2=c=E_{k_2}(m)$($|c_2|\le|c|$，若$|c_2|=|c|$，则$c_1=\theta$)；

(4)计算$f=c_2\,||\,F(c)$，$r=E_{k_1}(f)$，$\tau=H_2(r)$；

(5)计算$S=\omega-\tau\cdot sk_{\mathrm{ID}_A}$；

Alice 发送$\sigma=(c_1,r,S)$给解签密者 Bob。

Unsigncrypt: 解签密流程如下。

(1)计算$\tau=H_2(r)$，$r_1=S\cdot P+\tau\cdot pk_{\mathrm{ID}_A}$，$k_1=H_1(r_1)$；

(2)计算$r_2=r_1\cdot sk_{\mathrm{ID}_B}$，$k_2=H_1(r_2)$；

(3)计算$f'=D_{k_1}(r)$，$c_2'=[f']_{\bar{t}}$，$m=D_{k_2}(c_1\,||\,c_2')$；如果$[f']_t=F(c_1\,||\,c_2')$，则接受密文σ。

5 CPK-SC 分析

5.1 安全性分析

(1)保密性

定理 1 在随机预言模型中,如果存在一个 IND-IBSC-CCIA 敌手A能够在t时间内，进行最多q_H / q_K / q_S / q_U次 H / Keygen / Signcrypt / Unsigncrypt 查询，以优势ε赢得定义 2 中的游戏，则存在敌手C能够在时间t^*内，以优势$Adv_B^{\mathrm{DDH}(G,P)}(|n|)$解决 DDH 问题。其中：$Adv_B^{\mathrm{DDH}(G,P)}(|n|)>[\varepsilon-(\varepsilon+1)\max\{q_U/2^l,q_U/2^t\}](q_H-1)(q_H-q_K)/2q_H^2$，$t^*<t+[4q_S^2+(2q_{H_1}+1)q_S+3q_U]t_{pm}$，$t_{pm}$表示点乘运算所需时间。

证明 假设C得到随机实例(P,a_1P,a_2P,a_3P)和实例$\mathrm{str}_1,\mathrm{str}_2\in\{0,1\}^r$。$C$把$A$作为子例程并扮演$A$的挑战者。游戏开始，$C$将系统参数给$A$，同时，$C$需要维护列$L_H$ / L_{H_1} / L_{H_2} / L_F / L_P,分别记录A查询H / H_1 / H_2 / F / Keygen_{pk}的回答，初始化均为空。此外假设在 ID 用于 Signcrypt, Unsigncrypt 和 Keygen 查询时，A已查询过H(ID)，并且A对同一个 ID 只能进行一次 Keygen 查询。另外，Signcrypt

查询返回的密文，将不会用于 A 的 Unsigncrypt 查询中。

***H* 查询**：C 首先从 q_H 次查询中随机选取一次(不失一般性，设为第 i 次)，当 A 请求 $H(\mathrm{ID}_j)$ ($j\in\{1,2,\cdots,q_H\}$)时：

(a)若 $j\neq i$，C 查询 L_H，若 L_H 中含有该查询记录，则用此记录回复 A；否则 C 从随机带 Θ 中随机选取 r 位(记为 r_j)作为对 $H(\mathrm{ID}_j)$ 查询的回答，并将 (ID_j, r_j) 放入 L_H；

(b)若 $j=i$，用 str_1 回复 A，其中 str_1 是游戏开始时 C 获取的例值。

***H*$_1$ / *H*$_2$ / *F* 查询**：若 L_{H_1} / L_{H_2} / L_F 中有相应查询记录，则用记录回复 A；否则 C 随机选取 k / τ / φ 回复 A，并分别记录在 L_{H_1} / L_{H_2} / L_F 中。

Keygen 查询：

(a) Keygen_{pk} 查询：若 $\mathrm{ID}=\mathrm{ID}_i$，$C$ 用 a_2P 回复；否则，L_H 必含有(ID, r)，若 L_P 含有 (r, pk_{ID})，返回 pk_{ID}；否则，C 根据 r 组合公钥 pk_{ID}，返回 pk_{ID}，并将 (r, pk_{ID}) 存入 L_P。

(b) Keygen_{sk} 查询：若 $\mathrm{ID}=\mathrm{ID}_i$，$C$ 将失败并终止游戏；若 $\mathrm{ID}\neq\mathrm{ID}_i$，$C$ 根据 r 和映射算法，从 SKM 中选取元素组合私钥 sk_{ID}，返送给 A。

Signcrypt 查询：当 A 做关于$(m, \mathrm{ID}_A, \mathrm{ID}_B)$的 Signcrypt 查询时：

(a)若 $\mathrm{ID}_A\neq\mathrm{ID}_i$：$C$ 计算 Signcrypt $(m, sk_{\mathrm{ID}_A}, pk_{\mathrm{ID}_B})$并回复 A。

(b)若 $\mathrm{ID}_A=\mathrm{ID}_i$ 且 $\mathrm{ID}_B\neq\mathrm{ID}_i$：$C$ 随机选取 $S,\tau\in Z_n^*$，计算 $r_1=S\cdot P+\tau\cdot pk_{\mathrm{ID}_A}$，模拟 H_1 得到 k_1，如果 L_{H_1} 中包含$(r_1, *)$或 $r_1=a_1P$，重新选择 τ 并计算 r_1。计算 $r_2=r_1\cdot sk_{\mathrm{ID}_B}$，模拟 H_1 得 k_2。计算 $c=E_{k_2}(m)$，模拟 F 得 φ，计算 $f=c_2\,||\,\varphi$ 和 $r=E_{k_1}(f)$，并将 (r,τ) 放入 L_{H_2} 中。C 将密文 $\sigma=(c_1,r,S)$ 返送给 A，从 A 的角度看，密文 σ 是有效的。

(c)若 $\mathrm{ID}_A=\mathrm{ID}_B=\mathrm{ID}_i$：$C$ 随机选取 $S^*,\tau^*\in Z_n^*$，计算 $r_1^*=S^*\cdot P+\tau^*\cdot pk_{\mathrm{ID}_A}$，模拟 H_1 得到 k_1^*，如果 L_{H_1} 中包含$(r_1^*, *)$或 $r_1^*=a_1P$，重新选择 τ^* 并计算 r_1^*。C 随机选取 $r_2^*\in G$ 与 $k_2^*\in\{0,1\}^n$，确保 L_{H_1} 中不含有$(r_2^*, *)$和$(*, k_2^*)$，计算 $c^*=E_{k_2^*}(m)$，模拟 F 得 φ^*，计算 $f^*=c_2^*\,||\,\varphi^*$ 和 $r^*=E_{k_1^*}(f^*)$，并将 (r^*,τ^*) 放入 L_{H_2} 中。C 将密文 $\sigma^*=(c_1^*,r^*,S^*)$ 返送给 A，因为 A 不对 σ^* 进行 Unsigncrypt 查询，所以他并不知道 σ^* 是否是关于明文 m 的有效密文。

Unsigncrypt 查询：当 A 对从 ID_A 到 ID_B 的密文 $\sigma'=(c_1', r', S')$ 做 unsigncrypt 查询时：

(a)若 $\mathrm{ID}_B=\mathrm{ID}_i$，$C$ 总是回复 A “$\perp$”。所以下述情形 C 也总是回复 σ' 无效：L_{H_2} 包含 (r',τ')，L_{H_1} 包含 $(S'\cdot P+\tau'\cdot pk_{\mathrm{ID}_A}, k_1')$，$L_F$ 包含 $(c_1'\,||\,[D_{k_1'}(r')]_{\bar{t}}, x)$ ($x=[D_{k_1'}(r')]_t$ 的概率为 $1/2^t$)。而此时，从 A 的角度来看，若 L_F 中包含 $(c_1'\,||\,[D_{k_1'}(r')]_{\bar{t}}, [D_{k_1'}(r')]_t)$，则 σ' 为有效密文。

(b)若 $\mathrm{ID}_B\neq\mathrm{ID}_i$：若 L_{H_2} 不含有$(r', *)$，则回复 “$\perp$”；否则，L_{H_2} 中存在 (r',τ')，计算 $r_1'=S'\cdot P+\tau'\cdot pk_{\mathrm{ID}_A}$。若 L_{H_1} 中不含有$(r_1', *)$，则回复 “$\perp$”；否则，L_{H_1} 中存在(r_1', k_1')，计算 $f'=D_{k_1'}(r')$，$c'=c_1'\,||\,[f']_{\bar{t}}$。若 L_F 不含有$(c', *)$或存在(c', x)且 $[f']_t$，则回复 “$\perp$”；否则，计算 $r_2'=r_1'\cdot sk_{\mathrm{ID}_B}$。若 L_{H_1} 不含有$(r_2', *)$，随机选取 $k_2'\in\{0,1\}^n$，且 L_{H_1} 中不含有 $(*, k_2')$，将(r_2', k_2')存入 L_{H_1} 中，计算 $m'=D_{k_2'}(c')$，返回 m'。此时，拒绝一个有效密文的概率不超过 $\max\{q_U/2^{|n|}, q_U/2^l, q_U/2^t\}=\max\{q_U/2^l, q_U/2^t\}$ ($|n|>t$)。

综合(a),(b)可以得到，对所有查询，拒绝一个有效密文的概率不超过 $\max\{q_U/2^t, \max\{q_U/2^l, q_U/2^t\}\}=\max\{q_U/2^l, q_U/2^t\}$。

经过上述仿真阶段后，A 选择它希望挑战的身份 $(\mathrm{ID}_j,\mathrm{ID}_i)(j\neq i)$(如果仿真阶段 A 进行了 $H(\mathrm{ID}_j)$ 或 $\mathrm{Keygen}_{sk}(\mathrm{ID}_i)$ 查询，C 会失败。则 C 不失败的概率大于 $(1-1/q_H)\cdot(C_{q_H-1}^{q_K}/C_{q_H}^{q_K})$)并产生两个明文 m_0 和 m_1 ($|m_0|=|m_1|$)，C 随机选取 $b\in\{0,1\}$ 并签密 m_b 如下：

(a)置 $r_1''=a_1P$，$r_2''=a_3P$，$H(\mathrm{ID}_j)=\mathrm{str}_2$，并将 $(\mathrm{ID}_j,\mathrm{str}_2)$ 存入 L_H；

(b)随机选取 $S'',\tau''\in Z_n^*$，令 $pk_{\mathrm{ID}_j}=\tau''^{-1}(r_1''-S''\cdot P)$，将$(\mathrm{str}_2, \tau''^{-1}(r_1''-S''\cdot P))$存入 L_P；

(c)计算 $k_2''=H_1(r_2'')$，$c_{b_1}\,||\,c_{b_2}=c_b=E_{k_2''}(m_b)$，$\varphi''=F(c_b)$，$f=c_{b_2}\,||\,\varphi''$；

(d)计算 $k_1''=H_1(r_1'')$，$r''=E_{k_1''}(f)$，并将 (r'',τ'') 存入 L_{H_2}，将 $\sigma''=(c_{b_1}, r'', S'')$ 返送给 A。

像在仿真阶段一样，A 执行一系列查询，C 处理这些查询，最后，A 产生一个 $b'\in\{0,1\}$，他认为 $\sigma''=\mathrm{Signcrypt}(m_{b'}, sk_{\mathrm{ID}_j}, pk_{\mathrm{ID}_i})$。如果 $b'=b$，C 回复 1，否则回复 0。

通过上面的分析，我们可以获得定理 1 中的结论。　　证毕

(2)不可伪造性、公开验证性和前向安全性　如果有敌手能伪造 CPK-SC 签名，那么他就能伪造文献[10]中的 CPK-SMR。由于在选择消息和身份攻击下 CPK-SMR 具有存在性不可伪造性，因此，CPK-

表 1 签密后消息总长度

方案	$\lvert m \rvert \geq \lvert (\lvert n \rvert +1)/2 \rvert$	$\lvert m \rvert < \lvert (\lvert n \rvert +1)/2 \rvert$
文献[4]	$\lvert m \rvert + \lvert (\lvert n \rvert +1)/2 \rvert + \lvert G \rvert$	$\lvert m \rvert + \lvert n \rvert + \lvert G \rvert$
文献[8]	$\lvert m \rvert + \lvert n \rvert + \lvert G \rvert$	$\lvert m \rvert + \lvert n \rvert + \lvert G \rvert$
文献[9]	$\lvert m \rvert + \lvert n \rvert +2 \lvert G \rvert$	$\lvert m \rvert + \lvert n \rvert +2 \lvert G \rvert$
CPK-SC	$\lvert m \rvert + \lvert (\lvert n \rvert +1)/2 \rvert + \lvert n \rvert$	$\lvert m \rvert + \lvert (\lvert n \rvert +1)/2 \rvert + \lvert n \rvert$

注：为便于比较，以文献[4]中定义的冗余消息长度为基准，将本文中 t 设定为 $\lvert (\lvert n \rvert +1)/2 \rvert$。

表 2 签密算法运行效率

方案	Signcryption					Unsigncryption			
	pm	exps	pcs	inv	encry	pm	exps	pcs	decry
文献[4]	2	2	2	/	1	/	2	4	1
文献[8]	2	2	2	/	1	/	2	4	1
文献[9]	2	/	/	1	1	2	/	2	1
CPK-SC	2	/	/	/	2	3	/	/	2

注：表 2 中，pm/exps/pcs/inv 分别表示加法群上的点乘运算/乘法群上的指数运算/配对运算/求逆运算，encry 和 decry 分别表示对称密码算法的加、解密运算。符号“/”表示无此运算。

SC 也是 EUF-IBSC-ACMIA 安全的。

提交(k_2, m, σ)给第三方，第三方计算 $r_1 = S \cdot P + H_2(r) \cdot pk_{\mathrm{ID}_A}, k_1 = H_1(r_1), f' = D_{k_1}(r)$ 和 $c_2^{'} = [f']_{\bar{t}}$。如果 $[f']_t = F(c_1 \,||\, c_2^{'})$，则接受密文 σ，如果 $m = D_{k_2}(c_1 \,||\, c_2^{'})$，则通过验证。

即使第三方获取了 sk_{ID_A}，也无法破解 $r_1 \cdot sk_{\mathrm{ID}_B}$，因此，CPK-SC 满足前向安全性。

5.2 性能分析

本节从计算量和通信量两个方面对 CPK-SC 的性能进行分析。在前面提到的基于身份的签密方案中，只有文献[4，8，9]使用到了对称密码算法并且具有任意长消息处理能力，因此，这里将 CPK-SC 与文献[4，8，9]中提到的方案进行比较，结果见表 1 和表 2。

从上述比较可以看出，CPK-SC 具有较短的签密后密文总长度，尤其当消息长度小于某一特定值（如 $\lvert m \rvert < \lvert (\lvert n \rvert +1)/2 \rvert$）时优势更为明显。虽然 CPK-SC 多使用了一次对称密码算法，但由文献[11]中给出的计算复杂性关系可知，CPK-SC 的运算效率却是最高的。

6 结束语

基于 CPK 原理，本文提出了一个新的基于身份的签密方案，并在随机预言模型中给出了该方案的安全性证明，在 DDH 问题是困难的假设下，CPK-SC 是 IND-IBSC-CCIA 和 EUF-IBSC-ACMI 安全的。与目前存在的签密方案相比，CPK-SC 抛弃了双线性对运算，具有运算效率高、产生密文短等特点，更适合于计算和通信资源受限的环境。

参 考 文 献

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

[2] Malone-Lee J. Identity based signcryption. cryptology ePrint archive[R]. Report 2002/098, IACR, 2002.

[3] 南湘浩, 陈钟. 网络安全技术概论. 北京: 国防工业出版社, 2003, 第 2 章.
Nan Xiang-hao and Chen Zhong. A Profile to Network Security Techniques[M]. Beijing: National Defence Industry Press, 2003, Chapter 2.

[4] Chen H Y, Lü S W, and Liu Z H, *et al*.. An identity-based signcryption scheme with short ciphertext from pairings[C]. Emerging Directions in Embedded and Ubiquitous Computing workshops 2006, 2006, LNCS 4097: 342–351.

[5] Barbosa M and Farshim P. Certificateless signcryption[C]. ACM Symposium on Information, Computer and Communications Security, Tokyo, Japan. ACM, 2008: 369–372.

[6] Li F and Yu Y. An efficient and provably secure ID-based threshold signcryption scheme[C]. International conference on communications, circuits and systems. Xiamen, China, 2008: 488–492.

[7] Ren Y L and Gu D W. Efficient identity based signature/signcryption scheme in the standard model[C]. The 1th International Symposium on Data, Privacy and E-Commerce. Chengdu, China, 2007: 133–137.

[8] Libert B and Quisquater J J. New identity based signcryption schemes from pairings[C]. IEEE Information Theory Workshop. Paris, France, 2003: 155–158.

[9] Ma C S. Efficient short signcryption scheme with public verifiability[C]. Inscrypt 2006, 2006, LNCS 4318: 118–129.

[10] Chen Y G, Jia C F, and Lü S W, *et al*.. Signature scheme with arbitrary length message recovery in combined public key[C]. The 4th International conference on Mobile Ad-hoc and Sensor Networks. Wuhan, China, 2008: 55–58.

[11] Zhong X, Dai G Z, and Yang D M. An efficient online/offline signcryption scheme for MANET [C]. IEEE Advanced Information Networking and Applications Workshops. Ontario, Canada, 2007: 171–176.

陈永刚： 男，1980 年生，博士生，研究方向为信息安全与密码学.

贾春福： 男，1967 年生，教授，博士生导师，研究方向为信息安全.

吕述望： 男，1941 年生，教授，博士生导师，研究方向为信息安全与密码学.