# 新的基于身份的(t,n)门限签密方案①

朱春意[1]，陈 勤[1]，徐 坤[2]

[1](杭州电子科技大学 计算机学院，杭州 310017)
[2](宁波市公安局 网络警察支队，宁波 315040)

**摘 要：**针对现有的门限签密方案效率低不太实用的不足，以及基于身份的签密系统密钥托管问题，利用双线性对提出了一个新的基于身份的(t,n)门限签密方案。通过引入签密者秘密信息，实现了密钥生成中心的不可诬陷性。与典型的基于身份的门限签密方案相比，效率更高，实用性更强。

**关键词：**基于身份；密钥托管；门限签密；双线性对

## New ID-Based (t,n) Threshold Signcryption Scheme

ZHU Chun-Yi[1], CHEN Qin[1], XU Kun[2]

[1](College of Computer, Hangzhou Dianzi University, Hangzhou 310017, China)
[2](Cyber Cop Datachment Police of Ningbo, Ningbo 315040, China)

**Abstract:** Against the shortage of low efficiency of the existing threshold signcryption scheme and the key escrow in the id-based cryptosystem, a new identity-based (t, n) threshold signature encryption scheme is proposed from bilinear pairings. Our scheme can resist the private key generator to entrap through the introduction of secret information of the signcryptioner. Our scheme is more efficient and practical than the existing scheme.

**Keywords:** ID-based; key escrow; threshold signcryption; bilinear pairings

## 1 概述

签密能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能，同时实现了消息传输的保密性和认证性，而其计算量和通信成本都远远低于传统的“先签名后加密算法”，因而是消息安全传输较为理想的方法。

基于身份密码系统的提出简化了密钥管理问题。在该系统中，用户的身份信息可以是用户的姓名、身份证号码、E-MAIL 地址等，密钥生成中心（PKG）根据用户的身份信息生成用户的公私钥对，并通过安全信道发送给用户。

基于身份的(t,n)门限签密简化了密钥管理，实现了签名权利的分配，抗攻击能力更强，提高了系统的安全性，降低了计算量和通信成本，近年来被广泛研究。

S.Duan 等人在文献[4]中利用双线性对提出了一个基于身份的门限签密方案，并证明了它的健壮性。然而，在他们的方案里，一个密钥生成者 PKG 的系统私钥要发送给其它 PKG，造成了 PKG 私钥的泄漏，影响了方案的实际应用性。而在部分私钥生成阶段，签名成员收到部分私钥后无法对自己所得的部分私钥份额进行验证，影响了方案的安全性。

Fagen Li 和 Yong Yu 在文献[5]中提出了一个高效的基于身份的签密方案。他们的方案虽然高效却有一个安全漏洞，联合部分签名生成最终门限密文的指定职员可以根据自己收集到的部分签名恢复出群私钥。S.Sharmila Deva Selvi 等人虽然在文献[6]中给出了文献[5]的改进方案，然而，新方案还是无法抵抗 PKG 的不可诬陷性。

本文用双线性对提出的基于身份的门限签密方案实现了 PKG 的不可诬陷性，相比于 Fagen Li 等人在文献[5]中提出的方案以及 S.Sharmila Deva Selvi 等人在文献[6]中提出的方案效率更高。

① 收稿时间:2010-08-10;收到修改稿时间:2010-09-11

## 2 预备知识

### 2.1 双线性映射

设$G_1$是一个阶为素数 q 的循环加法群，$G_2$是一个阶为 q 的循环乘法群，P 是$G_1$的生成元。双线性映射[7]是指具有下列性质的映射 e：$G_1 \times G_1 \to G_2$：

(1)双线性。对所有的 P,Q$\in G_1$和 a,b$\in Z_q^*$，e(aP,bQ)=e(abP,Q)=e(P,Q)$^{ab}$

(2)非退化性。存在一个 P$\in G_1$，满足 e(P,P)$\neq 1$。

(3)可计算性。对 P,Q$\in G_1$，存在一个有效的算法计算 e(P,Q)。

双线性映射可以从超奇异椭圆曲线中的 Weil 和 Tate 配对中得到。

### 2.2 相关数学难题

$G_1$是一个加法群，4 个相关困难问题如下：

(1)DLP(discrete logarithm problem)难题。P,Q$\in G_1$，求正整数 n$\in Z_q^*$，使之满足 Q=nP 是困难的。

(2)CDHP(computational Diffie-Hellman problem)难题。已知 P,aP,bP，计算 abP 是困难的，其中 a,b$\in Z_q^*$。

(3)DDHP(decision Diffie-Hellman problem)难题。已知 P,aP,bP,cP$\in G_1$，其中 a,b,c$\in Z_q^*$,要判定 cab mod q 是否成立是困难的。

(4)双线性配对求逆难题。即给出 P$\in$G 和 e(P,Q)$\in V$,找 Q$\in G$ 还不存在有效的算法。

## 3 新的基于身份的(t,n)门限签密方案

本方案是基于文献[8]的秘密共享技术，利用双线性对提出的。方案中涉及四方：密钥生成中心 PKG，n 个签名者组成的身份为$ID_A$的发送者集合 A=$\{M_1,..,M_n\}$，最终门限签密的生成者 C，身份为$ID_B$的接收者 B。本方案中还需要一个公告牌[9]，用于公布一些公开信息，这就减少了 C 和集合 A 中签名成员的频繁交互，同时也减少了密文的长度。

### 3.1 系统初始化

给定安全参数 k，PKG 先选取椭圆曲线上 2 个 q 阶的循环加法群 $G_1$和循环乘法群 $G_2$，P 是 $G_1$的生成元，由 $G_1$和 $G_2$上的 Weil 对或 Tate 对的变形构成的双线性映射为 e：$G_1 \times G_1 \to G_2$。PKG 随机选取自己的系统私钥$s \in Z_q^*$，并计算自己的公钥$P_{pub} = sP \in G_1$；选取安全的对称密码算法$(E,D)$；并定义三个散列函数$H_1:\{0,1\}^{l_0} \to G_1, H_2:G_2 \to Z_q^*$，$H_3:G_2 \times \{0,1\}^n \to Z_q^*$，其中$l_1$是身份$ID$的比特长度，n 是明文的比特长度。PKG 公布系统参数$\{G_1,G_2,e,P,P_{pub},E,D,H_1,H_2,H_3\}$,保密主密钥 s。

### 3.2 密钥生成

C 随机选择$k_A \in Z_q^*$，计算$J_A = k_A P \in G_1$，并发送$J_A$给 PKG。PKG 计算发送者集合 A 的公钥$Q_A = H_1(ID_A, J_A)$,私钥$S_A = sQ_A$。并根据接收者 B 的身份计算 B 的公钥$Q_B = H_1(ID_B)$,私钥$S_B = sQ_B$，并通过安全信道发送$S_B$给接收者 B。

假设门限值 t 和 n 满足$1 \le t \le n < q$,为了在群 A 中分享私钥$S_A$，PKG 依次执行以下步骤：

(1)从$G_1^*$中随机选择$F_1,\ldots,F_{t-1}$，构造一个多项式$F(x) = S_A + xF_1 + \cdots + x^{t-1}F_{t-1}$，并计算$S_i = F(i), i = 0,\ldots n$。其中$S_0 = S_A$。

(2)秘密发送$S_i$给成员$M_i$，$i = 1,\ldots,n$，然后广播$y_0 = e(S_A, P)$和$y_j = e(S_j, P), j = 1,\ldots,t-1$。

(3)每个成员$M_i$通过等式$e(S_i,P) = \prod_{j=1}^{t-1} y_j^{i^j}$检查自己的份额是否合法。如果不合法，$M_i$广播一个错误，拒绝接受该部分私钥，并要求一个合法的份额。

### 3.3 签密

不失一般性，我们假设$M_1,\ldots,M_t$这 t 个成员代表集合 A 对明文 m 进行签密。

首先，每个签名者$M_i$计算$w_i = e(\eta_i S_i, Q_B)$，并发送给 C，其中$\eta_i = \prod_{j=1, j\neq i}^{t} -j(i-j)^{-1} \bmod q$。

C 随机选取$k_1 \in Z_q^*$，计算$w = \prod_{i=1}^{t} w_i$，$r_2 = H_2(w)$, $t = E_{r_2}(m)$, $r = e(Q_B,P)^{r_A}$, $v = H_3(r,m)$,并将$v$发布到公告牌上，保密$k_1$。

每个签名者$M_i$收到从公告牌上查询$v$后随机选择$k_{2i} \in Z_q^*$，计算$U_i = v\eta_i S_i + k_{2i} Q_B$，其中$\eta_i = \prod_{j=1, j\neq i}^{t} -j(i-j)^{-1} \bmod q$，$R_i = k_{2i} P$,$(U_i, R_i)$并将作为自己的部分签名发送给 C。

C 收到$M_i$发送来的部分签名$(U_i, R_i)$后，首先验证下面的等式是否成立：

$$e(U_i,P) = e(R_i, Q_B)(\prod_{j=0}^{t-1} y_j^{i^j})^{v\eta_i}$$

当且仅当等式成立，接受$M_i$的部分签名；否则，拒绝该部分签名，广播一个错误，并要求一个合法的部分签名。

C 收到所有 t 个签名者的部分签名并都验证通过后计

算：$R=\sum_{i=1}^{t}R_i$，$K=k_1^{-1}P$，$U=k_1(\sum_{i=1}^{t}U_i+r_AQ_B)$，将$(R,K)$发布到公告牌上，并生成最终的门限密文为：

$$\sigma=(U,t)$$

通过安全信道将$\sigma$发送给 B。

### 3.4 解签密

B 收到$\sigma$后，从公告牌上查询$(R,v)$，并依次计算：

$$w=e(S_B,Q_A)$$
$$r_2=H_2(w)$$
$$m=D_{r_2}(t)$$
$$r=e(U,K)e(Q_B,-R)e(Q_A,P_{pub})^{-v}$$

当且仅当$v=H_3(r,m)$成立时接收$\sigma$。

## 4 安全性和效率分析

### 4.1 正确性

可以通过以下等式证明：

$$w=\prod_{i=1}^{t}w_i=\prod_{i=1}^{t}e(\eta_iS_i,Q_B)$$
$$=e(\sum_{i=1}^{t}\eta_iS_i,Q_B)=e(S_A,Q_B)$$
$$=e(sQ_A,Q_B)=e(S_B,Q_A)$$

$$\begin{aligned}
&e(U,K)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=e(k_1^{-1}(\sum_{i=1}^{t}U_i+r_AQ_B),K)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=e(\sum_{i=1}^{t}(v\eta_iS_i+k_{2i}Q_B)+r_AQ_B,P)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=e(vS_A+\sum_{i=1}^{t}k_{2i}Q_B+r_AQ_B,P)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=e(vS_A,P)e(\sum_{i=1}^{t}k_{2i}Q_B,P)e(r_AQ_B,P)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=e(sQ_A,P)^ve(Q_B,\sum_{i=1}^{t}k_{2i}P)e(Q_B,P)^{r_A}e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=re(Q_A,sP)^ve(Q_B,R)e(Q_B,-R)e(Q_A,P_{pub})^{-v}\\
&=re(Q_A,P_{pub})^ve(Q_A,P_{pub})^{-v}\\
&=r
\end{aligned}$$

正确性证毕。

### 4.2 安全性

#### 4.2.1 机密性

本文提出的方案的机密性是基于椭圆曲线上离散对数难题困难性基础上的。在系统主密钥没有泄露和随机预言模式下，任何人想要通过$P_{pub}=sP$和$P$来计算系统私钥在计算上都是不可行的。攻击者要想获取明文 m 都必须获得签密者私钥$S_A=sQ_A$,因而攻击者无法由密文$\sigma$获取明文信息 m，我们的方案具有机密性。

#### 4.2.2 不可伪造性

本方案的不可伪造性是基于 DLP 难题的。在随机预言模式下，我们首先假设密钥生成中心 PKG 是可信的，签密者的私钥未知。攻击者要想伪造一个发送方的密文必须先获得 PKG 的系统私钥 s。已知 P 和$P_{pub}=sP$，根据 DLP 难题的困难性，攻击者无法计算出系统私钥 s，也就无法计算出发送方的私钥$S_A=sQ_A$，更无法伪造出发送方的签名$U=k_1(vS_A+k_2Q_B+r_AQ_B)$。

#### 4.2.3 PKG 的不可诬陷性

假设 PKG 按以下步骤生成一个密文$\sigma'$：

随机选取$r_A',k_1',k_2\in Z_q^*$，并计算：

$$w=e(S_A,Q_B),r_2=H_2(w),t'=E_{r_2}(m')$$
$$r'=e(Q_B,P)^{r_A'},v'=H_3(r',m'),R'=k_2P$$
$$U'=k_1'(v'S_A+k_2Q_B+r_A'Q_B)$$

$K'=k_1'^{-1}P$，并将$(v',R',K')$发布到公告牌上，生成门限密文$\sigma'=(U',t')$。

下面将证明 PKG 伪造的门限密文$\sigma'=(U',t')$跟真正的门限密文$\sigma=(U,t)$是有区分的。对于真正的门限密文有：

$$\begin{aligned}
&e(U,K)\\
&=e(k_1^{-1}(\sum_{i=1}^{t}U_i+r_AQ_B),k_1^{-1}P)\\
&=e(\sum_{i=1}^{t}v\eta_iS_i+\sum_{i=1}^{t}k_{2i}Q_B+r_AQ_B,P)\\
&=e(vS_A+\sum_{i=1}^{t}k_{2i}Q_B+r_AQ_B,P)\\
&=e(S_A,P)^ve(Q_B,\sum_{i=1}^{t}k_{2i}P)e(r_AQ_B,P)\\
&=e(S_A,P)^ve(Q_B,K_3)e(Q_B,P)^{r_A}
\end{aligned}$$

而对于 PKG 产生的门限密文：

$$\begin{aligned}
&e(U',K')\\
&=e(k_1'(v'S_A+k_2Q_B+r_A'Q_B),k_1'^{-1}P)\\
&=e(v'S_A+k_2Q_B+r_A'Q_B,P)\\
&=e(S_A,P)^{v'}e(Q_B,k_2P)e(r_A'Q_B,P)\\
&=e(S_A,P)^{v'}e(Q_B,R')e(Q_B,P)^{r_A'}
\end{aligned}$$

因此，当 PKG 生成上述密文诬陷集合 A 时，C 通过出示秘密信息$r_A$就可证明$\sigma'$是 PKG 伪造的。

4.2.4 不可否认性

前文已证，任何人想要伪造签密者的签名在计算上都是不可行的，又因为签名中包含着签密者的信息，所以签密者不能否认其签名。

4.3 效率分析

$G_2$ 中的模指数运算记为 E，$G_1$ 中的标量乘运算记为 M，而 $G_1$ 中的配对运算记为 P。在我们的方案中，由于设计了很多预运算(尤其是配对运算)，提高了方案的执行效率。在签密前,集合 A 中的部分签名成员可以预先计算 $\eta_i S_i$，$e(\eta_i S_i, Q_B)$；最终的门限密文生成者 C 可以预先计算 $e(Q_B, P)^{r_A}$，U 中的 $r_A Q_B$。在解签密前，接收者可以预先计算 $e(S_B, Q_A), e(Q_A, P_{pub})$。

Fagen Li 等人在文献[5]中已经证明了他们的方案跟文献[4]和文献[10]相比是更高效的，文献[6]是对文献[5]的改进，本方案与它们的效率比较见表 1。

在基于双线性对的密码体制中，对算法效率起决定作用的是中的配对运算，所以提高整个算法效率的关键是如何处理好配对运算。由表 1 知，本文所述方案需要 4 次配对运算；而文献[5]和文献[6]的方案则都需要 2t+4 次配对运算，所以我们的算法效率明显更高。

## 5 结束语

本文利用双线性对提出的基于身份的门限签密方案不但实现了 PKG 的不可诬陷性，而且相比于之前典型的基于身份的门限签密方案效率更高，更有优势，实用性更强。

表 1

| | 签密 | | | 解签密 | | | 密文长度 |
|---|---|---|---|---|---|---|---|
| | *M* | *P* | *E* | *M* | *P* | *E* | |
| 文献[5] | 4*t* | 2*t*+1 | *t* | 1 | 3 | 0 | $2\|G_1\|+\|q\|$ |
| 文献[6] | 4*t* | 2*t*+1 | *t* | 1 | 3 | 0 | $2\|G_1\|+\|q\|$ |
| 我们的方案 | 3*t*+2 | 2 | *t* | 1 | 2 | 1 | $\|G_1\|+\|q\|$ |

## 参考文献


1 Zheng Y. Digital signcryption or how to achieve cost (Signature&Encryption)<<Cost(Signature)+Cost(Encryption) Crypto'971 Berlin: Springer, 1997. 165−179.

2 Zheng Y. Signcryption and its applications in efficient public key solution. ISW'97. LNCS 1397, Springer-Verlag, 1998: 291−312.

3 Shamir A. Identity-based cryptosystems and signature schemes. Advances in Cryptology-Crypto'84, LNCS 196, New York: Springer-Verlag, 1984. 47−53.

4 Duan S, Cao Z, Lu R. Robust ID-based threshold signcryption scheme from pairings. 3rd International Conference on Information Security. Shanghai, China, 2004. 33−37.

5 Li FG, Yu Y. Click on a pin to refine search results Reset Map Center and Zoom An efficient and Provably Secure ID-Based Threshold Signcryption Scheme. 2008 International Conference on Communications, Circuits and Systems Proceedings ICCCAS 2008. Xiamen, Fujian Province, China, 2008. 488−492.

6 Selvi SS, Vivek SS, Rangan CP, Jain N. Cryptanalysis of Li et al.'s identity-based threshold signcryption scheme. Proc. of The 5th International Conference on Embedded and Ubiquitous Computing, EUC 2008. Shanghai, China, 2008. 127 − 132.

7 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. Advances in Cryptology- Crypro'2001, Berlin: Springer-Verlag, 2001. 213 − 229.

8 Baek J, Zheng Y. Identity-based threshold signature scheme from the bilinear pairings. International Conference on Information Technology: Coding and Computing-ITCC'04, LasVegas. Nevada, USA, 2004. 124−128.

9 彭华熹,冯登国.一个基于双线性映射的前向安全门限签名方案.计算机研究与发展,2007,44(4):574−580.

10 Peng C, Li X. An identity-based threshold signcryption scheme with semantic security. Computational Intelligence and Security-CIS 2005. Xi'an, China. 173−179.