无证书体制下的多接收者签密密钥封装机制

孙银霞　李 晖　李小青
(西安电子科技大学计算机网络与信息安全教育部重点实验室　西安　710071)

摘　要：无证书签密密钥封装机制(CLSC-KEM)与数据封装机制共同构成无证书混合签密方案。该文提出一个新的概念：无证书体制下的多接收者签密密钥封装机制(mCLSC-KEM)。给出了 mCLSC-KEM 的定义以及安全模型，并构造了一个具体的方案。该方案比一般性构造(对每个接收者分别运行 CLSC-KEM)高效很多，其密钥封装仅需计算 **1** 个双线性对，且对应的数据封装仅需运行 **1** 次对称加密，而一般性构造需计算 n 个双线性对和 n 次数据封装(设 n 个接收者)。在随机预言模型下，基于 Gap 双线性 Diffie-Hellman 问题，该文的方案是可证明安全的。

关键词：密码学；无证书；签密密钥封装机制；多接收者；双线性对；可证明安全；随机预言模型
中图分类号：TN918.2　　**文献标识码**：A　　**文章编号**：1009-5896(2010)09-2249-04
DOI: 10.3724/SP.J.1146.2009.01260

Certificateless Signcryption KEM to Multiple Recipients

Sun Yin-xia　Li Hui　Li Xiao-qing
(*Key Lab of Computer Networks and Information Security of Ministry of Education*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: Certificateless signcryption key encapsulation mechanism (CLSC-KEM), combined with a data encapsulation mechanism, is used to construct certificateless hybrid signcryption . This paper introduces a new concept: certificateless signcryption KEM to multiple recipients (mCLSC-KEM). The definition and the security models are given for this new primitive, and a concrete mCLSC-KEM scheme is presented. This scheme is much more efficient than the generic construction, for it needs to compute only **one** pairing during key encapsulation and **one** symmetric encryption during data encapsulation, in contrast to n pairings and n symmetric encryptions for the generic scheme. Our scheme is provably secure in the random oracle model, under the hardness assumption of the Gap-BDH problem.

Key words: Cryptography; Certificateless; Signcryption key encapsulation mechanism; Multiple recipients; Bilinear pairing; Provably secure; Random oracle model

1　引言

无证书公钥密码体制首先是由 Al-Riyami 和 Paterson 于 2003 年提出的[1]。该密码体制既克服了传统公钥体制需要管理大量公钥证书的缺点，又克服了基于身份公钥体制[2,3]的密钥托管问题。用户私钥由两部分组成，一部分由密钥生成中心 KGC 生成，另一部分由用户自己选取，因此完整的私钥只有用户自己知道；用户公钥由用户生成，且无需公钥证书。

“签密”是由 Zheng 于 1997 年提出的一个概念[4,5]，旨在以小于“签名再加密”的代价同时实现信息的认证性和保密性。基于身份和无证书体制下对签密的研究也已经取得了一些进展，比如文献[6–10]。然而，通常的签密方案要求被传输的消息取自某个特定的集合，这就限制了其应用范围。为了取消这种限制，Dent 于 2005 年提出了混合签密的概念[11,12]。一个混合签密方案由两部分构成：签密密钥封装机制(SC-KEM)和数据封装机制(DEM)。SC-KEM 运用公钥技术封装一个对称密钥 K，然后 DEM 运用对称加密技术和对称密钥 K 加密任意长的消息。由于 SC-KEM 和 DEM 各自独立，所以我们可以分别研究 SC-KEM 和 DEM，这不仅有利于构造安全又高效的签密方案，而且可以处理任意长度的消息。近几年，混合签密已引起了广泛的关注，并取得了一些成果比如文献[13–15]。在 2009 年，Li 等人[16]将混合签密的概念推广到无证书体制下，提出了无证书混合签密的概念，指出无证书混合签密可以由无证书签密密钥封装机制(CLSC-KEM)和数据封装机制构成，并且给出了一般构造和一个具体方案。随后，Selvi 等人[17]指出 Li 等人[16]的方案不具

2009-09-25 收到，2010-03-16 改回
国家自然科学基金(60772136)，国家 863 计划项目(2007AA01Z435)，中国科学院“九五”重大项目(2008BAH22B03，2007BAH08B01)和国家 111 项目(B08038)资助课题
通信作者：孙银霞　bela_suno@163.com

有存在不可伪造性，并改进了方案。然而，文献[17]中给出的攻击并不成立，因为对称密钥K'的改变会引起标签τ (= $\mathrm{Enc}_{K'}(m)$)的改变，从而导致W的改变，所以$\psi^* = (U,W)$不是K'的一个有效封装(从发送者ID_A到接收者ID_{B^*})，攻击失败。

现在考虑无证书体制下的这样一种情形：某个用户A给n个用户发送一个消息m(任意长度)。当然，A可以对每个接收者分别运行一次无证书混合签密算法，但这样做的运算量太大，不仅需要进行n次数据封装，而且通常需要计算n个双线性对(根据 MIRACL 的运行结果，对于 80 bit 的安全级别，计算一个 Tate 对需要 20 ms，而计算一个素数模指数只需要 8.8 ms)，这对于计算资源有限的通信环境(比如 Ad hoc 网络)而言，负担太重。那么，有没有方法可以简化运算以降低通信开销呢？

针对以上问题，本文提出了一个新的概念：无证书体制下的多接收者签密密钥封装机制(mCLSC-KEM)。给出了 mCLSC-KEM 的定义以及安全模型，并构造了一个高效的方案。由该 mCLSC-KEM 方案得到的无证书混合签密算法仅需 **1** 次双线性对运算和 **1** 次数据封装，大大降低了通信开销。在随机预言模型下，基于 Gap 双线性 Diffie-Hellman 问题，本文的方案是可证明安全的。

2 预备知识

本节定义无证书体制下的多接收者签密密钥封装机制(mCLSC-KEM)及其安全模型。

2.1 mCLSC-KEM 定义

本文把单接收者无证书签密密钥封装机制 CLSC-KEM[16]推广到多接收者的情形。无证书的多接收者签密密钥封装机制(mCLSC-KEM)由以下 5 个算法组成：

系统初始化算法(Setup)：由KGC完成，输入安全参数k，输出主密钥s和系统参数params，其中s保密，params公开。

提取部分私钥算法(Extract-Partial-Private-Key)：由 KGC 完成，输入 params，s和一个用户身份 ID，输出该用户的部分私钥 D_{ID}。

生成用户密钥算法(Generate-User-Keys)：由用户完成，输入 params 和用户身份 ID，输出一个秘密值x_{ID}和公钥$\mathrm{PK}_{\mathrm{ID}}$。秘密值$x_{\mathrm{ID}}$和部分私钥$D_{\mathrm{ID}}$构成用户的完整私钥$\mathrm{SK}_{\mathrm{ID}}$。

密钥封装算法(Encap)：由发送者完成，输入 params，发送者私钥、身份和公钥，n 个接收者的身份$\{\mathrm{ID}_i\}_{i=1}^n$和公钥$\{\mathrm{PK}_i\}_{i=1}^n$，以及一个标签$\tau$，输出一个对称密钥$K$和一个密文$\varphi$。

解封装算法(Decap)：由接收者$\mathrm{ID}_i (i \in [1,n] \cap Z^+)$完成，输入 params，密文$\varphi$，接收者私钥、身份和公钥，发送者身份和公钥，以及一个标签τ，输出一个对称密钥K或者“拒绝”(表示密文无效)。

2.2 mCLSC-KEM 安全模型

存在两类攻击者：第 1 类攻击者 $\boldsymbol{A}_{\mathrm{I}}$和第 2 类攻击者 $\boldsymbol{A}_{\mathrm{II}}$。第 1 类攻击者是一个普通的攻击者，他不知道 KGC 的私钥，但是可以替换任何用户公钥；第 2 类攻击者指好奇但诚实的 KGC，他已知任何用户的部分私钥，但是不替换任何用户公钥。

本文通过以下攻击者与挑战者之间的两个游戏来定义 mCLSC-KEM 的安全性。这两类攻击者在攻击阶段可以作如下询问：

提取部分私钥询问：$\boldsymbol{A}_{\mathrm{I}}$询问用户 ID 的部分私钥。挑战者运行算法 Extract-Partial-Private-Key(params, s, ID) $\rightarrow D_{\mathrm{ID}}$, 并把 D_{ID}返回给 $\boldsymbol{A}_{\mathrm{I}}$。

提取秘密值询问：$\boldsymbol{A}_{\mathrm{I}}$，$\boldsymbol{A}_{\mathrm{II}}$询问用户 ID 的秘密值。挑战者运行算法 Generate-User-Key(params, ID)$\rightarrow x_{\mathrm{ID}}$, 并把 x_{ID}返回给 $\boldsymbol{A}_{\mathrm{I}}$、$\boldsymbol{A}_{\mathrm{II}}$。如果该用户的公钥已被替换，则攻击者不能作此询问。

公钥询问：$\boldsymbol{A}_{\mathrm{I}}$，$\boldsymbol{A}_{\mathrm{II}}$询问用户 ID 的公钥。挑战者运行算法 Generate-User-Key(params, ID) $\rightarrow$ $\mathrm{PK}_{\mathrm{ID}}$, 并把 $\mathrm{PK}_{\mathrm{ID}}$返回给攻击者。

替换公钥：$\boldsymbol{A}_{\mathrm{I}}$替换用户 ID 的公钥。$\boldsymbol{A}_{\mathrm{I}}$可以用任何值替换用户 ID 的公钥。

Encap 询问：$\boldsymbol{A}_{\mathrm{I}}$，$\boldsymbol{A}_{\mathrm{II}}$对($\mathrm{ID}_s$, $\{\mathrm{ID}_i\}_{i=1}^n$,τ)进行 Encap 询问。挑战者运行算法 Encap(params, SK_s, ID_s, PK_s, $\{\mathrm{ID}_i\}_{i=1}^n$,$\{\mathrm{PK}_i\}_{i=1}^n$,$\tau$)$\rightarrow$($K$,$\varphi$), 并把($K$, φ)返回给攻击者。

Decap 询问：$\boldsymbol{A}_{\mathrm{I}}$，$\boldsymbol{A}_{\mathrm{II}}$对($\mathrm{ID}_s$, ID_i，τ，φ)进行 Decap 询问。挑战者运行算法 Decap(params, ID_s, PK_s, SK_i, ID_i,PK_i,τ,φ)$\rightarrow K/$“拒绝”，并把 K 或“拒绝”返回给攻击者。

2.2.1 认证性

初始化：挑战者运行算法 Setup，并把 params 发送给攻击者 $\boldsymbol{A}_{\mathrm{I}}$；把 params 和 s 同时发送给攻击者 $\boldsymbol{A}_{\mathrm{II}}$。

攻击：攻击者作一系列如上询问。

伪造：攻击者输出(τ^*,φ^*, ID_s^*, $\boldsymbol{L}^*$)。若φ^*有效，则攻击者赢得游戏。$\boldsymbol{A}_{\mathrm{I}}$不能同时询问过$\mathrm{ID}_s^*$的部分私钥和秘密值，或者同时询问过$\mathrm{ID}_s^*$的部分私钥和替换过$\mathrm{ID}_s^*$的公钥；$\boldsymbol{A}_{\mathrm{II}}$不能询问过$\mathrm{ID}_s^*$的秘密值。$\varphi^*$不能来源于攻击者对($\mathrm{ID}_s^*$, $\boldsymbol{L}^*$,τ^*)的 Encap 询问。定义攻击者在以上游戏中获胜的优势为攻击者赢得游戏的概率。

定义 1 如果没有任何多项式有界的攻击者在

以上游戏中以不可忽略的优势获胜，那么称一个 mCLSC-KEM 方案在选择消息攻击下具有强不可伪造性(sUF-CMA)。

2.2.2 保密性

初始化：挑战者运行算法 Setup，并把 params 发送给攻击者 $\boldsymbol{A}_{\mathrm{I}}$；把 params 和 s 同时发送给攻击者 $\boldsymbol{A}_{\mathrm{II}}$。

第 1 阶段攻击：攻击者作一系列如上询问。

挑战：攻击者输出他想挑战的发送者的身份 ID_s^* 和接收者的身份 $\boldsymbol{L}^*$，挑战者计算出对称密钥 K_0，并从对称密钥空间随机选择一个 K_1，把(K_0, K_1)发送给攻击者，然后攻击者选择一个标签 τ^*，挑战者计算出密文 φ^*，并把 φ^*发给攻击者。$\boldsymbol{A}_{\mathrm{I}}$ 不能同时询问过任何 $\mathrm{ID}_i^* \in \boldsymbol{L}^*$的部分私钥和秘密值，或者询问过 ID_i^* 的部分私钥并替换过其公钥；$\boldsymbol{A}_{\mathrm{II}}$ 不能询问过任何 $\mathrm{ID}_i^* \in \boldsymbol{L}^*$的秘密值。

第 2 阶段攻击：攻击者继续进行如第一阶段的询问，但是 $\boldsymbol{A}_{\mathrm{II}}$ 不能同时询问任何 $\mathrm{ID}_i^* \in \boldsymbol{L}^*$的部分私钥和秘密值，也不能同时询问 ID_i^* 的部分私钥和替换其公钥；$\boldsymbol{A}_{\mathrm{III}}$ 不能询问任何 $\mathrm{ID}_i^* \in \boldsymbol{L}^*$的秘密值。另外，攻击者不能对$(\mathrm{ID}_s^*, \mathrm{ID}_i^* \in \boldsymbol{L}^*, \tau^*, \varphi^*)$进行 Decap 询问，除非替换发送者或者接收者的公钥。

猜测：攻击者输出猜测 $\beta \in \{0,1\}$。定义攻击者在以上游戏中获胜的优势为$|2\Pr[\beta=0]-1|$。

定义 2　如果没有任何多项式有界的攻击者在以上游戏中以不可忽略的优势获胜，那么称一个 mCLSC-KEM 方案在选择密文攻击下具有不可区分性(IND-CCA)。

3　一个高效的 mCLSC-KEM 方案

本节给出一个高效的 mCLSC-KEM 方案，具体构造如下：

初始化(Setup)：设 G_1 和 G_2 分别是阶为素数 q 的加法循环群和乘法循环群，P 是 G_1 的一个生成元，$\hat{e}: G_1 \times G_1 \to G_2$ 是一个双线性对。H_1，H_2，H_3 和 H_4 是 4 个 hash 函数，其中 $H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \to \{0,1\}^n$，$H_3: \{0,1\}^* \to G_1$ 和 $H_4: \{0,1\}^* \to G_1$，这里 n 表示 DEM 的密钥长度。随机选择 $s \in Z_q^*$ 作为 KGC 的私钥，并计算其公钥 $P_0 = sP$。则系统的公共参数为 params $= \{G_1, G_2, q, P, \hat{e}, H_1, H_2, H_3, H_4, n, P_0\}$。

提取部分私钥(Extract-Partial-Private-Key)：输入一个用户身份 ID，KGC 计算 $Q_{\mathrm{ID}} = H_1(\mathrm{ID})$，再用自己的私钥 s 计算该用户的部分私钥 $D_{\mathrm{ID}} = sH_1(\mathrm{ID})$。

生成用户密钥(Generate-User-Keys)：用户 ID 随机选择 $x_{\mathrm{ID}} \in Z_q^*$ 作为其秘密值，并计算其公钥 $\mathrm{PK}_{\mathrm{ID}} = x_{\mathrm{ID}}P$。则该用户的完整私钥为$(D_{\mathrm{ID}}, x_{\mathrm{ID}})$。

密钥封装(Encap)：由发送者运行。输入 params，发送者私钥(D_s, x_s)、身份 ID_s 和公钥 PK_s，n 个接收者的身份 $\{\mathrm{ID}_i\}_{i=1}^n$ 和公钥 $\{\mathrm{PK}_i\}_{i=1}^n$，该算法按如下步骤进行：

(1)随机选择 $r \in Z_q^*$，$Q, Y \in G_1$；

(2)计算 $U = rP$，$T = \hat{e}(P_0, Q)^r$，$\{V_i \mid V_i = rQ + rQ_i, Q_i = H_1(\mathrm{ID}_i), 1 \le i \le n\}$，$\{Y_i \mid Y_i = rY + r\mathrm{PK}_i, 1 \le i \le n\}$；

(3) 计算对称密钥 $K = H_2(U, T, rY, \{\mathrm{ID}_i\}_{i=1}^n, \{\mathrm{PK}_i\}_{i=1}^n)$；

(4)输入一个标签 τ，计算 $W = D_s + rH_3(U, \tau, \mathrm{ID}_s, \mathrm{PK}_s) + x_s H_4(U, \tau, \mathrm{ID}_s, \mathrm{PK}_s)$；

(5) 输出 (K, φ)，这里 $\varphi = (U, W, \{V_i\}_{i=1}^n, \{Y_i\}_{i=1}^n)$。

解封装(Decap)：由接收者运行。输入 params，接收者私钥(D_i, x_i)、身份 ID_i 和公钥 PK_i，发送者身份 ID_s 和公钥 PK_s，标签 τ，以及密文 $\varphi = (U, W, \{V_i\}_{i=1}^n, \{Y_i\}_{i=1}^n)$，该算法按如下步骤进行：

(1)计算 $H = H_3(U, \tau, \mathrm{ID}_s, \mathrm{PK}_s)$ 和 $H' = H_4(U, \tau, \mathrm{ID}_s, \mathrm{PK}_s)$，并验证等式 $\hat{e}(P_0, Q_s)\hat{e}(U, H)\hat{e}(PK_s, H') = \hat{e}(P, W)$ 是否成立。

(2)如果成立，那么计算 $T = \dfrac{\hat{e}(P_0, V_i)}{\hat{e}(U, D_i)}$，$rY = Y_i - x_i U$ 和对称密钥 $K = H_2(U, T, rY, \{\mathrm{ID}_i\}_{i=1}^n, \{\mathrm{PK}_i\}_{i=1}^n)$，并输出 K；否则，输出“拒绝”。

4　安全性和效率分析

在随机预言模型下，基于 GDH′ 问题、CDH 问题和 GBDH 问题[16]，本文的 mCLSC-KEM 方案满足 sUF-CMA 安全性和 IND-CCA 安全性。

在无证书公钥体制下，当一个用户给 n 个用户签密一个消息 m(任意长度)时，他可以对每个用户分别使用无证书混合签密算法[16]，如表 1 所示，共需计算 n 个双线性对(p)和 n 次数据封装(DEM)，且随着接收者数量的增加而增加。众所周知，双线性对运算复杂，需要消耗较多的计算资源，所以在实际应用尤其是计算资源有限的通信环境中应当尽量减少双线性对的数量。本文的方案较好地做到了这一点，它仅需计算 **1** 个双线性对和 **1** 次数据封装，且**不**随接收者数量的增加而增加。另外，消息的密文长度也比一般性构造短。表 1 中 p 表示双线性对，$|P|$表示 G_1 中一个元素的长度，$|m|$表示消息 m 的长度。

5　结束语

本文提出了一个新的概念：无证书体制下的多接收者签密密钥封装机制(mCLSC-KEM)。给出了

表 1 与一般构造的比较

方案 (+DEM)	Encap	Decap	密文长度
一般性构造	np(+nDEM)	$5p$(+1DEM)	$2n\|P\|$ (+ $n\|m\|$)
本文方案	$1p$(+1DEM)	$6p$(+1DEM)	$2\|P\|+2n\|P\|$ (+$\|m\|$)

mCLSC-KEM 的定义和安全模型，并且构造了一个高效的方案。与一般性构造相比，本文的方案不仅减少(n–1)次数据封装，而且减少(n–1)次双线性对运算(n 指接收者数量)，从而大大提高了通信效率。在随机预言模型和 Gap 双线性 Diffie-Hellman(GBDH)假设下，方案是可证明安全的。

可以运用 twinning 技术[18]使方案的安全性归结于标准的双线性 Diffie-Hellman 问题，以避免使用 Gap 双线性 Diffie-Hellman 假设，但与此同时计算复杂性增加了。如何在两者之间实现最优化是一个待研究的问题。

参 考 文 献

[1] Al-Riyami S S and Paterson K G. Certificateless public key cryptography[C]. ASIACRYPT 2003, Berlin: Springer-Verlag, 2003, LNCS 2894: 452–473.

[2] Shamir A. Identity-based cryptosystems and signature schemes[C]. CRYPTO 1984, Berlin: Springer-Verlag, 1984, LNCS 196: 47–53.

[3] Boneh D and Franklin M. Identity-based encryption from the Weil pairing[C]. CRYPTO 2001, Berlin: Springer-Verlag, 2001, LNCS 2139: 213–229.

[4] Zheng Y. Digital signcryption or how to achieve cost (Signature & encryption) << cost(Signature) + cost (Encryption) [C]. CRYPTO 1997, Berlin: Springer-Verlag, 1997, LNCS 1294: 165–179.

[5] An JH, Dodis Y, and Rabin T. On the security of joint signature and encryption[C]. EUROCRYPT 2002, Berlin: Springer-Verlag, 2002, LNCS 2332: 83–107.

[6] Boyen X. Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography[C]. Cryptology -CRYPTO 2003, Berlin: Springer-Verlag, 2003, LNCS 2729: 383–399.

[7] Barreto PSLM, Libert B, McCullagh N, and Quisquater J J. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps[C]. Asiacrypt 2005, Berlin: Springer-Verlag, 2005, LNCS 3788: 515–532.

[8] 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, 29(9): 1641–1647.
Li Fa-gen, HuYu-pu, and Li Gang. An efficient identity-based signcryption scheme. *Chinese Journal of Computers*, 2006, 29(9): 1641–1647.

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

[10] Wu Chen-huang and Chen Zhi-xiong. A new efficient certificateless signcryption scheme[C]. International Symposium on Information Science and Engieering, Shanghai, China, IEEE Computer Society, 2008: 661–664.

[11] Dent A W. Hybrid signcryption schemes with outsider security[C]. ISC 2005, Berlin: Springer-Verlag, 2005, LNCS 3650: 203–217.

[12] Dent A W. Hybrid signcryption schemes with insider security[C]. ACISP 2005, Berlin: Springer-Verlag, 2005, LNCS 3574: 253–266.

[13] Bjørstad T E and Dent A W. Building better signcryption schemes with tag-kEMs[C]. PKC 2006, Berlin: Springer-Verlag, 2006, LNCS 3958: 491–507.

[14] Tan C H. Insider-secure signcryption KEM/tag-KEM schemes without random oracles[C]. The Third International Conference on Availability, Reliability and Security-ARES 2008, Barcelona, Spain, 2008: 1275–1281.

[15] Li Fa-gen, Shirase M, and Takagi T. Efficient signcryption key encapsulation without random oracles[C]. Information Security and Cryptology 2009, Berlin: Springer-Verlag, 2009, LNCS 5487: 47–59.

[16] Li Fa-gen, Shirase M, and Takagi T. Certificateless hybrid signcryption[C]. ISPEC 2009, Berlin: Springer-Verlag, 2009, LNCS 5451: 112–123.

[17] Selvi SSD, Vivek S S, and PanduRangan C. Breaking and re-building a certificateless hybrid signcryption scheme. Cryptology ePrint Archive, Report 2009/462, 2009.

[18] Cash D, Kiltz E, and Shoup V. The twin Diffie-Hellman problem and applications[J]. *Journal of Cryptology*, 2009, 22(4): 470–504.

孙银霞： 女，1979 年生，博士生，研究方向为密码学和网络安全.

李 晖： 男，1969 年生，教授，研究方向为信息论和网络安全.

李小青： 女，1981 年生，博士生，研究方向为网络安全.