软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2011,22(7):1690−1698 [doi: 10.3724/SP.J.1001.2011.03825]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

高效无证书混合签密*

孙银霞+, 李 晖

(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,陕西 西安 710071)

Efficient Certificateless Hybrid Signcryption

SUN Yin-Xia+, LI Hui

(Key Laboratory of Computer Networks and Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)

+ Corresponding author: E-mail: bela_suno@163.com

Sun YX, Li H. Efficient certificateless hybrid signcryption. *Journal of Software*, 2011,22(7):1690−1698. http://www.jos.org.cn/1000-9825/3825.htm

Abstract: Certificateless hybrid signcryption can handle messages of arbitrary length while the conventional certificateless signcryption cannot. This paper demonstrates that the attacks presented by Selvi, *et al*., do not hold, and proposes a new certificateless hybrid signcryption scheme, which outperforms all the existing schemes on both bandwidth usage and computation efficiency. Hence, this scheme is more suitable for the applications with a narrow bandwidth and limited computation resources such as ad hoc networks. This scheme has been proven to be secure in the random oracle model, under the bilinear Diffie-Hellman assumption.

Key words: certificateless hybrid signcryption; certificateless signcryption key encapsulation mechanism; DEM (data encapsulation mechanism); authenticity; confid- entiality; bilinear Diffie-Hellman; random oracle model

摘 要: 无证书混合签密能够处理无证书体制下任意长度的消息,而普通的无证书签密则不能处理.指出 Selvi 等人提出的攻击是不成立的,并构造了一个新的无证书混合签密方案.与现有方案相比,该方案具有密文长度短、计算速度快的优点,因此更适用于带宽窄、计算资源少的通信环境,如 ad hoc 网络.在随机预言模型和双线性 Diffie-Hellman 困难性假设条件下,该方案可证明是安全的.

关键词: 无证书混合签密;无证书签密密钥封装机制;数据封装机制;可认证性;机密性;双线性 Diffie-Hellman;随机预言模型

中图法分类号: TP309 **文献标识码**: A

公钥密码体制是由 Diffie 和 Hellman 于 1976 年提出来的.根据用户公钥的认证方式,可将公钥密码体制大致分为传统公钥体制、基于身份公钥体制和无证书公钥体制.传统公钥体制的用户公私钥由用户自己选取,证书中心给每个用户颁发一个公钥证书,因此,证书中心需要管理一个庞大的证书库,任务十分繁重.基于身份公钥体制[1,2]的用户身份就是用户的公钥,所以无需公钥证书,但用户私钥是由私钥生成中心 PKG 生成的,所以

* 基金项目: 国家自然科学基金(60772136); 国家高技术研究发展计划(863)(2007AA01Z435); 国家科技支撑计划(2008BAH22B03, 2007BAH08B01); 国家"111"项目(B08038)

收稿时间: 2007-12-17; 修改时间: 2008-03-27; 定稿时间: 2008-07-02

PKG 掌握着每个用户的私钥.为了阻止好奇的 PKG 解密用户的密文或伪造用户的签名,Al-Riyami 和 Paterson 于 2003 年提出了无证书公钥密码体制[3],用户的私钥由两部分组成:一部分由 PKG 生成,另一部分则由用户生成.

“签密”是由 Zheng 于 1997 年提出的密码概念[4,5],旨在以小于“签名再加密”的代价同时实现信息的可认证性和机密性.基于身份体制和无证书体制下对签密的研究也已取得了一些进展[6−11].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.一般的公钥加密也存在同样的局限性,“混合加密”则较好地解决了这一问题.混合加密的概念首先是由 Cramer 和 Shoup 正式提出[12],它由两部分构成:一部分用来封装对称密钥,另一部分用来加密任意长的数据.2005 年,Dent 把混合加密技术应用于签密领域,提出了混合签密的概念[13,14].类似地,混合签密由两部分构成:签密密钥封装机制(signcryption key encapsulation mechanism,简称 SC-KEM)和数据封装机制(data encapsulation mechanism,简称 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 是完全独立的两个模块,所以我们可以分别研究 SC-KEM 和 DEM,这不仅有利于构造安全而高效的签密方案,而且可以处理任意长度的数据.近几年来,混合签密已引起了广泛的关注[15−17].在 2009 年,Li 等人[18]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(certificateless SC-KEM,简称 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[19]指出 Li 等人[18]的方案不具有存在不可伪造性,并改进了方案.

本文的贡献

我们指出文献[1]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 $\tau(=\mathrm{Enc}_{K'}(m))$ 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.

众所周知,计算速度和密文长度是影响方案效率的两个主要因素.本文提出了一个新的无证书混合签密方案.与已有方案相比,该方案不仅计算速度快,而且密文长度短,因此更适合于实际应用,尤其是在计算资源少、可用带宽低的通信环境下.基于计算 Diffie-Hellman 问题与双线性 Diffie-Hellman 问题,新方案在随机预言模型下可证明是安全的.

1 预备知识

本节首先介绍无证书签密密钥封装机制(CLSC-KEM)、数据封装机制(DEM)和无证书混合签密的定义以及无证书混合签密的安全模型,然后简要介绍双线性对的基础知识及本文所依赖的相关困难问题.

1.1 CLSC-KEM定义

无证书签密密钥封装机制 CLSC-KEM 由以下 5 种算法组成:

(1) Setup:系统初始化算法.由PKG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.

(2) Extract-Partial-Private-Key:提取部分私钥算法.由 PKG 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}.

(3) Generate-User-Keys:生成用户密钥算法由用户完成输入 $params$ 和用户身份 ID 输出一个秘密值 x_{ID} 和公钥 PK_{ID}.秘密值 x_{ID} 和部分私钥 D_{ID} 构成用户的完整私钥 SK_{ID}.

(4) Encap:密钥封装算法.由发送者完成,输入 $params$,发送者私钥 SK_s、身份 ID_s 和公钥 PK_s 接收者身份 ID_r 和公钥 PK_r, 输出一个对称密钥 K 和一个密文φ.

(5) Decap:解封装算法.由接收者完成,输入 $params$,接收者私钥 SK_r 、身份 ID_r 和公钥 PK_r, 发送者身份 ID_s 和公钥 PK_s, 输出一个对称密钥 K.

1.2 DEM定义

数据封装机制包含下列两种算法:

(1) Enc:加密算法.输入对称密钥 K 和消息 m,输出密文 c.

(2) Dec:解密算法.输入对称密钥 K 和密文 c,输出消息 m 或⊥(表示密文无效).

1.3 无证书混合签密的定义

无证书混合签密由无证书签密密钥封装机制 CLSC-KEM 与数据封装机制 DEM 构成,具体算法如下:

(1) Setup:同CLSC-KEM.

(2) Extract-Partial-Private-Key:同 CLSC-KEM.

(3) Generate-User-Keys:同 CLSC-KEM.

(4) Signcrypt:签密算法.

① $(K,\phi) \leftarrow \text{Encap}(params, SK_s, \text{ID}_s, PK_s, \text{ID}_r, PK_r)$;

② $c \leftarrow \text{Enc}(K, m)$;

③ 输出密文 $C=(\phi,c)$.

(5) Unsigncrypt:解密验证算法.

① $K \leftarrow \text{Decap}(params, SK_r, \text{ID}_r, PK_r, \text{ID}_s, PK_s, \phi)$;

② $m/\perp \leftarrow \text{Dec}(K,c)$;

③ 输出明文 m 或者⊥(表示密文无效).

1.4 无证书(混合)签密安全模型

本文的无证书混合签密构造方法与文献[18]中的不同,所使用的无证书签密密钥封装机制不引入标签(tag),数据封装机制满足完整性和不可区分性.下面我们只从整体上考虑无证书混合签密的安全性.

无证书体制下存在两类攻击者:第 1 类攻击者 $\boldsymbol{A}_{\text{I}}$ 和第 2 类攻击者 $\boldsymbol{A}_{\text{II}}$.第 1 类攻击者是一个普通的攻击者,他不知道 PKG 的私钥,但是可以替换任何用户公钥;第 2 类攻击者是指好奇但诚实的 PKG,他已经知道任何用户的部分私钥,但是不替换任何用户公钥.

我们通过以下攻击者与挑战者之间的游戏来定义无证书(混合)签密的安全性.这两类攻击者在攻击阶段可作如下询问:

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

秘密值询问:$\boldsymbol{A}_{\text{I}}$,$\boldsymbol{A}_{\text{II}}$ 询问用户 ID 的秘密值.挑战者运行算法 Generate-User-Key($params$,ID) $\rightarrow x_{\text{ID}}$,并把 x_{ID} 返回给 $\boldsymbol{A}_{\text{I}}$,$\boldsymbol{A}_{\text{II}}$.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:$\boldsymbol{A}_{\text{I}}$,$\boldsymbol{A}_{\text{II}}$ 询问用户 ID 的公钥.挑战者运行算法 Generate-User-Key($params$,ID) $\rightarrow PK_{\text{ID}}$,并把 PK_{ID} 返回给攻击者.

替换公钥:$\boldsymbol{A}_{\text{I}}$ 替换用户的公钥.$\boldsymbol{A}_{\text{I}}$ 可以用指定范围内的任意值替换任意用户的公钥.

Signcrypt 询问:$\boldsymbol{A}_{\text{I}}$,$\boldsymbol{A}_{\text{II}}$ 对(ID_s,ID_r,m)进行签密询问.挑战者运行算法 Signcrypt($params$,SK_s,ID_s,PK_s,ID_i,PK_i,m) $\rightarrow C$,并把 C 返回给攻击者.

Unsigncrypt 询问:$\boldsymbol{A}_{\text{I}}$,$\boldsymbol{A}_{\text{II}}$ 对(ID_s, ID_r ,C)进行 Unsigncrypt 询问.挑战者运行算法 Unsigncrypt($params$,ID_s,PK_s,SK_r, ID_r, PK_r, C) $\rightarrow m/\perp$,并把 m 或⊥ 返回给攻击者.

1.4.1 可认证性

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

s 攻击:攻击者作一系列如上询问.

伪造:攻击者输出(ID_s^*, ID_r^* ,C^*).注意,$\boldsymbol{A}_{\text{I}}$ 不能询问过 ID_s^* 或 ID_r^* 的部分私钥;$\boldsymbol{A}_{\text{II}}$ 不能询问过 ID_s^* 或 ID_r^* 的秘密值.另外, C^*不能来自攻击者对某个(ID_s^*, ID_r^* ,m)的签密询问.若 C^*为一个有效密文,则攻击者获胜.

我们定义攻击者在以上游戏中的优势为攻击者获胜的概率 $\Pr[\boldsymbol{A}_{\text{I(II)}}\text{win}]$.

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,则称一个无证书(混合)签密方案在选择消息攻击下具有不可伪造性(UF-CMA).

1.4.2 机密性

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^*、接收者的身份 ID_r^* 和两个消息(m_0,m_1),然后挑战者随机选取一个消息 $m_\beta,\beta\in\{0,1\}$,计算其密文 C^*并发送给攻击者.注意,$\boldsymbol{A}_{\mathrm{I}}$ 不能询问过 ID_r^* 或 ID_s^* 的部分私钥;$\boldsymbol{A}_{\mathrm{II}}$ 不能询问过 ID_r^* 或 ID_s^* 的秘密值.

第 2 阶段攻击:攻击者继续进行如第 1 阶段的询问,但是受下列约束:(1) $\boldsymbol{A}_{\mathrm{I}}$ 不能询问 ID_r^* 或 ID_s^* 的部分私钥,$\boldsymbol{A}_{\mathrm{II}}$不能询问 ID_r^* 或 ID_s^* 的秘密值;(2) 攻击者不能对(ID_s^*, ID_r^*,C^*)进行 Unsigncrypt 询问,除非替换了发送者或者接收者的公钥.

猜测:攻击者输出猜测 $\beta'\in\{0,1\}$.

我们定义攻击者在以上游戏中获胜的优势为$|2\Pr[\beta'=\beta]-1|$.

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,则称一个无证书混合签密方案在选择密文攻击下具有不可区分性(IND-CCA).

1.5 双线性对与Diffie-Hellman问题

设 G_1 和 G_2 分别表示阶为素数 q 的加法循环群和乘法循环群.P 是 G_1 的一个生成元.若映射 $\hat{e}:G_1\times G_1\to G_2$ 满足下列性质,则称为双线性对.

(1) 双线性性:对任意 $a,b\in Z_q^*,\hat{e}(aP,bP)=\hat{e}(P,P)^{ab}$.

(2) 非退化性: $\hat{e}(P,P)\neq 1_{G_2}$.

(3) 可计算性:对所有 $P,Q\in G_1$,都能有效计算 $\hat{e}(P,Q)$.

双线性对 $\hat{e}$ 可以通过有限域上的超椭圆曲线上的 Tate 对或 Weil 对来构造.下面介绍本文所依赖的困难问题,这些困难问题都定义在(G_1,G_2,q,P)上.

计算 Diffie-Hellman(CDH)问题:任给(aP,bP),其中 $a,b\in Z_q^*$,计算 abP.

双线性 Diffie-Hellman(BDH)问题:任给(aP,bP,cP),其中 $a,b,c\in Z_q^*$,计算 $\hat{e}(P,P)^{abc}$.

2 Selvi 等人对 Li 等人方案攻击的回顾与分析

Li 等人的方案

(1) Setup:输入安全参数,输出公共参数 $G_1,G_2,q,\hat{e},P,P_{pub},n,H_1\sim H_4$,系统主密钥 s.

(2) Extract-Partial-Private-Key:输入用户身份 ID,计算用户的部分私钥 $D_{\mathrm{ID}}=sH_1(\mathrm{ID})$.

(3) Generate-User-Key:输入公共参数和用户身份 ID,选取秘密值 $x_{\mathrm{ID}}\in_R Z_q^*$,计算公钥 $PK_{\mathrm{ID}}=x_{\mathrm{ID}}P$.

(4) Encap:输入发送者私钥 (D_S,x_s), 公钥 PK_S 和身份 ID_s,接收者公钥 PK_r 和身份 ID_r,标签 τ,执行下列步骤:

① 选取 $r\in_R Z_q^*$;

② 计算 $U=rP,T=\hat{e}(P_{pub},H_1(\mathrm{ID}_r))^r$;

③ 计算 $K=H_2(U,T,rPK_r,\mathrm{ID}_r,PK_r)$;

④ 计算 $H=H_3(U,\tau,\mathrm{ID}_s,PK_s),H'=H_4(U,\tau,\mathrm{ID}_s,PK_s)$;

⑤ 计算 $W=D_s+rH+x_sH'$;

⑥ 输出密文 $\varphi=(U,W)$.

(5) Decap:输入接收者私钥 (D_r,x_r), 公钥 PK_r 和身份 ID_r,发送者公钥 PK_s 和身份 ID_s,密文 φ,标签 τ,执行下列步骤:

① 计算 $H=H_3(U,\tau,\mathrm{ID}_s,PK_s),H'=H_4(U,\tau,\mathrm{ID}_s,PK_s)$;

② 验证 $\hat{e}(P_{pub},H_1(\mathrm{ID}_s))\hat{e}(U,H)\hat{e}(PK_s,H')=\hat{e}(P,W)$ 是否成立?

③ 若是,计算 $T=\hat{e}(U,D_r)$, 输出 $K=H_2(U,T,x_rU,\mathrm{ID}_r,PK_r)$; 否则输出 $\perp$.

Selvi 等人对上述方案的攻击

- 在训练阶段,攻击者询问发送者 ID_A、接收者 ID_B 和标签 τ 的封装密文,并从挑战者处得到回答 $\psi=(U,W)$.
- 攻击者选择挑战发送者 ID_A 和挑战接收者 $\mathrm{ID}_{B^*}\neq\mathrm{ID}_B$, 并且已知 ID_{B^*} 的私钥.
- 攻击者输出伪造 $(\tau,\psi^*=\psi,\mathrm{ID}_A,\mathrm{ID}_{B^*})$, 其对应的对称密钥为 $K'=H_2(U,\hat{e}(U,D_{B^*}),x_{B^*}U,\mathrm{ID}_{B^*},PK_{B^*})$.

文献[19]称由于验证等式只与接收者和标签 τ 有关,而它们又是保持不变的,所以 $(\tau,\psi^*=\psi,\mathrm{ID}_A,\mathrm{ID}_{B^*})$ 能够顺利通过验证,攻击成功.

我们的分析.由上述攻击过程可见,Selvi 等人并没有考虑标签 τ 的实际含义,由文献[18]可知, $\tau=\mathrm{Enc}_{K'}(m)$, 所以对称密钥 K' 的改变会引起标签 τ 的改变,从而导致 W 的改变,因此 $\psi^*=(U,W)$ 并非 K' 的一个有效封装(从发送者 ID_A 到接收者 ID_{B^*}),攻击失败.

3 本文的方案

本节给出一个新的无证书混合签密方案,该方案由以下 5 种算法组成:

(1) Setup:输入安全参数 k,该算法执行以下步骤:

① 选取两个阶为素数 q 的循环群 G_1,G_2, $\hat{e}:G_1\times G_1\to G_2$ 是一个双线性对;

② 选取 G_1 的一个生成元 P;

③ 从 Z_q^* 中随机选取一个 s,并计算 $P_0=sP$;

④ 选取两个 hash 函数 $H_1:\{0,1\}^*\to G_1, H_2:Z_q^*\times G_2\times G_1\to\{0,1\}^\lambda$;

⑤ 选取一种对称加密算法(Enc,Dec),该算法满足可认证性和机密性[13],其密钥空间为 $\{0,1\}^\lambda$. 这里,(Enc,Dec) 可以用任意的对称加密模块,如 CBC,加上消息认证码,或者用认证加密模块[20−22],当然,我们更倾向于用计算速度快、密文冗余少的算法.

系统的公共参数为 $(G_1,G_2,q,\hat{e},P,P_0,H_1,H_2,\mathrm{Enc},\mathrm{Dec},\lambda)$, 系统的私钥为 s.

(2) Extract-Partial-Private-Key:输入系统的公共参数、系统的私钥和用户的身份 ID,生成用户的部分私钥 $D_{\mathrm{ID}}=sH_1(\mathrm{ID})$, 并通过秘密信道发送给用户.该算法由 PKG 运行.

(3) Generate-User-Key:输入系统的公共参数和用户身份 ID,该算法从 Z_q^* 中随机选取一个 x_{ID} 作为用户的秘密值,并计算公钥 $PK_{\mathrm{ID}}=x_{\mathrm{ID}}P$, 则用户的完整私钥为 $SK_{\mathrm{ID}}=(D_{\mathrm{ID}},x_{\mathrm{ID}})$. 该算法由用户运行.

(4) Signcrypt:输入系统的公共参数、发送者的私钥(D_s , x_s)、接收者的身份 ID_r 、公钥 PK_r 和消息 m,该算法执行以下步骤:

① 从 Z_q^* 中随机选择一个 r,记 $U=r$;

② 计算 $K=H_2(r,\hat{e}(D_s,Q_r),x_sPK_r)$, 这里, $Q_r=H_1(\mathrm{ID}_r)$;

③ 计算 $V=\mathrm{Enc}_K(m)$;

④ 输出密文 $C=(U,V)$.

(5) Unsigncrypt:输入系统的公共参数、发送者的身份和公钥(ID_s , PK_s)、接收者的私钥(D_r , x_r)和密文 $C=(U,V)$,该算法执行以下步骤:

① 计算 $K=H_2(U,\hat{e}(Q_s,D_r),x_rPK_s)$, 这里, $Q_s=H_1(\mathrm{ID}_s)$;

② 计算 $m/\perp=\mathrm{Dec}_K(V)$;

③ 输出明文 m 或 $\perp$.

容易看出,新方案由下面描述的无证书签密密钥封装机制和一个合适的数据封装机制(Enc,Dec)构成.

Encap	Decap
1. $r \in Z_q^*$	1. $Q_s \leftarrow H_1(\mathrm{ID}_s)$
2. $\varphi \leftarrow r$	2. $K \leftarrow H_2(\phi, \hat{e}(Q_s, D_r), x_r PK_s)$
3. $Q_r \leftarrow H_1(\mathrm{ID}_r)$	3. 输出 K
4. $K \leftarrow H_2(r, \hat{e}(D_s, Q_r), x_s PK_r)$	
5. 输出 (K, ϕ)	

4 安全性和效率分析

4.1 安全性证明

由下列定理 1~定理 4 可知,新方案既满足可认证性(UF-CMA 安全),又满足机密性(IND-CCA 安全).其中,我们只详细证明定理 1.

定理 1. 假设(Enc,Dec)具有可认证性.新方案在随机预言模型和 BDH 困难性假设下对第 1 类攻击者具有 UF-CMA 安全性.

详细地,如果存在一个第 1 类攻击者 $\boldsymbol{A}_{\mathrm{I}}$,能够以$\varepsilon$的优势伪造一个有效密文,其中对 H_1 预言器进行 q_1 次询问,则存在一种算法 B,能够以优势 $\frac{\varepsilon-\nu}{C_{q_1}^2}$ 解决 BDH 问题,或者存在一个攻击者能够以 $\nu(0<\nu<\varepsilon)$ 的优势攻破方案中对称加密方案的可认证性.

证明: 假设方案中使用的对称加密算法满足可认证性,换言之,攻击者至多以可忽略的概率 ν 伪造一个有效密文.现在,算法 B 得到一个随机的 BDH 问题实例(P,aP,bP,cP),目标是计算出 $\hat{e}(P,P)^{abc}$ 的值,B 把 $\boldsymbol{A}_{\mathrm{I}}$ 作为子程序并在游戏中扮演 $\boldsymbol{A}_{\mathrm{I}}$ 的挑战者.首先,B 提供给 $\boldsymbol{A}_{\mathrm{I}}$ 一组公共参数 $(G_1,G_2,q,\hat{e},P,P_0,H_1,H_2,\mathrm{Enc},\mathrm{Dec},\lambda)$, 其中 $P_0=aP$, H_1 和 H_2 是由 B 控制的随机预言器.B 选择两个正整数 $I,J,1\leqslant I,J\leqslant q_1$.

然后,$\boldsymbol{A}_{\mathrm{I}}$ 开始攻击,他可以进行如下一系列询问:

H_1 询问:B 保存一个 H_1 列表,由元素 (ID_i,Q_i,d_i) 组成,最初该列表为空.当 B 接收到对 ID_j 的 H_1 询问时,B 首先检查列表中是否已存在元素 (ID_j,Q_j,d_j), 如果是,则返回 Q_j ;否则,按如下步骤进行:

(1) 如果 $j\neq I$ 且 $j\neq J$, B 从 Z_q^* 中随机选取 d_j ,计算 $Q_j=d_jP$,并把 (ID_j,Q_j,d_j) 加入 H_1 列表,然后返回 Q_j ;

(2) 如果 $j=I$ 或者 J,B,则 B 返回 $Q_I=bP$ 或者 $Q_J=cP$,并把 $(\mathrm{ID}_j,Q_j,\perp)$ 加入 H_1 列表.

下面不妨设,攻击者在进行其他询问时,总是已进行过相应的 H_1 询问.

H_2 询问:B 保存一个 H_2 列表,由元素 (R_1,R_2,R_3,h) 组成,最初该列表为空.当 B 接收到询问时,B 首先检查列表中是否已存在对应的元素,如果是,则返回相应的结果;否则,B 从 $\{0,1\}^{\lambda}$ 中随机选取一个元素作为回答,并把该“询问-回答”加入 H_2 列表.

部分私钥询问:B 保存一个部分私钥列表,由元素 (ID_i,D_i) 组成,最初该列表为空.当 $\boldsymbol{A}_{\mathrm{I}}$ 询问用户 ID_i 的部分私钥时,如果 $i\neq I$ 且 $i\neq J$,则 B 从 H_1 列表中查找到 (ID_i,Q_i,d_i) ,计算出部分私钥 $D_i=d_iP_0$,并把 (ID_i,D_i) 加入部分私钥列表,然后把 D_i 返回给 A_{I};如果 $i=I$ 或者 J,则 B 退出游戏.

秘密值询问:B 保存一个秘密值列表,由元素 (ID_i,x_i) 组成,最初该列表为空.当 $\boldsymbol{A}_{\mathrm{I}}$ 询问用户 ID_i 的秘密值时,B 从 Z_q^* 中随机选取 x_i ,并把 (ID_i,x_i) 加入秘密值列表,然后把 x_i 返回给 $\boldsymbol{A}_{\mathrm{I}}$.

公钥询问:当 $\boldsymbol{A}_{\mathrm{I}}$ 询问用户 ID_i 的公钥时,B 检查秘密值列表是否存在 (ID_i,x_i) ,若存在,则计算 $Y_i=x_iP$,并返回给 $\boldsymbol{A}_{\mathrm{I}}$;否则,$B$ 首先进行“秘密值询问”操作,然后再计算公钥.

公钥替换:$\boldsymbol{A}_{\mathrm{I}}$ 可以把任何用户的公钥 Y_i 替换成 $Y_i'\in G_1$.$\boldsymbol{A}_{\mathrm{I}}$ 不能询问 Y_i' 对应的秘密值.

Signcrypt 询问:$\boldsymbol{A}_{\mathrm{I}}$ 询问 $(\mathrm{ID}_i,\mathrm{ID}_j,m)$ 的密文.如果 $\{\mathrm{ID}_i,\mathrm{ID}_j\}\neq\{\mathrm{ID}_I,\mathrm{ID}_J\}$,不妨设 $i\notin\{I,J\}$, 则 B 用 ID_i 的部分私钥和 ID_i (或 ID_j)的秘密值(若 ID_i 和 ID_j 的公钥均被替换,则把写入 H_2 列表的元素的第 3 部分记为 $dh(Y_i',Y_j')$,并

随机选取 $h\in\{0,1\}^{\lambda}$)计算密文,同时把结果返回给攻击者 $\boldsymbol{A}_{\mathrm{I}}$;如果 $\{\mathrm{ID}_i,\mathrm{ID}_j\}=\{\mathrm{ID}_I,\mathrm{ID}_J\}$,则 B 从对称加密算法(Enc,Dec)的密钥空间随机选取一个密钥 K,计算密文 $\mathrm{Enc}_K(m)$, 然后从 Z_q^* 中随机选取 r,得到完整密文 $C=(r,\mathrm{Enc}_K(m))$,并把 C 返回给 $\boldsymbol{A}_{\mathrm{I}}$.在此过程中,涉及到的新的 H_2 元素都被记录到 H_2 列表中.

Unsigncrypt 询问:$\boldsymbol{A}_{\mathrm{I}}$ 询问 $(\mathrm{ID}_i,\mathrm{ID}_j,C=(U,V))$ 的明文.如果 $\{\mathrm{ID}_i,\mathrm{ID}_j\}\neq\{\mathrm{ID}_I,\mathrm{ID}_J\}$,不妨设 $i\notin\{I,J\}$,则 B 用 ID_i 的部分私钥和 ID_i (或 ID_j)的秘密值(若 ID_i 和 ID_j 的公钥均被替换,则在查找 H_2 列表时,在前两项匹配的前提下,验证第 3 项 R_3 是否满足 $\hat{e}(P,R_3)=\hat{e}(Y_i',Y_j')$)来进行解密,并把解密结果返回给 $\boldsymbol{A}_{\mathrm{I}}$;如果 $\{\mathrm{ID}_i,\mathrm{ID}_j\}=\{\mathrm{ID}_I,\mathrm{ID}_J\}$,则 B 查找 H_2 列表是否有元素 (U,R_2,R_3,h) 存在,这里, R_3 满足 $\hat{e}(P,R_3)=\hat{e}(\tilde{Y}_i,\tilde{Y}_j)$, $\tilde{Y}_i$ 表示 Y_i或Y_i', $\tilde{Y}_j$ 表示, $R_2\in G_2$, $h\in\{0,1\}^{\lambda}$, 如果存在,则计算 $D_h(V)$,并把 (U,R_2,R_3) 加入一个新列表 L_0;否则,回答 $\perp$.设攻击者在输出伪造密文之前,已对该密文进行过 Unsigncrypt 询问.

伪造:最后,攻击者 $\boldsymbol{A}_{\mathrm{I}}$ 输出 $(\mathrm{ID}_i^*,\mathrm{ID}_j^*,C^*=(U^*,V^*))$.若 $\{\mathrm{ID}_i^*,\mathrm{ID}_j^*\}\neq\{\mathrm{ID}_I,\mathrm{ID}_J\}$,则 B 失败;否则,B 搜索 L_0 列表,找到元素 (U^*,R_2,R_3^*),这里 R_3^* 等于 ID_i^* 与 ID_j^* 公钥的 Diffie-Hellman 值, $R_2\in G_2$,然后输出 R_2 作为 BDH 问题的解答.

分析:令 $\boldsymbol{AskH}_2$ 表示 $\boldsymbol{A}_{\mathrm{I}}$ 询问 $H_2(U^*,\hat{e}(P,P)^{abc},R_3^*)$ 的值, ¬Abort 表示 B 不退出游戏.令事件 $\boldsymbol{E}$=$\boldsymbol{AskH}_2$|¬Abort,则 Pr[$\boldsymbol{A}_{\mathrm{I}}$win]=Pr[$\boldsymbol{A}_{\mathrm{I}}$win|$\boldsymbol{E}$]Pr[$\boldsymbol{E}$]+Pr[$\boldsymbol{A}_{\mathrm{I}}$win|¬$\boldsymbol{E}$]Pr[¬$\boldsymbol{E}$].如果 $\boldsymbol{E}$ 不发生,那么 $\boldsymbol{A}_{\mathrm{I}}$ 赢得游戏的概率最多为 ν, 即 Pr[$\boldsymbol{A}_{\mathrm{I}}$win|¬$\boldsymbol{E}$]$\leqslant\nu$, 又知 Pr[$\boldsymbol{A}_{\mathrm{I}}$ win]$\geqslant\varepsilon$, 可得:

$$\varepsilon\leqslant\Pr[\boldsymbol{A}_{\mathrm{I}}\mathrm{win}]\leqslant\Pr[\boldsymbol{E}]+\nu\ \Pr[\neg\boldsymbol{E}],$$

$$\Pr[E]\geqslant\frac{\varepsilon-\nu}{1-\nu}\geqslant\varepsilon-\nu,$$

$$\frac{\Pr[\boldsymbol{AskH}_2]}{\Pr[\neg Abort]}\geqslant\Pr[E]\geqslant\varepsilon-\nu,$$

$$\Pr[\boldsymbol{AskH}_2]\geqslant(\varepsilon-\nu)\Pr[\neg Abort]\geqslant\frac{\varepsilon-\nu}{C_{q_1}^2}.$$

B 能够解决 BDH 问题的概率等于 $\boldsymbol{AskH}_2$ 发生的概率 $\frac{\varepsilon-\nu}{C_{q_1}^2}$. □

定理 2. 假设(Enc,Dec)具有可认证性.新方案在随机预言模型和 CDH 困难性假设下对第 2 类攻击者 $\boldsymbol{A}_{\mathrm{II}}$ 具有 UF-CMA 安全性.

证明简述:算法 B 接收一个随机的 CDH 问题实例(aP,bP),其目标是求出 abP.B 把 $\boldsymbol{A}_{\mathrm{II}}$ 作为子程序并在游戏中扮演 $\boldsymbol{A}_{\mathrm{II}}$ 的挑战者,把被挑战发送者和接收者的公钥分别设为 aP 和 bP,最后 $\boldsymbol{A}_{\mathrm{II}}$ 若能以一个不可忽略的优势伪造一个有效密文,则其必定以一个不可忽略的概率询问过 $H_2(\cdot,\cdot,abP)$ (H_2 是一个随机预言器).最后,B 从 H_2 列表中随机选取一个匹配的元素并输出其第 3 项作为对 CDH 问题的解答. □

定理 3. 假设(Enc,Dec)具有机密性,且新方案满足 UF-CMA 安全性(已证).新方案在随机预言模型和 BDH 困难性假设下对第 1 类攻击者 $\boldsymbol{A}_{\mathrm{I}}$ 具有 IND-CCA 安全性.

证明简述:算法 B 接收一个随机的 BDH 问题实例(aP,bP,cP),其目标是求出 $\hat{e}(P,P)^{abc}$. B 把 $\boldsymbol{A}_{\mathrm{I}}$ 作为子程序并在游戏中扮演 $\boldsymbol{A}_{\mathrm{I}}$ 的挑战者,把 KGC 公钥 P_0 设为 aP,把被挑战发送者和接收者身份的 H_1 值分别设为 bP 和 cP, 最后,$\boldsymbol{A}_{\mathrm{I}}$ 若能以一个不可忽略的优势区分挑战密文,则其必定以一个不可忽略的概率询问过 $H_2(\cdot,\hat{e}(P,P)^{abc},\cdot)$ (H_1 和 H_2 是随机预言器).最后,B 从 H_2 列表中随机选取一个匹配的元素并输出其第 2 项作为对 BDH 问题的解答. □

定理 4. 假设(Enc,Dec)具有机密性,且新方案满足 UF-CMA 安全性(已证).新方案在随机预言模型和 CDH 困难性假设下对第 2 类攻击者 $\boldsymbol{A}_{\mathrm{II}}$ 具有 IND-CCA 安全性.

证明简述:算法 B 接收一个随机的 CDH 问题实例(aP,bP),其目标是求出 abP.B 把 $\boldsymbol{A}_{\mathrm{II}}$ 作为子程序并在游戏中扮演 $\boldsymbol{A}_{\mathrm{II}}$ 的挑战者,把被挑战发送者和接收者的公钥分别设为 aP 和 bP,最后 $\boldsymbol{A}_{\mathrm{II}}$ 若能以一个不可忽略的优势

区分挑战密文,则其必定以一个不可忽略的概率询问过 $H_2(\cdot,\cdot,abP)$ (H_2 是一个随机预言器).最后,B 从 H_2 列表中随机选取一个匹配的元素并输出其第 3 项作为对 CDH 问题的解答.

4.2 效率分析

本节从签密、解密认证的效率和密文长度这 3 个方面对新方案与已有无证书签密方案进行了比较.3 种主要的运算包括双线性对(p)、点乘运算(s)和指数运算(e).表 1 中,$|P|$表示 G_1 中一个元素的长度,$|r|$表示有限域 Z_q 中一个元素的长度,$|m|$表示明文长度.

Table 1 Comparison of certificateless signcryption schemes

表 1 无证书签密方案之间的比较

Scheme	Signcrypt			Unsigncrypt			Ciphertext-Length
	p	s	e	p	s	e	
Ref.[10]	1	4	1	5	1	0	$2\|P\|+\|m\|$
Ref.[11]	1	3	4	3	0	4	$2\|r\|+2\|P\|+\|m\|$
Ref.[19]	1	4	1	5	1	0	$2\|P\|+\|m\|$
Our scheme	1	1	0	1	1	0	$\|r\|+\|m\|+\tau$

由表 1 可知,新方案不仅在签密和解密认证的效率上(分别只需计算 1 次双线性对和 1 次点乘)比其他方案要高,而且产生的密文长度也最短.对于 80 比特的安全级别,$|P|$=320 比特,$|r|$=160 比特,如果数据封装采用 OCB[22],τ一般取 64 比特,那么密文长度比其他方案至少短 416 比特,这对于带宽窄的通信环境而言,优势是明显的.此外,文献[18]所提方案与新方案可以处理任意长度的消息,而文献[9,10]所提方案则不能.

5 总 结

本文指出文献[19]的攻击是不成立的,并提出了一个新的无证书混合签密方案,证明了其安全性.与已有方案相比,新方案的密文长度更短、运算速度更快.而且,如果两个用户之间频繁通信,那么他们可以预计算 $\hat{e}(Q_s,D_r)$ 和 x_rY_s, 则签密和解密认证的速度相当于对称加、解密.这些优点将使本文的方案在实际应用中体现出明显的优势,尤其是在计算资源和带宽都受限的通信环境,如 ad hoc 网络中.

本文的方案满足可认证性(不可伪造性、完整性)和保密性,但不提供不可否认性,然而,正如文献[5]中所指出的,大多数实际应用并不要求不可否认性.当然,如果不可否认性和效率能够兼得,则是最理想的.

References:

[1] Shamir A. Identity-Based cryptosystems and signature schemes. In: Blakley GR, Chaum D, eds. Proc. of the CRYPTO 1984. LNCS 196, Berlin: Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the CRYPTO 2001. LNCS 2139, Berlin: Springer-Verlag, 2001. 213−229. [doi: 10.1007/3-540-44647-8_13]

[3] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the ASIACRYPT 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[4] Zheng YL. Digital signcryption or how to achieve cost (signature & encryption)<<cost (signature)+cost (encryption). In: Kaliski BS, ed. Proc. of the CRYPTO 1997. LNCS 1294, Berlin: Springer-Verlag, 1997. 165−179. [doi: 10.1007/BFb0052234]

[5] An JH, Dodis Y, Rabin T. On the security of joint signature and encryption. In: Knudsen LR, ed. Proc. of the EUROCRYPT 2002. LNCS 2332, Berlin: Springer-Verlag, 2002. 83−107. [doi: 10.1007/3-540-46035-7_6]

[6] Boyen X. Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography. In: Boneh D, ed. Proc. of the Cryptology-CRYPTO 2003. LNCS 2729, Berlin: Springer-Verlag, 2003. 383−399. [doi: 10.1007/978-3-540-45146-4_23]

[7] Barreto PSLM, Libert B, McCullagh N, Quisquater JJ. Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. In: Roy B, ed. Proc. of the Asiacrypt 2005. LNCS 3788, Berlin: Springer-Verlag, 2005. 515−532.

[8] Li FG, Hu YP, Li G. An efficient identity-based signcryption scheme. Chinese Journal of Computers, 2006,29(9):1641−1647 (in Chinese with English abstract).

[9] Barbosa M, Farshim P. Certificateless signcryption. In: Abe M, Gligor V, eds. Proc. of the ACM Symp. on Information, Computer and Communications Security-ASIACCS 2008. New York: ACM Press, 2008. 369−372. [doi: 10.1145/1368310.1368364]

[10] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the Int'l Symp. on Information Science and Engineering 2008. IEEE Computer Society, 2008. 661−664. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4732302 [doi: 10.1109/ISISE. 2008.206]

[11] Liu ZH, Hu YP, Zhang XS, Ma H. Certificateless signcryption scheme in the standard model. Information Sciences, 2010,180(3): 452−464. [doi: 10.1016/j.ins.2009.10.011]

[12] Cramer R, Shoup V. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM Journal on Computing, 2003,33(1):167−226. [doi: 10.1137/S0097539702403773]

[13] Dent AW. Hybrid signcryption schemes with outsider security. In: Zhou JY, Lopez J, Deng RH, Bao F, eds. Proc. of the ISC 2005. LNCS 3650, Berlin: Springer-Verlag, 2005. 203−217. [doi: 10.1007/11556992_15]

[14] Dent AW. Hybrid signcryption schemes with insider security. In: Boyd C, Nieto JMG, eds. Proc. of the ACISP 2005. LNCS 3574, Berlin: Springer-Verlag, 2005. 253−266.

[15] Bjørstad TE, Dent AW. Building better signcryption schemes with tag-KEMs. In: Yung M, Dodis Y, Kiayias A, Malkin T, eds. Proc. of the PKC 2006. LNCS 3958, Berlin: Springer-Verlag, 2006. 491−507.

[16] Tan CH. Insider-Secure signcryption KEM/tag-KEM schemes without random oracles. In: Proc. of the 3rd Int'l Conf. on Availability, Reliability and Security-ARES 2008. Barcelona, 2008. 1275−1281. http://www.computer.org/portal/web/csdl/doi/10.1109/ARES.2008.112 [doi: 10.1109/ARES.2008.112]

[17] Li FG, Shirase M, Takagi T. Efficient signcryption key encapsulation without random oracles. In: Yung M, Liu P, Lin D, eds. Proc. of the Information Security and Cryptology 2009, LNCS 5487, Berlin: Springer-Verlag, 2009. 47−59. [doi: 10.1007/978-3-642-01440-6_6]

[18] Li FG, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Bao F, Li H, Wang GL, eds. Proc. of the ISPEC 2009. LNCS 5451, Berlin: Springer-Verlag, 2008. 112−123. [doi: 10.1007/978-3-642-00843-6_11]

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

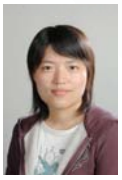
[20] Jutla CS. Encryption modes with almost free message integrity. In: Pfitzmann B, ed. Proc. of the Cryptology-EUROCRYPT 2001. LNCS 2045, Springer-Verlag, 2001. [doi: 10.1007/3-540-44987-6_32]

[21] Gligor V, Donescu P. Fast encryption and authentication: XCBC encryption and XECB authentication modes. In: Matsui M, ed. Proc. of the Fast Software Encryption. LNCS, Berlin: Springer-Verlag, 2001. [doi: 10.1007/3-540-45473-X_8]

[22] Rogaway P, Bellare M, Black J, Krovetz T. OCB: A block-cipher mode of operation for efficient authenticated encryption. In: Proc. of the 8th ACM Conf. on Computer and Communications Security (CCS-8). ACM Press, 2001. 196−205. [doi: 10.1145/501983.502011]

附中文参考文献

[8] 李发根,胡予濮,李刚. 一个高效的基于身份的签密方案.计算机学报,2006,29(9):1641−1647.



孙银霞(1979－),女,江苏常州人,博士生,主要研究领域为密码学,网络安全.

李晖(1969－),男,博士,教授,博士生导师,主要研究领域为信息论,网络安全.