ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.10, October 2009, pp.2810−2821
doi: 10.3724/SP.J.1001.2009.03426

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

基于签密的密码工作流密钥封装机制*

赖 欣[1+], 何大可[2]

[1](中国民用航空飞行学院 空管学院,四川 广汉 618307)

[2](信息安全与国家网格计算实验室(西南交通大学),四川 成都 610031)

Cryptographic Workflow Key Encapsulation Mechanism Based on Signcryption

LAI Xin[1+], HE Da-Ke[2]

[1](Air Traffic Management College, Civil Aviation Fight University of China, Guanghan 618307, China)

[2](Information Security and National Computing Grid Laboratory (IS&NC) SWJTU, Chengdu 610031, China)

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

Lai X, He DK. Cryptographic workflow key encapsulation mechanism based on signcryption. *Journal of Software*, 2009,20(10):2810−2821. http://www.jos.org.cn/1000-9825/3426.htm

Abstract: Cryptographic workflow is a special cryptography system working model in multi-user situations, in which a message is encrypted according to some policy so that only entities guided by the policy are able to decrpt the message. To realize the unforgeability of key encapsulation in without escrow cryptographic workflow, a new key encapsulation mechanism supporting cryptographic workflow based on signcryption is defined. Firstly, a generic model of key encapsulation supporting cryptographic workflow is defined. The corresponding security model of the generic model is also given. Following the generic model, a construction scheme for key encapsulation mechanism supporting cryptographic workflow is proposed by combining secret sharing scheme, ID-based encryption scheme and signcryption scheme. The security of the proposed scheme is proved in standard model with sequences of game. The proposed scheme can satisfy the receiver security and the external security characters in cryptographic work.

Key words: signcrytpion; key encapsulation; cryptographic workflow; identity-based encryption; secret sharing; receiver security; external security

摘 要: 密码工作流(cryptographic workflow)是多用户环境下一种特殊的密码系统工作模式,在这种工作模式下,加密消息需要依据某种策略进行,因此只有履行这一策略的实体才能进行消息解密.为保证在密码工作流模式下密钥封装能够同时实现密钥免托管性和密钥封装传递的不可伪造性,基于签密的思想定义了一个新的密码工作流模式下的密钥封装机制.首先定义了密码工作流模式下基于签密的密钥封装一般模型,并给出了相应的安全模型;其次,结合秘密共享方案、基于身份加密方案和签密方案,提出一个新的结构方案,并在标准模型(standard model)下利用序列游戏证明方法对该结构方案的安全性进行了详细证明.证明结果表明,该密钥封装结构方案能够达到密码工作流模式下要求的接收者安全和外部安全.

* Supported by the Key Laboratory of National Defense Science and Technology Fund of China under Grant No.51436050404QT2202 (国防科技重点实验室基金)

Received 2007-08-24; Accepted 2008-07-24

关键词: 签密;密钥封装;密码工作流;基于身份加密;秘密共享;接收者安全;外部安全
中图法分类号: TP309 文献标识码: A

密码工作流的概念是指在一个加密系统中解密成为一种授权行为,只有接收用户在拥有适当的授权证书集的条件下才能对密文进行解密,即用户所拥有的授权证书集将作为解密密钥或部分解密密钥.密码工作流的概念最初来自于 Chen 的思想[1],由 Paterson 在文献[2]中首次用密码工作流这一术语对其进行了命名.随后,Al-Riyami 等人在文献[3]中基于身份加密方案给出了一个密码工作流加密方案,同时为该类方案建立了安全模型,并且在随机预言机模型下对他们提出的方案进行了安全证明.从结构上来看,Al-Riyami 方案是属于 KEM-DEM 结构的混合加密方案[4].其中,KEM 是利用一个非对称加密方案产生一个短暂会话密钥及其封装,DEM 利用 KEM 产生的会话密钥和一个对称加密算法加密明文.KEM 与 DEM 的安全性是分别独立的,如果 KEM 是一个可证明安全的非对称加密方案的输出,那么 DEM 块的特性就是短暂会话密钥随机性的结果.因此,KEM-DEM 结构下的混合加密体制也是获得可证明 IND-CCA2 安全实际有效的公钥加密的最自然的方法.而密钥封装机制 KEM 是混合加密方案的核心,Dent 等人在文献[5]中给出了几种安全 KEM 的结构方案.Barbosa 等人在 Al-Riyami 方案的基础上对密码工作流进行了进一步形式化定义,提出了一个密码工作流密钥封装机制模型并建立了安全模型,同时在标准模型下对他们提出的一个结构方案进行了证明[6].

Barbosa 与 Al-Riyami 的方案都将加密过程分为一个秘密共享层和一个基于身份的加密层.数据加密时使用的会话密钥按照发送者指定证书集的读取结构,利用秘密共享方案进行分割,从而使得只有具有资格证书集的用户才能恢复会话密钥从而解密密文.他们的方案中都使用了基于身份的加密方案来实现授权证书的分发.为了防止基于身份密码方案潜在的密钥托管特性,上述方案都使用了标准的公钥加密方案来消除因接收者不明确而导致的多个可信授权中心(TA)可能串通非法解密发送者消息的问题.但 Al-Riyami 的方案中并没有考虑传输密钥封装的不可伪造性问题,Barbosa 方案则利用了一次签名方案来弥补这一缺陷,通过提供数据不可伪造性安全从而在标准模型下获得方案的选择密文安全.另外,上述两个方案的会话密钥秘密分享都直接作为密文进行传输,在传输过程中可能导致恶意的主动攻击者对会话密钥秘密分享进行篡改.

可见,要同时实现在密码工作流模式下密钥封装机制的密钥免托管性和数据的不可伪造性,需要分别使用公钥加密方案和签密方案.而在 1997 年,Zheng 提出了一种新的密码原形——签密.该密码原形可以在一个逻辑步骤内同时进行加密和数字签名,且比单独使用公钥加密算法和签名算法的执行效率更高,算法结构更简洁.因此,签密已成为一种在公钥环境下提倡使用的密码原形.使用签密密钥封装更可同时利用签密和混合密码体制两者的优势,首先保证密钥封装 KEM 可同时满足保密性安全和不可伪造性安全,进而提高数据封装 DEM 块的传输安全性.本文借鉴了签密密钥封装的思想,定义了在密码工作流模式下的基于签密的密钥封装机制的一般模型,并对其进行了安全定义.在所提出的模型的基础上,结合秘密共享方案、基于身份加密方案和签密方案,本文给出一个新的结构方案,并在标准模型下对该结构方案的安全性进行了证明.

1 相关密码组件及其安全定义

1.1 基于身份的加密方案(IBE)

一个基于身份的加密方案(identity-based encryption,简称 IBE)由 4 种算法组成[7,8]:

- 主密钥生成概率算法:输入安全参数 1^k,返回一对主私钥和主公钥(Msk,Mpk).

$$(Msk,Mpk)\leftarrow \boldsymbol{G}_{IBE}(1^k).$$

- 私钥提取概率算法:输入主私钥 Msk 和一个用户身份标示串 $ID\in\{0,1\}^*$,返回相应的私钥 S_{ID}.

$$S_{ID}\leftarrow \boldsymbol{EX}_{IBE}(ID,Msk).$$

- 加密概率算法:输入明文消息 m,一个用户身份表示串 $ID\in\{0,1\}^*$和主公钥 Mpk,输出密文 C.

$$C\leftarrow \boldsymbol{E}_{IBE}(m,ID,Mpk).$$

- 解密确定算法:输入密文 C 和私钥 S_{ID},输出一个明文消息 m 或一个停止符$\perp$.

$$m/\perp\leftarrow \boldsymbol{D}_{IBE}(C,S_{ID}).$$

对于所有消息和用户身份,如果有$(Msk,Mpk)\leftarrow \boldsymbol{G}_{IBE}(1^k)$以及 $S_{ID}\leftarrow \boldsymbol{EX}_{IBE}(ID,Msk)$,则必须满足:

$$m=\boldsymbol{D}_{IBE}(C\leftarrow \boldsymbol{E}_{IBE}(m,ID,Mpk),S_{ID}).$$

一个 IBE 方案的保密性可由表 1 所示的挑战者和攻击者之间的适应性选择密文不可区分安全游戏(IND-CCA2 game)来表示.游戏中,*Oracle* 表示攻击者可以进行私钥提取预言机和解密预言机询问,对攻击者的限制是:不能用挑战身份 ID^*询问私钥提取预言机,也不能用挑战密文 C^*询问解密预言机.游戏结束后,攻击者能够获取的优势是 $Adv_{\mathrm{IBE}}^{\mathrm{IND\text{-}CCA2}}(A)=|\Pr[b'=b]-1/2|$.如果一个基于身份的加密方案是 IND-CCA2 安全的,那么攻击者的优势必须是可以忽略的.

Table 1 Adaptive chosen ciphertext attack indistinguishable game

表 1 适应性选择密文攻击不可区分游戏

1. $(Msk,Mpk)\leftarrow \boldsymbol{G}_{IBE}(1^k)$
2. $(state,m_0,m_1,ID^*)\leftarrow A_1^{oracle}(Mpk)$
3. $b\leftarrow_R\{0,1\}$
4. $C^*\leftarrow \boldsymbol{E}_{IBE}(m_b,ID^*,Mpk)$
5. $b'\leftarrow A_2^{oracle}(C^*,state)$

1.2 秘密共享方案(SS)

首先,我们给出秘密共享方案中读取结构的定义.$\mathcal{P}$是集合 $P=\{X_1,X_2,\ldots,X_n\}$所有子集的集合,如果它是一个读取结构,则必须满足:$\forall A\in\mathcal{P}$并且$\forall B\subseteq P,A\subseteq B\Rightarrow B\in\mathcal{P}$,如果 $Q\in\mathcal{P}$那么称集合 $Q\subseteq P$ 是读取结合的一个资格子集.

一个秘密共享方案(secret sharing,简称 SS)由一对算法组成[9,10]:

- 秘密分享概率算法:输入安全参数 1^k,一个需共享的秘密串 s 和一个读取结构$\mathcal{P}$.对应于 $P=\{X_1,\ldots,X_n\}$中的每一项,输出串的秘密分享 $\boldsymbol{shr}=\{shr_1,\ldots,shr_n\}$.

$$\boldsymbol{shr}\leftarrow \boldsymbol{S}\{1^k,s,\mathcal{P}\}.$$

- 秘密恢复确定算法:输入秘密分享 $\boldsymbol{shr}=\{shr_1,\ldots,shr_n\}$和对应的读取结构$\mathcal{P}$,输出一个恢复的秘密共享串 s 或者一个停止符$\perp$.

$$s/\perp\leftarrow \boldsymbol{S}^{-1}(\boldsymbol{shr},\mathcal{P}).$$

对所有的读取结构和共享串,一个秘密共享方案必须满足:

$$s\leftarrow \boldsymbol{S}^{-1}((\boldsymbol{shr})\leftarrow \boldsymbol{S}(1^k,s,\mathcal{P})).$$

秘密共享可分为完善秘密共享方案和计算安全秘密共享方案.为简化安全证明过程,本文将采用完善秘密共享方案的安全定义.所谓完善秘密共享即对任何秘密分享,非资格子集成员都不能获得秘密串 s 的任何信息.

1.3 签密方案(SC)

一个签密方案(sign cryption,简称 SC)由 3 种算法组成[11]:

- 密钥生成概率算法:输入安全参数 1^k,输出用户的公/私密钥对(VEK,SDK),VEK 用于加密与签名验证,SDK 用于解密与签名.

$$(SDK,VEK)\leftarrow \boldsymbol{G}_{SC}(1^k).$$

- 签密概率算法:输入发送者私钥 SDK_S 和接收者公钥 VEK_R 以及明文消息 m,输出一个签密消息 sc.

$$sc\leftarrow \boldsymbol{SE}(SDK_S,VEK_R,m).$$

- 解签密确定算法:输入发送者公钥 VEK_S 和接收者私钥 SDK_R 以及签密消息 sc,输出明文消息 m 或者停止符号$\perp$.

$$m/\perp\leftarrow \boldsymbol{VD}(SDK_R,VEK_S,sc).$$

对所有的消息 m 以及所有由 $\boldsymbol{G}_{SC}(1^k)$产生的密钥对(SDK_S,VEK_S)和(SDK_R,VEK_R),签密方案必须满足:

$$m\leftarrow \boldsymbol{VD}(SDK_R,VEK_S,\boldsymbol{SE}(SDK_S,VEK_R,m)).$$

讨论签密方案的安全性必须区分攻击类型,即签密方案的安全可以分别在外部攻击者模型与内部攻击者模型下进行讨论.本文采用外部攻击模型,即攻击者只能获得公开信息,比如发送者和接收者的公钥等信息.由于签密方案可以同时提供加密和签名功能,因此安全性讨论将涉及到加密的保密性和签名的不可伪造性.

在外部攻击模型下,签密的保密性可由表 2 的抗适应性选择密文攻击不可区分安全游戏来形式化表示.游戏中,*Oracle* 表示攻击者可以进行解签密预言机询问,但对攻击者的限制是不能用挑战密文进行解签密询问.攻击者赢得游戏的优势是 $Adv_{SC}^{\text{IND-CCA2}}(A)=|\Pr[b'=b]-1/2|$,如果一个签密方案是 IND-CCA2 安全的,那么攻击者的优势必须是可忽略的.

在外部攻击模型下,签密方案的不可伪造性可由表3的抗选择消息不可伪造安全游戏(UF-CMA game)来形式化表示.*Oracle* 表示攻击者可以进行签密预言机询问.如果攻击者输出的 *sc* 是一个没有询问过的消息 *m* 的有效签密密文,攻击者赢得游戏且优势是 $Adv_{SC}^{\text{UF-CMA}}(A)=\Pr[adversary\ wins]$,如果一个签密方案是 UF-CMA 安全的,那么攻击者的优势必须是可忽略的.

Table 2 Adaptive chosen ciphertext attack indistinguishable game

表 2 适应性选择密文攻击不可区分游戏

1. $(SDK_S,VEK_S)\leftarrow \boldsymbol{G}_{SC}(1^k)$
2. $(SDK_R,VEK_R)\leftarrow \boldsymbol{G}_{SC}(1^k)$
3. $(m_0,m_1,state)\leftarrow A_1^{oracle}(VEK_S,VEK_R)$
4. $b\leftarrow_R\{0,1\}$
5. $sc\leftarrow \boldsymbol{SE}(SDK_S,VEK_R,m_b)$
6. $b'\leftarrow A_2^{oracle}(sc,state)$

Table 3 Chosen message unforgeability game

表 3 选择消息攻击不可伪造性游戏

1. $(SDK_S,VEK_S)\leftarrow \boldsymbol{G}_{SC}(1^k)$
2. $(SDK_R,VEK_R)\leftarrow \boldsymbol{G}_{SC}(1^k)$
3. $sc\leftarrow A^{oracle}(VEK_S,VEK_R)$

2 基于签密的密码工作流密钥封装机制的一般模型

本节中,我们首先基于签密的思想定义一个密码工作流密钥封装机制一般模型,并给出该模型的安全定义.本模型中,短暂会话密钥及其封装的生成不仅与接收方的公钥有关,还与发送方的私钥相关.

2.1 一般模型定义

定义 1. 基于签密的密码工作流密钥封装机制(WF-SCKEM)的一般模型可由 5 种算法组成:

- 授权中心密钥生成概率算法:输入安全参数 1^k,输出 m 个可信证书授权中心的私钥/公钥对 $(Msk_i,Mpk_i)_{i=1}^m$,即 $(Msk_i,Mpk_i)_{i=1}^m\leftarrow \boldsymbol{G}_{\text{WF-SCKEM}}^{\text{TA}}\left(1^k,m\right)$.
- 用户密钥生成概率算法:输入安全参数 1^k,输出用户私钥/公钥(SK,PK),即 $(SK,PK)\leftarrow \boldsymbol{G}_{\text{WF-SCKEM}}^{\text{User}}(1^k)$.
- 证书提取概率算法:输入证书提取策略 X,其中包含了策略的标示 ID_P 和可信授权中心公钥 Mpk,输入对应的私钥 Msk,输出证书 crd,即 $crd\leftarrow \boldsymbol{X}_{\text{WF-SCKEM}}(X,Msk)$.
- 密钥封装概率算法:输入一个策略集 $P=\{X_1,\ldots,X_n\}$上的读取结构$\mathcal{P}$,以及接收者的公钥 PK_R 和发送者私钥 SK_S,输出一对(k,c).其中,k 是 DEM 将使用的短暂会话密钥,c 是会话密钥的封装,即
$$(k,c)\leftarrow \boldsymbol{Encap}_{\text{WF-SCKEM}}(\mathcal{P},PK_R,SK_S).$$
- 解封装确定算法:输入一个会话密钥封装 c 和资格证书集 $\{crd\}_{i=1}^n$,以及发送者的公钥 PK_S 和接收者私钥 SK_R,输出一个会话密钥 k 或一个停止符⊥,即 $k/\perp\leftarrow \boldsymbol{Decap}_{\text{WF-SCKEM}}(c,[crd]_{i=1}^l,SK_R,PK_S)$.

对具有 n 证书提取策略的读取结构$\mathcal{P}$,在各 TA 正确产生主密钥对,用户正确产生公/私密钥对以及用户从各 TA 处成功获得授权证书后,一个安全的 WF-SCKEM 必须满足:

$$k=\boldsymbol{Decap}_{\text{WF-KEM}}(\boldsymbol{Encap}_{\text{WF-KEM}}(\mathcal{P},PK_S,SK_R),\boldsymbol{crd},SK_S,PK_R).$$

2.2 安全定义

一个密码工作流密钥封装机制的安全性需要从两方面加以定义[3]:其一是接收者安全(receiver security),即确保只有拥有正确证书集的用户才可以恢复短暂会话密钥从而解密密文;其二是外部安全(external security),其目的是为了获得方案的免托管特性.由于证书的分发完全由 TA 控制,多个 TA 串谋将完全有能力获得恢复短暂会话密钥所需的全部证书集.因此,如果不具有外部安全,很容易造成多个 TA 串谋非法解密发送者消息的情况.外部安全的获得是通过发送者明确指定接收者的方式来获得的,通过接收者的公钥加密部分信息,从而使得只有指定接收者在持有正确私钥的条件下才能恢复短暂会话密钥.下面我们利用挑战者和攻击者之间的攻击游戏对上述安全特性进行形式化描述.

2.2.1 接收者安全

在具有 m 个 TA、读取结构由 n 个策略项组成的情况下,接收者安全定义为在适应性选择证书攻击下的不可区分性((m,n)-IND-CCCA).定义 2 给出攻击者和挑战者适应性选择证书攻击下的不可区分性游戏((m,n)-IND-CCCA game),见表 4.在挑战游戏中,攻击者将从挑战处获得 m 个 TA 的主公钥,挑战发送方公钥和挑战接收方公钥,甚至挑战接收方私钥.*Oracle* 表示攻击者可以进行证书提取预言机询问和解封装预言机询问,但要求是攻击者不能进行关于挑战读取结构 $\mathcal{P}^*$ 上策略项的证书提取询问,并且攻击者不能用挑战密钥封装 c^* 进行解封装询问.从攻击者具有的能力上看,因为拥有挑战接收方私钥,因此已经拥有部分挑战密文的解密能力.该攻击游戏强调了即使攻击者拥有合法的解密私钥,但是如果不具备发送者指定的证书集,仍然无法恢复会话密钥.攻击者在游戏中的优势为 $Adv^{(m,n)\text{-IND-CCCA}}_{\text{WF-SCKEM}}(A):=|\Pr[b'=b]-1/2|$.如果一个 WF-SCKEM 是($m$,$n$)-IND-CCCA 安全的,那么攻击者的优势必须是可以忽略的(注: $\mathbb{K}_{\text{WF-SCKEM}}=\{0,1\}^{|\mathcal{K}|}$ 为会话密钥空间).

Table 4 Adaptive chosen certificate attack indistinguishable game

表 4 适应性选择证书攻击不可区分游戏

Definition 2. (m,n)-IND-CCCA game.

1. $(Msk_i,Mpk_i)_{i=1}^m \leftarrow \boldsymbol{G}^{\text{TA}}_{\text{WF-SCKEM}}(1^k,m)$
2. $(SK_S^*,PK_S^*)/(SK_R^*,PK_R^*) \leftarrow \boldsymbol{G}^{\text{User}}_{\text{WF-SCKEM}}(1^k)$
3. $(state,\mathcal{P}^*) \leftarrow A_1^{oracle}((Mpk_i)_{i=1}^m,PK_S^*,PK_R^*,SK_R^*)$
4. $k_0 \leftarrow \mathbb{K}_{\text{WF-SCKEM}}$
5. $(k_1,c^*) \leftarrow \boldsymbol{Encap}_{\text{WF-SCKEM}}(\mathcal{P}^*,PK_R^*,SK_S^*)$
6. $b \leftarrow_R \{0,1\}$
7. $b' \leftarrow A_2^{oracle}(k_b,c^*,PK_S^*,PK_R^*,SK_R^*,state)$

2.2.2 外部安全

在具有 m 个 TA、读取结构由 n 个策略项组成的情况下,外部安全定义为在适应性选择密文攻击下的不可区分性((m,n)-IND-CCA2).定义 3 给出攻击者和挑战者的适应性选择密文攻击不可区分性游戏((m,n)-IND-CCA2 game),见表 5.在挑战游戏中,攻击者将从挑战处获得 m 个 TA 的主公钥和主私钥,挑战发送方公钥和挑战接收方公钥.*Oracle* 表示攻击者可以进行解封装预言机询问,但要求攻击者不能用挑战密钥封装 c^* 进行解封装询问.从攻击者具有的能力上看,因为拥有所有 TA 的主公钥和主私钥,已经拥有完全的证书提取能力.该攻击游戏强调了即使是多个 TA 窜谋拥有了发送者指定的证书集,但是,如果他们不具有合法的用户解密私钥,仍然无法恢复会话密钥.攻击者在游戏中的优势为 $Adv^{(m,n)\text{-IND-CCA2}}_{\text{WF-SCKEM}}(A):=|\Pr[b'=b]-1/2|$.如果一个 WF-SCKEM 是($m$,$n$)-IND-CCA2 安全的,那么攻击者的优势必须是可以忽略的.

Table 5 Adaptive chosen ciphertext attack indistinguishable game

表 5 适应性选择密文攻击不可区分游戏

Definition 3. (m,n)-IND-CCA2 game.

1. $(Msk_i,Mpk_i)_{i=1}^{m} \leftarrow \boldsymbol{G}_{\text{WF-SCKEM}}^{\text{TA}}\left(1^k,m\right)$
2. $(SK_S^*,PK_S^*)/(SK_R^*,PK_R^*) \leftarrow \boldsymbol{G}_{\text{WF-SCKEM}}^{\text{User}}(1^k)$
3. $(state,\mathcal{P}^*) \leftarrow A_1^{oracle}((Msk_i,Mpk_i)_{i=1}^{m},PK_S^*,PK_R^*)$
4. $k_0 \leftarrow \mathbb{K}_{\text{WF-SCKEM}}$
5. $(k_1,c^*) \leftarrow \boldsymbol{Encap}_{\text{WF-SCKEM}}(\mathcal{P}^*,PK_R^*,SK_S^*)$
6. $b \leftarrow_R \{0,1\}$
7. $b' \leftarrow A_2^{oracle}(k_b,c^*,PK_S^*,PK_R^*,state)$

3 基于签密的密码工作流密钥封装机制结构方案

根据上文提出的一般模型,结合基于身份加密方案 IBE、秘密共享方案 SS 和签密方案 SC,本节提出一个基于签密的密码工作流密钥封装机制结构方案.根据上文给出的安全定义,我们在标准模型下对该结构方案的安全性进行讨论.

3.1 WF-SCKEM结构方案

在 WF-SCKEM 结构方案中,可信授权中心 TA 的主密钥生成、用户证书提取直接采用基于身份加密方案 IBE 的主密钥生成算法和私钥提取算法.

授权中心密钥生成 $\boldsymbol{G}_{\text{WF-SCKEM}}^{\text{TA}}\left(1^k,m\right)$:$m$ 个 TA 执行 $\boldsymbol{G}_{\text{IBE}}(1^k)$算法,获得各自的主公私密钥对$(Msk_i,Mpk_i)$.各 TA 向系统用户发布它的主公钥 Mpk_i,并保密主私钥 Msk_i.

证书提取 $\boldsymbol{X}_{\text{WF-SCKEM}}(X,Msk)$:用户提交证书提取策略 $X=(ID_P,Mpk)$给 Mpk 对应的 TA,TA 利用其主私钥 Msk 以及 IBE 方案的私钥提取算法计算 $crd \leftarrow \boldsymbol{EX}_{IBE}(ID_P,Msk)$,得到 X 对应的证书 crd.令 $\boldsymbol{crd}=(crd,X)$并通过安全信道将其返回给用户.

用户密钥生成 $\boldsymbol{G}_{\text{WF-SCKEM}}^{\text{User}}(1^k)$:采用签密方案的密钥生成算法$(SDK,VEK) \leftarrow \boldsymbol{G}_{SC}(1^k)$计算得到用户的私钥 SDK 和公钥 VEK,用户发布公钥保密私钥.

密钥封装算法 $\boldsymbol{Encap}_{\text{WF-SCKEM}}(\mathcal{P},SDK_S,VEK_R)$:输入读取结构$\mathcal{P}$,发送方私钥 SDK_S 和接收者公钥 VEK_R 后,结合秘密共享方案 SS、基于身份加密方案 IBE 和签密方案 SC,密钥封装过程执行如下:

- $k \leftarrow_R \{0,1\}^{|\mathcal{K}|}$;
- $\boldsymbol{shr} \leftarrow \boldsymbol{S}(1^k,k,\mathcal{P})$;
- For j=1 to n do $\{(ID_P,Mpk) \leftarrow X_j; c_j \leftarrow \boldsymbol{E}_{IBE}([shr]_j \| VEK_S,ID_P,Mpk);\}$;
- $\overline{c} \leftarrow (c_1,\ldots,c_n,\mathcal{P})$;
- $c \leftarrow \boldsymbol{SE}(SDK_S,VEK_R,\overline{c})$;

返回(k,c).

解封装算法 $\boldsymbol{Decap}_{\text{WF-SCKEM}}(c,[crd]_{j=1}^{l},VEK_R,SDK_S)$:输入密钥封装 c,资格证书集$[crd]_{j=1}^{l}$,发送方公钥 VEK_S 与接收方私钥 SDK_R 后,结合秘密共享方案 SS、基于身份加密方案 IBE 和签密方案 SC,解封装过程执行如下:

- $\overline{c}' \leftarrow \boldsymbol{VD}(SDK_S,VEK_R,c)$; If $\overline{c}'=\perp$ return $\perp$;
- Parse $(c_1',\ldots,c_n',\mathcal{P}') \leftarrow \overline{c}'$
- For j=1 to l do

  $\{(crd,X) \leftarrow [\boldsymbol{crd}]_j$; Find c_j' corresponding to crd;

  $[shr]_j' \| VEK_S' \leftarrow \boldsymbol{D}_{\text{IBE}}(c_j',crd)$; If $[shr]_j' \| VEK_S'=\perp$ return $\perp$;

  If $VEK_S' \neq VEK_S$ return $\perp$;$\}$;

- $k' \leftarrow \boldsymbol{S}^{-1}(1^k, \boldsymbol{shr}', \mathcal{P})$ if $k'=\perp$ return $\perp$

返回 k'.

3.2 方案的安全性讨论

根据第 2 节的安全定义,我们在标准模型下利用序列游戏(sequences of games)[12]证明方法对提出的结构方案的接收者安全性和外部安全性分别进行讨论.

3.2.1 接收者安全证明

定理 1. 如果 WF-SCKEM 结构方案中使用的 IBE 方案是 IND-CCA2 安全的,秘密共享方案是完善安全的,签密方案是关于不可伪造性 UF-CMA 安全的,那么该 WF-SCKEM 结构方案是关于接收者安全(m,n)-IND-CCCA 安全的,且攻击者的攻击优势为 $Adv_{\text{WF-SCKEM}}^{(m,n)\text{-IND-CCCA}}(A) \le Adv_{\text{SC}}^{\text{UF-CMA}}(B_1) + 2m \cdot Adv_{\text{IBE}}^{\text{IND-CCA2}}(B_2)$.

证明:根据定义 2 给出的(m,n)-IND-CCCA 安全定义可知,攻击者 A 掌握的信息包括:挑战者给出的挑战发送者公钥 VEK_S^*、挑战接收者公钥/私钥 VEK_R^*, SDK_R^* 以及 m 个 TA 的主公钥 $(Mpk_i)_{i=1}^m$、攻击者自己提交的读取结构 $\mathcal{P}^*$.因此,对于挑战接收方将具有解封过程中完全的解签密能力.因此,我们着重考察用 IBE 加密会话密钥分享得到的密文 $\overline{c}^*$ 的不可区分性.结构方案的接收者安全性需依靠 SC 方案的不可伪造性安全以及 IBE 方案的不可区分性安全来获得.为此,我们利用一系列转换游戏 $Game_0,\ldots,Game_3$ 对定理 1 进行证明.令 $Succ_i$ 表示在游戏 $Game_i$ 中攻击者正确猜测挑战比特的事件:

$Game_0$:表示初始的(m,n)-IND-CCCA 攻击游戏,由定义 2 可得 $Adv_{\text{WF-SCKEM}}^{(m,n)\text{-IND-CCCA}}(A) = |\Pr[Succ_0] - 1/2|$.

$Game_1$:对 $Game_0$ 进行如下修改得到 $Game_1$:对所有的解封装询问,如果解封装过程中涉及到挑战发送者公钥 VEK_S^*,那么一律返回停止符$\perp$.从 $Game_0$ 到 $Game_1$ 转换中,A 成功概率是可以忽略的.用 E 表示攻击者 A 能够提交一个关联公钥 VEK_S^* 的有效密文 c,且该密文不同于挑战密文 c^*.该事件说明,在未知私钥 SDK_S^* 的前提下,A 也能构造一个有效密文.如果 E 事件发生,那么一定存在一种算法 B_1 可以利用 E 攻击签密方案的 UF-CMA 安全.如果事件 E 不发生,那么 $Game_0$ 等价于 $Game_1$,即$|\Pr[Succ_0]-\Pr[Succ_1]| \le \Pr[E]$,而 $\Pr[E] = Adv_{\text{SC}}^{\text{UF-CMA}}(B_1)$,因此有

$$|\Pr[Succ_0] - \Pr[Succ_1]| \le Adv_{\text{SC}}^{\text{UF-CMA}}(B_1).$$

$Game_2$:对 $Game_1$ 进行如下修改得到 $Game_2$:因为攻击者 A 已知挑战发送者公钥 VEK_S^*、挑战接收者公钥/私钥 VEK_R^*, SDK_R^*,那么他完全具有解封装过程中涉及的解签密能力.攻击者对挑战密文解签密后可得到 $\overline{c}^* = (c_1^*,\ldots,c_n^*,\mathcal{P}^*)$,因此,如果攻击者重用 c_i^* 和 $\mathcal{P}^*$继续进行解封装过程中的 $\boldsymbol{D}_{IBE}(c_j^*,\cdot)$ 询问,挑战者将立即返回停止符$\perp$.在 $Game_1$ 中对所有的解封装询问,如果涉及到了发送者公钥 VEK_S^*,那么将立即返回停止符$\perp$.而如果用挑战 c_i^* 进行 $\boldsymbol{D}_{\text{IBE}}(c_j^*,\cdot)$ 询问必然会返回 VEK_S^*,因此 $Game_2$ 等价于 $Game_1$,即 $\Pr[Succ_2]=\Pr[Succ_1]$.

$Game_3$:$Game_2$ 进行如下修改得到 $Game_3$:利用另一个随机密钥 k_2 的秘密分享结果来构造 c_j.对攻击者 A 来说,$Game_3$ 与 $Game_2$ 的区别也是可忽略的,他不能从这个转变过程获取任何(m,n)-IND-CCCA 攻击的优势.我们对此进行证明.如果 $\Pr[Succ_3]-\Pr[Succ_2]$是不可忽略的,那么一定存在一个与本方案中 IBE 方案完全一致的外部 IBE 方案攻击者 B_2,他可以插入到 $Game_3$ 与 $Game_2$ 之间,并将利用 A 作为一个子算法,成功地攻击一个外部 IBE 方案的 IND-CCA2 安全性.这一情况下,挑战游戏中将存在 4 个实体:外部 IBE 方案 IND-CCA2 挑战者、外部 IBE 方案 IND-CCA2 攻击者 B_2、WF-SCKEM 结构方案(m,n)-IND-CCCA 挑战者、WF-SCKEM 结构方案(m,n)-IND-CCCA 攻击者 A.为了利用攻击者 A,B_2 将完全控制(m,n)-IND-CCCA 挑战者和攻击者 A 之间的信息通道,并利用外部 IBE 方案 IND-CCA2 挑战者提供的相关信息仿真(m,n)-IND-CCCA 攻击游戏.执行过程如下:

- B_2 从 $1,\ldots,n$ 中随机挑选一个值 t;n 是策略项的个数.
- B_2 自己创建 $m-1$ 个主密钥对 $(Mpk_i, Msk_i)_{i=1}^{m-1}$,并把从外部 IBE 方案 IND-CCA2 挑战者处获得的挑战主公钥 Mpk^*作为第 m 个主公钥(对于 Mpk^*对应的主私钥他一无所知).B_2 随机地对把 m 个主密钥 $\{(Mpk_i)_{i=1}^{m-1}, Mpk^*\}$ 排序,并连同从本方案(m,n)-IND-CCCA 挑战者处获得挑战发送者公钥 VEK_S^*,接收者公钥、私钥 VEK_R^*, SDK_R^* 一并发送给攻击者 A.

- 攻击者 A 根据获得的 m 个主密钥 $\{(Mpk_i)_{i=1}^{m-1}, Mpk^*\}$,构建挑战读取结构 $\mathcal{P}^*$,并提交给 B_2.
- 根据 A 给定的挑战读取结构 $\mathcal{P}^*$,B_2 按照如下方式构建挑战密文 $\overline{c}^*$:
  - B_2 首先检查,如果 Mpk^* 没有与挑战读取结构中的第 t 项策略相关联,那么 B_2 终止游戏,定义该事件为 $Event1$.令 X_t 是第 t 项策略,其中包含了 Mpk^* 且对应策略项标示定义为 ID_P^*.在 B_2 没有终止游戏的条件下,$\mathcal{P}^*$ 中的策略项将是如下形式:

    $$X_1=(Mpk_1, ID_{P1}),...,X_t=(Mpk^*, ID_P^*),...,X_n=(Mpk_n, ID_{Pn}).$$

  - B_2 从会话密钥空间中随机选择 3 个密钥 k_0,k_1,k_2,并将 k_1,k_2 在挑战读取结构下 $\mathcal{P}^*$ 经过秘密共享方案计算得到 $\boldsymbol{shr}_1^*=[shr_1^*]_{j=1}^n$ 并且 $\boldsymbol{shr}_2^*=[shr_2^*]_{j=1}^n$.
  - B_2 将 $[shr_1^*]_{j=1}^{t-1}\|VEK_S^*$,在对应策略 $(Mpk_j, ID_{Pj})_{j=1}^{t-1}$ 下,利用 IBE 加密算法加密得到 $[c_1^*]_{j=1}^{t-1}$,即 $[c_1^*]_j \leftarrow \boldsymbol{E}_{IBE}([shr_1]_j\|VEK_S^*, ID_{Pj}, Mpk_j)$,构建挑战秘密分享加密的 1,…,$t$–1 部分;对第 t 个分享加密的构造,B_2 首先定义 $m_0=[shr_1^*]_t\|VEK_S^*$,$m_1=[shr_2^*]_t\|VEK_S^*$,并将 m_0,m_1 以及 ID_P^* 作为外部 IBE 方案 IND-CCA2 游戏的挑战消息发送给外部 IBE 方案 IND-CCA2 挑战者;随后,B_2 用 $[shr_2^*]_j\|VEK_S^*$ 及对应策略项 $(Mpk_j, ID_{Pj})_{j=t+1}^n$ 在 IBE 加密算法计算下得到 $[c_2^*]_{j=t+1}^n$,即 $[c_2^*]_j \leftarrow \boldsymbol{E}_{IBE}([shr_2]_j\|VEK_S^*, Mpk_j, ID_{Pj})$ 构造余下的 t+1,…,n 个挑战分享的加密结果.
  - 外部 IBE 方案 IND-CCA2 挑战者随机选择一个比特 $\overline{b}\leftarrow_R\{0,1\}$,并计算挑战密文 $\boldsymbol{E}_{IBE}(m_{\overline{b}}, ID_P^*, Mpk^*)$ 返回给 B_2.此时,B_2 构造的 $\overline{c}^*$ 将有如下形式:

    $$\{[c_1^*]_{j=1}^{t-1}, \boldsymbol{E}_{\mathrm{IBE}}(m_{\overline{b}}, ID_P^*, Mpk^*), [c_2^*]_{j=t+1}^n, \mathcal{P}^*\}.$$

  - B_2 随机选择一个比特 b,将 k_b 构造的 $\overline{c}^*=\{[c_1^*]_{j=1}^{t-1}, \boldsymbol{E}_{\mathrm{IBE}}(m_{\overline{b}}, ID_P^*, Mpk^*), [c_2^*]_{j=t+1}^n, \mathcal{P}^*\}$ 提交给攻击者 A.
- 对 A 的证书提取询问,B_2 如下处理:关于 m–1 个 B_2 自己创建的主公钥的证书提取询问 (Mpk_i, ID_P),B_2 可以直接利用 IBE 方案的私钥提取算法计算证书并响应;如果是关于外部 IBE 方案挑战主公钥的证书提取询问 (Mpk^*, ID_{Pi}),B_2 将询问传递给外部 IBE 方案挑战者,在从外部 IBE 方案挑战者处返回响应证书后再将其返回给攻击者 A;如果是攻击者 A 提出的关于 (Mpk^*, ID_P^*) 的证书提取询问,B_2 将视其为非法提问并终止游戏,定义该事件为 $Event2$.
- 对 A 的解封装询问,B_2 如下处理:通过执行证书提取询问获得需要的证书;如果在询问中没有包含 (Mpk^*, ID_P^*),B_2 将调用 IBE 的解密算法进行计算并给出响应.如果在询问的 c_j^* 与 (Mpk^*, ID_P^*) 关联,那么 B_2 将立即返回停止符 $\perp$.
- 最后,B_2 将从攻击者 A 处得到一个关于 (m,n)-IND-CCCA 攻击游戏的猜测比特 b'.如果 $b=b'$,B_2 将向外部 IBE 方案的 IND-CCA2 挑战者提交他的猜测比特 $\hat{b}=1$;如果 $b\neq b'$,则提交 $\hat{b}=0$.

在这个执行过程中,如果要攻击者 A 具有优势,必须首先保证 B_2 不会终止游戏,即事件 $Event1$ 与事件 $Event2$ 不会发生.定义 B_2 终止游戏为事件 $Fail$,如果事件 $Evnet1$ 不发生,则必须保证攻击者 A 输出一个策略集中的第 t 部分必须与外部 IBE 方案 IND-CCA 挑战者给出的公钥 Mpk^* 相关联,而这一事件的概率等于 $\frac{1}{m}$;如果事件 $Event2$ 不发生,则意味着在 n 项策略中至少有一项是不能进行证书提取询问的,这一事件的概率为 $\frac{1}{n}$.而事件 $Event1$ 与 $Event2$ 是相互独立的,因此我们可以得到:

$$\Pr[\neg Fail]=\Pr[\neg Event1\wedge\neg Event2]=\Pr[\neg Event1]\Pr[\neg Event2]\geq\frac{1}{mn}.$$

因为 $\hat{b}$ 是由 B_2 就外部 IBE 方案 IND-CCA2 安全返回的猜测比特,而 $\overline{b}$ 是外部 IBE 方案挑战者选择的比特,那么,B_2 在外部 IBE 方案 IND-CCA2 安全游戏中可以获得的优势是

$$Adv_{\mathrm{IBE}}^{\mathrm{IND\text{-}CCA2}}(B_2)=\frac{1}{2}\Pr[\neg Fail]\cdot|\Pr[\hat{b}=1|\overline{b}=1\wedge\neg Fail]-\Pr[\hat{b}=1|\overline{b}=0\wedge\neg Fail]| \quad (1)$$

在 B_2 没有终止游戏的前提下,观察整个游戏的执行过程可以发现,只有在 $t=n$ 与 $t=1$ 两种情况下得到的 $\bar{c}$ 对攻击者 A 的猜测可能是有利的.我们对这两种情况进行讨论:

当 $t=n$ 时,我们用表 6 来表示在 B_2 的选择 b 比特、外部 IBE 方案挑战者选择 $\bar{b}$ 比特取值的情况下,B_2 提交给攻击者 A 的密钥和 $\bar{c}^*$ 的构造.观测表 6 可见,只有在 $\bar{b}=0$ 的条件下,构造 $\bar{c}^*$ 对应的秘密分享才完全都是来自于 k_1 的秘密分享,这种情况相当于攻击者 A 在 $Game_2$ 环境中进行猜测.攻击者 A 在 $Game_2$ 游戏中成功的概率即为 $\Pr[Succ_2]=\Pr[b'=b]=\Pr[\hat{b}=1\mid t=n\wedge\bar{b}=0\wedge\neg Fail]$, $\Pr[t=n]=\frac{1}{n}$,即有

$$\Pr[Succ_2]=\frac{1}{n}\Pr[\hat{b}=1\mid\bar{b}=0\wedge\neg Fail].$$

Table 6 Construction of k_b and $\bar{c}^*$ when $t=n$

表 6 $t=n$ 时,k_b 与 $\bar{c}^*$ 的构造

	b=0	b=1
$\bar{b}=0$	$k_0,\{[c_1^*]_{j=1}^{n-1},\boldsymbol{E}_{\mathrm{IBE}}([shr_1^*]_{t=n}\|\|VEK_S^*,ID_P^*,Mpk^*),\mathcal{P}^*\}$	$k_1,\{[c_1^*]_{j=1}^{n-1},\boldsymbol{E}_{\mathrm{IBE}}([shr_1^*]_{t=n}\|\|VEK_S^*,ID_P^*,Mpk^*),\mathcal{P}^*\}$
$\bar{b}=1$	$k_0,\{[c_1^*]_{j=1}^{n-1},\boldsymbol{E}_{\mathrm{IBE}}([shr_2^*]_{t=n}\|\|VEK_S^*,ID_P^*,Mpk^*),\mathcal{P}^*\}$	$k_1,\{[c_1^*]_{j=1}^{n-1},\boldsymbol{E}_{\mathrm{IBE}}([shr_2^*]_{t=n}\|\|VEK_S^*,ID_P^*,Mpk^*),\mathcal{P}^*\}$

当 $t=1$ 时,我们用表 7 来表示在 B_2 的选择 b 比特和外部 IBE 方案挑战者选择 $\bar{b}$ 比特取值的情况下,B_2 提交给攻击者 A 的密钥和 $\bar{c}^*$ 的构造.观测表 7 可见,只有在 $\bar{b}=1$ 的条件下,构造 $\bar{c}^*$ 对应的秘密分享才完全都是来自于 k_2 的秘密分享,这种情况相当于攻击者 A 在 $Game_3$ 环境中进行猜测.攻击者 A 在 $Game_3$ 游戏中成功的概率即为 $\Pr[Succ_3]=\Pr[b'=b]=\Pr[\hat{b}=1\mid t=1\wedge\bar{b}=1\wedge\neg Fail]$, $\Pr[t=1]=\frac{1}{n}$,即有 $\Pr[Succ_3]=\frac{1}{n}\Pr[\hat{b}=1\mid\bar{b}=1\wedge\neg Fail]$.综合 $\Pr[Succ_2]$,$\Pr[Succ_3]$表达式可得:

$$n\,|\Pr[Succ_3]-\Pr[Succ_2]|=\Pr[\hat{b}=1\mid\bar{b}=1\wedge\neg Fail]-\Pr[\hat{b}=1\mid\bar{b}=0\wedge\neg Fail] \tag{2}$$

Table 7 Construction of k_b and $\bar{c}^*$ when $t=1$

表 7 $t=1$ 时,k_b 与 $\bar{c}^*$ 的构造

	b=0	b=1
$\bar{b}=0$	$k_0,\{\boldsymbol{E}_{\mathrm{IBE}}([shr_1^*]_{t=1}\|\|VEK_S^*,ID_P^*,Mpk^*),[c_2^*]_{j=1}^{n-1},\mathcal{P}^*\}$	$k_1,\{\boldsymbol{E}_{\mathrm{IBE}}([shr_1^*]_{t=1}\|\|VEK_S^*,ID_P^*,Mpk^*),[c_2^*]_{j=1}^{n-1},\mathcal{P}^*\}$
$\bar{b}=1$	$k_0,\{\boldsymbol{E}_{\mathrm{IBE}}([shr_2^*]_{t=1}\|\|VEK_S^*,ID_P^*,Mpk^*),[c_2^*]_{j=1}^{n-1},\mathcal{P}^*\}$	$k_1,\{\boldsymbol{E}_{\mathrm{IBE}}([shr_2^*]_{t=1}\|\|VEK_S^*,ID_P^*,Mpk^*),[c_2^*]_{j=1}^{n-1},\mathcal{P}^*\}$

结合公式(1)、公式(2)可得 B_2 赢得 IND-CCA2 游戏的优势为

$$Adv_{\mathrm{IBE}}^{\text{IND-CCA2}}(B_2)=\frac{n}{2}\Pr[\neg Fail]\cdot|\Pr[Succ_3]-\Pr[Succ_2]| \tag{3}$$

将 $\Pr[\neg Fail]$代入公式(3)可得:

$$|\Pr[Succ_2]-\Pr[Succ_3]|\le 2m\cdot Adv_{\mathrm{IBE}}^{\text{IND-CCA2}}(B_2) \tag{4}$$

最后观察 $Game_3$ 可见,在对由随机密钥 k_2 的秘密分享生成挑战 $\bar{c}^*$ 时,因为与 k_0,k_1 完全没有关联,因此攻击者 A 将完全没有猜测优势,只能进行随机猜测,即 $\Pr[Succ_3]=\frac{1}{2}$.

综合上述 $Game_0$,…,$Game_3$ 序列游戏,由序列游戏证明定理[12]结果可得:

$$Adv_{\text{WF-SCKEM}}^{(m,n)\text{IND-CCCA}}(A)\le Adv_{\mathrm{SC}}^{\text{UF-CMA}}(B_1)+2m\cdot Adv_{\mathrm{IBE}}^{\text{IND-CCA2}}(B_2).$$ □

3.2.2 外部安全证明

定理 2. 如果 WF-SCKEM 结构方案中使用的签密方案是关于不可伪造性 UF-CMA 安全的、关于保密性 IND-CCA2 安全的,那么 WF-SCKEM 结构方案的外部安全性是(m,n)-IND-CCA2 安全的,且攻击者的攻击优势为 $Adv_{\text{WF-SCKEM}}^{\text{IND-CCA2}}(A)\le Adv_{\mathrm{SC}}^{\text{UF-CMA}}(B_1)+2Adv_{\mathrm{SC}}^{\text{IND-CCA2}}(B_2)$.

证明:根据定义 3 给出的(m,n)-IND-CCA 安全性定义可知,攻击者 A 可以从挑战者处获得的信息包括:挑战者给出的发送者公钥 VEK_S^*、接收者公钥 VEK_R^* 以及 m 个主密钥对 $(Mpk_i,Msk)_{i=1}^m$.因此,攻击者完全具有 IBE 方

案的解密能力和 SS 方案的秘密恢复能力.结构方案的外部安全必须依靠签密方案的不可伪造性以及保密性提供.为此,我们利用一系列转换游戏 $Game_0,\ldots,Game_2$,对定理 2 进行证明.令 $Succ_i$ 表示在游戏 $Game_i$ 中攻击者正确猜测挑战比特的事件.

$Game_0$:表示初始的(m,n)-IND-CCA2 攻击游戏,由上述定义 3 可得 $Adv_{\text{WF-SCKEM}}^{(m,n)\text{-IND-CCA2}}(A)=|\Pr[Succ_0]-1/2|$.

$Game_1$:对 $Game_0$ 进行如下修改得到 $Game_1$:对所有的解封装询问,如果解封装涉及到挑战发送者公钥 VEK_S^*,那么一律返回停止符⊥.在从 $Game_0$ 到 $Game_1$ 的转换过程中,A 成功的概率是可以忽略的.用 E 表示攻击者 A 能够提交一个关联公钥 VEK_S^* 的有效解封装密文 c,且该密文不同于挑战密文 c^*,该事件说明,在未知私钥 SDK_S^* 的前提下,A 也能构造一个有效密文.如果 E 事件发生,那么一定存在一种算法 B_1 可以利用 E 攻击签密方案的 UF-CMA 安全案.如果事件 E 不发生,那么 $Game_0$ 等价于 $Game_1$,即$|\Pr[Succ_0]-\Pr[Succ_1]|\leq\Pr[E]$.而 $\Pr[E]=Adv_{\text{SC}}^{\text{UF-CMA}}(B_1)$,因此有 $|\Pr[Succ_0]-\Pr[Succ_1]|\leq Adv_{\text{SC}}^{\text{UF-CMA}}(B_1)$.

$Game_2$:$Game_1$ 进行如下修改得到 $Game_2$,即利用另一个随机密钥 k_2 的秘密分享结果来构造挑战密钥封装.对攻击者 A 来说,$Game_3$ 与 $Game_2$ 的区别也是可忽略的,他并不能从这个转变过程获取任何(m,n)-IND-CCA2 攻击的优势.我们对此进行证明.

如果 $\Pr[Succ_2]-\Pr[Succ_1]$是不可忽略的,那么一定存在一个与本方案中 SC 方案完全一致的外部 SC 方案攻击者 B_2,他可以插入到 $Game_2$ 与 $Game_1$ 之间,并将利用 A 作为一个子算法,从而成功地攻击外部 SC 方案的 IND-CCA2 安全性.这一情况下,整个挑战游戏中将存在 4 个实体:外部 SC 方案 IND-CCA2 挑战者、外部 SC 方案 IND-CCA2 攻击者 B_2、本方案(m,n)-IND-CCA2 挑战者、本方案(m,n)-IND-CCA2 攻击者 A.为了利用攻击者 A,B_2 将完全控制(m,n)-IND-CCA2 挑战者和 A 之间的信息通道,并利用外部 SC 方案 IND-CCA2 挑战者提供的相关信息构造攻击者 A 所需的各种参数.执行过程如下:

- B_2 把从外部 SC 方案 IND-CCA2 挑战者处获得的挑战公钥 (VEK_S^*,VEK_R^*) (对于 (VEK_S^*,VEK_R^*) 对应的私钥 B_2 一无所知),连同从本方案(m,n)-IND-CCA2 挑战者处获得的 m 个主密钥对 $(Msk_i,Mpk_i)_{i=1}^m$ 一并发送给攻击者 A.
- 攻击者 A 根据得到的主公钥对 $(Mpk_i)_{i=1}^m$ 产生一个挑战读取结构 $\mathcal{P}^*$,并提交给 B_2.
- 根据 A 给定的挑战读取结构 $\mathcal{P}^*$,B_2 按如下方式构建挑战密钥封装:
  - B_2 从会话密钥空间中随机选择 3 个密钥 k_0,k_1,k_2,并将 k_1,k_2 在挑战读取结构 $\mathcal{P}^*$ 下经过秘密共享方案计算得到 $\boldsymbol{shr}_1^*=[shr_1^*]_{j=1}^n$ 并且 $\boldsymbol{shr}_2^*=[shr_2^*]_{j=1}^n$.
  - B_2 将 $[shr_1^*]_{j=1}^n\|VEK_S^*$ 以及 $[shr_2^*]_{j=1}^n\|VEK_S^*$,在对应策略 $(Mpk_j,ID_{Pj})_{j=1}^n$ 下利用 IBE 加密算法分别加密得到 $[c_1^*]_{j=1}^n$ 与 $[c_2^*]_{j=1}^n$.B_2 定义 $m_0=\{[c_1^*]_{j=1}^n,\mathcal{P}^*\}$, $m_1=\{[c_2^*]_{j=1}^n,\mathcal{P}^*\}$,并将 m_0,m_1 作为外部 SC 方案 IND-CCA2 游戏的挑战消息发送给外部 SC 方案 IND-CCA2 挑战者.
  - 外部 SC 方案 IND-CCA2 挑战者随机选择一个比特 $\bar{b}\leftarrow_R\{0,1\}$,并计算挑战密文 $\boldsymbol{SC}(m_{\bar{b}},SDK_S^*,VEK_R^*)$,返回给 B_2.
  - B_2 随机选择一个比特 b,将 k_b 和 $c^*=\boldsymbol{SC}(m_{\bar{b}},SDK_S^*,VEK_R^*)$ 作为挑战密钥和密钥封装返回给攻击者 A.
- 对 A 的解封装询问,B_2 如下处理:如果不涉及挑战密钥封装的解密询问,B_2 将直接利用解密封装算法进行响应;如果询问关于挑战封装解密询问,那么 B_2 将立即返回停止符⊥.
- 最后,B_2 将从攻击者 A 处得到一个关于(m,n)-IND-CCA2 攻击游戏的猜测比特 b'.如果 $b=b'$,B_2 将向外部 SC 方案的 IND-CCA2 挑战者提交他的猜测比特 $\hat{b}=1$;如果 $b\neq b'$,则 $\hat{b}=0$.

观测整个执行过程可见,只要不进行非法解密询问,B_2 都将正常执行.同时,因为 $\hat{b}$ 是由 B_2 就外部 SC 方案 IND-CCA2 安全返回的猜测比特,而 $\bar{b}$ 是外部 SC 方案挑战者给出的选择比特,那么 B_2 在外部 SC 方案 IND-CCA2 安全游戏中可以获得的优势是

$$Adv_{SC}^{\text{IND-CCA2}}(B_2)=\frac{1}{2}|\Pr[\hat{b}=1|\bar{b}=1]-\Pr[\hat{b}=1|\bar{b}=0]| \quad (5)$$

我们用表 8 列出在 B_2 的选择比特 b 和外部 IBE 方案挑战者选择比特 $\bar{b}$ 不同取值的情况下,B_2 提交给攻击者 A 的密钥和挑战密钥封装的情形.

观察表8可以发现,在 $\bar{b}=0$ 的条件下,构造的挑战密钥封装的秘密分享都是来自于 k_1 的秘密分享,这种情况相当于攻击者 A 在 $Game_1$ 环境中进行猜测.如果攻击者 A 在 $Game_1$ 游戏中成功,概率即为

$$\Pr[Succ_1]=\Pr[b'=b]=\Pr[\hat{b}=1|\bar{b}=0].$$

在 $\bar{b}=1$ 的条件下,构造的挑战封装的秘密分享都是来自于 k_2 的秘密分享,这种情况相当于攻击者 A 在 $Game_2$ 环境中进行猜测.如果攻击者 A 能在 $Game_2$ 游戏中成功的概率即为 $\Pr[Succ_2]=\Pr[b'=b]=\Pr[\hat{b}=1|\bar{b}=1]$.

综合 $\Pr[Succ_2]$,$\Pr[Succ_1]$表达式可得:

$$|\Pr[Succ_2]-\Pr[Succ_1]|=|\Pr[\hat{b}=1|\bar{b}=1]|-|\Pr[\hat{b}=1|\bar{b}=0]| \quad (6)$$

结合公式(5)、公式(6)可得 $|\Pr[Succ_2]-\Pr[Succ_1]|=2Adv_{SC}^{\text{IND-CCA2}}(B_2)$.

表 8 Construction of k_b and c^*

表 8 k_b 与 c^*的构造

	b=0	b=1
$\bar{b}=0$	$k_0, \mathbf{SC}(([c_1^*]_{j=1}^n,\mathcal{P}^*),SDK_S^*,VEK_R^*)$	$k_1, \mathbf{SC}(([c_1^*]_{j=1}^n,\mathcal{P}^*),SDK_S^*,VEK_R^*)$
$\bar{b}=1$	$k_0, \mathbf{SC}(([c_2^*]_{j=1}^n,\mathcal{P}^*),SDK_S^*,VEK_R^*)$	$k_1, \mathbf{SC}(([c_2^*]_{j=1}^n,\mathcal{P}^*),SDK_S^*,VEK_R^*)$

最后观察 $Game_2$ 可见,由随机密钥 k_2 的秘密分享生成挑战密钥封装与 k_0,k_1 完全没有关联,攻击者 A 将完全没有猜测优势只能进行随机猜测,即 $\Pr[Succ_2]=\frac{1}{2}$.

综合上述 $Game_0$,…,$Game_2$ 序列游戏,由序列游戏证明定理[12]结果可得:

$$Adv_{\text{WF-SCKEM}}^{(m,n)\text{-IND-CCA2}}(A)\le Adv_{SC}^{\text{UF-CMA}}(B_1)+2Adv_{SC}^{\text{IND-CCA2}}(B_2). \quad \square$$

4 结 语

本文提出了基于签密的密码工作流密钥封装体制的定义及安全定义.结合秘密共享方案、基于身份加密方案和签密方案给出一个基于签密的密码工作流密钥封装机制的结构方案,并在标准模型下对该结构方案的安全性进行了证明.本文提出的结构方案是对 Al-Riyami 方案和 Barbosa 方案在结构上的进一步改进,新的结构方案利用签密综合了 Barbosa 方案中对公钥加密和一次性签名的分别使用,在保证同等安全性的同时简化了方案结构.签密方案的本质是在同一逻辑步骤内实现加密和签名,因此,新的结构方案必然比分别执行公钥加密算法和一次性签名算法的结构方案具有更高的执行效率,但具体的执行效率与所采用的密码组件算法相关,比如采用 Sakai-Kasahara 私钥提取结构的 IBE 方案[13],将比采用 Boneh-Franklin 结构的 IBE 方案具有更高的执行效率.在标准模型下,我们就新结构方案的接收者安全性和外部安全性进行了证明.证明结果表明,只要构成结构方案的各组成密码部件是可证明安全的,那么新的结构方案也是可证明安全的.另外,Al-Riyami 方案和 Barbosa 方案都是对 IBE 加密的会话密钥秘密分享进行直接传输,这样很容易造成在传输过程中主动攻击者对传输密文的非法篡改.而新方案在 IBE 方案对会话密钥秘密分享进行加密后,再以指定接收者的公钥和发送者私钥进行签密.这样,一方面可以保证密码工作流方案要求的免托管安全特性,防止多个 TA 串谋对明文消息进行非法解密,另一方面,也可以有效防止在密文传输过程中主动攻击者对密文的非法篡改.

References:

[1] Chen L, Harrison K, Soldera D, Smart NP. Applications of multiple trusted authorities in pairing based cryptosystems. In: Davida GI, Frankel Y, Rees O, eds. Proc. of the InfraSec 2002. LNCS 2437, Berlin, Heidelberg: Springer-Verlag, 2002. 260–275.

[2] Paterson KG. Cryptography from pairings: A snapshot of current research. Information Security Technical Report, 2002,7(3): 41−54.

[3] Al-Riyami SS, Malone-Lee J, Smart NP. Escrow-Free encryption supporting cryptographic workflow. Int'l Journal of Information Security, 2006,5(3):217−229.

[4] Cramer R, Shoup V. A practical public-key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Proc. of the Advances in Cryptology—CRYPTO'98. LNCS 1462, Berlin, Heidelberg: Springer-Verlag, 1998. 13−25.

[5] Dent AW. A designer's guide to KEMs. In: Paterson KG, ed. Proc. of the Cryptography and Coding: The 9th IMA Int'l Conf. LNCS 2898, Berlin, Heidelberg: Springer-Verlag, 2003. 133−151.

[6] Bartbosa M, Farshim P. Secure cryptographic workflow in the standard model. In: Joye M, ed. Proc. of the Progress in Cryptology —INDOCRYPT 2006. LNCS 3429, Berlin, Heidelberg: Springer-Verlag, 2006. 379−393.

[7] Boneh D, Franklin M. Identity-Based encryption from the weil pairing. SIAM Journal on Computing, 2003,32(3):586−615.

[8] Canetti R, Halevi S, Katz J. Chosen-Ciphertext security from identity-based encryption. In: Biham E, ed. Proc. of the Advances in Cryptology—EUROCRYPT 2004. LNCS 3027, Berlin, Heidelberg: Springer-Verlag, 2004. 207−222.

[9] Benaloh J, Leichter J. Generalized secret sharing and monotone functions. In: Goldwasser S, ed. Proc. of the Advances in Cryptology—CRYPTO'88. LNCS 403, Berlin, Heidelberg: Springer-Verlag, 1990. 27−35.

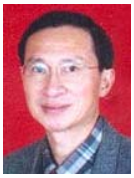
[10] Krawczyk H. Secret sharing made short. In: Stinson DR, ed. Proc. of the Advances in Cryptology—CRYPTO'93. LNCS 0773, Berlin, Heidelberg: Springer-Verlag, 1994. 136−146.

[11] Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption. Journal of Cryptology, 2007,20(2):203−235.

[12] Shoup V. Sequences of games: A tool for taming complexity in security proofs. Cryptology ePrint Report, 2004/332, 2004. http://eprint.iacr.org/2004/332

[13] Chen L, Cheng Z. Security proof of Sakai-Kasahara's identity-based encryption scheme. In: Smart NP, ed. Proc. of the Cryptography and Coding: The 10th IMA Int'l Conf. LNCS 3706, Berlin, Heidelerg: Springer-Verlag, 2005. 442−459.

赖欣(1977－),女,四川德阳人,博士生,主要研究领域为密码学,信息安全.



何大可(1944－),男,教授,博士生导师,主要研究领域为密码学,信息安全.