DOI:10.13718/j.cnki.xsxb.2019.01.014

一个 CCA 安全的基于身份的门限加密方案①

董梦景, 包小敏

西南大学 数学与统计学院,重庆 400715

摘要:提出一个非交互的基于身份的门限加密方案,该方案在随机预言器模型下可证明是 CCA 安全的. 首先利用一个简单的提高安全性的方法,得到一个将一般的基于身份加密方案的安全性从 CPA 提高至 CCA 的通用方法,接着运用该转化方法,构造了一个 CCA 安全的基于身份的门限加密方案实例且密文的传输效率较之前的方法有大幅提高.

关 键 词:基于身份加密;门限方案;BDH 假设;选择密文攻击安全

中图分类号:TN918.6 **文献标志码**:A **文章编号**:1000-5471(2019)01-0084-05

在已有文献中门限方案大都是 CPA 安全的[1-3],而真正达到 CCA 安全的门限方案很少. 文献[4]中分析了门限方案很难达到 CCA 安全的原因,也就是在门限方案中每一次部分解密之前先要进行密文份额有效性检验,而检验需要用到整体私钥,但是门限方案中每个解密服务器不可能拥有私钥(它们有的只是部分私钥),因此我们希望解密过程中的有效性可以公开检验,使得每个解密服务器都可以独立进行检验. 虽然文献[5]中的门限方案做到了这一点,但解密并不高效. 本文构造了一个既能达到 CCA 安全,又能公开验证密文有效性的高效的基于身份的非交互门限加密方案(TIBE).

1 预备知识

1.1 安全性概念

为了清楚地描述加密方案的安全性概念,密码学中经常会提到一个交互游戏. 游戏有两个参与者,一个称为挑战者,另一个是攻击者. 挑战者作为加密方案的所有者建立系统,攻击者对系统发起挑战,挑战者接受攻击者的挑战.

一个公钥密码方案的安全性概念可以由弱到强分为选择明文攻击安全(简称 CPA 安全),非适应性选择密文攻击安全(简称 CCA1)以及适应性选择密文攻击安全(简称 CCA2)3 个级别. 若非特别说明,下文中提到 CCA 安全均指 CCA2 安全.

1.2 基于身份的公钥密码体制及其安全性

下面介绍基于身份的公钥密码体制的形式化定义及其安全模型. 基于身份的加密方案的安全性定义最早由文献[6]提出,我们这里采用文献[7]中更为简洁的定义.

1.2.1 基于身份的加密方案的形式化定义

一个基于身份的加密方案 $IBE=(Setup, KeyD, Enc, Dec)$ 由 4 个多项式时间算法构成.

① 收稿日期:2018-09-07

作者简介:董梦景(1995-),女,硕士研究生,主要从事编码理论和密码学的研究.

通信作者:包小敏,博士,教授.

$Setup(k)$ 算法中可信机构 PKG 输入安全参数 k，输出一个二元组 (PK, msk). 其中 PK 是主公钥，msk 是主私钥. PKG 公开 PK，保密 msk. 记为 $(PK, msk) \leftarrow Setup(1^k)$.

$KeyD(ID, msk)$ 算法中 PKG 收到用户 ID 后，为 ID 分发私钥 SK_{ID}，记为 $SK_{ID} \leftarrow KeyD_{msk}(ID)$.

$Enc(PK, ID, M)$ 算法中信息发送方用 ID 加密信息 M，输出密文 C，记为 $C \leftarrow Enc_{PK}(ID, M)$.

$Dec(ID, SK_{ID}, C)$ 算法中拥有身份 ID 的用户用私钥 SK_{ID} 解密，记为 $M \leftarrow Dec_{SK_{ID}}(ID, C)$.

1.2.2　基于身份的加密方案的安全性

IBE 的选择身份安全性定义可以通过以下挑战者 $\mathscr{C}$ 和攻击者 $\mathscr{A}$ 之间的游戏来描述，对于该安全性的定义具体可见文献[6－8]. 攻击者 $\mathscr{A}$ 在选择身份 CPA 安全游戏中的成功优势[6] 定义为 $Adv_{\mathscr{A},IBE}^{IND\text{-}ID\text{-}CPA}(k) = \left| Pr_{\mathscr{A}}^{IBE}[b = b'] - \frac{1}{2} \right|$.

如果对任何多项式时间的攻击者 $\mathscr{A}$，存在一个可忽略的函数 $negl(k)$，使得 $Adv_{\mathscr{A},IBE}^{IND\text{-}ID\text{-}CPA}(k) \leqslant negl(k)$，那么就称这个基于身份的加密方案在选择身份攻击下具有不可区分性，或者称为选择身份 CPA 安全. 基于身份的加密方案的 CCA 安全定义与 CPA 安全定义最大的不同是攻击者除了可以询问私钥，还能对除了挑战密文之外的密文做解密询问.

1.3　基于身份的门限密码体制及其安全性

接下来简单介绍基于身份的门限密码(简记为 TIBE) 的形式化定义及其安全模型.

1.3.1　基于身份的门限加密方案的形式化定义

一个基于身份的门限加密方案包括以下 7 个算法：

$Setup(n, t, k)$ 算法中输入解密服务器个数 n，门限值 t，安全参数 k，输出一个三元组 $(PK, VK, \boldsymbol{K}_{msk})$，其中 PK 是系统参数，VK 是验证密钥. $\boldsymbol{K}_{msk} = (msk_1, msk_2, \cdots, msk_n)$ 是 n 个主密钥份额组成的向量，解密服务器 i 拥有 (i, msk_i) 用于获得私钥份额.

$ShareKeyGen(PK, i, msk_i, ID)$ 算法中输入系统参数 PK，身份 ID 以及主密钥份额 (i, msk_i)，输出 ID 的第 i 个解密私钥份额 $dk_i = (i, \hat{dk}_i)$.

$ShareVerify(PK, VK, ID, dk_i)$ 算法中验证 dk_i 是否是身份 ID 的有效解密份额，输出“Valid”或者“Invalid”.

$Combine(PK, VK, ID, \{dk_1, dk_2, \cdots, dk_t\})$ 输出身份 ID 对应的私钥 SK_{ID} 或者“$\perp$”.

$Encrypt(PK, ID, M)$ 算法中输入系统参数 PK，身份 ID 和信息 M，输出密文 C.

$ValidateCT(PK, ID, C)$ 算法验证 C 是否为有效密文，输出“Valid”或者“Invalid”.

$Decrypt(PK, ID, SK_{ID}, C)$ 算法解密输出明文 M 或者“$\perp$”.

1.3.2　基于身份的门限加密方案的安全性

TIBE 的安全性需要考虑选择身份攻击 CPA 安全以及密钥生成一致性两方面. 可以用两个游戏来描述：选择身份攻击 CPA 安全游戏和密钥生成一致性游戏[5].

在选择身份攻击 CPA 安全游戏中攻击者的优势定义为 $Adv_{\mathscr{A},TIBE}^{IND\text{-}ID\text{-}CPA}(k) = \left| Pr[b = b'] - \frac{1}{2} \right|$；密钥生成一致性游戏中攻击者的优势定义为 $Adv_{\mathscr{A},TIBE}^{CD\text{-}ID}(k) = Pr[\text{攻击者获胜}]$.

如果对任何多项式时间的攻击者 $\mathscr{A}$ 以及任意的 n 和 $t(0 < t \leqslant n)$，存在可忽略的函数 $negl(k)$，使得 $Adv_{\mathscr{A},TIBE}^{IND\text{-}ID\text{-}CPA}(k) \leqslant negl(k)$ 和 $Adv_{\mathscr{A},TIBE}^{CD\text{-}ID}(k) \leqslant negl(k)$ 都成立，那么就说 TIBE 方案是选择身份攻击 CPA 安全的.

2　CCA 安全的 IBE

2.1　CPA 转 CCA 的简单方法

目前 CCA2 被认为是公钥加密方案的安全性概念中最强的，为了实现加密方案的 CCA 安全，文献[9]

提出一个将CPA安全的加密方案转化成CCA安全的加密方案的简单方法，转化方法如下：

设$\prod:=(\mathcal{K},\mathcal{E},\mathcal{D})$是一个CPA安全的加密方案，$H:\{0,1\}^k\longrightarrow\{0,1\}^l$是一个Hash函数.

1) $\overline{\mathcal{K}}(1^k):=\mathcal{K}(1^k)$

2) $\overline{\mathcal{E}}_{\mathrm{pk}}^H:\{0,1\}^{k-k_0}\times\{0,1\}^{k_0}\longrightarrow\{0,1\}^*$，定义为：$\overline{\mathcal{E}}_{\mathrm{pk}}^H(x,r):=\mathcal{E}_{\mathrm{pk}}((x\|r),H(x\|r))$，其中$x\in\{0,1\}^{k-k_0}$且$r\in\{0,1\}^{k_0}$.

3) $\overline{\mathcal{D}}_{\mathrm{sk}}^H(y):\{0,1\}^*\longrightarrow\{0,1\}^{k-k_0}\cup\{\mathrm{null}\}$定义如下

$$\overline{\mathcal{D}}_{\mathrm{sk}}^H(y):=\begin{cases}[\mathcal{D}_{\mathrm{sk}}(y)]^{k-k_0}, & \text{如果 } *\\ \mathrm{null}, & \text{否则}\end{cases}$$

其中：$[\mathcal{D}_{\mathrm{sk}}(y)]^{k-k_0}$指的是$\mathcal{D}_{\mathrm{sk}}(y)$的前$(k-k_0)$比特，“$*$”指存在$\mathcal{D}_{\mathrm{sk}}(y)$使得$y=\mathcal{E}_{\mathrm{pk}}(\mathcal{D}_{\mathrm{sk}}(y),H(\mathcal{D}_{\mathrm{sk}}(y)))$. 文献[9]证明了通过这样的转化，CPA安全的解密方案确实能达到CCA安全，得到了如下的CCA安全转化定理.

定理1 假设$\prod=(\mathcal{K},\mathcal{E},\mathcal{D})$是一个CPA安全的加密方案，则$\overline{\prod}=(\overline{\mathcal{K}},\overline{\mathcal{E}},\overline{\mathcal{D}})$是随机预言器模型下CCA2安全的加密方案.

2.2 构造CCA安全的IBE

下面将上述转化方法应用到一个选择身份攻击CPA安全的IBE中得到一个随机预言器模型下CCA安全的IBE.

假设$\prod=(Setup,KeyD,\mathcal{E},\mathcal{D})$是一个选择身份CPA安全的*IBE*方案，$H:\{0,1\}^{k+k_0}\longrightarrow\{0,1\}^l$是一个安全Hash函数，下面构造$\prod'=(Setup,KeyD,Enc,Dec)$.

$Setup(k)$算法中可信机构PKG输入安全参数k，输出一个二元组(PK,msk)，其中PK是主公钥，msk是主私钥. PKG公开PK，保密msk，记为$(PK,msk)\leftarrow Setup(1^k)$.

$KeyD(ID,msk)$算法中PKG在收到身份ID后，为身份ID分发私钥SK_{ID}，记为$SK_{\mathrm{ID}}\leftarrow KeyD_{\mathrm{msk}}(ID)$.

$Enc(PK,ID,M)$算法中对于信息$m\in\{0,1\}^k$，随机选择$r\in\{0,1\}^{k_0}$，同样用主公钥和身份ID加密，记为$C\leftarrow\overline{\mathcal{E}}_{\mathrm{PK,ID}}^H(m,r)=\mathcal{E}_{\mathrm{PK,ID}}((m\|r),H(m\|r))=(y_1,y_2)$.

$Dec(ID,SK_{\mathrm{ID}},C)$算法中拥有身份$ID$的用户先检查密文是否有效. 若有效，用私钥$SK_{\mathrm{ID}}$解密，记为$m\leftarrow\overline{\mathcal{D}}_{SK_{\mathrm{ID}}}^H(ID,C)=[D_{SK_{\mathrm{ID}}}(ID,C)]^k$，其中$[D_{SK_{\mathrm{ID}}}(ID,C)]^k$表示$D_{SK_{\mathrm{ID}}}(ID,C)$的前$k$个比特. 否则，拒绝解密，并输出“null”.

定理1保证了$\prod'$是一个CCA安全的IBE.

3 CCA安全的TIBE

下面构造一个CCA安全的TIBE方案实例.

3.1 方案描述

设BDH假设成立，$H:\{0,1\}^k\longrightarrow\mathbb{Z}_p$是一个安全的Hash函数，再假设$e:\mathbb{G}\times\mathbb{G}\rightarrow\mathbb{G}_1$是一个双线性映射[10]，其中群$\mathbb{G}_1$中元素的二进制长度不超过$k$.

$Setup(n,t,k)$算法设$\mathbb{G}$是p阶群，在$\mathbb{G}$中随机选择生成元g,g_2,h_1以及一个$t-1$次随机多项式$f\in\mathbb{Z}_p[X]$. 令$\alpha=f(0)$，$g_1=g^\alpha$，$msk_i=g_2^{f(i)}$. 服务器i的主密钥份额为(i,msk_i). 设置系统参数$PK=(\mathbb{G},g,g_1,g_2,h_1)$，主密钥份额集$\boldsymbol{K}_{\mathrm{msk}}=(msk_1,\cdots,msk_n)$，公开的验证密钥为$VK=(g^{f(1)},\cdots,g^{f(n)})=(u_1,\cdots,u_n)$.

$ShareKeyGen(PK,i,msk_i,ID)$算法随机选$r\in\mathbb{Z}_p$，计算$w_{i,0}=msk_i\cdot(g_1^{\mathrm{ID}}h_1)^r$，$w_{i,1}=g^r$，然后输出身份ID的第$i$个会话私钥份额$dk_i=(i,(w_{i,0},w_{i,1}))$.

ShareVerify(PK, VK, ID, dk_i)算法中为了验证 dk_i 是身份 ID 的有效会话私钥份额，判断 $e(u_i, g_2) \cdot e(g_1^{\mathrm{ID}} h_1, w_{i,1}) = e(g, w_{i,0})$ 是否成立，若成立，输出“Valid”；否则，输出“Invalid”.

Combine(PK, VK, ID, $\{dk_1, dk_2, \cdots, dk_t\}$)算法中如果上一步验证未通过，输出“$\perp$”并退出，否则选择 $\lambda_1, \cdots, \lambda_t \in \mathbb{Z}_p$，使得 $\alpha = f(0) = \sum_{i=1}^{t} \lambda_i f(i)$，然后计算 $w_0 = \prod_{i=1}^{t} w_{i,0}^{\lambda_i}$，$w_1 = \prod_{i=1}^{t} w_{i,1}^{\lambda_i}$，输出身份 ID 对应的会话私钥 $d_{ID} = (w_0, w_1)$.

Encrypt(PK, ID, M) 算法中为了加密 $M \in \{0,1\}^{k-k_0}$，进行以下两步

(a) 随机选 $v \in \{0,1\}^{k_0}$，令 $s = H(M \| v)$；

(b) 计算并输出密文 $C = (y_1, y_2, y_3) = (e(g_1, g_2)^s \oplus (M \| v), g^s, g_1^{s \cdot \mathrm{ID}} h_1^s)$.

ValidateCT(PK, ID, C) 算法中为了验证 $C = (y_1, y_2, y_3)$ 是否为有效密文，判断 $e(y_2, g_1^{\mathrm{ID}} h_1) = e(y_3, g)$ 是否成立，若成立，输出“Valid”；否则，输出“Invalid”.

Decrypt(PK, ID, d_{ID}, C)算法中如果密钥有效性或者密文有效性检验有一个通不过，那么拒绝解密；否则，输出明文 $M' = \left[y_1 \oplus \frac{e(y_2, w_0)}{e(y_3, w_1)} \right]^{k-k_0}$.

3.2　方案的正确性与安全性

如果 $C = (y_1, y_2, y_3)$ 是 ID 加密的有效密文，并且 d_{ID} 是 ID 的有效会话私钥，那么解密一定是正确的，因为 $(w_0, w_1) = (g_2^{\alpha} (g_1^{\mathrm{ID}} h_1)^{\bar{r}}, g^{\bar{r}})$，其中 $\bar{r} = r(\lambda_1 + \cdots + \lambda_t)$. 进一步，利用双线性性质就有

$$\left[y_1 \oplus \frac{e(y_2, w_0)}{e(y_3, w_1)} \right]^{k-k_0} = \left[(M \| v) \oplus e(g_1, g_2)^s \oplus \frac{e(g, g_2^{\alpha})^s \cdot e(g, g_1^{\mathrm{ID}})^{s\bar{r}} \cdot e(g, h_1)^{s\bar{r}}}{e(g_1^{\mathrm{ID}}, g)^{s\bar{r}} \cdot e(h_1, g)^{s\bar{r}}} \right]^{k-k_0} =$$

$$[(M \| v) \oplus e(g_1, g_2)^s \oplus e(g, g_2^{\alpha})^s]^{k-k_0} = [(M \| v)]^{k-k_0} = M$$

假设 BDH 问题是难解的，本文构造中所使用的文献[5]中的基于身份的门限方案已经被证明了是选择身份 CPA 安全的，按照文献[9]中的方法转化得到我们构造的基于身份的门限方案，于是结合定理 1 不难得到下面的定理.

定理 2　假设 BDH 问题是难解的，那么上述构造得到的 TIBE 是 CCA 安全的.

4　总　　结

本文利用文献[9]中提高安全性的方法，提出一个既能达到 CCA 安全，解密私钥份额的有效性又能公开验证的基于身份的门限加密方案(TIBE)，比文献[5,7]中提高安全性的方法更加高效. 因为已有文献中 CPA 安全到 CCA 安全的转化需要在加密时额外加入一个一次签名，导致传输密文长度增大(密文多了验证密钥和签名两部分). 在传输效率上本文的构造比之前的方法至少提高了两倍.

参考文献：

[1] SHAMIR A. How to Share a Secret [J]. Communication of the ACM, 1979, 22(11): 612－613.

[2] DESMEDT Y. Society and Group Oriented Cryptography: a New Concept [J]. Cryptography, 1987, 20(5): 739－760.

[3] DESMEDT Y, FRANKEL Y. Threshold cryptosystems [C]//On Advances in Cryptology. New York: Springer-Verlag, 1989.

[4] SHOUP V, GENNARO R. Securing Threshold Cryptosystems Against Chosen Ciphertext Attack [C] //International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1998.

[5] BONEH D, BOYEN X, HALEVI S. Chosen Ciphertext Secure Public Key Threshold Encryption without Random Oracles [C]//Cryptographers Track at the RSA Conference on Topics in Cryptology. New York: Springer-Verlag, 2006: 226－243.

[6] BONEH D, FRANKLIN M. Identity Based Encryption from the Weil Pairing [J]. IEEE Trans on Wireless Commun, 2003, 32(3): 213－229.

[7] BONEH D, CANETTI R, HALEVI S, et al. Chosen-Ciphertext Security from Identity-Based Encryption [C]//Proceedings of Eurocrypt 2004. New York: Springer-Verlag, 2004: 207－222.

[8] BONEH D, BOYEN X. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles [J]. Proceedings of Eurocrypt, 2004, 2004(4): 172.

[9] FUJISAKI E, OKAMOTO T. How to Enhance the Security of Public-Key Encryption at Minimum Cost [C]//International Workshop on Public Key Cryptography. Berlin: Springer, 1999: 53－68.

[10] 李帅丽，郑 严，包小敏. 基于双线性对与身份的数字签名方案研究 [J]. 西南大学学报(自然科学版)，2009，31(5)：71－74.

A CCA-Secure Identity-Based Threshold Encryption

DONG Meng-jing[1], BAO Xiao-min[2]

School of Mathematics and Statistics, Southwest University, Chongqing 400715, China

Abstract: In this paper, a non-interactive threshold encryption scheme has been presented based on identity in order to prove the scheme of CCA-secure in the random oracle model. First, a simple conversion has been used to get a general method which improves the security of an identity-based encryption from CPA to CCA, then in the method, a CCA-secure identity-based threshold encryption scheme has been constructed. In the existing literature, there are few CCA-secure threshold schemes, in order to improve the security from CPA to CCA, some approaches existing need to add an one-time signature additionally for each encryption and the length of transmitting ciphertext will be increased (ciphertext has two more parts: verification key and signature). However, in the construction of this paper, the transmission efficiency is at least twice than that of previous methods.

Key words: identity-based encryption; threshold scheme; BDH assumption; secure against chosen ciphertext attack

责任编辑 张 枸