软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(10):2795−2804 [doi: 10.3724/SP.J.1001.2012.04183]

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

密文策略的属性基并行密钥隔离加密*

陈剑洪[1,2,3+], 陈克非[1,3], 龙 宇[1], 万中美[4], 于 坤[2], 孙成富[2], 陈礼青[2]

[1](上海交通大学 计算机科学与工程系,上海 200240)

[2](淮阴工学院 计算机工程学院,江苏 淮安 223003)

[3](上海市可扩展计算与系统重点实验室(上海交通大学),上海 200240)

[4](河海大学 理学院,江苏 南京 210098)

Ciphertext Policy Attribute-Based Parallel Key-Insulated Encryption

CHEN Jian-Hong[1,2,3+], CHEN Ke-Fei[1,3], LONG Yu[1], WAN Zhong-Mei[4], Yu Kun[2], SUN Cheng-Fu[2], CHEN Li-Qing[2]

[1](Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200240, China)

[2](School of Computer Engineering, Huaiyin Institute of Technology, Huaian 223003, China)

[3](Shanghai Key Laboratory of Scalable Computing and Systems (Shanghai Jiaotong University), Shanghai 200240, China)

[4](College of Science, Hohai University, Nanjing 210098, China)

+ Corresponding author: E-mail: jianhong_chen_cis@163.com, http://www.sjtu.edu.cn

Chen JH, Chen KF, Long Y, Wan ZM, Yu K, Sun CF, Chen LQ. Ciphertext policy attribute-based parallel key-insulated encryption. *Journal of Software*, 2012,23(10):2795−2804 (in Chinese). http://www.jos.org.cn/1000-9825/4183.htm

Abstract: The key-exposure problem has perhaps been the most devastating attack on a cryptosystem. Conventional public key cryptosystems can revoke public keys in the case of key-exposure. However, the public key for an attribute- based scheme represents an attribute set should not be changed. Key-Insulation is a crucial technique for protecting private keys. To deal with the key-exposure problems in an attribute-based cryptosystem, this paper extends the parallel key-insulated mechanism to ciphertext policy attribute-based encryption scenarios and introduces the primitive of ciphertext policy attribute-based parallel key-insulated encryption (CPABPKIE). After formalizing the definition and security notions for CPABPKIE, a concrete CPABPKIE scheme is presented. The security the proposed CPABPKIE scheme can be proved in the selective-ID model. The new primitive does not increase the risk of helper key-exposure, and allows frequent key updating.

Key words: ciphertext policy; attribute-based; encryption; parallel key-insulated

摘 要: 对于公钥密码体制来说,私钥泄漏是一种十分严重的威胁.传统密码系统可以通过撤销公钥来应对私钥泄漏,但在属性基密码系统里,公钥由属性集合表示,对这些属性集合的撤销不太可行.目前,密钥隔离机制是减轻密钥泄漏所带来危害的一种有效方法.为了处理属性基密码系统中的密钥泄露问题,将并行密钥隔离机制引入到密文

* 基金项目: 国家自然科学基金(60970111, 61133014, 60903189, 60903020, 61103183); 淮安市科技支撑计划(工业)(HAG2011044, HAG2011045)

收稿时间: 2011-05-10; 修改时间: 2011-09-02; 定稿时间: 2012-01-16

策略的属性基加密中,提出了密文策略的属性基并行密钥隔离加密(ciphertext policy attribute-based parallel key-insulated encryption,简称 CPABPKIE)的概念.在给出 CPABPKIE 的形式化定义和安全模型的基础上,构建了一个不需要随机预言机模型的选择ID安全的CPABPKIE方案.所提方案允许较频繁的临时私钥更新,同时可以使协助器密钥泄漏的几率保持较低,因此增强了系统防御密钥泄漏的能力.

关键词: 密文策略;属性基;加密;并行密钥隔离

中图法分类号: TP309 **文献标识码**: A

随着计算机和网络通信技术的发展,公钥密码学得到了广泛的应用.然而,由于病毒、木马或操作系统漏洞等引起的密钥泄漏也变得越来越广泛.为了处理公钥密码系统中的密钥泄露问题,Dodis 等人[1]提出了密钥隔离机制.密钥隔离机制可以被看作是前向安全机制的补充,它既保证前向安全,又保证后向安全.其中心思想是:用户私钥被分为两部分,即放在用户设备中的临时私钥和放在协助器中的协助器密钥;用户设备的计算能力强但安全性差,而协助器的计算能力弱但物理安全性强;通过用户设备与协助器的交互来定期更新临时私钥;在整个系统生命周期内,对于一个具有 N 个时间片段的密钥隔离密码方案,用户的公钥保持不变.如果最多有 N–1 个时间片段发生密钥泄漏,并且剩余的时间片段仍是安全的,那么称该方案是(N–1,N)密钥隔离的.针对多个协助器,Hanaoka 等人[2]提出了并行密钥隔离机制.在 Asiacrypt 2005 会议上,Hanaoka 等人[3]最先将密钥隔离机制引入到身份基加密系统中.随后,Weng 等人[4]在 Indocrypt 2006 会议上提出了标准模型下安全的身份基并行密钥隔离加密方案.在 PKC 2007 会议上,Libert 等人[5]又提出了基于 PKI(公钥基础设施)的标准模型下安全的并行密钥隔离加密方案.

属性基公钥密码学的概念是由 Sahai 和 Waters[6]在 Eurocrypt 2005 首次提出来的.Sahai 和 Waters 首先提出了一个属性基加密的雏形,即门限结构的属性基加密(TABE).在该方案里,每个用户的私钥与一个属性集合相对应.加密算法输入为一个属性集合和消息,即生成的密文与一个属性集合相对应.当用户私钥的属性集合与密文的属性集合中相交的个数大于某一个系统预设的门限值时可以对密文解密.在 CCS 2006 上,Goyal 等人[7]提出了密钥策略的属性基加密(KPABE)体制.在该方案里,密钥对应于一个访问结构而密文对应于一个属性集合,当属性集合中的属性能够满足该访问结构时可以对密文解密.在 SP 2007 会议上,Bethencourt 等人[8]提出了密文策略的属性基加密(CPABE)体制.由于 Bethencourt 等人方案的证明不能规约到一个广为人知的复杂性假设,Cheung 和 Newport[9]在 CCS 2007 会议上又提出一个新的 CPABE 方案.在该 CPABE 方案里,密文对应于一个访问结构而密钥对应于一个属性集合,当属性集合中的属性能够满足该访问结构时可以对密文解密.与 KPABE 相比,CPABE 更符合实际.这是因为,在 CPABE 系统中,每个用户可以根据自己的属性集合从可信中心(authority)得到密钥,接着可由加密者对明文进行访问控制(控制规则可用与门等实现).为了解决 CPABE 系统中的密钥泄露问题,本文提出了密文策略的属性基并行密钥隔离加密(ciphertext policy attribute-based parallel key-insulated encryption,简称 CPABPKIE)的概念.在给出 CPABPKIE 的形式化定义和安全模型的基础上,构建了一个不需要随机预言机模型的选择 ID 安全的 CPABPKIE 方案.所提方案允许较频繁的临时私钥更新,同时可以使协助器密钥泄漏的几率保持较低,因此增强了系统防御密钥泄漏的能力.

1 预备知识

在本文中,用 $\mathbb{Z}_p$ 表示集合(0,1,2,…,p–1),用 $\mathbb{Z}_p^*$ 表示 $\mathbb{Z}_p\backslash\{0\}$,用 $a\in_R S$ 表示均匀随机地在集合 S 中选取元素 a.

1.1 双线性映射

设 G_1 和 G_2 均为 p 阶循环乘法群.双线性映射是指满足下列性质的一个映射:

(1) 双线性:对于所有的 $g_1,g_2\in G_1$,对于所有的 $a,b\in \mathbb{Z}_p^*$,均有 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$ 成立;

(2) 非退化性:存在 $g_1,g_2\in G_1$,满足 $e(g_1,g_2)\neq 1$;

(3) 可计算性:对于所有的 $g_1,g_2\in G_1$,存在一个有效的算法计算 $e(g_1,g_2)$.

1.2 DBDH假设

定义 1(判定双线性 Diffie-Hellman 问题(DBDH 问题)). 给定$(g,g^a,g^b,g^c)\in G_1^4$, 判断 $e(g,g)^z=e(g,g)^{abc}$ 是否成立.这里,$a,b,c,z\in\mathbb{Z}_p$ 是未知的.

一个多项式时间敌手$\mathcal{B}$的针对群(G_1,G_2)上的 DBDH 问题的优势定义为

$$Adv^{\mathrm{DBDH}}_{(G_1,G_2),\mathcal{A}}=|\Pr[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^{abc})=1]-\Pr[\mathcal{A}(g,g^a,g^b,g^c,e(g,g)^z)=1]|.$$

这个概率取决于 a,b,c,z 的随机选择和$\mathcal{B}$的输出.

定义 2(DBDH 假设). 若任意多项式 t 时间敌手$\mathcal{B}$针对群(G_1,G_2)上的 DBDH 困难问题的优势 $Adv^{\mathrm{DBDH}}_{(G_1,G_2),\mathcal{A}}$ 均小于ϵ,则称群(G_1,G_2)上的(t,ϵ)-DBDH 假设成立.

2 CPABPKIE 的形式化定义及其安全模型

2.1 语法定义

设给定一个属性集合 S,与属性相关联的访问结构[9]是一个输出 0 或 1 的规则 W.S 满足 W(记作 $S\vDash W$)当且仅当对于 S,W 回答为 1.访问结构可以是布尔表达式、门限树等.一个 CPABPKIE 方案由以下 6 种算法构成:

① *Setup*(κ):给定安全参数κ,可信中心运行这个系统创建算法,生成主密钥 *msk* 和系统公共参数 *cp*;

② *KeyGen*(*msk*,*cp*,S):给定系统主密钥 *msk*、系统公共参数 *cp* 以及表示用户身份的属性集合 $S\subseteq\mathcal{N}$($\mathcal{N}$为全体属性的集合),可信中心运行这个私钥提取算法来生成与 S 相关的初始私钥 $TK_{S,0}$ 和两个协助器密钥 $(HK_{S,1},HK_{S,0})$;

③ *HelperUpt*(*cp*,t,S,$HK_{S,t}$):给定系统公共参数 *cp*、时间片段参数 t、用来表示用户身份的属性集合 S 以及第 t 个协助器密钥 $HK_{S,t}$(这里,$t=t \bmod 2$),这种协助器密钥更新算法为拥有属性集合 S 的用户生成用于时间片段 t 的更新信息 $\mathrm{UI}_{S,t}$;

④ *UserUpt*(*cp*,S,$TK_{S,t-1}$,t,$UI_{S,t}$):给定系统公共参数 *cp*、用户属性集合 S、用户在时间片段 $t-1$ 时的临时私钥 $TK_{S,t-1}$、下一时间片段参数 t 以及对应的更新信息 $UI_{S,t}$,用户使用这种用户私钥更新算法来产生时间片段 t 的临时私钥 $TK_{S,t}$,并将 $TK_{S,t-1}$ 和 $UI_{S,t}$ 删除;

⑤ *Encryption*(*cp*,t,W,M):用户运行这种加密算法,用访问结构 W、时间片段 t 和公共参数 PK 对明文 M 进行加密.这种算法输出一个密文(t,E),使得由时间段参数 t 和属性集合 S 生成的临时私钥可以用来解密(t,E)当且仅当 $S\vDash W$;

⑥ *Decryption*(*cp*,(t,E),S,$UI_{S,t}$):这种解密算法首先检查 $TK_{S,t}$ 中的属性集合 S 是否满足 E 中的访问结构:若是,则输出明文空间中的明文 M;否则,输出“reject”.

2.2 安全概念

为方便起见,将一个满足挑战访问结构 W^*的属性集合定义为受限属性集合.

2.2.1 密钥隔离安全性

在这种情况下,我们考虑敌手会获得某些临时私钥(即与属性集合相关的临时私钥会发生泄漏).另外,敌手可以获得任意非受限属性集合 S 的全部协助器密钥,甚至可以获得受限属性集合 S^*的部分(非全部)协助器密钥.具体地说,在密钥隔离意义下,如果没有任何多项式有界的敌手以一个不可忽略的优势赢得以下游戏,则称一个 CPABPKIE 方案在适应性选择明文攻击下具有不可区分性(IND-CPABPKIE-PKI-CPA):

Init:敌手宣布挑战访问结构 W^*和挑战时间片段参数 t^*;

Setup:挑战者运行 Setup 算法,同时告诉敌手公开参数;

Phase 1:敌手$\mathcal{A}$发出一系列适应性的查询,查询类型的定义如下所示:

- 私钥生成查询$\langle S\rangle$:挑战者运行 *KeyGen* 算法得到与属性集合 S 对应的初始私钥 $TK_{S,0}$ 和协助器密钥 $(TK_{S,0},TK_{S,1})$,然后把这些结果发送给敌手;

- 协助器密钥查询$\langle S,\eta\rangle$:挑战者运行 *KeyGen* 算法生成 $HK_{S,\eta}$,然后把 $HK_{S,\eta}$发送给敌手;
- 临时私钥查询$\langle S,t\rangle$:挑战者运行 *UserUpt* 算法得到与属性集合 S 和时间片段 t 对应的临时私钥 $TK_{S,t}$,然后把 $TK_{S,t}$ 发送给敌手;

Challenge:敌手输出两个长度相等的明文 M_0,M_1,挑战者抛取一个随机选择$\mu\in\{0,1\}$,并用 W^*和 t^*对 M_μ加密,密文被发送给敌手;

Phase 2:重复 Phase 1;

Guess:最后,$\mathcal{A}$输出一个值ν'作为对ν的猜测.

将上述游戏称为 IND-CPABPKIE-PKI-CPA 游戏.游戏还要求敌手必须满足以下条件:

1) 敌手$\mathcal{A}$不允许对任何受限属性集合进行私钥生成查询;
2) 敌手$\mathcal{A}$不允许对任何受限属性集合和挑战时间片断参数 t^*进行临时私钥查询;
3) 敌手$\mathcal{A}$不能同时进行临时私钥查询$\langle S^*,t^*-1\rangle$和协助器密钥查询$\langle S^*,t^* \bmod 2\rangle$;
4) 敌手$\mathcal{A}$不能同时进行临时私钥查询$\langle S^*,t^*+1\rangle$和协助器密钥查询$\langle S^*,(t^*+1) \bmod 2\rangle$;
5) 敌手$\mathcal{A}$不能同时进行协助器查询$\langle S,0\rangle$和协助器查询$\langle S,1\rangle$.

2.2.2 强密钥隔离安全性

在这种情况下,我们考虑敌手会获得全部协助器密钥(即协助器会发生密钥泄漏).我们允许敌手获得任意属性集合(包括受限属性集 S^*)的全部协助器密钥,同时不允许敌手通过临时私钥查询来获得受限属性集合 S^*的任何临时私钥.敌手可以通过临时私钥查询来获得非受限属性集合 S 的任意临时私钥(由于该类查询可以隐含于私钥提取查询中,因此我们在下面的游戏中不显式地为敌手提供该类查询).具体地说,在强密钥隔离意义下,如果没有任何多项式有界的敌手以一个不可忽略的优势赢得以下游戏,则称一个 CPABPKIE 方案在适应性选择明文攻击下具有不可区分性(IND-CPABPKIE-sPKI-CPA):

Init:同 IND-CPABPKIE-PKI-CPA 游戏;

Setup:同 IND-CPABPKIE-PKI-CPA 游戏;

Phase 1:敌手$\mathcal{A}$发出一系列适应性的查询,查询类型的定义如下所示:

- 私钥生成查询$\langle S\rangle$:同 IND-CPABPKIE-PKI-CPA 游戏;
- 协助器密钥查询$\langle S,\eta\rangle$:同 IND-CPABPKIE-PKI-CPA 游戏;

Challenge:同 IND-CPABPKIE-PKI-CPA 游戏;

Phase 2:重复 Phase 1;

Guess:同 IND-CPABPKIE-PKI-CPA 游戏.

将上述游戏称为 IND-CPABPKIE-sPKI-CPA 游戏.游戏还要求敌手必须满足以下条件:敌手$\mathcal{A}$不允许对任何受限属性集合进行私钥生成查询.

3 CPABPKIE 方案设计

基于 Cheung 和 Newport[9]的 CPABE 方案,本节将给出一个具体的 CPABPKIE 方案.

3.1 方案描述

对于整数 $i\in\mathbb{Z}_p$ 和一个由$\mathbb{Z}_p$ 中的元素组成的集合 S,定义拉格郎日系数为 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$.为方便起见,与文献[9]一样,定义全体属性集为$\mathcal{N}=\{1,\ldots,n\}$,其中,$n$ 为某个自然数.将属性 i 和它的否$\neg i$ 称作属性字.设访问结构是一个输入为属性字的与门,记作 $W=\wedge_{i\in I}\underline{i}$,其中,$I\subseteq\mathcal{N}$,且每个 $\underline{i}$ 都是属性字(即,i 或$\neg i$).

Setup:给定安全参数κ,可信中心执行如下操作:

1) 选取两个阶均为素数 p(由安全系数κ决定)的乘法群 G_1 和 G_2,设 g 为群 G_1 的一个随机生成元,又设 e 为双线性映射 $e:G_1\times G_1\to G_2$;

2) 随机选取 $y,t_1,\ldots,t_{3n}\in_R\mathbb{Z}_p,g_1,h_1\in_R G_1$;

3) 令 $Y=e(g,g)^y$,对于每个 $k\in1,\ldots,3n$,令 $T_k=g^{t_k}$;

4) 选取一个伪随机函数 F:给定一个κ比特的输入参数 x 和一个κ比特的种子 s,函数 F 将输出一个κ比特长的随机字符串 $F_s(x)$;

5) 定义 $H_w:Z_p\to G_1$ 为函数 $H_w(x)=g_1^x h_1$;

6) 返回系统主密钥 $msk=(y,t_1,\ldots,t_{3n})$和系统公共参数 $cp=(G_1,G_2,e,g,g_1,Y,h_1,T_1,\ldots,T_{3n},H_w)$.

从表 1 可以看出,系统公共参数 T_i,T_{n+i} 以及 T_{2n+i} 分别对应着 i 的 3 种出现方式:“正”、“负”以及“不在意”.出于临时私钥成员随机化的需要,我们必须为不出现在与门 W 中的每个属性提供一个“不在意”的出现方式.

Table 1 Common parameters

表 1 系统公共参数

	1	2	...	n
正	T_1	T_2	...	T_n
负	T_{n+1}	T_{n+2}	...	T_{2n}
不在意	T_{2n+1}	T_{2n+2}	...	T_{3n}

KeyGen:可信中心负责执行的私钥生成算法按照以下步骤为输入的属性集合 $S\subseteq\mathcal{N}$产生初始私钥和协助器密钥:

1) 每一个 $i\notin S$ 被隐含地认为是一个负属性;

2) 对于每一个 $i\in\mathcal{N}$,随机选取 $r_i\in_R\mathbb{Z}_p$,并令 $r=\sum_{i=1}^{n}r_i$;

3) 随机选取两个协助器密钥 $HK_{S,1},HK_{S,0}\in_R\{0,1\}^\kappa$;

4) 计算 $k_{S,-1}=F_{HK_{S,1}}(-1),k_{S,0}=F_{HK_{S,0}}(0)$.若函数 F 的输入参数长度小于κ比特,则可以通过在前面填充若干个“0”来达到κ比特;

5) 令 $\hat{D}'_{S,0}=g^{y-r}H_w(-1)^{k_{S,-1}}H_w(0)^{k_{S,0}},\hat{D}''_{S,0}=g^{k_{S,-1}}$,以及 $\hat{D}'''_{S,0}=g^{k_{S,0}}$;

6) 对于每一个 $i\in\mathcal{N}$:若 $i\in S$,令 $D_i=g^{\frac{r_i}{t_i}}$;否则,令 $D_i=g^{\frac{r_i}{t_{n+i}}}$;

7) 对于每一个 $i\in\mathcal{N}$,令 $F_i=g^{\frac{r_i}{t_{2n+i}}}$;

8) 计算初始私钥为

$$TSK_{S,0}=(\hat{D}'_{S,0},\hat{D}''_{S,0},\hat{D}'''_{S,0},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}}) \tag{1}$$

这里,我们使用 $r=\sum_{i=1}^{n}r_i$ 的目的是将所有 D_i 成员绑定在一起以及将所有 F_i 成员绑定在一起.使用 F_i 的目的是为了在算法 *Decryption* 中恢复出所有的 r_i.若加密时 i 为“不在意”(i 不出现在与门 W 中),那么 F_i 将作为 D_i 的替代出现在算法 *Encryption* 里.

HelperUpt:给定属性集合 S 和时间片段参数 t,第ι个协助器(这里,$\iota=t \bmod 2$)首先计算 $k_{S,t-2}=F_{HK_{S,\iota}}(t-2)$,$k_{S,t}=F_{HK_{S,\iota}}(t)$,然后将对应时间片段 t 的更新信息设定为 $UI_{S,t}=(UI_{S,t}^{\langle1\rangle},UI_{S,t}^{\langle2\rangle})=\left(\frac{H_w(t)^{k_{S,t}}}{H_w(t-2)^{k_{S,t-2}}},g^{k_{S,t}}\right)$.

UserUpt:在时间片段 t 内,给定与属性集合 S 相对应的前一时间片段的临时私钥 $TK_{S,t-1}$ 及时间片段 t 的更新信息 $UI_{S,t}$,该算法按如下步骤生成时间片段 t 的临时私钥 $TK_{S,t}$:

1) 将 $TK_{S,t-1}$ 分解为 $TK_{S,t-1}=(\hat{D}'_{S,t-1},\hat{D}''_{S,t-1},\hat{D}'''_{S,t-1},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}})$,将 $UI_{S,t}$ 分解为 $UI_{S,t}=(UI_{S,t}^{\langle1\rangle},UI_{S,t}^{\langle2\rangle})$;

2) 将属性集合 S 相对应的时间段 t 的临时私钥 $TK_{S,t}$ 设定为

$$TK_{S,t}=(\hat{D}'_{S,t},\hat{D}''_{S,t},\hat{D}'''_{S,t},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}})=(\hat{D}'_{S,t-1}UI_{S,t}^{\langle1\rangle},,\hat{D}'''_{S,t-1},UI_{S,t}^{\langle2\rangle},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}}) \tag{2}$$

注意,若令 $\tau=t \bmod 2$ 及 $\eta=1-\tau$,则临时私钥 $TK_{S,t}$ 具有如下形式:

$$TK_{S,t}=(g^{y-r}H_w(t-1)^{k_{S,t-1}}H_w(t)^{k_{S,t}},g^{k_{S,t-1}},g^{k_{S,t}},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}}),$$

其中,$k_{S,t-1}=F_{HK_{S,\eta}}(t-1),k_{S,t}=F_{HK_{S,\tau}}(t)$.

Encryption:给定时间片段参数 t、与门 $W=\wedge_{i\in I}\underline{i}$ 和明文 $M\in G_2$,加密者按照以下步骤进行加密:

1) 随机选取 $s\in_R\mathbb{Z}_p$;

2) 对于每个 $i\in I$:若 $\underline{i}=i$,令 $E_i=T_i^s$;若 $\underline{i}=\neg i$,令 $E_i=T_{n+i}^s$;

3) 对于每个 $i\in\mathcal{N}\backslash I$:令 $E_i=T_{2n+i}^s$;

4) 输出密文为 $(t,E)=(t,(W,E'=M\cdot Y^s,E''=g^s,E'''=H_w(t-1)^s,E''''=H_w(t)^s,\{E_i\}_{i\in\mathcal{N}}))$.

Decryption:假定有一个密文为 $(t,E)=(t,(W,E',E'',E''',E'''',\{E_i\}_{i\in\mathcal{N}}))$, 这里, $W=\wedge_{i\in I}\underline{i}$;同时,我们有一个针对属性集合 S 和时间片断参数 t 的临时私钥 $\mathrm{TK}_{S,t}=(g^{y-r}H_w(t-1)^{k_{S,t-1}}H_w(t)^{k_{S,t}},g^{k_{S,t-1}},g^{k_{S,t}},\{D_i\}_{i\in\mathcal{N}},\{F_i\}_{i\in\mathcal{N}})$. 这种算法检查 S 是否满足 W:若是,输出 failure;否则,执行以下步骤:

1) 对于每个 $i\in I$,计算 $e(E_i,D_i)$.若 $\underline{i}=i$ 且 $i\in S$,则 $e(E_i,D_i)=e\left(g^{t_i\cdot s},g^{\frac{r_i}{t_i}}\right)=\hat{e}(g,g)^{r_i\cdot s}$.类似地,若 $\underline{i}=\neg i$ 且 $i\notin S$,则 $e(E_i,D_i)=\hat{e}\left(g^{t_{n+i}\cdot s},g^{\frac{r_i}{t_{n+i}}}\right)=\hat{e}(g,g)^{r_i\cdot s}$;

2) 对于每个 $i\notin I$,计算 $e(E_i,F_i)=e\left(g^{t_{2n+i}\cdot s},g^{\frac{r_i}{t_{2n+i}}}\right)=e(g,g)^{r_i\cdot s}$;

3) 通过如下操作来解密:

$$\begin{aligned}M&=\frac{E'e(E''',\hat{D}''_{S,t})e(E'''',\hat{D}'''_{S,t})}{e(E'',\hat{D}'_{S,t})\prod_{i=1}^{n}e(g,g)^{r_i\cdot s}}\\&=\frac{M\cdot Y^s e(H_w(t-1)^s,g^{k_{S,t-1}})e(H_w(t)^s,g^{k_{S,t}})}{e(g^s,g^{y-r}H_w(t-1)^{k_{S,t-1}}H_w(t)^{k_{S,t}})e(g,g)^{r\cdot s}}\\&=\frac{M\cdot Y^s e(H_w(t-1)^s,g^{k_{S,t-1}})e(H_w(t)^s,g^{k_{S,t}})}{e(g^s,g^{y-r})e(g^s,H_w(t-1)^{k_{S,t-1}})e(g^s,H_w(t)^{k_{S,t}})e(g,g)^{r\cdot s}}\\&=\frac{M\cdot Y^s}{e(g,g)^{y\cdot s}}\\&=\frac{M\cdot Y^s}{Y^s}.\end{aligned}$$

3.2 安全证明

定理 1. 若群(G_1,G_2)上的 DBDH 困难问题成立且 F 是一个伪随机函数,则第 3.1 节的 CPABPKIE 方案是 IND-CPABPKIE-PKI-CPA 安全的.具体地说,假定群(G_1,G_2)上的 DBDH 困难问题成立且 F 是一个伪随机函数,则:若存在一个针对我们方案的 IND-CPABPKIE-PKI-CPA 敌手$\mathcal{A}$,那么可以构造一个模拟器$\mathcal{B}$来区分一个 BDH 元组和一个随机元组.

证明:假定一个多项式时间敌手$\mathcal{A}$可以以概率ϵ赢得 IND-CPABPKIE-PKI-CPA 游戏.我们构建一个模拟器$\mathcal{B}$,以概率 $\frac{\epsilon}{2}$ 区分一个 BDH 元组和一个随机元组.挑战者首先设定群 G_1 和 G_2,建立在 G_1 和 G_2 之上的设为双线性映射 e 以及 G_1 的一个生成元 g;然后,挑战者随机选取 $a,b,c,z\in_R\mathbb{Z}_p,\nu\in_R\{0,1\}$.如果 $\nu=0$,DBDH 挑战者设定$(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^{abc})$;否则,DBDH 挑战者设定$(A,B,C,Z)=(g^a,g^b,g^c,e(g,g)^z)$.挑战者把$(g,A,B,C,Z)$交给$\mathcal{B}$.$\mathcal{B}$在 IND-

CPABPKIE-PKI-CPA 游戏中扮演着挑战者的角色.$\mathcal{B}$抛取一个随机币$COIN\in\{1,2\}$,若$COIN=1$,$\mathcal{B}$与$\mathcal{A}$进行下面的 Game1,否则进行 Game 2.

Game 1:在该游戏中,假定敌手不会通过协助器密钥查询来获得与受限属性集合对应的任何协助器密钥.算法$\mathcal{B}$充当挑战者和敌手$\mathcal{A}$进行如下游戏:

Init:在初始化阶段,$\mathcal{B}$收到来自$\mathcal{A}$的挑战与门$W^*=\wedge_{i\in I^*}\underline{i}$和挑战时间片断参数$t^*$.

Setup:$\mathcal{B}$按如下方式为$\mathcal{A}$生成公共参数:

1) 令$g_1=A=g^a$和$Y=e(A,B)=e(g,g)^{ab}$;
2) 对于每个$i\in\mathcal{N}$,随机选取$\alpha_i,\beta_i,\gamma_i\in_R\mathbb{Z}_p$.对于每个$i\in I^*$,若$\underline{i}=i$,令$T_i=g^{\alpha_i},T_{n+i}=B^{\beta_i},T_{2n+i}=B^{\gamma_i}$;若$\underline{i}=\neg i$,令$T_i=B^{\alpha_i},T_{n+i}=g^{\beta_i},T_{2n+i}=B^{\gamma_i}$.对于每个$i\notin I^*$,令$T_i=B^{\alpha_i},T_{n+i}=B^{\beta_i},T_{2n+i}=g^{\gamma_i}$;
3) 随机选取$\beta\in_R\mathbb{Z}_p^*$,并定义$h_1=g_1^{-t^*}g^{\beta}\in G_1$.

注意到,从$\mathcal{A}$的角度来看,这些公共参数的分布与真实构造是一致的.与第 3.1 节所提方案一样,我们定义$H_w:Z_p\to G_1$为函数$H_w(x)=g_1^xh_1=g_1^{x-t^*}g^{\beta}$.另外,根据公式(1)和公式(2),给定一个属性集合S,对于每个$i\in S$,S的初始私钥和所有临时私钥共享着相同的r_i.此外,所有临时私钥互相依赖,即:$TK_{S,t-1}$和$TK_{S,t}$共享着相同的$k_{S,t-1}$;同时,$TK_{S,t}$和$TK_{S,t+1}$共享着相同的$k_{S,t}$.为了模拟这些关系,算法$\mathcal{B}$维持初始为空的列表R^{list}和K^{list}.我们定义了算法$RQuery(S,i)$,使得:对于一个输入$\langle S,i\rangle$,若R^{list}包含一个元组$(S,i,\hat{r})$,则返回$\hat{r}$;否则,选择$\hat{r}\in_R\mathbb{Z}_p$,并将$(S,i,\hat{r})$添加到R^{list},再返回$\hat{r}$.类似地,我们定义了算法$KQuery(S,t)$,使得:对于一个输入$\langle S,t\rangle$,若K^{list}包含一个元组$(S,t,\hat{k})$,则返回$\hat{k}$;否则,选择$\hat{k}\in_R\mathbb{Z}_p$,并将$(S,t,\hat{k})$添加到K^{list},再返回$\hat{k}$.

Phase 1:按照 IND-CPABPKIE-PKI-CPA 游戏的定义,在本阶段,敌手$\mathcal{A}$将进行如下一系列的查询.算法$\mathcal{B}$按照如下方法应答:

协助器密钥查询:算法$\mathcal{B}$维持一个初始为空的列表HK^{list}.考虑$\mathcal{B}$收到$\mathcal{A}$的一个协助器密钥查询$\langle S,\iota\rangle$,算法$\mathcal{B}$搜寻列表HK^{list}来获得元组$(S,\iota,HK_{S,\iota})$(如果HK^{list}不包含该元组,它选择$HK_{S,\iota}\in_R\mathbb{Z}_p^*$,并将$(S,\iota,HK_{S,\iota})$添加到$HK^{\text{list}}$.

私钥生成查询:假设$\mathcal{A}$查询关于集合$S\subseteq\mathcal{N}$的初始私钥和两个协助器密钥,这里,$S\not\models W^*$.那么,一定存在$j\in I^*$,使得:要么$j\in S$且$\underline{j}=\neg j$,要么$j\notin S$且$\underline{j}=j$.$\mathcal{B}$选择这样的j.

不失一般性,假定$j\notin S$且$\underline{j}=j$.$\mathcal{B}$按下列方式定义初始私钥:

1) 通过执行协助器密钥查询$\langle S,1\rangle$和$\langle S,0\rangle$来获得协助器密钥$HK_{S,1}$与$HK_{S,0}$;
2) 计算$k_{S,-1}=F_{HK_{S,1}}(-1)$和$k_{S,0}=F_{HK_{S,0}}(0)$;
3) 设置$\hat{D}''_{S,0}=g^{k_{S,-1}}$和$\hat{D}'''_{S,0}=B^{\frac{-1}{0-t^*}}g^{k_{S,0}}$;
4) 令$\tilde{k}_{S,0}=k_{S,0}-\frac{b}{0-t^*}$,可得$\hat{D}'''_{S,0}=g^{\tilde{k}_{S,0}}$和

$$B^{\frac{-\beta}{0-t^*}}H_w(0)^{k_{S,0}}=B^{\frac{-\beta}{0-t^*}}(g_1^{0-t^*}g^{\beta})^{k_{S,0}}=g^{ab}(g_1^{0-t^*}g^{\beta})^{k_{S,0}}g^{-ab}B^{\frac{-\beta}{0-t^*}}=g^{ab}(g_1^{0-t^*}g^{\beta})^{k_{S,0}}g_1^{-b}g^{\frac{-b\beta}{0-t^*}}=$$

$$g^{ab}(g_1^{0-t^*}g^{\beta})^{k_{S,0}}(g_1^{0-t^*}g^{\beta})^{-\frac{b}{0-t^*}}=g^{ab}(g_1^{0-t^*}g^{\beta})^{k_{S,0}-\frac{b}{0-t^*}}=g^{ab}H_w(0)^{\tilde{k}_{S,0}}$$

5) 对于每个$i\in\mathcal{N}$,计算$r'_i=RQuery(S,i)$;
6) 令$r_j=ab+r'_j\cdot b$;
7) 对于每个$i\neq j$,令$r_i=r'_i\cdot b$;
8) 令$r=\sum_{i=1}^{n}r_i=ab+\sum_{i=1}^{n}r'_ib$;
9) 令

$$\hat{D}'_{S,0}=\left(\prod_{i=1}^{n}\frac{1}{B^{r'}}\right)B^{\frac{-\beta}{0-t^*}}H_w(-1)^{k_{S,-1}}H_w(0)^{k_{S,0}}=g^{-\sum_{i=1}^{n}r'\cdot b}g^{ab}H_w(-1)^{k_{S,-1}}H_w(0)^{\tilde{k}_{S,0}}=$$

$$g^{ab-r}g^{ab}H_w(-1)^{k_{S,-1}}H_w(0)^{\tilde{k}_{S,0}}=g^{2ab-r}H_w(-1)^{k_{S,-1}}H_w(0)^{\tilde{k}_{S,0}};$$

10) 对于每个 $j\in I^*\backslash S$ 和 $\underline{j}=j$,令 $D_j=A^{\frac{1}{\beta_j}}g^{\frac{r'_j}{\beta_j}}=g^{\frac{ab+r'_jb}{b\beta_j}}=g^{\frac{r_j}{b\beta_j}}$;

11) 对于 $i\neq j\wedge i\in S$,若 $i\in I^*\wedge\underline{i}=i$,令 $D_i=B^{\frac{r'_i}{\alpha_i}}=g^{\frac{r_i}{\alpha_i}}$;若$(i\in I^*\wedge\underline{i}=\neg i)\vee i\notin I^*$,令 $D_i=g^{\frac{r'_i}{\alpha_i}}=g^{\frac{r_i}{b\alpha_i}}$;

12) 对于 $i\neq j\wedge i\notin S$,若$(i\in I^*\wedge\underline{i}=i)\vee i\notin S$,令 $D_i=g^{\frac{r'_i}{\beta_i}}=g^{\frac{r_i}{b\beta_i}}$;若 $i\in I^*\wedge\underline{i}=\neg i$,令 $D_i=B^{\frac{r'_i}{\beta_i}}=g^{\frac{r_i}{\beta_i}}$;

13) 对于 $j\in I^*\backslash S\wedge\underline{j}=j$,令 $F_j=A^{\frac{1}{\gamma_j}}g^{\frac{r'_j}{\gamma_j}}=g^{\frac{ab+r'_jb}{b\gamma_j}}=g^{\frac{r_j}{b\gamma_j}}$;

14) 对于 $i\neq j\wedge i\in I^*$,令 $F_i=g^{\frac{r'_i}{\gamma_i}}=g^{\frac{r_i}{b\gamma_i}}$;

15) 对于 $i\neq j\wedge i\notin I^*$,令 $F_i=B^{\frac{r'_i}{\gamma_i}}=g^{\frac{r_i}{\gamma_i}}$.

临时私钥查询:敌手$\mathcal{A}$可以通过对任意非受限属性集合 S 进行私钥生成查询来得到初始私钥和两个协助器密钥,从而$\mathcal{A}$可以利用这些信息来间接得到属性集合 S 在任何时间片段内的临时私钥.因此不失一般性,假定敌手$\mathcal{A}$只对受限集合 $S^*\subseteq\mathcal{N}$进行临时私钥查询,这里,$S^*\models W^*$.总体来说,当收到一个临时私钥查询$\langle S,t\rangle$时(不失一般性,假定 t 为偶数;若 t 为奇数,可以类似处理),$\mathcal{B}$按照与私钥生成查询相同的方式选择$j\in I^*$,使得:要么 $j\in S$ 且 $\underline{j}=\neg j$,要么 $j\notin S$ 且 $\underline{j}=j$.不失一般性,假定 $j\notin S$ 且 $\underline{j}=j$.$\mathcal{B}$计算 $k_{S,t-1}=KQuery(S,t-1)$和 $k_{S,t}=KQuery(S,t)$.注意,由于函数 F 是一个伪随机函数,并且敌手不知道相应种子 $HK_{S,1}$ 和 $HK_{S,0}$ 的值,因此从敌手$\mathcal{A}$的角度来说,按照上述方法计算出来的指数 $k_{S,t-1}$ 和 $k_{S,t}$ 与真实环境是不可区分的.$\mathcal{B}$根据如下方式来为$\mathcal{A}$生成临时私钥:

1) 设置 $\hat{D}''_{S,t}=g^{k_{S,t-1}}$ 和 $\hat{D}'''_{S,t}=B^{\frac{-1}{t-t^*}}g^{k_{S,t}}$;

2) 令 $\tilde{k}_{S,t}=k_{S,t}-\frac{b}{t-t^*}$,可得 $\hat{D}'''_{S,t}=g^{\tilde{k}_{S,t}}$ 和

$$B^{\frac{-\beta}{t-t^*}}H_w(t)^{k_{S,t}}=B^{\frac{-\beta}{t-t^*}}(g_1^{t-t^*}g^{\beta})^{k_{S,t}}=g^{ab}(g_1^{t-t^*}g^{\beta})^{k_{S,t}}g^{-ab}B^{\frac{-\beta}{t-t^*}}=g^{ab}(g_1^{t-t^*}g^{\beta})^{k_{S,t}}g_1^{-b}g^{\frac{-b\beta}{0-t^*}}=$$

$$g^{ab}(g_1^{t-t^*}g^{\beta})^{k_{S,t}}(g_1^{t-t^*}g^{\beta})^{-\frac{b}{t-t^*}}=g^{ab}(g_1^{t-t^*}g^{\beta})^{k_{S,t}-\frac{b}{t-t^*}}=g^{ab}H_w(t)^{\tilde{k}_{S,t}};$$

3) 对于每个 $i\in\mathcal{N}$,计算 $r'_i=RQuery(S,i)$;

4) 令 $r_j=ab+r'_j\cdot b$;

5) 对于每个 $i\neq j$,令 $r_i=r'_i\cdot b$;

6) 令 $r=\sum_{i=1}^{n}r_i=ab+\sum_{i=1}^{n}r'_i\cdot b$;

7) 令

$$\hat{D}'_{S,t}=\left(\prod_{i=1}^{n}\frac{1}{B^{r'}}\right)B^{\frac{-\beta}{t-t^*}}H_w(t-1)^{k_{S,t-1}}H_w(t)^{k_{S,t}}=g^{-\sum_{i=1}^{n}r'\cdot b}g^{ab}H_w(t-1)^{k_{S,t-1}}H_w(t)^{\tilde{k}_{S,t}}=$$

$$g^{ab-r}g^{ab}H_w(t-1)^{k_{S,t-1}}H_w(t)^{\tilde{k}_{S,t}}=g^{2ab-r}H_w(t-1)^{k_{S,t-1}}H_w(t)^{\tilde{k}_{S,t}};$$

8) 按照与私钥生成查询同样的方式构造 D_i 和 F_i.

Challenge:敌手$\mathcal{A}$向模拟器提交两个长度相等的挑战明文 M_1 和 M_0.模拟器随机选取$\mu\in_R\{0,1\}$,然后返回 M_μ 的加密密文.输出密文为

$$E=(t^*,(W^*,E'=M_\mu Z,E''=C,E'''=C^\beta,E''''=(CA^{-1})^\beta,\{C^{\alpha_i}\mid i\in I^*\wedge\underline{i}=i\},\{C^{\beta_i}\mid i\in I^*\wedge\underline{i}=\neg i\},\{C^{\gamma_i}\mid i\notin I^*\})).$$

Phase 2:重复 Phase 1;

Guess:$\mathcal{A}$将产生一个对μ的猜测μ'.若$\mu'=\mu$,在 DBDH 游戏中,$\mathcal{B}$回答“DBDH”来表明$\mathcal{B}$被给与一个 BDH 元组;否则,$\mathcal{B}$回答“random”来表明$\mathcal{B}$被给与一个随机四元组.

Game 2:在该游戏中,假定敌手会通过协助器密钥查询来获得受限属性集合S的其中一个协助器密钥,这里,$S^*\subseteq\mathcal{N}$且 $S^*\models W^*$.$\mathcal{B}$抛取随机币$\eta\in_R\{0,1\}$来猜测敌手$\mathcal{A}$将查询属性集合 S 的第η个协助器密钥.不失一般性,假定$\eta=1$($\eta=0$ 的情形可以类似处理).注意到,对于受限属性集合及偶数的时间片段参数 t,由于敌手$\mathcal{A}$没有获得 $HK_{S,0}$,它将无法获得指数 $HK_{S,1}$ 的任何信息.该游戏定义与前面游戏相同的函数 $RQuery$.与 Game1 一样,算法$\mathcal{B}$采取同样方法来处理 Init,Setup,Challenge 及 Phase 1 的协助器密钥查询和私钥生成查询.此外,算法$\mathcal{B}$按照如下方法应答敌手$\mathcal{A}$的临时私钥查询:

临时私钥查询:与 Game 1 一样,这里假定敌手$\mathcal{A}$只对挑受限属性集合 S($S^*\subseteq\mathcal{N}$且 $S^*\models W^*$)进行临时私钥查询.对于一个临时私钥查询$\langle S,t\rangle$,下面来处理当 t 为奇数时的情形(t 为偶数的情形可类似处理).注意到,由于$\mathcal{A}$不知道 $HK_{S,0}$,所以$\mathcal{A}$无法计算 $k_{S,t-1}$.$\mathcal{B}$计算 $k_{S,t-1}=RQuery(S,t-1)$,$k_{S,t}=F_{\mathrm{HK}_{S,1}}(t)$, 再执行 Game 1 中临时私钥查询的第 1 步至第 8 步.

下面分析$\mathcal{B}$在 Game 1 和 Game 2 中的优势.首先对 Game 1 进行分析.若 $Z=e(g,g)^{abc}$,则 E 是一个有效密文,其中,$\mathcal{A}$的优势是ϵ.于是,$\Pr[\mathcal{B}\rightarrow\text{“DBDH”}|Z=e(g,g)^{abc}]=\Pr[\mu'=\mu|Z=e(g,g)^{abc}]=\frac{1}{2}+\epsilon$.若 $Z=e(g,g)^{z}$,则从$\mathcal{A}$的角度来看,E'是完全随机的.所以,无论μ'如何分布,$\mu'\neq\mu$成立的概率总是$\frac{1}{2}$.于是,

$$\Pr[\mathcal{B}\rightarrow\text{“random”}|Z=e(g,g)^{z}]=\Pr[\mu'\neq\mu|Z=e(g,g)^{z}]=\frac{1}{2}.$$

因此,在 Game1 中,$\mathcal{B}$的优势为$\frac{\epsilon}{2}$.类似地我们可以看出,$\mathcal{B}$在 Game 2 中的优势为$\frac{\epsilon}{2}$.于是,算法$\mathcal{B}$在 DBDH 游戏中的总优势为$\frac{1}{2}\left(\frac{\epsilon}{2}+\frac{\epsilon}{2}\right)=\frac{\epsilon}{2}$. □

定理 2. 若群(G_1,G_2)上的 DBDH 困难问题成立且 F 是一个伪随机函数,则第 3.1 节的 CPABPKIE 方案是 IND-CPABPKIE-sPKI-CPA 安全的.具体地说,假定群(G_1,G_2)上的 DBDH 困难问题成立且 F 是一个伪随机函数,则:若存在一个针对我们方案的 IND-CPABPKIE-sPKI-CPA 敌手$\mathcal{A}$,那么可以构造一个模拟器$\mathcal{B}$来区分一个 BDH 元组和一个随机元组.

证明:证明与定理 1 类似.需要注意的是:不再向敌手$\mathcal{A}$提供临时私钥查询. □

3.3 选择密文安全

我们可以运用文献[10]中的技术来获得选择密文安全.

4 结 论

本文深入研究了如何将 Hanaoka 等人[2]的并行密钥隔离机制扩展到密文策略的属性基加密[9]中去.首先给出了密文策略的属性基并行密钥隔离加密的形式化定义和安全模型;然后,提出了一个具体的密文策略的属性基并行密钥隔离加密方案;最后,在不需要随机预言机的选择 ID 模型下,给出了所提方案的安全性证明.

References:

[1] Dodis Y, Katz J, Xu S, Yung M. Key-Insulated public-key cryptosystem. In: Knudsen LR, ed. Proc. of the EUROCRYPT 2002. LNCS 2332, Heidelberg: Springer-Verlag, 2002. 65−82. [doi: 10.1007/3-540-46035-7_5]

[2] Hanaoka G, Hanaoka Y, Imai H. Parallel key-insulated public key encryption. In: Yung M, ed. Proc. of the PKC 2006. LNCS 3958, Heidelberg: Springer-Verlag, 2006. 105−122. [doi: 10.1007/11745853_8]

[3] Hanaoka Y, Hanaoka G, Shikata J, Imai H. Identity-Based hierarchical strongly key-insulated encryption and its application. In: Roy B, ed. Proc. of the Asiacrypt 2005. LNCS 3958, Heidelberg: Springer-Verlag, 2006. 495−514. [doi: 10.1007/11593447_27]

[4] Weng J, Liu S, Chen K, Ma C. Identity-Based parallel key-insulated encryption without random oracles: Security notions and construction. In: Barua R, Lange T, eds. Proc. of the Indocrypt 2006. LNCS 4329, Heidelberg: Springer-Verlag, 2006. 409−423. [doi: 10.1007/11941378_29]

[5] Libert B, Quisquater JJ, Yung M. Parallelkey-Insulated public key encryption without random oracles. In: Okamoto T, Wang X, eds. Proc. of the PKC 2007. LNCS 4450, Heidelberg: Springer-Verlag, 2007. 298−314. [doi: 10.1007/978-3-540-71677-8_20]

[6] Sahai A, Waters B. Fuzzy identity-based encryption. In: Cramer R, ed. Proc. of the Eurocrypt 2005. LNCS 3494, Heidelberg: Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[7] Goyal V, Pandey O, Saha A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Wright R, Vimercati SDCD, eds. Proc. of the ACM CCS 2006. New York: ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

[8] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Pfitzmann B, McDaniel P, eds. Proc. of the IEEE SP 2007. Los Angeles: IEEE Computer Society, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[9] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Vimercati SDCD, Syverson P, eds. Proc. of the ACM CCS 2007. New York: ACM Press, 2007. 456−465. [doi: 10.1145/1315245.1315302]

[10] Sahai A. Non-Malleable non-interactive zero knowledge and adaptive chosen-ciphertext security. In: Beame P, ed. Proc. of the IEEE FOCS'99. Los Angeles: IEEE Computer Society, 1999. 543−553. [doi: 10.1109/SFFCS.1999.814628]

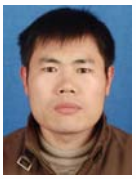
陈剑洪(1973－),男,江苏淮安人,博士,讲师,主要研究领域为密码学,信息安全.

陈克非(1959－),男,博士,教授,博士生导师,主要研究领域为密码学,信息安全.

龙宇(1980－),女,博士,助理研究员,主要研究领域为密码学,信息安全.

万中美(1973－),女,博士,讲师,主要研究领域为密码学,信息安全.

于坤(1972－),男,博士,讲师,主要研究领域为计算机网络.



孙成富(1979－),男,博士,讲师,主要研究领域为密码学,信息安全.

陈礼青(1982－),男,讲师,CCF 会员,主要研究领域为密码学,信息安全.