一对多场景下的公钥时控性可搜索加密

袁 科[1,2],刘哲理[2],贾春福[2],杨 骏[2],吕述望[3]
(1.河南大学计算机与信息工程学院,河南开封 475004;2.南开大学计算机与控制工程学院,天津 300071;
3.中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 为有效解决多接收者时间相关密文检索问题,采用广播加密技术提出一对多公钥时控性可搜索加密机制——发送者将加密的数据发送至云服务器,使得仅授权用户组成员可检索下载包含特定关键词的密文,但只能在指定的未来时间之后解密.给出方案及其安全游戏模型的形式化定义,提出两种基于 q-DBDHI 问题的可证明安全方案,并严格证明所提方案在自适应选择明文攻击下是安全的.效率分析表明,两种方案在执行过程中,实现了计算、存储、传输规模与用户规模无关;与相关方案相比,方案2具有更高效率.

关键词: 定时发布;可搜索加密;一对多;可证明安全
中图分类号: TP309.07 **文献标识码:** A **文章编号:** 0372-2112 (2015)04-0760-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.04.019

Public Key Timed-Release Searchable Encryption in One-to-Many Scenarios

YUAN Ke[1,2], LIU Zhe-li[2], JIA Chun-fu[2], YANG Jun[2], LÜ Shu-wang[3]
(1. *School of Computer and Information Engineering, Henan University, Kaifeng, Henan* 475004, *China*;
2. *College of Computer and Control Engineering, Nankai University, Tianjin* 300071, *China*;
3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: To solve the multi-receiver time-dependent ciphertext retrieval problem efficiently, by borrowing the technique of identity-based broadcast encryption, we propose a cryptosystem of one to many public key timed-release searchable encryption (PKTRSE$_{OM}$). In our PKTRSE$_{OM}$ model, the sender transmits an encrypted message to cloud server so that only the intended authorized user group member can search the target ciphertext containing specified keywords, but cannot decrypt it until the release time in the future. We formalize the notion of PKTRSE$_{OM}$ and its security game model. Then, we construct two provably secure PKTRSE$_{OM}$ schemes which are secure under the q-DBDHI assumption and give the rigorous proof for both schemes. The efficiency analysis shows that the two schemes achieve constant costs from the sender's and the recipient's points of view in the running process of the system and the second scheme is more efficient than the relevant schemes.

Key words: timed-release; searchable encryption; one-to-many; provable security

1 引言

杂志采用纸质媒介出版发行是传统上常用的方式,这种方式存在一些问题:(1)将纸质杂志传递至大量的订阅用户成本高、耗时长、且不方便;(2)难以查找目标内容;(3)形式单调,不能表现多种媒体形式;(4)已出版的杂志中如果存在错误,则无法修正.应对这些问题,不难想到采用电子媒介.但是,这又会产生新问题:(1)电子媒介可快速轻易地被复制,如何保护电子多媒体杂志的版权?一种自然的想法是对其实施加密变换;(2)如果电子杂志被加密,如何在其密文中检索目标内容?(3)如何将电子杂志以简易方式传输至大量的订阅者?一种自然想法是将其上传至云服务器,然后订阅者自行下载;(4)如果上传至云服务器,如何

收稿日期:2014-01-27;修回日期:2014-09-02;责任编辑:马兰英
基金项目:国家"973"重点基础研究计划(No.2013CB834204);国家自然科学基金(No.61272423, No.61300241, No.61402521);天津市自然科学基金(No.13JCNJC00300);高等学校博士科学专项卡科研基金(No.20120031120036);中国民航大学信息安全测评中心开放课题(No.CAAC-ISECCA-201403)

保障大量的订阅者同时及时获取电子杂志?

本文采用公钥时控性可搜索加密(Public Key Timed-Release Searchable Encryption, PKTRSE)技术解决上述问题. PKTRSE 是 TRE[1](timed-release encryption)与 PEKS[2](public key encryption with keyword search)技术的组合,旨在发送带有具体关键词的消息到未来. 一对一 PKTRSE[3](one to one PKTRSE, $\text{PKTRSE}_{\text{OO}}$)只能解决单收发用户场景,即一发送者将带有指定解密时间的消息加密发送至服务器;一接收者在解密时间到达后,检索其感兴趣关键词对应的密文,并下载解密. 为满足共享云加密存储的需求:数据拥有者可将其数据密文分享给其他多个授权用户. 若采用 $\text{PKTRSE}_{\text{OO}}$ 技术,发送者需使用多个接收者的公钥分别加密,分别发送. 这种方法的明显缺陷是,对于发送者而言,加密计算代价、密文规模、通信代价都是 $O(N)$. N 是授权接收者的个数,当 N 很大时,该缺陷将成为一严重问题.

本文目标是设计一种新的加密机制——一对多 PKTRSE(one to many PKTRSE, $\text{PKTRSE}_{\text{OM}}$),使得在发送者和接收者看来,计算、存储、传输规模与 N 无关. 在 $\text{PKTRSE}_{\text{OM}}$ 模型中,一发送者加密一个带有指定解密时间的消息到云服务器,授权用户组成员可以在任何时间检索下载包含特定关键词的密文,但不能解密,直到指定的解密时间.

1.1　论文贡献

论文解决了多接收者云加密存储场景下的时间相关密文检索问题. 文中给出 $\text{PKTRSE}_{\text{OM}}$ 方案及其安全游戏模型的形式化定义,构造出基于 q-DBDHI[4](Decisional Bilinear Diffie-Hellman Inversion)问题的两种可证明安全的具体方案,并给出所提方案是抗不可区分的、身份与发布时间可选、自适应选择明文攻击(Indistinguishable, Selective Identity and Release Time, Adaptive Chosen Plaintext Attack, IND-sID-T-CPA1)的安全性证明.

本文采用基于身份的广播加密(Identity-Based Broadcast Encryption, IBBE)技术[5],使得 $\text{PKTRSE}_{\text{OM}}$ 满足目标要求. 主要优点有:(1)系统运行过程中,加解密计算代价、密文规模、公私钥规模、通信代价是 $O(1)$ 的,与授权用户规模不相关;(2)用户组管理员可动态地增加用户,而不用修改其他用户的参数;(3)用户公钥是其身份的 Hash 值,无需验证用户公钥真实性;(4)方案中一些双线性对运算可提前计算;(5)用户访问云服务器可保持其身份隐私性. 不足之处是一旦涉及删除用户操作,系统需要更新.

1.2　相关工作

TRE 机制中,发送者加密一消息,接收者在指定的时间之前不能解密. TRE 由 May[6] 于 1993 年首次提出,并由 Rivest 等[1]于 1996 年进一步深入探究. 此后,其理论与应用方面都得到很大完善[7]. 特别地,在一对多 TRE 相关研究工作方面. Cathalo 等[8]、Chalkias 等[9]与 Liang 等[10]所做工作没有实现 $O(1)$ 代价. 其中,Liang 等方案作适当修改可达 $O(1)$ 规模. 2010 年,Emura 等[11]提出基于代理重加密技术的 TRE 概念用于解决多接收者 TRE 问题. 2011 年,Emura 等[12]对其之前工作[11]作了进一步完善. 其方案除了产生代理重加密密钥的操作是 $O(N)$ 代价外(可提前计算),其他操作都实现了 $O(1)$ 代价,但非常复杂,且不能做到用户对代理匿名. 另外,其方案中用户公私钥形式采用 PKE(Public Key Encryption)密码机制实现,存在用户公钥真实性需验证的问题.

PEKS 机制中,服务器可测试由发送者生成的关键词标签和由接收者生成的关键词陷门是否包含相同关键词,进而实现密文检索. PEKS 由 Boneh[2] 于 2004 年首次提出. 此后,很多改进与扩展方案被提出. 特别地,在一对多 PEKS 相关研究工作方面. Hwang 与 Lee[13]、Bao 等[14]、Zhao 等[15],分别提出了多用户场景下的 PEKS,但都未能完全做到 $O(1)$ 代价.

2　$\text{PKTRSE}_{\text{OM}}$ 模型

假设用户 Bob 准备将带有关键词 $W_1,\cdots,W_n$ 的消息 M 加密发送给一授权用户组,且任一授权用仅在指定的时间 T 之后才能对其解密. Bob 发送如下数据至云服务器:$[Enc(MPK,ts_{\text{pub}},\mathcal{P},M,T,\cdots),KwTag(MPK,\mathcal{P},W_1,\cdots)\parallel\cdots\parallel KwTag(MPK,\mathcal{P},W_n,\cdots),T]$. 其中,$MPK$ 为主公钥,ts_{pub} 为时间服务器公钥,$\mathcal{P}$ 为所有授权用户公钥的积. 系统目标是:任一授权用户 u_i 可发送一个关键词陷门 T_W 至云服务器,云服务器可定位包含关键词 W 的所有密文而不能获知任何信息. 具体地,u_i 使用其私有参数生成 T_W,云服务器将对应密文发送至 u_i. 然后,u_i 使用时间服务器在时间 T 颁布的时间陷门 S_T 与自己的私有参数解密密文. 本文称这样的系统为非交互 $\text{PKTRSE}_{\text{OM}}$ 系统.

定义 1　非交互 $\text{PKTRSE}_{\text{OM}}$ 方案 ξ　该方案包括时间服务器、云服务器、发送者与授权用户组 4 个实体,以及算法 10 元组 $\xi_{\text{PKTRSE}_{\text{OM}}}=(Ini,Setup,KeyGen,TRSetup,Enc,KwTag,KwTrd,Search,RtTrd,Dec)$. 具体地:

Ini. 输入安全参数,生成系统通用基本参数.

Setup. 确定授权用户组,并输出一些系统参数.

KeyGen. 生成各授权用户的公私钥对(upk,usk).

TRSetup. 生成时间服务器的公私钥对($ts_{\text{pub}}, ts_{\text{priv}}$).

Enc. 使用 $MPK, ts_{\text{pub}}, \mathcal{P}$ 等参数,生成消息 M 在时间 T 之后才能解密的密文.

KwTag. 使用 $MPK, \mathcal{P}$ 等参数,生成关键词 W 对应的标签.

KwTrd. 使用 $MPK, \mathcal{P}, usk_i$ 等参数,生成关键词 W 对应的陷门 T_W.

Search. 给定一个关键词 W'的标签与一个关键词 W 的陷门,判定 $W = W'$是否成立.

RtTrd. 使用参数 ts_{priv},生成时间 T 对应的陷门 S_T.

Dec. 使用 $usk_i, \mathcal{P}, S_T$ 等参数,生成密文 C 对应的明文 M.

下面给出 $\text{PKTRSE}_{\text{OM}}$方案不可区分的、身份与发布时间可选、自适应选择密文攻击(IND-sID-T, Adaptive Chosen Ciphertext Attack, IND-sID-T-CCA1)安全的游戏模型[4,16]. 安全游戏中,挑战者 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 交互如下:

Initialization $\mathcal{A}$ 输出其试图攻击的对象:一授权用户集合 $U^* = \{u_j^* \mid u_j^* = ID_j^*, j = 1, \cdots, N\}$ 与一解密时间 T^*. 其中,u_j^* 是一授权用户,ID_j^* 是其相应的身份标识,N 是授权用户的数量.

Setup $\mathcal{B}$ 生成系统参数、MPK 与 ts_{pub},并输出给 $\mathcal{A}$.

Phase 1 $\mathcal{A}$ 发起 $1, \cdots, m$ 次查询,$\mathcal{B}$ 分别予以响应. 其中第 i 次查询-响应如下:

(1)私钥查询 查询用户 u_i 的私钥 usk_i,其中,$ID_i \notin U^*$. $\mathcal{B}$ 运行算法 *KeyGen*,生成 usk_i 并输出给 $\mathcal{A}$.

(2)时间陷门查询 查询时间 T_i 的陷门 S_{T_i},其中,$T_i \neq T^*$. $\mathcal{B}$ 运行算法 *RtTrd*,生成 S_{T_i}并输出给 A.

(3)解密查询 查询密文 C_i^* 对应的明文 M_i^*. $\mathcal{B}$ 首先运行算法 *KeyGen*,生成用户 u_i^* 的私钥 usk_i^*;然后运行算法 *Dec*,使用 $usk_i^*, \mathcal{P}, S_{T'}$ 等参数,生成密文 C_i^* 对应的明文 M_i^* 并输出给 $\mathcal{A}$.

上述查询是自适应的,即第 i 次查询可以利用之前 $1, \cdots, i-1$ 次查询的结果.

Challenge $\mathcal{A}$ 输出两对明文,$\mathcal{B}$ 挑战如下:

(1)检索阶段 $\mathcal{A}$ 输出一对试图被挑战的明文 $\mathcal{M}_0, \mathcal{M}_1$. 算法 $\mathcal{B}$ 选择随机数 $\mathfrak{b} \in \{0,1\}$,并设置挑战密文 $\mathcal{C} = Enc(W, \mathcal{M}_{\mathfrak{b}}, \cdots)$. $\mathcal{B}$ 将 $\mathcal{C}$ 作为挑战输出给 $\mathcal{A}$.

(2)解密阶段 $\mathcal{A}$ 输出一对试图被挑战的明文 M_0, M_1. 算法 $\mathcal{B}$ 选择随机数 $\mathsf{b} \in \{0,1\}$,并设置挑战密文 $C = Enc(MPK, \mathcal{P}, ts_{\text{pub}}, M_{\mathsf{b}}, T, \cdots)$. $\mathcal{B}$ 将 (C, T) 作为挑战输出给 $\mathcal{A}$.

Phase 2 $\mathcal{A}$ 发起另外的至多 $m+1, \cdots, num$ 次私钥、时间陷门与解密查询. $\mathcal{B}$ 以与 Phase 1 相同的方式给予响应.

Guess $\mathcal{A}$ 输出对 $\mathfrak{b}, \mathsf{b}$ 的猜测 $\mathfrak{b}', \mathsf{b}' \in \{0,1\}$. 如果 $\mathfrak{b} = \mathfrak{b}', \mathsf{b} = \mathsf{b}'$,则 $\mathcal{A}$ 赢得游戏.

我们称这样的敌手 $\mathcal{A}$ 为 IND-sID-T-CCA1 敌手,定义敌手 $\mathcal{A}$ 攻击 $\text{PKTRSE}_{\text{OM}}$方案 ξ 的优势为:

$$Adv_{\xi,\mathcal{A}}^{\text{CCA1}} = \Pr[\mathfrak{b} = \mathfrak{b}', \mathsf{b} = \mathsf{b}'] - 1/4$$

上述概率值基于 $\mathcal{B}$ 与 $\mathcal{A}$ 之间交互数据的随机性.

定义 2 $\xi_{\text{PKTRSE}_{\text{OM}}}$方案是$(t', q_{ID}, q_T, q_C, \varepsilon)$-IND-sID-T-CCA1 安全的,如果任意 t'时间内,敌手 $\mathcal{A}$ 至多进行自适应 q_{ID}次选择私钥查询、q_T 次选择时间查询与 q_C 次选择解密查询,有 $Adv_{\xi,\mathcal{A}}^{\text{CCA1}} < \varepsilon$.

定义 3 $\xi_{\text{PKTRSE}_{\text{OM}}}$方案是$(t', q_{ID}, q_T, \varepsilon)$-IND-sID-T-CPA1 安全的,如果 ξ 是$(t', q_{ID}, q_T, 0, \varepsilon)$-IND-sID-T-CCA1 安全的,有 $Adv_{\xi,\mathcal{A}}^{\text{CPA1}} < \varepsilon$.

3 $\text{PKTRSE}_{\text{OM1}}$方案

本节提出一个具体的构造方案 $\text{PKTRSE}_{\text{OM1}}$,并给出其在 CPA1 攻击模型下的安全性证明. 该方案更加注重安全性. 为防止用户组管理员授权非法用户解密,此方案以消息发送者作为管理员.

3.1 方案表述

$\text{PKTRSE}_{\text{OM1}}$方案工作过程包括如下 10 个阶段:

Ini. 时间服务器选择安全参数 $k \in \mathbb{Z}^+$,并执行下述操作:

(1)输入 k 并生成素数 p. 令 G_1 与 G_2 是阶为素数 p 的乘法群,$e: G_1 \times G_1 \to G_2$ 是一可容许的双线性映射,$g \in G_1$ 是任一生成元.

(2)选择 hash 函数 $H: \{0,1\}^* \to \mathbb{Z}_p^*$.

(3)公开通用系统参数 $ts_{\text{g}} = <p, G_1, G_2, g, e, H>$.

Setup. 用户组管理员执行下述操作:

(1)选择 hash 函数 $\mathscr{H}: \{0,1\}^* \to G_1$.

(2)为生成 IBBE 参数,选择随机数 $x, y \in \mathbb{Z}_p^*$,并定义 $X = g^x, Y = g^y$. 保密主私钥 $MSK = (x, y)$,公开主公钥 $MPK = (X, Y)$.

(3)确定授权用户集合 $U = \{u_j \mid u_j = ID_j, j = 1, \cdots, N\}$. 其中,$u_j$ 是一授权用户,ID_j 是其相应身份标识,N 是授权用户数量.

KeyGen(MSK, U). 用户组管理员为每一授权用户产生公私钥对,执行下述操作:

(1)计算生成所有授权用户公钥,输出其公钥集合,公开公钥的积. 具体地,对于任一用户 u_j,其公钥 $upk_j = H(ID_j)$;授权用户公钥的集合 $U_{pk} = \{H(ID_j) \mid j = 1, \cdots, N\}$,公钥的积 $\mathcal{P} = \prod_{j=1}^{N} H(ID_j)$.

(2)计算生成所有授权用户的私钥. 具体地,对于任一用户 u_j,挑选一随机数 $r_j \in \mathbb{Z}_p^*$,计算 $K_j = g^{1/H(ID_j)x + r_j y}$

$\in G_1^*$,得私钥 $usk_j=(r_j,K_j)$. 如果 $H(ID_j)x+r_jy=0 \pmod p$,则重选 r_j.

(3)通过某种安全方式将各私钥分发至相应用户.

TRSetup. 时间服务器选取一随机数 $s\in\mathbb{Z}_p^*$ 作为其私钥 ts_{priv},并以 g^s 作为其公钥 ts_{pub}.

Enc$(MPK,G,ts_{\text{pub}},M,T)$. 发送者选取随机数 $k_1,k_2\in\mathbb{Z}_p^*$,加密一组消息 $M\in G_2$;输出密文 $C=(c_1,c_2,c_3',c_4)$,其中,$c_1=X^{k_1\mathcal{P}}$,$c_2=Y^{k_1}$,$c_3=(ts_{\text{pub}})^{k_2}$,$c_3'=c_3\oplus\mathcal{H}(e((ts_{\text{pub}})^{yk_1},\mathcal{H}(T)))$,$c_4=e(g,g)^{k_1+k_2}M$.

KwTag(MPK,P,W). 发送者选取随机数 $k_3\in\mathbb{Z}_p^*$,生成关键词标签 $KWT=(E,\varepsilon)$. 其中,$E=X^{k_3\mathcal{P}/H(W)}$,$\varepsilon=e(g,g)^{k_3}$.

KwTrd(MPK,usk_i,W). 当用户 u_i 检索包含关键词 W 的密文时,使用其私钥生成对应陷门 $T_W=(F,L,H(ID_i))$,并发送至云服务器. 其中,$F=Y^{r/H(W)}$,$L=K_i^{H(W)}$.

Search(KWT,T_W). 当云服务器收到检索请求时,测试等式 $e(E^{H(ID_i)/\mathcal{P}}F,L)=\varepsilon$ 是否成立. 如果成立,则找到了目标密文 C,允许请求者下载(C,T);否则,拒绝其下载任何内容.

RtTrd(ts_{priv},T). 时间服务器生成并发布每一时间点的陷门 S_T. 对于时间点 T,$S_T=(r_t,K,K')$,其中,随机数 $r_t\in\mathbb{Z}_p^*$,$K=g^{1/s(H(T)+r_t)}$,$K'=(\mathcal{H}(T))^s$. 如果

$H(T)+r_t=0 \pmod p$,则重选 r_t.

Dec$(usk_i,\mathcal{P},S_T,C)$. 任一授权用户 u_i 在发送者指定的解密时间到达之后,使用其私钥与时间服务器发布的对应 S_T 解密密文;输出明文

$$M=\frac{c_4}{e(c_1^{H(ID_i)/\mathcal{P}}c_2^{r_t},K_i)e(c_3^{H(T)+r_t},K)},$$

其中,$c_3=c_3'\oplus\mathcal{H}(e(c_2,K'))$

3.2　安全性证明

$\text{PKTRSE}_{\text{OMI}}$是一种非交互式、抗自适应选择明文攻击、带有随机预言机的安全方案.

定理 1　若(t,q,ε) – DBDHI 假设在 G_1 上成立,则上述方案 $\text{PKTRSE}_{\text{OMI}}$,对于任意 $q_s<q-1$ 与 $t'<t-o(t)$,是$(t',q_s,\varepsilon^2/e)$-IND-sID-T-CPA1 安全的.

证明　易知,敌手 $\mathcal{A}$ 成功攻击 $\text{PKTRSE}_{\text{OMI}}$ 系统,当且仅当 G 破解任一授权用户的私钥 usk_i 与时间服务器的私钥 ts_{priv}. 下文我们将把 usk_i 与 ts_{priv}的安全性归约到 q-DBDHI 问题. 因此,如果我们假设 $\mathcal{A}$ 攻击 usk_i 或 ts_{priv} 拥有优势 ε,则 $\mathcal{A}$ 成功攻击 $\text{PKTRSE}_{\text{OMI}}$ 系统拥有优势 ε^2/e. 我们构建挑战者算法 $\mathcal{B}$,$\mathcal{B}$ 使用 $\mathcal{A}$ 解决 q-DBDHI 问题. $\mathcal{B}$ 的输入是:随机的$(q+2)$-元组$(g,g^{\alpha},\cdots,g^{\alpha^q},\mathrm{T})\in(G_1^*)^{q+1}\times G_2^*$ 与$(q+2)$-元组$(g,g^{\alpha'},\cdots,g^{(\alpha')^q},\mathfrak{T})\in(G_1^*)^{q+1}\times G_2^*$. 其中,随机数 $\alpha,\alpha'\in\mathbb{Z}_p^*$ 对于 $\mathcal{B}$ 是未知数. $\mathcal{B}$ 的目标输出是 1,如果 $\mathrm{T}=e(g,g)^{1/\alpha}$且 $\mathfrak{T}=e(g,g)^{1/\alpha'}$;否则,输出 0. $\mathcal{B}$ 以身份与解密时间可选的安全性游戏方式与 $\mathcal{A}$ 进行交互如下:

Preparation　$\mathcal{B}$ 选取随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,构造生成元 $h\in G_1^*$,$q-2$ 对$(m_i,h^{1/\alpha m_i})$;选取随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,构造生成元 $h\in G_1^*$,$q-2$ 对$(m_i,h^{1/\alpha' m_i})$. 具体如下:

(1)选取一组随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,并生成多项式 $f(z)=\prod_{i=1}^{q-2}(z+m_i)$,对其计算展开,可得 $f(z)=\sum_{i=0}^{q-2}c_iz^i$. 其中,常量 $c_0\neq 0$.

(2)计算 $h=\prod_{i=1}^{q-1}(g^{(\alpha^i)})^{c_{i-1}}=g^{\alpha f(\alpha)}$,$v=\prod_{i=1}^{q-1}(g^{(\alpha^{i+1})})^{c_{i-1}}=g^{\alpha^2 f(\alpha)}$. 显然,$v=h^{\alpha}$.

(3)确认 $h\in G_1^*$. 如果 $h\in G_1$,且 $h=1$,则表明至少存在某一 $m_j=-\alpha$,从而 $\mathcal{B}$ 直接在游戏中胜出. 因此,我们假设所有的 $m_j\neq-\alpha$.

(4)对任一 $i=1,\cdots,q-2$,$\mathcal{B}$ 可轻易构造出二元组$(m_i,h^{1/\alpha m_i})$. $\mathcal{B}$ 可令 $f_i(z)=\frac{\alpha f(z)}{\alpha m_i}=\frac{f(z)}{m_i}=\sum_{j=0}^{q-2}\frac{c_j}{m_j}z^j=\sum_{j=0}^{q-2}d^jz^j$,则可得 $h^{\frac{1}{\alpha m_i}}=h^{\frac{\alpha f(\alpha)}{\alpha m_i}}=h^{f_i(\alpha)}=\prod_{j=0}^{q-2}(g^{(\alpha^j)})^{d^j}$.

(5)$\mathcal{B}$ 计算 $\mathrm{T}_h=\mathrm{T}^{c'}\mathrm{T}_0$,其中 $\mathrm{T}_0=\prod_{i=0}^{q-2}\prod_{j=0}^{q-3}e(g^{(\alpha^i)},g^{(\alpha^j)})^{c_ic_{j+1}}$. 若 $c=f(\alpha)$且 $\mathrm{T}=e(g,g)^{1/\alpha}$,则 $\mathrm{T}_h=e(g^{f(\alpha)/\alpha},g^{f(\alpha)})=e(h,h)^{1/\alpha}$;若 T 均匀分布于 G_2^*,则 T_h 均匀分布于 $G_2\backslash\{\mathrm{T}_0\}$.

类似地,$\mathcal{B}$ 选取随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,构造生成元 $h=\prod_{i=1}^{q-1}(g^{(\alpha')^i})^{c'_{i-1}}=g^{\alpha' f'(\alpha')}$,随机选取 $\mathfrak{T}$,计算产生 $\sigma=h^{\alpha'}$,$q-2$ 对$(m_i,h^{1/\alpha' m_i})$,$\mathfrak{T}_h$. 其中,如果 $c'=f'(\alpha')$且 $\mathfrak{T}=e(g,g)^{1/\alpha'}$,则 $\mathfrak{T}_h=e(h,h)^{1/\alpha'}$.

最后,$\mathcal{B}$ 输出 $h,v,\mathrm{T}_h,(m_i,h^{1/\alpha m_i}),\sigma,\mathfrak{T}_h,(m_i,h^{1/\alpha' m_i})$,其中 $i=1,\cdots,q-2$.

Initialization　$\mathcal{A}$ 输出其试图攻击对象:一授权用户集合 $U^*=\{u_j^*\mid u_j^*=ID_j^*,j=1,\cdots,N\}$ 与一解密时间 T^*.

Setup　$\mathcal{B}$ 生成 *MPK* 与 ts_{pub},执行下述操作:

(1)选取随机数 $a\in\mathbb{Z}_p^*$,令 $b=\mathcal{P}=\prod_{j=1}^{N}H(ID_j^*)$.

(2)计算 $X=v^{ab}=h^{\alpha ab}$,$Y=v=h^{\alpha}$,$ts_{\text{pub}}=v=h^{\alpha'}$. 在 $\mathcal{A}$ 的角度,X,Y 与 U^* 不相关,ts_{pub}与 T^* 不相关.

(3)公开 $params=(h,MPK,ts_{\text{pub}})$作为公共参数.

(4)$\mathcal{B}$ 间接定义了 $x=\alpha ab$,$y=\alpha$,使得 $X=h^x$,$Y=h^y$;$s=\alpha'$,使得 $ts_{\text{pub}}=h^s$. 但同时 x,y,s 对 $\mathcal{B}$ 是未知数.

$\mathcal{H}$-queries. $\mathcal{A}$ 可随时向随机预言机 $\mathcal{H}$ 发起查询. 作为响应,$\mathcal{B}$ 维护一 4 元组$(T_j,\mathsf{h}_j,w_j,b_j)$的 $\mathcal{H}$ 表. $\mathcal{H}$ 表初

始为空表. 当 $\mathcal{A}$ 查询 $T_i \neq T^*$ 时,$\mathcal{B}$ 执行下述操作之一:

(1)T_i 未被查询过. G 生成随机数 $b_i \in \{0,1\}$,且使 $\Pr[b_i=0]=1/(q-1)$. $\mathcal{B}$ 选取随机数 $w_i \in \mathbb{Z}_p$,若 $b_i=0$,则 $\mathcal{B}$ 计算 $\mathsf{h}_i = \psi h^{w_i}$;否则,$\mathcal{B}$ 计算 $\mathsf{h}_i = h^{w_i} \in G_1$. $\mathcal{B}$ 添加 $(T_i, \mathsf{h}_i, w_i, b_i)$ 至 $\mathcal{H}$ 表,并输出 $\mathcal{H}(T_i)=\mathsf{h}_i$ 至 $\mathcal{A}$.

(2)T_i 已被查询过. $\mathcal{B}$ 输出 $\mathcal{H}(T_i)=\mathsf{h}_i$ 至 $\mathcal{A}$.

Phase 1 敌手 $\mathcal{A}$ 发起 $q_s < q-1$ 次用户私钥与时间陷门查询. 当 $\mathcal{A}$ 发起第 i 次查询 $ID_i \notin U^*$ 对应的私钥与 $T_i \neq T^*$ 对应的陷门时,需以私钥 $(r_i, h^{1/(\mathcal{H}(ID_i)x+r_iy)})$ 与陷门 $(r_{\mathsf{t}}, h^{1/(sH(T_i)+r_{\mathsf{t}})}, \psi, \mathcal{H}(T_i)^s)$ 作为响应. 其中,r_i 与 r_{t} 均匀分布于 $\mathbb{Z}_p^*$. 另外,为便于表述,我们将时间陷门包括的 3 项,前两项记为 S_{T1},第 3 项记为 S_{T2}. 算法 $\mathcal{B}$ 响应查询请求如下:

(1)令 $(m_i, h^{1/\alpha m_i})$ 与 $(\psi_{m_i}, h^{1/\alpha' m_i})$ 是 Preparation 阶段产生的第 i 对二元组. 定义 $h_i = h^{1/\alpha m_i}$ 与 $\hbar_i = h^{1/\alpha' m_i}$.

(2)$\mathcal{B}$ 构造 $r_i, r_{\mathsf{t}} \in \mathbb{Z}_p^*$,满足 $r_i \alpha m_i = H(ID_i)x + r_i y$ 与 $r_{\mathsf{t}} \alpha' m_i = s(H(T_i)+r_{\mathsf{t}})$,将 x, y, s_1, s_2 的值代入两式可得:$r_i \alpha m_i = H(ID_i)\alpha ab + r_i \alpha$,$r_{\mathsf{t}} \alpha' m_i = \alpha'(H(T_i)+r_{\mathsf{t}})$. 显然,未知数 α 与 α' 将会被约简掉;且可得 $r_i = H(ID_i)ab/(m_i-1)$,$r_{\mathsf{t}} = H(T_i)/(\psi_{m_i}-1)$.

(3)$\mathcal{B}$ 将 ID_i 对应私钥 $(r_i, h_i^{1/r_i})$ 与 T_i 对应 $S_{T,1} = (r_{\mathsf{t}}, \hbar_i^{1/r_i})$ 作为对 $\mathcal{A}$ 查询请求的响应. $(r_i, h_i^{1/r_i})$ 是 ID_i 对应的合法私钥,理由是:① $h_i^{1/r_i} = (h^{1/\alpha m_i})^{1/r_i} = h^{1/r_i \alpha m_i} = h^{1/(\mathcal{H}(ID_i)x+r_iy)}$;②由于 m_i 均匀分布于 $\mathbb{Z}_p^* / \{-\alpha\}$,因此 r_i 均匀分布于 $\mathbb{Z}_p^*$. 其中 r_i 需满足 $\mathcal{H}(ID_i)x + r_i y \neq 0 \pmod p$. 同理,可知 $(r_{\mathsf{t}}, \mathsf{h}_i^{1/r_i})$ 是时间 T_i 对应的合法 $S_{T,1}$.

(4)$\mathcal{B}$ 从 $\mathcal{H}$ 表中取出 T_i 对应的 $(T_i, \mathsf{h}_i, w_i, b_i)$. 如果 $b_i=0$,则 $\mathcal{B}$ 报错,整个游戏在此处终止;否则,说明 $\mathsf{h}_i = h^{w_i} \in G_1$. $\mathcal{B}$ 输出 $(ts_{\text{pub}})^{w_i}$ 至 $\mathcal{A}$. 由于 $(ts_{\text{pub}})^{w_i} = h^{sw_i} = h^{ws} = \mathcal{H}(T_i)^s$,说明 $(ts_{\text{pub}})^{w_i}$ 是与 T_i 对应的合法 S_{T2}.

Challenge $\mathcal{A}$ 输出两对明文,$\mathcal{B}$ 响应如下:

(1)检索阶段,$e(E^{H(ID_i)/\wp}F, L) = \mathcal{E} \Leftrightarrow \dfrac{\mathcal{E}\mathcal{M}}{e(E^{H(ID_i)/\wp}F, L)} = \mathcal{M}$,当且仅当 T_W 合法. 由上式可将检索阶段的测试转化为下述挑战方式. $\mathcal{A}$ 输出两组明文 $\mathcal{M}_0, \mathcal{M}_1 \in G_2$. $\mathcal{B}$ 以如下方式对 $\mathcal{A}$ 响应. 首先,选择随机数 $\mathcal{b} \in \{0,1\}$ 与 $\mathcal{l} \in \mathbb{Z}_p^*$;其次,输出密文 $\mathcal{C} = (h^{ab^2\mathcal{l}/H(W)}, \mathbf{T}_h^{\mathcal{l}} \mathcal{M}_{\mathcal{b}})$;然后,定义 $k_3 = \mathcal{l}/\alpha \in \mathbb{Z}_p^*$. 若 $\mathbf{T}_h = e(h,h)^{1/\alpha}$,我们有:

$$h^{ab^2\mathcal{l}/H(W)} = h^{\alpha ab k_3 \wp/H(W)} = X^{k_3 \wp/H(W)},$$

$$\mathbf{T}_h^{\mathcal{l}} = e(h,h)^{\mathcal{l}/\alpha} = e(h,h)^{k_3}$$

显然,$\mathcal{C}$ 是在 U^*, k_3 下明文 $\mathcal{M}_{\mathcal{b}}$ 的合法密文. 其中,k_3 均匀分布于 $\mathbb{Z}_p^*$. 如果 $\mathbf{T}_h$ 均匀分布于 $G_2 \backslash \{\mathbf{T}_0\}$,则对 $\mathcal{A}$ 而言,密文 $\mathcal{C}$ 独立于 $\mathcal{b}$.

(2)解密阶段,$\mathcal{A}$ 输出两组明文 $M_0, M_1 \in G_2$. $\mathcal{B}$ 以如下方式对 $\mathcal{A}$ 响应. 首先,选择随机数 $\mathsf{b} \in \{0,1\}$,$l, l' \in \mathbb{Z}_p^*$;其次,输出密文 $(C, T^*) = ((h^{ab^2l}, h^l, h^{l'} \oplus \mathcal{H}(e(\psi^l, \mathcal{H}(T^*)))), \mathbf{T}_h^l \mathfrak{T}_h^{l'} M_b), T^*)$;然后,定义 $k_1 = l/\alpha \in \mathbb{Z}_p^*$ 与 $k_2 = l'/\alpha' \in \mathbb{Z}_p^*$. 如果 $\mathbf{T}_h = e(h,h)^{1/\alpha}$ 且 $\mathfrak{T}_h = e(h,h)^{1/\alpha'}$,我们有:

$$h^{ab2l} = h^{\alpha ab k_1 \wp} = X^{k_1 \wp} \qquad h^{l'} = h^{\alpha' k_2} = (ts_{\text{pub}})^{k_2}$$

$$h^l = h^{\alpha k_1} = Y^{k_1} \qquad \psi^l = h^{\alpha' \alpha k_1} = (ts_{\text{pub}})^{\gamma k_1}$$

$$\mathbf{T}_h^l = e(h,h)^{l/\alpha} = e(h,h)^{k_1} \qquad \mathfrak{T}_h^{l'} = e(h,h)^{l'/\alpha'} = e(h,h)^{k_2}$$

显然,(C, T^*) 是在 U^*, T^*, k_1, k_2 下明文 M_b 的合法密文. 其中,k_1, k_2 均匀分布于 $\mathbb{Z}_p^*$. 如果 $\mathbf{T}_h$ 均匀分布于 $G_2 \backslash \{\mathbf{T}_0\}$ 且 $\mathbf{T}_h$ 均匀分布于 $G_2 \backslash \{\mathbf{T}_0\}$,则对 $\mathcal{A}$ 而言,密文 (C, T^*) 独立于 b.

Phase 2 $\mathcal{A}$ 发起另外的至多 $q_s < q-1$ 次私钥与时间陷门查询;$\mathcal{B}$ 以之前相同方式响应.

Guess $\mathcal{A}$ 输出对 $\mathcal{b}, \mathsf{b}$ 的猜测 $\mathcal{b}', \mathsf{b}' \in \{0,1\}$. 如果 $\mathcal{b} = \mathcal{b}', \mathsf{b} = \mathsf{b}'$,$\mathcal{B}$ 输出 1;否则,$\mathcal{B}$ 输出 0.

上述安全游戏表明,当输入的 c, c' 满足 $c = f(\alpha)$,$c' = f'(\alpha')$,且 $\mathbf{T}, \mathfrak{T}$ 满足 $\mathbf{T} = e(g,g)^{1/\alpha}$,$\mathfrak{T} = e(g,g)^{1/\alpha'}$ 时;则有 $\mathbf{T}_h = e(h,h)^{1/\alpha}$,$\mathfrak{T}_h = e(h,h)^{1/\alpha'}$. 在此情况下,$\mathcal{B}$ 以概率 1 构造出合法密文;进而,敌手 $\mathcal{A}$ 才能使用其优势猜测 $\mathcal{b}, \mathsf{b}$ 的值. 由于 $\mathcal{A}$ 猜中 $\mathcal{b}$ 值的优势等价于 $\mathcal{A}$ 构造出 $\mathbf{T}_h^{\mathcal{l}}$,而 $\Pr[\mathcal{A}\text{构造出}\mathbf{T}_h^{\mathcal{l}}] \geq \varepsilon + (\varepsilon+1)/(p-1) \geq \varepsilon$;$\mathcal{A}$ 猜中 b 值的优势等价于 $\mathcal{A}$ 同时构造出 $\mathbf{T}_h^l$ 与 $\mathfrak{T}_h^{l'}$,而 $\Pr[\mathcal{A}\text{构造出}\mathbf{T}_h^{\mathcal{l}}] = \Pr[\mathcal{A}\text{构造出}\mathfrak{T}_h^{l'}] \geq \varepsilon + (\varepsilon+1)/(p-1) \geq \varepsilon$,$\Pr[\mathcal{A}\text{构造出}\mathbf{T}_h^l \mid \mathcal{A}\text{构造出}\mathbf{T}_h^{\mathcal{l}}] = 1$,且 $\mathbf{T}_h^{\mathcal{l}}, \mathbf{T}_h^l$ 都与 $\mathfrak{T}_h^{l'}$ 相互独立. 由此可得 $\Pr[\mathcal{A}(\mathcal{b}=\mathcal{b}', \mathsf{b}=\mathsf{b}')] - 1/4 \geq \varepsilon^2$,即 $\mathcal{A}$ 猜中 $\mathcal{b}, \mathsf{b}$ 值的优势至少为 ε^2. 当输入的 $\mathbf{T}, \mathfrak{T}$ 均匀分布于 G_2^*,则有 $\mathbf{T}_h$ 均匀分布于 $G_2 \backslash \{\mathbf{T}_0\}$,$\mathfrak{T}_h$ 均匀分布于 $G_2 \backslash \{\mathfrak{T}_0\}$. 在此情况下,$\mathcal{B}$ 以概率 $\dfrac{1}{p^2} \approx 0$ 构造出合法密文;进而,可认为 $\mathcal{A}$ 不能使用其优势猜测 $\mathcal{b}, \mathsf{b}$ 值,由此可得 $\Pr[\mathcal{A}(\mathcal{b}=\mathcal{b}', \mathsf{b}=\mathsf{b}')] - 1/4 = 0$. 综上,当 α 与 α' 均匀分布于 $\mathbb{Z}_p^*$,$\mathbf{T}$ 与 $\mathfrak{T}$ 均匀分布于 G_2^*,我们有

$$\begin{aligned}&\Pr[\mathcal{B}(g, g^{\alpha}, \cdots, g^{\alpha^q}, e(g,g)^{1/\alpha}) \\ &= 0 \cap \mathcal{B}(g, g^{\alpha'}, \cdots, g^{(\alpha')^q}, e(g,g)^{1/\alpha'}) = 0] \\ &- \Pr[\mathcal{B}(g, g^{\alpha}, \cdots, g^{\alpha^q}, \mathbf{T}) \\ &= 0 \cap \mathcal{B}(g, g^{\alpha'}, \cdots, g^{(\alpha')^q}, \mathfrak{T}) = 0] \geq (1/4 + \varepsilon^2) - 1/4 = \varepsilon^2\end{aligned}$$

另外,在 S_{T2} 的查询中,游戏不终止的可能性至少为 $1/e$[2](e 为自然对数的底). 因此,$\mathcal{B}$ 使用 $\mathcal{A}$ 同时解决两个不相关的 q-DBDHI 问题的优势至少是 ε^2/e.

3.3 方案优点与不足

$\text{PKTRSE}_{\text{OMI}}$ 方案的主要优点:(1)用户公私钥与密

文规模都为 $O(1)$;(2)减少了对管理员的安全依赖;(3)用户可匿名访问云服务器,但不能做到终端匿名. 主要不足:(1)授权用户组所有成员私钥都由管理员产生,管理员计算负担重;(2)只有管理员才能作为发送者发送消息,使得此方案只适用于电子多媒体杂志等应用场景. 下文给出解决上述问题的方案 $\mathrm{PKTRSE}_{\mathrm{OM2}}$.

4 $\mathrm{PKTRSE}_{\mathrm{OM2}}$方案

本节提出使用基于身份的公钥基础设施系统(Public Key Infrastructure System Based on Identity, PKISI)的构造方案 $\mathrm{PKTRSE}_{\mathrm{OM2}}$,并给出其在 CPA1 攻击模型下的安全性证明. 该方案更注重可用性.

4.1 方案表述

$\mathrm{PKTRSE}_{\mathrm{OM2}}$方案工作过程包括如下 10 个阶段:

Ini. 时间服务器和 PKISI 系统分别生成并公开通用系统参数.

时间服务器选择安全参数 $k \in \mathbb{Z}^+$,并执行下述操作:

(1)输入 k 并生成素数 p. 令 G_1 与 G_2 是阶为素数 p 的乘法群,$e: G_1 \times G_1 \to G_2$ 是一可容许的双线性映射,$g \in G_1$ 是任一生成元.

(2)选择 hash 函数 $H: \{0,1\}^* \to \mathbb{Z}_p^*$.

(3)公开通用系统参数 $ts_g = <p, G_1, G_2, g, e, H>$.

PKISI 系统选择安全参数 $k' \in \mathbb{Z}^+$,并执行下述操作:

(1)输入 k'并生成素数 p. 令 $\mathcal{G}_1$ 与 $\mathcal{G}_2$ 是阶为素数 p 的乘法群,$\boldsymbol{e}: \mathcal{G}_1 \times \mathcal{G}_1 \to \mathcal{G}_2$ 是一可容许的双线性映射,$\boldsymbol{g} \in \mathcal{G}_1$ 是任一生成元.

(2)选择 hash 函数 $\mathcal{H}: \{0,1\}^* \to \mathbb{Z}_p^*$.

(3)为生成 IBBE 参数,选择随机数 $x, y \in \mathbb{Z}_p^*$,并定义 $X = \boldsymbol{g}^x$,$Y = \boldsymbol{g}^y$. 生成主公钥 $MPK = (X, Y)$ 与主私钥 $MSK = (x, y)$.

(4)公开通用系统参数 $pkisi_g = <\mathrm{p}, \mathcal{G}_1, \mathcal{G}_2, \boldsymbol{g}, \boldsymbol{e}, \mathcal{H}, MPK>$.

Setup $(\mathrm{p}, \mathcal{H})$. 用户组管理员执行下述操作:

(1)确定授权用户集合 $U = \{u_j \mid u_j = ID_j, j = 1, \cdots, N\}$.

(2)计算所有组内成员的公钥积 $\mathcal{P}$,并将其公开.

(3)生成随机数 $r \in \mathbb{Z}_p^*$,并将其以某种安全方式(比如,分别使用各用户的公钥对其加密)分发给各授权用户.

KeyGen$(pkisi_g)$. 该阶段包括下述操作:

(1)每一授权用户计算生成其自身公钥,并发送至 PKISI 系统. 具体地,对于任一用户 u_j,其公钥 $upk_j = \mathcal{H}(ID_j)$.

(2)PKISI 系统收到用户身份公钥后,计算生成所有授权用户的私钥. 具体地,对于任一用户 u_j,挑选一随机数 $r_j \in \mathbb{Z}_p^*$,计算 $K_j = \boldsymbol{g}^{1/(\mathcal{H}(ID_j)x + r_j y)} \in \mathcal{G}_1^*$,得私钥 $usk_j = (r_j, K_j)$. 如果 $\mathcal{H}(ID_j)x + r_j y = 0 \pmod p$,则重选 r_j.

(3)通过某种安全方式将各私钥分发至相应用户.

TRSetup. 时间服务器选取两个随机数 $s_1, s_2 \in \mathbb{Z}_p^*$,并定义 $\mathrm{S} = g^{s_1}$,$\mathcal{S} = g^{s_2}$. 保密其私钥 $ts_{\mathrm{priv}} = (s_1, s_2)$,公开其公钥 $ts_{\mathrm{pub}} = (\mathrm{S}, \mathcal{S})$.

Enc$(ts_g, pkisi_g, \mathcal{P}, r, ts_{\mathrm{pub}}, M, T)$. 发送者选取随机数 $k_1 \in \mathbb{Z}_p^*$,$k_2 \in \mathbb{Z}_p^*$,加密一组消息 $M \in \mathcal{G}_2$;输出密文 $C = (c_1', c_2, c_3, c_4, c_5)$,其中,$c_1 = X^{k_1 \mathcal{P}}$,$c_1' = c_1 \oplus X^{rH(T)}$,$c_2 = Y^{k_1}$,$c_3 = S^{k_2 H(T)} \mathcal{S}^{k_2}$,$c_4 = S^{k_2}$,$c_5 = \boldsymbol{e}(\boldsymbol{g}, \boldsymbol{g})^{k_1} e(g, g)^{k_2} M$.

KwTag$(pkisi_g, r, W)$. 发送者生成关键词标签 $KWT = (F, \mathcal{T})$,其中,$F = X^{r/(W)}$,$\mathcal{T} = \boldsymbol{e}(\boldsymbol{g}, \boldsymbol{g})^r$.

KwTrd$(pkisi_g, r, usk_i, W)$. 当任一授权用户 u_i 检索包含关键词 W 的密文时,使用其私钥生成对应陷门 $T_W = (F', L, Q)$,并发送至云服务器. 其中,$F' = X^{(r - \mathcal{H}(ID_i))/\mathcal{H}(W)}$,$L = Y^{r/\mathcal{H}(W)}$,$Q = K_i^{r\mathcal{H}(W)}$.

Search(KWT, T_W). 当云服务器收到检索请求时,测试等式 $\boldsymbol{e}(\frac{FL}{F'}, Q) = \mathcal{T}$ 是否成立. 如果成立,则找到了目标密文 C,允许请求者下载(C, T);否则,拒绝其下载任何内容.

RtTrd(ts_{priv}, T). 时间服务器生成并发布每一时间点的陷门 S_T. 对于时间点 T,$S_T = (r_t, K)$,其中,随机数 $r_t \in \mathbb{Z}_p^*$,$K = g^{1/(H(T)s_1 + s_2 + r_t s_1)} \in G_1^*$. 如果 $H(T)s_1 + s_2 + r_t s_1 = 0 \pmod p$,则重选 r_t.

Dec$(ts_g, pkisi_g, usk_i, \mathcal{P}, r, S_T, C)$. 任一授权用户 u_i 在发送者指定的解密时间达到之后,使用其私钥与时间服务器发布的对应 S_T 解密密文;输出明文

$$M = \frac{c_5}{\boldsymbol{e}(c_1^{\mathcal{H}(ID_i)/\mathcal{P}} c_2^{r_i}, K_i)\, e(c_3 c_4^{r_i}, K)}$$,其中,$c_1 = c_1' \oplus X^{rH(T)}$

4.2 安全性证明

$\mathrm{PKTRSE}_{\mathrm{OM2}}$是一种非交互式、抗自适应选择明文攻击、标准模型下安全的方案.

定理 2　若(t, q, ε)-DBDHI 假设在 G_1 与 $\mathcal{G}_1$ 上成立,则上述方案 $\mathrm{PKTRSE}_{\mathrm{OM2}}$,对于任意 $q_s < q - 1$ 与 $t' < t - o(t)$,是(t', q_s, ε^2)-IND-sID-T-CPA1 安全的.

证明　易知,敌手 $\mathcal{A}$ 成功攻击 $\mathrm{PKTRSE}_{\mathrm{OM2}}$ 系统,当且仅当 $\mathcal{A}$ 破解任一授权用户的私钥 usk_i 与时间服务器的私钥 ts_{priv}. 下文我们将把 usk_i 与 ts_{priv}的安全性归约到 q-DBDHI 问题. 因此,如果我们假设 $\mathcal{A}$ 攻击 usk_i 或 ts_{priv} 拥有优势 ε,则 $\mathcal{A}$ 攻击 $\mathrm{PKTRSE}_{\mathrm{OM2}}$ 系统拥有优势 ε^2. 我

们构建挑战者算法 $\mathcal{B}$,$\mathcal{B}$ 使用 $\mathcal{A}$ 解决 q-DBDHI 问题. $\mathcal{B}$ 的输入是:随机的 $(q+2)$ - 元组 $(\boldsymbol{g},\boldsymbol{g}^{\alpha},\cdots,\boldsymbol{g}^{\alpha^q},\mathrm{T})\in(\mathcal{G}_1^*)^{q+1}\times\mathcal{G}_2^*$ 与 $(q+2)$ - 元组 $(g,g^{\alpha'},\cdots,g^{(\alpha')^q},\mathfrak{T})\in(G_1^*)^{q+1}\times G_2^*$. 其中,随机数 $\alpha\in\mathbb{Z}_p^*,\alpha'\in\mathbb{Z}_p^*$ 对于 $\mathcal{B}$ 是未知数. $\mathcal{B}$ 的目标输出是 1,如果 $\mathrm{T}=\boldsymbol{e}(\boldsymbol{g},\boldsymbol{g})^{1/\alpha}$ 且 $\mathfrak{T}=e(g,g)^{1/\alpha'}$;否则,输出 0. $\mathcal{B}$ 以身份与解密时间可选的安全性游戏方式与 $\mathcal{A}$ 进行交互如下:

Preparation 类似于方案 $\mathrm{PKTRSE}_{\mathrm{OMI}}$ 安全证明中所述. $\mathcal{B}$ 选取随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,构造生成元 $h\in\mathcal{G}_1^*$,随机选取 T,计算产生 $v=h^{\alpha},q-2$ 对 $(m_i,h^{1/\alpha m_i})$,T_h;选取随机数 $m_1,\cdots,m_{q-2}\in\mathbb{Z}_p^*$,构造生成元 $k\in G_1^*$,随机选取 $\mathfrak{T}$,计算产生 $\sigma=k^{\alpha'},q-2$ 对 $(m_i,k^{1/\alpha' m_i})$,$\mathfrak{T}_k$. 最后,$\mathcal{B}$ 输出 $h,v,\mathrm{T}_h,(m_i,h^{1/\alpha m_i}),k,\sigma,\mathfrak{T}_k,(m_i,k^{1/\alpha' m_i})$,其中,$i=1,\cdots,q-2$.

Initialization $\mathcal{A}$ 输出其试图攻击对象:一授权用户集合 $U^*=\{u_j^*\mid u_j^*=ID_j^*,j=1,\cdots,N\}$ 与一解密时间 T^*.

Setup $\mathcal{B}$ 生成 MPK 与 ts_{pub},执行下述操作:

(1)选取随机数 $a_1\in\mathbb{Z}_p^*,a_2\in\mathbb{Z}_p^*$;令 $b_1=\mathcal{P}=\prod_{j=1}^{N}\mathcal{H}(ID_j^*)$,$b_2=H(T^*)$.

(2)计算 $X=v^{a_1b_1}=h^{\alpha a_1b_1}$,$Y=v=h^{\alpha}$,$\mathrm{S}=\sigma^{a_2b_2}=k^{\alpha' a_2b_2}$,$\mathcal{S}=\sigma=k^{\alpha'}$. 在敌手 $\mathcal{A}$ 的角度,X,Y 与 U^* 不相关,$\mathrm{S},\mathcal{S}$ 与 T^* 不相关.

(3)公开 $params=(h,k,MPK,ts_{\mathrm{pub}})$ 作为公共参数.

(4)$\mathcal{B}$ 间接定义了 $x=\alpha a_1b_1,y=\alpha$,使得 $X=h^x,Y=h^y$;$s_1=\alpha' a_2b_2,s_2=\alpha'$,使得 $\mathrm{S}=k^{s_1},\mathcal{S}=k^{s_2}$. 但同时 x,y,s_1,s_2 对 $\mathcal{B}$ 是未知数.

Phase 1 $\mathcal{A}$ 发起 $q_s<q-1$ 次用户私钥与时间陷门查询. 当 $\mathcal{A}$ 发起第 i 次查询 $ID_i\notin U^*$ 对应的私钥与 $T_i\neq T^*$ 对应的陷门,需以私钥 $(r_i,h^{1/(\mathcal{H}(ID_i)x+r_iy)})$ 与陷门 $(r_{\mathrm{t}},k^{1/(H(T_i)s_1+s_2+r_{\mathrm{t}}s_1)})$ 作为响应,其中,r_i 与 r_{t} 分别均匀分布于 $\mathbb{Z}_p^*$ 与 $\mathbb{Z}_p^*$. $\mathcal{B}$ 响应查询请求如下:

(1)令 $(m_i,h^{1/\alpha m_i})$ 与 $(m_i,k^{1/\alpha' m_i})$ 是 Preparation 阶段产生的第 i 对二元组. 定义 $h_i=h^{1/\alpha m_i}$ 与 $k_i=k^{1/\alpha' m_i}$.

(2)$\mathcal{B}$ 构造 $r_i\in\mathbb{Z}_p^*$ 与 $r_{\mathrm{t}}\in\mathbb{Z}_p^*$,满足 $r_i\alpha m_i=\mathcal{H}(ID_i)x+r_iy$ 与 $r_{\mathrm{t}}\alpha' m_i=H(T_i)s_1+s_2+r_{\mathrm{t}}s_1$. 将 x,y,s_1,s_2 的值代入两式可得:$r_i\alpha m_i=\mathcal{H}(ID_i)\alpha a_1b_1+r_i\alpha,r_{\mathrm{t}}\alpha' m_i=H(T_i)\alpha' a_2b_2$. 显然,未知数 α 与 α' 将会被约简掉;且可得 $r_i=\mathcal{H}(ID_i)a_1b_1/(m_i-1)$ 与 $r_{\mathrm{t}}=(H(T_i)a_2b_2+1)/(m_i-a_2b_2)$.

(3)$\mathcal{B}$ 将 ID_i 对应私钥 $(r_i,h_i^{1/r_i})$ 与 T_i 对应时间陷门 $(r_{\mathrm{t}},k_i^{1/r_{\mathrm{t}}})$ 作为对 $\mathcal{A}$ 查询请求的响应. $(r_i,h_i^{1/r_i})$ 是 ID_i 对应的合法私钥,理由是:① $h_i^{1/r_i}=(h^{1/\alpha m_i})^{1/r_i}=h^{1/r_i\alpha m_i}=h^{1/(\mathcal{H}(ID_i)x+r_iy)}$;②由于 m_i 均匀分布于 $\mathbb{Z}_p^*/\{-\alpha\}$,因此 r_i 均匀分布于 $\mathbb{Z}_p^*$. 其中 r_i 需满足 $\mathcal{H}(ID_i)x+r_iy\neq0(\mathrm{mod}\ p)$. 同理,可知 $(r_{\mathrm{t}},k_i^{1/r_{\mathrm{t}}})$ 是时间 T_i 对应的合法陷门.

Challenge $\mathcal{A}$ 输出两对明文,$\mathcal{B}$ 响应如下:

(1)检索阶段 $\boldsymbol{e}(\frac{FL}{F'},Q)=\mathcal{T}\Leftrightarrow\frac{\mathcal{T}M}{\boldsymbol{e}(\frac{\mathcal{T}L}{F'},Q)}=\mathcal{M}$,当且仅当 T_W 合法. 由上式可将检索阶段的测试转化为下述挑战方式. $\mathcal{A}$ 输出两组明文 $\mathcal{M}_0,\mathcal{M}_1\in G_2$. $\mathcal{B}$ 以如下方式对 $\mathcal{A}$ 响应. 首先,选择随机数 $\mathfrak{b}\in\{0,1\}$ 与 $\mathfrak{l}\in\mathbb{Z}_p^*$;其次,输出密文 $\mathcal{C}=(h^{a_1b_1\mathfrak{l}/H(W)},\mathfrak{T}_h^{\mathfrak{l}}\mathcal{M}_{\mathfrak{b}})$;然后,定义 $r=\mathfrak{l}/\alpha\in\mathbb{Z}_p^*$. 如果 $\mathfrak{T}_h=\boldsymbol{e}(h,h)^{1/\alpha}$,我们有:

$$h^{a_1b_1\mathfrak{l}/H(W)}=h^{\alpha a_1b_1r/H(W)}=X^{r/H(W)},$$

$$\mathfrak{T}_h^{\mathfrak{l}}=\boldsymbol{e}(h,h)^{\mathfrak{l}/\alpha}=\boldsymbol{e}(h,h)^{r}$$

显然,$\mathcal{C}$ 是在 U^*,r 下明文 $\mathcal{M}_{\mathfrak{b}}$ 的合法密文. 其中,r 均匀分布于 $\mathbb{Z}_p^*$. 如果 T_h 均匀分布于 $G_2\backslash\{\mathrm{T}_0\}$ 且 T_h 均匀分布于 $G_2\backslash\{\mathrm{T}_0\}$,则对 $\mathcal{A}$ 而言,密文 $\mathcal{C}$ 独立于 $\mathfrak{b}$.

(2)解密阶段 $\mathcal{A}$ 输出两组明文 $M_0,M_1\in G_2$. $\mathcal{B}$ 以如下方式对 $\mathcal{A}$ 响应. 首先,选择随机数 $\mathsf{b}\in\{0,1\},l\in\mathbb{Z}_p^*$ 与 $l'\in\mathbb{Z}_p^*$;其次,输出密文 $(C,T^*)=((h^{a_1b_1^2l}\oplus h^{a_1b_1lH(T^*)},h^l,k^{a_2b_2^2l'}k^{l'},k^{a_2b_2l'},\mathrm{T}_k^{l'}\mathfrak{T}_k^{l'}M_{\mathsf{b}}),T^*)$;然后,定义 $k_1=l/\alpha\in\mathbb{Z}_p^*$ 与 $k_2=l'/\alpha'\in\mathbb{Z}_p^*$. 如果 $\mathrm{T}_h=\boldsymbol{e}(h,h)^{1/\alpha}$ 且 $\mathfrak{T}_k=e(k,k)^{1/\alpha'}$,我们有:

$$h^{a_1b_1^2l}=h^{\alpha a_1b_1k_1\mathcal{P}}=X^{k_1P}\qquad k^{a_2b_2l'}=k^{\alpha' a_2b_2k_2}=\mathrm{S}^{k_2}$$

$$h^{a_1b_1lH(T^*)}=h^{\alpha a_1b_1rH(T^*)}=X^{rH(T^*)}\qquad \mathrm{T}_h^{l}=\boldsymbol{e}(h,h)^{l/\alpha}=\boldsymbol{e}(h,h)^{k_1}$$

$$h^l=h^{\alpha k_1}=Y^{k_1}\qquad \mathfrak{T}_k^{l'}=e(k,k)^{l'/\alpha'}=e(k,k)^{k_2}$$

$$k^{a_2b_2^2l'}k^{l'}=k^{\alpha' a_2b_2k_2H(T^*)}k^{\alpha' k_2}=\mathrm{S}^{k_2H(T^*)}\mathcal{S}^{k_2}$$

显然,(C,T^*) 是在 U^*,T^*,r,k_1,k_2 下明文 M_{b} 的合法密文. 其中,r,k_1 均匀分布于 $\mathbb{Z}_p^*$,k_2 均匀分布于 $\mathbb{Z}_p^*$. 如果 T_h 均匀分布于 $\mathcal{G}_2\backslash\{\mathrm{T}_0\}$ 且 $\mathfrak{T}_k$ 均匀分布于 $G_2\backslash\{\mathfrak{T}_0\}$,则对 $\mathcal{A}$ 而言,密文 (C,T^*) 独立于 b.

Phase 2 $\mathcal{A}$ 发起另外的至多 $q_s<q-1$ 次私钥与时间陷门查询;$\mathcal{B}$ 以之前相同方式响应.

Guess $\mathcal{A}$ 输出对 $\mathfrak{b},\mathsf{b}$ 的猜测 $\mathfrak{b}',\mathsf{b}'\in\{0,1\}$. 如果 $\mathfrak{b}=\mathfrak{b}',\mathsf{b}=\mathsf{b}'$,$\mathcal{B}$ 输出 1;否则,$\mathcal{B}$ 输出 0.

上述安全游戏表明,当输入的 c,c' 满足 $c=f(\alpha),c'=f'(\alpha')$,且 $\mathrm{T},\mathfrak{T}$ 满足 $\mathrm{T}=\boldsymbol{e}(\boldsymbol{g},\boldsymbol{g})^{1/\alpha},\mathfrak{T}=e(g,g)^{1/\alpha'}$ 时;则有 $\mathrm{T}_h=\boldsymbol{e}(h,h)^{1/\alpha},\mathfrak{T}_k=e(k,k)^{1/\alpha'}$. 在此情况下,$\mathcal{B}$ 以概率 1 构造出合法密文;进而,敌手 $\mathcal{A}$ 才能使用其优势猜测 $\mathfrak{b},\mathsf{b}$ 的值. 由于 $\mathcal{A}$ 猜中 $\mathfrak{b}$ 值的优势等价于 $\mathcal{A}$ 构造出 $\mathrm{T}_h^{\mathfrak{l}}$,而 $\Pr[\mathcal{A}\text{构造出}\mathrm{T}_h^{\mathfrak{l}}]\geq\varepsilon+(\varepsilon+1)/(p-1)\geq\varepsilon$;$\mathcal{A}$ 猜中 b 值的优势等价于 $\mathcal{A}$ 同时构造出 T_h^{l} 与 $\mathfrak{T}_k^{l'}$,而 $\Pr[\mathcal{A}\text{构造出}\mathrm{T}_h^{l}=\Pr[\mathcal{A}\text{构造出}\mathfrak{T}_k^{l'}]\geq\varepsilon+(\varepsilon+1)/(p-1)$

$\geq\varepsilon$,$\Pr[\mathcal{A}$ 构造出 $\mathbf{T}_h^{\prime}|\mathcal{A}$ 构造出 $\mathbf{T}_h^{\prime}]=1$,且 $\mathbf{T}_h^{\prime}$,$\mathbf{T}_h^{\prime}$ 都与 $\mathfrak{T}_{\ell}^{l'}$ 相互独立. 由此可得 $\Pr[\mathcal{A}(\ell=\ell',\mathrm{b}=\mathrm{b}')]-1/4\geq\varepsilon^2$,即 $\mathcal{A}$ 猜中 ℓ,b 值的优势至少为 ε^2. 当输入的 $\mathbf{T}$ 均匀分布于 $\mathcal{G}_2^*$ 且 $\mathfrak{T}$ 均匀分布于 G_2^*,则有 $\mathbf{T}_h$ 均匀分布于 $\mathcal{G}_2\backslash\{\mathbf{T}_0\}$ 且 $\mathfrak{T}_{\ell}$ 均匀分布于 $G_2\backslash\{\mathfrak{T}_0\}$. 在此情况下,$\mathcal{B}$ 以概率 $\frac{1}{p\mathrm{p}}\approx 0$ 构造出合法密文;进而,可认为 $\mathcal{A}$ 不能使用其优势去猜测 ℓ,b 值,由此可得 $\Pr[\mathcal{A}(\ell=\ell',\mathrm{b}=\mathrm{b}')]-1/4=0$. 综上,当 α 均匀分布于 $\mathbb{Z}_{\mathrm{p}}^*$,$\alpha'$ 均匀分布于 $\mathbb{Z}_p^*$,$\mathbf{T}$ 均匀分布于 $\mathcal{G}_2^*$,$\mathfrak{T}$ 均匀分布于 G_2^*,我们有

$$\begin{aligned}&\Pr[\mathcal{B}(\boldsymbol{g},\boldsymbol{g}^{\alpha},\cdots,\boldsymbol{g}^{\alpha^{\gamma}},\boldsymbol{e}(\boldsymbol{g},\boldsymbol{g})^{1/\alpha})\\&=0\cap\mathcal{B}(g,g^{\alpha'},\cdots,g^{(\alpha')^{\gamma}},e(g,g)^{1/\alpha'})=0]\\&-\Pr[\mathcal{B}(\boldsymbol{g},\boldsymbol{g}^{\alpha},\cdots,\boldsymbol{g}^{\alpha^{\gamma}},\mathbf{T})\\&=0\cap\mathcal{B}(g,g^{\alpha'},\cdots,g^{(\alpha')^{\gamma}},\mathfrak{T})=0]\geq(1/2+\varepsilon^2)-1/2=\varepsilon^2\end{aligned}$$

即,$\mathcal{B}$ 使用 $\mathcal{A}$ 同时解决两个不相关的 q-DBDHI 问题的优势至少是 ε^2.

4.3　方案优点与不足

$\mathrm{PKTRSE}_{\mathrm{OM2}}$方案的主要优点:(1)用户公私钥与密文规模都为 $O(1)$;(2)用户可匿名访问云服务器,但不能做到终端匿名;(3)管理员计算负担小. 主要不足:(1)在系统 Setup 建立阶段和取消对某些用户授权的情况下,需使用组内用户的公钥加密分发保密参数 r;(2)只有授权用户组成员才能作为发送者发送消息.

5　效率分析

方案 $\mathrm{PKTRSE}_{\mathrm{OM1}}$ 与 $\mathrm{PKTRSE}_{\mathrm{OM2}}$ 效率比较如表 1 所示. 采用 Canetti 等[16] 提出的增加一次签名操作可将 $\mathrm{PKTRSE}_{\mathrm{OM}}$ CPA 方案转换为 $\mathrm{PKTRSE}_{\mathrm{OM}}$ CCA 方案. $\mathrm{PKTRSE}_{\mathrm{OM}}$ CCA 方案中的时间控制加密操作部分与 $O(1)$的 TR-PRE[12] 方案效率比较如表 2 所示. 两表只统计相对比较耗时的 6 种基本操作 BP、$\mathrm{Exp}_{\mathrm{ec}}$、$\mathrm{Exp}_{\mathrm{dl}}$、Mtp、Sig 与 Ver 的运算次数. 其中,BP 表示双线性对运算,$\mathrm{Exp}_{\mathrm{ec}}$表示有限域椭圆曲线离散对数乘法群上的幂运算,$\mathrm{Exp}_{\mathrm{dl}}$表示有限域离散对数乘法群上的幂运算,Mtp 表示将任意长度的二进制串映射为有限域椭圆曲线离散对数乘法群上某一元素的 Hash 运算,Sig 表示签名操作,Ver 表示验证操作. 由于其他运算相对这 6 种运算耗时几乎可忽略,因此,未予统计. 另外,也未统计通用且可提前计算的基本操作.

表 1　方案 $\mathrm{PKTRSE}_{\mathrm{OM1}}$ 与 $\mathrm{PKTRSE}_{\mathrm{OM2}}$ 效率比较

方案	发送者	接收者	时间服务器	云服务器
$\mathrm{PKTRSE}_{\mathrm{OM1}}$	$\mathrm{BP}+5\ \mathrm{Exp}_{\mathrm{ec}}+2\ \mathrm{Exp}_{\mathrm{dl}}+2\mathrm{Mtp}$	$3\mathrm{BP}+5\ \mathrm{Exp}_{\mathrm{ec}}+\mathrm{Mtp}$	$2\ \mathrm{Exp}_{\mathrm{ec}}+\mathrm{Mtp}$	$\mathrm{BP}+\mathrm{Exp}_{\mathrm{ec}}$
$\mathrm{PKTRSE}_{\mathrm{OM2}}$	$7\mathrm{Exp}_{\mathrm{ec}}+3\ \mathrm{Exp}_{\mathrm{dl}}$	$2\mathrm{BP}+7\ \mathrm{Exp}_{\mathrm{ec}}$	$\mathrm{Exp}_{\mathrm{ec}}$	BP

表 2　与其他相关方案效率比较

方案	发送者加密	接收者解密	密文规模
TR-PRE[12]	$5\ \mathrm{Exp}_{\mathrm{ec}}+5\ \mathrm{Exp}_{\mathrm{dl}}+\mathrm{Sig}$	$5\mathrm{BP}+2\ \mathrm{Exp}_{\mathrm{ec}}+3\ \mathrm{Exp}_{\mathrm{dl}}+\mathrm{Ver}$	11 项
$\mathrm{PKTRSE}_{\mathrm{OM1}}$ CCA	$\mathrm{BP}+4\ \mathrm{Exp}_{\mathrm{ec}}+\mathrm{Exp}_{\mathrm{dl}}+2\mathrm{Mtp}+\mathrm{Sig}$	$3\mathrm{BP}+3\ \mathrm{Exp}_{\mathrm{ec}}+\mathrm{Mtp}+\mathrm{Ver}$	7 项
$\mathrm{PKTRSE}_{\mathrm{OM2}}$ CCA	$6\mathrm{Exp}_{\mathrm{ec}}+2\ \mathrm{Exp}_{\mathrm{dl}}+\mathrm{Sig}$	$2\mathrm{BP}+4\ \mathrm{Exp}_{\mathrm{ec}}+\mathrm{Ver}$	8 项

结合 Chalkias 等[9] 给出的前 4 种操作的运算耗时,由表 1 可知,方案 $\mathrm{PKTRSE}_{\mathrm{OM2}}$ 效率明显高于 $\mathrm{PKTRSE}_{\mathrm{OM1}}$. 分析表 2 可知:(1)$\mathrm{PKTRSE}_{\mathrm{OM2}}$ CCA 与 TR-PRE 方案的发送者加密代价基本相等,代价较小;(2)$\mathrm{PKTRSE}_{\mathrm{OM}}$ CCA 方案接收者解密代价和存储代价较小. 总之,方案 $\mathrm{PKTRSE}_{\mathrm{OM2}}$效率更高.

6　结论及未来工作

为解决多用户云加密存储问题,本文提出一种新的概念 $\mathrm{PKTRSE}_{\mathrm{OM}}$——一对多 PKTRSE. $\mathrm{PKTRSE}_{\mathrm{OM}}$模型中,发送者将加密的数据发送至云服务器,每一目标接收者提前检索带有特定关键词的密文,但不能解密,直到提前指定的未来解密时间到达. 论文给出 $\mathrm{PKTRSE}_{\mathrm{OM}}$ 方案模型及其安全游戏模型的形式化定义;提出基于 q-DBDHI 问题的两种安全方案,前者更注重安全性,后者更注重实用性;并分别给出两种方案是抗 IND-sID-T-CPA1 攻击的安全性证明. 效率分析表明,两种方案在执行过程中,都实现了计算、存储、传输规模与用户规模无关;和相关方案相比,$\mathrm{PKTRSE}_{\mathrm{OM2}}$具有更高效率. 不足之处,两种方案都主要适用于授权用户组成员稳定时间长的场景,或组成员虽更新频繁,但更新主要是增加用户的场景. 未来工作中,我们将使用代理重加密技术解决上述问题.

参考文献

[1] R L Rivest, A Shamir, D A Wagner. Time-lock puzzles and timed-release crypto, MIT/LCS/TR-684 [R/OL]. Cambridge, MA: MIT's Laboratory of Computer Science.

http://publications. csail. mit. edu/lcs/pubs/pdf/MIT-LCS-TR-684. pdf,1996 - 02 - 01.

[2] D Boneh, G D Crescenzo, R Ostrovsky, G Persiano. Public key encryption with keyword search[A]. Proceedings of the 23rd International Conference on Advances in Cryptology-Eurocrypt 2004[C]. Berlin: Springer, 2004. 506 - 522.

[3] K Yuan, Z Liu, C Jia, J Yang, S Lv. Public key timed-release searchable encryption[A]. Proceedings of the 4th IEEE International Conference on Emerging Intelligent Data and Web Technologies[C]. Piscataway, NJ: IEEE, 2013. 241 - 248.

[4] D Boneh, X Boyen. Efficient selective-id secure identity-based encryption without random oracles[A]. Proceedings of the 23rd International Conference on Advances in Cryptology-EUROCRYPT 2004 [C]. Berlin: Springer, 2004. 223 - 238.

[5] C Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys [A]. Proceedings of the 13th International Conference on Advances in Cryptology-ASIACRYPT 2007[C]. Berlin: Springer, 2007. 200 - 215.

[6] T May. Timed-release crypto [EB/OL]. http://www. cyphernet. org/cyphernomicon/chapter14/14. 5. html, 1993.

[7] 袁科,刘哲理,贾春福,马昊玉,吕述望. TRE 加密技术研究[J]. 计算机研究与发展,2014,51(6):1206 - 1220.
Yuan Ke, Liu Zhe-li, Jia Chun-fu, Ma Hao-yu, Lü Shu-wang. Research on timed-release encryption[J]. Journal of Computer Research and Development, 2014, 51(6): 1206 - 1220. (in Chinese)

[8] J Cathalo, B Libert, J-J Quisquater. Efficient and non-interactive timed-release encryption[A]. Proceedings of the 7th International Conference on Information and Communications Security[C]. Berlin: Springer, 2005. 291 - 303.

[9] K Chalkias, D Hristu-Varsakelis, G Stephanides. Improved anonymous timed-release encryption [A]. Proceedings of the 12th European Symposium on Computer Security-ESORICS 2007[C]. Berlin: Springer, 2007. 311 - 326.

[10] K Liang, Q Huang, R Schlegel, D S Wong, C Tang. A conditional proxy broadcast re-encryption scheme supporting timed-release [A]. Proceedings of the 9th International Conference on Information Security Practice and Experience[C]. Berlin: Springer, 2013. 132 - 146.

[11] K Emura, A Miyaji, K Omote. A timed-release proxy re-encryption scheme and its application to fairly-opened multicast communication [A]. Proceedings of the 4th International Conference on Provable Security [C]. Berlin: Springer, 2010. 200 - 213.

[12] K Emura, A Miyaji, K Omote. A timed-release proxy re-encryption scheme[J]. IEICE Trans on Fundamentals of Electronics, Communications and Computer Sciences, 2011, E94-A(8): 1682 - 1695.

[13] Y H Hwang, P J Lee. Public key encryption with conjunctive keyword search and its extension to a multi-user system[A]. Proceedings of the 1st International Conference on Pairing-Based Cryptography - Pairing 2007[C]. Berlin: Springer, 2007. 2 - 22.

[14] F Bao, R H Deng, X Ding, Y Yang. Private query on encrypted data in multi-user settings[A]. Proceedings of the 4th International Conference on Information Security Practice and Experience[C]. Berlin: Springer, 2008. 71 - 85.

[15] F Zhao, T Nishide, K Sakurai. Multi-user keyword search scheme for secure data sharing with fine-grained access control [A]. Proceedings of the 14th International Conference on Information Security and Cryptology-ICISC 2011[C]. Berlin: Springer, 2012. 406 - 418.

[16] R Canetti, S Halevi, J Katz. Chosen-ciphertext security from identity-based encryption [A]. Proceedings of the 23rd International Conference on Advances in Cryptology-Eurocrypt 2004[C]. Berlin: Springer, 2004. 207 - 222.

作者简介

袁 科 男,1982 年生,河南南阳人,博士,2014 年毕业于南开大学,现为河南大学副教授,主要研究方向:密码学、信息安全.
E-mail: yuanke_hhhh@163.com

刘哲理 男,1978 年生,山东潍坊人,副教授、博士后、硕士生导师,主要研究方向:密码学应用、信息安全.
E-mail: liuzheli@nankai.edu.cn

贾春福(通信作者) 男,1967 年生,河北文安人,教授、博士生导师,主要研究方向:信息安全与可信计算、恶意代码发现与分析.
E-mail: cfjia@nankai.edu.cn