doi:10.11959/j.issn.1000-436x.2015031

云环境下安全密文区间检索方案的新设计

王少辉[1,2,3]，韩志杰[1,2,4]，陈丹伟[1,2]，王汝传[1,2]

(1. 南京邮电大学 计算机学院，江苏 南京 210003；2. 江苏省无线传感网高技术研究重点实验室，江苏 南京 210003；
3. 网络与数据安全四川省重点实验室，四川 成都 610054；4. 河南大学 计算机与信息工程学院，河南 郑州 475004)

摘 要：针对目前密文区间检索多次断言存在信息泄露等问题，有单断言的密文区间检索方案(SRQSAE 方案)，并证明方案在唯密文攻击下的隐私安全性。对 SRQSAE 方案的安全性进行了分析，分析结果表明 SRQSAE 方案并不能隐藏搜索关键字的大小关系排序。通过在每次生成搜索索引或陷门消息时引入不同随机数的方法，提出了单断言的密文区间检索新方案。新方案对搜索关键字、区间的大小关系提供了很好的隐私保护；而且新方案在安全性提高的同时，并不以损失效率为代价。

关键词：云存储；区间检索；密文检索；隐私性；区间陷门

中图分类号：TP309 **文献标识码**：A

New construction of secure range query on encrypted data in cloud computing

WANG Shao-hui[1,2,3], HAN Zhi-jie[1,2,4], CHEN Dan-wei[1,2], WANG Ru-chuan[1,2]

(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210003, China;
3. Network and Data Security Key Laboratory of Sichuan Province, Chengdu 610054, China;
4. School of Computer and Information Engineering, Henan University, Zhengzhou 475004, China)

Abstract: To solve the information leakage problem resulting from several assertions of previous range query solutions, there is a secure range query scheme with one assertion (SRQSAE scheme), and the scheme is claimed to be secure against ciphertext-only attack. The security analysis on SRQSAE scheme is presented, and it shows SRQSAE scheme can not hide the size of search keyword. A new scheme of secure range query on encrypted data is proposed through introducing random numbers in the generation of search index and trapdoor. The new scheme can provide the privacy guarantee on search range and search keyword, and it achieves high level needs of security without losing efficiency.

Key words: cloud storage; range query; search on encrypted data; privacy; interval trapdoor

1 引言

近年来，云计算越来越受到学术界和产业界的关注，而作为云计算重要应用业务之一的云存储是从云计算概念衍生和发展起来的一种数据外包存储服务技术。通过使用云存储，企业用户可以不用考虑存储管理、数据备份、容灾等问题，从而可以大大较低数据存储设备管理和维护的工作量和成本。

由于数据外包将数据完全存储在半可信的云存储服务器中，用户已经在物理上不再拥有这些外包存储的数据，所以为了保护外包数据的私密性，用户通常会将外包数据加密之后再存储在云服务器上，密文形式的数据存储大大降低了外包数据的信息泄露问题。然而密文存储给数据检索带来

收稿日期：2013-09-07；**修回日期**：2013-12-07

基金项目：国家自然科学基金资助项目(61373139, 61373006)；江苏省自然科学基金资助项目(BK2012833)；江苏省科技支撑计划基金资助项目(61003236)

Foundation Items: The National Natural Science Foundation of China (61373139, 61373006); The Natural Science Foundation of Jiangsu Province(BK2012833); S&T Supporting Project of Jiangsu Province (61003236)

了一定困难。实现密文检索最直接的解决方案是将密文全部传送给授权请求用户，由用户在本地进行解密后再进行相关检索操作，但这必然导致昂贵的网络 I/O 和传输的费用代价，从而在实际中并不可行。

在众多同时解决云存储数据隐私性和数据可检索性问题的方法中，可检索加密(SE, searchable encryption)是目前最受关注的方法之一。SE 要求用户在上传加密数据的同时，上传搜索关键字的索引；而授权用户可以生成检索陷门标识发送给云存储服务器；云服务器返回与陷门标识相匹配的关键字索引对应的加密数据。根据基于的密码机制的不同，SE 方案可以分为 2 大类。一类是基于私钥算法的 SE 方案[1~7]，在该构架下，只有拥有私钥的合法用户才能生成检索陷门标识；另一类是基于公钥算法的 SE 方案[8~12]，此时任何用户都可以利用数据拥有者的公钥信息生成检索陷门标识。在 SE 方案的设计中，搜索索引或检索陷门要隐藏搜索关键字的信息是需要重点考虑的问题。

区间检索(range query)[13]是在线数据分析中最常用到的检索方式之一。授权用户对检索区间生成检索陷门标识，而服务器返回关键字在检索区间范围内的所有数据文件。早期对密文区间检索的研究主要集中于保证搜索关键字的可用性，最直接的方法是应用保序加密算法[14,15]。在保序加密中，区间索引和搜索关键字的密文之间和明文具有同样的大小排序关系，显然保序加密将搜索关键字的大小关系完全泄露给了云服务器。Hacigumu 等[16,17]提出通过对搜索关键字进行分桶的方式实现密文区间检索，在此类方案中，服务器可以直接获得多个搜索关键字对应同一个区间索引。上述方案要实现密文区间检索，服务器均需要对区间索引进行多次断言。每次断言都意味着服务器要进行等值匹配判断或大小比较判断，从而会向服务器泄露关键字的相关信息。针对上述信息泄露的问题，蔡克等[18]第一次提出基于单断言来实现密文区间检索的方案(SRQSAE 方案)，即服务器只需要对区间索引进行一次断言，就可以获知搜索关键字是否属于该检索区间，并证明了方案在唯密文攻击场景下，可以保护敏感数据的排列信息和敏感数据的归并信息不会被泄露。

本文对满足隐私性的安全密文区间检索方案进行了研究。对 SRQSAE 方案的安全性进行了详细分析，分析表明在唯密文攻击下，SRQSAE 方案并不能隐藏搜索关键字的大小关系排序，可以唯一地确定关键字的大小序列。通过在搜索索引、陷门标识生成中引入随机数，提出了安全密文区间检索的新方案，并证明了新方案在已知明文—密文攻击场景下可以提供隐私性保障，也就是说，即使攻击者获知一些关键字和对应索引值，仍然无法推断得到搜索关键字的大小信息。

2 系统模型和安全定义

在本节中，给出了云存储环境下密文区间检索方案的定义和方案所要满足的隐私性安全需求，如关键字隐私性、搜索区间隐私性等，本文考虑基于私钥机制的密文检索方案。

如图 1 所示，云存储服务涉及 3 个不同的实体：数据所有者(DO, data owner)将自己的数据文件存储在云存储服务平台上，为了数据的安全性，DO 通常将数据文件加密，并为数据构建区间索引一同存储；云存储服务器(CSS, cloud storage server)由云服务供应商进行管理和维护，提供存储服务，并检验与授权用户(AU, authorized user)发起的区间检索请求相匹配的索引，CSS 承担大量的处理任务，向 AU 返回检索结果。这里不考虑数据加密的问题，只考虑搜索索引的建立和匹配验证等问题。

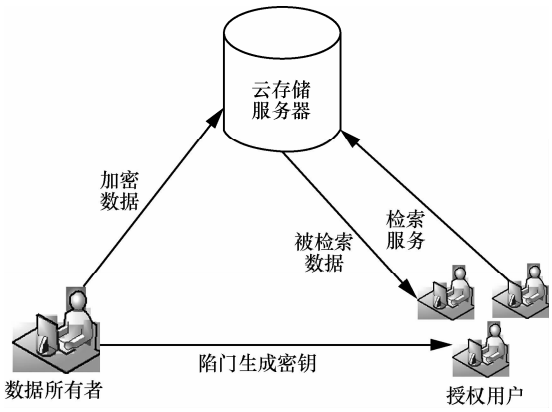

图 1 云存储环境下密文检索构架

定义 1 (密文区间检索方案) 云存储环境下的密文区间检索方案通常由如下 4 个多项式时间算法组成。

1) Setup。输入系统的安全参数，DO 生成私钥 SK，并将其安全的发送给授权用户 AU。

2) BuildIndex(v,SK)。对搜索关键字 v，DO 利用私钥 SK 生成区间索引 $\boldsymbol{I}_v$，并将其连同加密数据一同发送给 CSS。

3) Trapdoor (H,L,SK)。授权用户 AU 利用私钥 SK，对检索区间的上下界 H 和 L，生成相应的检索陷门信息 $\boldsymbol{T}$，并发送给 CSS 进行检索请求。

4) Search($\boldsymbol{I}$, $\boldsymbol{T}$)。云存储服务器 CSS 根据区间索引 $\boldsymbol{I}$ 和陷门信息 $\boldsymbol{T}$，判断搜索关键字是否在被检索区间范围内。如果成立，则输出 Yes，并将关键字所对应的加密数据发送给 AU；否则输出 No，说明搜索关键字并不在请求的搜索区间内。

云存储环境的密文区间检索的安全威胁主要来源于 CSS 和恶意的外部敌手。一般假设 CSS 是半可信的，即 CSS 会忠实地执行 AU 提交的区间检索请求，并返回根据检索请求得到的检索结果。但是 CSS 会利用掌握的一切资源来进行分析，如搜索关键字的区间索引和区间搜索陷门等，期望获得有用的信息，如关键字的大小排序关系。

密文区间检索方案的安全性主要包括搜索关键字和检索区间的隐私性，如关键字的值，关键字的大小排序关系，检索区间请求的上下界等信息。针对外部敌手和 CSS 分别给出隐私性的定义。

定义 2（对外部攻击者的隐私性）。通过攻击者 A 分别和挑战者 B、模拟器 S 进行的 2 个游戏来定义密文区间检索方案对外部攻击者的隐私性。挑战者 B 同时充当 CSS 和 AU 的角色，游戏分为 2 个阶段，Learning 阶段和 Attack 阶段，其中，Learning 阶段对 2 个游戏一样。

Learning：

1) 挑战者 B 运行 Setup 算法生成系统私钥 SK；

2) 敌手 A 可以向挑战者 B 进行 BuildIndex 和 Trapdoor 预言机的询问；对于每一次询问，攻击者选择关键字 v (或检索区间上下界 H 和 L)给挑战者 B，挑战者计算相应的区间索引 $\boldsymbol{I}_v$ (或陷门信息 $\boldsymbol{T}$) 后返还给攻击者。模拟者 S 可以获得 Learning 阶段的所有消息。

Game1 Attack：

3) 挑战者选择搜索关键字序列 $\{v_1,v_2,\cdots,v_n\}$，分别计算搜索索引 $\{\boldsymbol{I}_1,\boldsymbol{I}_2,\cdots,\boldsymbol{I}_n\}$。攻击者此时可以访问 EXECUTE 预言机，对于攻击者的访问，预言机将返回一次正确的检索请求和应答的交互消息。交互消息由挑战者完全生成，该预言机模拟了攻击者进行被动侦听攻击的能力。

Game2 Attack：

游戏 2 的攻击阶段与游戏 1 的不同之处在于，攻击者访问 EXECUTE 预言机时，返回由模拟器 S 生成的相应消息，这里，模拟器 S 并不具有系统私钥 SK。

若攻击者在游戏 1 和游戏 2 结束时输出 1 的概率差 $|\Pr\{1\leftarrow \mathrm{Game1}_{A,B}\}-\Pr\{1\leftarrow \mathrm{Game2}_{A,S}\}|$ 可忽略，称密文区间检索方案满足外部攻击者隐私性。

定义 3　(对 CSS 的隐私性)同定义 2 一样，通过攻击者 A 分别和挑战者 B、模拟器 S 进行的 2 个游戏来定义密文区间检索方案对 CSS 的隐私性。此时攻击者 A 模拟 CSS 的行为，而挑战者模拟 AU 的行为。Learning 阶段和定义 2 一样。

Game1' Attack：

挑战者选择搜索关键字序列 $\{v_1,v_2,\cdots,v_n\}$，计算并发送给攻击者相应的区间索引序列 $\{\boldsymbol{I}_1,\boldsymbol{I}_2,\cdots,\boldsymbol{I}_n\}$。攻击者此时可以访问 Query 预言机，攻击者询问此预言机时，该预言机将返回挑战者生成的陷门 $\boldsymbol{T}$ 作为应答；攻击者可以调用 Search($\boldsymbol{I}$, $\boldsymbol{T}$) 来观察查询结果。

Game2' Attack：

游戏 2 的攻击阶段与游戏 1 的不同之处在于，攻击者访问 Query 预言机时，返回由模拟器 S 生成的陷门信息 $\boldsymbol{T}$。

若攻击者在游戏 1 和游戏 2 结束时输出 1 的概率差 $|\Pr\{1\leftarrow \mathrm{Game1}'_{A,B}\}-\Pr\{1\leftarrow \mathrm{Game2}'_{A,S}\}|$ 可忽略，则称密文区间检索方案满足对 CSS 的隐私性。

3　对 SRQSAE 方案的安全分析

蔡克等在文献[18]中第一次提出基于单断言的密文区间检索方案 SRQSAE 方案，即服务器只需对区间索引进行一次断言，就可以获知搜索关键字是否属于该检索区间。基于单断言的区间检索可以在一定程度上减少区间检索过程中的信息泄露问题。在本节中，首先简单介绍 SRQSAE 方案，然后对该方案的安全性进行详细的分析，分析结果表明，该方案并不能满足唯密文攻击情景下的关键字隐私性，云服务器或外部攻击者可以获知搜索关键字的大小排序关系。

3.1　SRQSAE 方案简介

SRQSAE 方案的设计基于如下定理。

定理 1[18]　如图 2 所示，给定一个坐标原点为 O 的单位圆，这里只考虑上半圆。对于任意的半圆上的 3 个点 A、B 和 C，半径 OA 和 OB，OB 和 OC，OA 和 OC 的夹角分别是 θ_1、θ_2 和 θ_3，其中，

$\theta_i \in (0,\pi), i=1,2,3$。则半径 OB 在 OA 和 OC 之间当且仅当 $\cos\theta_3 < \cos\theta_1 \cos\theta_2$ 成立。

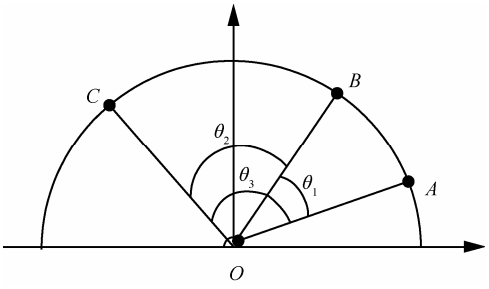

图 2 单位圆不同半径和角度关系

SRQSAE 方案首先定义了一个区间判断到单断言的映射函数

$$F: D \to (0,\pi), F(v) = \theta = \arccos\left(-\frac{v}{v_{\max}}\right) \quad (1)$$

其中，D 是搜索关键字的取值空间，$v_{\max}$ 是搜索关键字取值的最大值。在下文的讨论中，直接假设搜索关键字取值于 $(0,\pi)$，不再考虑映射函数 F。

SRQSAE 方案主要包含了如下几个步骤。

1) Setup。数据拥有者 DO 随机选择 2×2 的可逆矩阵 $\boldsymbol{M}$，并计算相应的逆矩阵 $\boldsymbol{M}^{-1}$。方案的私钥为 $SK=\{\boldsymbol{M},\boldsymbol{M}^{-1}\}$。DO 将私钥安全的发送给合法用户 AU。

2) BuildIndex(θ, SK)。数据拥有者利用私钥 $\boldsymbol{M}$，计算搜索关键字 θ 的区间索引值为 $\boldsymbol{I}_\theta=[\cos\theta,\sin\theta]\boldsymbol{M}$。DO 将加密数据和关键字索引值发送给云存储服务器 CSS。

3) Trapdoor(θ_H,θ_L,SK)。利用私钥 $\boldsymbol{M}^{-1}$，合法用户 AU 对区间索引的上限和下限值 (θ_H,θ_L) 分别计算

$$\begin{cases} \boldsymbol{T}_H = \boldsymbol{M}^{-1}[\cos\theta_H, \sin\theta_H]^{\mathrm{T}} \\ \boldsymbol{T}_L = \boldsymbol{M}^{-1}[\cos\theta_L, \sin\theta_L]^{\mathrm{T}} \\ T_{\text{range}} = \cos(\theta_H - \theta_L) \end{cases} \quad (2)$$

最终生成的陷门信息为 $\boldsymbol{T}=\{T_{\text{range}},\boldsymbol{T}_1,\boldsymbol{T}_2\}$，为了安全性，这里要求 $\boldsymbol{T}_1, \boldsymbol{T}_2$ 并不总是固定等于 $\boldsymbol{T}_H, \boldsymbol{T}_L$，其对应关系是随机的。AU 将陷门信息发送给 CSS。

4) Search($\boldsymbol{I}, \boldsymbol{T}$)。云存储服务器利用陷门信息 $\boldsymbol{T}=\{T_{\text{range}},\boldsymbol{T}_1,\boldsymbol{T}_2\}$，检验 $T_{\text{range}} < (\boldsymbol{I}\boldsymbol{T}_1)\times(\boldsymbol{I}\boldsymbol{T}_2)$ 是否成立。如果成立，则输出 Yes 意味着关键字在被索引区间范围内；否则输出 No。最终，CSS 将输出结果为 Yes 的关键字对应的加密数据发送给 AU。

3.2 对 SRQSAE 方案的安全分析

在本节中，将说明在唯密文的攻击场景下，也就是攻击者只能获得区间索引值或陷门信息，SRQSAE 方案并不能隐藏索引关键字的大小排列关系。在给出 SRQSAE 方案的安全分析之前，首先回顾一些关于矩阵的基本定理，定理 2 和定理 3 易证，这里不再赘述。

定理 2 区间 $(0,\pi)$ 上任意不相等的角 θ_1 和 θ_2，矩阵 $\boldsymbol{M}=\begin{bmatrix}\cos\theta_1, \sin\theta_1 \\ \cos\theta_2, \sin\theta_2\end{bmatrix}$ 一定是可逆矩阵。

定理 3 对于任意的可逆矩阵 $\boldsymbol{M}_1$ 和 $\boldsymbol{M}_2$，有式 $(\boldsymbol{M}_1\boldsymbol{M}_2)^{-1}=\boldsymbol{M}_2^{-1}\boldsymbol{M}_1^{-1}$ 恒成立。并且对于 2×2 的可逆矩阵 $\boldsymbol{M}=\begin{bmatrix}a, b \\ c, d\end{bmatrix}$，其逆矩阵 $\boldsymbol{M}^{-1}$ 可以表示为 $\boldsymbol{M}^{-1}=\frac{1}{|\boldsymbol{M}|}\begin{bmatrix}d, -b \\ -c, a\end{bmatrix}$，其中 $|\boldsymbol{M}|=ad-bc$。

如果攻击者能够获得区间索引值所对应的关键字，则 SRQSAE 方案显然是不安全的。假设方案私钥矩阵 $\boldsymbol{M}=\begin{bmatrix}a, b \\ c, d\end{bmatrix}$，显然有 $ad-bc\neq0$。如果攻击者获得了 2 个搜索关键字与其对应的索引值，不妨假设为 $(\theta_1, \boldsymbol{I}_{\theta_1})$ 和 $(\theta_2, \boldsymbol{I}_{\theta_2})$，则可以得到如下的方程组

$$\begin{cases} \boldsymbol{I}_{\theta_1} = [\cos\theta_1, \sin\theta_1]\begin{bmatrix}a, b \\ c, d\end{bmatrix} = [r_{11}, r_{12}] \\ \boldsymbol{I}_{\theta_2} = [\cos\theta_2, \sin\theta_2]\begin{bmatrix}a, b \\ c, d\end{bmatrix} = [r_{21}, r_{22}] \end{cases} \quad (3)$$

利用定理 2，通过求解方程组(3)，可以唯一地获得私钥矩阵 $\boldsymbol{M}$。

下面利用定理 2 和定理 3，可以得到如下结论。

定理 4 在唯密文的攻击场景下，SRQSAE 方案并不能隐藏索引关键字的大小排序关系；也就是说 CSS 或非法用户可以获知搜索关键字的排列关系。

证明 假设 CSS 中存储的搜索区间索引值为 $\boldsymbol{I}_1, \boldsymbol{I}_2, \cdots, \boldsymbol{I}_n$，其分别利用关键字 $\theta_1, \theta_2, \cdots, \theta_n$ 生成，也就是说对任意的 $k=1,2,\cdots,n$，有

$$\boldsymbol{I}_k = [\cos\theta_k, \sin\theta_k]\boldsymbol{M}$$

CSS 首先选择索引向量 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$，构造矩阵 $\boldsymbol{I}=\begin{bmatrix}\boldsymbol{I}_1\\ \boldsymbol{I}_2\end{bmatrix}=\begin{bmatrix}\cos\theta_1, \sin\theta_1\\ \cos\theta_2, \sin\theta_2\end{bmatrix}\boldsymbol{M}$，由定理 2 和定理 3 知矩阵 $\boldsymbol{I}$ 可逆，并且有

$$\boldsymbol{I}^{-1}=\boldsymbol{M}^{-1}\begin{bmatrix}\cos\theta_1, \sin\theta_1\\ \cos\theta_2, \sin\theta_2\end{bmatrix}^{-1}$$
$$=\frac{1}{\sin(\theta_2-\theta_1)}\boldsymbol{M}^{-1}\begin{bmatrix}\sin\theta_2, -\sin\theta_1\\ -\cos\theta_2, \cos\theta_1\end{bmatrix}$$

下面 CSS 选择搜索索引 $\boldsymbol{I}_3$，并计算得到

$$\boldsymbol{I}_3\boldsymbol{I}^{-1}=\left[\cos\theta_3, \sin\theta_3\right]\boldsymbol{M}\frac{1}{\sin(\theta_2-\theta_1)}\boldsymbol{M}^{-1}\cdot$$
$$\begin{bmatrix}\sin\theta_2, -\sin\theta_1\\ -\cos\theta_2, \cos\theta_1\end{bmatrix}=\left(\frac{\sin(\theta_2-\theta_3)}{\sin(\theta_2-\theta_1)}, \frac{\sin(\theta_3-\theta_1)}{\sin(\theta_2-\theta_1)}\right)$$

对任意 $j,k=1,2,\cdots,n$，$\theta_k\in(0,\pi)$，则 $\theta_j-\theta_k$ 必定取值于区间 $(-\pi,0)\cup(0,\pi)$。从而知道如果 $\sin(\theta_j-\theta_k)<0$，则必有 $\theta_j<\theta_k$；反之如果 $\sin(\theta_j-\theta_k)>0$，有 $\theta_j>\theta_k$。

向量 $\boldsymbol{I}_3\boldsymbol{I}^{-1}$ 的 2 个非零元素按照正负取值必然属于下面 4 种情况中的一种。

1) $\frac{\sin(\theta_2-\theta_3)}{\sin(\theta_2-\theta_1)}>0$ 并且 $\frac{\sin(\theta_3-\theta_1)}{\sin(\theta_2-\theta_1)}<0$

2) $\frac{\sin(\theta_2-\theta_3)}{\sin(\theta_2-\theta_1)}>0$ 并且 $\frac{\sin(\theta_3-\theta_1)}{\sin(\theta_2-\theta_1)}>0$

3) $\frac{\sin(\theta_2-\theta_3)}{\sin(\theta_2-\theta_1)}<0$ 并且 $\frac{\sin(\theta_3-\theta_1)}{\sin(\theta_2-\theta_1)}>0$

4) $\frac{\sin(\theta_2-\theta_3)}{\sin(\theta_2-\theta_1)}<0$ 并且 $\frac{\sin(\theta_3-\theta_1)}{\sin(\theta_2-\theta_1)}<0$

以情况 1)为例，说明如何确定搜索关键字的排序情况。在情况 1)的条件下，可以得到如下 2 种情况

$$\begin{cases}\sin(\theta_2-\theta_3)>0, \sin(\theta_2-\theta_1)>0, \sin(\theta_3-\theta_1)<0\\ \sin(\theta_2-\theta_3)<0, \sin(\theta_2-\theta_1)<0, \sin(\theta_3-\theta_1)>0\end{cases}$$

也就是说可以得到 θ_1，θ_2 和 θ_3 的 2 种排序关系：

$$\theta_2>\theta_3, \theta_2>\theta_1, \theta_3<\theta_1 \quad (4)$$

$$\theta_2<\theta_3, \theta_2<\theta_1, \theta_3>\theta_1 \quad (5)$$

如图 3 所示，此时 CSS 可以得到 θ_1 位于 θ_2 和 θ_3 之间，但是此时无法比较 θ_2 和 θ_3 的排序。类似地可以讨论在情况 2)、情况 3)或情况 4)下的大小排序关系，这里不再赘述。

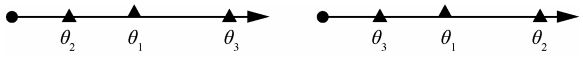

图 3　在情况 1 下，θ_1 与 θ_2 和 θ_3 的排序关系

在关键字 θ_1，θ_2 和 θ_3 满足情况 1)的条件下，继续考虑区间索引 $\boldsymbol{I}_4$。类似上面的讨论，此时需要分别计算 $\boldsymbol{I}_4$ 与 $(\boldsymbol{I}_1,\boldsymbol{I}_2)$ 和 $(\boldsymbol{I}_1,\boldsymbol{I}_3)$ 的关系。注意这里不需要将 $\boldsymbol{I}_4$ 与 $(\boldsymbol{I}_2,\boldsymbol{I}_3)$ 进行比较。下面说明 θ_1，θ_2,θ_3,θ_4 的排序关系也只有 2 条。

当比较 $\boldsymbol{I}_4$ 与 $(\boldsymbol{I}_1,\boldsymbol{I}_2)$ 的关系时，如果得出结论 θ_4 位于 θ_1 和 θ_2 之间，或者 θ_2 位于 θ_1 和 θ_4 之间，此时可以直接获得 θ_1，θ_2，θ_3，θ_4 的排序关系。图 4 给出了当 θ_4 位于 θ_1 和 θ_2 之间的时候，θ_1，θ_2，θ_3，θ_4 的 2 种排序关系。但是如果得出结论是 θ_1 位于 θ_4 和 θ_2 之间，此时 θ_4 在图 3 中 2 条坐标轴的位置不唯一，各存在 2 种可能性。这时需要将 $\boldsymbol{I}_4$ 与 $(\boldsymbol{I}_1,\boldsymbol{I}_3)$ 进行比较，可以唯一确定 θ_4 在 2 条坐标轴上的位置。

图 4　θ_4 在 θ_2 和 θ_1 之间时的排序关系

类似上面的讨论，CSS 依次对关键字索引 $\boldsymbol{I}_5,\boldsymbol{I}_6,\cdots,\boldsymbol{I}_n$ 进行考察，可以看出对任意的 $k=5,6,\cdots,n$，要确定 $\boldsymbol{I}_k$ 所对应的 θ_k 在坐标轴的位置，最差的情况，CSS 需要进行 $k-2$ 次比较。最终，可以得到搜索关键字 $\theta_1,\theta_2,\cdots,\theta_n$ 的 2 条大小关系排序序列。

以图 4 为例，说明 CSS 如何在接收到的区间陷门消息中寻找信息，以唯一确定关键字的大小排序。同上面的讨论一样，区间陷门也无法隐藏搜索区间上下界的大小关系。假设 CSS 接收到 2 次陷门信息 $\{\boldsymbol{T}_{11},\boldsymbol{T}_{12}\}$ 和 $\{\boldsymbol{T}_{21},\boldsymbol{T}_{22}\}$ 分别对应的搜索区间为 $(\theta_{L1},\theta_{H1})$ 和 $(\theta_{L2},\theta_{H2})$，CSS 可以利用上面的方法分别判断出 θ_{L2}，θ_{H2} 与 θ_{L1},θ_{H1} 的大小关系，不妨假设有有 $\theta_{L2}>\theta_{H1}$。如果当陷门是 $\{\boldsymbol{T}_{11},\boldsymbol{T}_{12}\}$ 时，有搜索索引 $\boldsymbol{I}_2$ 匹配；而陷门是 $\{\boldsymbol{T}_{21},\boldsymbol{T}_{22}\}$ 时，有搜索索引 $\boldsymbol{I}_3$ 与之匹配，则 CSS 可以判断 $\theta_1,\theta_2,\theta_3,\theta_4$ 的大小排序关系必然与图 4 的左边排序一致。从而可以看出 CSS 可以利用搜索陷门与索引的匹配情况来确定关键字的大小关系排序。

上面给出了 CSS 如何判定搜索关键字的大小，对于外部的攻击者而言，他们没有搜索索引信息，但是他们同样可以侦听搜索陷门消息，并分析搜索陷门的大小排序，从而为返回的加密文件的关键字

建立大小关系。

综上所述，SRQSAE 方案不能隐藏搜索关键字的大小排序。 证毕。

4 密文区间检索新方案

在对 SRQSAE 方案的安全性进行分析时，文献[18]只是证明了给定 2 个搜索索引 $\boldsymbol{I}_1$ 和 $\boldsymbol{I}_2$，SRQSAE 方案对其相应搜索关键字 θ_1 和 θ_2 的大小是不可区分的。但是当考虑超过 2 个搜索索引时，如 $\boldsymbol{I}_1$, $\boldsymbol{I}_2$ 和 $\boldsymbol{I}_3$，此时索引关键字 θ_1, θ_2, θ_3 的取值就不再是任意的，其必须保证如下方程组(6)中，矩阵 $\boldsymbol{M}$ 的解存在。

$$\begin{cases}\boldsymbol{I}_{\theta_1}=[\cos\theta_1,\sin\theta_1]\begin{bmatrix}a, & b\\ c, & d\end{bmatrix}=[r_{11},r_{12}]\\ \boldsymbol{I}_{\theta_2}=[\cos\theta_2,\sin\theta_2]\begin{bmatrix}a, & b\\ c, & d\end{bmatrix}=[r_{21},r_{22}]\\ \boldsymbol{I}_{\theta_3}=[\cos\theta_3,\sin\theta_3]\begin{bmatrix}a, & b\\ c, & d\end{bmatrix}=[r_{31},r_{32}]\end{cases} \tag{6}$$

这也是 SRQSAE 方案不能保证索引关键字大小排序关系的原因。

在本节中，给出了一个改进的密文区间检索新方案，与 SRQSAE 方案中 BuildIndex，Trapdoor 算法是确定性算法不同，新方案在索引生成和陷门生成时，都引入随机数，从而对关键字信息、搜索区间上下界信息进行了很好的隐藏。

4.1 安全的密文区间检索新方案

新的安全密文区间检索方案主要分为如下 4 个步骤。

1) Setup。DO 首先随机选择一个 4×4 的可逆矩阵 $\boldsymbol{M}$，并计算其相应的逆矩阵 $\boldsymbol{M}^{-1}$。令 $[\boldsymbol{M}]_{3\times4}$ 表示矩阵 $\boldsymbol{M}$ 的第 1 行、第 2 行和第 4 行；而 $[\boldsymbol{M}^{-1}]_{4\times3}$ 表示逆矩阵 $\boldsymbol{M}^{-1}$ 的第 1 列、第 2 列和第 3 列。则方案的私钥为 SK 为 $\{[\boldsymbol{M}]_{3\times4},[\boldsymbol{M}^{-1}]_{4\times3}\}$。DO 将 SK 安全的发送给 AU。

2) BuildIndex(θ, SK)。对于任意的搜索关键字 θ，数据拥有者首先随机选择 $\alpha_i\in R$，则关键字 θ 所对应的区间搜索索引为

$$\boldsymbol{I}_\theta=[\cos\theta,\sin\theta,\alpha_i][\boldsymbol{M}]_{3\times4} \tag{7}$$

DO 将加密数据和关键字区间索引一并发送给云存储服务器。

3) Trapdoor(θ_H,θ_L,SK)。对于搜索区间的上限和下限值 (θ_H,θ_L)，授权用户首先选择随机数 $\beta,\gamma\in R$，并计算

$$\begin{cases}\boldsymbol{T}_H=[\boldsymbol{M}^{-1}]_{4\times3}[\cos\theta_H,\sin\theta_H,\beta]^{\mathrm{T}}\\ \boldsymbol{T}_L=[\boldsymbol{M}^{-1}]_{4\times3}[\cos\theta_L,\sin\theta_L,\gamma]^{\mathrm{T}}\\ T_{\text{range}}=\cos(\theta_H-\theta_L)\end{cases} \tag{8}$$

最终的陷门信息为 $\boldsymbol{T}=\{T_{\text{range}},\boldsymbol{T}_1,\boldsymbol{T}_2\}$，为了安全性，同样要求 $\boldsymbol{T}_1$, $\boldsymbol{T}_2$ 并不总是固定等于 $\boldsymbol{T}_H$, $\boldsymbol{T}_L$，其对应关系是随机的。AU 将陷门信息发送给 CSS。

4) Search($\boldsymbol{I}$, $\boldsymbol{T}$)。接收到陷门 $\boldsymbol{T}=\{T_{\text{range}},\boldsymbol{T}_1,\boldsymbol{T}_2\}$ 后，CSS 对每个搜索索引检验式(9)是否成立。

$$T_{\text{range}}<(\boldsymbol{I}\boldsymbol{T}_1)\times(\boldsymbol{I}\boldsymbol{T}_2) \tag{9}$$

如果成立，则输出 Yes 意味着索引在搜索区间范围内，否则输出 No，说明索引不在搜索区间内。最终，CSS 将输出结果为 Yes 的关键字对应的加密数据发送给 AU。

4.2 安全分析

在本节中，给出密文区间检索方案的安全分析。首先阐述方案的正确性。也就是说在搜索区间的关键字一定能满足式(9)。

正确性 由于 $[\boldsymbol{M}]_{3\times4}$ 表示矩阵 $\boldsymbol{M}$ 的第 1 行、第 2 行和第 4 行，从而计算 $[\cos\theta,\sin\theta,\alpha_1][\boldsymbol{M}]_{3\times4}$ 就相当于计算 $[\cos\theta,\sin\theta,0,\alpha_1]\boldsymbol{M}$，即有

$$[\cos\theta,\sin\theta,\alpha_1][\boldsymbol{M}]_{3\times4}=[\cos\theta,\sin\theta,0,\alpha_1]\boldsymbol{M}$$

同样的对于 $[\boldsymbol{M}^{-1}]_{4\times3}$，必有下列 2 个等式成立。

$$[\boldsymbol{M}^{-1}]_{4\times3}[\cos\theta_H,\sin\theta_H,\beta_1]^{\mathrm{T}}=\boldsymbol{M}^{-1}[\cos\theta_H,\sin\theta_H,\beta_1,0]^{\mathrm{T}};$$

$$[\boldsymbol{M}^{-1}]_{4\times3}[\cos\theta_L,\sin\theta_L,\gamma_1]^{\mathrm{T}}=\boldsymbol{M}^{-1}[\cos\theta_L,\sin\theta_L,\gamma_1,0]^{\mathrm{T}}$$

从而有

$$\begin{aligned}(\boldsymbol{I}\boldsymbol{T}_1)\times(\boldsymbol{I}\boldsymbol{T}_2)=&([\cos\theta,\sin\theta,0,\alpha_1]\boldsymbol{M}\boldsymbol{M}^{-1}[\cos\theta_H,\\ &\sin\theta_H,\beta_1,0]^{\mathrm{T}})([\cos\theta,\sin\theta,0,\alpha_1]\boldsymbol{M}\boldsymbol{M}^{-1}[\cos\theta_L,\\ &\sin\theta_L,\gamma_1,0]^{\mathrm{T}})=\cos(\theta-\theta_H)\cos(\theta-\theta_L)\end{aligned}$$

利用定理 1，可知方案是正确的。

下面首先证明即使攻击者通过 Learning 阶段，可同时获得搜索关键字与其对应的搜索索引，其仍然无法获得方案的私钥值。

定理 5 假设攻击者在 Learning 阶段获得了 k 对关键字和索引值 $(\theta_i,\boldsymbol{I}_i),i=1,2,\cdots,k$，攻击者不能获得系统的私钥 SK。

证明　设私钥 $[\boldsymbol{M}]_{3\times4}=\begin{bmatrix}u_1,r_1,s_1,t_1\\u_2,r_2,s_2,t_2\\u_3,r_3,s_3,t_3\end{bmatrix}$，$\theta_i$ 对应的搜索索引为 $\boldsymbol{I}_i=[l_{i1},l_{i2},l_{i3},l_{i4}]$，由搜索索引生成算法知存在随机数 $v_1,v_2,\cdots,v_k$，得到如下方程组

$$\begin{cases}\cos\theta_i u_1+\sin\theta_i u_2+v_i u_3=l_{i1}\\ \cos\theta_i r_1+\sin\theta_i r_2+v_i r_3=l_{i2}\\ \cos\theta_i s_1+\sin\theta_i s_2+v_i s_3=l_{i3}\\ \cos\theta_i t_1+\sin\theta_i t_2+v_i t_3=l_{i4}\end{cases},\ i=1,2,\cdots,k \quad (10)$$

为了方便对上面 $4k$ 个方程进行处理，不妨将未知量 v_iu_3，v_ir_3，v_is_3，v_it_3 分别用变量 x_i，y_i，z_i，w_i 来表示，且有 $\frac{x_{i+1}}{x_i}=\frac{y_{i+1}}{y_i}=\frac{z_{i+1}}{z_i}=\frac{w_{i+1}}{w_i}=m_i$，$m_i$ 的值不定。可以将方程组(10)用方程组(11)来表示

$$\begin{cases}\cos\theta_i u_1+\sin\theta_i u_2+x_i=l_{i1}\\ \cos\theta_i r_1+\sin\theta_i r_2+y_i=l_{i2}\\ \cos\theta_i s_1+\sin\theta_i s_2+z_i=l_{i3}\\ \cos\theta_i t_1+\sin\theta_i t_2+w_i=l_{i4}\\ x_{i+1}+m_i x_i=0\\ y_{i+1}+m_i y_i=0\\ z_{i+1}+m_i z_i=0\\ w_{i+1}+m_i w_i=0\end{cases},\ i=1,2,\cdots,k \quad (11)$$

方程的未知变量依次是

$$u_1,u_2,r_1,r_2,s_1,s_2,t_1,t_2,\{x_i,y_i,z_i,w_i\}_{i=1,2,\cdots,k}$$

也就是说方程组(11)中共含有 $8k-4$ 个方程，而含有 $4k+8$ 个未知变量。对方程组(11)的系数行列式矩阵 $\boldsymbol{M}^*$ 进行行列化简，可以得到如下的一般形式

$$\begin{bmatrix}\boldsymbol{0}_{4\times8}, & \boldsymbol{I}_{4\times4}, & \boldsymbol{0}_{4\times4(k-1)}\\ \boldsymbol{A}^1_{4\times8}, & \boldsymbol{0}_{4\times4}, & \boldsymbol{0}_{4\times4(k-1)}\\ \boldsymbol{A}^2_{4\times8}, & \boldsymbol{0}_{4\times4}, & \boldsymbol{0}_{4\times4(k-1)}\\ & \cdots & \\ \boldsymbol{A}^{k-1}_{4\times8}, & \boldsymbol{0}_{4\times4}, & \boldsymbol{0}_{4\times4(k-1)}\\ \boldsymbol{0}_{4(k-1)\times8}, & \boldsymbol{0}_{4(k-1)\times4}, & \boldsymbol{I}_{4(k-1)\times4(k-1)}\end{bmatrix} \quad (12)$$

其中，$\boldsymbol{0}_{4\times8}$ 表示 4 行 8 列的零矩阵，$\boldsymbol{I}_{4(k-1)\times4(k-1)}$ 则表示 $4(k-1)$ 行 $4(k-1)$ 列的单位矩阵，对于任意的 $j=1,2,\cdots,k-1$，矩阵 $\boldsymbol{A}^j_{4\times8}$ 具有如下的形式。

$$\boldsymbol{A}^j_{4\times8}=\begin{bmatrix}\beta_j,\ \mu_j,0,0,0,0,0,0\\ 0,0,\beta_j,\ \mu_j,0,0,0,0\\ 0,0,0,0,\beta_j,\ \mu_j,0,0\\ 0,0,0,0,0,0,\beta_j,\ \mu_j\end{bmatrix}$$

其中，$\beta_j=\cos\theta_j+(-1)^{j-1}m_1\cdots m_j\cos\theta_1$，$\mu_j=\sin\theta_j+(-1)^{j-1}m_1\cdots m_j\sin\theta_1$。显然如果选择合适的 $m_1,m_2,\cdots,m_{k-1}$，可以使 $\boldsymbol{A}^1_{4\times8},\boldsymbol{A}^2_{4\times8},\cdots,\boldsymbol{A}^{k-1}_{4\times8}$ 构成的 $4(k-1)$ 行 8 列子矩阵的秩为 8，从而 $\boldsymbol{M}^*$ 的秩恰好为 $4k+8$。而满足条件的 $m_1,m_2,\cdots,m_{k-1}$ 有无穷多组。

另一个值得注意的是当矩阵 $\boldsymbol{M}^*$ 的秩为 $4k+8$ 时，矩阵 $[\boldsymbol{M}^*\,|\,\boldsymbol{I}^*]$ 的秩也等于 $4k+8$，其中，$\boldsymbol{I}^*=[\{l_{i1},l_{i2},l_{i3},l_{i4}\}_{i=1,2,\cdots,k},\boldsymbol{0}_{1\times4(k-1)}]^{\mathrm{T}}$，也就是说对于任意一组 $\{m_1,m_2,\cdots,m_{k-1}\}$，攻击者可以唯一地计算得到方程组(11)的解，从而攻击者无法获得系统的密钥矩阵。　　证毕。

下面证明方案可以隐藏关键字或搜索区间的大小关系排序。

定理 6　新方案在唯密文攻击场景下可以隐藏搜索关键字或搜索区间的大小排序关系。

证明　SRQSAE 方案在唯密文攻击场景下不能隐藏超过 2 个搜索关键字的大小排序关系，给定任意的搜索索引值 $\boldsymbol{I}_1$，$\boldsymbol{I}_2,\cdots,\boldsymbol{I}_k$，当 $k>2$ 时，关键字 $\theta_1,\theta_2,\cdots,\theta_k$ 的大小将不再是随机的，否则会造成方程组(6)无解，而新方案通过随机数的引入，很好地解决了 SRQSAE 方案存在的不足。

对于搜索索引值 $\boldsymbol{I}_1$，$\boldsymbol{I}_2,\cdots,\boldsymbol{I}_k$，考虑任意大小的互异关键字 $\theta_1,\theta_2,\cdots,\theta_k$，考察方程组(11)是否存在解，如果方程组(11)对于任意的关键字总是存在解的，则易知新方案很好地隐藏了关键字的大小排序关系。由定理 5 的讨论，当序列 $m_1,m_2,\cdots,m_{k-1}$ 选择适当的取值时，方程组(11)存在解。也就是说对于任意关键字的取值，总能找到合适的私钥矩阵 $\boldsymbol{M}$，从而攻击者无法对关键字的大小关系做出判定。

同理，可以说明新方案可以隐藏检索区间上下界的大小关系，这里不再赘述。　　证毕。

最后说明新方案可以提供隐私性的保护。

定理 7　新方案在已知明文—密文的攻击场景下，可以提供针对恶意攻击者或者半可信 CSS 的隐私性保护。

证明　这里只证明方案对 CSS 满足隐私性，类似可证明方案对外部攻击者的隐私性。从密文区间检索方案对恶意攻击者或 CSS 的隐私性定义看，关键是能够构造出模拟者 S 的行为，使攻击者对与实际系统挑战者交互还是与模拟者交互不可区分，从而攻击者无法通过实际方案的交互获得有用的信息。

通过 Learning 阶段，模拟者和攻击者占有相同的资源，在 Attack 阶段，按照密文区间检索新方案的消息构造方式，可以定义模拟者 S 的行为如下。

1) EXECUTE 质询。对于关键字 $\theta_i, i=1,\cdots,k$，模拟者 S 随机选择向量 $\boldsymbol{I}_i' \in R^{1\times 4}$，生成并输出搜索索引 $I'=\{\boldsymbol{I}_i'\}_{i=1,\cdots,k}$。

2) Query 质询。当为搜索区间 (θ_H,θ_L) 生成陷门时，模拟者 S 首先计算得到满足关键字和索引值为 $(\theta_i,\boldsymbol{I}_i')_{i=1,2,\cdots,k}$ 的私钥 $[\boldsymbol{M}']_{3\times 4}$，构造可逆矩阵 $\boldsymbol{M}'$ 并得到相应私钥 $[\boldsymbol{M}'^{-1}]_{4\times 3}$，模拟者 S 利用式(8)生成并输出陷门信息 $\boldsymbol{T}'$。

由定理 5 知，即便攻击者获得了关键字和索引值对，也无法获知系统的私钥矩阵。从而可以看出在密文区间检索新方案中，模拟者 S 生成的搜索索引 $\boldsymbol{I}'$ 的分布和真实的搜索索引 $\boldsymbol{I}$ 的分布不可区分，同时 $\boldsymbol{T}'$ 的分布和真实的陷门信息 $\boldsymbol{T}$ 的分布也不可区分。也就是说真实的搜索关键字、搜索区间的上下界所对应的搜索区间集合、陷门集合与随机选择的集合计算不可区分，从而攻击者无法判断接收到的向量 $\boldsymbol{I}'(\boldsymbol{T}')$ 是合法消息还是随机值，从而无法判断其是在实际的环境中交互，还是在模拟的环境中交互，从而攻击者无法通过实际方案的交互获得有用的信息。 证毕。

4.3 性能分析

如表 1 所示，将密文区间检索新方案与 SRQSAE 方案分别就存储需求、运算量和传输数据量进行了比较，与其他密文检索方案的比较可以参考文献[18]。

表 1 新方案与 SRQSAE 方案的性能比较

性能	实体	新方案	SRQSAE 方案
存储	AU	12	4
	CSS	$4n$	$2n$
传输量	AU	9	5
运算量	AU	PRG + 24M + 16A	8M + 4A
	CSS	9M + 6A	5M + 2A

从表 1 可以看出，假设总的记录数为 n。从存储的角度看，在授权用户处，新方案需要存储密钥矩阵 $[\boldsymbol{M}^{-1}]_{4\times 3}$，共 12 个元素；而 CSS 需要存储 n 个 4 元索引向量，共 $4n$ 个元素。相较而言，SRQSAE 方案中 AU 需要存储 4 个元素，CSS 需要存储 $2n$ 个元素。

从数据传输的角度看，新方案中 AU 需要传输 9 个元素，而 SRQSAE 方案需要传输 5 个元素。

从计算量的角度看，新方案中 AU 需要生成 2 个随机数，并进行 2 次矩阵和向量运算以生成搜索陷门。细分到数字乘法和加法的话，AU 需要调用伪随机数生成器算法(PRG)，并进行 24 个乘法(M)运算，运算 16 个加法(A)运算。而 CSS 需要对 n 个搜索索引检验式(9)是否成立，每次检验需要进行 9 个乘法和 6 个加法运算。在 SRQSAE 方案中，AU 和 CSS 所做的运算同新方案一致，所不同的是由于矩阵的维数相对较小，从而所要做的乘法或者加法的数目较少。分别是 AU 需要 8 次乘法运算和 4 次加法运算，而 CSS 需要 5 次乘法运算和 2 次加法运算。可以看出，新方案在各项指标中要逊于 SRQSAE 方案，但是从应用的角度看，运算仅涉及快速的随机数生成算法和简单的数据加法和乘法运算，从而新方案仍然是高效的。

5 结束语

本文对蔡克等首次提出的单断言密文区间检索方案 SRQSAE 方案的安全性进行了分析，分析结果表明在唯密文攻击下，SRQSAE 方案并不能隐藏搜索关键字的大小排序关系。进而提出了单断言的密文区间检索新方案。在新方案中，每次生成搜索索引或搜索陷门生成时，都需要引入不同的随机数。本文证明了在已知明文-密文的攻击下，新方案可以保证隐私性，即能很好地隐藏搜索关键字、搜索区间的大小关系。而且相比较 SRQSAE 方案，新方案在安全性提高的同时，所带来的存储和计算上的损失对于功能强大的云存储服务器而言是可以忽略的。

目前所提出的区间检索新方案针对的是已知明文—密文的攻击场景，攻击者在 Attack 阶段主要是被动的侦听信道，而没有考虑攻击者在 Attack 阶段做主动的攻击，如伪造、篡改陷门信息等。下一步工作将对攻击者的能力进一步放宽，考察在更一般的安全模型下，安全密文区间检索方案的设计问题。

参考文献：

[1] GOLDREICH O, OSTROVSKY R. Software protection and simulation on oblivious RAMs[J]. Journal of the ACM, 1996, 43(3): 431-473.

[2] SONG D, WAGNER D, PERRIG A. Practical techniques for searching on encrypted data[A]. SSP 2000, Proceedings of the 2000 IEEE Symposium on Security and Privacy[C]. Seattle, USA, 2006.44-55.

[3] GOH E J. Secure indexes[EB/OL]. http://eprint.iacr.org/ 2003/216.

[4] CHANG Y, MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[A].ACNS'05, Proceedings of Applied Cryptography and Network Security, LNCS 3531[C]. Berlin, Germany, 2005. 442-455.

[5] CURTMOLA R, GARAY J, KAMARA S, OSTROVSKY R. Searchable symmetric encryption: improved definitions and efficient constructions[A]. CCS 2006, Proceedings of ACM Conference on Computer and Communications Security[C]. New York, USA, 2006. 79-88.

[6] LIESDONK P, SEDGHI S, DOUMEN J, HARTEL P H, JONKER W. Computationally efficient searchable symmetric encryption[A]. SDM 2010, Proceedings of Workshop on Secure Data Management, LNCS 6358[C]. Berlin, Germany, 2010. 87-100.

[7] KUROSAWA K, OHTAKI Y. UC-secure searchable symmetric encryption[A]. FC 2012, Proceedings of Financial Cryptography and Data Security, LNCS 7397[C]. Berlin, Germany, 2012. 285-298.

[8] BONEH D, CRESCENZO G D, OSTROVSKY R, PERSIANO G. Public key encryption with keyword search[A]. Advances in Cryptology: EUROCRYPT 2004, LNCS 3027[C]. Berlin, Germany, 2004. 506-522.

[9] ABDALLA M, BELLARE M, CATALANO D, *et al*. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions[J]. Journal of Cryptology, 2008, 21(3): 350-391.

[10] BELLARE M, BOLDYREVA A, O'NEIL A. Deterministic and efficiently searchable encryption[A]. Advances in Cryptology: CRYPTO 2007, LNCS 4622[C]. Berlin, Germany, 2007. 535-552.

[11] CAMENISCH J, KOHLWEISS M, RIAL A, *et al*. Blind and anonymous identity-based encryption and authorized private searches on public-key encrypted data[A]. PKC'09, Proceedings of Public Key Cryptography, LNCS 5443[C]. Berlin, Germany, 2009. 196-214.

[12] BONEH D, SAHAI A, WATERS B. Functional encryption: Definitions and challenges[A]. TCC 2011, Proceedings of Theory of Cryptography, LNCS 6597[C]. Berlin, Germany, 2011. 253-273.

[13] SHI E, BETHENCOURT J, CHAN T, *et al*. Multi-dimensional range query over encrypted data[A]. SP 2007, Proceedings of the IEEE Symposium on Security and Privacy[C]. Seattle, USA, 2007. 350-364.

[14] AGRAWAL R, KIERNAN J, SRIKANT R, *et al*. Order preserving encryption for numeric data[A]. SIGMOD 2004, Proceedings of ACM SIGMOD Conference[C]. New York, USA, 2004. 563-574.

[15] BOLDYREVA A, CHENETTE N, LEE Y, *et al*. Order preserving symmetric encryption[A]. Advances in Cryptology: EUROCRYPT 2009, LNCS 5479[C]. Berlin, Germany, 2009. 224-241.

[16] HACIGUMUS H, IYER B, LI C, *et al*. Executing SQL over encrypted data in the database-service-provider model[A]. SIGMOD 2002, Proceedings of ACM SIGMOD Conference on Management of Data[C]. New York, USA, 2002. 216-227.

[17] HORE B, MEHROTRA S, TSUDIK G. A privacy-preserving index for range queries[A]. CLDB 2004, Proceedings of Very Large Databases Conference[C]. Seattle, USA, 2004. 720-731.

[18] 蔡克, 张敏, 冯登国. 基于单断言的安全的密文区间检索[J]. 计算机学报, 2011, 34(11): 2093-2103.
CAI K, ZHANG M, FENG D G. Secure range query with single assertion on encrypted data[J]. Chinese Journal of Computers, 2011, 34(11): 2093-2103.

作者简介：

王少辉（1977-），男，山东潍坊人，南京邮电大学副教授，主要研究方向为密码学、信息安全。

韩志杰（1979-），男，河南周口人，河南大学副教授，主要研究方向为信息安全与对等计算等。

陈丹伟（1970-），男，陕西商洛人，南京邮电大学教授，主要研究方向为网络安全、云计算安全等。

王汝传（1943-），男，安徽合肥人，南京邮电大学教授，主要研究方向为信息安全、无线传感器网络等。