$\Sigma o\phi o\varsigma$ -Forward Secure Searchable Encryption 阅读笔记

李忆诺

2024 年 3 月 19 日

1 基本信息

1.1 论文来源

Bost R .$\Sigma o\phi o\varsigma$: Forward Secure Searchable Encryption[C]//Acm Sigsac Conference on Computer & Communications Security.ACM, 2016.DOI:10.1145/2976749.2978303.

1.2 概述

本文构建了一种具有最优搜索和更新复杂度的前向私有 SSE 方案，称为 $\Sigma o\phi o\varsigma$。它的性能与现有方案相似，其结构比以前的前向私有结构更简单，且能够保证正向私有结构的安全性。

2 论文要点

2.1 背景

可搜索对称加密 SSE，旨在通过交换泄露来提高效率。但其中的确定性加密算法引发的自适应攻击威力极大，由于服务器可以知道新添加的文档与之前的搜索查询是否匹配，这种攻击甚至可以揭示过去查询的内容。这强调了不泄露此信息的必要性，即前向私有结构。

2.2 价值

本文的主要贡献在于：

- 提出一种前向私有 SSE 方案，它具有最优搜索和更新复杂度；
- 该方案在保证正向私有结构安全性的基础上，还能维持现有泄露结构的效率；
- 该方案结构设计简单，且可以轻松扩展到针对恶意对手的安全性；
- 该方案即使在持久存储上，对于搜索与更新都非常有效。

2.3 问题陈述

构建一个前向私有动态 SSE 方案，需满足：$\Pi = (Setup, Search, Update)$
除此之外，设计的 SSE 方案必须达到两个安全属性：**正确性**和**机密性**。

2.4 方法

2.4.1 前向安全 (Forward Privacy)

前向安全是指更新操作不会泄露之前的查询信息，也就是说，服务器不知道更新的关键字是否在之前被查询过。这意味着，动态更新时，泄露的信息只能严格包含操作类型、文件标识符和文件大小，而没有任何其他的信息。

2.4.2 陷门置换 (Trapdoor Permutation, TDP)

本文的核心思想是：**陷门置换 (Trapdoor Permutation, TDP)**

在一个关键字 w 对应的搜索令牌序列 $ST_0, ST_1, ..., ST_c$ 中，服务器可以从后往前（从已有的 ST_c 到最开始的 ST_0 计算 ST，而只有用户可以从前往后生成（从已有的 ST_c 生成 ST_{c+1}，以控制服务器可以搜索的索引范围，确保前向安全。

使用 TDP 方案，除了可以满足前向安全，还可以减少服务器和用户的存储开销：因为都只需要存储当前的 ST_c.

总的来说，通过规定旧的搜索令牌不能用于搜索新添加的文档，来保证前向安全。

为每个 (关键字，文档) 对 (w, ind) 生成对应的搜索令牌 ST(search token)，即每个关键字 w 对应一个令牌序列 ST_1, ST_2, ST_c，每当添加一个 w 上的对 (w, ind) 时，只能由用户使用陷门密钥 SK 产生一个新的搜索令牌序列 ST_{c+1}。

为了减少存储开销，TDP 应当满足：

- 使用公钥 PK 可以很方便地从 ST_i 计算 ST_{i-1}，而只有使用密钥 SK 才能从 ST_i 计算 ST_{i+1}，即需要保证陷门置换函数 π 是单向的。
- 当需要检索时，用户将保存的 ST_c 发送给服务器，服务器通过计算生成前面的 ST_i。

2.5 结果

本文使用 4 个越来越大的数据集和英文维基百科来评估 $\Sigma o\phi o\varsigma$ 的性能。

在不包括 RPC 的情况下，对于四个数据集每个匹配文档的搜索时间最终稳定于 $0.008ms$ 以下，足以说明其搜索效率之高。并且，结果集越大，搜索算法就越快。

在包括 RPC 的情况下，每个匹配文档的搜索时间最终稳定于 $0.015ms$ 左右，这足以证明：对于给定的查询，通过 RPC 向客户端发送匹配的文档索引不能同时完成，如果 RPC、磁盘访问和 RSA 计算没有很好地交织在一起，就会产生瓶颈。

对于更新，在大型和小型数据集上，该方案每秒大约 4300 (w, ind) 的更新吞吐量，该评估包括所有成本。

相比之下，本文提出的方案具有更高的搜索吞吐量，且该方案的存储量更小，所需成本更低。

3 评论

3.1 局限性

对于 $\Sigma o\phi o\varsigma$，磁盘访问是其构建的瓶颈。

此外，该方案的删除操作是将对应的 (w, ind) 添加到删除实例中，并没有真正意义上地删除，因此并不能实现后向安全。

3.2 扩展阅读

Bost R , Minaud B , Ohrimenko O .Forward and Backward Private Searchable Encryption from Constrained Cryptographic Primitives[C]//Acm Sigsac Conference.ACM, 2017:1465-1482.DOI:10.1145/3133956.3133980.

3.3 启示

SSE 方案必须达到两个安全属性：**正确性**和**机密性**

- 正确性：搜索协议必须为每个查询返回正确的结果，除非概率可以忽略不记。
- 机密性：使用显示世界与理想世界的形式化，由泄露函数 $\mathcal{L}$ 参数化，描述协议向对手泄露的内容，并形式化为有状态算法。