基于非对称与对称密码原语的隐私信息检索方案综述

刘佳涛1

(1. 西安电子科技大学 网络与信息安全学院，陕西 西安 710071)

摘要：随着大数据、云计算等技术的快速发展，全球的数据量引来指数爆炸式的增长，巨量数据的存储问题越来越引起业界关注。目前云存储技术作为主流的数据外包存储模式，被广泛应用于商业之中。这种存储模式虽然极大地满足了当下数据存储的需求，但同时也存在存储成本高、安全性低、可靠性弱和数据传输延迟高等问题。隐私信息检索 (PIR) 技术的提出极大地解决了数据的隐私安全问题，使客户端能够访问公开数据库，同时隐藏真实的访问内容，对保护用户的隐私有着非凡的意义。但是由于 PIR 使用场景的严苛以及对安全性的高要求，其具体实现

其中仍然存在着非常多的安全性漏洞，其中一种名叫volume泄露的漏洞近期引起学术界广泛的关注，Kellaris等人[1]将其确定为对基于加密云的数据结构安全性的主要威胁之一。并且随着技术的进步，对该漏洞的攻击手段呈现出高效化和多样化。同时，为了预防这类攻击，volume隐藏的SSE方案也被相继提出，并被一步一步完善。本文就将针对不同攻击的攻击原理与不同方案的应对策略进行总结，旨在思考可搜索加密的泄露与进一步的防御措施。

关键词：对称可搜索加密；泄露滥用攻击；volume隐藏

# Overview of Volume Leakage Abuse Attack and Volume Hiding SSE Scheme

## Liu Jiatao1

(1. School of Electronic Engineering, Xidian University., Xi’an 710071, China)

**Abstract:** With the rapid development of big data, cloud computing and other technologies, the global data volume has attracted exponential explosive growth, and the storage problem of huge amount of data has increasingly drawn the industry's attention. Currently, cloud storage technology is widely used in business as the mainstream data outsourcing storage model. Although this storage model greatly meets the current demand for data storage, it also has problems such as high storage cost, low security, weak reliability and high data transmission delay. The proposed Symmetric Searchable Encryption (SSE) technology greatly solves the data privacy and security problems, enabling clients to outsource the storage of private data to untrusted servers while retaining the ability to issue search queries to outsourced data, which is of great significance for protecting users' privacy. However, there are still very many security vulnerabilities, and one of them, called volume leakage, has recently attracted widespread academic attention, with Kellaris et al [1] identifying it as one of the main threats to the security of encrypted cloud-based data structures. And with the advancement of technology, the means of attack on this vulnerability has shown to be efficient and diverse. Meanwhile, to prevent such attacks, volume hiding SSE schemes have been proposed one after another and have been improved step by step. In this paper, we will summarize the attack principles of different attacks and the response strategies of different schemes, aiming to think about the leakage of searchable encryption and further defense measures.

**Key Words:** Symmetric Searchable Encryption；Leakage Abuse Attacks；Volume Hiding

1. **引言**

随着大数据与云计算技术的发展，全球的数据量迎来了爆炸式的增长，Seagate和IDC联合研究[2]表明，到2025年全球数据量将达到163ZB。巨量的数据必然带来存储方面的压力，个人的存储能力已经越来越不能满足需求，所以将数据上传到云服务器，在云端实现数据的计算与存储必然是大势所趋。但是，科技永远是一把锋利的双刃剑，云计算技术虽然可以极大促进信息化时代的发展，但与此同时，隐私问题也将受到前所未有的挑战。当数据上传至服务器以后，用户就失去了对数据的绝对掌控力，用户的隐私也将被赤裸裸的暴露在服务器面前。服务器完全有可能监守自盗，严重损害用户的隐私。一种看似可行的策略就是用户将数据加密以后再上传给服务器，这样看似解决了问题，但是又会带来新的效率方面的问题，例如当用户需要检索数据时，就需要将加密数据全部下载后再在本地解密，这样反而有点画蛇添足。为了解决隐私保护问题的同时兼顾效率，Song等人[3]在2000年提出了可搜索加密（SSE）的概念，使得客户端能够将私有数据的存储外包给不受信任的服务器，同时保留对外包数据发出搜索查询的能力，对保护用户的隐私有着非凡的意义。此后，对称可搜索加密的方案层出不穷，Goh等人[4]首次提出了安全索引的概念并给出了安全性证明，而Curtmola[5]等人在此基础上提出了对称可搜索加密的定义与其安全性证明。之后，可搜索加密方案的研究如雨后春笋般蓬勃发展，向着更多的功能性（例如多用户[6]、可验证[7]、可连接查询[8]、动态更新[9]以及通配符查询[10]等）和更高的安全性（前向安全[11]与后向安全[12]）纵深发展。

但是，可搜索加密在取得长足发展的同时，也面临着诸多威胁。由于可搜索加密允许方案存在一定的泄露，而针对这些泄露的泄露滥用攻击[13]-[16]也在不断的发展。一般来说，泄露滥用攻击是攻击者利用辅助信息与方案允许的泄露模式发动的，目的是为了恢复出用户查询对应的底层明文。攻击者可能是第三方也有可能是服务器本身，而根据假设程度的不同，攻击者可以进行窃听等被动攻击和注入攻击等主动攻击。而在一般情况下，我们假设服务器是诚实且好奇的，它只会尽可能多的收集查询中的泄露信息，但并不会主动发动攻击。

Kellaris等人[1]在中引入了Volume泄漏攻击，Grubbs等人[17][18] 、Lacharité等人在**[18]**中对该种攻击进行了更加深入的研究，对该攻击的相应研究进展与相应的计算复杂度在图1.1中给出。我们可以看到目前针对Volume的泄露滥用攻击的效率一直在提升，而且攻击方法也开始呈现出多样化与复杂化。所以对于防御Volume泄露滥用攻击的研究在当下凸显得越发重要。本文我们将重点描述由Zhang等人提出的最新攻击——BVA(Binary Variable-Parameter Attack)与BVMA(Binary Volumetric Matching Attack)。



图1.1 搜索结果数量泄漏攻击发展历程

而针对Volume隐藏的对称可搜索加密方案[20]-[25]也被相继提出，本文我们将重点描述Wang[25]等人提出的不需要填充虚拟值的HR(Hash Ring)方案。

1. **Volume泄露滥用攻击**
   1. **注入攻击下的泄露模式与注入信息**

由于BVA与BVMA攻击[25]为注入攻击，所以我们主要总结了注入攻击下对称可搜索加密的泄露模式，主要可以概括为以下几类：

* 访问模式（access pattern，ap）：匹配查询的文件的标识符；
* 访问注入模式（access injection pattern，aip）：匹配查询的被注入文件的标识符；
* 搜索模式（search pattern ，sp）：一个查询是否与之前重复；
* 响应长度模式（response length pattern ，rlp）：返回的文件数量；
* 响应大小模式（response size pattern ，rsp）：返回的文件中包含的总词数；
* 容量模式（volume pattern ，vp）：包含rlp和rsp模式。

而BVA与BVMA攻击主要利用了响应长度模式和响应大小模式，对应的收集到的注入信息也主要包含一下几种：

* 注入长度（injection length ，ILen）：被注入文件的数量；
* 注入大小（injection size，ISize）：被注入文件包含的总字数；
* 注入容量（injection volume）：包含ILen与ISize。
  1. **注入攻击模型**

为了获取一般的注入攻击模型，假设对手能够主动生成和注入文件。我们将对手视为一个诚实但好奇的服务器，它遵循协议但仍然可以将文件注入客户数据库。我们将整个攻击过程分为三个阶段，见图2.1。

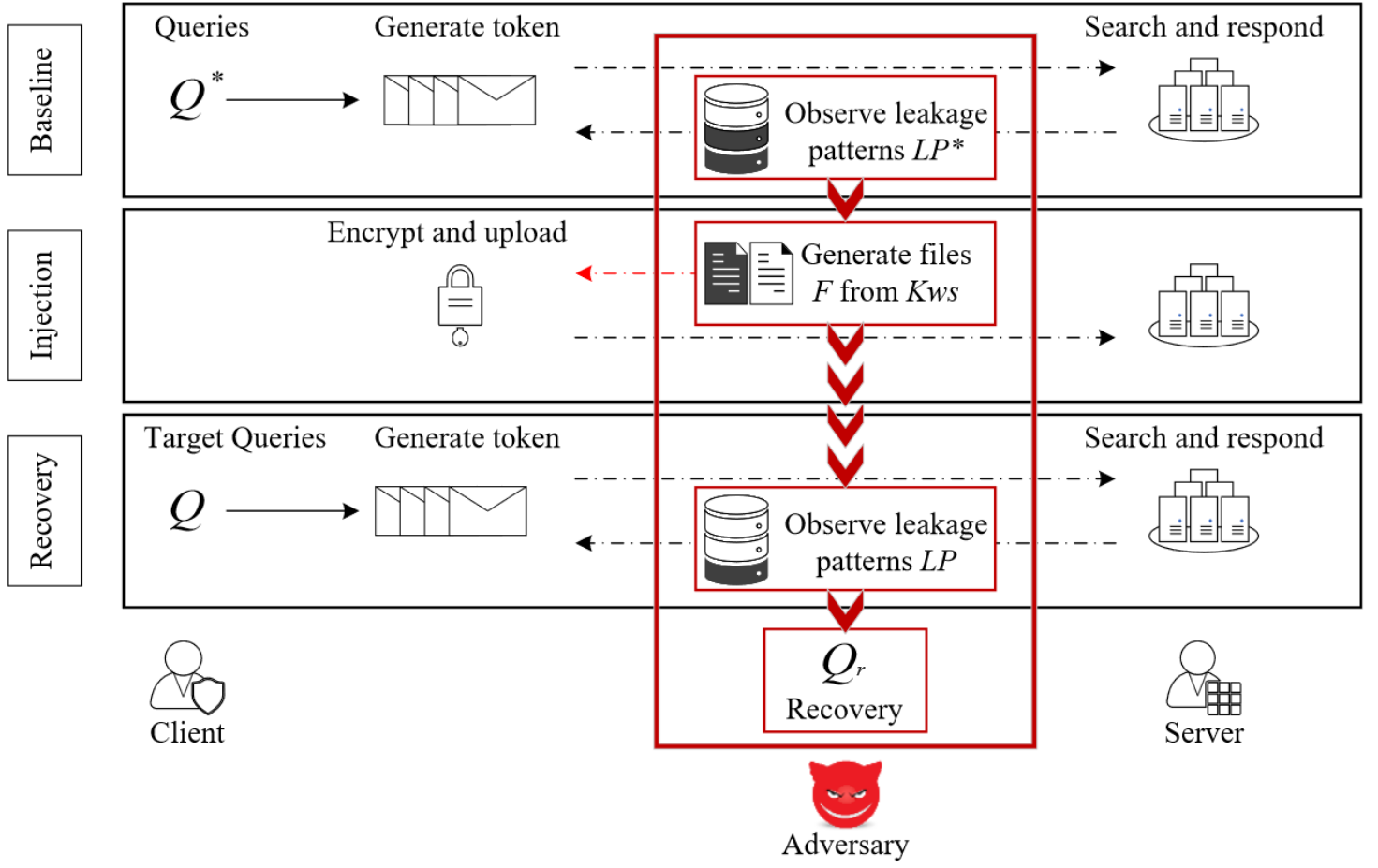


图2.1 注入攻击模型

* 基准阶段（baseline phase）：对手将客户端的查询泄漏观察为先验知识（前提是客户端向服务器发送查询）。这一步对于注入攻击很重要（ZKP攻击[26]和single-round攻击[27]除外）。这是因为对手应该从基准阶段的观察中获得关键字和响应文件之间的相关性。这个想法是比较查询恢复注入之前（基准）和注入之后的响应结果之间的volume差异。
* 注入阶段（injection phase）：在注入阶段，对手应该使用其已知的关键字和从基准阶段获得的信息认真小心地生成注入文件。接下来，客户端将文件加密并上传到服务器。
* 恢复阶段（recovery phase）：在恢复阶段，对手获得目标查询的泄漏，并通过组合所有已知信息、、和来恢复它们。

我们让表示对手观察到的目标查询集，表示查询恢复结果。我们将恢复率称为。我们将注入文件的数量表示为，将注入文件的字数表示为，其中是注入文件的集合。注入攻击的目标是通过仅利用已知的关键字域和预注入泄漏来获得较高的并使和尽可能“小”。

* 1. **BVA攻击**

BVA(Binary Variable-Parameter Attack)攻击使用动态参数来灵活设置文件的大小来调整恢复率。以恢复率的轻微损失为代价，它可以显着减少注入量。与decoding攻击[28]不同，它不需要完整准确地计算，降低了计算成本。同时BVA 会针对不同的数据集调整适当的。这可能会影响回收率和注入量。例如，设置较小的γ可以减小注入大小，但可能会牺牲掉一部分恢复率。

BVA（见图2.2）的工作原理如下：

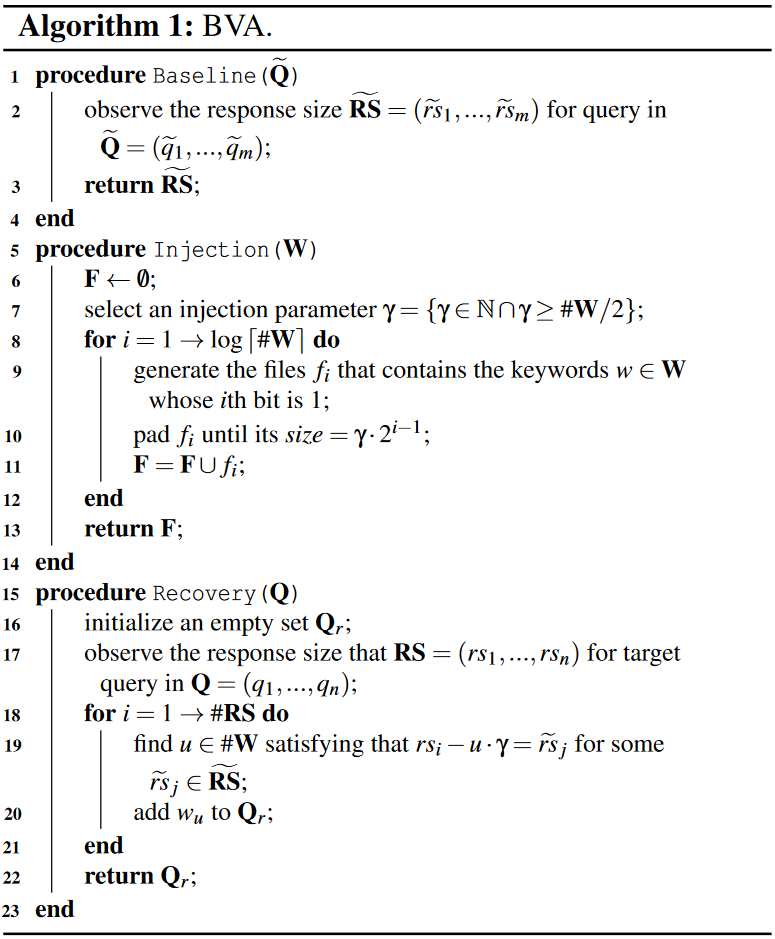


图2.2 BVA攻击算法流程

在基准阶段，对手观察并记录未知查询的响应大小。在注入阶段，它根据注入参数以二进制方式生成并注入文件。在最后一个阶段，对手观察客户端的查询序列与响应大小并作为攻击目标。它旨在恢复中的所有查询。

* BVA—Baseline：对手观察一系列查询的响应大小（第2行）。
* BVA—Injection：对手利用集合标识关键字全集，并用集合 标识注入的文件。首先，敌手自适应地选择满足和的注入参数，以确保每个文件可以容纳一半的关键字（第7行）。其次，每个文件的大小为，并且包含第位等于1的关键字，因此当查询时，注入文件的总响应大小为（第 8-12 行）。
* BVA—Recovery：对于目标查询，敌手再次观察到。对于响应大小为的查询，它遍历（从基准阶段获得）得到一个，满足条件：。然后对手用恢复查询（第 18-21 行）。
  1. **BVA举例**

假设已知明文关键词集，选择安全参数取，并将所有文件的标识符转化为二进制，即，随后生成注入文件，使得每个文件包含所有第位为1的关键词，如图2.3生成注入文件:

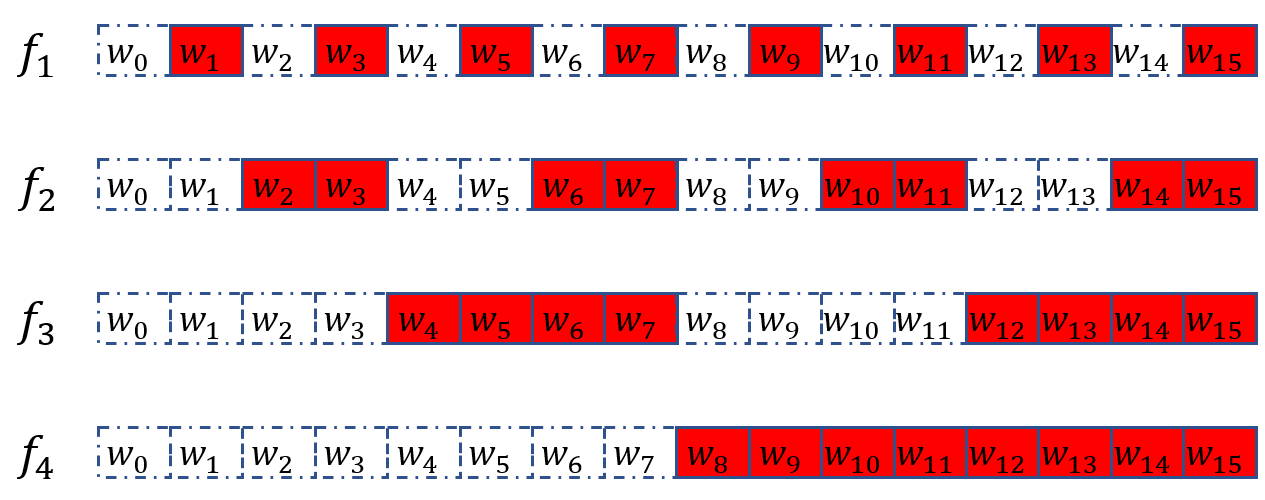


图2.3 生成的注入文件

然后将每个注入文件填充至，即填充后文件的大小为8，16，32，64，如图2.4所示：

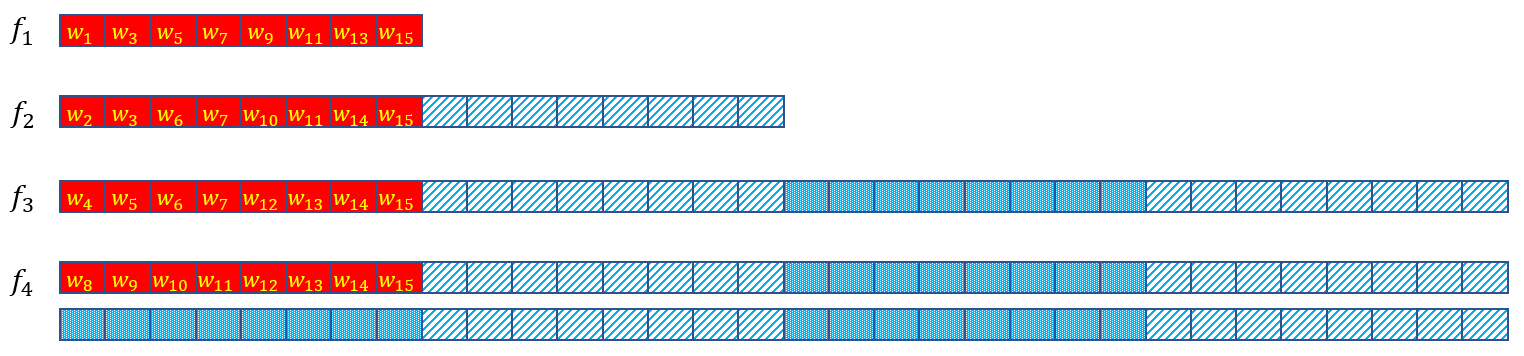


图2.4 BVA填充后的注入文件

将生成好的注入文件注入，随后由客户上传至服务器。敌手对客户在注入完成后的查询继续进行观察，如果注入后的某次查询比注入前的某次查询的rsp多了，那我们可以认为这两次的查询都对应着关键词。

例如，假设注入前的查询的响应长度为15，而注入后的查询的响应长度为87，，，则我们可以认为查询与对应的底层明文为。

* 1. **BVMA攻击**

为了进一步优化注入大小并提高最坏情况下的恢复率（即），Liu等人又通过结合vp和sp提出了BVMA(Binary Volumetric Matching Attack)攻击。通过仔细控制每个注入文件的大小，BVMA 可以确保每个已知关键字都有不同的注入量。对于任何查询，它都可以根据注入前后响应结果的差异来揭示底层关键字。BVMA是第一个结合了响应长度和大小模式（以及 sp）的注入攻击。该组合可以以较小的注入量精确过滤已知的候选关键字，从而提高恢复率。

BVA（见图2.5）的工作原理如下：

* BVMA—Baseline：这类似于 BVA的基准阶段，但经过一段时间的观察，敌手可从中得到查询的响应长度和响应大小以及从搜索模式中得到的查询频率。（第2行）
* BVMA—Injection：敌手仍以二进制方式注入文件。不同于BVA（其中注入文件的大小取决于，敌手设置文件的大小为，包含第位为1的关键字（第711行）。对于关键字，我们将其注入长度记录为，注入大小等于。每个关键字都有一对唯一的注入大小和长度，因此敌手可以以较高的概率区分不同的关键字。
* BVA—Recovery：敌手结合泄漏模式来过滤候选关键词。对于目标查询，敌手通过添加所有来生成候选集，其中（第16行）。一开始，敌手利用rsp从中移除不满足的（第21-23行）。这个条件意味着和分别不是的原始响应大小和底层关键字。在第二个过滤阶段，我们通过利用 rlp排除那些不满足的候选关键字（第24-26行）。如果条件不成立，我们确认和分别不是注入前的响应长度和正确的恢复关键字。然后我们从候选集中删除对。最后，我们可以使用sp从CA的剩余候选关键字中识别基准阶段和恢复阶段之间最接近的查询频率（第28行）。我们注意到sp适度提高了恢复率。但即使不使用它，BVMA 仍然可以实现大约 80% 的恢复率，如图2.6。

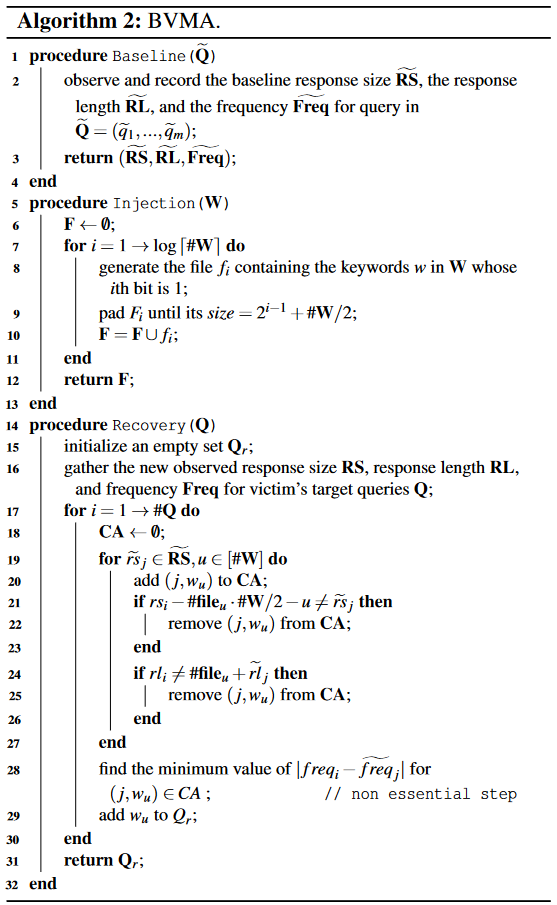


图2.5 BVMA攻击算法流程

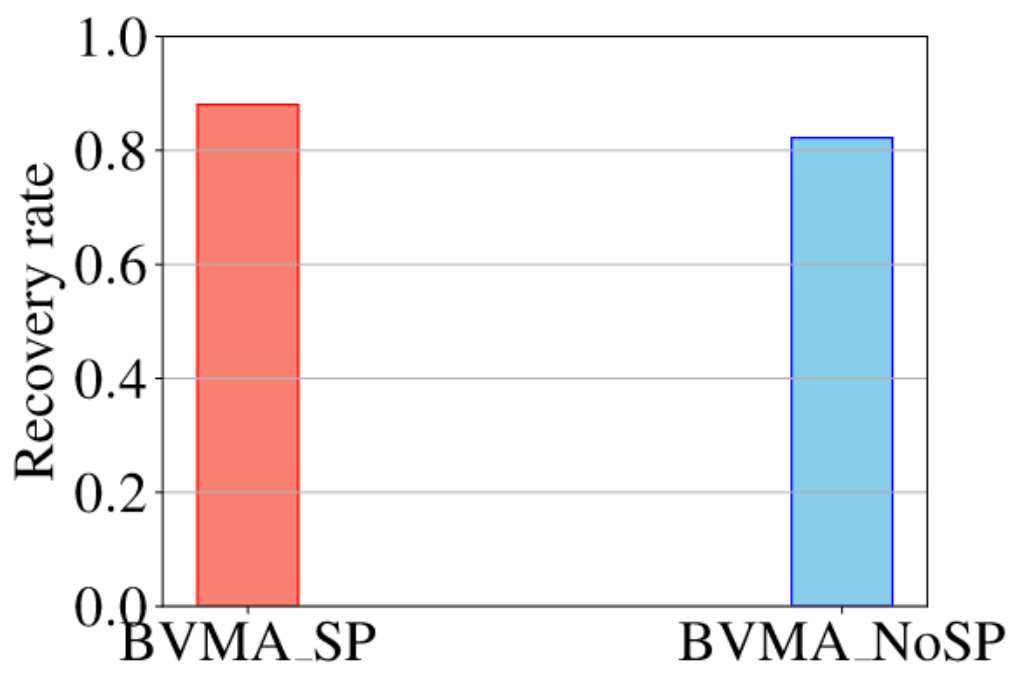


图2.6 sp对BVMA恢复率的影响

* 1. **BVMA举例**

首先根据2.4中的数据集生成图2.3中的注入文件。随后将每个文件填充至，即填充后文件的大小为9，10，12，16，如图2.7所示：

这样关键词对应的rsp为 ，对应的rlp为将转为二进制后包含的1的个数。

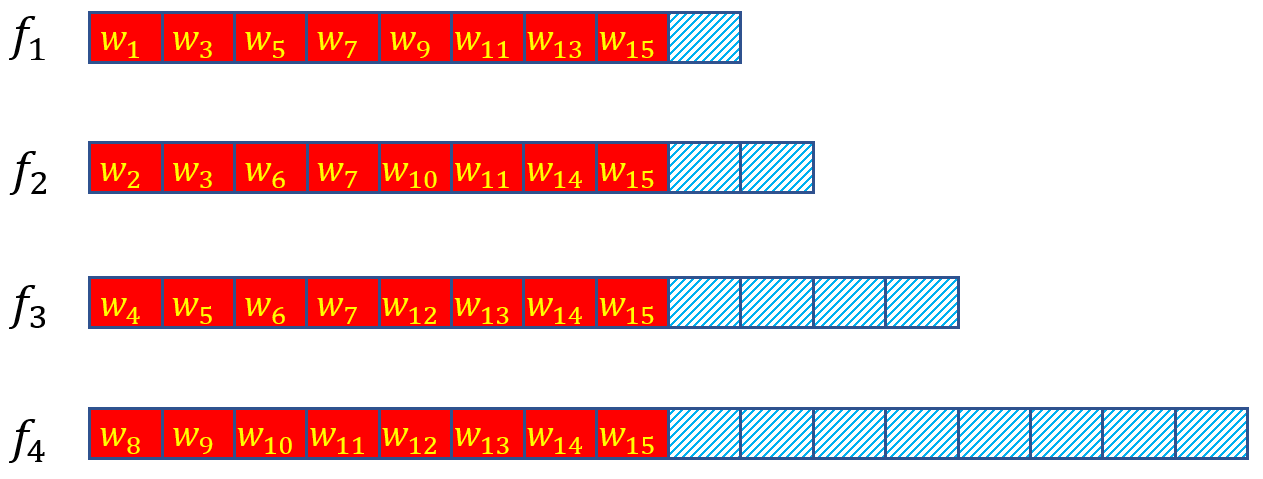


图2.7 BVMA填充后的注入文件

将生成好的注入文件注入，随后由客户上传至服务器。敌手对客户在注入完成后的查询继续进行观察，如果注入后的某次查询比注入前的某次查询的rsp多了𝑢+#𝐖/2⋅，rlp多了将转为二进制后包含的1的个数，那我们可以认为这两次的查询都对应着关键词。

例如，假设注入前的查询的响应大小为3，响应长度为15，而注入后的查询的响应大小，响应长度为40，，则我们可以认为查询与对应的底层明文为。

* 1. **对抗TC策略**

TC(Threshold Countermeasure)[26]表示阈值策略，指客户能够将每个（加密的）文件的词数限制在一个较小的阈值，以防御注入攻击。阈值T在实践中可以设置得相对较小以对抗注入攻击，而不会严重影响动态 SSE 的功能。例如，Enron数据集(#W = 3000)中只有3%的文件包含超过500个单词。如果使用T = 500的 TC，我们可以从索引中跳过这3%的文件。在此设置下，动态 SSE 可以有效地抵抗先前的攻击。Liu等人提出了一种通用的转换方法来“保护”Volume泄露滥用攻击。主要使用了cutting和refilling的方法分别拆分原始数据集，但是分别保证rsp和rlp保持不变。

* Cutting：对于每个原始文件拆分为文件集合，包含个子文件，每个中包含个关键词，每个中包含不同的关键词，这样可以保证rlp在转换前后保持不变。
* Refilling：在Cutting的基础上，为每个生成个副本，每个size为，构成集合，随后生成尽可能少的文件，加起来包含的所有关键词，每个文件的size为，构成集合，这样可以保证rsp在转换前后保持不变。

1. **Volume隐藏SSE方案**

为了应对日益强大的Volume泄露滥用攻击，Volume隐藏SSE方案也得到了长足的发展。本文我们将重点描述Wang[25]等人提出的不需要填充虚拟值的HR(Hash Ring)方案。

* 1. **Hash Ring**

Hash Ring最早被提出是为了解决负载均衡问题。为了将一组对象分配给一些服务器，哈希函数将对象（的标识符）或服务器作为输入，输出位作为标识符环中的槽标识符，模（即0到）。当足够大的时候，标识符冲突的概率可以忽略不计。每个对象都将分配给从其顺时针方向放置在第一个插槽中的服务器。如图3.1，对象与被分配给，而对象与则分配给。

数据同样可以利用这种结构来构建索引，如图3.2，每个索引（红色节点）被唯一分配给一个对应的值（蓝色节点）。而为了解决Volume Hiding问题，在两个蓝色节点中插入一个不存在的虚拟索引（红色圆圈），将其分配给顺时针遇到的第一个值（蓝色节点），如图3.3。

* 1. **方案描述**

方案完整描述见如图3.4。

* Setup：
  1. 数据结构：设 是的所有（非加密）键对应值的数量。客户端为哈希环初始化数组

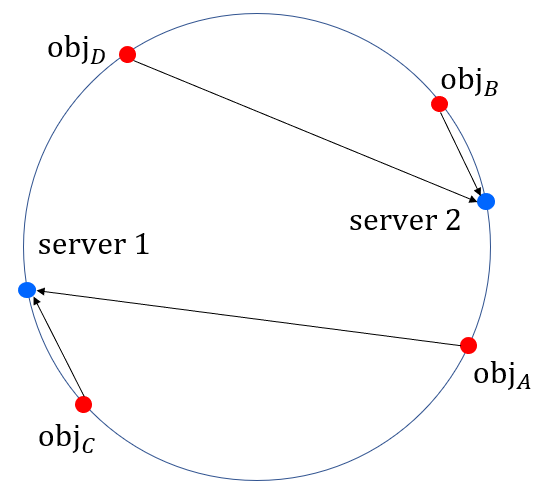


图3.1 Hash Ring

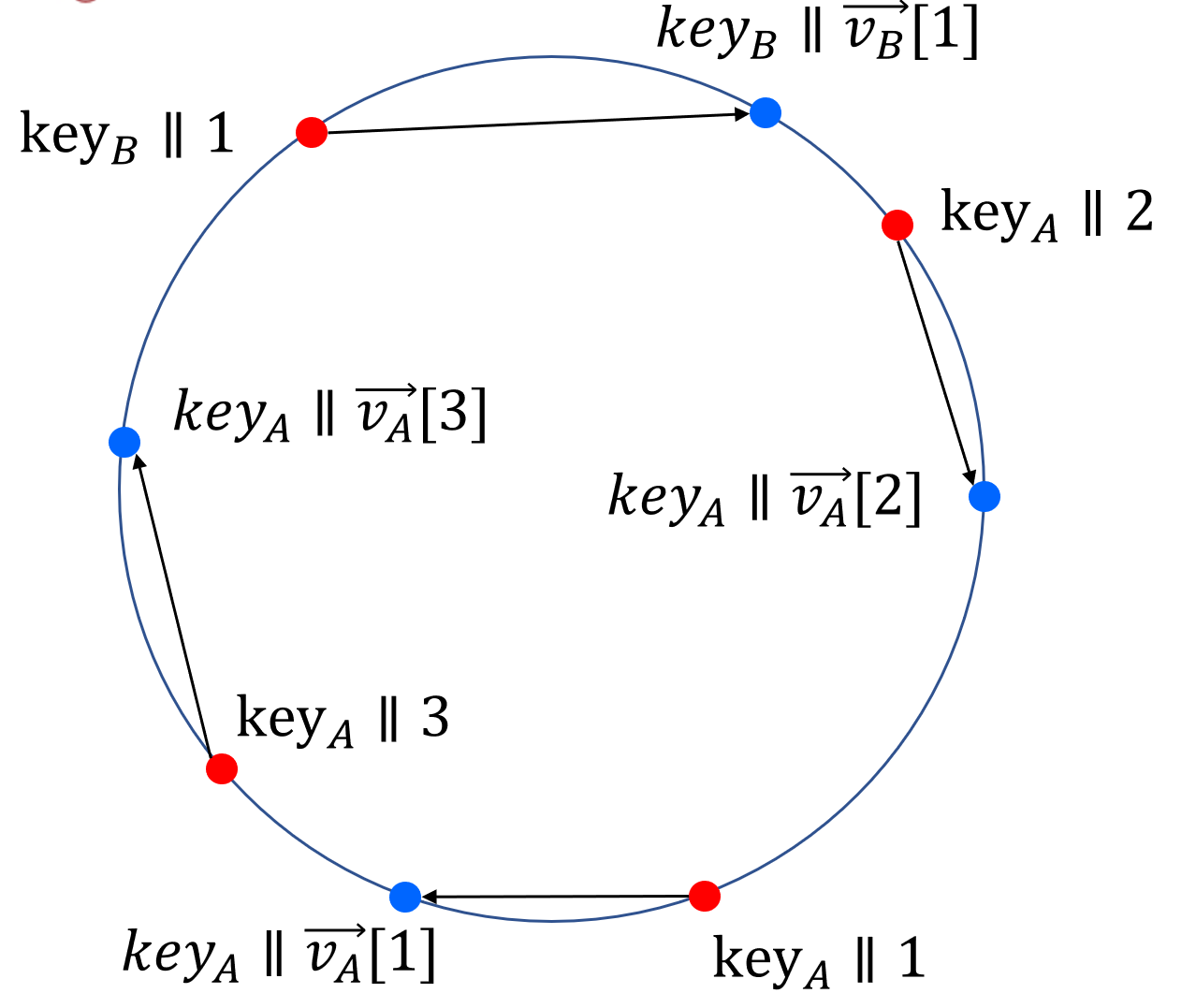


图3.2 Hash Ring构建SSE索引

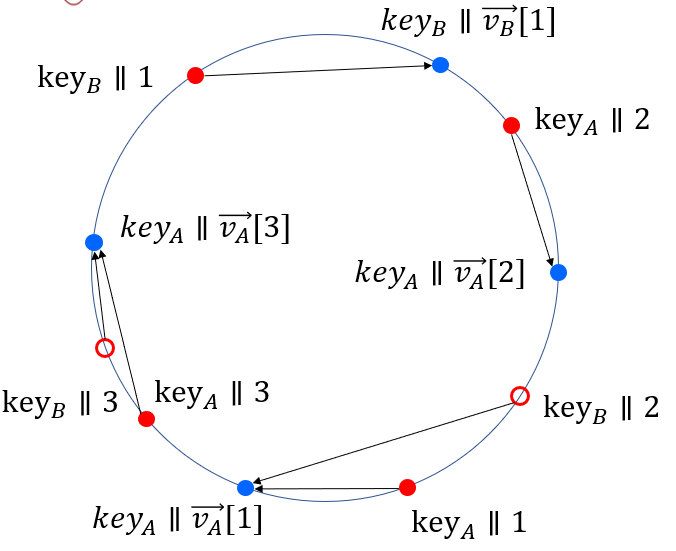


图3.3 Hash Ring构建Volume Hiding的SSE索引

、、和字典、，它们最初都是空的。

1. 客户状态：对于每个，客户端随机选取一个比特长的比特串。存储volume与。
2. 哈希环HR：对于关联的每一个值，客户端通过确定一hash环槽，将其放入U中某个未被占用的槽中，将键值元组存储在 中。
3. 红色节点：作为密文的边界，HR的个槽被占用了个。然后将存储在中的这些位置按升序排序。
4. 蓝色节点：存储密文，对于每个，客户端从中随机抽取一个整数，对于，则在

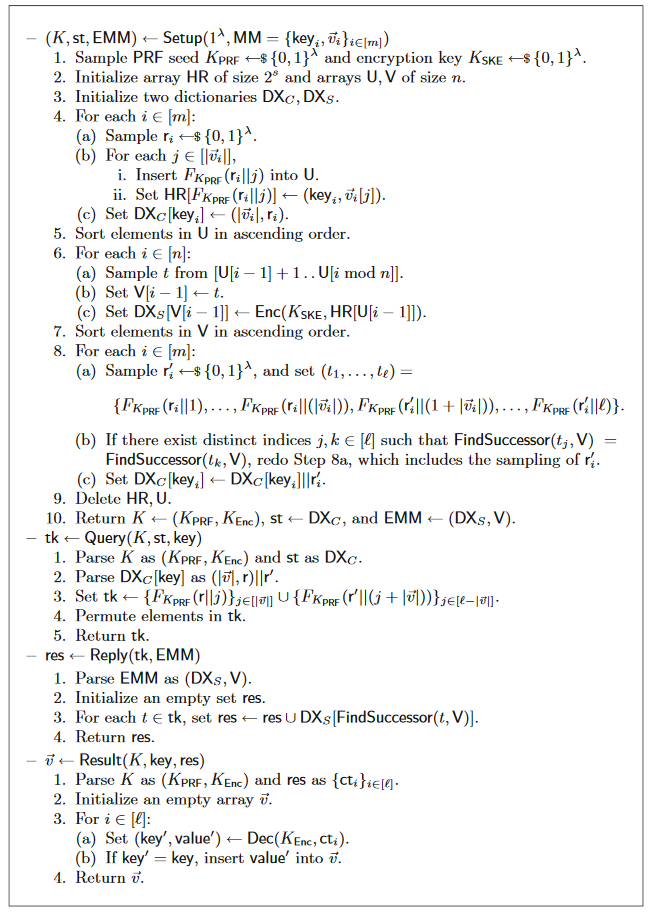


图3.4 Hash Ring Volume隐藏SSE方案完整流程

中取。客户端将设置为，并在中存储处的键值元组的加密。

1. 用于生成令牌的红环tk：对应于的每个，客户端采样另一个位随机数，并输出一个元组 ：

其中前个值是对应的值，其余都是虚假值。

* Query：
  1. 为了搜索，客户在中搜索出。
  2. 然后计算令牌：
  3. 客户讲令牌打乱后发送给服务器。
  4. **方案不足**

该方案虽然号称可以到达动态Volume Hiding的效果，但是其实只是采用了批更新的策略，即在积累够一定数量的更新操作后，将其全部更新为一个新的数据库，本质上并没有真正意义实现细粒度的更新。

1. **结 论**

本文针对Volume泄露滥用攻击与Volume隐藏SSE方案进行了阐述，了解了Volume泄露的含义。对已有的Volume泄露滥用攻击与Volume隐藏SSE方案进行了一个总结，并重点描述了BVA攻击、BVMA攻击与Hash Ring方案。通过以上工作，就如何更深度的利用Volume泄露以及建立更强大的Volume隐藏方案（例如动态方案）进行了深刻的思考。

**参考文献：**

1. Georgios Kellaris, George Kollios, Kobbi Nissim, and Adam O’Neill. 2016. Generic Attacks on Secure Outsourced Databases. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016. 1329–1340.
2. <https://www.idc.com/cn/home>
3. D.X.Song, D.Wagner, and A.Perrig, “Practical techniques for searches on encrypted data,” in Proceeding 2000 IEEE Symposium on Security and Privacy. S&P2000, 2000, pp. 44–55. doi: 10.1109/SECPRI.2000.848445.
4. E.-J.Goh, “Secure Indexes.” 2003.[Online].Available: <https://eprint.iacr.org/2003/216>
5. R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” in Proceedings of the 13thACM Conference on Computer and Communications Security, in CCS’06. New York, NY, USA: Association for Computing Machinery, 2006, pp.79–88. doi: 10.1145/1180405.1180417.
6. Mei L, Xu C, Xu L, et al. Practical Multi-Source Multi-Client Searchable Encryption With Forward Privacy: Refined Security Notion and New Constructions[J]. IEEE Transactions on Dependable and Secure Computing, 2023
7. Wang J, Chen X, Sun S F, et al. Towards efficient verifiable conjunctive keyword search for large encrypted database[C]//Computer Security: 23rd European Symposium on Research in Computer Security, ESORICS 2018, Barcelona, Spain, September 3-7, 2018, Proceedings, Part II 23. Springer International Publishing, 2018: 83-100.
8. D.Cash, S.Jarecki, C.Jutla, H. Krawczyk, M.-C.Roşu, and M. Steiner, “Highly-Scalable Searchable Symmetric Encryption with Support for Boolean Queries,” in Advances in Cryptology – CRYPTO 2013, R. Canetti and J.A. Garay, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 353–37
9. Demertzis I, Chamani J G, Papadopoulos D, et al. Dynamic searchable encryption with small client storage[J]. Cryptology ePrint Archive, 2019.
10. C.Hu and L.Han, “Efficient wildcard search over encrypted data,” International Journal of Information Security, vol. 15, no. 5, pp. 539–547,Oct. 2016, doi: 10.1007/s10207-015-0302-0.
11. Bost, R. Σoφoς : Forward secure searchable encryption. In: E.R. Weippl, S. Katzenbeisser, C. Kruegel, A.C. Myers, and S. Halevi (eds.), ACM CCS 16, pp. 1143–1154. ACM Press (Oct. 2016).
12. Bost R, Minaud B, Ohrimenko O. Forward and backward private searchable encryption from constrained cryptographic primitives[C]//Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017: 1465-1482.
13. M. Damie, F. Hahn, andA. Peter, “A HighlyAccurate Query-RecoveryAttack against Searchable Encryption using Non-Indexed Documents,” in 30th USENIX Security Symposium (USENIX Security 21), USENIX Association, Aug. 2021, pp. 143–160. [Online].Available:https://www.usenix.org/conference/usenixsecurity21/presentation
14. S. Oya and F. Kerschbaum, “Hiding the Access Pattern is Not Enough: Exploiting Search Pattern Leakage in Searchable Encryption,” in 30th USENIX Security Symposium (USENIX Security 21), USENIX Association, Aug. 2021, pp. 127–142. [Online].Available:https://www.usenix.org/conference/usenixsecurity21/presentation/oya
15. D. Pouliot and C. V. Wright, “The Shadow Nemesis: Inference Attacks on Efficiently Deployable, Efficiently Searchable Encryption,” inProceedings of the 2016ACM SIGSACConference onComputer andCommunications Security, inCCS ’16. New York,NY,USA:Association forComputingMachinery,2016, pp. 1341–1352. doi: 10.1145/2976749.2978401.
16. J. Ning et al., “LEAP: Leakage-AbuseAttack on Efficiently Deployable, Efficiently Searchable Encryption with Partially Known Dataset,” in Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security, in CCS ’21. New York,NY,USA:Association forComputingMachinery,2021, pp. 2307–2320. doi: 10.1145/3460120.3484540.
17. Grubbs P, Lacharité M S, Minaud B, et al. Pump up the volume: Practical database reconstruction from volume leakage on range queries[C]//Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. 2018: 315-331.
18. Lacharité M S, Minaud B, Paterson K G. Improved reconstruction attacks on encrypted data using range query leakage[C]//2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018: 297-314.
19. Zhang X, Wang W, Xu P, et al. High Recovery with Fewer Injections: Practical Binary Volumetric Injection Attacks against Dynamic Searchable Encryption[J]. arXiv preprint arXiv:2302.05628, 2023.
20. Kamara S, Moataz T. Computationally volume-hiding structured encryption[C]//Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part II 38. Springer International Publishing, 2019: 183-213.
21. Zhao Y, Wang H, Lam K Y. Volume-hiding dynamic searchable symmetric encryption with forward and backward privacy[J]. Cryptology ePrint Archive, 2021.
22. Amjad G, Patel S, Persiano G, et al. Dynamic volume-hiding encrypted multi-maps with applications to searchable encryption[J]. Cryptology ePrint Archive, 2021.
23. Patel S, Persiano G, Yeo K, et al. Mitigating leakage in secure cloud-hosted data structures: Volume-hiding for multi-maps via hashing[C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. 2019: 79-93.
24. Wang J, Sun S F, Li T, et al. Practical Volume-Hiding Encrypted Multi-Maps with Optimal Overhead and Beyond[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. 2022: 2825-2839.
25. Wang J, Chow S S M. Simple Storage-Saving Structure for Volume-Hiding Encrypted Multi-maps: (A Slot in Need is a Slot Indeed)[C]//Data and Applications Security and Privacy XXXV: 35th Annual IFIP WG 11.3 Conference, DBSec 2021, Calgary, Canada, July 19–20, 2021, Proceedings. Cham: Springer International Publishing, 2021: 63-83.
26. Yupeng Zhang, Jonathan Katz, and Charalampos Papamanthou. All your queries are belong to us: The power of file-injection attacks on searchable encryption. In 25th USENIX Security Symposium, USENIX Security 16, pages 707–720, 2016.
27. Rishabh Poddar, Stephanie Wang, Jianan Lu, and Raluca Ada Popa. Practical volume-based attacks on encrypted databases. In IEEE European Symposium on Security and Privacy, pages 354–369, 2020.
28. Laura Blackstone, Seny Kamara, and Tarik Moataz. Revisiting leakage abuse attacks. In 27th Annual Network and Distributed System Security Symposium, 2020.
29. Karger, D.R., Lehman, E., Leighton, F.T., Panigrahy, R., Levine, M.S., Lewin, D.: Consistent hashing and random trees: distributed caching protocols for relieving hot spots on the world wide web. In: Annual ACM Symposium on the Theory of Computing (STOC), pp. 654–663 (1997)