Leakage-Abuse Attacks Against Searchable Encryption

文献5：针对密文检索的泄露利用攻击

Zhou Jiancong

2022.4.14

主要贡献

本文是一篇类综述性质的文章，主要贡献如下：

1、对L1-L4由高至低给出了4个级别的安全性定义

2、针对in-place及encrypted-index 2种主流的SE方案技术路线，概述了目前5种主流方案，并断言加密索引方案具备更好的安全性，可能成为未来的趋势

3、针对攻击模型，分析了攻击模式、敌手知识、敌手目标的概念；

4、针对基于索引的攻击及对基于部分明文的攻击，详细阐述了5种攻击方案（其中4种是作者原创）

提纲

① SE方案的4个安全级别

② SE方案的2大技术路线

③ 攻击模型

④ 索引恢复攻击

⑤ 部分明文恢复攻击

⑥ 个人Idea&问题

1-SE方案4个安全性级别

级别	名称	泄露内容	安全性
L1	Query-revealed occurrence pattern （查询时泄露的出现模式）	①全部索引数量（$N=\|D_W\|$）[6] ②检索时，泄露访问模式（Access Patern）[6]	最高
L2	Fully-revealed occurrence pattern （完全泄露的出现模式）	①关键词的出现模式（Occurrence Patern）	高
L3	Fully-revealed occurrence pattern with keyword order （完全泄露关键词顺序的出现模式）	①关键词的出现模式（Occurrence Patern） ②命中关键词在文档的顺序（Document Order）	低
L4	Full plaintext under deterministic word-substitution cipher （全明文下的确定性密码替换）	①关键词在文档中出现的位置信息（Access Patern） ②每个关键词出现的频次（Search Patern）	最低

1-SE方案4个安全性级别-例证

假设搜索的明文相同（“dog”），从左至右为L4至L1，Server端被泄露的内容

L4泄露内容

Document 1
8OG4qbr Wavtgpc TP1l2tf optdn0n
t2EK8Sp 5LLEuwc SflnwMp FzlwsWH
bZO1Hpf hB1iYbT

Document 2
Ba2donz aSby7AV Pk9MnzP KJvrBga
ojtE0fS t2EK8Sp isxWNuS

“dog” → Wavtgpc

Document 1
8OG4qbr **Wavtgpc** TP1l2tf optdn0n
t2EK8Sp 5LLEuwc **Wavtgpc** FzlwsWH
bZO1Hpf hB1iYbT

Document 2
Ba2donz aSby7AV Pk9MnzP KJvrBga
ojtE0fS **Wavtgpc** isxWNuS

① 关键词出现的位置信息
② 关键词出现频次

L3泄露内容

0	D02	D08	D10	D11	D19	D77	D84	
1	D05	D08	D12	D35				
2	D11	D24	D55	D61	D63	D69	D71	D77	D91
3	D18	D35	D40	D59	D84	D85			

“dog” → 1, 2

0	D02	D08	D10	D11	D19	D77	D84	
1	D05	D08	**D12**	D35				
2	D11	D24	D55	D61	D63	D69	D71	D77	D91
3	D18	D35	D40	D59	D84	D85			

① 关键词的出现模式
② 命中关键词在文档中的顺序

L2泄露内容

0	D02	D08	D10	D11	D19	D77	D84	
1	D05	D08	D12	D35				
2	D11	D24	D55	D61	D63	D69	D71	D77	D91
3	D18	D35	D40	D59	D84	D85			

“dog” → 1

0	D02	D08	D10	D11	D19	D77	D84	
1	**D05**	**D08**	**D12**	**D35**				
2	D11	D24	D55	D61	D63	D69	D71	D77	D91
3	D18	D35	D40	D59	D84	D85			

① 关键词的出现模式

L1泄露内容

Cz1 J57 Eyj FG0 SQJ Kot vXT c23 u47
PId F17 RN7 hB0 BJI GGI wZV l8H aHc
tvo 0G0 1YC mlz 3dT j07 imb g3L j6n

“dog” → <key>

Cz1 **D05** Eyj FG0 SQJ Kot vXT e23 u47
PId F17 RN7 **D08** BJI GGI **D12** l8H aHc
tvo 0G0 1YC mlz 3dT **D35** imb g3L j6n

① 所有关键词的数量
② 检索时泄露关键词命中文档

2-SE方案2大技术路线

- In-place SE schemes
- Client端直接加密的文档数据，检索时Server端通过对每个文档的keywords进行迭代检索，这是最简单的方案，并且与现有的许多API都兼容

2-1 Full-text substitution cipher

编号	名称	描述
1	初始化过程	Client解析每个文档，提取每个关键词进行确定性加密后上传至Server端
2	检索过程	Client对待检索关键字加密后上传至Server端，Server端进行逐一比对
3	安全级别	L4
4	泄露内容	（1）关键词在文档中出现的位置信息 （2）每个关键词出现的频次
5	优势	（1）方案简单，易于实现及部署，与很多现有的API兼容 （2）支持boolean search 及 phrase search
6	不足	（1）泄露信息最多（攻击者可以知道密文的位置并统计词频） （2）不支持stemming（词干提取），wildcard（通配符），approximate-match searching （模糊查询）

2-2 Appended-keywords SE

编号	名称	描述
1	初始化过程	对文档D进行常规的随机对称加密，并在生成密文的后面附上计数器值对应的伪随机函数FK(Wi[ci])
2	检索过程	Client端计算关键词的FK值，然后上传至Server端进行检索
3	安全级别	L4（若允许重复，允许频率信息检索） L3（直接PRF值） L2（上传PRDF值之前先对PRF值排序）
4	泄露内容	（1）co-occurrence relationships （2）counts of the number of unique indexed keywords （3）密文长度 （4）关键词出现顺序
5	优势	（1）遗留兼容的（例如增加或删除hash很容易） （2）可以在关键字提取过程中支持词干提取
6	不足	敌手可以学习co-occurence pattern(几个关键词同时出现在文档中)、唯一索引关键字的数量、密文长度以及关键字在文档中出现的顺序。

备注：文献【8】和【14】采用了上述方案。

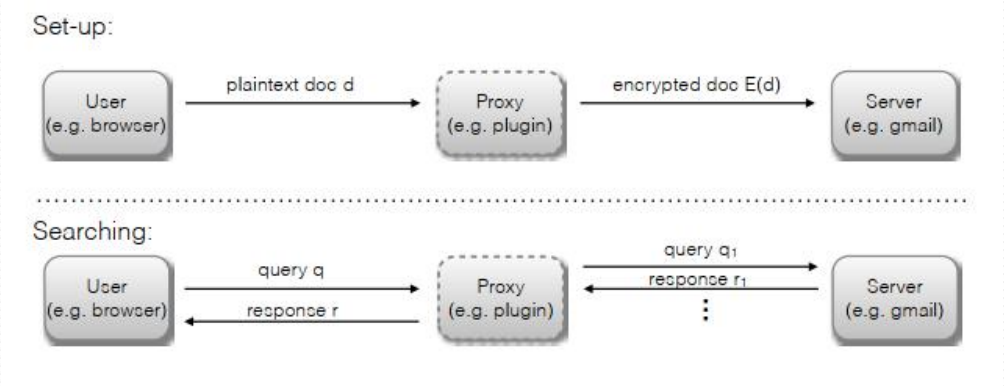
2-2 Appended-PRF SE的应用

- 已在工业界广泛应用
- 已经较为成熟并在Skyhigh Networks，CipherCloud，bitglass等多个商用加密产品中应用
- 兼容遗留方案（legacy compatible），可以很好的支持密文插入与检索

2-2 Appended-PRF SE的应用

- 介绍了2款产品，对应文献【8】和【14】

文献【8】旨在在用户端和服务端之间建立代理，托管SE加密，实现对恶意网站的防护



文献【14】旨在允许向不可信的移动应用程序输入机密数据，它通过操作系统在移动应用程序的GUI上插入一个透明的加密层实现

在ShadowCrypt中，网页是不受信任的，应用程序可能是恶意的，加密仍然应该阻止应用程序学习关于明文数据的信息。

2-SE方案2大技术路线

- Encrypted-index SE
- 基于索引加密的SE方案是指在Client端上传数据之前首先将索引加密。
- 检索时需要Client端对每个查询都生成一个trapdoor并发送给Server，trapdoor允许服务器只解密与搜索词对应的文档标识符
- 我们之前精读的文献1-4中，除了关于数据结构的文献2，都是基于Encrypted-Index SE方案

2-3 Unencrypted inverted index

编号	名称	描述
1	初始化过程	索引的反向索引I(inverted index)以明文直接传至Server端，并且客户端会随机打乱关键词和对应行的关系
2	检索过程	Client端向Server端发送trapdoor，Server返回关键词对应一行
3	安全级别	L2
4	泄露内容	Server端可以直接观察所有结果集的长度，并且对所有关键词构造co-occurrence matrix
5	优势	
6	不足	

2-3 Encrypted inverted index, no result length hiding

编号	名称	描述
1	初始化	相比unencrypted inverted index方案每一行的索引将作为一个整体加密，在发出查询之前，不会从索引中读取重复的文档id
2	检索	Client端检索时通过向Server发送trapdoor，Server解密与关键字对应的索引行。
3	安全级别	由于是过渡方案未定义
4	泄露内容	未查询时，每行的长度是暴露的 查询完成时，服务器获得关于结果集中文档重叠的信息。
5	优势	支持boolean查询
6	不足	boolean查询除上述内容外，存在额外泄露

2-4 Fully length-hiding SE

编号	名称	描述
1	初始化	-
2	检索	-
3	安全级别	L1
4	泄露内容	全部索引的长度之和
5	优势	每个检索结果集合的长度也是保密的
6	不足	-

文献【18】通过填充list为固定长度，使得检索结果的长度保密；
文献【6】使用交织的链表结构代替了填充，实现了检索结果的长度保密；
文献【4】实现boolean查询，比暴露一行中的所有单词泄露了更少的信息。

2-SE方案2大技术路线对比

- 考虑到 encrypted-index SE方案对比In-place SE schemes方案普遍存在的泄露更少，作者断言encrypted-index SE会是未来的发展趋势。

3-攻击模型-3种攻击模式

假设：一是敌手都是Server端，攻击动机是尽可能地获取更多文档的明文信息

攻击名称	描述	主动/被动	研究现状
被动监听	一个honest-but-curious的服务端会严格遵守协议，会监听Client与Server端的通信，但并不进行任何主动的攻击动作	被动	大量研究
选择文档攻击	一个主动的Server端可以执行chosen-document attack，并欺骗客户端将一个选择的文档包含在文档集中，以便学习到更多的明文信息	主动	研究较少
选择查询攻击	敌手服务器可能通过诱导客户端发出某些查询来发起选择查询攻击，从而暴露该查询所泄露的信息	主动	目前条件下不现实

3-攻击模型-3种攻击模式

- 关于chosen-document attack，作者举了2个实例。
- 假设使用SE自动对邮件的收件箱进行加密及备份，恶意的Server端可以发送一封他们选择的电子邮件消息给受害者。只要它在进入受害者的收件箱之前没有被垃圾邮件过滤器删除，这将成功地迫使SE应用于随后由Server端观察到的密文的消息。
- 另一个例子是《ShadowCrypt》。回想一下，在这里，用户单击网页中的一个按钮，指示浏览器应该对某个表单字段中的数据进行加密。这个网页被认为是恶意的。这里，可以使用点击顶起类型的技术来装载选中文档攻击。这个网页有一个“加密字段”的按钮隐藏在一个看起来无害的框架后面，用户必须在正常的网站交互中点击这个按钮。网页可以使用这种技术，让用户在不知情的情况下指示ShadowCrypt加密网页选择的数据。作者承认，对他们的系统进行点击劫持攻击是可能的，实际上，它们可能会产生比我们在这里考虑的更直接的攻击向量。然而，这表明主动攻击通常是可能的

3-攻击模型-敌手知识

名称	敌手掌握的知识	备注
Distributional query knowledge	查询的上下文信息 （如了解查询的目标是日志）	
Known queries	已知部分查询内容 （如掌握部分keyword-query对）	
Distributional document knowledge	文档的上下文信息 （如了解文档的内容是邮件、聊天记录）	
Known documents	已知部分文档明文 （如掌握部分keyword-query对）	
Fully-known document set	已知文档全部明文信息	需要额外获取的信息是全部或部分查询信息

3-攻击模型-敌手目标

查询恢复：Query recovery (QR)

- 查询恢复的目标是确定客户机发出的查询的纯文本。其在某些查询未知的情况下被考虑，包括文档完全或部分已知的情况。

部分密文恢复：Partial plaintext recovery (PR)

- 敌手通过学习关键字到加密密文的映射，尽可能多地重建Client端的索引文档。其可能会将纯文本暴露为“一堆文字”或按文档顺序还原。

* 文档存在：document presence （不是本文重点）

- 敌手只是希望确定已知的纯文本文档是否存在于Client端的索引中

* 文档表示符：document identification（不是本文重点）

- Server想要找到SE方案中已知文档的文档id之间的对应关系

3-攻击方案概述

Objective	Prior Knowledge	Pas/Act	Min Leakage	Known Constructions	Where
Query Recovery	Fully Known Docs	Passive	L1	All	[9], § 4.2
Query Recovery	Partially Known Docs	Passive	L1	All	§ 4.3
Plaintext Recovery	Known Doc Subset	Passive	L3	–	§ 5.1
Plaintext Recovery	Distributional	Chosen Doc	L3	–	§ 5.2
Plaintext Recovery	Distributional	Chosen Doc	L2	Shadowcrypt, Mimesis	§ 5.2

4-索引恢复攻击

- IKK Attack
- Query Recovery with a Counting Attack
- Query Recovery from Partially Known Documents

4-1 IKK Attack（前人工作）

- M. S. Islam[8]的文章使用了安然电子邮件数据集，在某些词汇大小发查询还原率超过80%。
- 攻击假设Server端知道一个固定的大小为m的搜索关键词集合，并且对于文档集合D的知识是分布式的（即可以精确构造一个m×m的同时出现矩阵C）
- Server通过观察q个查询构造1个标准化的关于C置换的子矩阵C_t，利用模拟退火方法找出最佳的C_t，矩阵的row是对查询词的猜测集合
- 优点：成功率在很大程度上与查询数量无关
- 不足：对手的优势强烈地依赖于考虑的关键字的数量m，对于关键词数量很大时性能很差。

4-2 Query Recovery with a Counting Attack

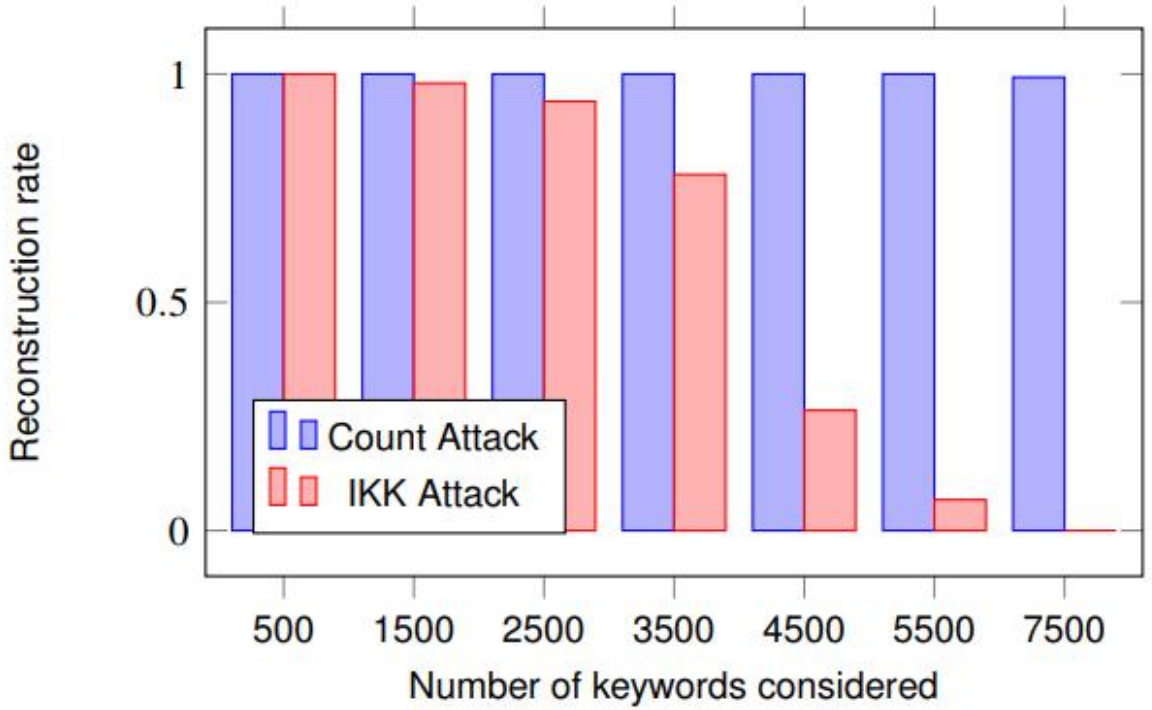
- IKK方案需要知道出现矩阵C（还需知道文档的全部明文信息），本方案的假设更强，除此之外还需知道命中关键词返回的索引数。
- 攻击的目标是获取Client端检索的关键词明文
- 该攻击利用这样一个假设，如果count(w)等于某值对应的关键字是唯一的（如只有关键词‘cat’满足count=9），那么根据count(w) = count(q)，通过观测count(q)的值，查询关键词就可知。

4-2 Query Recovery with a Counting Attack

- IKK方案需要知道出现矩阵C（还需知道文档的全部明文信息），本方案的假设更强，除此之外还需知道命中关键词返回的索引数。
- 该攻击利用这样一个假设，如果count(w)等于某值对应的关键字是唯一的（如只有关键词‘cat’满足count=9），那么根据count(w) = count(q)，通过观测count(q)的值，查询关键词就可知。

4-2 Query Recovery with a Counting Attack对比IKK

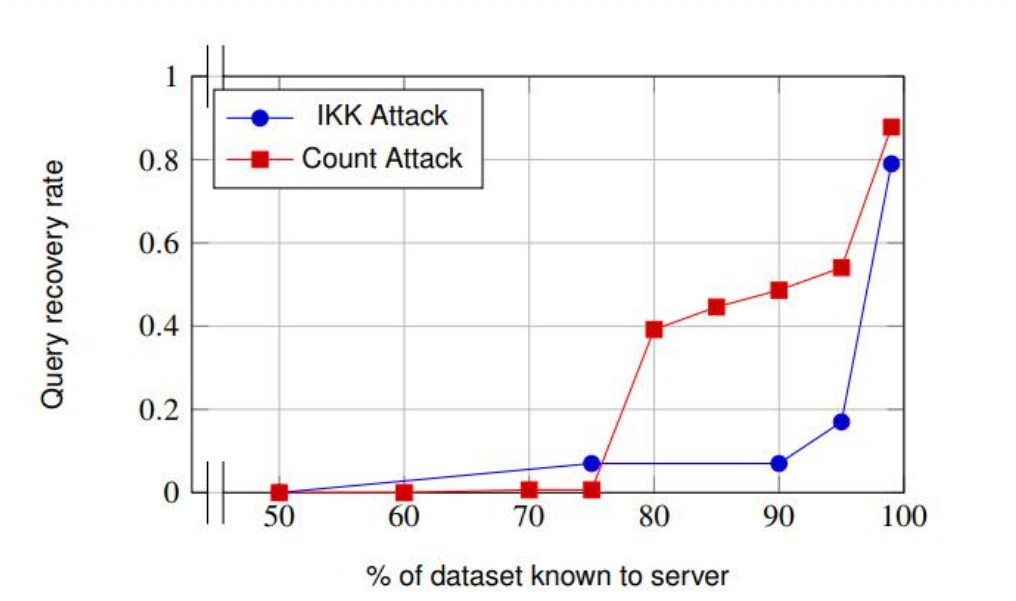
- **还原率**：关键词数量较大时，还原率显著优势
- **还原速度**：IKK需要数小时，本方案只需几秒



对策：使用填充，客户端附上虚假文档ID条目填充索引，以降低计数攻击的有效性

4-3 Query Recovery from Partially Known Documents

- 该方案相较4-2放宽了要求，Server端不要求已知全部的明文信息，知道部分的明文信息即可，攻击目标依然是获取搜索的关键词明文。
- 算法允许在一个共出现计数窗口内的关键字和候选，而不是要求精确相等
- 需要服务器仅了解80%的数据集才能进行重要的查询恢复

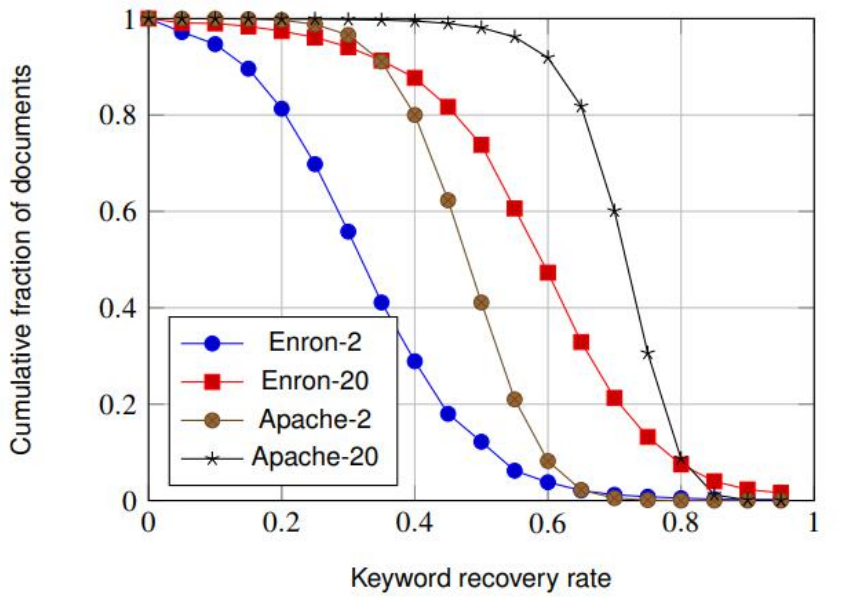


5-部分明文恢复攻击

- Known-Document Attacks（L3:Order of Hashes Known）
- Known-Document Attacks（L2:Order of Hashes Unknown）
- Active Attacks（L3：Hash order known , chosen document）
- Active Attacks（L2：Hash order unknown , chosen document）

5-1 Known-Document Attacks（L3:Order of Hashes Known）

- 不隐藏”关键词在文档中顺序-哈希后顺序“的对应关系



原始邮件

The attached contract is ready for signature. Please print 2 documents and have Atmos execute both and return same to my attention. I will return an original for their records after ENA has signed. Or if you prefer, please provide me with the name / phone # / address of your customer and I will Fed X the Agreement.

还原的关键词

attach contract signatur pleas print 2 document have execut both same will origin ena sign prefer provid name agreement

- 左图（横坐标表示关键词还原率，纵坐标表示文档内容的一致程度）为给定2个或20个明文文档，以5%为间隔，量化Server端在少量文档解析出的明文关键词百分比。曲线越往右下降，表明关键字还原率越高，即给定明文文档越多且文档聚集率越高，能够还原的关键词就越多。
- 右图是一个实例，还原的关键词已经能够包含部分原始邮件中的敏感内容
- 此外，文档的公开性越强（被更多人接收），关键词越容易被还原

5-1 Unknown-Document Attacks（L2:Order of Hashes Known）

- 若Hash存储在关键字的顺序是随机的,Server（虽然拥有很多文件明文信息）不能立即确定每个关键字对应文档中的Hash,即使它知道的文档对应关键字Hash集合

- 作者给出了不确定性（ambiguity）的概念，当服务器知道多个文档时，可以通过在已知文档中使用关键字的共现模式来减少歧义，但是对其没有详细描述

5-2 Active Attacks

- 在主攻攻击中，Server端的能力除了监听Client端加载的数据外，还可以在那些将由Client端处理的文档中“植入”，并将其添加到上传的数据集
- 这种攻击模型可以被看作是用于加密的选择明文攻击模型(CPA)的模拟
- 例如，恶意服务端向客户端发送一封电子邮件，然后客户端将其编入索引并上传到服务器
- 我们假设，通过观察有效载荷长度和/或文档上传的时间，对手可以确定哪个索引或数据库条目对应于他放置的文档，我们以关键字还原率来衡量明文恢复的水平

5-2 Active Attacks（L3：Hash order known , chosen document）

- Server端可以将任意关键字集合及文档植入数据库中，然后通过加密可以了解关键字对应的所有哈希值。我们不进一步探讨这种简单但显然非常具有破坏性的攻击

5-2 Active Attacks（L2：Hash order unknown , chosen document）

- 提出并分析了一个基于相关语料（orpus）分析的攻击，该攻击允许服务器权衡错误概率与插入文件的大小和数量，给出了一个有效和灵活的攻击策略。
- 从已知的相关语料库中，敌手生成一个按频率排序的关键字列表。固定文档大小k，敌手将排序的关键字列表分成k个大小相等的切片。然后，通过从每个切片中选择排名最高的词，生成一个k-word文档。目标是最大化给定文档中关键字之间的频率距离（frequency distance）
- 敌手还计算客户端上传的数据中关键字哈希值的频率分布并观察植入文档中的单词的哈希值，根据它们在上传数据集中的频率对其进行排序，并根据自己的语料库猜测这些哈希值对应于相同级别的关键字。只要两个数据集之间的关键字频率不存在排序颠倒（rank reversals），所有k种猜测都是正确的。对手可以对所有已知的关键字或他能够插入的尽可能多的文档重复这个过程。

5-2 Active Attacks（L2：Hash order unknown , chosen document）

实验过程：

- 实验分为两组，第一组将单个数据集分成两半，服务端“训练”50%的文档以学习关键字频率，而客户端处理另一半文档并将加密的关键字上传到服务器。
- 第二组使用来自Enron数据集的关键字集和频率来攻击Apache数据集，反之亦然。

实验结论：

- 正如预期的那样，每个文档k中切片/关键字的数量越大，出错的概率就越大，因为文档中的单词出现的频率更接近，从而增加了客户机和服务器数据集之间发生排序反转的可能性
- 为了恢复w个关键字，对手必须至少植入w/k个文档，更多的是为了允许错误率。文档大小的选择必须由攻击者期望的错误率和被检测的概率决定。无论如何，即使是能够植入少量文档的对手，也能通过这种攻击掌握敏感的关键字选择