西安電子科技大學
XIDIAN UNIVERSITY

Cash方案实现架构

——汇报人：张中俊

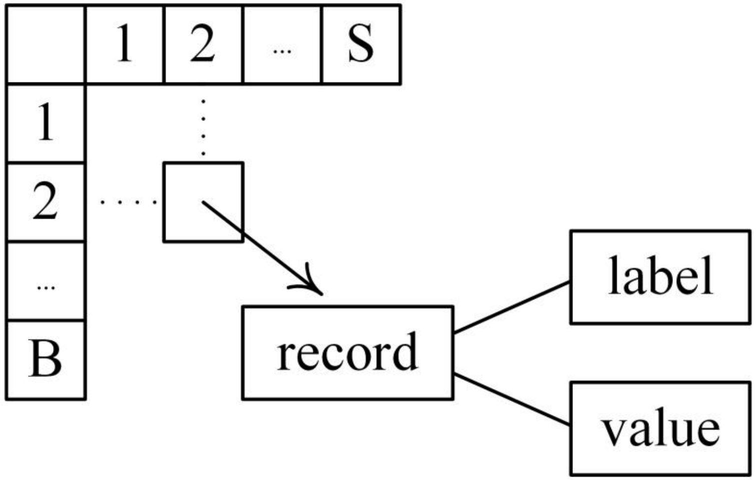
TSet实例化

- TSet定义:$\Sigma = (TSetSetup, TSetGetTag, TSetRetrieve)$
- TSet正确性：只需满足对于所有的W、T，任意的$w \in W$，

若: 1. $(TSet, K_T) \leftarrow TSetSetup(T)$

2. $stag \leftarrow TSetGetTag(K_T, w)$

则一定有：$TSetRetrieve(TSet, stag) = T[w]$

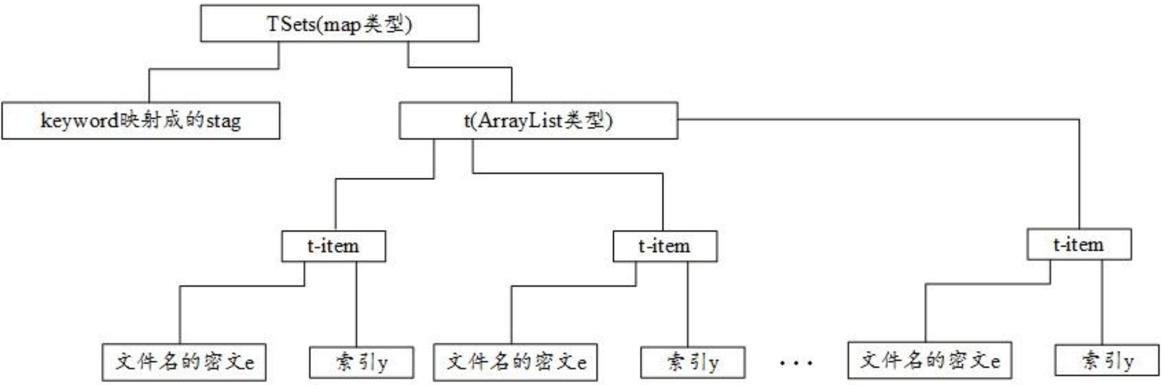


图：Cash给出的一种TSet方案

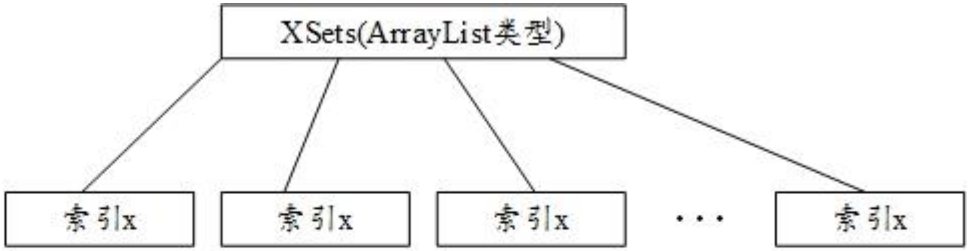
TSet实例化

- 给定安全参数λ，给出两个PRF和一个哈希函数H：
  F: 输入为1~|D[w]|中的整数和$stag$ 输出为 $\{0,1\}^{\lambda}$
  $\overline{F}$: 将关键词w 映射为 $stag$
  H: 将$\{0,1\}^{\lambda}$ 映射为 $\{1,2,\cdots,B\}\times\{0,1\}^{\lambda}\times\{0,1\}^{n(\lambda)+1}$
- TSetSetup
  - 对每个关键词 $stag \leftarrow \overline{F}(K_T, w)$
  - 对关键词的每一个文件名 $(b, L, K) \leftarrow H(F(stag, i))$
  - $record \leftarrow \{value: (\beta|s_i) \oplus K, label: L\}$，最后一个文件名$\beta = 0$
  - 将record放在Tset矩阵的第b行中
- TSetRetrieve
  - 计算得到(b, L, K)
  - 遍历TSet的第b行，将record的value中的β提取出来
  - 如果$\beta = 0$，停止搜索

Cash方案的总览



图：TSets的结构

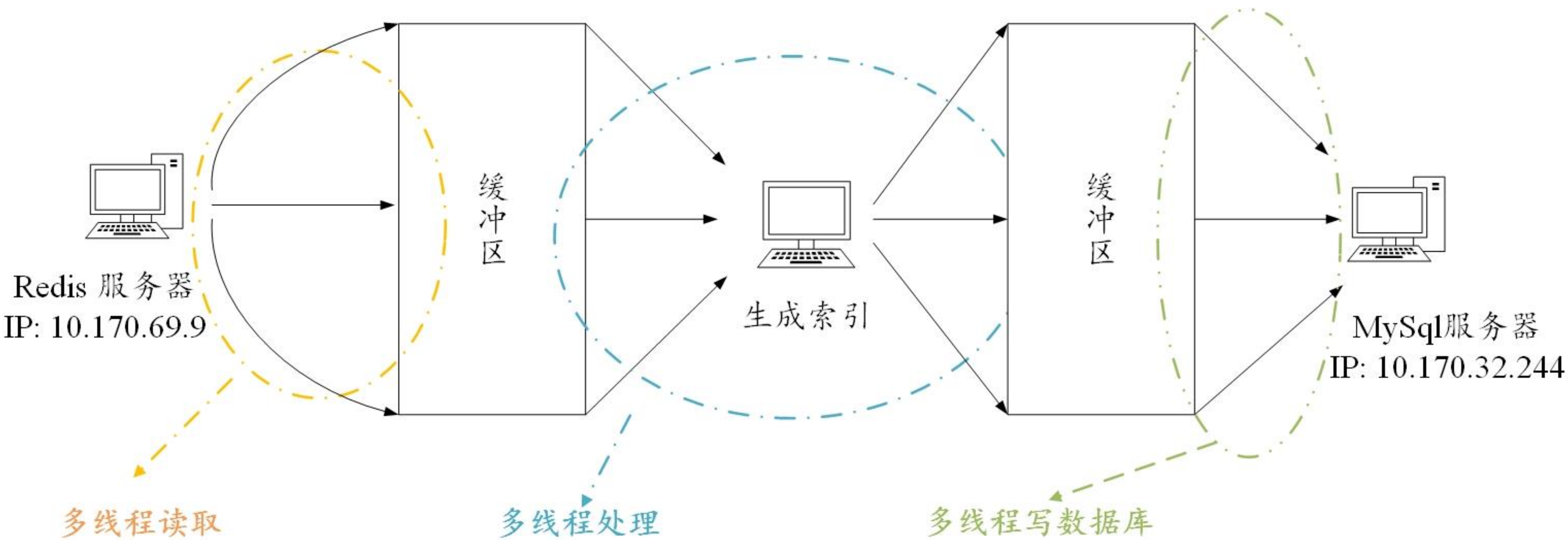


图：XSets的结构

- 索引y：$F_p(K_I, ind) \cdot \left(F_p(K_Z, w||c)\right)^{-1}$
- 索引x：$g^{F_P(K_X,w)\cdot F_p(K_I,ind)}$
- 搜索的token：$xtoken[c,i] = g^{F_p(K_Z,w_1||c)\cdot F_p(K_X,w_i)}$
- 搜索：$xtoken[c,i]^y \in XSets$

如何存储原始文件

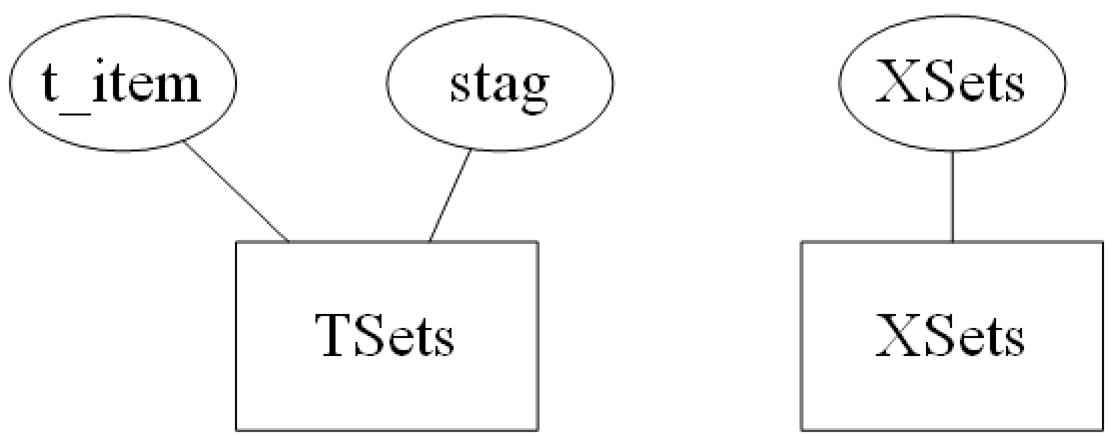
- 使用redis数据库存储，原因如下：
  1. no-sql类型的数据库，完美契合关键词-文件名的数据形式
  2. 内存型数据库，读取速度快



图：整体架构

如何存储TSet和XSet

- 存储在MySql数据库中
- 存储类型主要考虑在搜索时候各个字段的行为：
  - 在搜索中，XSets中主要是做匹配，存储为字符串类型即可，长度为311，分配400的长度
  - 在搜索中，TSets中的stag也是为了做匹配，存储为字符串类型即可，测试下长度为74，分配100的长度
  - 在搜索中，需要密文e和索引y，我们将其存储为blob类型，之后再反序列化为ArrayList<t_item>对象



图：数据库的E-R图

如何存储Master Key

- 本算法设计到的Master Key包括：
  - KI：用于生成索引y
  - Kz：用于生成索引y
  - Kx：用于生成索引x
  - Ks：用于生成加密文件名的密钥Ke
  - Kt:
  - g：双线性对的生成元
- 把他们序列化到txt文本文件中，用到的时候再反序列化出来。

- pairing不必存储，因为我们使用的pairing是固定的

一个小想法

- 密文e是冗余的
- EDBSetup算法中的算法框架：

```
for w in W:
        for ind in DB.get(w):
                生成e
```

这样的话，文件名的密文是冗余的。

如何修改方案，使得只生成一次文件名即可。

搜索的详细步骤——客户端

1. 首先做出预测，含有关键词w1的文件不超过100个
2. 接着生成如下的xtoken矩阵，其中kws是所有搜索的关键词
3. 生成w1对应的stag
4. 提交stag 和 xtoken到服务器

	i = 1	i = 2	……	i = |kws|
c=0				
c=1				
……				
c=99				

搜索的详细步骤——服务器

- 根据stag找到t
- t中的每一个t_item都是备选答案，且t中的y等于$y = F_p(K_I, ind) \cdot \left(F_P(K_Z, w_1 || \mathrm{c})\right)^{-1}$
- 遍历t中的每一个t_item，从i=2开始检查（i=1是w1，肯定满足），如果都有$xtoken[c, i]^y \in XSets$，则第c个t_item就是答案

- 索引x：$g^{F_P(K_X, w) \cdot F_p(K_I, ind)}$
- $xtoken[c, i] = g^{F_p(K_Z, w_1 || \mathrm{c}) \cdot F_p(K_X, w_i)}$