西安电子科技大学
XIDIAN UNIVERSITY

VDB实验汇报

——张中俊

Vi生成过程

- abiding:9:{'7a780da0-cf1b-469f-a500-de94a241c1ad.txt', 'bd311d49-3258-464a-8eae-a8374e0d5c4a.txt', 'a9875554-1f61-4e48-9709-ec0edd17d19e.txt', 'c69ae895-9f49-4ae5-9fc5-13b107c25c1c.txt', 'fc857357-0e37-44dd-8fd6-e5576677e07f.txt', 'eefe2512-9ef4-4e09-9227-7a56c55d4fa2.txt', 'ba5dfd2e-6ff0-4d7a-b48f-36ec82d43617.txt', 'f89f60e4-b8ed-45f0-aad4-a3c4c91c414c.txt', '4a0ac863-47cf-4b36-aeca-2856444aa3a2.txt‘}
- 关键词为abiding
- 该关键词包含在9个文件中

Vi生成过程

1. 将所有的文件名级联，得到str
2. 将str转化为byte数组（编码格式为utf-8）,记作str_byte
3. 对str_byte进行MD5签名
4. 将str_byte映射到Zr域中

```
MessageDigest md = MessageDigest.getInstance("MD5");
byte[] bytes = md.digest(str.getBytes( charsetName: "utf-8"));
return pairing.getZr().newElementFromHash(bytes,  i: 0, bytes.length);
```

- 有如下的三张表：

1. 表SetupOutput_H_5表示数组H中5行记录
2. 表SetupOutput_H_500表示数组H中有500行记录
3. 表SetupOutput_H_6549表示数组H中有6549行记录

```
mysql> desc setupoutput_h_500;
+-------+---------+------+-----+---------+-------+
| Field | Type    | Null | Key | Default | Extra |
+-------+---------+------+-----+---------+-------+
| i     | int(11) | NO   | PRI | NULL    |       |
| j     | int(11) | NO   | PRI | NULL    |       |
| H_ij  | blob    | YES  |     | NULL    |       |
+-------+---------+------+-----+---------+-------+
3 rows in set (0.07 sec)
```

q=500时候

```
Running com.zhong.VDB_UpdateTest
10次update所用时间为: 317 ms
```

```
Running com.zhong.VDB_QueryTest
数据库加载成功!!!
数据库连接成功!!!
q=500 10次query所用时间为: 58405 ms
```

```
Running com.zhong.VDB_VerifyTest
数据库加载成功!!!
数据库连接成功!!!
q=500 10次verify所用时间为: 556 ms
```

- 比C实现的差一个数量级

VDB				
次数	setup	query	verify	update
0	0	0	0	0
1000	302000000	607048.4	7403.365	3928.157

q=6549的时候

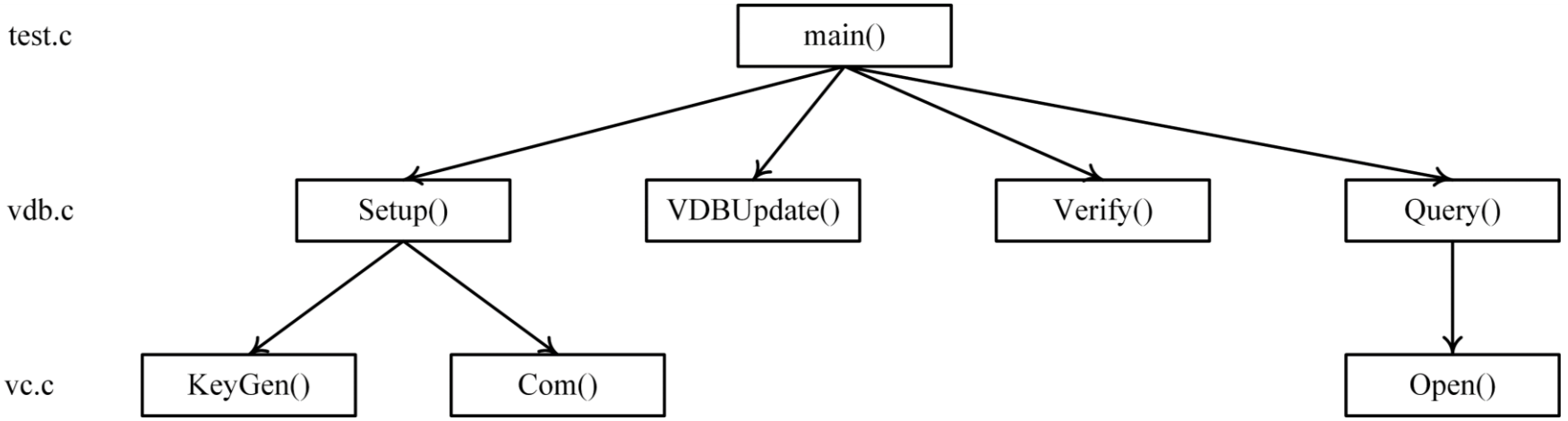
```
Running com.zhong.VDB_UpdateTest
10次update所用时间为: 589 ms
```

```
Running com.zhong.VDB_QueryTest
数据库加载成功!!!
数据库连接成功!!!
q=6549 10次query所用时间为: 762727 ms
```

```
Running com.zhong.VDB_VerifyTest
数据库加载成功!!!
数据库连接成功!!!
q=6549 10次verify所用时间为: 666 ms
```

- $\frac{762727}{58405} = \frac{6549}{500}$
- query和q成线性关系 update和verify与q无关

结果分析


test.c
main()
vdb.c
Setup()
VDBUpdate()
Verify()
Query()
vc.c
KeyGen()
Com()
Open()

结果分析-Query

- Open()函数：
  1. $delta[i] = H[i][1]^{v[1]} \cdot H[i][2]^{v[2]} \cdots H[i][i-1]^{v[i-1]} \cdot H[i][i+1]^{v[i+1]} \cdots H[i][q]^{v[q]}$
  2. 相对于q-1次乘幂运算，q-2次乘法运算
  3. 举例 $q = 4, i = 2$，则$delta[2] = H[2][1]^{v[1]} \cdot H[2][3]^{v[3]} \cdot H[2][4]^{v[4]}$

- 结论： Query的时间 与 q成线性关系

结果分析-Verify

- $temp1 = e(HT[T], g)$
- $temp2 = Hash(c_{up}[0], c_{up}[T])$
- $temp3 = e(temp2, Y)$
- $temp4 = \frac{c_{dn[T]}}{h[i]^{v[i]} \cdot HT[T]}$
- $temp1 = e(temp4, h[i])$
- $temp3 = e(delta[i], g)$

- 结论：
  1. Verify的时间 与 q的大小无关
  2. Verify的时间 与 H无关

结果分析-VDBUpdate

- $temp1 = \frac{m_{new}}{v[i]}$
- $temp2 = \frac{h[i]}{temp1}$
- $temp3 = \frac{c_{dn}[i]}{HT[i]}$
- $c_{up}[i] = temp3 * temp2$
- $c_{dn}[i] = HT[i] * c_{up}[i]$

- 结论：
  1. VDBUpdate的时间 与 q的大小无关
  2. VDBUpdate的时间 与 H无关

谢谢各位专家的指导！