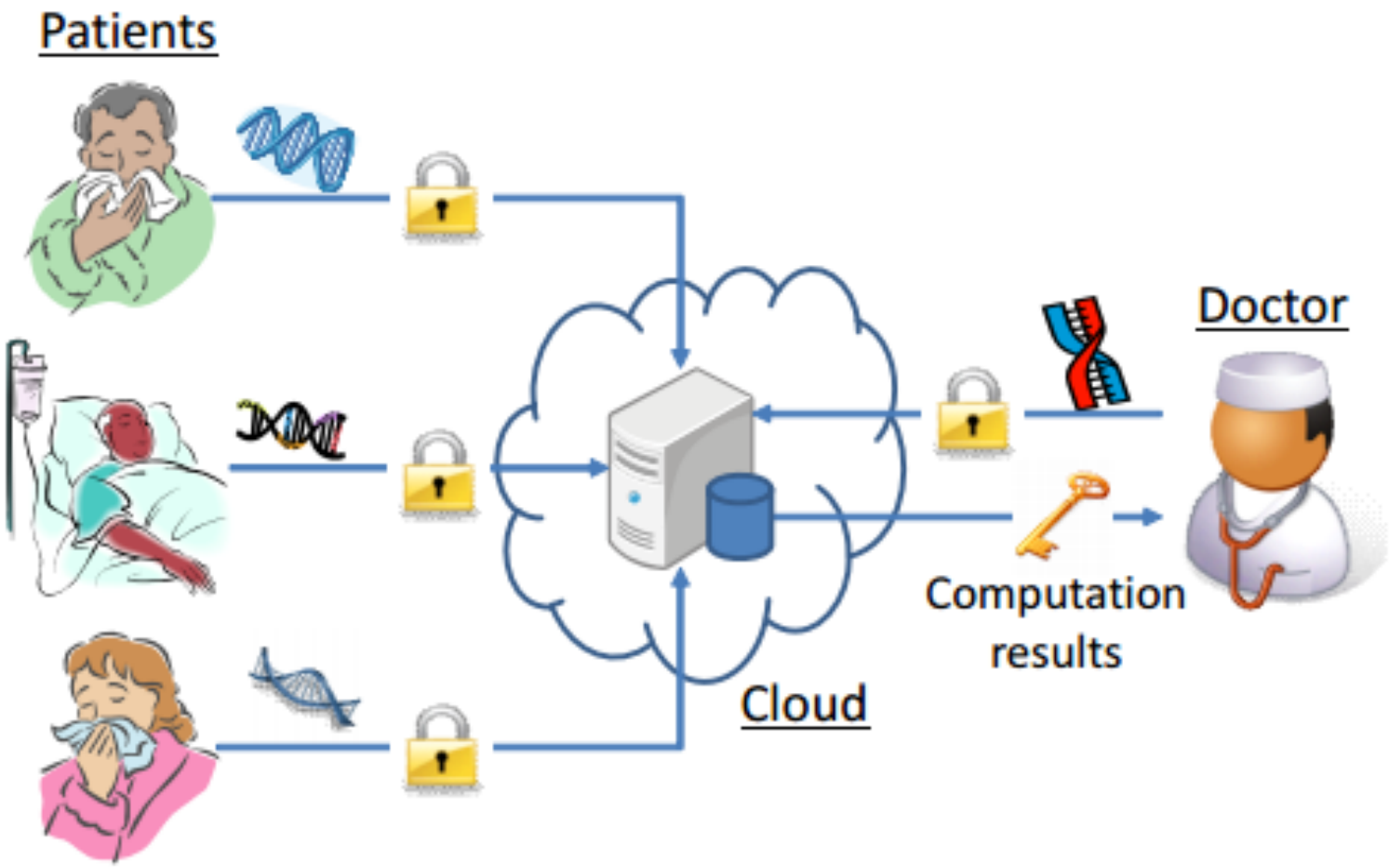
2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

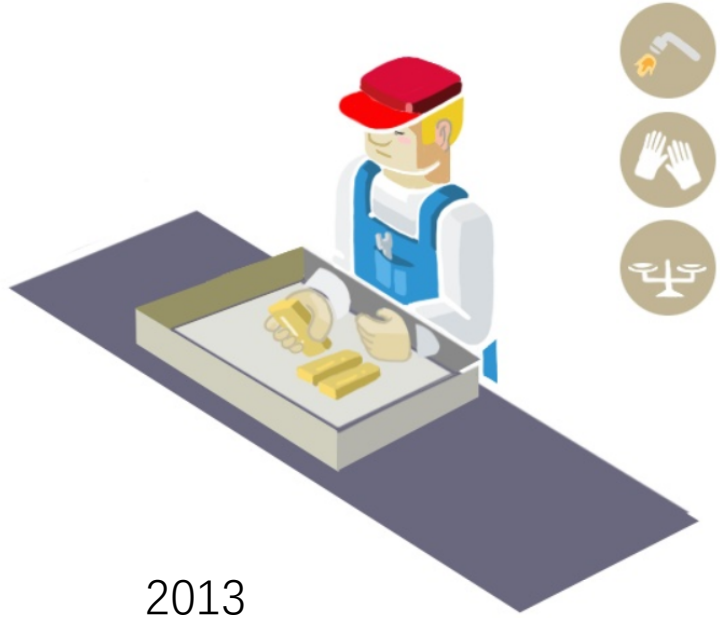
LEAF：基于同态加密的高效密文检索技术

分享人：郁昱

应用场景



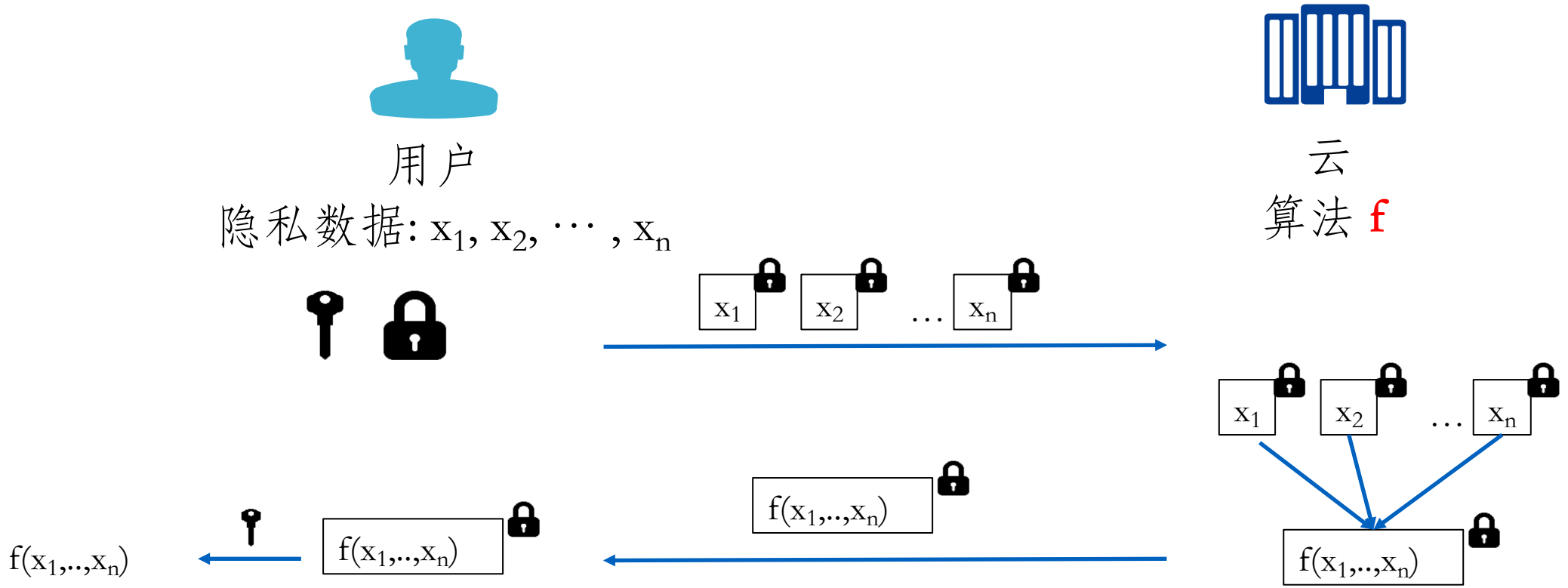
（全）同态加密

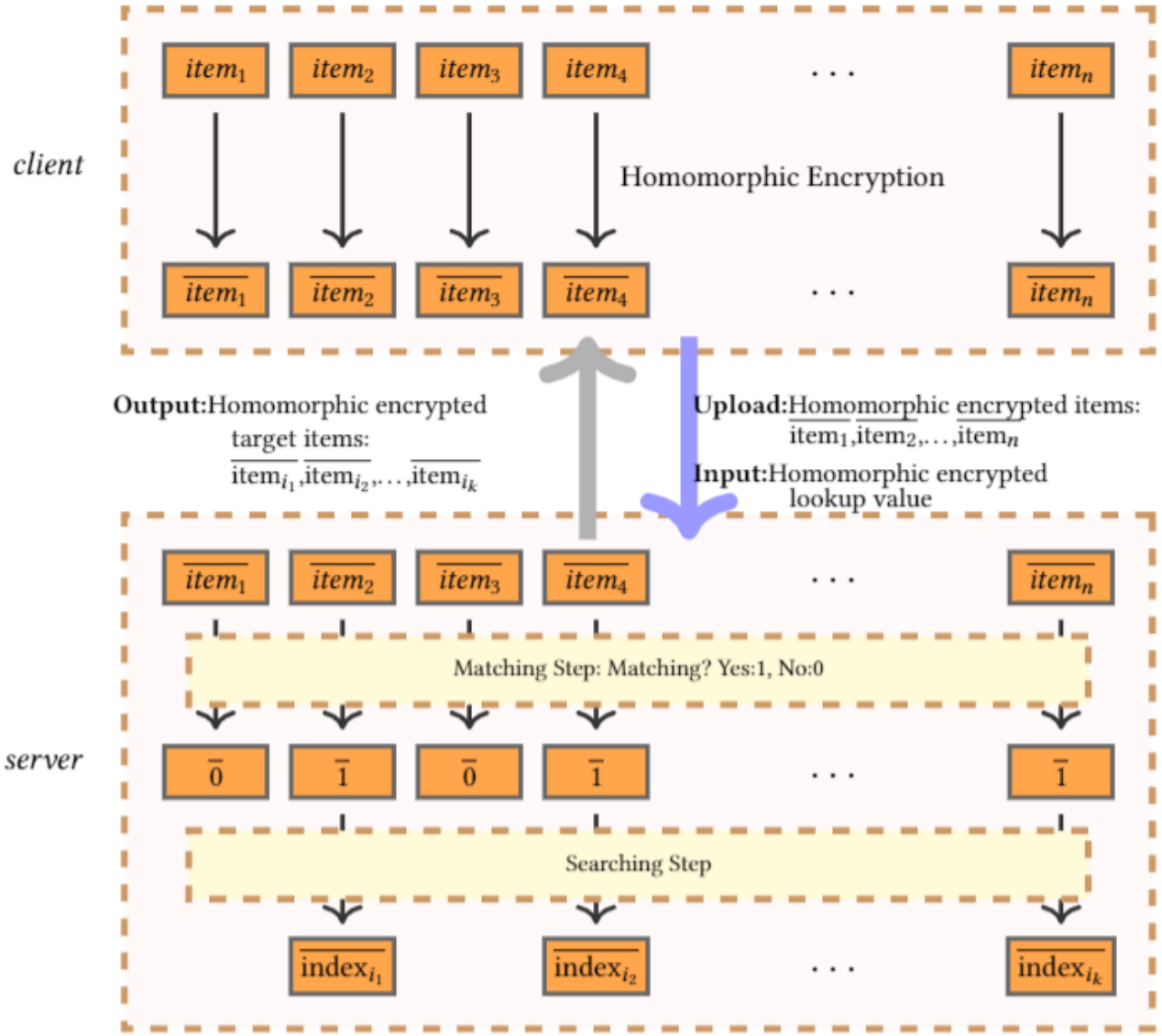


1978	1984 1999	2009	2011 2012	2013
同态加密概念的提出，思想来源于RSA算法	弱同态加密算法 ElGamal，Paillier	全同态方案理论突破 第一代全同态方案 （基于理想格和整数）	第二代全同态方案 （基于RLWE/LWE） 以BGV为代表	第三代全同态方案 （基于RLWE/LWE） 以GSW为代表
R. L. Rivest L. Adleman M. L. Dertouzos	T. ElGamal P. Paillier	C. Gentry	Z. Brakerski C. Gentry V. Vaikuntananthan	C. Gentry A. Sahai B. Waters

同态加密分类

- f=ADD: 加法同态
- f=MUL: 乘法同态
- f={ADD,MUL}: 全同态




client
$item_1$ $item_2$ $item_3$ $item_4$ . . . $item_n$
Homomorphic Encryption
$\overline{item_1}$ $\overline{item_2}$ $\overline{item_3}$ $\overline{item_4}$ . . . $\overline{item_n}$
Output:Homomorphic encrypted target items: $\overline{item_{i_1}}, \overline{item_{i_2}}, \ldots, \overline{item_{i_k}}$
Upload:Homomorphic encrypted items: $\overline{item_1}, \overline{item_2}, \ldots, \overline{item_n}$
Input:Homomorphic encrypted lookup value
server
$\overline{item_1}$ $\overline{item_2}$ $\overline{item_3}$ $\overline{item_4}$ . . . $\overline{item_n}$
Matching Step: Matching? Yes:1, No:0
$\overline{0}$ $\overline{1}$ $\overline{0}$ $\overline{1}$ . . . $\overline{1}$
Searching Step
$\overline{index_{i_1}}$ $\overline{index_{i_2}}$ . . . $\overline{index_{i_k}}$

效率影响因素

- 乘法次数
- 电路深度

Razborov-Smolenski近似方法

$$p(r_j) = \sum_{i=1}^{k} r_j[i] \cdot v[i] \mod 2$$

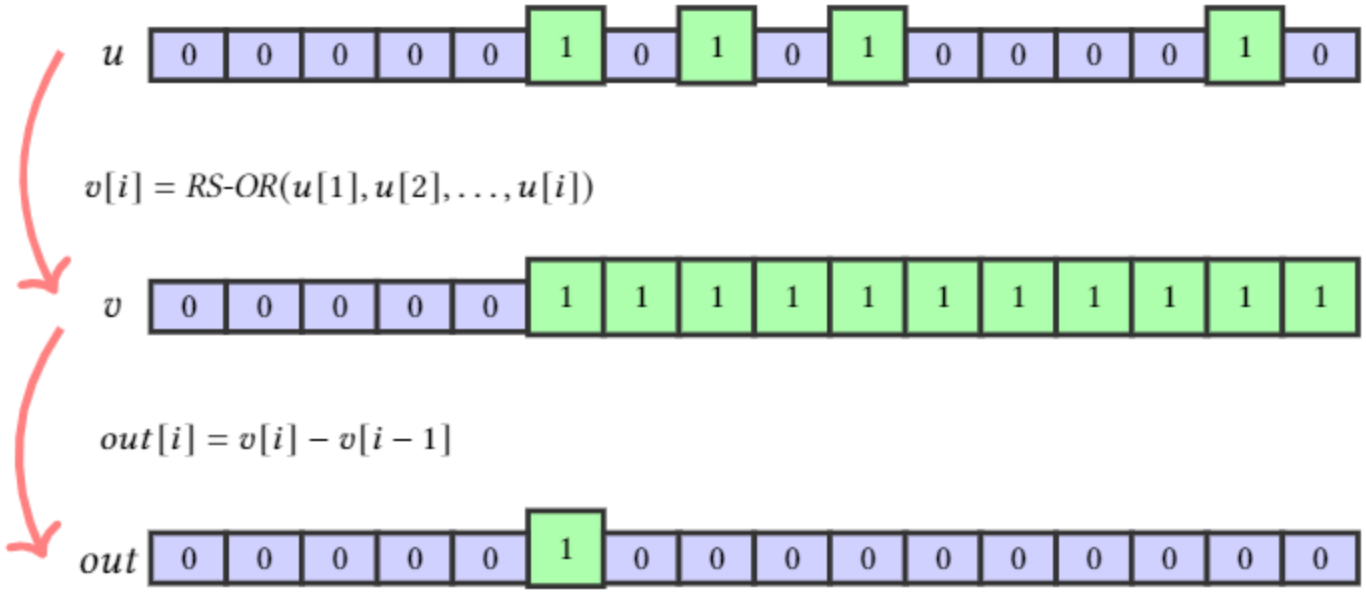
$$RS\text{-}OR(v[1], \ldots, v[k]) = OR\big(p(r_1), \ldots, p(r_{N(\varepsilon)})\big)$$

$$= 1 - \prod_{j=1}^{N(\varepsilon)} \big(1 - p(r_j)\big) \mod 2$$

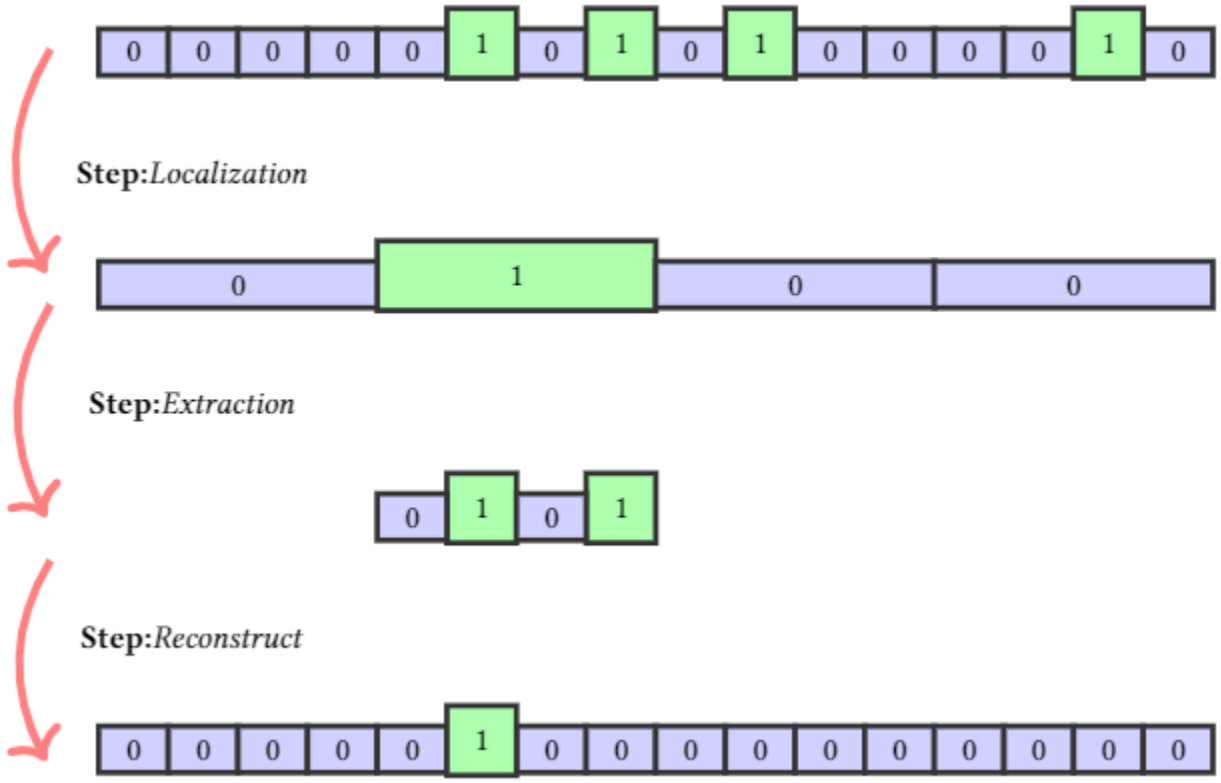
出错率 $\leq \frac{\varepsilon}{n} \leq 2^{-80}$

乘法次数/度：从k降到$N(\varepsilon) = \left\lceil \log(\frac{n}{\varepsilon}) \right\rceil$

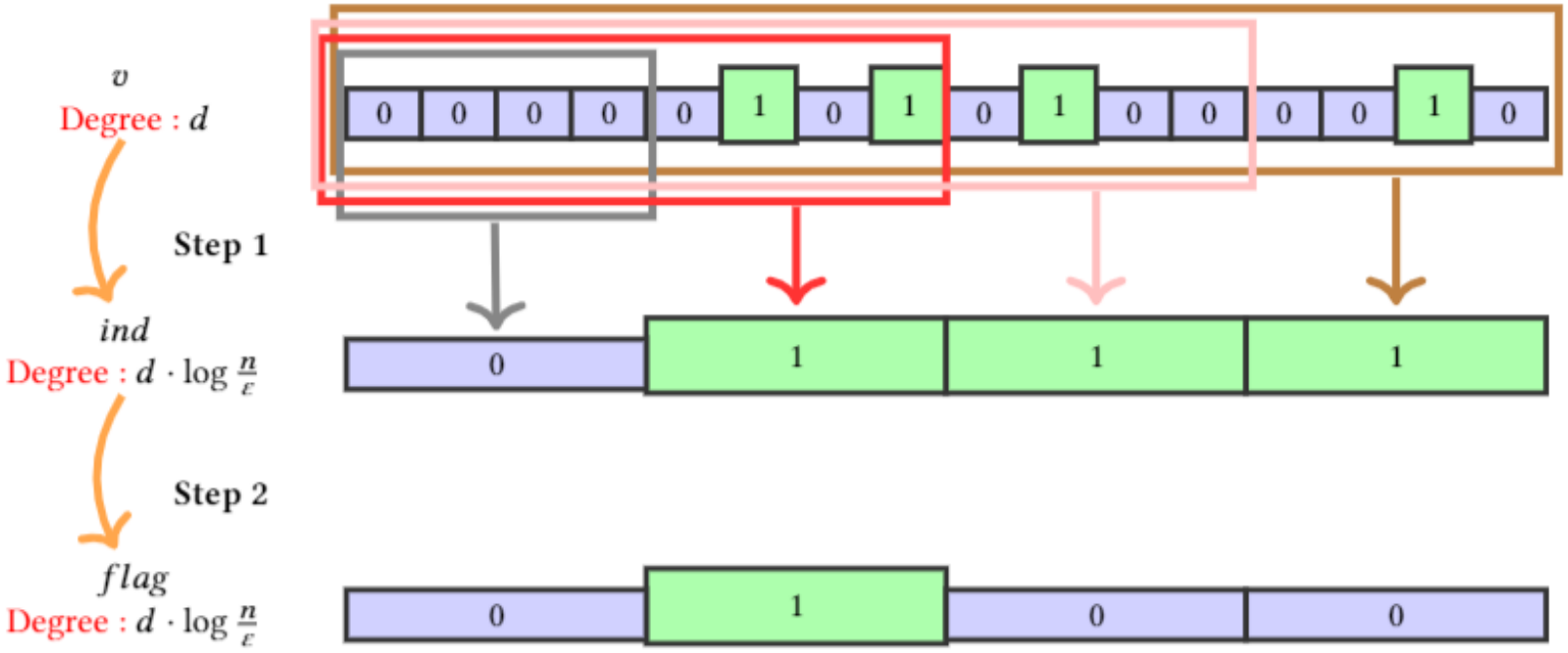
AGHL算法


u
0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 0
v[i] = RS-OR(u[1], u[2], ..., u[i])
v
0 0 0 0 0 1 1 1 1 1 1 1 1 1 1 1
out[i] = v[i] − v[i − 1]
out
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0

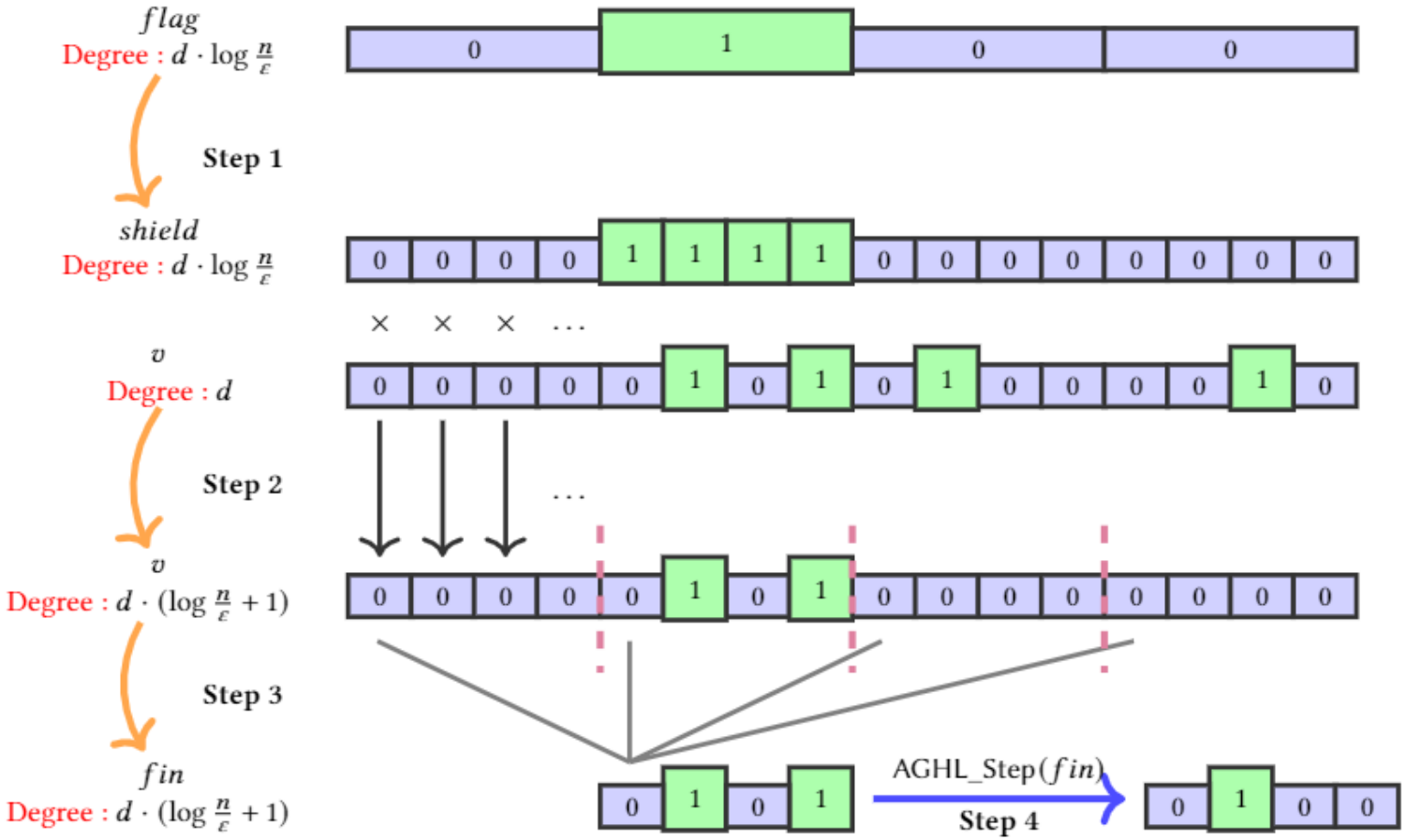
LEAF算法概览

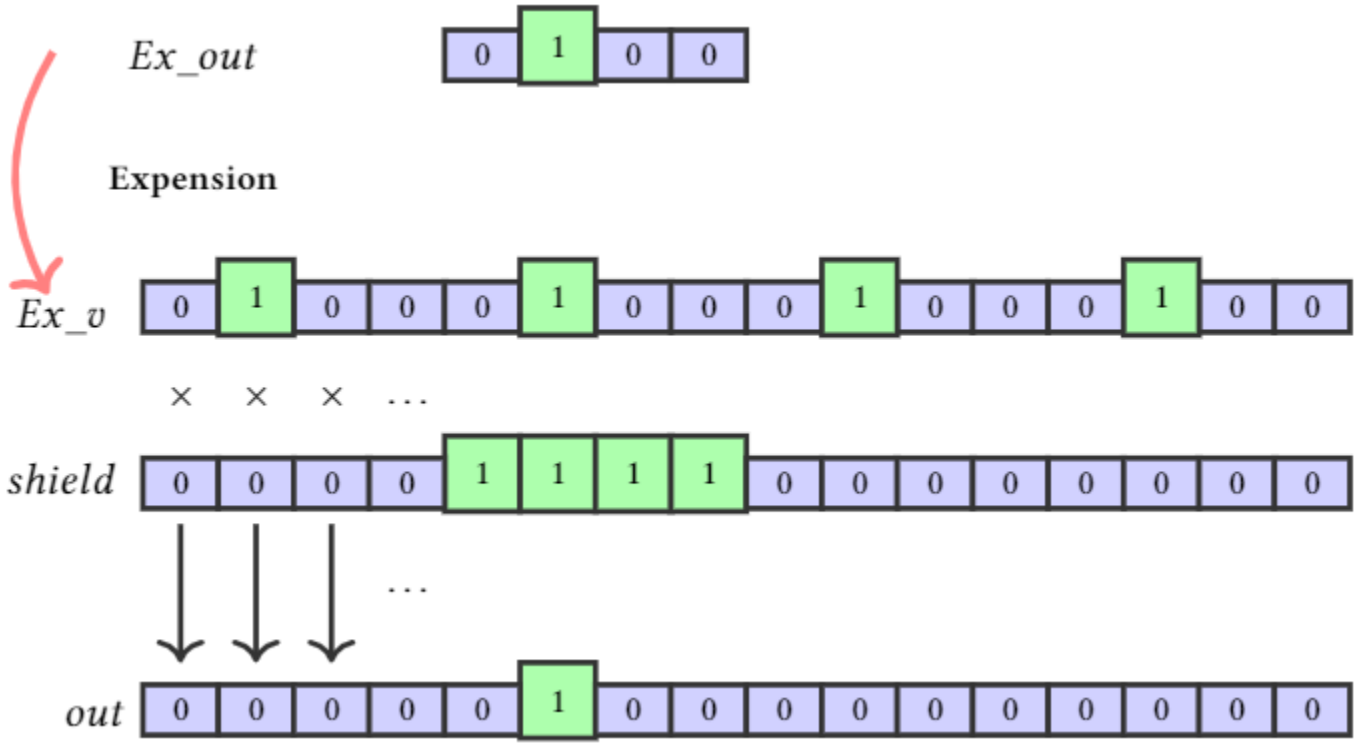

0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 0
Step:Localization
0 1 0 0
Step:Extraction
0 1 0 1
Step:Reconstruct
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0

定位


v
Degree : d
Step 1
ind
Degree : d · log n/ε
Step 2
flag
Degree : d · log n/ε
0 0 0 0 0 1 0 1 0 1 0 0 0 0 1 0
0 1 1 1
0 1 0 0

提取


flag
Degree : $d \cdot \log \frac{n}{\varepsilon}$
Step 1
shield
Degree : $d \cdot \log \frac{n}{\varepsilon}$
v
Degree : d
Step 2
v
Degree : $d \cdot (\log \frac{n}{\varepsilon} + 1)$
Step 3
fin
Degree : $d \cdot (\log \frac{n}{\varepsilon} + 1)$
AGHL_Step(fin)
Step 4


Ex_out
0 1 0 0
Expension
Ex_v
0 1 0 0 0 1 0 0 0 1 0 0 0 1 0 0
× × × ...
shield
0 0 0 0 1 1 1 1 0 0 0 0 0 0 0 0
...
out
0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0

参数选择

$$t \cdot \log(\frac{n}{\varepsilon}) + 2n + k \cdot \log(\frac{n}{\varepsilon})$$

其中：$t \cdot k = n$

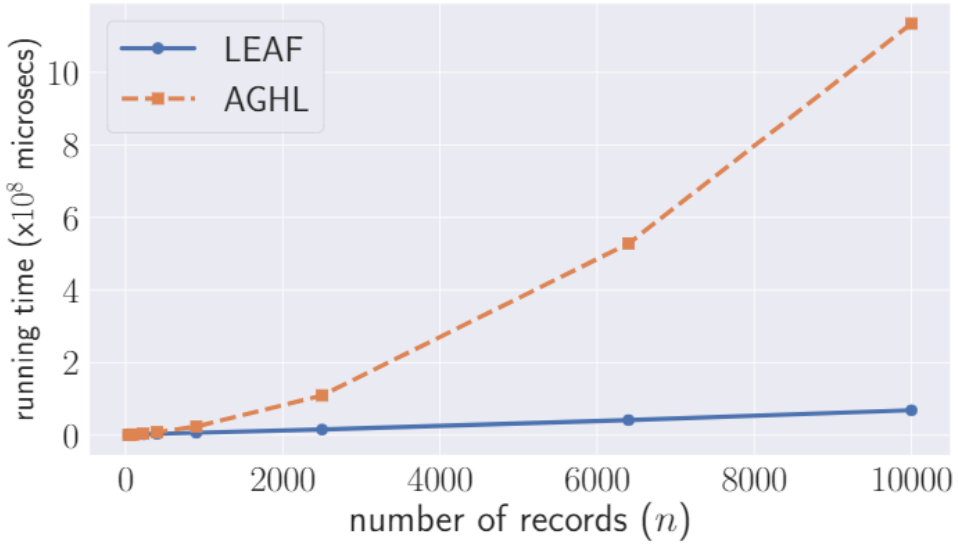
$$\frac{\partial\left(t \cdot \log(\frac{n}{\varepsilon}) + \frac{n}{t} \cdot \log(\frac{n}{\varepsilon})\right)}{\partial t} = 0$$

$$t = \sqrt{n}$$

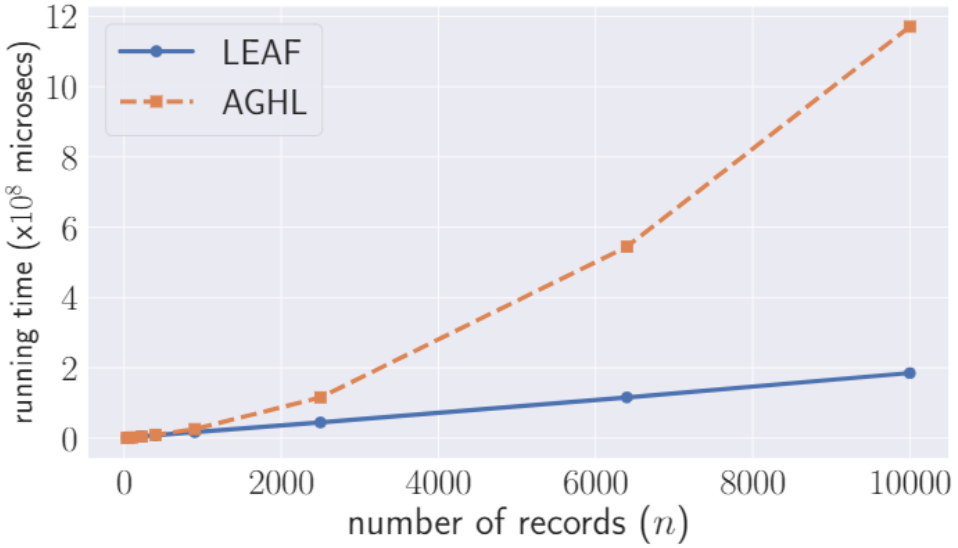
算法复杂度对比

Algorithm Name	Degree of Function	Number of Multiplications	Time Complexity
Folklore	$O(n)$	$O(n^2)$	$O(n^2 \log^{\omega} n)$
SPiRiT Det.	$O(\log^3 n)$	$O(n \log^2 n)$	$O(n \log^2 n (\log\log n)^{\omega})$
AGHL	$O(\log n)$	$O(n \log n)$	$O(n \log n (\log\log n)^{\omega})$
LEAF	$O(\log^2 n)$	$O(n)$	$O(n(\log\log n)^{\omega})$
LEAF^{+}	$O(\log n)$	$O(n)$	$O(n(\log\log n)^{\omega})$
Full LEAF	/	$O(n)$	$O(n)$

实验结果



(a) pure searching



(b) searching and matching


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音