中国科学技术大学

读书报告

布隆过滤器及其衍生的新型数据结构

作者姓名：　柳枫

学科专业：　网络空间安全

导师姓名：　薛开平教授

完成时间：　二〇二四年八月六日

目　录

符 号 说 明

a	The number of angels per unit area
N	The number of angels per needle point
A	The area of the needle point
σ	The total mass of angels per unit area
m	The mass of one angel
$\sum_{i=1}^{n} a_i$	The sum of a_i

第 1 章　简　　介

1.1　布隆过滤器

在构造网络安全协议时，我们通常会使用到许多不同类型的数据结构。其中，布隆过滤器作为一种经典的数据结构，在诸如隐私集合求交、可搜索加密、隐私信息检索等密码学协议中有着广泛的应用。布隆过滤器是一种用于快速判断元素是否存在于某一集合的数据结构，它具有空间效率高、判断速度快的特点。以大小为 n 的集合 S 为例，对应的布隆过滤器构造只需要 $O(n)$ 的存储开销以及 $O(1)$ 的判断复杂度。布隆过滤器的构造如下图所示，它是使用 k 个哈希函数 $\{h_1, \cdots, h_k\}$ 构造的哈希表结构。在构造过程中，对于每个在集合 S 中的元素 x，首先使用这 k 个哈希函数计算出 k 个位置，然后对过滤器中该位置上的比特置为 1。在判断元素是否属于集合 S 时，只需要通过哈希函数计算该元素的 k 个位置，然后检查过滤器上这 k 个位置上的比特是否全为 1，是的话返回 True，否则返回 False。

1.2　分类

这里引用文献[1]

参 考 文 献

[1] 张响鸽, 张聪, 刘巍然, 等. 隐私集合运算中的关键数据结构研究[J/OL]. 密码学报, 2024, 11(2): 263-281. DOI: 10.13868/j.cnki.jcr.000679.