THE AUGMENTED BINARY TREE RECONSTRUCTION PROBLEM: NEW ALGORITHMS AND DIRECTIONS

Problem Statement: Algorithms for Augmented Binary Tree Reconstruction by an Adversary

Setup: Binary tree with 'augmented nodes, 2^d leaves with random unknown identifiers.

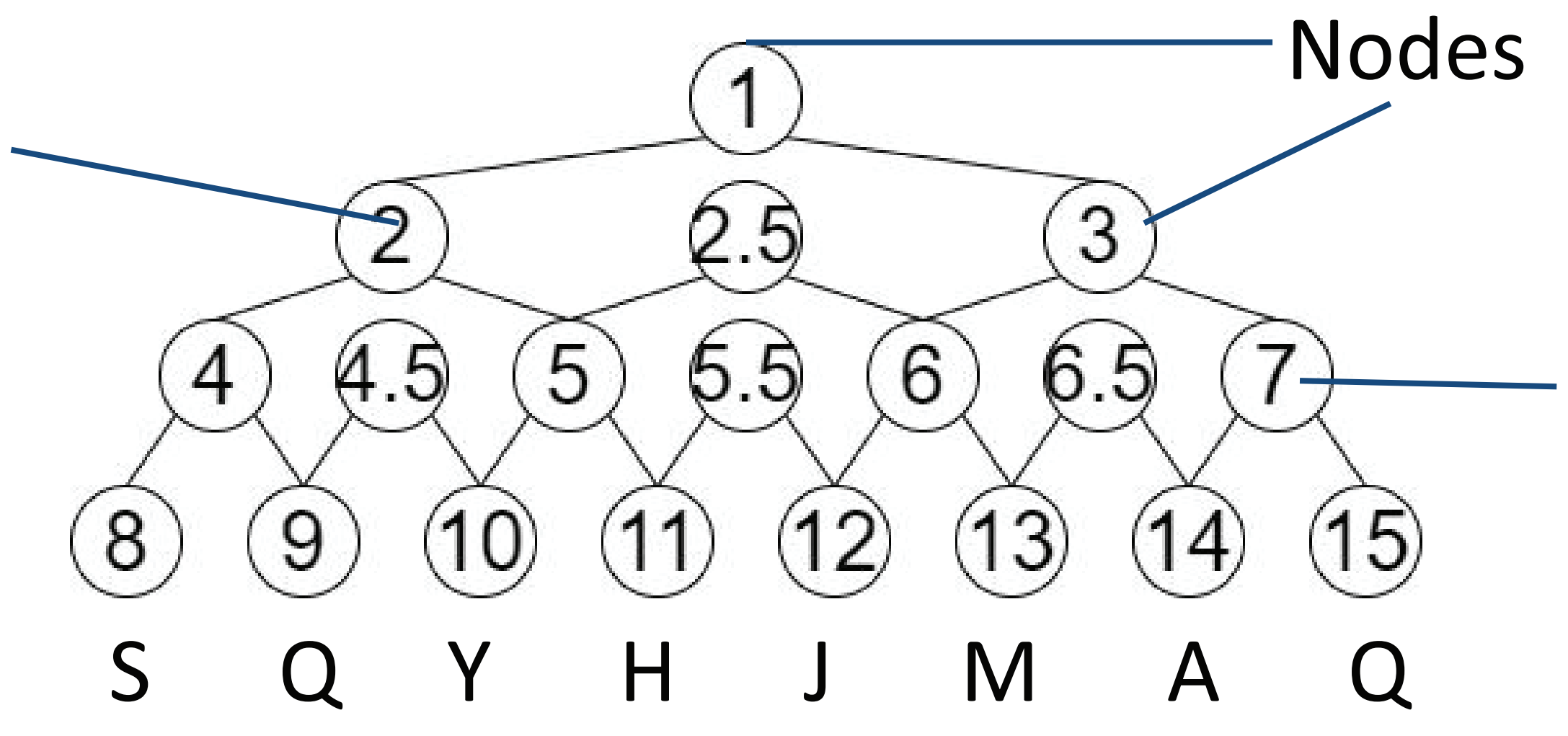
Queries: Adversary observes (x, P_x), x is a node in the tree, P_x is the set of identifiers of leaf descendents of x. (e.g. (4, {S, Q}).

Inferences: Notice that observing multiple queries will reveal additional information to Adversary. (e.g. given (4, {S, Q}), (4.5, {Y, Q}), can tell P_9 ={Q} = P_4 n P_9 without querying).

Our goal: Design a Reconstruction Algorithm that is optimal and efficient.

Input: Series of queries

Output: As many leaf node identifiers as possible.



Child node (descendent) of 1

Nodes

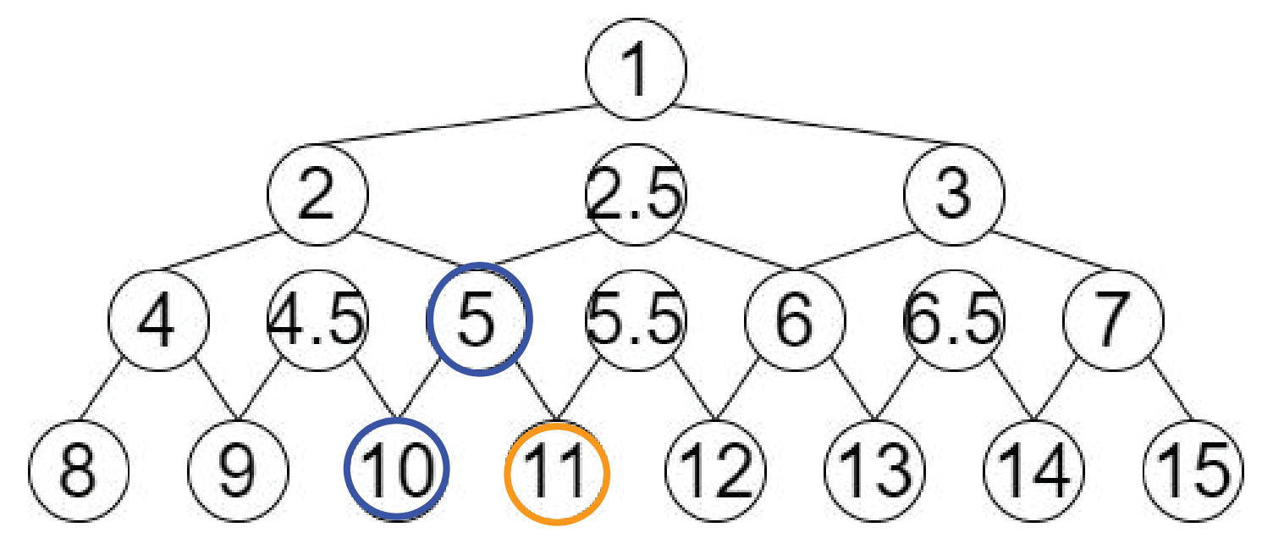
Parent node (ancestor) of 14 and 15

Algorithm 1: Recursive Neighbour Search (RNS)

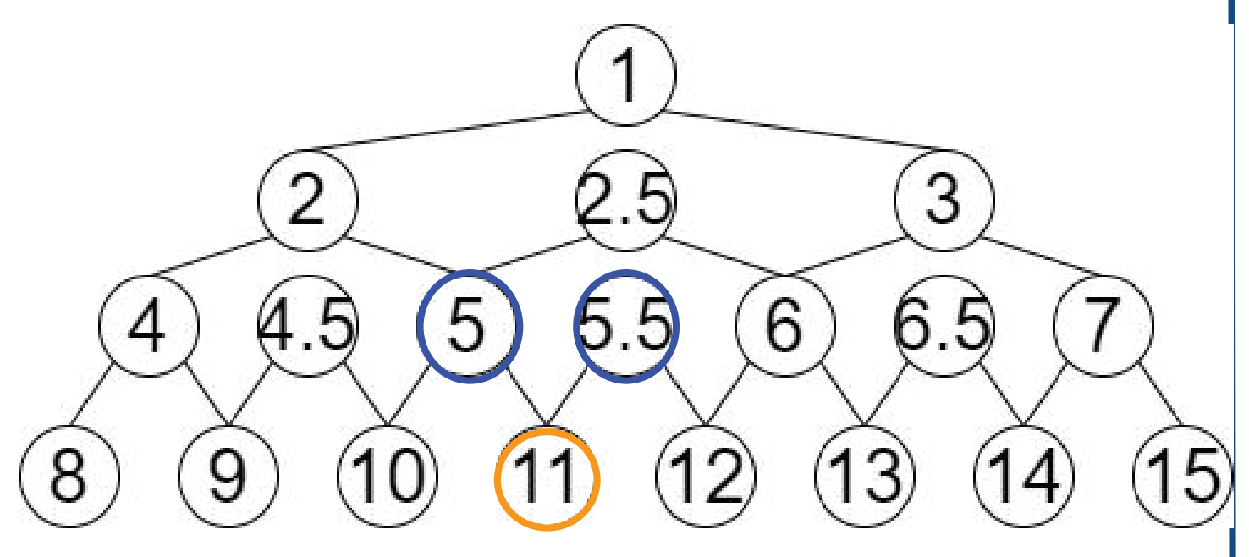
- Uses relationships between neighbouring nodes to compute others
- Repeatedly scans tree and implements these equations, until no more changes

🟦 Given node

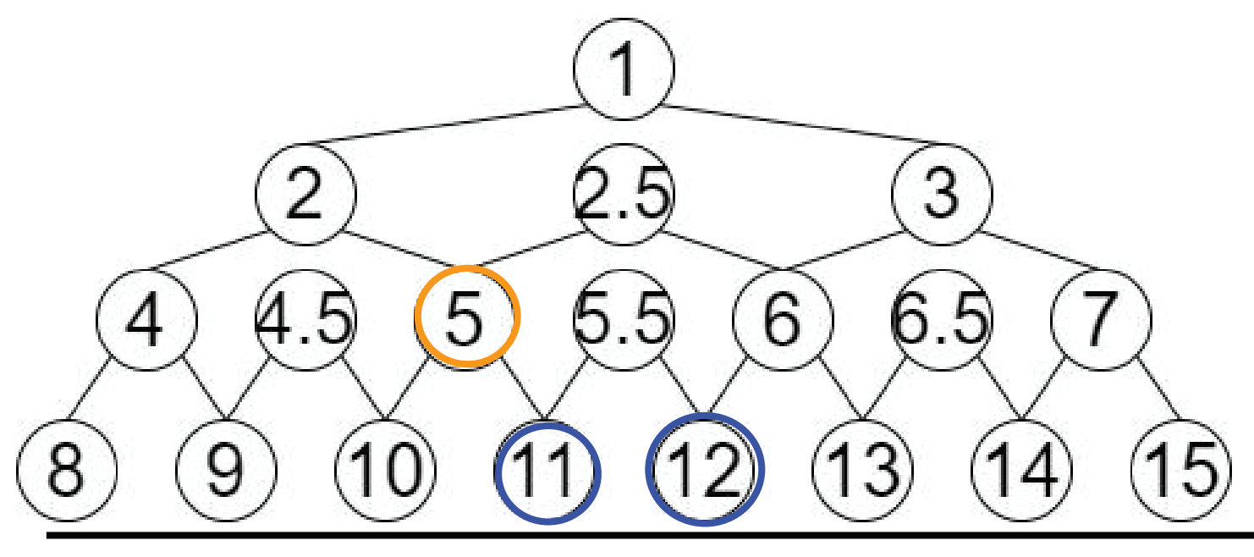
🟧 Computed node



$$P_{2x} = P_x \setminus P_{2x+1}$$

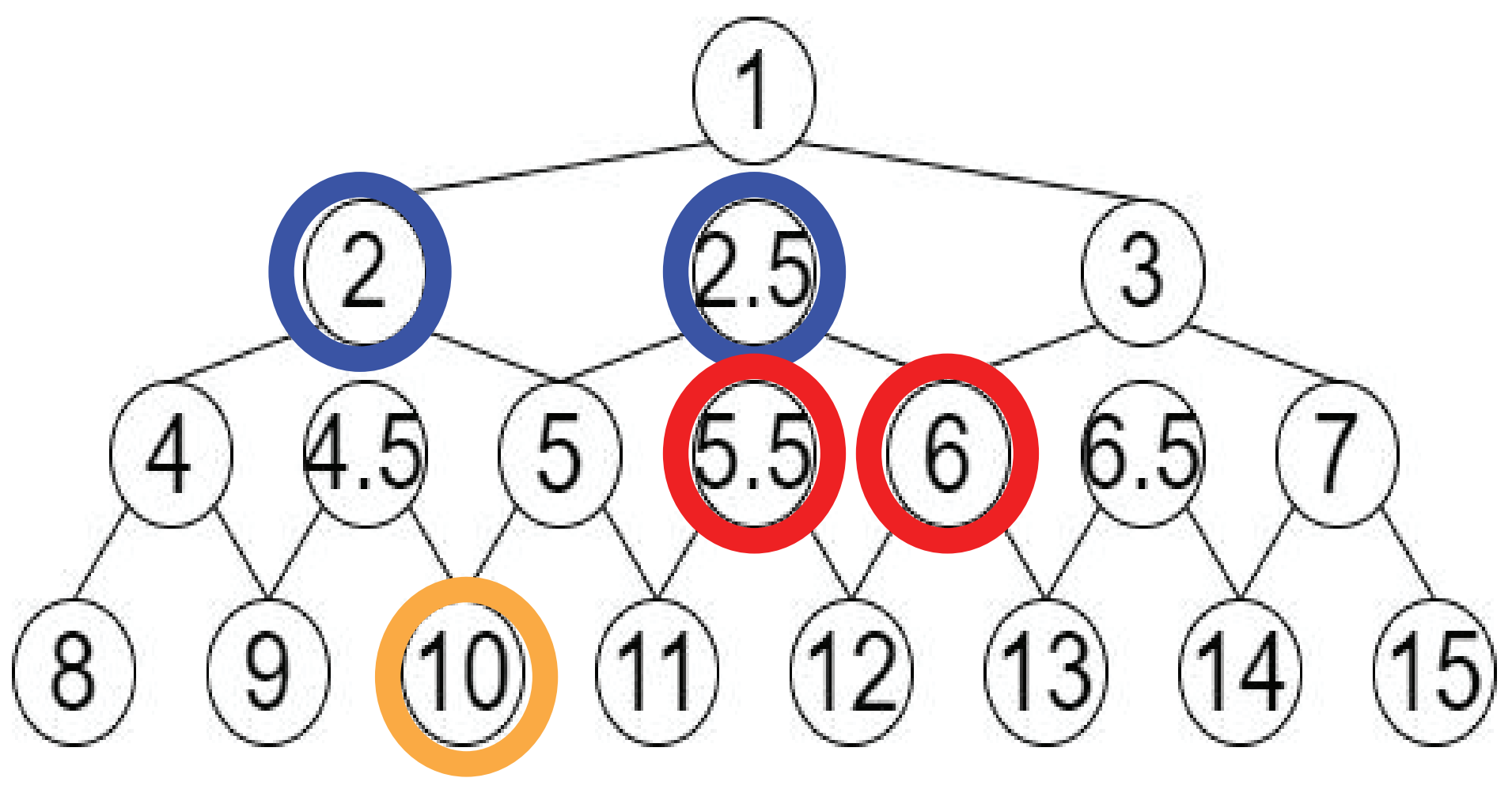


$$P_{2x+1} = P_x \cap P_{x+0.5}$$



$$P_x = P_{2x} \cup P_{2x+1}$$

Algorithm 2: One-pass Union-Intersection Search



🟦 Given node (ancestor)

🟧 Computed node

🟥 Given node (non-ancestor)

Involves finding intersection of all ancestors of target node and subtracting union of all non-ancestors of target node.

E.g.

$$P_{10} = P_2 \bigcap P_{2.5} \setminus P_{5.5} \bigcup P_6$$

General formula:

$$P_x = \bigcap_{n\in I} P_n \setminus \bigcup_{n\in U} P_n$$

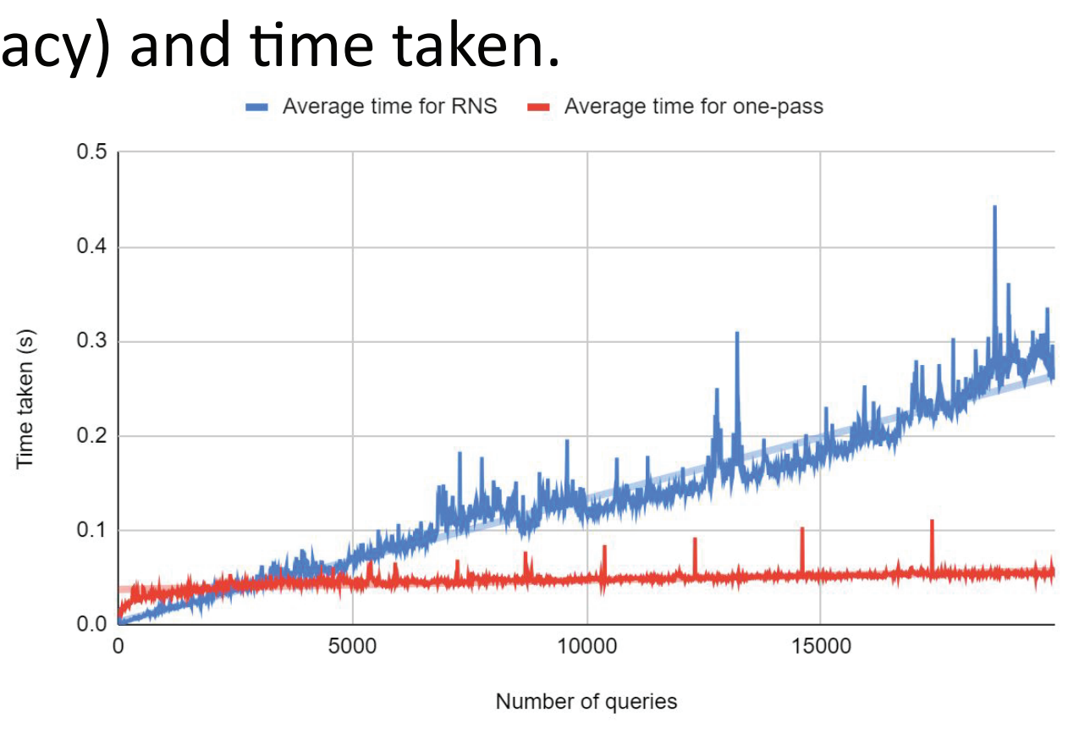
Results

🟦 RNS 🟥 One-pass

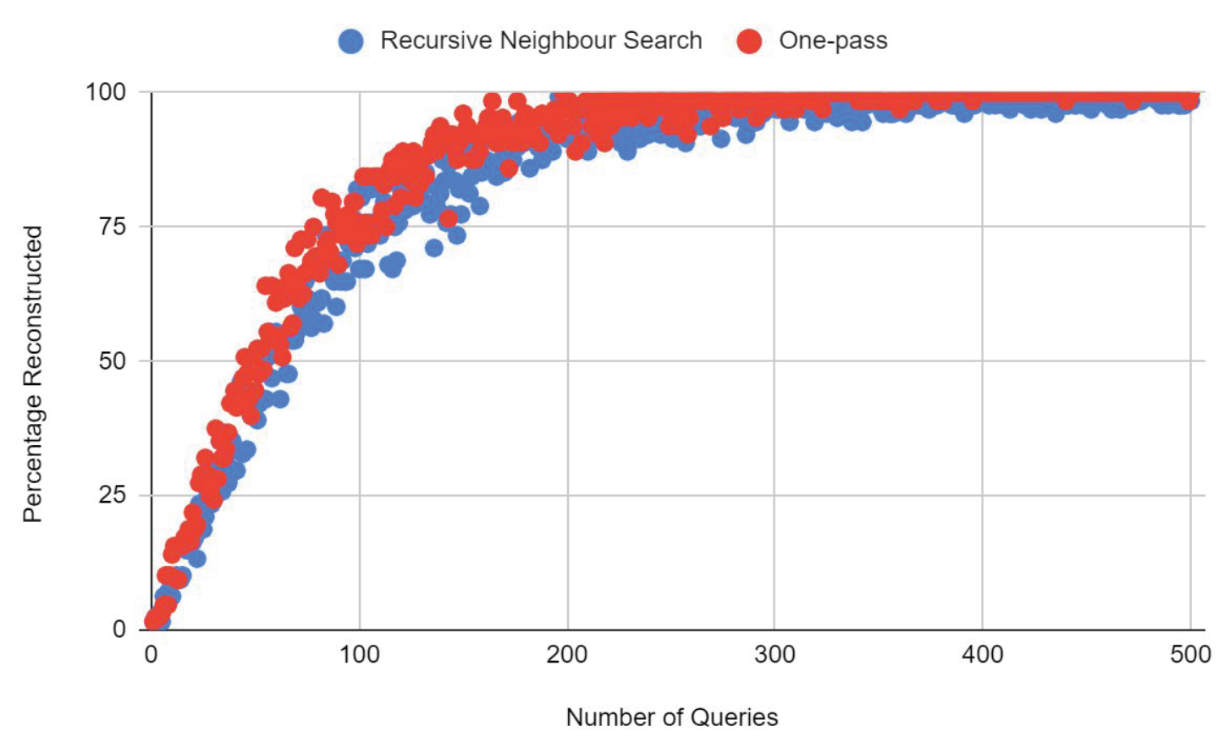
We did experiments by implementing them in Python and observed two metrics: percentage reconstructed (accuracy) and time taken.

One-pass has near constant time taken, though slower at lower query number.

RNS faster at low query number but time taken increases more significantly.



Accuracy of One-pass higher than RNS on each number of queries on average.



Conclusion: One-pass is an optimal and more efficient algorithm as it is faster at higher query number and more accurate.

Cryptography Application

- Augmented binary trees used in Range Searchable Encryption
- Adversary can use our algorithms to reconstruct sensitive information in a server.
- Can observe queries and use nodes received to reconstruct data from the tree
- A form of Leakage Abuse Attack.

Impact of work

- Can be used to gauge security of RSE schemes that use augmented binary trees.
- Future work could find ways to mitigate possible weaknesses

Members:
Julian Tay Yu Sheng, Dunman High School
Tey Yik Jin Ryden, Anglo-Chinese School (Independent)
Mentor:
Dr Ruth Ng Ii-Yung, DSO National Laboratories

YDSP
Young Defence Scientists Programme
DSTA
Defence Science & Technology Agency
DSO
NATIONAL LABORATORIES