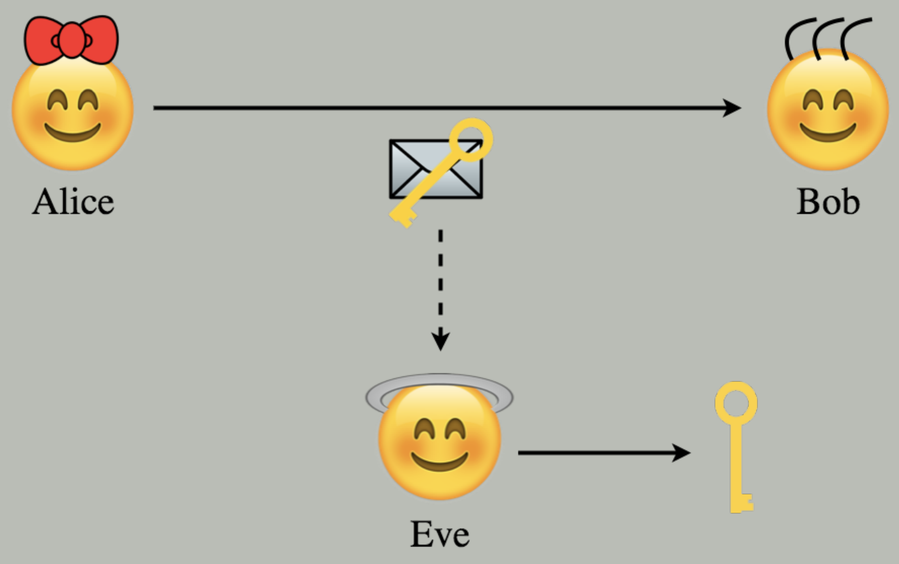
Radboud Universiteit

Time-Memory Analysis of Parallel Collision Search Algorithms

Monika Trimoska

Cryptanalysis

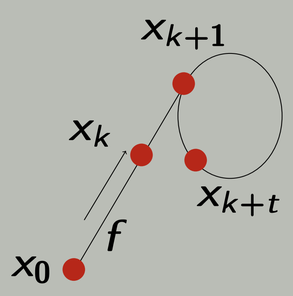


Goal
Determine minimum key length requirements.

Collision search

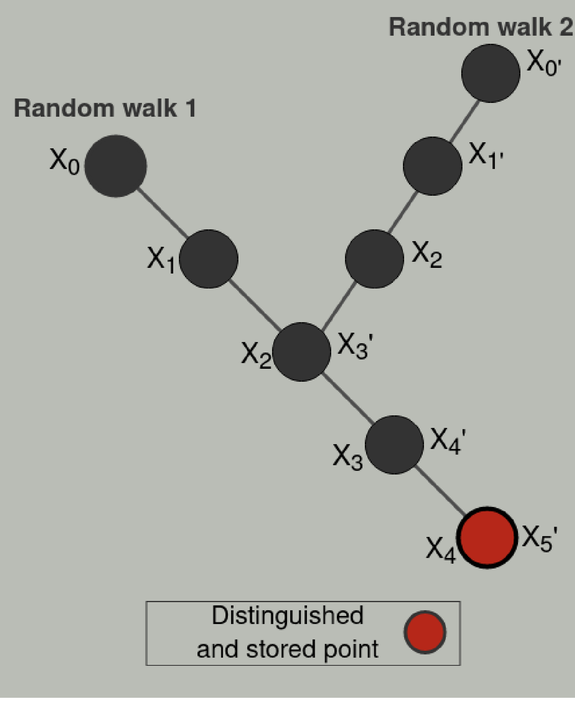
Collision
Given a random map $f : S \to S$ on a finite set S of cardinality N, we call collision any pair R, R' of elements in S such that $f(R) = f(R')$.

Pollard's Rho method



- Ideally, f is a random mapping.
- Expected number of steps until the collision is found: $\sqrt{\frac{\pi N}{2}}$.

Parallel Collision Search



- Proposed by van Oorschot & Wiener (1996).
- Distinguished points : a set of points having an easily testable property.
  ex. The x-coordinate has 3 trailling zero bits: 10101101000.
- Only distinguished points are stored in memory.

Data structure

Requirements
- ➔ Space efficient
- ➔ Thread-safe
- ➔ Fast look-up and insertion

Commonly used structure:
Hash table.

Alternative:
Packed Radix-Tree-List (PRTL).

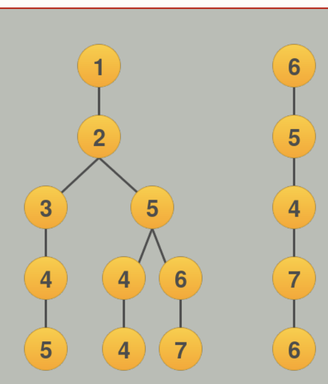


Figure: Exemple of a radix tree holding the set 12345, 12544, 12567, 65476.

Packed Radix-Tree-List

- ➔ Construct a radix tree up to certain level.
- ➔ Add the points to linked lists, each list starting from a leaf on the tree.

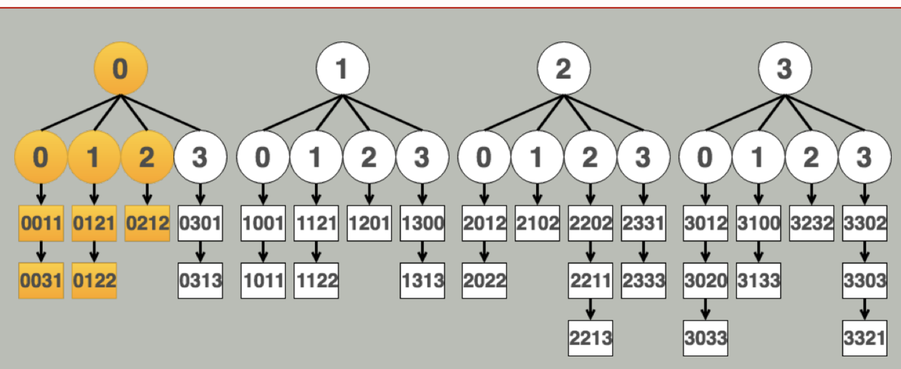
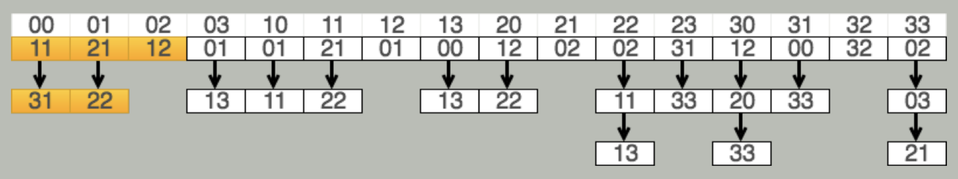


Figure: Exemple of a PRTL holding the set 0011, 0031, 0121, 0122, 0212, etc.

PRTL implementation



- ➔ Saving space on common prefixes.
- ➔ The stored data is packed in a single vector.
- ➔ We can estimate the optimal branching level.

Collision search applications

One collision application
- (Elliptic Curve) Discrete Logarithm Problem.

Multi-collision applications
- Attack on the 3-DES with three independent keys.
- (EC)DLP in the multi-user setting.
- Computational Supersingular Isogeny Problem.

Joint work with Gilles Dequen and Sorina Ionica