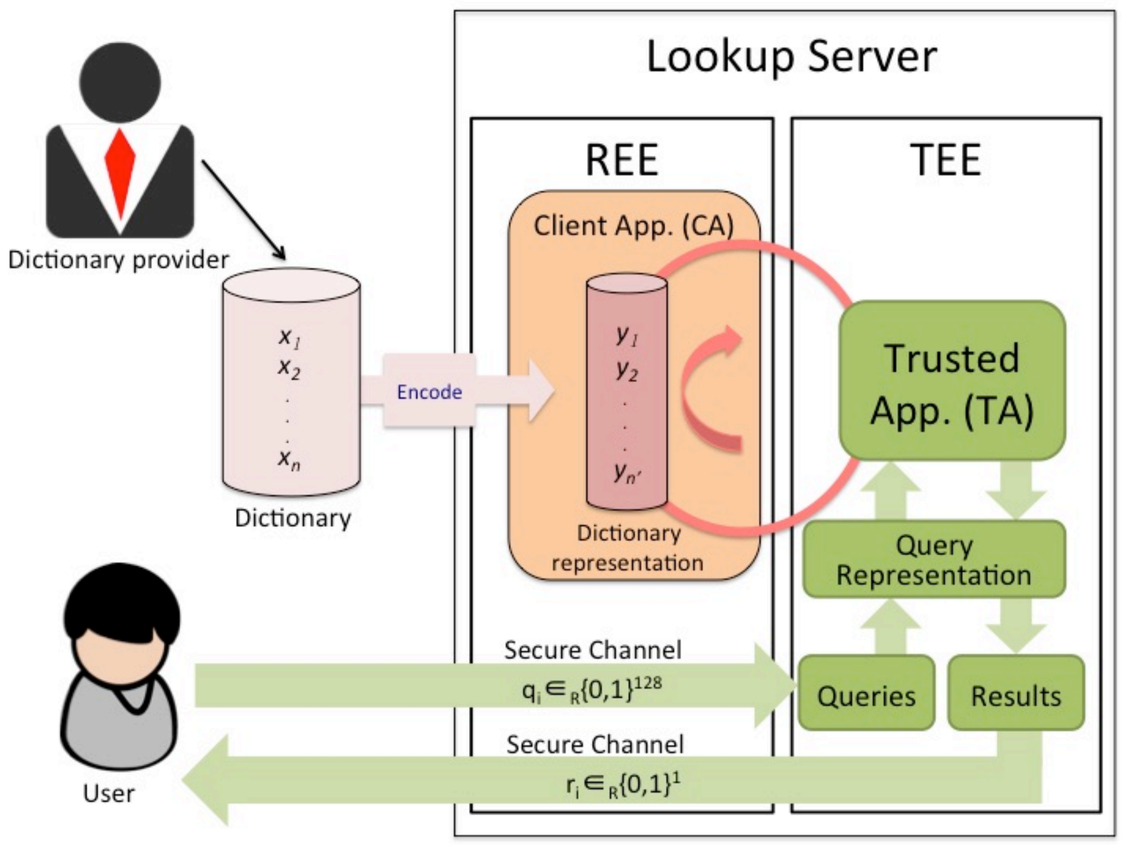
Cloud Security
Secure Systems Group

Sandeep Tamrakar, Jian Liu, Andrew Paverd, Jan-Erik Ekberg(+), N. Asokan, Benny Pinkas(*)

Scalable Private Membership Test Using Trusted Hardware

Intel SGX and ARM TrustZone

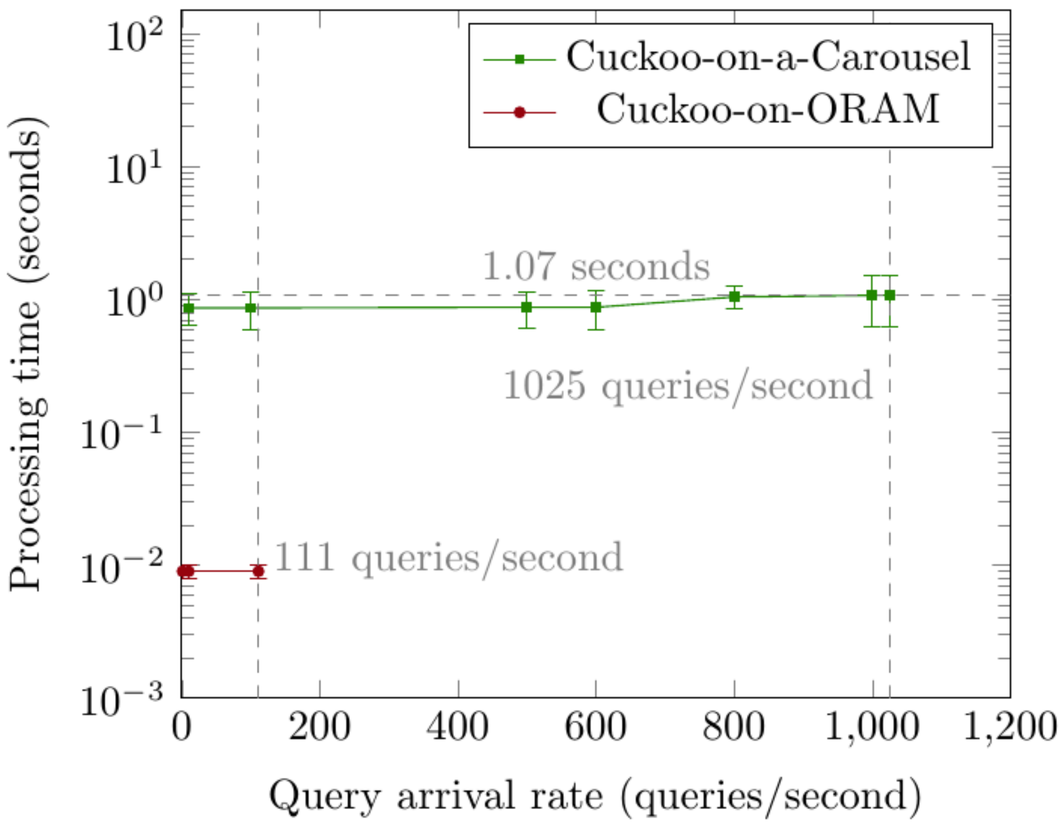
- **Motivation:** Existing cloud-based malware checking services raise privacy concerns (e.g. infer personal traits of users based on queried apps).
- **Goal:** Effective and efficient private membership test scheme that is implemented on trusted hardware, provides query privacy with acceptable latency, and supports simultaneous queries



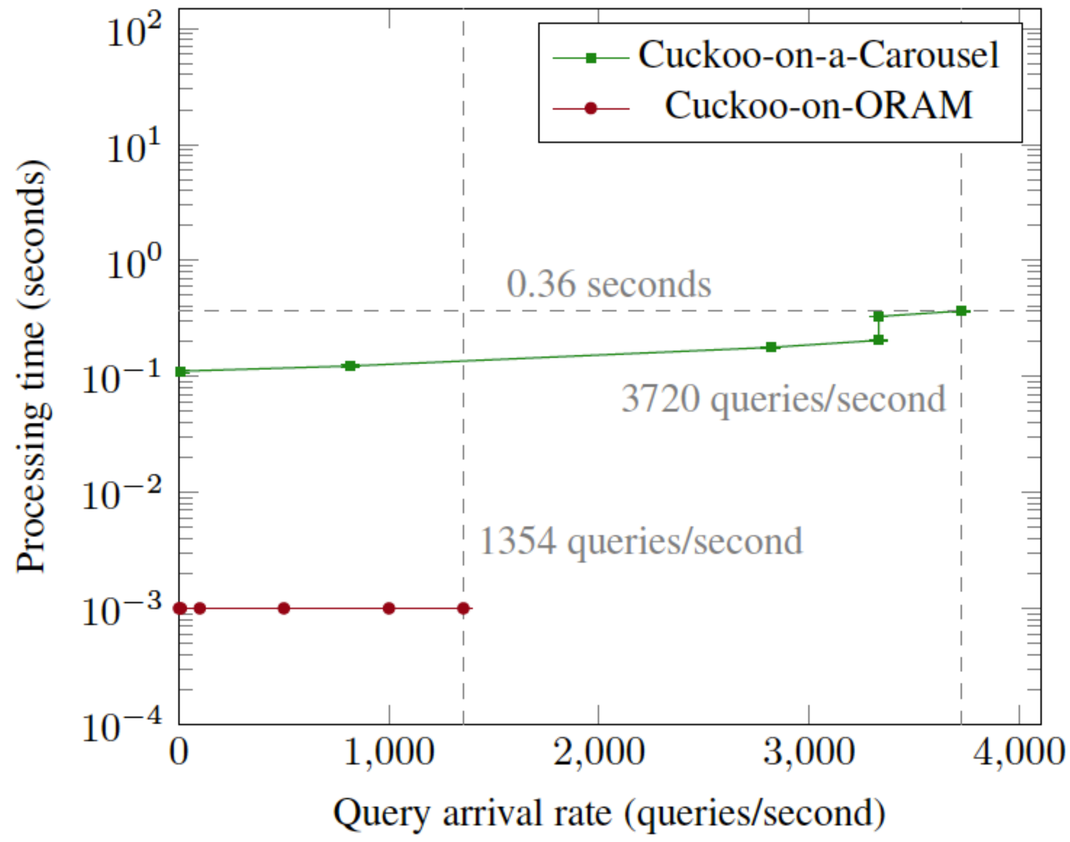
The Carousel approach

- Carousel: continuously circle malware dictionary through trusted hardware to ensure query privacy
- Different data structures for efficient yet privacy-preserving computation of responses: Sequence of differences, Bloom filter and Cuckoo hash
- Systematic and extensive experimental evaluation on ARM TrustZone (Kinibi from Trustonic) and Intel SGX
- Supports ~67 million items with 2^{-10} false positive rate
- Sustainable query rate – 1025 queries/sec on ARM TrustZone and 3720 queries/sec on Intel SGX

ARM TrustZone



Intel SGX



Steady-state processing time for uniform query arrival rates (average and variance over 1000 runs).

(+) Trustonic
(*) Bar Ilan University

Aalto University
CloSe
TRUSTONIC
Academy of Finland
Bar-Ilan University
אוניברסיטת בר-אילן