CERIAS

The Center for Education and Research in Information Assurance and Security

HashRand: Asynchronous Random Beacon From Lightweight Cryptography

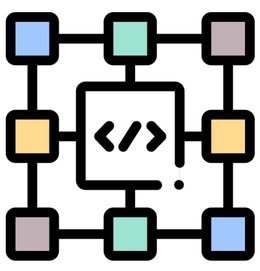
Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter

Appeared at ACM CCS 2024. Eprint 2023/1755

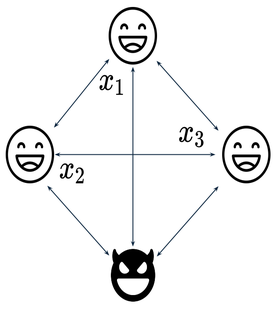
1. Introduction

Random Beacons provide secure randomness for numerous applications

Online Lotteries

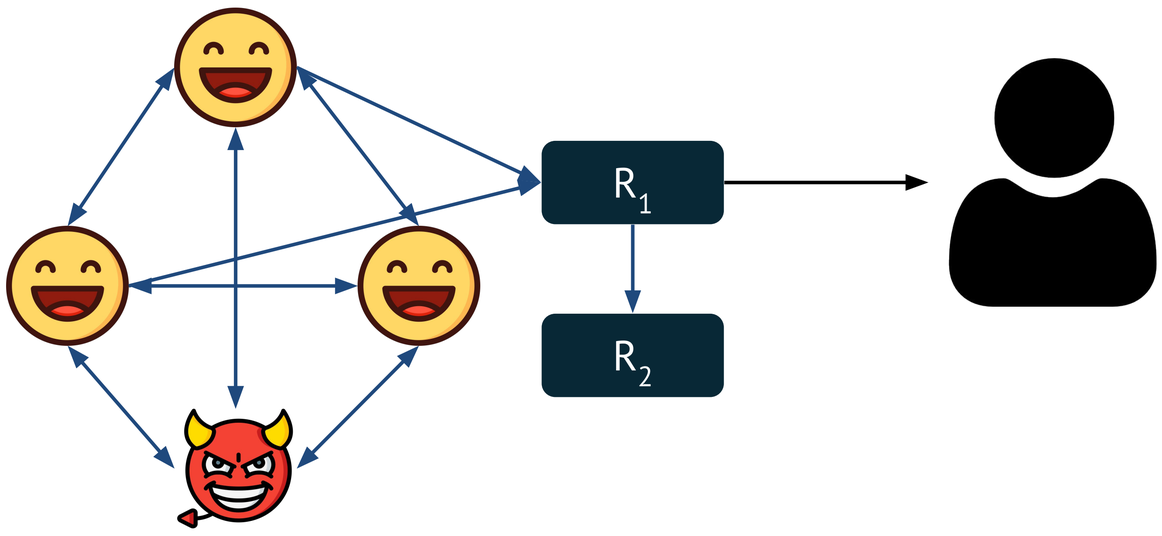


Web3 Apps



Multi-Party Computation

- Sources like Random.org and NIST Beacon have a **single point of failure**
- Distributed Random Beacons



- **Agreement and Liveness:** Honest parties must output the same value, parties must keep outputting values

- **Unpredictability:** Adversary must not be able to predict values without honest parties participating

2. Scalability problem of prior beacons

Existing Solutions like Spurt [S&P'22] are **computationally expensive**

- Use expensive discrete-log cryptography

- At **n=100**, computation itself takes **t>5** seconds per beacon!

3. Lightweight Cryptography

Cryptographic primitives like Hash functions and Symmetric Key Encryption

Computationally Efficient: 1000x cheaper than Public Key Cryptography!

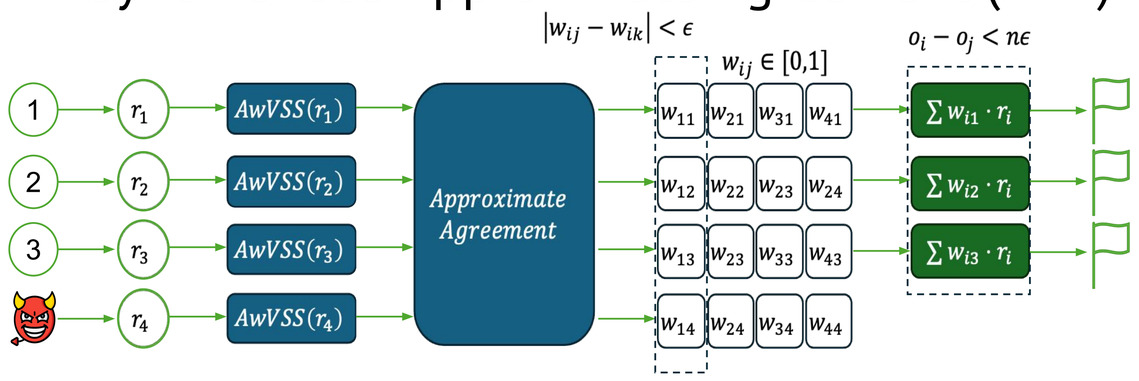
Cherry On Top: Post-Quantum Secure!

Operation	Computation Time
DLog Exponentiation	70 microseconds
Bilinear Pairing	600 microseconds
SHA-2 Hash Computation	0.5 microseconds
Hardware Accelerated MAC	0.04 micro seconds

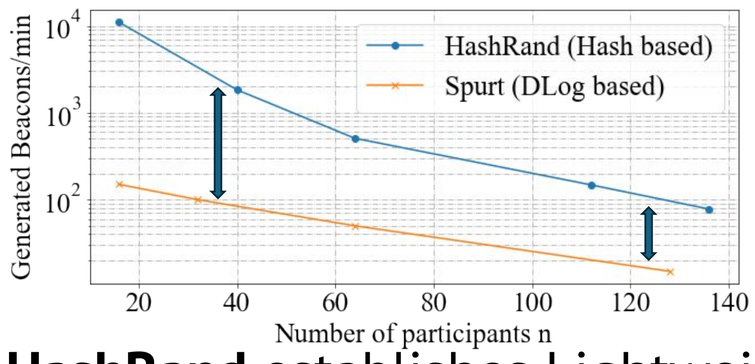
4. HashRand: Hash-based Beacon

Utilize Computationally Efficient primitives that use only Hash computations

- Asynchronous weak Verifiable Secret Sharing (AwVSS)
- Asynchronous Approximate Agreement (AAA)



5. Results



HashRand's throughput is **20x** and **5x** greater than Spurt at **n=40,136** respectively

HashRand establishes Lightweight Cryptography as a viable path for scalability and Post-Quantum Security

PURDUE UNIVERSITY

CERIAS