Rondo: Scalable and Reconfiguration-Friendly Randomness Beacon

Xuanji Meng, Xiao Sui, Zhaoxin Yang, Kang Rong, Wenbo Xu, Shenglong Chen, Ying Yan, Sisi Duan

Tsinghua University, Ant Group

NDSS 2025, February 10, 2025

What is a Distributed Randomness Beacon (DRB)?

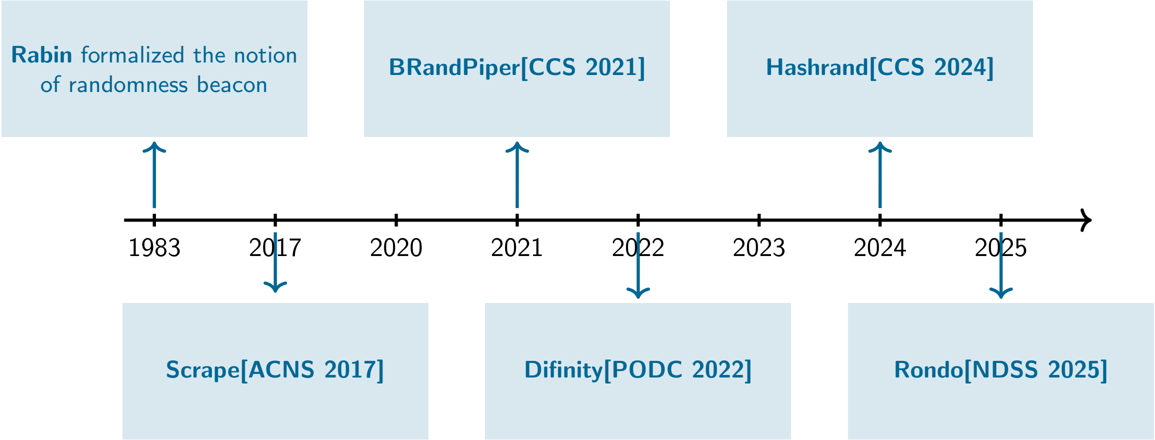
DRBs provide unpredictable, publicly verifiable randomness.

- Essential for decentralized applications and cryptographic protocols.
- Enables fairness and security in trustless environments.

Key Applications:

- **Blockchain Smart Contracts:** Secure lotteries, validator selection (Ethereum, Chainlink VRF).
- **Consensus Mechanisms:** Leader election in PoS blockchains.
- **Online Voting Systems:** Preventing bias and manipulation.
- **Zero-Knowledge Proofs:** Generating public randomness for privacy-preserving protocols.

Existing DRB Protocols



DRB: Prior Works

Protocols	Reconfigurable	Communication	Timing
Scrape (2017)	No	$O(n^4)$	sync.
BRandPiper (2021)	Yes	$O(n^3)$	sync.
Dfinity(2022)	No	$O(n^3)$	partial.
Hashrand (2024)	No	$O(n^2 \log n)$	async.
Rondo (2025)	Yes	$O(n^2 \log n)$	partial.

Table: Comparison of DRB Protocols

Research Question

Can we build a distributed randomness beacon protocol that is both **scalable** and **reconfiguration-friendly** in the **partially synchronous** network?

Challenges in Existing DRB Protocols

Major Issues with Current Approaches:

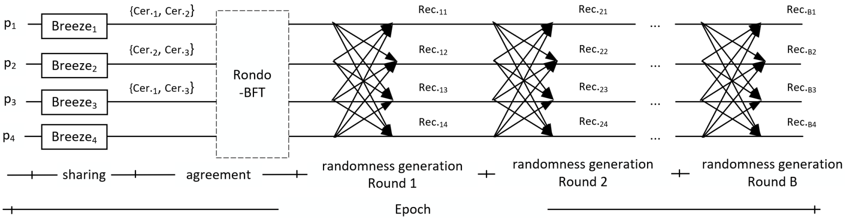
- **High Message Complexity:** Many DRBs require $O(n^3)$ communication, leading to scalability issues.
- **Static Membership:** Existing solutions often lack dynamic reconfiguration, making them impractical for real-world deployments.
- **Latency and Throughput Limitations:** Many protocols suffer from increased latency as network size grows.
- **Computational Overhead:** Inefficient cryptographic primitives increase computational costs.
- **Existing Solutions:** Approaches like threshold BLS signatures (e.g., Drand, Dfinity) improve security but suffer from high aggregation overhead. Others, such as Chainlink VRF, rely on external trusted oracles.

Key Contributions of Rondo

- **AVSS-PO:** Asynchronous Verifiable Secret Sharing with Partial Output for efficiency.
- **Rondo-BFT:** Byzantine Fault-Tolerant consensus with dynamic reconfiguration.
- **Optimized Polynomial Commitments:** Breeze enables scalable batch verification.
- **Superior Performance:** Achieves high throughput with reduced latency.

Rondo Protocol Workflow

- **Commitment Phase:** Nodes generate and share secrets using AVSS-PO.
- **Validation Phase:** Partial output verification ensures correctness.
- **Agreement Phase:** Rondo-BFT finalizes the randomness beacon.
- **Reconstruction Phase:** The final randomness output is determined.

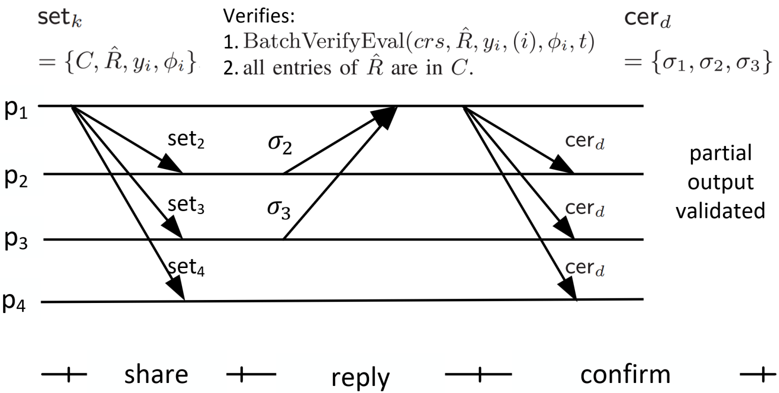


Rondo-BFT: Efficient and Reconfigurable Consensus

- **Built on HotStuff:** Extends HotStuff to support randomness beacon generation.
- **Dynamic Reconfiguration:** Allows nodes to join and leave without compromising security.
- **Low Latency:** Reduces consensus overhead while ensuring finality in a few rounds.
- **Byzantine Fault Tolerance:** Ensures correctness even when a fraction of nodes are malicious.

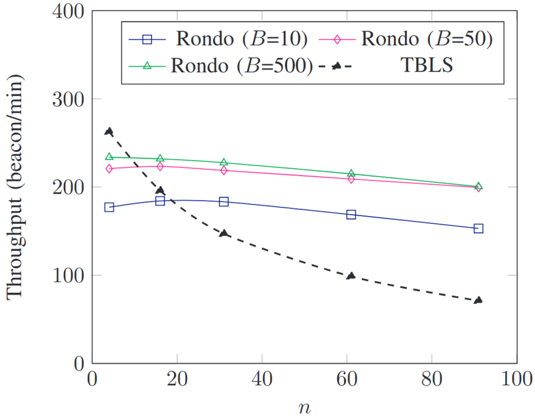
Breeze: Instantiation of AVSS-PO

- Uses batch polynomial evaluation for efficiency.
- Reduces proof size and improves verification speed.
- Lowers computational overhead while maintaining security.

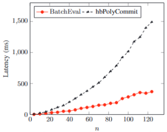


Performance Evaluation

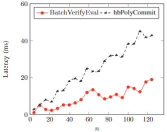
- Tested on 91 Amazon EC2 instances.
- **Metrics:** Throughput, latency, and scalability.
- **Results:** Rondo achieves stable performance as *n* grows.



Additional Performance Results



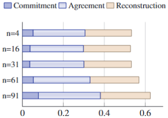
(a) Proof generation time of our scheme and that for hbACSS.



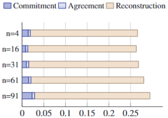
(b) Verification time and that for hbACSS.

n	latency (ms)		
	def.	opt.	imp.
4	16	14	2
16	140	137	3
32	449	438	11
64	1679	1633	46
128	6161	5921	240

(c) Latency of reconstructing B secrets where $B = 2n$.

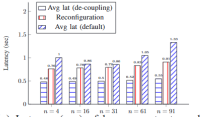


(d) Amortized latency (sec) breakdown of Rondo, B=10.

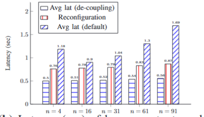


(e) Amortized latency (sec) breakdown of Rondo, B=50.

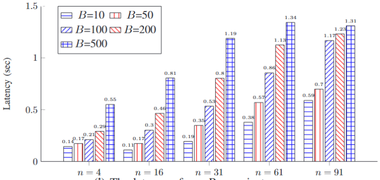
(f) Amortized latency (sec) breakdown of Rondo, B=500.



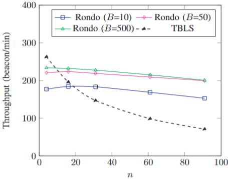
(g) Latency (sec) of beacon outputs and reconfiguration, B=10.



(h) Latency (sec) of beacon outputs and reconfiguration, B=50.



(i) The latency of one Breeze instance.



(j) The throughput of Rondo and TBLS based scheme.

Conclusion and Contact

Dance with Rondo,
Enjoy the randomness!
A scalable beacon that evolves,
Reconfiguration-friendly.

Contact: Xuanji Meng
Email: `mxj21@mails.tsinghua.edu.cn`

Paper Link