Ethereum Foundation, Cryptography Research Team:

Gottfried Herold, George Kadianakis, Dmitry Khovratovich, Mary Maller, Mark Simkin, Antonio Sanso, Arantxa Zapico, Zhenfei Zhang

Analysis of MinRoot report:

[https://crypto.ethereum.org/events/minrootanalysis2023.pdf

](https://crypto.ethereum.org/events/minrootanalysis2023.pdf)

Ethereum has an efficient and straightforward randomness beacon known as RANDAO. It is acknowledged that this beacon's randomness can be biased to a small degree. To the best of our knowledge, this bias is not currently being exploited in Ethereum's consensus protocol (source: https://eth2book.info/capella/part2/building_blocks/randomness/). At the Ethereum Foundation, we have been trying, and to some extent, facing challenges in building a functional VDF since the establishment of the cryptography research team in 2019. The goal has always been to discover a better solution than RANDAO for generating shared randomness.

Our initial attempt to build VDFs involved an RSA-based approach, which necessitated a trusted setup. However, during an audit conducted by ZenGo, the planned secure multiparty computation for the setup was subjected to an attack. As a result, we transitioned to the MinRoot VDF. In the context of VDFs, it's essential to ensure that no attacker can compute the function significantly faster than honest users. Consequently, honest users must employ high-end ASICs to establish a fast baseline. While attempting to make the RSA solution functional, we recognized the critical importance of hardware. Therefore, MinRoot was designed with simplicity in hardware as a primary consideration. It is worth noting that MinRoot had not undergone the same level of scrutiny as older assumptions, such as the RSA-based timelock assumptions.

MinRoot was initially designed as a VDF with the security goal that no attacker should be able to compute the function more than a factor of c=2 faster than the reference implementation, even when employing massive parallelism. The attack mentioned in the report represents the culmination of a three-day effort undertaken by world-leading cryptanalysts and cryptographers. The assumption that the round functions of MinRoot (2021), as well as those of Sloth++ (Boneh et al., 2018), and VeeDo (StarkWare, 2020), cannot be parallelized has been refuted. Specifically, the exponentiation part of the round function can be parallelized, thanks to the structure of a prime field, making it vulnerable to an index-calculus attack—the same one used for computing discrete logarithms over integers. The attack demonstrates that the computation of the root in a 256-bit field can be achieved using 2^25 processors and 2^40 memory faster than using a single processor. The degree of acceleration depends on the chosen latency-communication model. While this specific attack could theoretically be countered by increasing the size of the prime field, it nonetheless highlights our lack of understanding of what attacks to look for when designing VDFs.

From a practical perspective, it has become apparent that we have few tried and tested design patterns for building concretely efficient VDFs and similarly we also do not have many attack blueprints that we can use to assess the security of new candidate constructions reliably. This situation is different from practical hash functions and symmetric encryption schemes. There we have many decades of research efforts that resulted in SHA-3 and AES, we have design patterns and we have various attack tools that help us evaluate new candidates efficiently. These tools are not helpful for evaluating the security of VDFs because the properties of delay and collision-resistant hash functions are unrelated.

Indeed, MinRoot was considered secure based on the assumption that classical attacks developed for hash functions and encryption schemes were appropriate to evaluate the security of VDFs as well. The VDF workshop showed that VDFs are prone to very different kinds of attacks that have yet to be explored thoroughly.

A relevant part of the attack surface, including the attack found at the workshop, comes from the possibility of slightly speeding up even basic computations by massive parallelism. As this is a wasteful use of parallel resources, such usage is underexplored, and we lack the necessary experience to assess its impact on candidate VDFs.

The cryptography research team agrees that a better understanding of VDFs is essential if we are to continue down this design avenue. At present we do not recommend using VDFs within Ethereum. Ongoing research and substantial improvements are important factors in potentially revising our perspective on this topic in the future.