A Cryptographic Note on the Rainstorm Hash Function

(Cris)

December 15, 2024

Introduction

This note provides a high-level cryptographic commentary on the Rainstorm hash function, which features a 1024-bit internal state and processes data in 512-bit blocks. While Rainstorm borrows some conceptual elements from established hashing paradigms, it does not directly follow a well-analyzed structure like the sponge construction used in SHA-3 finalists, nor does it rely on standard, rigorously studied primitives. Instead, it employs carefully chosen primes and rotation constants to achieve desired avalanche properties.

As Rainstorm has not yet undergone extensive public cryptanalysis, the observations here serve as preliminary considerations for cryptographers interested in evaluating its security.

Conceptual Similarities to Established Hashes

Rainstorm shares certain thematic elements with known cryptographic hash functions:

- **Large Internal State and Block-Based Absorption:** The use of a 1024-bit internal state and a 512-bit block size recalls the design philosophy of sponge-based constructions (e.g., Keccak/SHA-3), which operate by absorbing input into a large state and applying a fixed permutation. While Rainstorm's transform differs in detail, the general pattern of input absorption followed by repeated mixing rounds bears conceptual resemblance to such designs.
- **Simple Arithmetic and Bitwise Operations:** Rainstorm's mixing relies on XOR, addition-like operations (in this case, subtraction mod 2^{64}), and rotations. This mirrors a common trend in modern hashes (e.g., BLAKE2, Skein) that forgo complicated S-boxes in favor of simple, fast, and hardware-friendly operations. Although these primitives are widely used, the specific combination and parameters in Rainstorm have not been previously analyzed to the same extent.

Potential Avenues for Cryptanalysis and Attack

Despite these conceptual parallels, Rainstorm's security remains unestablished. Potential weaknesses and cryptanalytic angles include:

- **Novelty of the Core Mixing Function:** Rainstorm's core mixing step (`weakfunc`) is a custom design with no standard reference primitive. Unlike SHA-3's Keccak permutation or BLAKE2's ChaCha-inspired round function, Rainstorm does not build on a widely scrutinized component. Cryptanalysts may attempt reduced-round attacks or differential analyses to identify whether certain input differences propagate through the rounds in a non-uniform or predictable way.

- **Choice of Subtraction vs. Addition:** Many hash functions rely on addition mod 2^{64}, which has been studied extensively. Rainstorm uses subtraction mod 2^{64} alongside XOR and rotation. While addition and subtraction are isomorphic in mod 2^{64} arithmetic, the specific pattern might introduce subtle biases. Cryptanalysts could investigate whether subtraction interacts with the chosen rotation and XOR patterns to yield exploitable structural properties.

- **Constants and Rotation Schedules:** Rainstorm's constants are prime-based and chosen for good avalanche properties as indicated by tests like SMHasher3. However, such tests catch only relatively coarse statistical weaknesses. A more granular cryptanalysis might reveal differential characteristics or linear trails that remain undetected by these broad tests. The fixed rotation amounts and constants might form weak points if attackers can construct differential paths with relatively high probability.

- **Keyed Initialization and Length Dependence:** The initialization of the internal state depends on the seed and message length, both linearly integrated. While this ensures domain separation, it also creates a direct algebraic relationship between seed, length, and initial state words. Cryptanalysts may explore scenarios where multiple messages differ only in length or seed to determine if these relationships simplify certain attacks.

- **Additional Rounds for Larger Outputs:** Rainstorm applies extra rounds when producing longer outputs (e.g., for 128-, 256-, or 512-bit digests). While additional mixing may enhance security, it could also introduce structures that differ from the base case. A thorough cryptanalysis would examine whether certain output sizes are more susceptible to analysis than others, potentially using truncated outputs or focusing on properties of the final mixing stages.

Comparison to Established Processes (e.g., SHA-3 Competition)

During the SHA-3 competition, candidates underwent rigorous third-party cryptanalysis, differential attacks, and attempts to find structural weaknesses. This process was transparent and involved the broader cryptographic community. Rainstorm's current status more closely resembles a preliminary proposal: it shows promising avalanche behavior and passes heuristic tests, but has not yet faced the same level of scrutiny.

For Rainstorm to gain confidence, a similar public and professional cryptanalysis effort is necessary. Attacks that were effective at distinguishing or breaking other SHA-3 candidates might be adapted to probe Rainstorm for non-random behavior.

Conclusion

While Rainstorm's design choices appear reasonable at a surface level—incorporating large internal states, carefully chosen constants, and simple bitwise operations—the absence of a well-known, deeply analyzed primitive leaves it open to a wide range of cryptanalytic investigations. Researchers may attempt differential, linear, rotational, or algebraic attacks, as well as attempts to break reduced-round versions.

In summary:

- Rainstorm shares some structural concepts with established hash functions but does not rely on a known, vetted permutation or function.

- Potential weaknesses lie in the unexplored properties of its custom mixing steps and arithmetic choices.

- A comprehensive and public cryptanalysis effort is needed to determine whether Rainstorm can offer security properties comparable to established standards.

This note thus serves as an invitation and a guidepost for cryptanalysts. By applying the methods developed during the SHA-3 competition and other cryptographic evaluations, the community can determine if Rainstorm stands up to rigorous cryptographic standards or if its structure conceals exploitable weaknesses.