A Novel Cryptographic Hash Code Algorithm Based on Cellular Automata

Mohanka, Rishabh (School: Suncoast Community High School)

Cryptographic hash code algorithms are vital to the security of information and data -- hash codes are like unique fingerprints for one's data (can be files, passwords, etc.). The validity of a one-way cryptographic hash code function is determined by its pre-image resistance, second pre-image resistance, and collision resistance. With the advent of faster computers and more powerful GPUs that can hash billions of passwords per second, slower and more resource intensive hash code algorithms are needed to better secure future passwords. The scientist's engineering goal is to successfully develop a cryptographic hash code algorithm based on chaotic cellular automata. Cellular automata are arrays of cells with certain colors which can represent the states of cells, and they recursively evolve through time according a specific set of rules. The scientist devised a novel method to classify chaotic and complex CA. The scientist devised a novel method to classify chaotic CA, and the scientist developed a novel cryptosystem to generate hash codes based on those chaotic CA. Through various performance benchmarks such as computational speed and randomness, the CAHash function proved to be slow and resource intensive yet extremely random proving no correlation between inputs and outputs. The scientist’s engineering goal was complete because a novel cryptographic hash code algorithm based on chaotic cellular automata was successfully developed. In the future, the CAHash function can be improved by being used as a key derivation function to secure passwords and by using work factors to slow it down.