Mitigation and Improving SHA-1 Hash Standard Using Collision Detection Approach

Zeyad Al-Odat, and Samee Khan

1North Dakota State University (NDSU), 2National Science Foundation (NSF)

Abstract
We introduce collision detection and an improved version of SHA-1 standard, which helps to protect weak primitives from any possible collision attack, we proposed two designs to help protect and improve SHA-1 standard, the first one employ near collision detection approach which previously proposed by Marc Stevens, and the second one is our proposal of detection of SHA-1 collision attack using two block calculation scheme.

Methods and Materials

Enhanced SHA-1 Architecture: The idea of counter SHA-1 collision attack can be depicted in figure 3 below, the input message is processed and checked using collision detection mechanism.

Collision Detection Mechanism: we are presenting two approaches for SHA-1 counter collision attack as seen in figures 4 and 5, by which we can detect any possibility of collision occurrence by only checking one message, and from here comes the challenge, detect the collision from only one message, after that invalidate the output hash in case of collision.

Results

Both of the above mentioned approaches were tested and verified for part of the published disturbance vectors.

Discussion and Future Work
We presented Counter Cryptanalyst method to protect SHA-1 hash function from collision attack, and improve the hash computation to support entities that still using SHA-1 hash standard. The proposed approaches can be further improved to get more secure and trusted SHA-1 hash function, also help speed up the process of computing the hash values, as the new approaches may consume more time to calculate the hash than original one. This work used to protect digital signature as seen in figure 7 below. Can be further improved in term of speed and memory.

Conclusions
We are presenting two methods to improve SHA-1 standard against collision attack, the first approach relay on Marc’s approach for detecting SHA-1 collision attack, the other approach take advantage of two block Collision attack to help speed up the process of detecting collision. Truncated SHA-512/1024 is suggested to replace suspicious message's hash outputs.

Acknowledgment
We would like to thank the Center for Computationally Assisted Science and Technology (CCAST) of NDSU.

Contact
Zeyad A Al-Odat
North Dakota State University
[NDSU Dept 2480, PO Box 6050]
Email: info@genigraphics.com
[7017303344]

Table 2 represents two messages that collide to the same hash value output

References