Further Musings on the Wang *et al*. MD5 Collision: Improvements and Corrections on the Work of Hawkes, Paddon, and Rose

By Gregory Hirshman

Collision for MD5

M_0: 02dd31d1c4eee6c5069a3d695cf9af98**8**7b5ca2fab7e46123e580440897ffbb8
0634qd5502b3f4098388e4835a41**7**125e82551089fc9cdf7**f**2bd1dd95b3c3780

M_1: d11d0b969c7b41dcf497d8e4d555655a**c**79a73350cfdebfo66f129308fb109d1
797f2775eb5cd530baade8225c15**c**c79ddcb74ed6dd3c55f**d**80a9bb1e3a7cc35

M_0': 02dd31d1c4eee6c5069a3d695cf9af98**0**7b5ca2fab7e46123e580440897ffbb8
0634qd5502b3f4098388e4835a41**f**125e82551089fc9cdf7**7**2bd1dd95b3c3780

M_1: d11d0b969c7b41dcf497d8e4d555655a**4**79a73350cfdebfo66f129308fb109d1
797f2775eb5cd530baade8225c15**4**c79ddcb74ed6dd3c55f**5**80a9bb1e3a7cc35

H: 9603161fa30f9dbf9f65ffbcf41fc7ef

A collision occurs when two or more input messages produce the same message digest, H. In the case above, (M_0, M_1) and (M_0', M_1') yield the same value of H.

Idea Behind My Paper:

- The recent successful attack on the widely used hash function, the MD5 Message Digest Algorithm, was a breakthrough in cryptanalysis.

- The original paper, published in 2004 by Wang *et al*., described this attack in an obscure and elliptical manner.

- Hawkes, Paddon, and Rose subsequently presented the attack in more detail, but even their paper contained numerous unproven statements and several significant errors.

- My paper will explicate their work, prove many of their assertions, and provide original corrections and illustrations to make the differential attack on MD5 more accessible to the mathematically literate reader.

Explication and Elaboration:

- My paper provides the following explication and elaboration.

- First, it compares the unorthodox description of MD5 by Hawkes, Paddon, and Rose to the original description by Ron Rivest.

- Second, it supplies examples for the three conditions that they present for the T_t before they begin their description of the differential.

- Third, it expands on the description of the first block of the differential by explaining the conditions on the T_t in each step.

- Fourth, it presents an original step by step analysis of the description of the second block based only on the table that they provide.

Assertions and Proofs:

- Hawkes, Paddon, and Rose provide assertions for all of bit conditions for the propagation of the differences through the f_t functions for the first block.

- My paper proves all of these assertions except for those mentioned in the sections labeled "Obtaining the Correct ΔQ_t." (since the discussion that they provide for these conditions was sufficient).

- My paper then provides a similar list of assertions for the propagation of the differences through the f_t functions for the second block based only on a few tables that they provide.

- My paper proves all of these assertions as well.

Errors and Corrections:

- My paper corrects two significant errors in work of Hawkes, Paddon, and Rose.

- First, it demonstrates that the complexity of the attack is only about half as great as they believed, i.e., my paper proves the complexity to be 2^{42} rather than 2^{43}.

- Second, it shows that their *Case Two* does not succeed in fulfilling the conditions for the collision differential to hold.