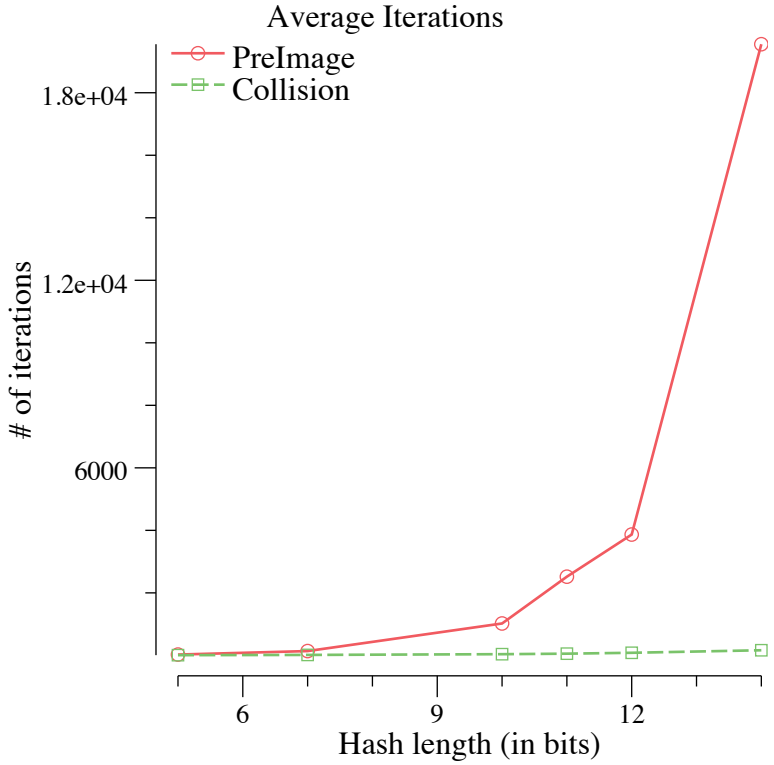
Trevor Lyon
Friday, January 27, 2017
CS465

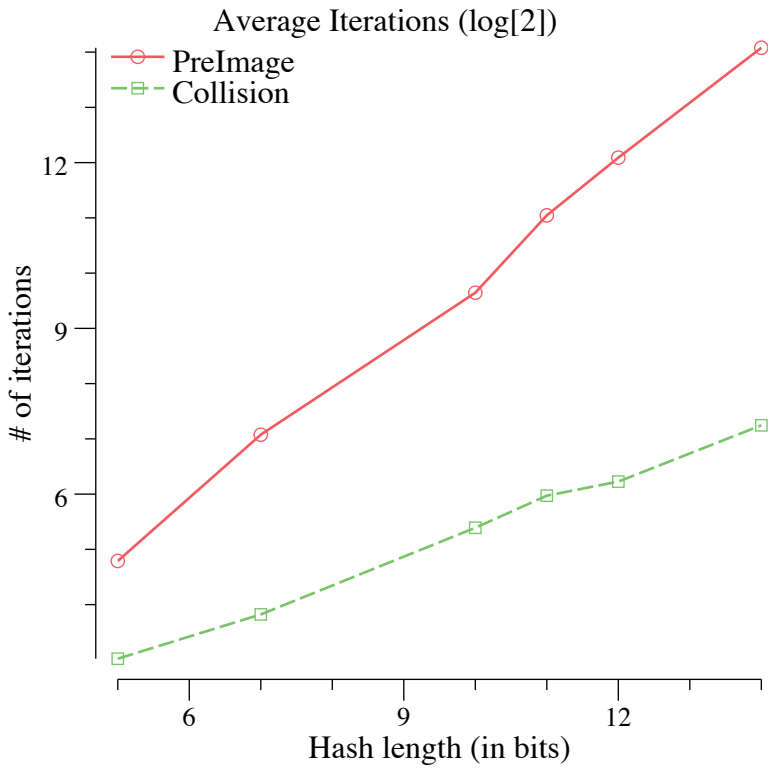
Theoretical and Practical Difference Between a Pre-Image Attack and Collision Attack

In theory, the running time for a collision attack is $O(2^{n/2})$ and the running time for a Pre-Image attack is $O(2^n)$. I implemented both the Pre-Image and Collision attacks in Go. I ran 60 attacks at 6 different bit sizes (5, 8, 10, 11, 12, 14). Taking the average number of iterations over the 60 attacks and plotting them, we can see the relationship between the two different approaches.

The first graph shows the two lines, one for pre-image and one for collision, and the relationship between the bit size of the hash and the average number of iterations it took to succeed. The second graph shows the logarithmic (base 2) relationship between the two.

It can be clearly seen that the relationship between the two is exponential. On the logarithmic graph, the red line, representing the pre-image attack, follows a y=x line which is consistent with the $O(2^n)$ theoretical time. The green line, representing the collision attack follows a y=x/2 line which is also consistent with the $O(2^{n/2})$ theoretical time.





Bit size:	Collision Average	Pre-Image Average
5	7.52	26.36
7	14.98	138.17
10	38.60	1020.95
11	55.15	2518.10
12	83.32	3866.08
14	164.45	19552.45