Better Birthday Attacks via Min-cuts on Boolean Circuits

Ryan Dorson, Dr. Jonathan Katz

Combinatorial Algorithms Applied Research REU

Introduction

- Hash functions map input of arbitrary length to output of fixed length such that it is difficult to find a collision, two inputs that map to the same output
  - Collisions create vulnerability (e.g., compromising a password)
  - Birthday attack is a probabilistic method that finds collisions
  - Collision detection is achieved by generating hash value lists and searching for matches within the lists
- Boolean circuits can be used to model hash functions
  - Vertices correspond to logic gates & input bits, edges connect vertices
  - A min-cut is a partitioning into two disjoint subsets of vertices, such that the number of edges across the partition (min-cut size) is minimized
  - Two inputs with the same min-cut values yield the same outputs, implying a collision
- This work focuses on the discovery of a more efficient variant of the birthday attack, with an eye toward the need for stronger hash functions
  - Key Idea: The modified birthday attack on hash functions modeled as Boolean circuits uses lists of min-cut values, rather than hash values
  - If the min-cut size is smaller than the number of output bits, then shorter lists are sufficient to find a collision
  - With shorter lists, the efficiency of the birthday attack increases, enabling attackers to find collisions with fewer operations
- Goal: Find a min-cut size smaller than the number of output bits and smaller than the number of unfixed input bits
  - In order to reduce the min-cut size, some bits of the input can be fixed (set to either 0 or 1), allowing the circuit to be simplified

Method

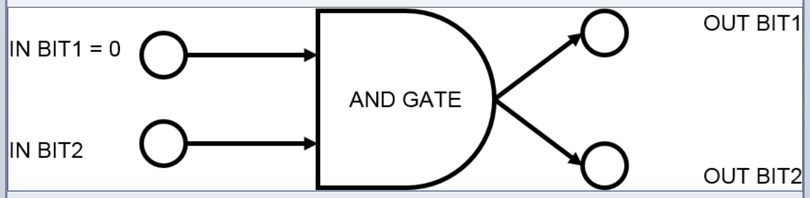
- The MD4 and SHA-1 hash functions were modeled as Boolean circuits using the Java Universal Network/Graph Framework (JUNG)
- Code was developed to:
  - Evaluate these circuits based on input
  - Simplify the circuits by fixing input bits
  - Find min-cut edges of the circuits
- Minimal min-cut sizes were determined by conducting trials
  - Randomly chosen input bits were fixed
  - Circuits were simplified
  - Resultant min-cut sizes were examined

MD4	SHA-1
500 random gates, 1000 trials	500 random gates, 1000 trials
500-640 gates, 10 trials each	500-672 gates, 10 trials each
0-640 gates in increments of 10	0-672 gates in increments of 10

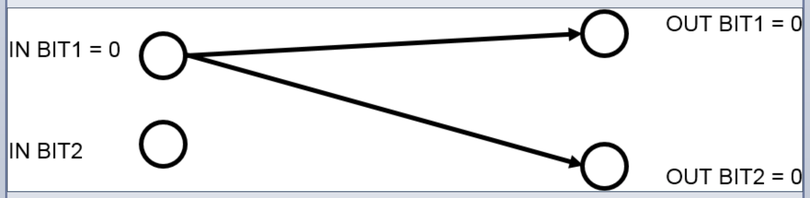
- Exhausting possibilities for any number of fixed gates was not possible
  - Slow speed of the JUNG library's min-cut algorithm (Edmonds-Karp)
  - Large circuits (SHA-1 has ~60,000 vertices and ~120,000 edges)
- If a small min-cut size had been found, then detecting collisions would have been simplified via the modified birthday attack

Circuit Simplification

Boolean Circuit with one fixed input

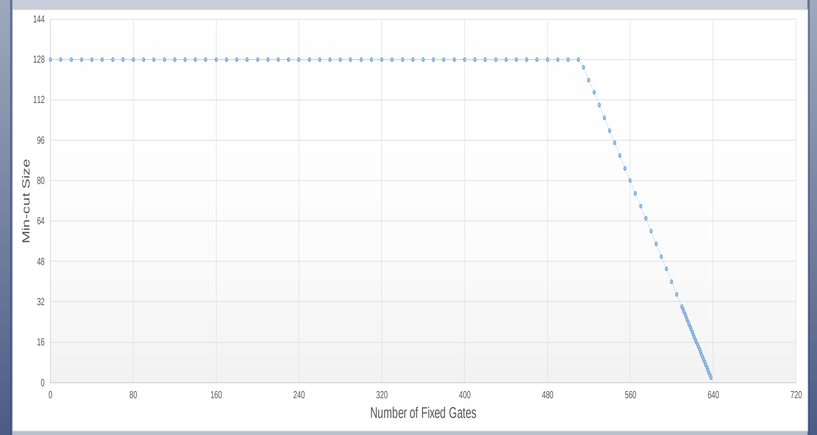


Simplified Boolean circuit with fewer edges



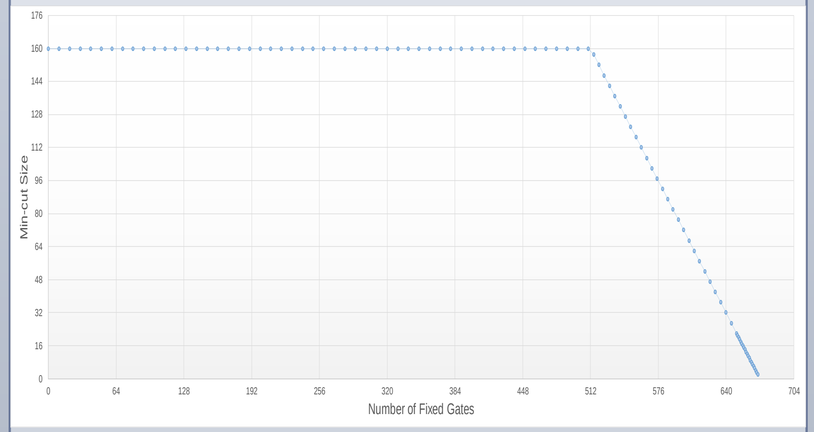
MD4 Results

Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size
0	128	200	128	400	128	555	85	619	21
10	128	210	128	410	128	560	80	620	20
20	128	220	128	420	128	565	75	621	19
30	128	230	128	430	128	570	70	622	18
40	128	240	128	440	128	575	65	623	17
50	128	250	128	450	128	580	60	624	16
60	128	260	128	460	128	585	55	625	15
70	128	270	128	470	128	590	50	626	14
80	128	280	128	480	128	595	45	627	13
90	128	290	128	490	128	600	40	628	12
100	128	300	128	500	128	605	35	629	11
110	128	310	128	510	128	610	30	630	10
120	128	320	128	515	125	611	29	631	9
130	128	330	128	520	120	612	28	632	8
140	128	340	128	525	115	613	27	633	7
150	128	350	128	530	110	614	26	634	6
160	128	360	128	535	105	615	25	635	5
170	128	370	128	540	100	616	24	636	4
180	128	380	128	545	95	617	23	637	3
190	128	390	128	550	90	618	22	638	2



SHA-1 Results

Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size	Num Fixed	Min-cut Size
0	160	200	160	400	160	555	117	651	21
10	160	210	160	410	160	560	112	652	20
20	160	220	160	420	160	565	107	653	19
30	160	230	160	430	160	570	102	654	18
40	160	240	160	440	160	575	97	655	17
50	160	250	160	450	160	580	92	656	16
60	160	260	160	460	160	585	87	657	15
70	160	270	160	470	160	590	82	658	14
80	160	280	160	480	160	595	77	659	13
90	160	290	160	490	160	600	72	660	12
100	160	300	160	500	160	605	67	661	11
110	160	310	160	510	160	610	62	662	10
120	160	320	160	515	157	615	57	663	9
130	160	330	160	520	152	620	52	664	8
140	160	340	160	525	147	625	47	665	7
150	160	350	160	530	142	630	42	666	6
160	160	360	160	535	137	635	37	667	5
170	160	370	160	540	132	640	32	668	4
180	160	380	160	545	127	645	27	669	3
190	160	390	160	550	122	650	22	670	2



Results

- Min-cut size not found to be smaller than the number of output bits
- Modified birthday attack not found to be more efficient than the classic birthday attack at finding collisions in MD4 and SHA-1.

Conclusions

- This particular approach did not indicate a vulnerability for systems that use MD4 and SHA-1
- Future work might include:
  - More exhaustive search for small min-cut sizes
  - Use of faster algorithm, faster computer, or more execution time
  - Identification of vulnerabilities not found here or provision of further confidence in results