Single Block Attacks and Statistical Tests on CubeHash

Benjamin Bloom    Alan Kaminsky

Department of Computer Science
B. Thomas Golisano College of Computing and Information Sciences
Rochester Institute of Technology

October 3, 2009
23rd Midwest Conference on
Combinatorics, Cryptography, and Computing
Invented by Daniel Bernstein, U. of Illinois at Chicago
Submitted to the NIST SHA-3 Competition
One of 51 in Round 1; one of 14 in Round 2
Based on the “sponge construction:”
CubeHash Parameters

- **CubeHash**
  - $r = \text{Number of mixing rounds per message block (} r \geq 1\text{)}$
  - $b = \text{Number of bytes per message block (} 1 \leq b \leq 128\text{)}$
  - $h = \text{Size of hash value in bits (} h = 8, 16, 24, \ldots, 512\text{)}$

- CubeHash expected to be more secure with:
  - More mixing rounds (larger $r$)
  - Smaller message blocks (smaller $b$)

- Recommendation for SHA-3 Round 2: CubeHash16/32-$h$
Outline

1. Introduction
2. Single Block Attack
3. Parallel Implementation
4. Attack Results
5. Statistical Tests
Single Block Attack

CubeHash Round Function

Input state, thirty-two 32-bit words

+ (mod 2^{32})

<<< 7

swap

xor

swap

+ (mod 2^{32})

<<< 11

swap

xor

swap

Output state, thirty-two 32-bit words

Benjamin Bloom, Alan Kaminsky (RIT)
Attacks and Tests on CubeHash
MCCCC 2009
Single Block Attack

CubeHash Computation, Single Block Message

- State
- Message
- b bytes
- State
- r rounds
- State
- 0x80 Message padding byte
- State
- r rounds
- State
- 1Finalization word
- State
- 10 rounds
- State
- H
- h/8 bytes
Single Block Attack

State

Message

b bytes

State

Must be equal

r reverse rounds

State

0x80 Message padding byte

State

1 Finalization word

State

10 reverse rounds

State

H

H

T

h /8 bytes

Benjamin Bloom, Alan Kaminsky (RIT)

Attacks and Tests on CubeHash

MCCCC 2009
Single block attack finds a preimage in $2^{8(128-b)}$ trials

Brute force attack finds a preimage in $2^h$ trials

If $2^{8(128-b)} < 2^h$, the single block attack is faster than brute force

- $h = 224$ and $b > 100$
- $h = 256$ and $b > 96$
- $h = 384$ and $b > 80$
- $h = 512$ and $b > 64$

However, single block attack does not break CubeHash16/32-$h$
Outline

1. Introduction
2. Single Block Attack
3. Parallel Implementation
4. Attack Results
5. Statistical Tests
The single block attack is massively parallel

Implemented to run on a hybrid SMP cluster parallel computer

- Partition $n$ trials among $K_p$ processes (nodes)
- Partition each process’s trials among $K_t$ threads
- In each thread, record number of successes and smallest successful trial number $T$
- Shared-memory parallel reduction between threads in each process
- Message-passing parallel reduction between processes

Implemented in Java using the Parallel Java Library

http://www.cs.rit.edu/~ark/pj.shtml
Parallel Program Performance

- “tardis” computer, 10 nodes, 4 CPUs per node, 2.6 GHz clock
- CubeHash1/127-512, $2^{32}$ trials
**CubeHash* \( r/b - 512 \), \( \nu \) different hash values, \( n \) trials per hash value

<table>
<thead>
<tr>
<th>( b )</th>
<th>( \nu )</th>
<th>( n )</th>
<th>( r )</th>
</tr>
</thead>
<tbody>
<tr>
<td>127</td>
<td>100</td>
<td>( 2^{32} )</td>
<td>1</td>
</tr>
<tr>
<td>126</td>
<td>100</td>
<td>( 2^{32} )</td>
<td>2</td>
</tr>
<tr>
<td>125</td>
<td>100</td>
<td>( 2^{32} )</td>
<td>4</td>
</tr>
<tr>
<td>124</td>
<td>10</td>
<td>( 2^{40} )</td>
<td>8</td>
</tr>
</tbody>
</table>


- **CubeHash8/124-512**

- **Original message:**
  
  951fefce947916ccbaf6134ab2b377a54db9f0b7c1f4932b5bc68147dce57828
  ba5b054f446fecc05c9086e96555fada9118b5598364d1b023f425bced094505
  7c33e9fbbe20ff096ba9740f4d278f4922d5178ae650210fa9680512bf998ef1
  2e9f246b5266e40c6240b7a681566d4a3817c19319bbcaede6cf93df

- **Second preimage for** $T = 2,860,087,247$:
  
  d901bc3da81f07c292d9d074825b0fddaf87304fde1fe54fd9cd7c88befbfbbf
  644e39d6d437a99ab9d19dc4f5c3fbf2a61a51533afa4f27c7fabc51c356bbl1e
  2b23d1252ca8e4c421a883c2c43d69abf7a2adc257b219408717ad04ec13b21
  6cf31959fed1e6450c1795280361003affb2cfa6bc0aa786f434911

- **Hash value of original message and second preimage:**
  
  b130c28fbb1dc8aa1135c2a85e46826ab272247a61c246a041664b1e9bad2bd2
  e14c0e0f19386c4838b2214140e6477d7b1b1804128fd9e13a039c8ad26f5ba6
Outline

1. Introduction
2. Single Block Attack
3. Parallel Implementation
4. Attack Results
5. Statistical Tests
Null Hypothesis

- CubeHash behaves as a random mapping

- Statistical tests
  - $\chi^2$ tests of number of successful trials
  - Kolmogorov-Smirnov tests of smallest successful trial number $T$
Tests of Number of Successful Trials

- \( n \) trials
- \( \Pr[\text{success}] = q = 2^{-8(128-b)} \)
- Expected number of successful trials \( s = n \cdot q \)
- Expected number of unsuccessful trials \( = n - s \)
- Observed number of successful trials \( o \)
- Observed number of unsuccessful trials \( = n - o \)
- \( \chi^2 = \frac{(o - s)^2}{s} + \frac{((n - o) - (n - s))^2}{n - s} = \frac{(o - s)^2}{s} + \frac{(o - s)^2}{n - s} \)
- \( p = p\text{-value of } \chi^2 \) for a chi-square distribution with 1 d.o.f.
### χ² Tests of Number of Successful Trials

<table>
<thead>
<tr>
<th></th>
<th>( b = 127 )</th>
<th>( b = 126 )</th>
<th>( b = 125 )</th>
<th>( b = 124 )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>( n = 2^{32} )</td>
<td>( n = 2^{32} )</td>
<td>( n = 2^{32} )</td>
<td>( n = 2^{40} )</td>
</tr>
<tr>
<td>( r = 1 )</td>
<td>( s = 16,777,216 )</td>
<td>( s = 65,536 )</td>
<td>( s = 256 )</td>
<td>( s = 256 )</td>
</tr>
<tr>
<td></td>
<td>( o = 16,768,519 )</td>
<td>( o = 66,254 )</td>
<td>( o = 290 )</td>
<td>( o = 290 )</td>
</tr>
<tr>
<td></td>
<td>( \chi^2 = 4.52604 )</td>
<td>( \chi^2 = 7.86639 )</td>
<td>( \chi^2 = 4.51563 )</td>
<td>( \chi^2 = 4.51563 )</td>
</tr>
<tr>
<td></td>
<td>( p = 0.033383 )</td>
<td>( p = 0.005036 )</td>
<td>( p = 0.033587 )</td>
<td>( p = 0.033587 )</td>
</tr>
<tr>
<td>( r = 2 )</td>
<td>( s = 16,777,216 )</td>
<td>( s = 65,536 )</td>
<td>( s = 256 )</td>
<td>( s = 256 )</td>
</tr>
<tr>
<td></td>
<td>( o = 16,764,484 )</td>
<td>( o = 66,086 )</td>
<td>( o = 300 )</td>
<td>( o = 277 )</td>
</tr>
<tr>
<td></td>
<td>( \chi^2 = 9.70003 )</td>
<td>( \chi^2 = 4.61585 )</td>
<td>( \chi^2 = 7.56250 )</td>
<td>( \chi^2 = 1.72266 )</td>
</tr>
<tr>
<td></td>
<td>( p = 0.001843 )</td>
<td>( p = 0.031678 )</td>
<td>( p = 0.005960 )</td>
<td>( p = 0.189351 )</td>
</tr>
<tr>
<td>( r = 4 )</td>
<td>( s = 16,777,216 )</td>
<td>( s = 65,536 )</td>
<td>( s = 256 )</td>
<td>( s = 256 )</td>
</tr>
<tr>
<td></td>
<td>( o = 16,763,353 )</td>
<td>( o = 66,188 )</td>
<td>( o = 304 )</td>
<td>( o = 209 )</td>
</tr>
<tr>
<td></td>
<td>( \chi^2 = 11.4999 )</td>
<td>( \chi^2 = 6.48667 )</td>
<td>( \chi^2 = 9.00000 )</td>
<td>( \chi^2 = 8.62891 )</td>
</tr>
<tr>
<td></td>
<td>( p = 0.000696 )</td>
<td>( p = 0.010869 )</td>
<td>( p = 0.002700 )</td>
<td>( p = 0.003309 )</td>
</tr>
<tr>
<td>( r = 8 )</td>
<td>( s = 16,777,216 )</td>
<td>( s = 65,536 )</td>
<td>( s = 256 )</td>
<td>( s = 256 )</td>
</tr>
<tr>
<td></td>
<td>( o = 16,767,205 )</td>
<td>( o = 64,713 )</td>
<td>( o = 203 )</td>
<td>( o = 287 )</td>
</tr>
<tr>
<td></td>
<td>( \chi^2 = 5.99701 )</td>
<td>( \chi^2 = 10.3354 )</td>
<td>( \chi^2 = 10.9727 )</td>
<td>( \chi^2 = 3.75391 )</td>
</tr>
<tr>
<td></td>
<td>( p = 0.014330 )</td>
<td>( p = 0.001305 )</td>
<td>( p = 0.000925 )</td>
<td>( p = 0.052684 )</td>
</tr>
</tbody>
</table>
K-S Tests of $\chi^2$ Distributions

- Expected (red) and observed (black) distributions of $\chi^2$ for CubeHash1/127-512
## K-S Tests of $\chi^2$ Distributions

<table>
<thead>
<tr>
<th></th>
<th>$b = 127$</th>
<th>$b = 126$</th>
<th>$b = 125$</th>
<th>$b = 124$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r = 1$</td>
<td>$D$ 0.081986</td>
<td>$D$ 0.099036</td>
<td>$D$ 0.091300</td>
<td>$D$ 0.449424</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.495247</td>
<td>$p$ 0.266442</td>
<td>$p$ 0.359208</td>
<td>$p$ 0.023479</td>
</tr>
<tr>
<td>$r = 2$</td>
<td>$D$ 0.093538</td>
<td>$D$ 0.062532</td>
<td>$D$ 0.051574</td>
<td>$D$ 0.217311</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.330395</td>
<td>$p$ 0.817055</td>
<td>$p$ 0.947710</td>
<td>$p$ 0.676334</td>
</tr>
<tr>
<td>$r = 4$</td>
<td>$D$ 0.126019</td>
<td>$D$ 0.098237</td>
<td>$D$ 0.068251</td>
<td>$D$ 0.283495</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.076778</td>
<td>$p$ 0.275138</td>
<td>$p$ 0.725416</td>
<td>$p$ 0.339452</td>
</tr>
<tr>
<td>$r = 8$</td>
<td>$D$ 0.092620</td>
<td>$D$ 0.062538</td>
<td>$D$ 0.071269</td>
<td>$D$ 0.191768</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.342026</td>
<td>$p$ 0.816968</td>
<td>$p$ 0.674332</td>
<td>$p$ 0.813183</td>
</tr>
</tbody>
</table>

- Conclusion: Null hypothesis not disproved at 0.001 significance
K-S Tests of Smallest Successful $T$ Distributions

- $\Pr[\text{success}] = q = 2^{-8(128-b)}$
- $\Pr[T \text{ failures then 1 success}] = (1 - q)^T q$
- $\Pr[\leq T \text{ failures then 1 success}] = \sum_{i=0}^{T} (1 - q)^i q = 1 - (1 - q)^{T+1}$
Expected (red) and observed (black) distributions of smallest successful $T$ for CubeHash1/127-512
### K-S Tests of Smallest Successful $T$ Distributions

<table>
<thead>
<tr>
<th>$r$</th>
<th>$b = 127$</th>
<th>$b = 126$</th>
<th>$b = 125$</th>
<th>$b = 124$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$D$ 0.105274</td>
<td>$D$ 0.070612</td>
<td>$D$ 0.080661</td>
<td>$D$ 0.240533</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.205371</td>
<td>$p$ 0.685513</td>
<td>$p$ 0.516467</td>
<td>$p$ 0.547622</td>
</tr>
<tr>
<td>$r = 2$</td>
<td>$D$ 0.066822</td>
<td>$D$ 0.083771</td>
<td>$D$ 0.083605</td>
<td>$D$ 0.245708</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.749153</td>
<td>$p$ 0.467318</td>
<td>$p$ 0.469881</td>
<td>$p$ 0.519894</td>
</tr>
<tr>
<td>$r = 4$</td>
<td>$D$ 0.047921</td>
<td>$D$ 0.115872</td>
<td>$D$ 0.111087</td>
<td>$D$ 0.193748</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.972475</td>
<td>$p$ 0.127049</td>
<td>$p$ 0.158740</td>
<td>$p$ 0.803264</td>
</tr>
<tr>
<td>$r = 8$</td>
<td>$D$ 0.089831</td>
<td>$D$ 0.054503</td>
<td>$D$ 0.067466</td>
<td>$D$ 0.213803</td>
</tr>
<tr>
<td></td>
<td>$p$ 0.378969</td>
<td>$p$ 0.920626</td>
<td>$p$ 0.738502</td>
<td>$p$ 0.695875</td>
</tr>
</tbody>
</table>

**Conclusion:** Null hypothesis not disproved at 0.001 significance.
Single block attack finds second preimages in CubeHash
Attack is massively parallel
Attack breaks reduced-strength versions of CubeHash
Attack does not break full-strength SHA-3 versions
Statistical tests do not disprove randomness of CubeHash
This work supports CubeHash’s viability as a cryptographic one-way hash function
Technical report

Source code and full results
http://www.cs.rit.edu/~ark/parallelcrypto/cubehash01/
Contact Information

Alan Kaminsky
Department of Computer Science
B. Thomas Golisano College of Computing and Information Sciences
Rochester Institute of Technology
102 Lomb Memorial Drive
Rochester, NY 14623
585-475-6789
http://www.cs.rit.edu/~ark/
ark@cs.rit.edu