RC6—The elegant AES choice

Ron Rivest rivest@mit.edu

Matt Robshaw mrobshaw@supanet.com

Yiqun Lisa Yin yiqun@nttmcl.com

RC6 is the right AES choice

- Security
- Performance
- Ease of implementation
- Simplicity
- Flexibility

RC6 is simple: only 12 lines

```
B = B + S[ 0 ]
D = D + S[ 1 ]
for i = 1 to 20 do
   {
      t = ( B x ( 2B + 1 ) ) <<< 5
      u = ( D x ( 2D + 1 ) ) <<< 5
      A = ( ( A ⊕ t ) <<< u ) + S[ 2i ]
      C = ( ( C ⊕ u ) <<< t ) + S[ 2i + 1 ]
      (A, B, C, D) = (B, C, D, A)
    }
A = A + S[ 42 ]
C = C + S[ 43 ]
```

Simplicity

- Facilitates and encourages analysis
  - allows rapid understanding of security
  - makes direct analysis straightforward (contrast with Mars and Twofish)
- Enables easy implementation
  - allows compilers to produce high-quality code
  - obviates complicated optimizations
  - provides good performance with minimal effort

RC6 security is well-analyzed

- RC6 is probably most studied AES finalist
  - RC6 is based on RC5
  - RC6 analysis builds directly on RC5 analysis
  - original RC6 analysis is very detailed
  - RC6 simplified variants studied extensively
  - small-scale versions allowed experimentation

RC6 key schedule is rock-solid

- Studied for more than six years
- Secure
  - thorough mixing
  - one-way function
  - no key separation (cf. Twofish)
  - no related-key attacks (cf. Rijndael)

Original analysis still accurate

- RC6 meets original design criteria
- Security estimates from 1998 still good today; independent analyses supportive.
- Secure, even in theory, even with analysis improvements far beyond those seen for DES during its lifetime
- RC6 provides a solid, well-tuned margin for security

32-bit Performance

- Excellent performance
- 32-bit CPUs are
  - NIST reference platform
  - a significant fraction of installed computers throughout the AES lifetime
  - becoming more prevalent in cheaper devices (e.g. ARM)

Smart Card Suitability

- RC6 fits in the cheapest smart cards, and well-suited for many (e.g. ARM processor)
- Bandwidth, not CPU, likely to be most significant bottleneck
- 8-bit CPUs will become far less important over the AES lifetime

Performance on 64-bit CPUs

- Generally good 64-bit performance
- IA64-performance only fair but anomalous--slower than Pentium!
  - Note 3x improvement with IA64++
- Future chips will optimize AES
- In addition, RC6 gains dramatically with multi-block processing compared to other schemes

Major Trends: Java and DSPs

- Increasing use of Java
  - for e-commerce and embedded apps.
  - RC6 provides excellent speed with minimal code size and memory usage
- Increasing use of DSP chips
  - likely to be more significant than IA64 or 8-bit processors
  - RC6 gives excellent performance

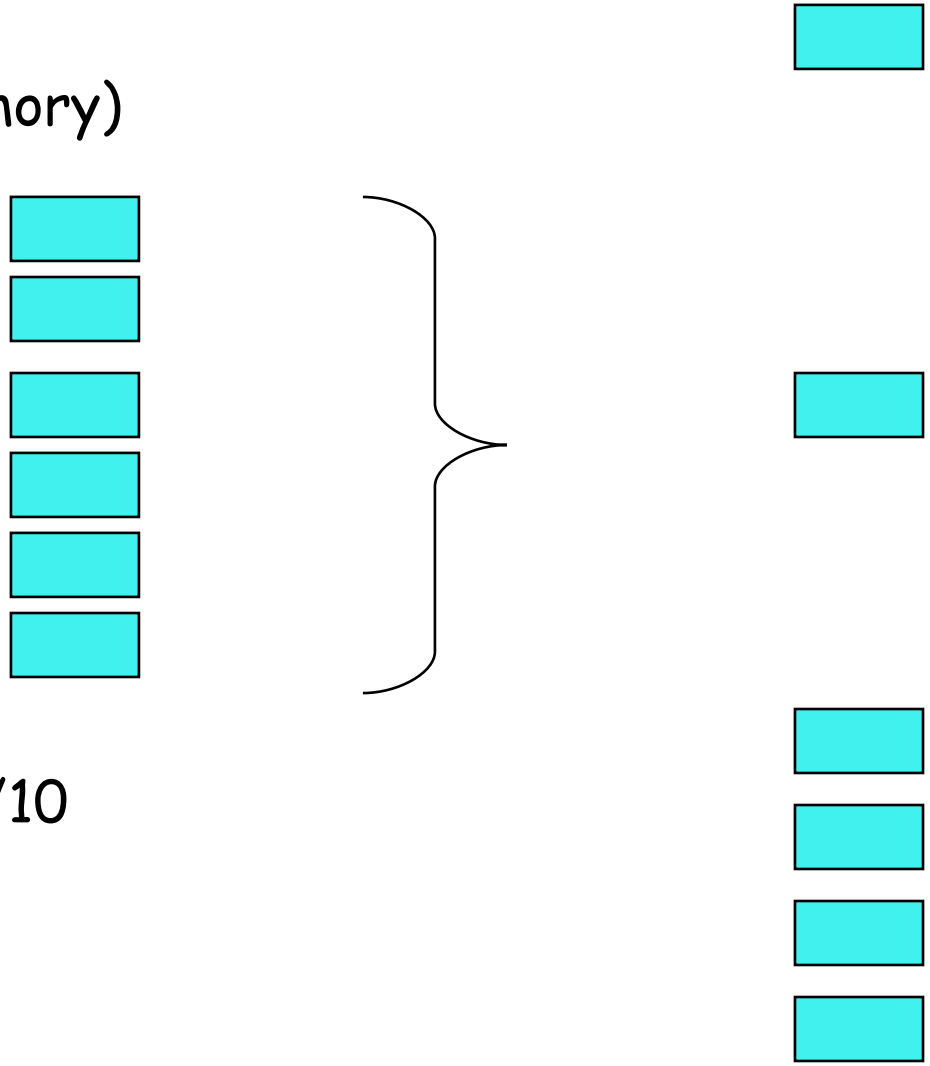
Flexibility

- RC6 is fully parameterized
  - key size, number of rounds, and block length can be readily changed
  - well-suited for hash functions
- RC6 is only AES finalist that naturally gives DES and triple-DES compatible variants (64-bit blocks)

How do we grade candidates?

- Security (corroborated)
- Performance (speed+memory)
  - 32-bit (30%)
  - Java (20%)
  - DSP (15%)
  - 64-bit (15%)
  - Hardware (15%)
  - 8-bit (5%)
- Ease of implementation
- Simplicity
- Flexibility

Overall: 40/25/15/10/10



Conclusions

- RC6 is a simple yet remarkably strong cipher
  - good performance on most important platforms
  - simple to code for good performance
  - excellent flexibility
  - the most studied finalist
  - the best understood finalist
- RC6 is the secure and "elegant" choice for the AES

(The End)