



AES and Future Resiliency: More Thoughts and Questions

**Don B. Johnson
djohnson@certicom.com
Third AES Conference**



Cat Fight

**NIST has placed 5
Cats in a Bag.
See who survives.
Better to find out
now, rather than
later.
Good job!**





I Cheated and Looked Ahead

I read what each finalist team had to say.

SURPRISE!

Each team said that their algorithm had so many advantages it should be chosen.

Given the expertise on each team, I also wonder which algorithms (besides their own) they like and dislike and why?



Pop Quiz: Which Algorithm Is

Best on smartcard?

Best on FPGA?

Best on purpose-built hardware?

Best on Pentium/Alpha/RISC?

Best for DSP decryption of video?

Best for IPSEC?

Get different answers!



The Future?

Who knows what the future holds in store?

We do not know what we do not know!

Best guess is that the future is similar to the past, at least in many ways.

Should try to prepare for the unexpected.

Adversary attacks in future, when more is known. This is an unfair battle!



Quantum Computing?

Quantum computing MIGHT allow a square root attack on symmetric key.

Limit due to quantum decoherence?

What about parallel qubit engines?

What does a 40, 80 or 100 qubit engine imply, if anything, to AES finalists?

Can someone (NIST?) try to answer this?



Space-Time Wormhole Attack?



Scenario: In 2011, a physicist at Sandia discovers that 4th dimensional space-time wormholes exist!

Science-Fiction attack

What does this mean for the AES?

Do not ask me! How should I know!



Combo Attacks



A new attack is discovered which has an advantage of a few bits. A concern?

Multiple attacks each of only a few bits might result in a real attack on a product.

A few bits here and there can add up.

An attack in practice can exploit errors by standards, implementations, users.



Why Choose One AES Winner?



Interoperability - all products use winner

Simplicity - products only deal with one choice, documentation is simpler

Cost Effectiveness - one is cheaper

Testing - testing one is easier

Net: There should be good reasons for not choosing only one winner.



Multiple Winners?



NIST should seek design disparity among AES winners for: future resiliency, crypto knowledge, Super AES, crypto toolbox, possible patents (M. Smid), target diffusion, avoidance of artificial tiebreakers, constraints of other standards bodies & recognition of the AES decision being multidimensional.



Multiple Winners - 2

Space probe - HW is fixed (J. Coffin)

AES Selection time versus Internet time

Infrastructure Overoptimization - only DES
meant products were not flexible

NIST as AES Process Architect

NIST or Marketplace?

One or many may give different answers.



How to Handle a Nightmare

Have one winner & plan to add rounds if
winner gets broken.

- ◆ Adding rounds is RC6 philosophy

Have a ranked order of winners?

Have an unordered list of winners?

Claim: Any choice is plausible.



Adding Rounds

Software should be “easy” to modify to add rounds. But there are “ripple” effects.

Hardware may be designed to be able to add rounds, but may lose efficiency.

BIG IF: What if adding rounds (more of the same) does not address the concern?

Might be better to add disparate rounds.



Ranked AES Winners

NIST selects a winner and a backup (say).

Every product implements the winner.

If you can/must, also do backup for insurance.

This at least does not put all eggs in one basket.



Unranked AES Winners

Unranked AES winners would be similar to asymmetric ideas in new FIP 186-2 (use DSA, RSA and/or ECDSA).

Concern: How to address potential for bloated products due to feature creep?



Small and Big Systems

Small products (clients) will hit some constraint, would like to choose one good algorithm that minimizes limitations of product. Often have a short lifecycle.

Big products (servers) can do a handful of algorithms, if needed in order to be interoperable with clients.



NIST AES Evaluation

Any of 31 non-null subsets **COULD** be justified by NIST.

Too **MANY** answers!

NIST indicates by its selection (by reverse engineering) what criteria it considers most important.


Important for NIST not to appear arbitrary.




Less is More?

NIST as AES process architect decides to “do the least” & let marketplace decide:

- A) NIST could issue “bills of health” for some number of finalists.
- B) NIST could issue recommendations for Federal government use, ordered or not, using whatever criteria it desires.



The Future



This page intentionally left blank.

