The First SHA-3
Candidate Conference

NIST's Plan for Handling Tunable Parameters

Speaker: Souradyuti Paul

Souradyuti.Paul@nist.gov

February 27, 2009

Tunable Parameters (1)

- What are they?
  - Specify the hash algorithm in terms of some parameters, say, u,v,w.
  - The hash $H_{u,v,w}$(Message)
  - Different u,v,w impact the security-performance
  - Examples: block-length, # of rounds etc.

Tunable Parameters (2)

Federal Register Notice, Vol. 72, No. 212/Friday, November 2, 2007, Notice

"In addition, ***the submitted algorithm may include a tunable security parameter****, such as the number of rounds, which would allow the selection of a range of possible security/performance tradeoffs. If such a parameter is provided, the submission document must specify a recommended value for each digest size specified in Section 3, with justification.* ***The submission should also provide any bounds that the designer feels are appropriate for the parameter, including a bound below which the submitter expects cryptanalysis to become practical.*** *The tunable parameter may be used to produce weakened versions of the submitted algorithm for analysis, and permit NIST to select a different security/performance tradeoff than originally specified by the submitter, in light of discovered attacks or other analysis, and in light of the alternative algorithms that are available.* ***NIST will consult with the submitter of the algorithm if it plans to select that algorithm for SHA–3, but with a different parameter value than originally specified by the submitter.*** *Submissions that do not include such a parameter should include a weakened version of the submitted algorithm for analysis, if at all possible."*

Tunable Parameters (3)

- Motivation:
  - **Flexibility**
    - An algorithm with a tunable parameter allows the selection of a range of possible security/performance tradeoffs in diverse applications
  - **Analysis of the Weakened Versions**
    - More insight into the algorithm
    - Useful to determine the preferred values of the parameters
      - Ex., if t=5 is weak then set t=5+k. What is k?

Tunable Parameters (4)

- Many of the submissions have tunable parameters
- The designers' recommendations are important

Adjustment of Tunable Parameters

- NIST will allow the submitters to adjust the tunable parameters for the 2nd round
  - Different recommended values
  - Different ranges of values

Other Changes for the 2nd Round

- Submitters can make editorial changes, add analysis or examples etc.
- Submitters may make relatively minor algorithm changes to the algorithms selected for the 2nd round
  - Must explain why

Nature of Changes

- Algorithm changes have potential risks
  - May invalidate existing analysis
  - Effect of change must be clear
  - Must explain why
- Start preparations now: little time for making modifications after selection

The First SHA-3
Candidate Conference

Role of Performance in the First Cut

Speaker: Souradyuti Paul

Souradyuti.Paul@nist.gov

February 27, 2009

Reference Platforms

- We initially focus on
  - Intel Architecture 32-bit (IA-32)
  - Advanced Micro Devices 64-bit (AMD64)

- The most common platforms
  - We have plenty of data on these platforms
  - These platforms are used extensively

- Performance on other platforms will not be overlooked

Speed of SHA-2: An Important Benchmark

- If we adjust tunable parameters to run as fast as SHA-256, SHA-512 on IA-32 and AMD64, is the algorithm secure?
  - If not that hurts its chances

- Beyond that we don't intend to make the first cut strongly driven by performance

Memory Requirements

- For the 1st round we focus on software implementations
  - RAM requirements
  - Code size

- Is the algorithm implementable on constrained environments? (Smart cards)

Hardware Issues

- We will consider obvious hardware issues for the 1st round
- In the 2nd round we expect to have more time for hardware details
  - Hardware implementations
  - Gate counts (FPGA and ASIC)

Other Issues Under Consideration

- Is the algorithm parallelizable?
- Is the algorithm description clear and the design easily analyzable?
- Is the algorithm suitable for various embedded systems?

Additional Considerations

- A convincing argument for exceptionally good or bad performance on constrained hardware environments or smart card processors
- Is there much data on that?
- We encourage analysis by the public

Discussion

- Issue 1: Adjustment of tunable parameters for the 2nd round
- Issue 2: Your opinion on minor changes
- Issue 3: Reference platforms
- Issue 4: Constrained environments
- Issue 5: Hardware applications
- Issue 6: Parallelizability
- Others