The First SHA-3 Candidate Conference

The Way Forward

Bill Burr
william.burr@nist.gov
February 27, 2009
What Have We Learned?

- Leuven is a great place
- We have many good candidates
- Hashes are everywhere
  - Even the low end
  - The low end is always with us
    - How often do low end apps need a collision resistant hash?
Dissonances

• High-end vs. low-end
  - Different focus in different submissions

• Standards ought have few options
  - Anything over $2^{200}$ is overkill
  - So parameterize performance/security

• Proofs are good (maybe necessary), but,
  - How much performance is a proof worth?
Additional Thoughts

• May help to submit to eBash
• Only one “tweek”
• If we think we need to adjust performance parameters in evaluation, we’ll consult with the designer.
The Plan

- Cut down to about 15 2\textsuperscript{nd} round candidates by Crypto 2009 to focus cryptanalysis
  - A balanced group with different approaches
  - Most would be a good final selection
  - Will cut some very good hashes
- 2\textsuperscript{nd} SHA-3 conference close to Crypto 2010
- Post your comments & analysis by June 1 if you can
Thanks!!!