JH

Hongjun Wu[1,2]

[1]Institute for Infocomm Research
[2]Nanyang Technological University

March 24, 2012, Washington D.C.

- Low evaluation cost
- Large security margin
- Implementation

Lessons from SHA-1

- Difficult to analyze
  - difficult to find the best differential trail
  - it took **10 years** to break it
- Not that secure
  - Large differential probability
    - SHA-1: 2^{-83} for steps 17--80 (2005)

Lessons from SHA-1

How to design a hash function with **low evaluation cost against differential attack**?

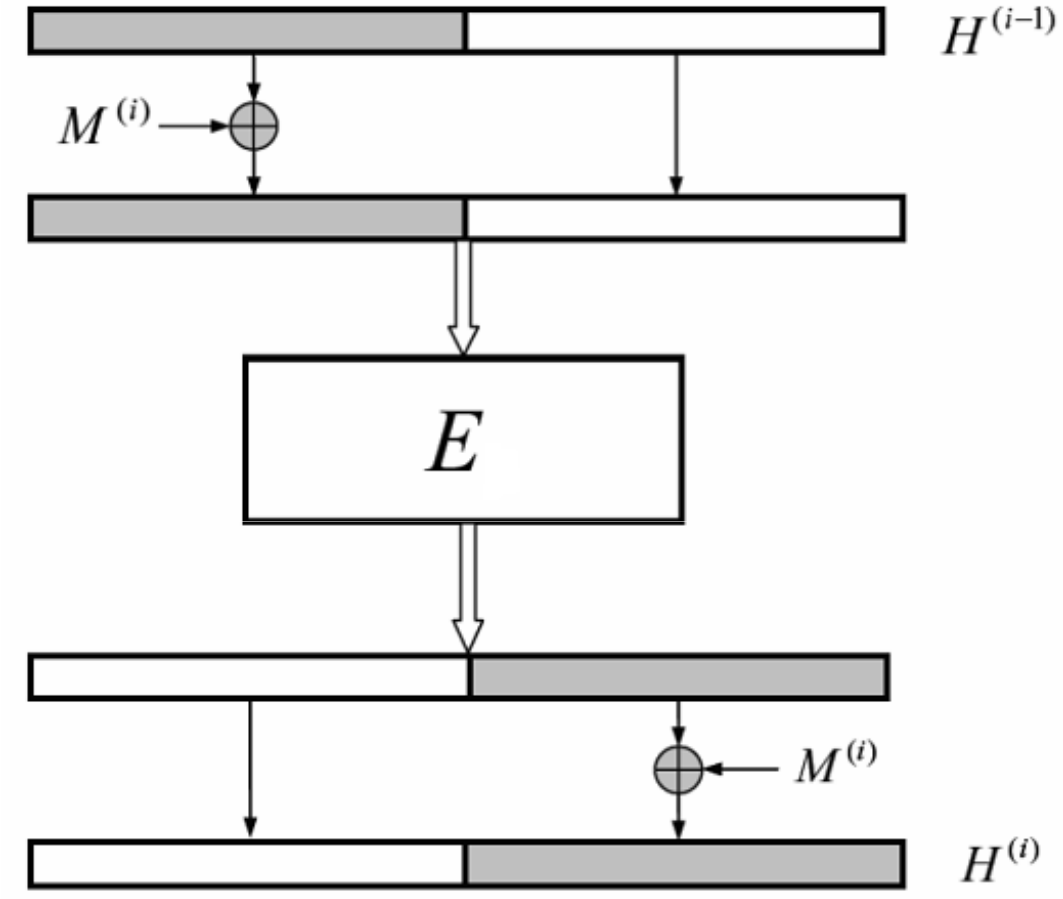
=> JH was designed to solve this problem

Low Evaluation Cost

- Low evaluation cost of JH against differential attack due to:
  - JH compression function structure
    - Analyze the differential propagation in only **one permutation**
  - SPN+MDS in JH
    - Easy to find the best differential trail

Low Evaluation Cost

- JH compression function structure



Low Evaluation Cost

- JH compression function structure
  - New
  - Resist the rebound collision attack
  - Need to analyze the differential trail in only one permutation
- DM, MMO
  - Need to analyze the interaction between two differential paths

Low Evaluation Cost

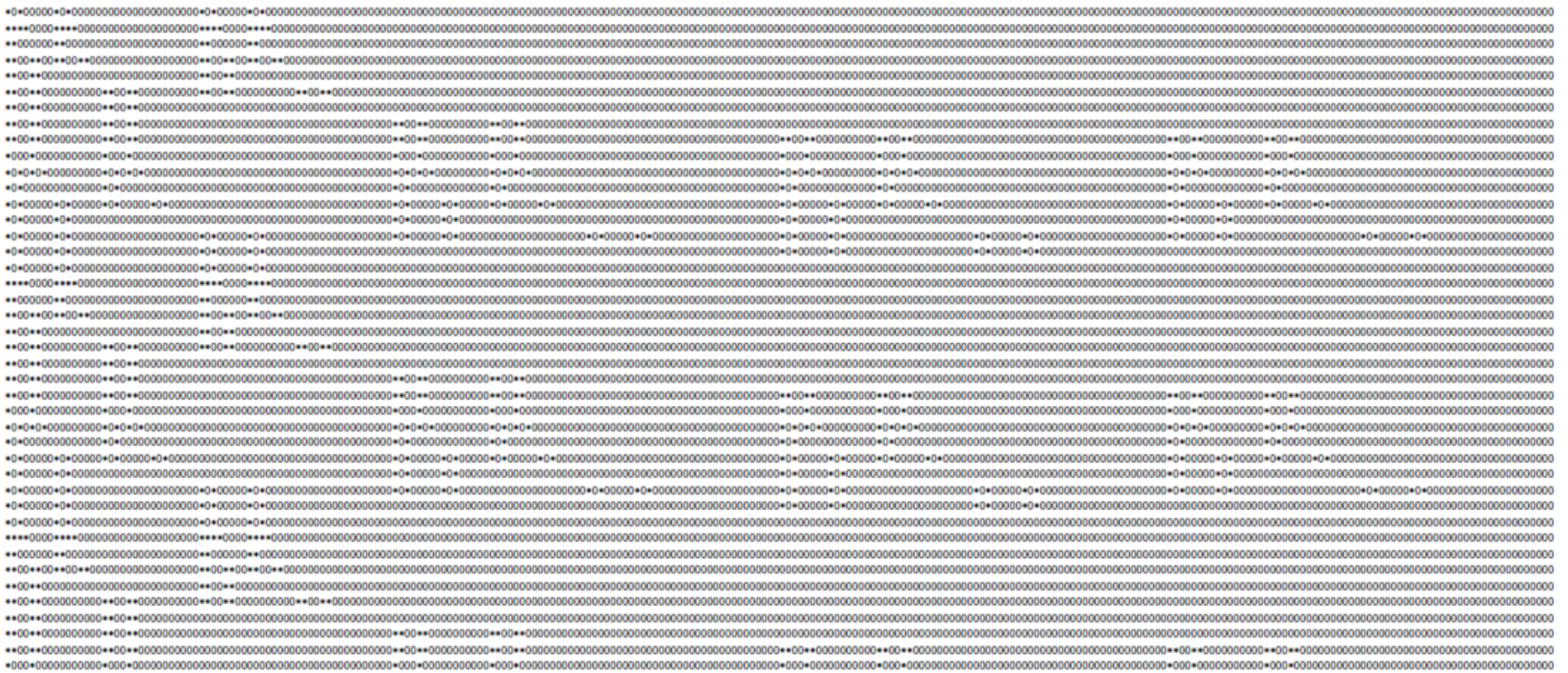
- SPN+MDS (8-dimensional array in JH)
  - SPN + MDS (Rijndael approach) can be analyzed easily against differential attack
    - Easy to find the best differential trail in short period
  - ARX is probably the most difficult to analyze against differential attack

Low Evaluation Cost

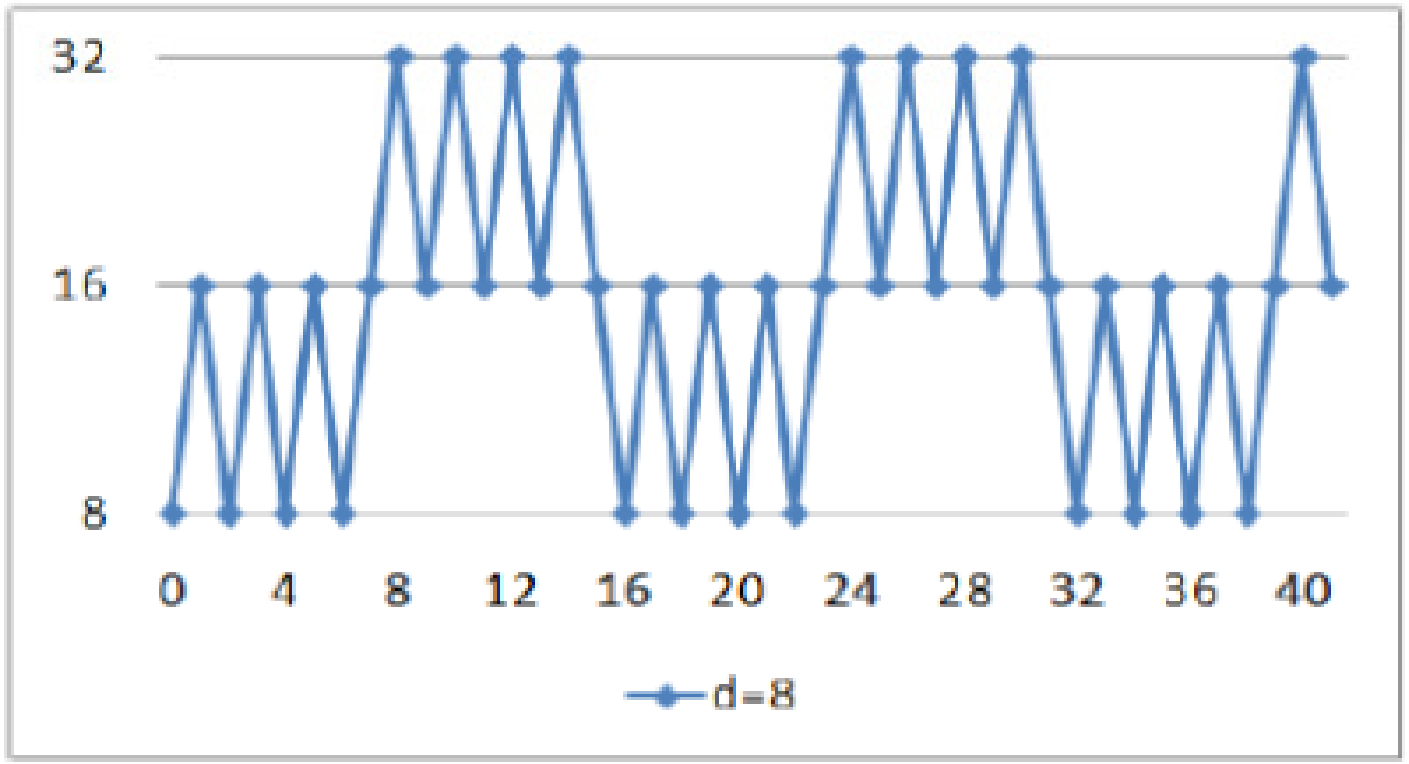
- The evaluation cost of JH against the differential/truncated differential attack is low
  - I was able to finish the analysis before submission
  - My student independently verified the differential/truncated differential attack within 4 months (learning + analysis + coding)
    - TAN Yong Seng. Cryptanalysis of JH, Final Year Project Report, NTU, 2010/2011

Low Evaluation Cost

- A differential path in JH

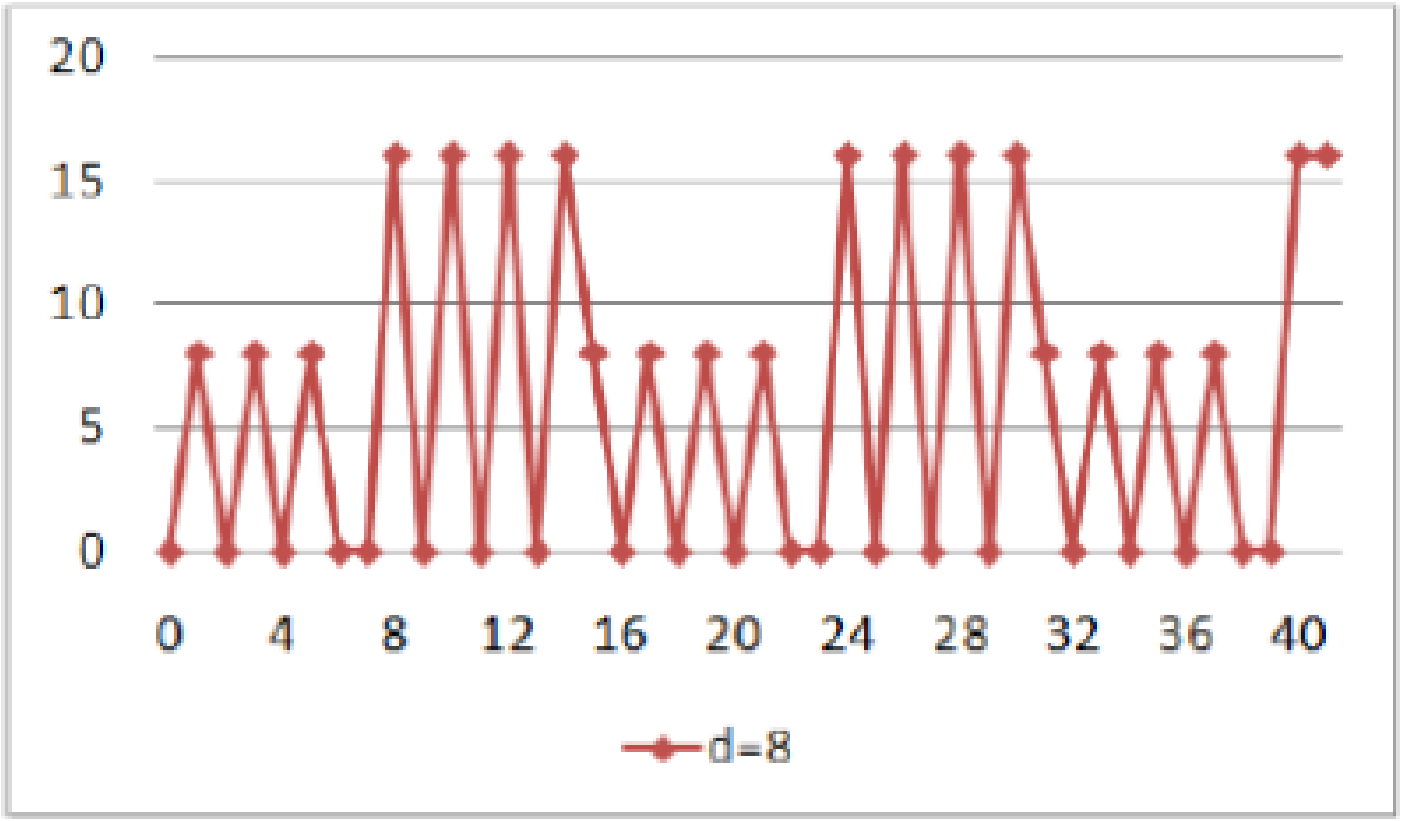


Low Evaluation Cost



Number of active sboxes in differential attack (Tan, 2011)

Low Evaluation Cost



Number of shrinkings in truncated differential attack (Tan, 2011)

Large Security Margin

- Truncated differential attack is the most powerful attack against JH
- JH has large security margin against truncated differential attack that can be easily verified:
  - Assume that message modification can remove 16 rounds, the complexity of the truncated collision attack is **more than 2^{512}**
  - Assume that message modification can remove 24 rounds, the complexity of the truncated collision attack is **more than 2^{400}**

Large Security Margin

- Recent rebound attack on JH
  - Naya-Plasencia, Toz, Varici, Asiacrypt 2011
  - Semi-free-start near-collision attack on 37 rounds
  - Complexity: 2^{352}
- Does this attack affects the differential collision security margin of JH?
  - No.
  - The JH structure is strong against the rebound attack , and the message size is half of the state size

Large Security Margin

- Security proof of compression function structure:
  - Indifferentiable with less than 2^{256} queries

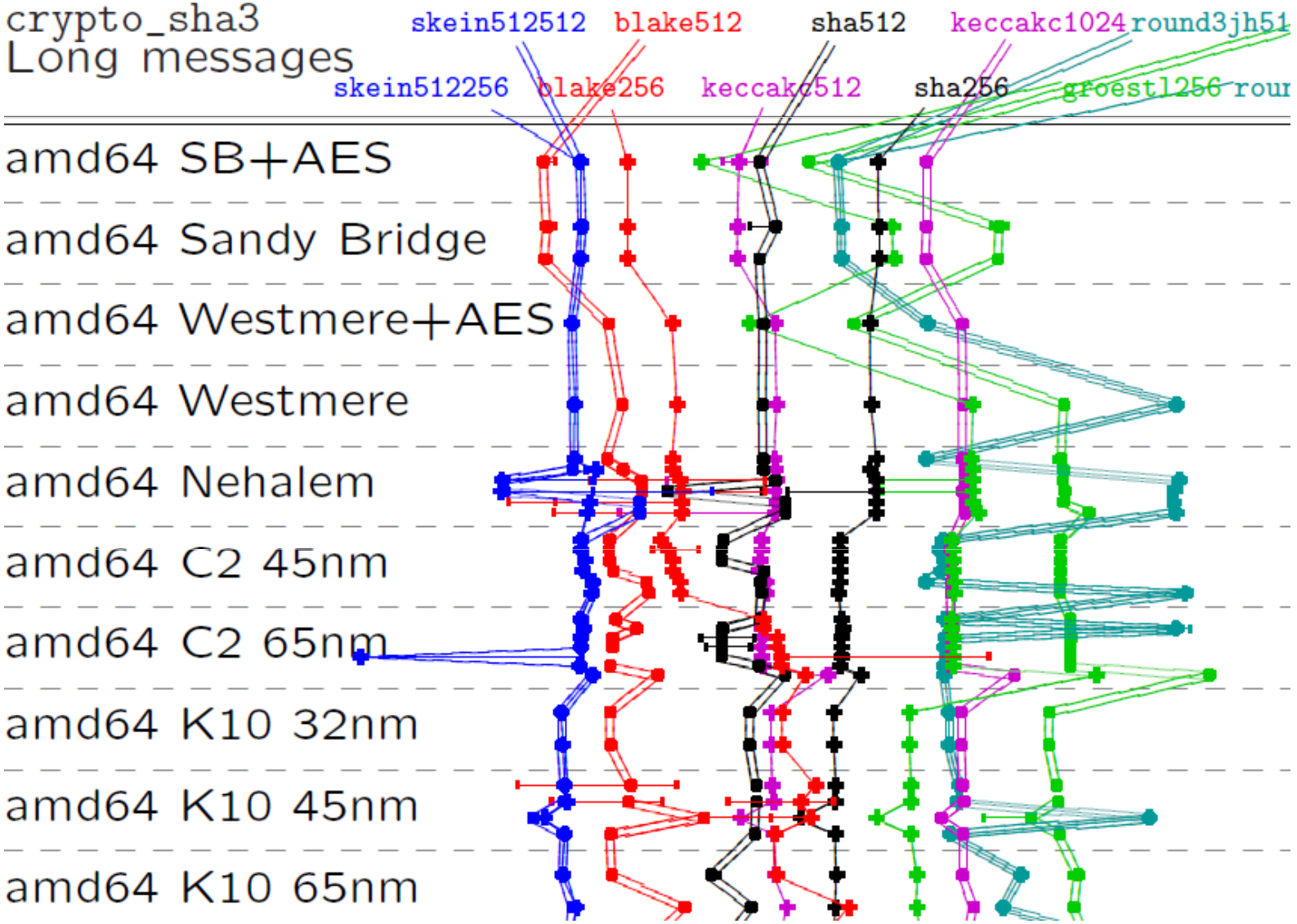
    (Andreeva et al., Paul et. al., the 3rd SHA-3 conference)

Software Implementation

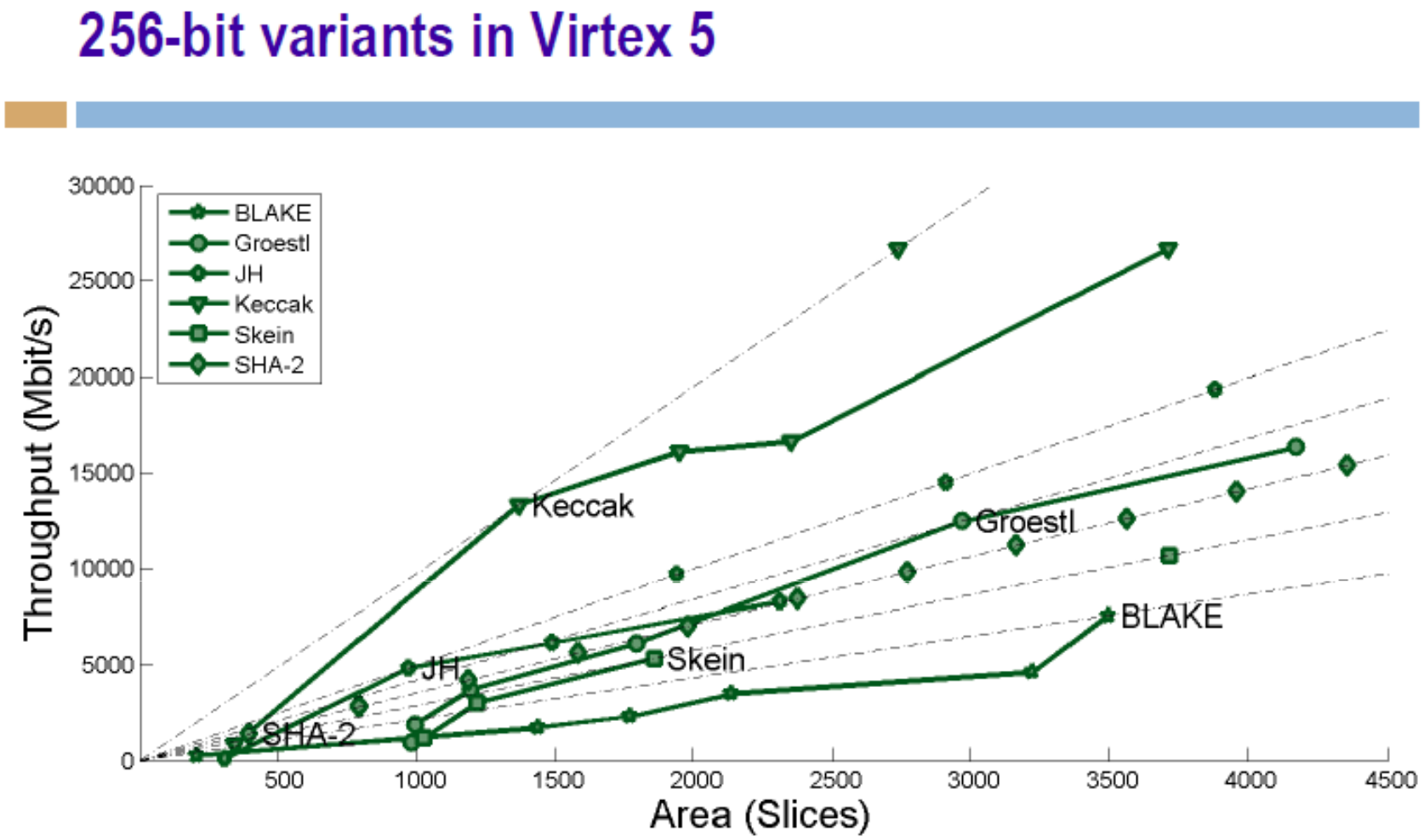
- Fully benefit from the 128-bit SIMD instructions available on many platforms:
  - Common Intel/AMD CPUs
  - Neon SIMD in ARM CPUs
- The Sbox computation benefits from 256-bit AVX instruction

Software Implementation

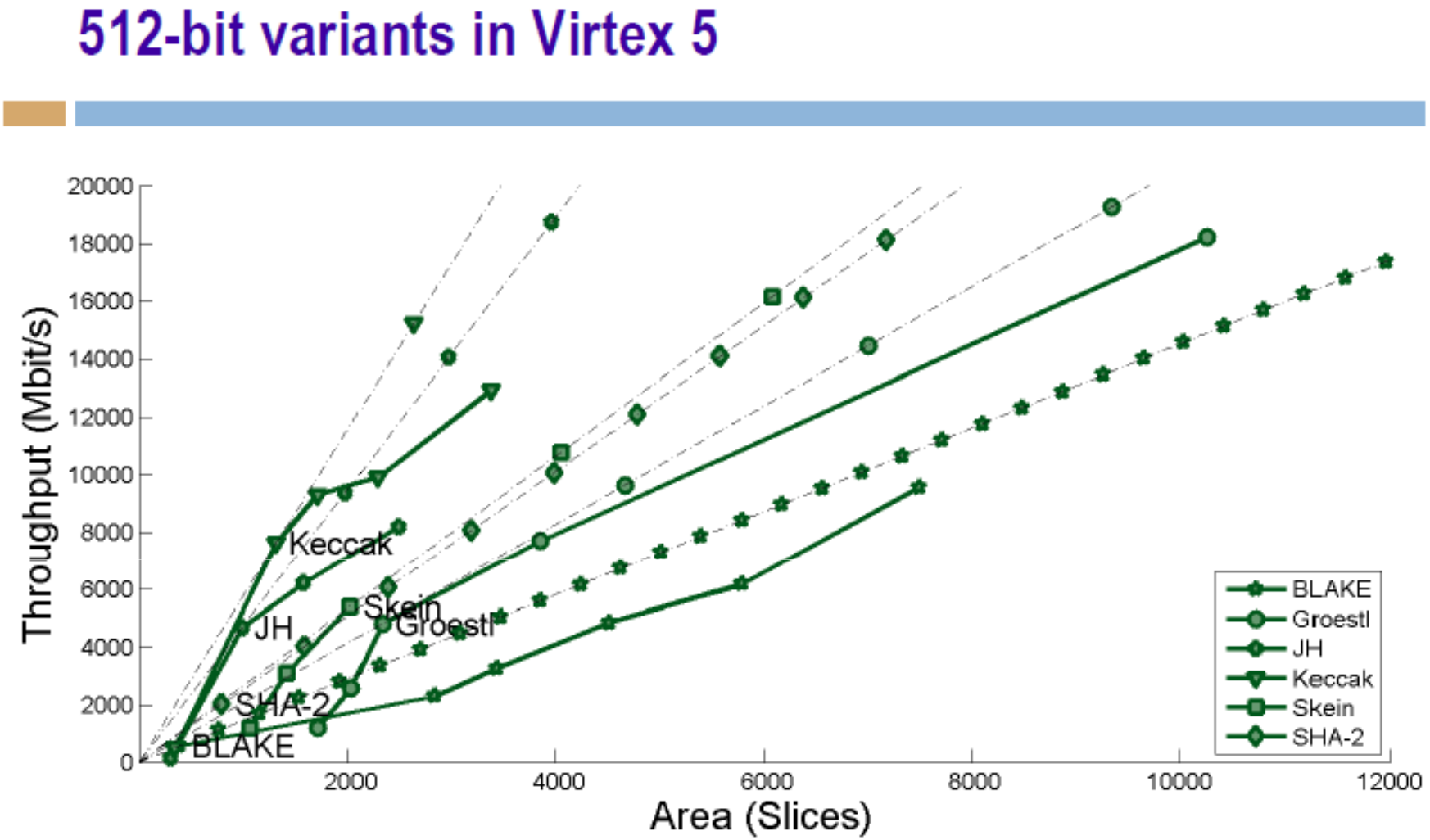
(Bernstein, Lange, the 3rd SHA-3 conference)



Efficient Implementation: Hardware
(Gaj, The 3rd SHA-3 Conference)



Efficient Implementation: Hardware
(Gaj, The 3rd SHA-3 Conference)



Efficient Implementation

- Flexible design
  - If we need a light-weight hash function
    - Just use the 6-dimensional array in JH
      - **4 times smaller than JH**
    - Achieve about 128-bit security for collision, preimage and second-preimage, no resistance against length-extension

      (if we need a light-weight hash function, we do not need 256-bit preimage resistance)

Conclusion

- JH can be analyzed easily against differential/truncated differential attack
- JH has large security margin against differential/truncated differential attacks
- JH fully benefits from SIMD instruction
- JH is very fast in hardware

Acknowledgements

- Thanks to NIST
  - It is not that difficult to design a hash function today,
  - but it is difficult to select from 64 submissions
- Thanks to all the researchers
  - for implementing and analyzing JH
- Thanks to Prof Preneel
  - for the suggestion on round number

Q & A