Konkurs SHA3
Algorytm StreamHash

mgr inż. Michał Trojnara
Opiekun: prof. Zbigniew Kotulski

Plan prezentacji

- Informacje o konkursie SHA3
- Algorytm StreamHash
- Kryptoanaliza StreamHash

National Institute of Standards and Technology

http://csrc.nist.gov/groups/ST/hash/sha-3/

Konkurs SHA3 – wstęp (2006)

08	Second Cryptographic Hash Workshop: Assess current status, discuss hash function development strategy, and encourage further research.
4Q	Draft the preliminary minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions.

Konkurs SHA3 – rok 1 (2007)

1Q	Publish the preliminary minimum acceptability requirements, submission requirements, and evaluation criteria for public comments. Present the draft minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions at the RSA Conference and at FSE 2007.
4/27	Public comment period ends.
2Q	Resolve comments.
4Q	Finalize and publish the minimum acceptability requirements, submission requirements, and evaluation criteria for candidate hash functions. Request submissions for new hash functions.

Konkurs SHA3 – rok 2 (2008)

4Q	Submission deadline for new hash functions.

Konkurs SHA3 – rok 3 (2009)

2Q	Review submitted functions, and select candidates that meet basic submission requirements. Host the **First Hash Function Candidate Conference** to announce first round candidates. Submitters present their functions at the workshop. Call for public comments on the first round candidates.

Konkurs SHA3 – rok 4 (2010)

2Q	Public comment period ends. Note: Depending on the number and quality of the submissions, NIST may either extend the length of the initial public comment period to allow sufficient time for the public analysis of the candidate algorithms, or may include additional rounds of analysis in order to successively reduce the number of candidate algorithms for further consideration as finalist algorithms. In these cases, NIST may host multiple workshops to discuss analysis results on candidate algorithms until it is ready to select the finalists. Note that subsequent dates in the timeline assume that the initial comment period will not be extended or additional rounds will not be required.
2Q	Hold the **Second Hash Function Candidate Conference**. Discuss the analysis results on the submitted candidates. Submitters may identify possible improvements for their algorithms.
3Q	Address the public comments on the submitted candidates; select the finalists. Prepare a report to explain the selection. Announce the finalists. Publish the selection report.
4Q	Submitters of the finalist candidates announce any tweaks to their submissions. Final round begins.

Konkurs SHA3 – rok 5 (2011)

4Q	Public comment period ends for the final round.

Konkurs SHA3 – rok 6 (2012)

1Q	Host the **Final Hash Function Candidate Conference**. Submitters of the finalist algorithms discuss the comments on their submissions.
2Q	Address public comments, and select the winner. Prepare a report to describe the final selection(s). Announce the new hash function(s).
3Q	Draft the revised hash standard. Publish the draft standard for public comments.
4Q	Public comment period ends. Address public comments. Send the proposed standard to the Secretary of Commerce for signature.

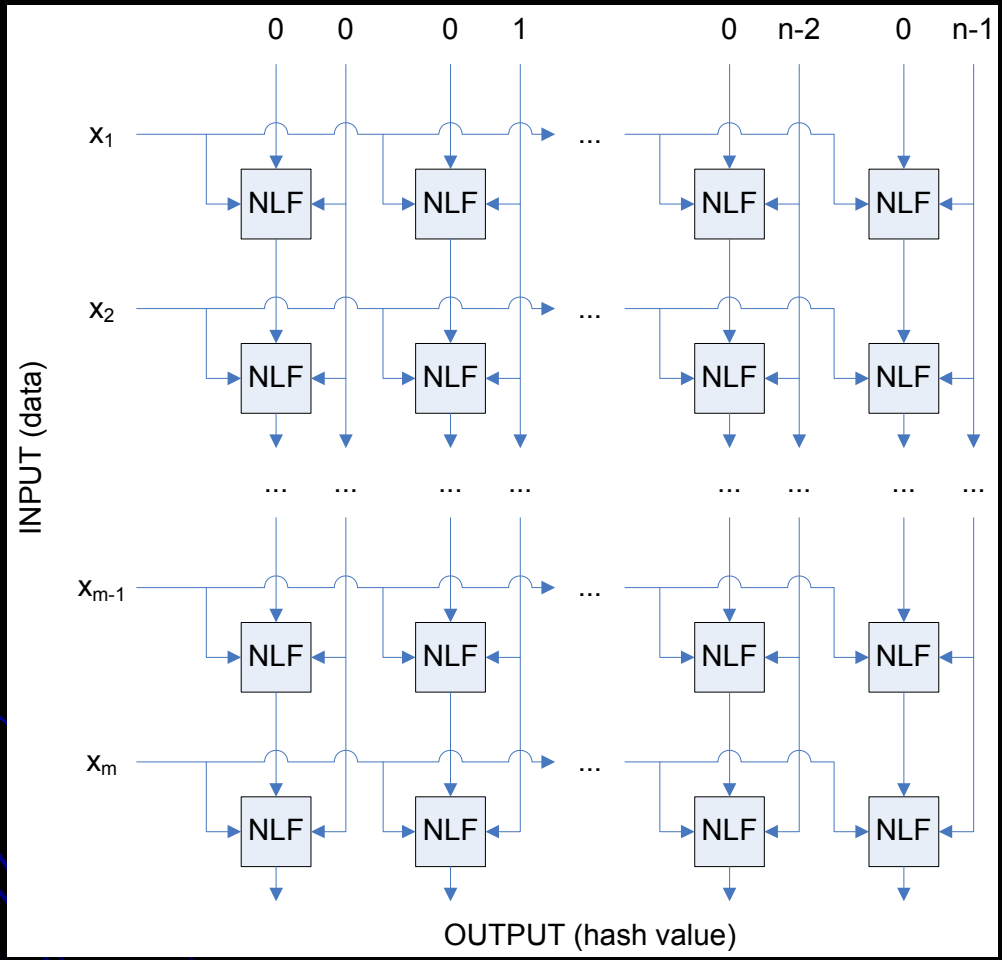
Konkurs SHA3 - wymagania

- Odporność na ataki
  - Collision Finding Attack
  - First Preimage Finding Attack
  - Second Preimage Finding Attack
  - Length Extension Attack
  - Multicollision Attack

Konkurs SHA3 - kandydatury

- Statystyka
  - 64 zgłoszenia wpłynęły do NIST
  - 51 z nich przyjętych do 1 rundy
  - 8 z nich zostało złamanych i wycofanych
- Przykładowe zgłoszenia
  - CubeHash - D. J. Bernstein
  - MD6 - Ronald L. Rivest
  - Skein - Bruce Schneier

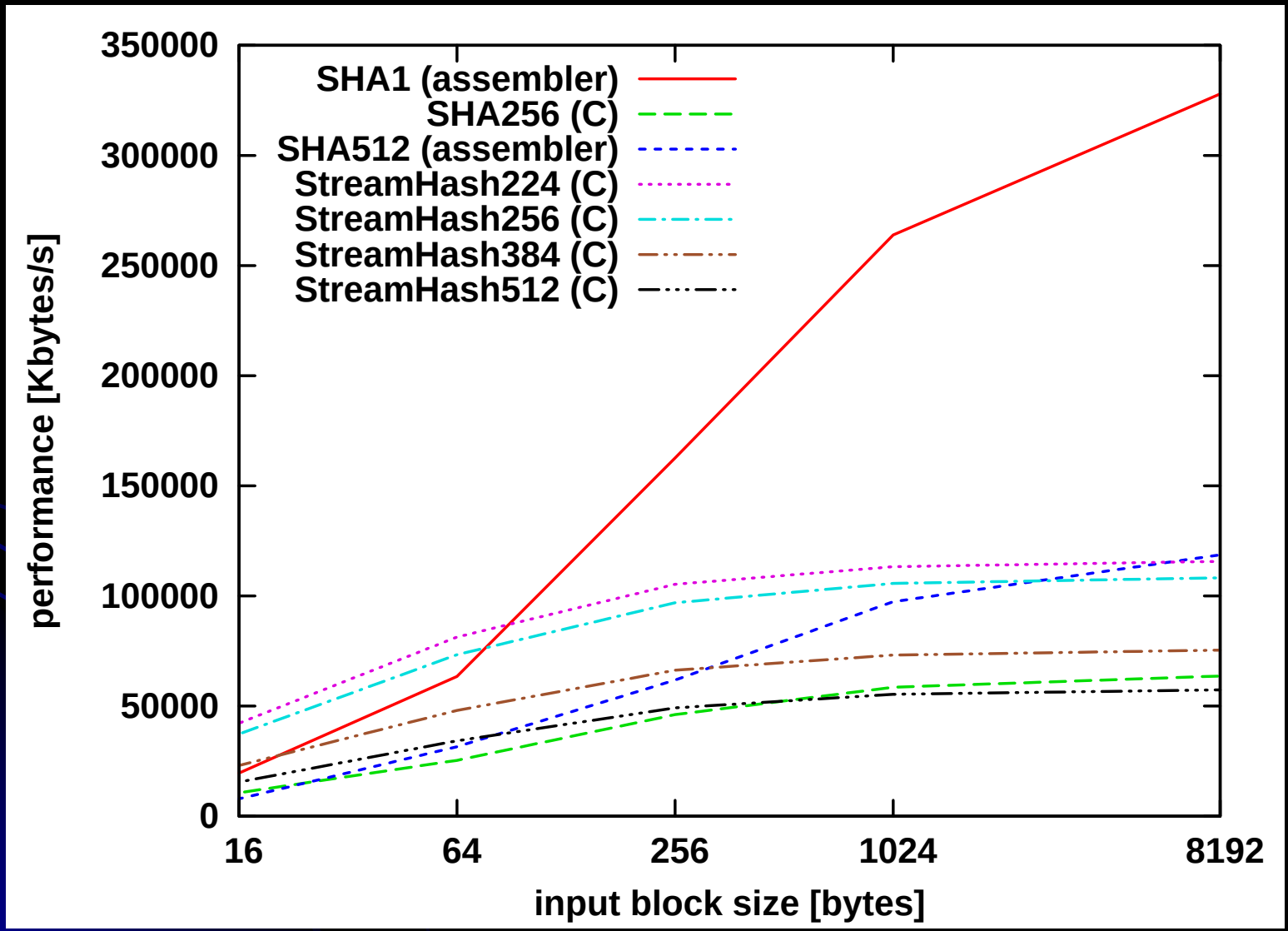
StreamHash - struktura



StreamHash - NLF

$$state_i := state_i \oplus S\text{-}BOX[LSB(state_i) \oplus b \oplus i]$$

StreamHash - wydajność



StreamHash - kryptoanaliza

- Dmitry Khovratovich, Ivica Nikolić (University of Luxembourg) „Cryptanalysis of StreamHash”
  `http://lj.streamclub.ru/papers/hash/streamhash.pdf`
- Tor E. Bjørstad (University of Bergen, Norway) „Collision for StreamHash”
  `http://ehash.iaik.tugraz.at/uploads/7/7b/Streamhash.txt`

Dziękuję za uwagę