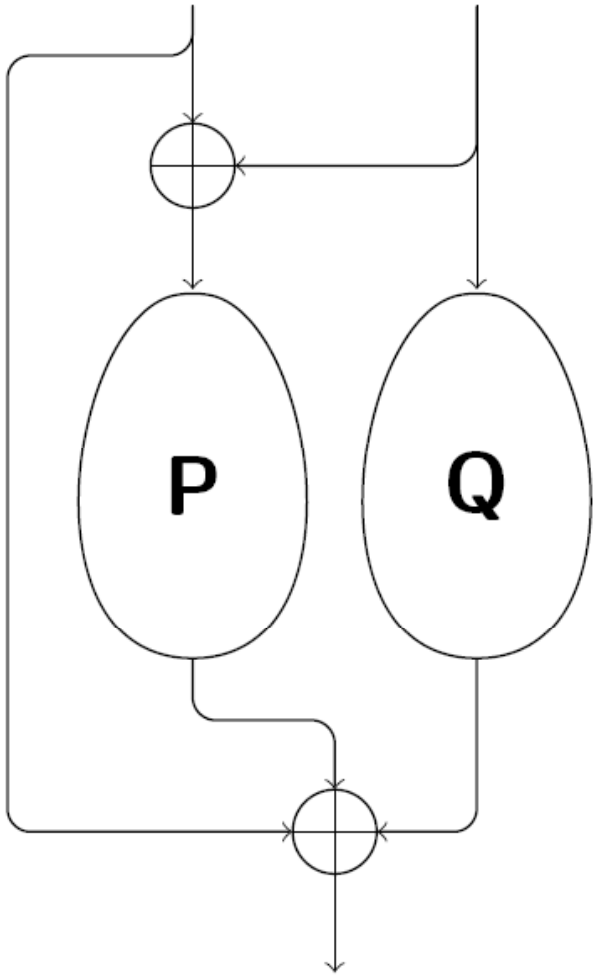
Grøstl Update



How to get assurance of security for a new primitive?

- Cryptanalysis
- Cryptanalysis
- Cryptanalysis

- Proofs save cryptanalysis time

Proofs for Grøstl

- Ideal-Permutation model
  - Optimal preimage, 2^{nd}-preimage, and collision security
  - Most of it available since 2008

- Standard model
  - **Good** bounds against classes of differential attacks
  - Available since 2008

Intensive Cryptanalysis as Assurance

Lots of external cryptanalysis, thanks to

- Paulo Barreto
- Christina Boura
- Anne Canteaut
- Christophe De Canniere
- Le Dong
- Sareh Emami
- Dengguo Feng
- Henri Gilbert
- Jian Guo
- Kota Ideguchi
- Jeremy Jean
- John Kelsey
- Dmitry Khovratovich
- Gaetan Leurent
- Yang Li
- Kazuo Ohta
- Maria Naya-Plasencia
- Thomas Peyrin
- Josef Pieprzyk
- Bart Preneel
- Vincent Rijmen
- Kazuo Sakiyama
- Yu Sasaki
- Ron Steinfeld
- Elmar Tischhauser
- Lei Wang
- Shuang Wu
- Wenling Wu
- Zian Zou

Cryptanalysis and Tweak

- Internal differential attacks [Peyrin10] and improvements [IdeguchiTischhauserPreneel10, Naya-Plasencia11] ruled out

- **All other attack vectors**
  - Rebound, SuperSbox and similar attacks on reduced hash function [Mendel+10, Leurent10], compression function [Mendel+09, Mendel+09b], and non-randomness properties [Lamberger+09, GilbertPeyrin10,Sasaki+10]
  - Zero-sum distinguishers [Boura+11]

  remain valid or are redone in [Schlaeffer10]
- **New cryptanalysis**
  - Improved rebound [JeanNayaPeyrin12]
  - Meet-in-the-middle [Wu+12]
  - Chosen-Multitarget-Preimage [Emami+12]
  - Biclique [Khovratovich12]

  is independent of the tweak or applies to earlier versions only

Improved rebound by [JeanNayaPeyrin12]

Improves upon a relevant cryptanalytic sub-problem that is **open for almost 3 years** and was tackled by several groups during this time

Best paper FSE 2012

Grøstl-256 (128-bit collision security)

year	#rounds	complexity	better than generic, if…
2009-2010	8 rounds	2^64	dimension of subspace of allowable differences is 64
2012	9 rounds	2^368	not allowing birthday effect for most bits in the generic case

Security margin illustrated

- 9 rounds differential permutation distinguisher (banana)

- 6 rounds compression function collision
- 3 rounds hash function collision

Large, well understood security margin

Simplicity helped a lot

Attacks on up to 5 rounds may be possible

Implementations

Performance on high-end CPUs

- Current Intel architectures: <10 cycles per byte
  - using AES-NI
  - faster than SHA-256, same as SHA-512
- Upcoming AVX2 will provide speed-up for vperm, table-based, and AES-NI implementations

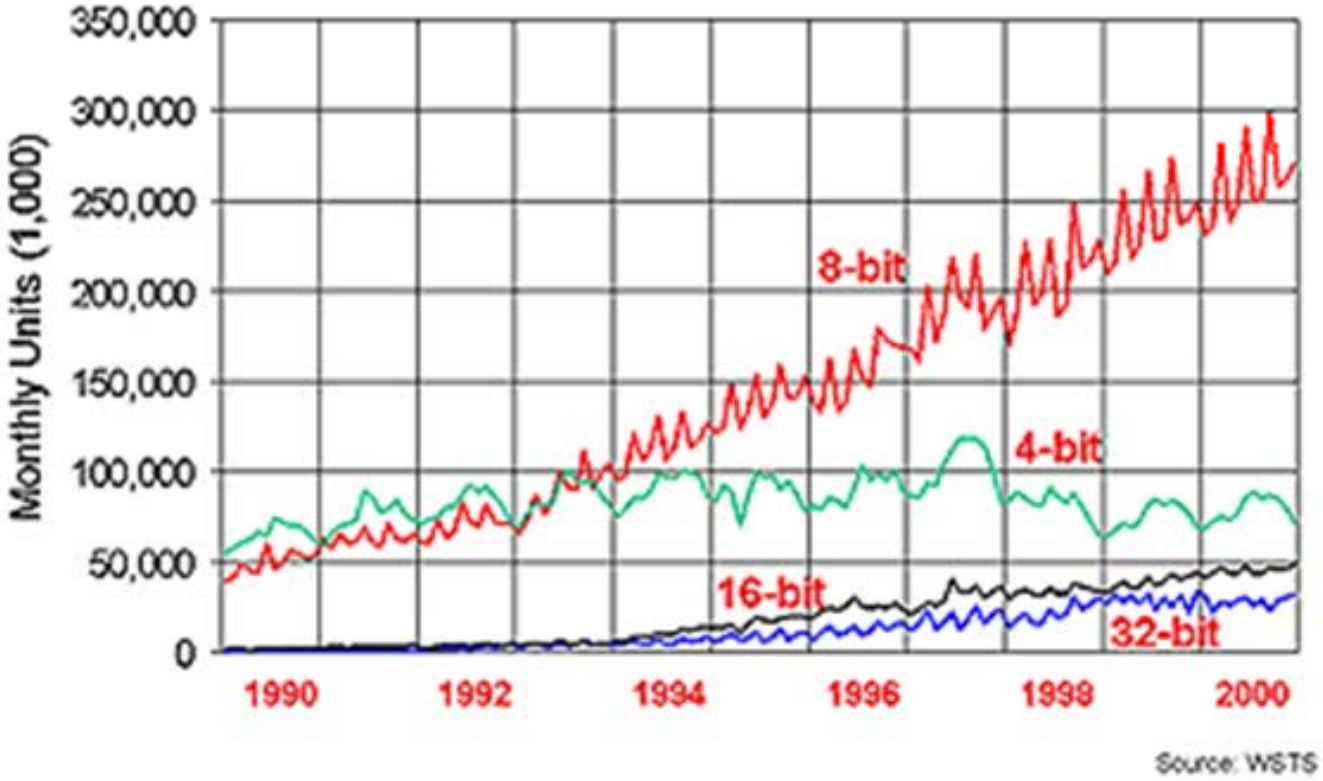
Parallelizability

- Tree-mode can benefit Grøstl-256 and Groestl-512.

- In contrast to SHA-2 we don’t need tree-mode to take advantage of AVX-2

8-bit Platform

55% of the CPU market is 8-bit CPUs [S06]



8-bit Platform

Recent improvements put Grøstl ahead of all other finalists and SHA-2 (ebash and XBX)

- ATMega platform (chosen by XBX team)
- Fastest (starting from 447 cycles/byte)
- Lowest ROM (starting from 1406 bytes)
- Lowest RAM consumption (starting from 192 bytes)

Instruction Set Extensions

- Under-researched
- Grøstl clearly benefits from existing AES ISE
- [Constantin+12] concludes that Grøstl gains the most

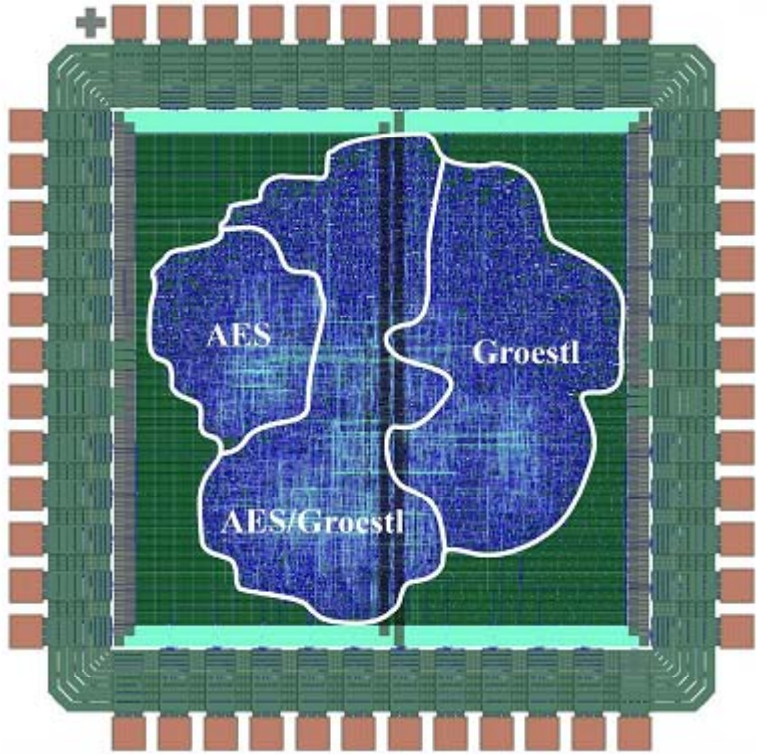
Hardware Implementations

- High-speed ASICs
  - High speed: Position 2, other metrics: 3-5
- High-speed FPGAs
  - High speed: Position 2, other metrics: 2-4
- Low-cost ASICs
  - Smallest [KavunYalcin12]
  - Best throughput/area ratio [KavunYalcin12]
- Low-cost FPGAs
  - Always position 1 [Junk12]
  - Position 1-2 [Kaps+11], [Kerkhof+11]

Resource reuse with AES

- Useful in constrained environments

- Example: Low-cost ASIC
- AES alone 3.5kGates
- With smallest Grøstl, AES overhead is less than 1.5kGates[C12]



Side-channel attacks

Software: Constant-time implementations are often the fastest way to implement Grøstl (vperm, AES-NI). In other cases, bit-sliced implementation strategies are available

Hardware cost of countermeasures:

- Research on this for SHA-2 and SHA-3 is still in its infancy
- Largely unpublished experience in industry (e.g. Gemalto, Infineon) suggests strong dislike of SHA-2
- Large body of work on attacks on AES and countermeasures is of great benefit for Grøestl

Conclusion

Unique features of Grøstl

(1) Highest assurance through early proofs, bounds, and cryptanalysis

(2) Large, well understood security margin

(2) Fastest, and smallest (both ROM and RAM) in 8-bit CPUs

(3) Faster than SHA-2 on high end CPUs, AND top in several hardware categories

(4) Various resource reuses with AES (HW,SW)

(5) Cost of side-channel countermeasures potential selling factor for SHA-3

References

[Constantin+12] Jeremy Constantin, Andreas Burg, and Frank K. Gurkaynak. Investigating the Potential of Custom Instruction Set Extensions for SHA-3 Candidates on a 16-bit Microcontroller Architecture. Cryptology ePrint Archive, Report 2012/050, 2012.

[C12] Putting together what fits together – GrAEStl, material and data used with permission from authors

[S06] Semico Research Corporation, 2006

For all other references on cryptanalysis and implementation, please refer to OFFICIAL COMMENT: Grostl (Round 3): “Update on Finalist Groestl” from March 20, 2012

Grøstl Update