Really fast syndrome-based hashing

D. J. Bernstein
University of Illinois at Chicago

Joint work with:

Tanja Lange
Technische Universiteit Eindhoven

Christiane Peters
Technische Universiteit Eindhoven

Peter Schwabe
Academia Sinica

Remember FSB?
SHA-3 submission by Augot–Finiasz–Gaborit–Manuel–Sendrier.
FSB compression function
(plus Whirlpool output filter).

Simple compression function.
Well-understood attack ideas:
information-set decoding,
linearization, Wagner.
FSB-256 seems quite secure.

Bad: Not actually fast.
Schwabe asm, Core 2 Q9550,
FSB-256: 95.53 cycles/byte.

What we've done:
RFSB compression function.

Our asm, Core 2 Q9550,
RFSB-509: 13.62 cycles/byte.
Faster than SHA-256;
faster than JH;
faster than Grøstl.
Plus extra speed features:
incremental hashing,
fast batch verification.

Cost $> 2^{128}$ for all known
collision attacks on RFSB-509.