SHARCS vs. SWIFFT

D. J. Bernstein
University of Illinois at Chicago

Thanks to: NSF ITR–0716498

EUROCRYPT '97,

Bellare–Micciancio: Compress $(m_1, m_2, \ldots, m_{16})$ to B-bit output $f_1(m_1) + f_2(m_2) + \cdots + f_{16}(m_{16})$.

FSE 2008, yesterday, Lyubashevsky–Micciancio–Peikert–Rosen: "SWIFFT"; "provable security"; $B = 512$;
fastest known collision attack
"takes time at least 2^{106}
and requires almost as much space."

SHARCS 2007, Bernstein:
time $2^{B/13} \approx 2^{40}$
using circuit of size $2^{2B/13} \approx 2^{80}$.

Or time $2^{B/7}$, circuit size $2^{B/7}$.
Many other tradeoffs possible.

cr.yp.to/papers.html#genbday

Also some analysis of constants:

cr.yp.to/papers.html#expandxor

SHARCS talk also mentioned idea—

not written up yet—

to achieve slightly better exponents:

e.g., time $2^{2B/15}$, size $2^{2B/15}$.