ChaCha20

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498

Review of Salsa20

4 modifications per quarter-round:

```
x4 ^= (x0+x12) <<< 7
x8 ^= (x4+x0) <<< 9
x12 ^= (x8+x4) <<< 13
x0 ^= (x12+x8) <<< 18
```

16 modifications per round.
128 modifications in Salsa20/8.
320 modifications in Salsa20/20.

Key words kept separate? No!
("I also see each use of a k word as a missed opportunity to spread changes through the n words.")
Constants kept separate? No!

ChaCha20 and Cha20

Salsa20 temporarily allocates separate word for storing sum. Missed diffusion opportunity!

ChaCha20 takes this opportunity:

```
x0+=x12; x4^=x0; x4<<<=16
x8+=x4; x12^=x8; x12<<<=12
x0+=x12; x4^=x0; x4<<<=8
x8+=x4; x12^=x8; x12<<<=7
```

Cha20: like ChaCha20 but transposes twice as often. Easier to analyze trail width?