ChaCha20

D. J. Bernstein
University of Illinois at Chicago

NSF ITR–0716498
Review of Salsa20

4 modifications per quarter-round:
\[ x_4 \oplus= (x_0+x_{12}) \ll 7 \]
\[ x_8 \oplus= (x_4+x_0) \ll 9 \]
\[ x_{12} \oplus= (x_8+x_4) \ll 13 \]
\[ x_0 \oplus= (x_{12}+x_8) \ll 18 \]

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:
\[
\begin{align*}
x_0 &= x_{12}; \\
x_4 &= x_0; \\
x_4 &= x_4 \ll \ll 16
\end{align*}
\]
\[
\begin{align*}
x_8 &= x_4; \\
x_{12} &= x_8; \\
x_{12} &= x_{12} \ll \ll 12
\end{align*}
\]
\[
\begin{align*}
x_0 &= x_{12}; \\
x_4 &= x_0; \\
x_4 &= x_4 \ll \ll 8
\end{align*}
\]
\[
\begin{align*}
x_8 &= x_4; \\
x_{12} &= x_8; \\
x_{12} &= x_{12} \ll \ll 7
\end{align*}
\]

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