# ChaCha 20

Seed : 256 bits (8 chunks of 32-bits)

Constants: 128 bits (4 chunks)

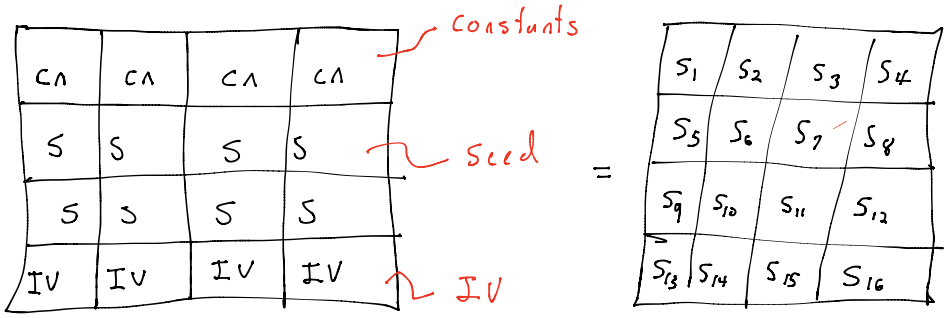
IV: nonce / counter: 128 bits (4 chunks)

- counter → stop and pick up later
- nonce → Encrypt same message twice, diff c

$$PRG(seed, IV) = k$$

$$Enc(m, k) = m \oplus k = c$$

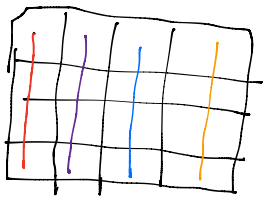
PRG:



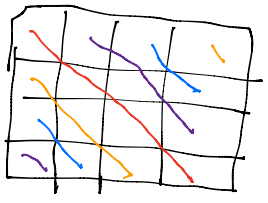

Let R be round function. It does the following 20 times (the "20" in chacha20)

$\times 20$

$R(s_1, s_5, s_9, s_{13})$ —
$R(s_2, s_6, s_{10}, s_{14})$ —
$R(s_3, s_7, s_{11}, s_{15})$ —
$R(s_4, s_8, s_{12}, s_{16})$ —



$R(s_1, s_6, s_{11}, s_{16})$ —
$R(s_2, s_7, s_{12}, s_{13})$ —
$R(s_3, s_8, s_9, s_{14})$ —
$R(s_4, s_5, s_{10}, s_{15})$ —



R is defined as follows:

R(a, b, c, d):

$a = a + b$
$d = d \oplus a$
$d = d \lll 16$
$c = c + d$
$b = b \oplus c$
$b = b \lll 12$
$a = a + b$
$d = a \oplus d$
$d = d \lll 8$
$c = c + d$
$b = b \oplus c$
$b = b \lll 7$

Output: current grid + previous grid.