Significantly Improved Multi-bit Differentials for Reduced Round Salsa and ChaCha

Arka Rai Choudhuri

Johns Hopkins University

USA

Subhamoy Maitra

Indian Statistical Institute

India

FSE 2017, Tokyo

Salsa and ChaCha

ARX based stream ciphers.

Designed by Dan Bernstein.

Salsa and ChaCha

ARX based stream ciphers.

Designed by Dan Bernstein.

Salsa accepted into the **eStream** software portfolio (2007).

Salsa and ChaCha

ARX based stream ciphers.

Designed by Dan Bernstein.

Salsa accepted into the **eStream** software portfolio (2007).

ChaCha designed to address some concerns about Salsa (2008).

Motivation

Motivation

Standardization process for inclusion of cipher suite based on ChaCha20-Poly1305 AEAD in **TLS1.3** is almost complete.

Motivation

Standardization process for inclusion of cipher suite based on ChaCha20-Poly1305 AEAD in **TLS1.3** is almost complete.

Existing cryptanalysis treats ciphers as **black-boxes**.

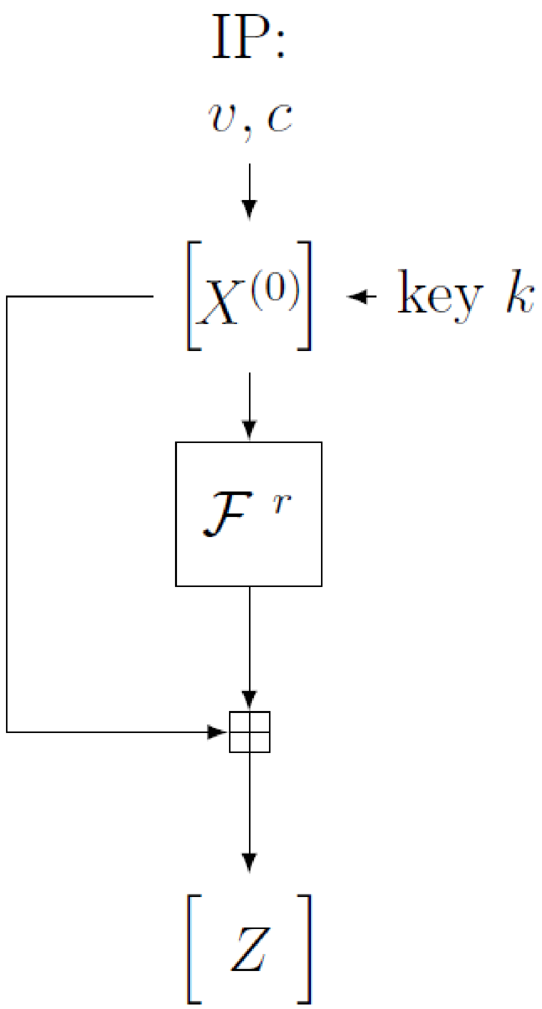
Motivation

Standardization process for inclusion of cipher suite based on ChaCha20-Poly1305 AEAD in **TLS1.3** is almost complete.

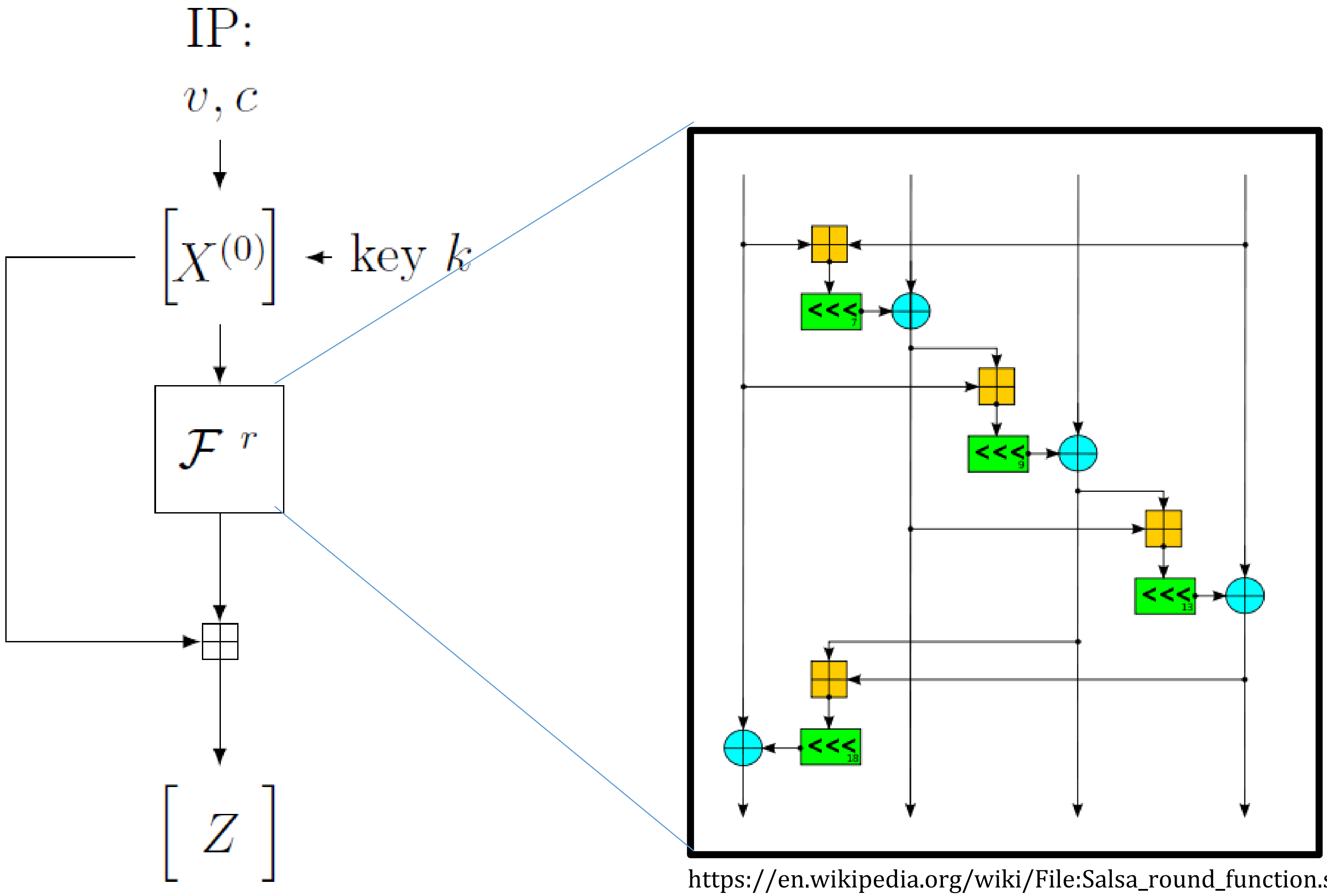
Existing cryptanalysis treats ciphers as **black-boxes**.

Brute force search for multiple components in cryptanalysis.

Structure



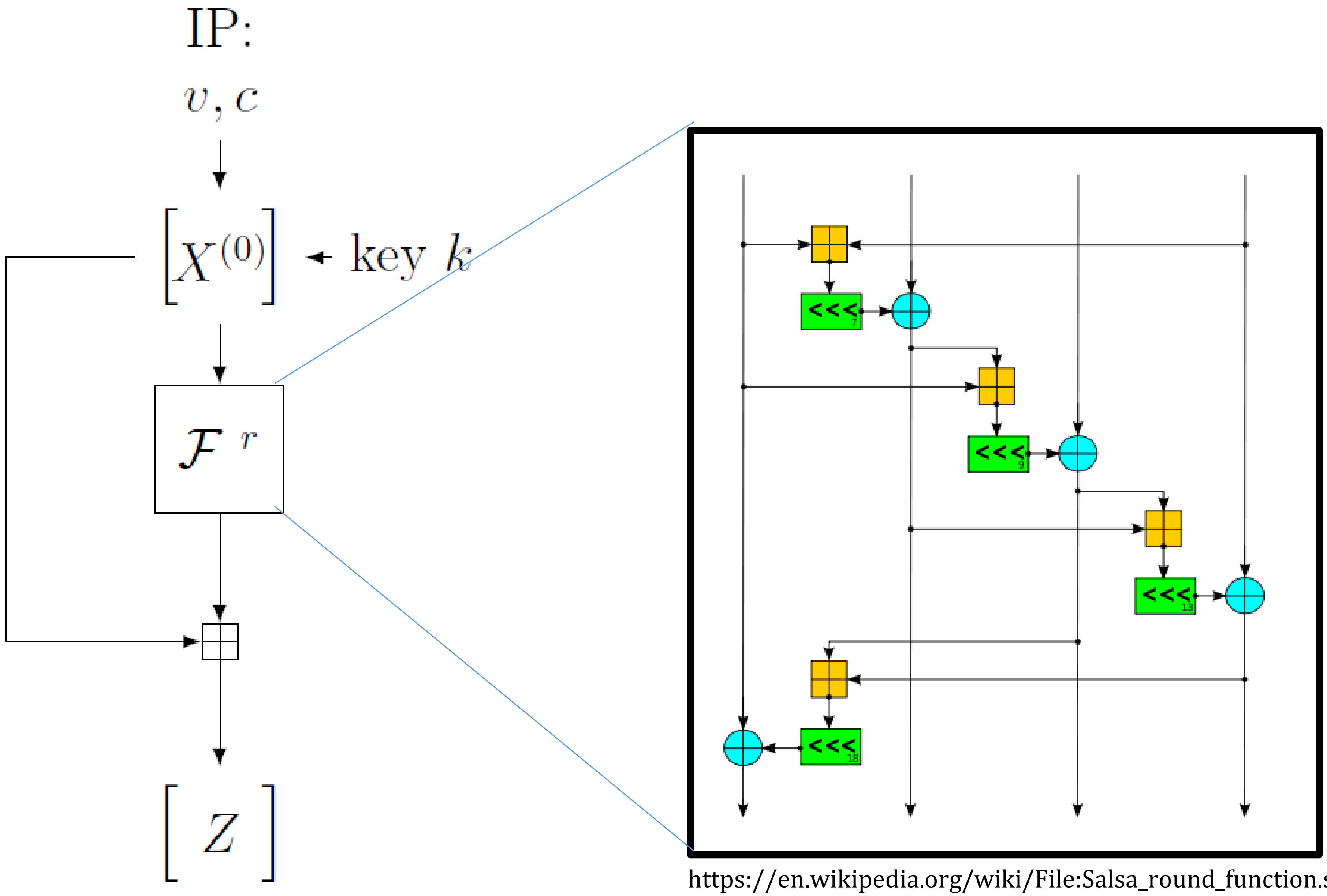
Structure



https://en.wikipedia.org/wiki/File:Salsa_round_function.svg

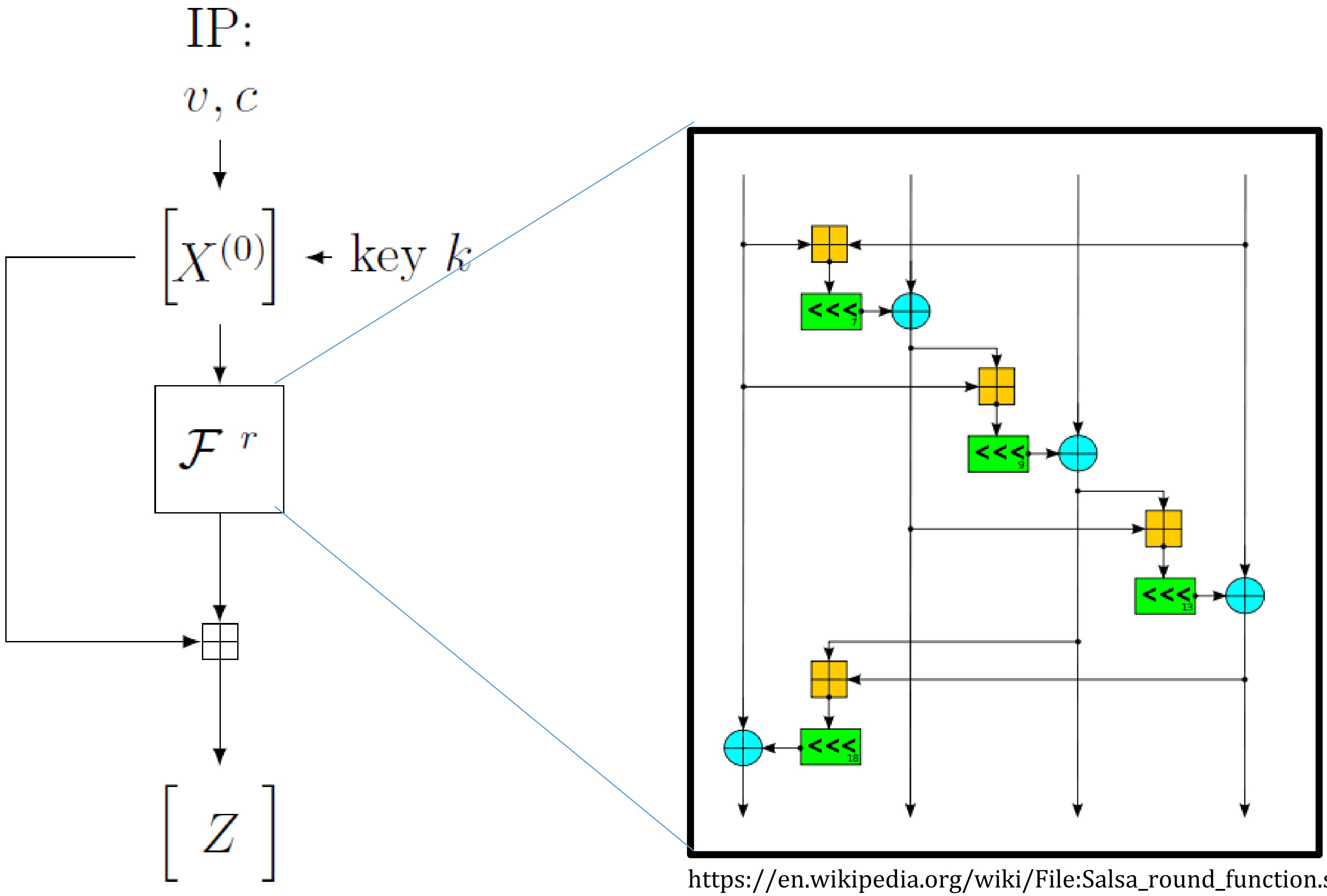
Structure

Easy to implement.



https://en.wikipedia.org/wiki/File:Salsa_round_function.svg

Structure

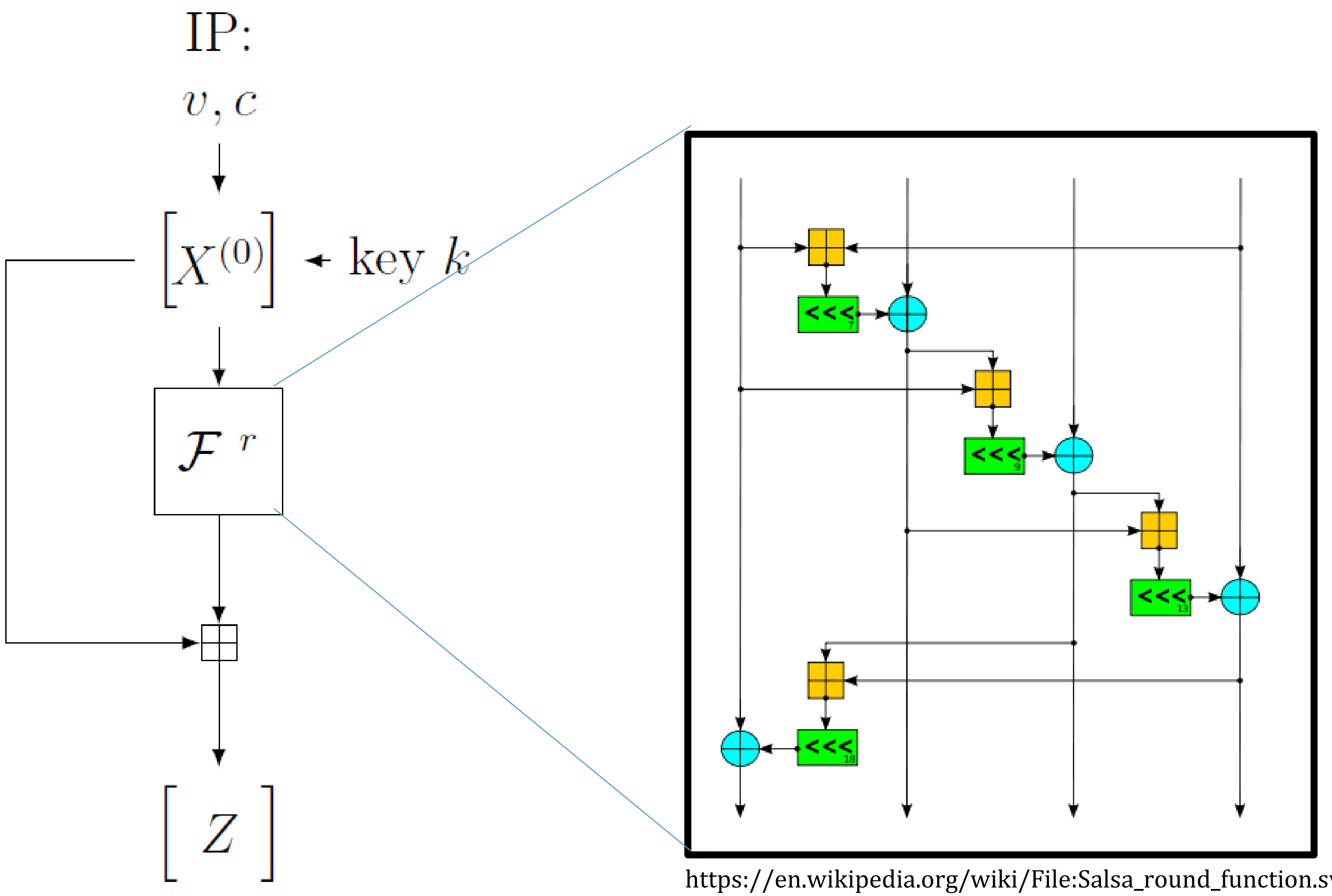


https://en.wikipedia.org/wiki/File:Salsa_round_function.svg

Easy to implement.

Fast on PCs.

Structure



https://en.wikipedia.org/wiki/File:Salsa_round_function.svg

Easy to implement.

Fast on PCs.

No security guarantees.

Non Randomness

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$$

$$\bigoplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$$

$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \longrightarrow \boxed{\mathrm{Salsa}^{\mathrm{r}}} \longrightarrow$$

$$\oplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \longrightarrow \boxed{\mathrm{Salsa}^{\mathrm{r}}} \longrightarrow$$

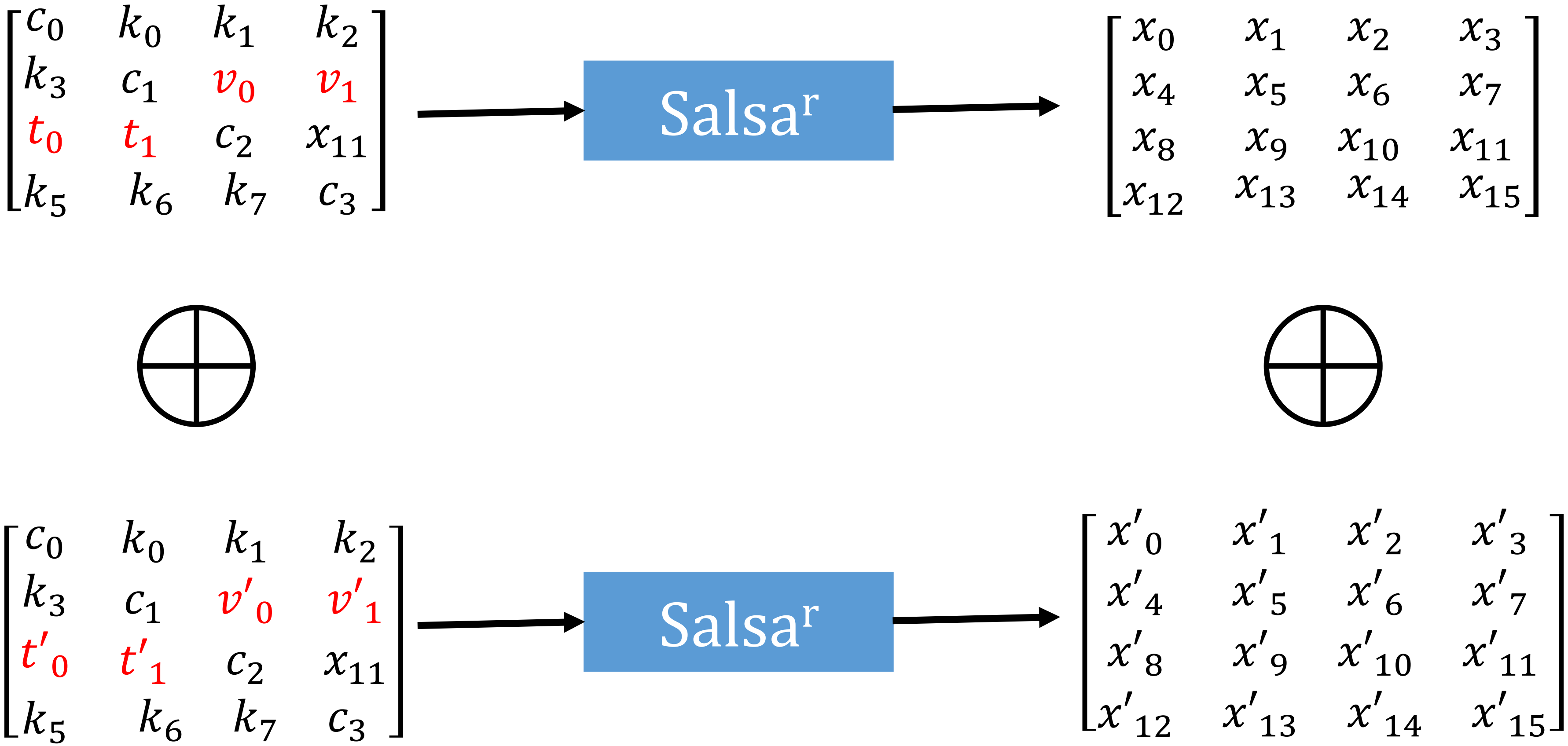
$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \longrightarrow \boxed{\mathrm{Salsa}^{\mathrm{r}}} \longrightarrow \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

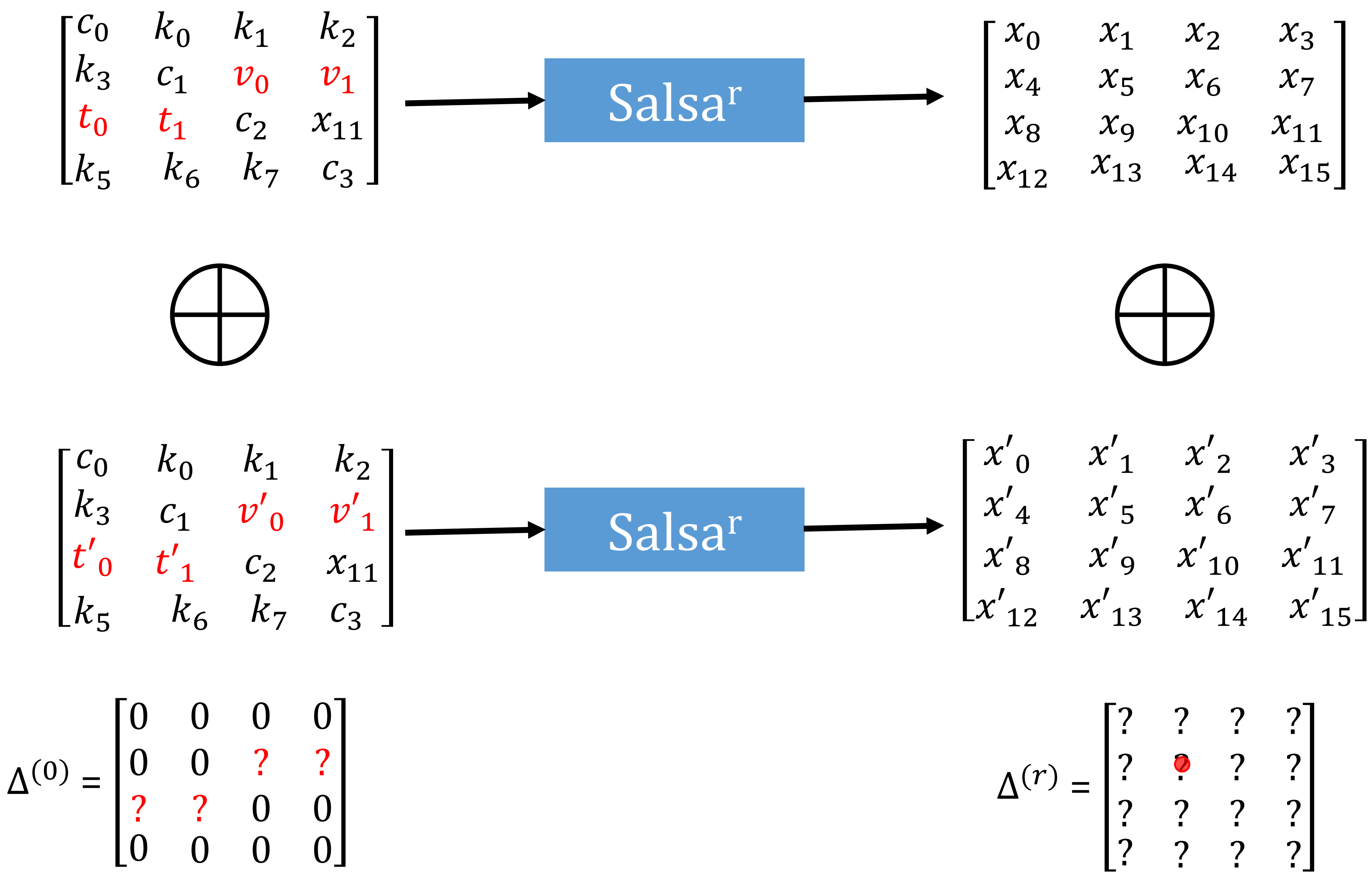
$$\bigoplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \longrightarrow \boxed{\mathrm{Salsa}^{\mathrm{r}}} \longrightarrow \begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$$

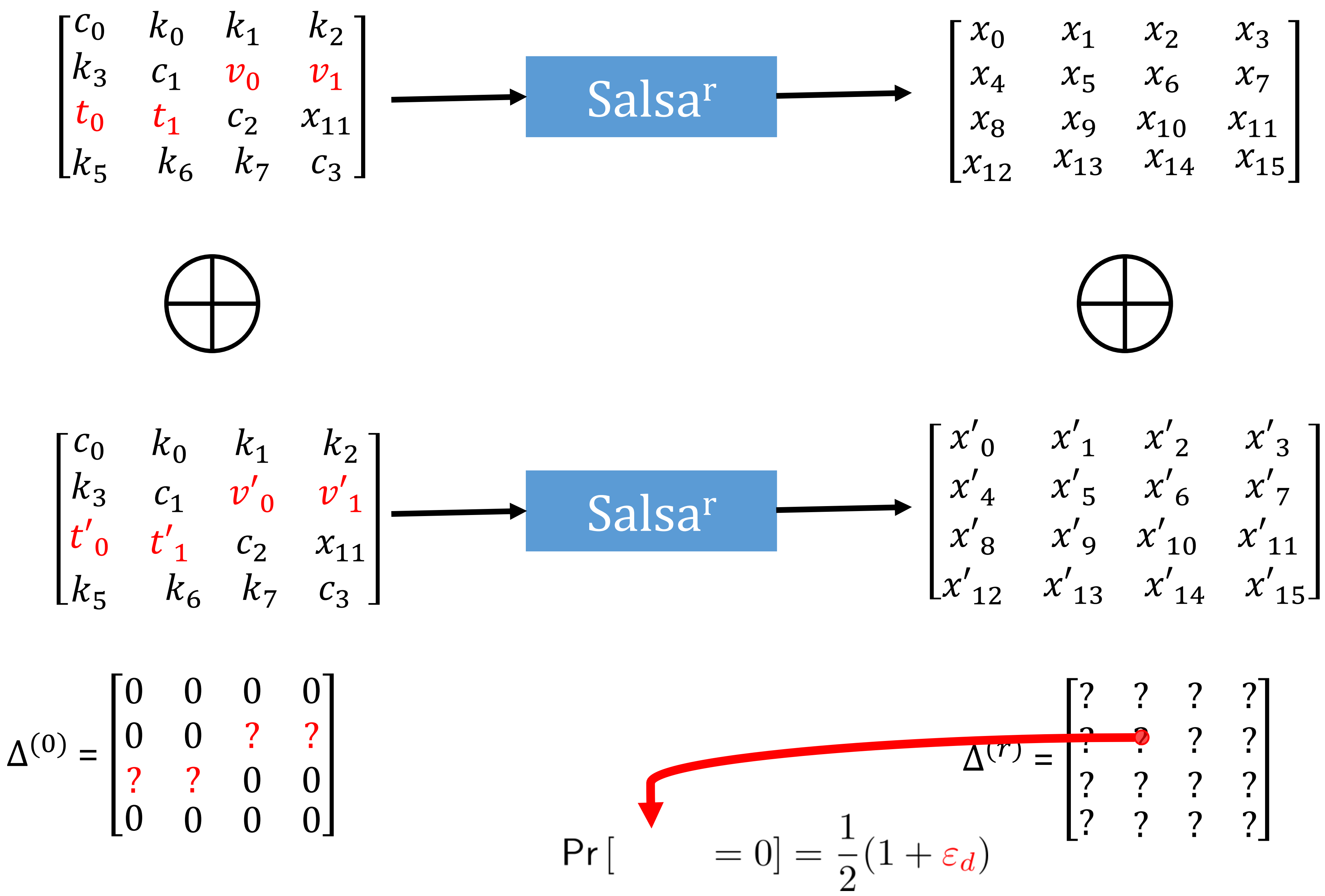
$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$



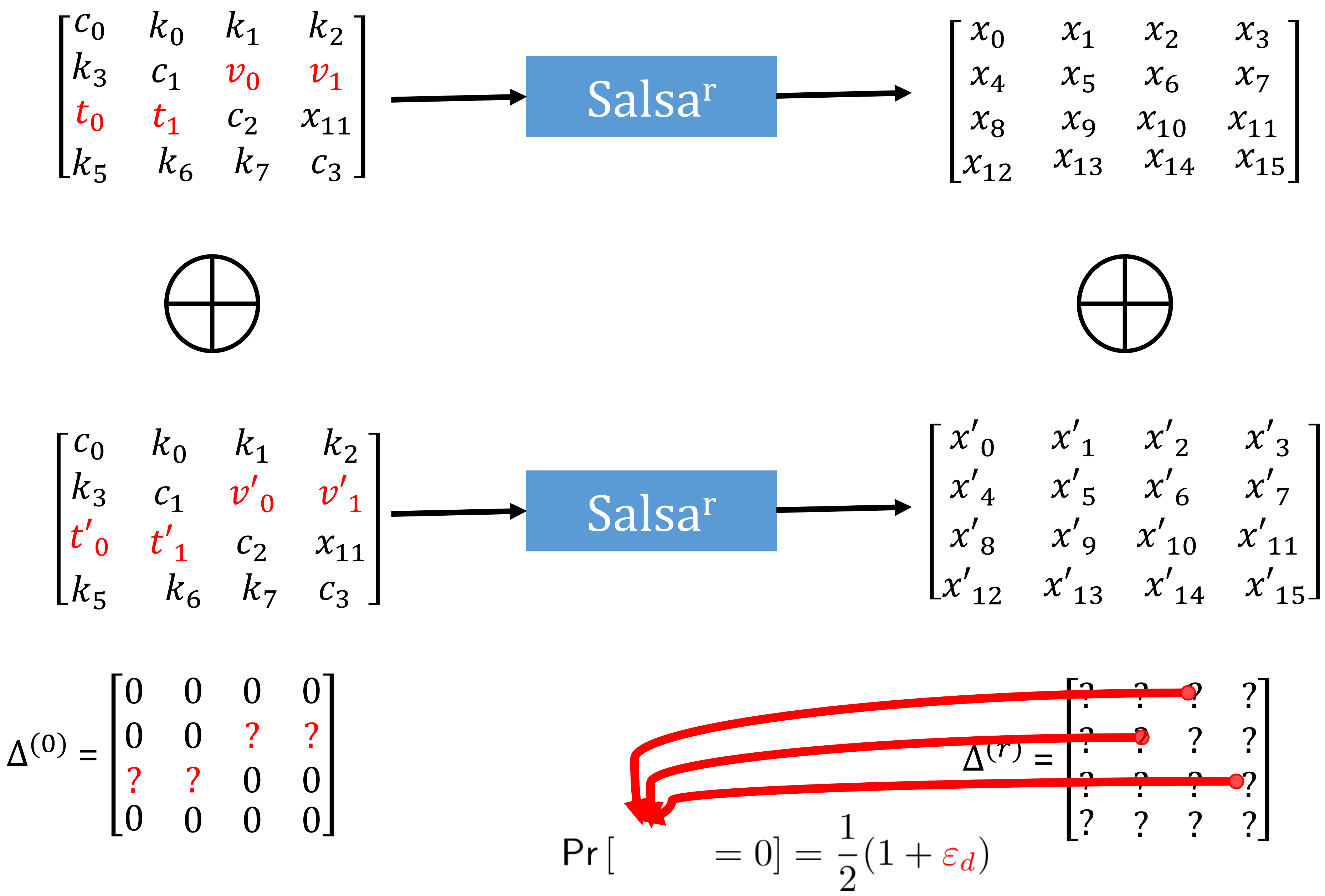
$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$



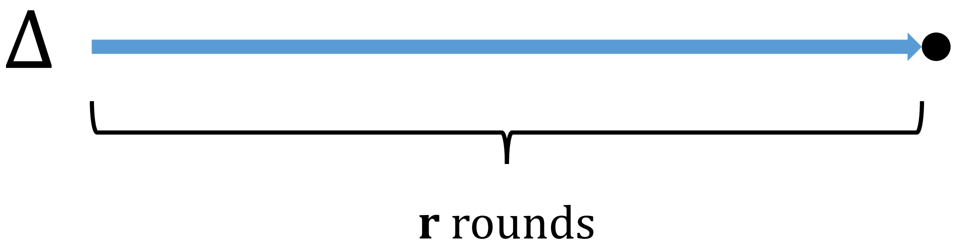
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
Salsa^r
$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$
$\oplus$
$\oplus$
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
Salsa^r
$\begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$
$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$\Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$



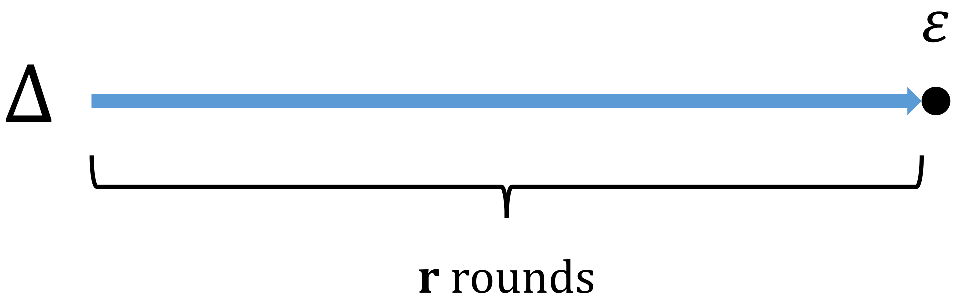
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
Salsa^r
$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$
$\bigoplus$
$\bigoplus$
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
Salsa^r
$\begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$
$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$\Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$
$\Pr[\quad = 0] = \frac{1}{2}(1 + \varepsilon_d)$


Salsa^r
Salsa^r
Δ^(0) =
Δ^(r) =
Pr[= 0] = 1/2 (1 + ε_d)

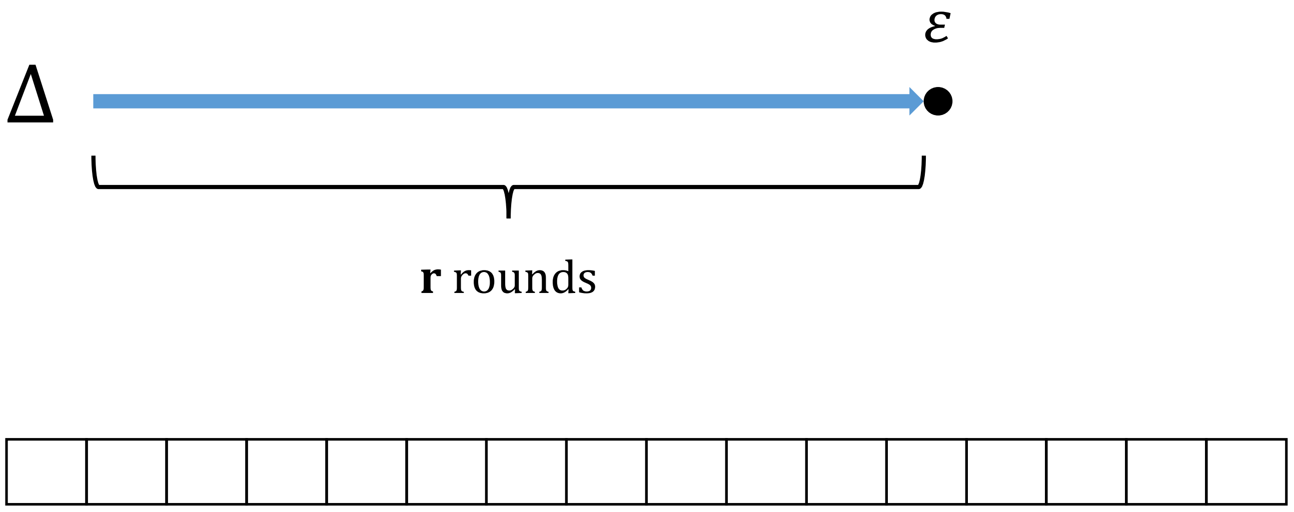
Attack idea (for **R** rounds) [Aumasson et al. 08]



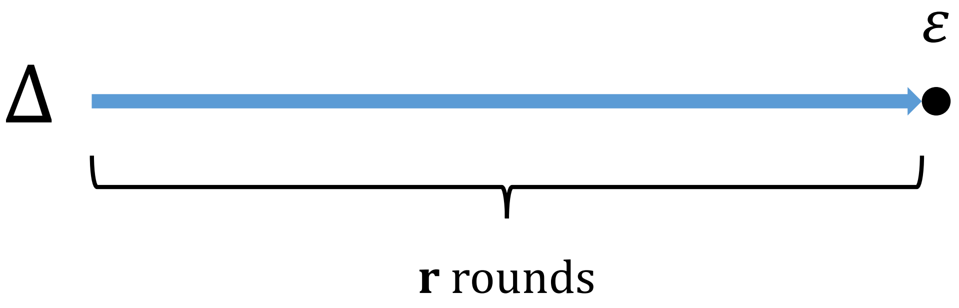
Attack idea (for **R** rounds) [Aumasson et al. 08]

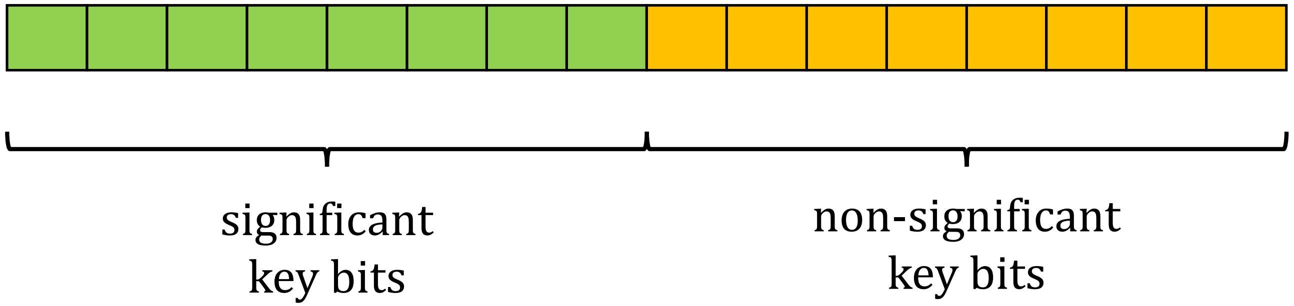


Attack idea (for **R** rounds) [Aumasson et al. 08]

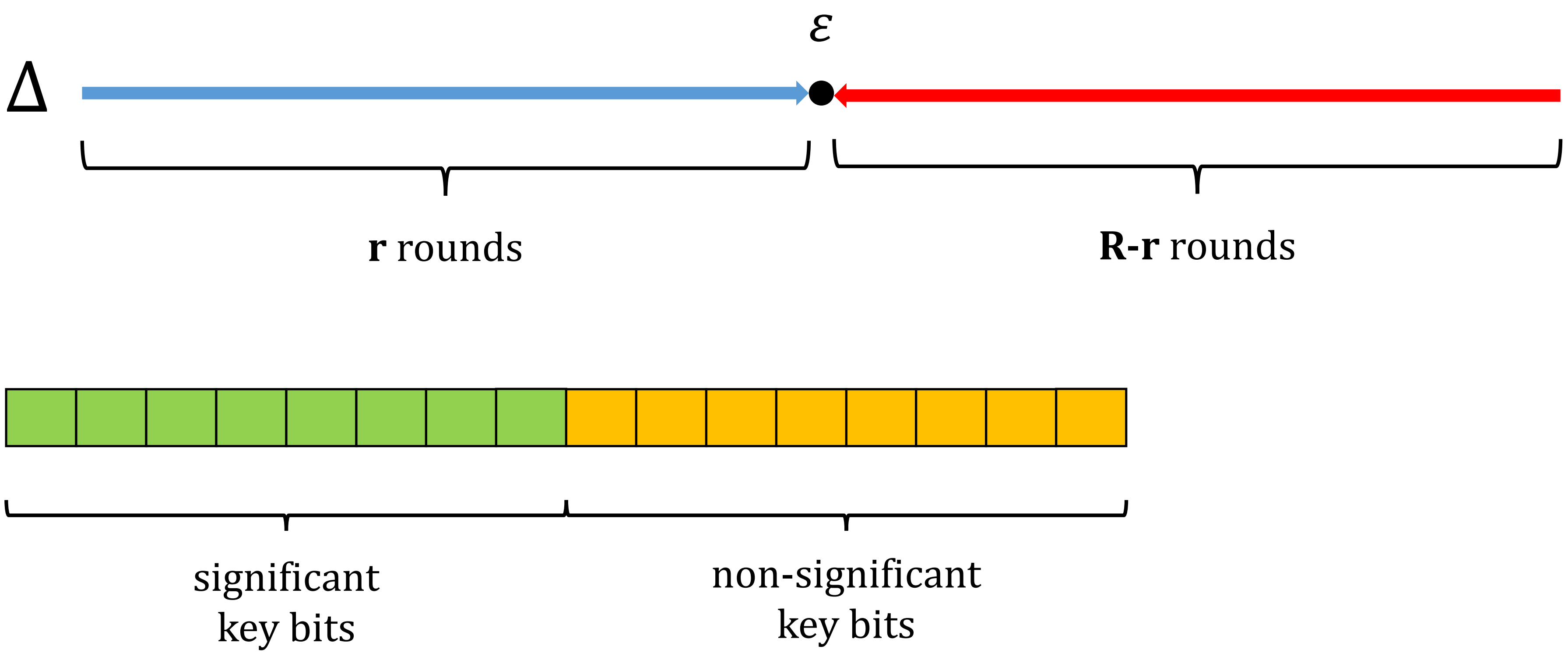


Attack idea (for **R** rounds) [Aumasson et al. 08]

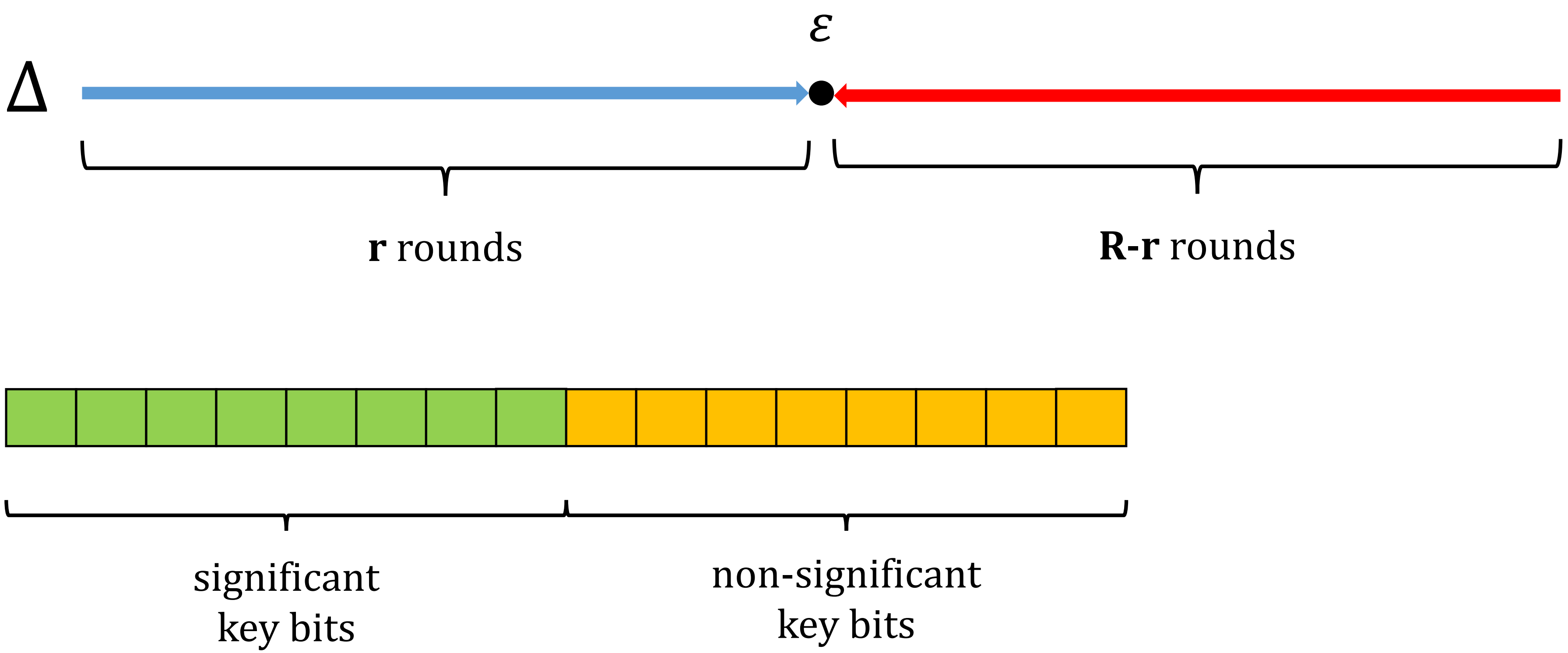




Attack idea (for **R** rounds) [Aumasson et al. 08]

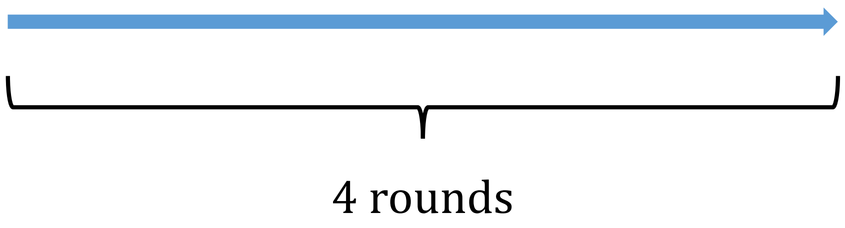


Attack idea (for **R** rounds) [Aumasson et al. 08]

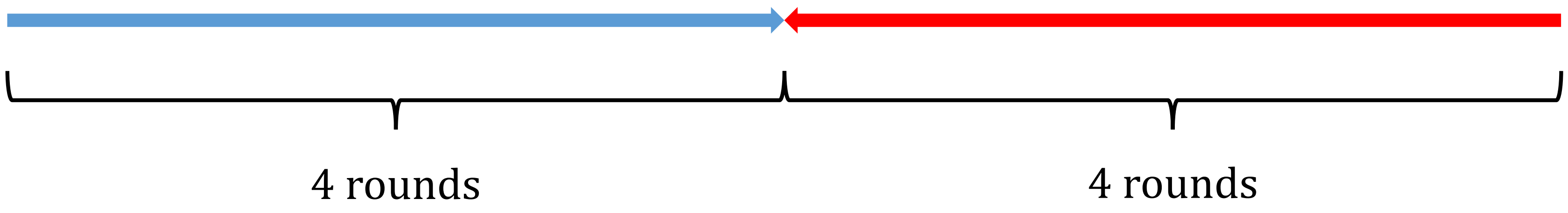


Complexity of attack **increases** with **increase** in number of significant bits.

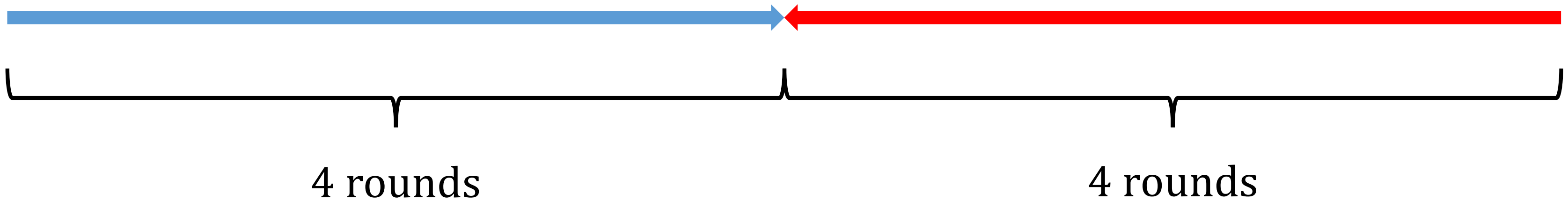
Salsa



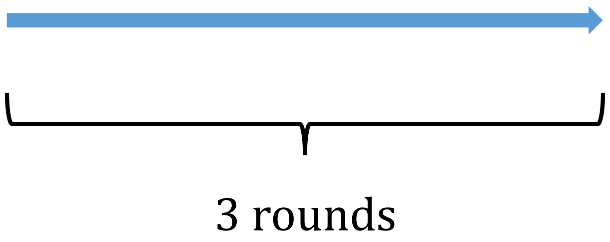
Salsa



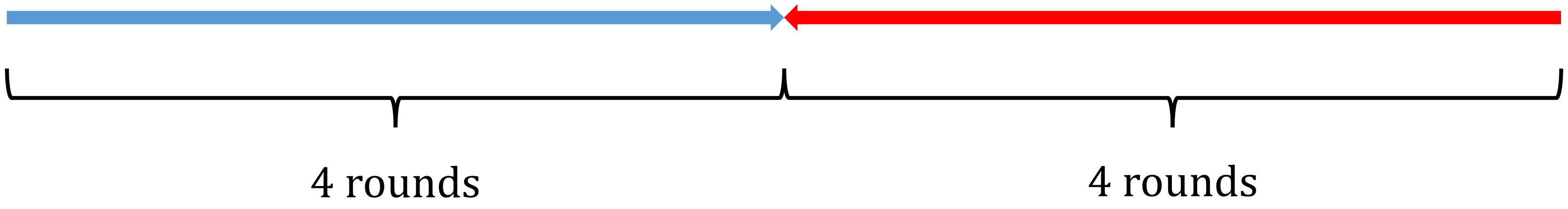
Salsa



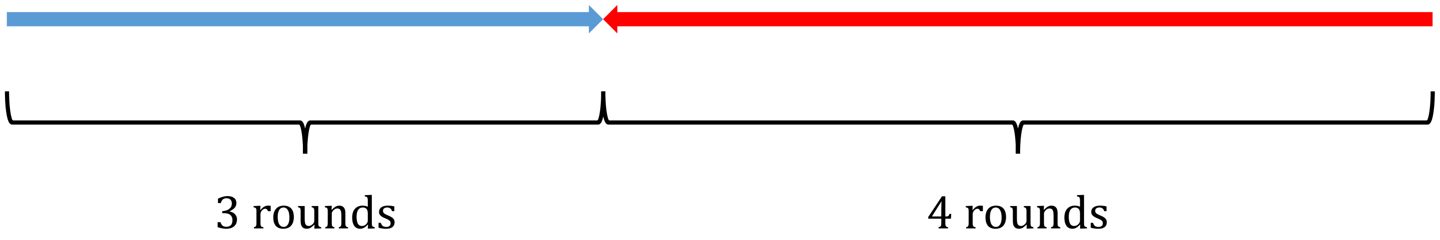
ChaCha



Salsa



ChaCha



Salsa update function

Salsa update function

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

Salsa update function

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

$$\left.\begin{aligned} b &= b \oplus ((a + d) \lll 7), \\ c &= c \oplus ((b + a) \lll 9), \\ d &= d \oplus ((c + b) \lll 13), \\ a &= a \oplus ((d + c) \lll 18). \end{aligned}\right\}$$

Salsa update function

$$\begin{bmatrix} a & x_1 & x_2 & x_3 \\ b & x_5 & x_6 & x_7 \\ c & x_9 & x_{10} & x_{11} \\ d & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

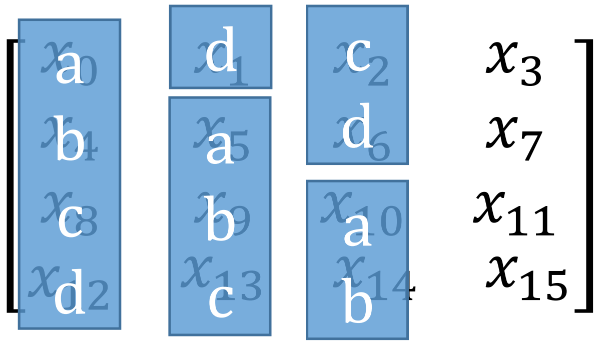
$$\left.\begin{array}{rcl} b & = & b \oplus ((a + d) \lll 7), \\ c & = & c \oplus ((b + a) \lll 9), \\ d & = & d \oplus ((c + b) \lll 13), \\ a & = & a \oplus ((d + c) \lll 18). \end{array}\right\}$$

Salsa update function

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

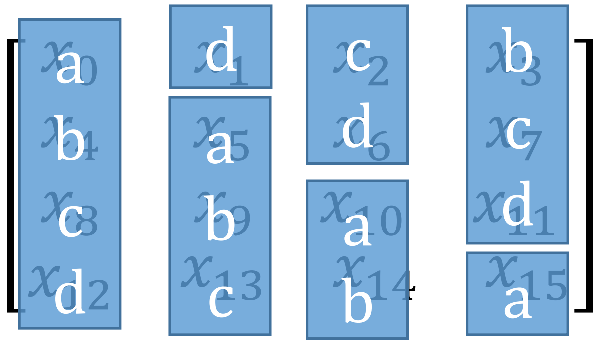
$$\left.\begin{aligned} b &= b \oplus ((a + d) \lll 7), \\ c &= c \oplus ((b + a) \lll 9), \\ d &= d \oplus ((c + b) \lll 13), \\ a &= a \oplus ((d + c) \lll 18). \end{aligned}\right\}$$

Salsa update function



$$\left.\begin{aligned}
b &= b \oplus ((a + d) \lll 7),\\
c &= c \oplus ((b + a) \lll 9),\\
d &= d \oplus ((c + b) \lll 13),\\
a &= a \oplus ((d + c) \lll 18).
\end{aligned}\right\}$$

Salsa update function



$$\left.\begin{aligned}
{\color{blue}b} &= b \oplus ((a + d) \lll 7), \\
{\color{blue}c} &= c \oplus (({\color{blue}b} + a) \lll 9), \\
{\color{blue}d} &= d \oplus (({\color{blue}c} + {\color{blue}b}) \lll 13), \\
{\color{blue}a} &= a \oplus (({\color{blue}d} + {\color{blue}c}) \lll 18).
\end{aligned}\right\}$$

Differential-Linear Biases

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

$$\oplus \qquad\qquad\qquad\qquad \oplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$$

$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

$$\Pr[\qquad = 0] = \frac{1}{2}(1 + \varepsilon_d)$$

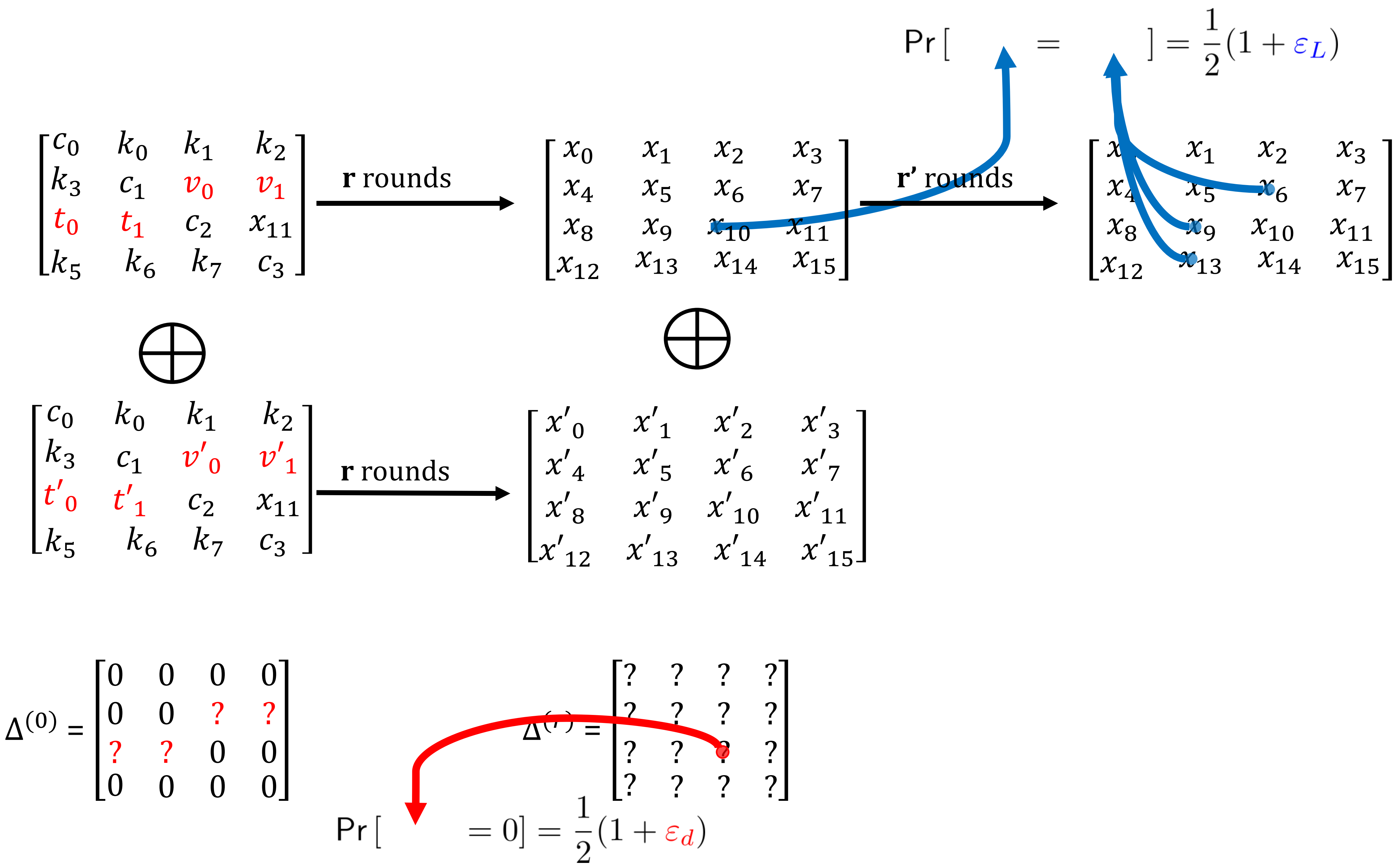
$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & {\color{red}v_0} & {\color{red}v_1} \\ {\color{red}t_0} & {\color{red}t_1} & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \xrightarrow{\textbf{r'} \text{ rounds}} \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

$$\oplus \qquad\qquad\qquad\qquad \oplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & {\color{red}v'_0} & {\color{red}v'_1} \\ {\color{red}t'_0} & {\color{red}t'_1} & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$$

$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & {\color{red}?} & {\color{red}?} \\ {\color{red}?} & {\color{red}?} & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & {\color{red}?} & ? \\ ? & ? & ? & ? \end{bmatrix}$$

$$\Pr[\quad = 0] = \frac{1}{2}(1 + {\color{red}\varepsilon_d})$$



$\Pr[\quad = \quad] = \frac{1}{2}(1+\varepsilon_L)$
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
r rounds
$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$
r' rounds
$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$
$\oplus$
$\oplus$
$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix}$
r rounds
$\begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$
$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$
$\Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$
$\Pr[\quad = 0] = \frac{1}{2}(1+\varepsilon_d)$

$$\Pr[\quad = \quad] = \frac{1}{2}(1+\varepsilon_L)$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v_0 & v_1 \\ t_0 & t_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix} \xrightarrow{\textbf{r'} \text{ rounds}} \begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

$$\bigoplus \qquad\qquad\qquad\qquad \bigoplus$$

$$\begin{bmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & v'_0 & v'_1 \\ t'_0 & t'_1 & c_2 & x_{11} \\ k_5 & k_6 & k_7 & c_3 \end{bmatrix} \xrightarrow{\textbf{r} \text{ rounds}} \begin{bmatrix} x'_0 & x'_1 & x'_2 & x'_3 \\ x'_4 & x'_5 & x'_6 & x'_7 \\ x'_8 & x'_9 & x'_{10} & x'_{11} \\ x'_{12} & x'_{13} & x'_{14} & x'_{15} \end{bmatrix}$$

$$\Delta^{(0)} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & ? & ? \\ ? & ? & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \qquad \Delta^{(r)} = \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

$$\Pr[\quad = 0] = \frac{1}{2}(1+\varepsilon_d)$$

Given ε_d and ε_L, we can find the **differential-linear** bias for **r+r'** rounds.

Linear approximation with $\varepsilon_L = 1$

Let's look at the Salsa update function again

Linear approximation with $\varepsilon_L = 1$

Let's look at the Salsa update function again

$$\left.\begin{array}{rcl} {\color{blue}b} & = & b \oplus ((a+d) \lll 7), \\ {\color{blue}c} & = & c \oplus (({\color{blue}b}+a) \lll 9), \\ {\color{blue}d} & = & d \oplus (({\color{blue}c}+{\color{blue}b}) \lll 13), \\ {\color{blue}a} & = & a \oplus (({\color{blue}d}+{\color{blue}c}) \lll 18). \end{array}\right\}$$

Let's look at the Salsa update function again

$$
\begin{aligned}
d &= d \oplus ((c + b) \lll 13), \\
a &= a \oplus ((d + c) \lll 18).
\end{aligned}
$$

Get rid of the carry.

$$d[13] = d[13] \oplus (c[0] \oplus b[0]),$$
$$a[18] = a[18] \oplus (d[0] \oplus c[0]).$$

Move things around, from the linearity of XOR

$$\Delta d[13] \oplus \Delta c[0] \oplus \Delta b[0] = \Delta d[13]$$
$$\Delta a[18] \oplus \Delta d[0] \oplus \Delta c[0] = \Delta a[18].$$

Move things around, from the linearity of XOR

$$\Delta d[13] \oplus \Delta c[0] \oplus \Delta b[0] = \Delta d[13]$$
$$\Delta a[18] \oplus \Delta d[0] \oplus \Delta c[0] = \underbrace{\Delta a[18]}_{\varepsilon}.$$

Move things around, from the linearity of XOR

$$\Delta d[13] \oplus \Delta c[0] \oplus \Delta b[0] = \Delta d[13]$$

$$\underbrace{\Delta a[18] \oplus \Delta d[0] \oplus \Delta c[0]}_{\varepsilon} = \underbrace{\Delta a[18]}_{\varepsilon}.$$

Move things around, from the linearity of XOR

$$\begin{aligned} \Delta d[13] \oplus \Delta c[0] \oplus \Delta b[0] &= \Delta d[13] \\ \underbrace{\Delta a[18] \oplus \Delta d[0] \oplus \Delta c[0]}_{\varepsilon} &= \underbrace{\Delta a[18]}_{\varepsilon}. \end{aligned}$$

Lets us search over 8 possible bits instead of $\binom{512}{3}$ 3 bit combinations.

Similar idea for ChaCha, but involves more bits because of a more involved state update function.

Similar idea for ChaCha, but involves more bits because of a more involved state update function.

"Unlike Salsa20, our exhaustive search showed no bias in 4-round ChaCha, be it with one, two, or three target output bits."

Salsa

Reference	$\|\varepsilon\|$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$

4 rounds

Reference	$\|\varepsilon\|$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$

5 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$
This work	$\approx \mathbf{2^{0}}$

4 rounds

Reference	$\lvert\varepsilon\rvert$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$
This work	$\approx \mathbf{2^{-3.13}}$

5 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$
This work	$\approx \mathbf{2^{0}}$

4 rounds

Reference	$\lvert\varepsilon\rvert$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$
This work	$\approx \mathbf{2^{-3.13}}$

5 rounds

ChaCha

Reference	$\lvert\varepsilon\rvert$
Aumasson et al. (2008)	$2^{-5.26}$
Maitra (2016)	$2^{-2.83}$

3 rounds

Reference	$\lvert\varepsilon\rvert$

4 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$
This work	$\approx \mathbf{2^{0}}$

4 rounds

Reference	$\lvert\varepsilon\rvert$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$
This work	$\approx \mathbf{2^{-3.13}}$

5 rounds

ChaCha

Reference	$\lvert\varepsilon\rvert$
Aumasson et al. (2008)	$2^{-5.26}$
Maitra (2016)	$2^{-2.83}$
This work	$\mathbf{2^{0}}$

3 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-2.33}}$

4 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$
This work	$\approx \mathbf{2^{0}}$

4 rounds

Reference	$\lvert\varepsilon\rvert$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$
This work	$\approx \mathbf{2^{-3.13}}$

5 rounds

Distinguisher with complexity $\approx 2^{8}$

2^{47} improvement

ChaCha

Reference	$\lvert\varepsilon\rvert$
Aumasson et al. (2008)	$2^{-5.26}$
Maitra (2016)	$2^{-2.83}$
This work	$\mathbf{2^{0}}$

3 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-2.33}}$

4 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
Tsunoo et al. (2007)	$2^{-5.24}$
Aumasson et al. (2008)	$2^{-2.93}$
Maitra, Paul, Meier (2015)	$2^{-2.35}$
Maitra (2016)	$2^{-2.12}$
This work	$\approx \mathbf{2^{0}}$

4 rounds

Reference	$\lvert\varepsilon\rvert$
Fischer et al. (2006)	$2^{-10.34}$
Maitra, Paul, Meier (2015)	$2^{-9.05}$
This work	$\approx \mathbf{2^{-3.13}}$

5 rounds

Distinguisher with complexity $\approx 2^{8}$

2^{47} improvement

ChaCha

Reference	$\lvert\varepsilon\rvert$
Aumasson et al. (2008)	$2^{-5.26}$
Maitra (2016)	$2^{-2.83}$
This work	$\mathbf{2^{0}}$

3 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-2.33}}$

4 rounds

Distinguisher with complexity $\approx 2^{6}$

Linear approximation with $\varepsilon_L < 1$

Linear approximation with $\varepsilon_L < 1$

$$(x + y)[i]$$

Linear approximation with $\varepsilon_L < 1$

$$(x+y)[i] \;=\; x[i] \oplus y[i] \oplus x[i-1] \qquad \text{w.p. } \tfrac{1}{2}\left(1+\tfrac{1}{2}\right)$$

Linear approximation with $\varepsilon_L < 1$

$$(x+y)[i] \quad = \quad x[i] \oplus y[i] \oplus x[i-1] \qquad \text{w.p. } \tfrac{1}{2}\left(1+\tfrac{1}{2}\right)$$

$$(x+y)[i] \oplus (x+y)[i+1]$$

Linear approximation with $\varepsilon_L < 1$

$$(x+y)[i] \;=\; x[i] \oplus y[i] \oplus x[i-1] \qquad \text{w.p. } \tfrac{1}{2}\left(1+\tfrac{1}{2}\right)$$

$$(x+y)[i] \oplus (x+y)[i+1] = x[i+1] \oplus y[i+1] \qquad \text{w.p. } \tfrac{1}{2}\left(1-\tfrac{1}{2}\right)$$

$$d[13] = d[13] \oplus c[0] \oplus b[0]$$

$$d[13] = d[13] \oplus c[0] \oplus b[0]$$

$$d[13] = d[13] \oplus c[0] \oplus b[0]$$

$$d[13] = d[13] \oplus c[0] \oplus b[0]$$

$$d[13] = d[13] \oplus c[0] \oplus b[0]$$

Combination of 19 bits from the subsequent round

Salsa

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-15.13}}$

6 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-95.13}}$

7 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-15.13}}$

6 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-95.13}}$

7 rounds

ChaCha

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-7.2}}$

5 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-57.2}}$

6 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-15.13}}$

6 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-95.13}}$

7 rounds

Distinguisher with complexity $\approx 2^{32}$

2^{41} improvement

ChaCha

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-7.2}}$

5 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-57.2}}$

6 rounds

Salsa

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-15.13}}$

6 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-95.13}}$

7 rounds

Distinguisher with complexity $\approx 2^{32}$
2^{41} improvement

ChaCha

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-7.2}}$

5 rounds

Reference	$\lvert\varepsilon\rvert$
This work	$\approx \mathbf{2^{-57.2}}$

6 rounds

Distinguisher with complexity $\approx 2^{16}$

Salsa

Reference	$\|\varepsilon\|$
This work	$\approx \mathbf{2^{-15.13}}$

6 rounds

Distinguisher with complexity $\approx 2^{32}$
2^{41} improvement

Reference	$\|\varepsilon\|$
This work	$\approx \mathbf{2^{-95.13}}$

7 rounds

ChaCha

Reference	$\|\varepsilon\|$
This work	$\approx \mathbf{2^{-7.2}}$

5 rounds

Distinguisher with complexity $\approx 2^{16}$

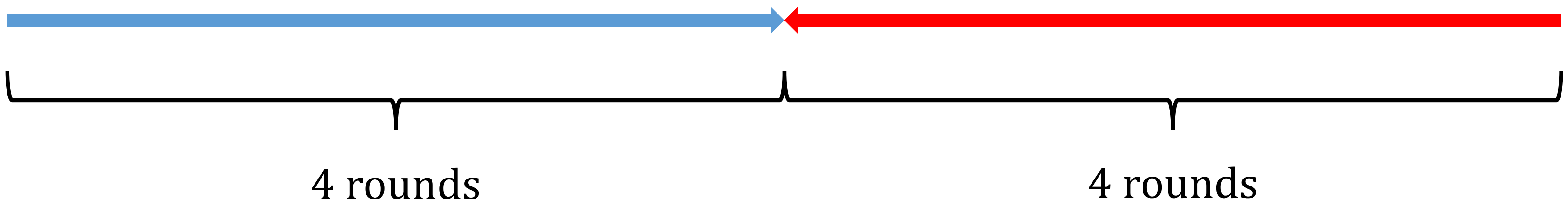
Reference	$\|\varepsilon\|$
This work	$\approx \mathbf{2^{-57.2}}$

6 rounds

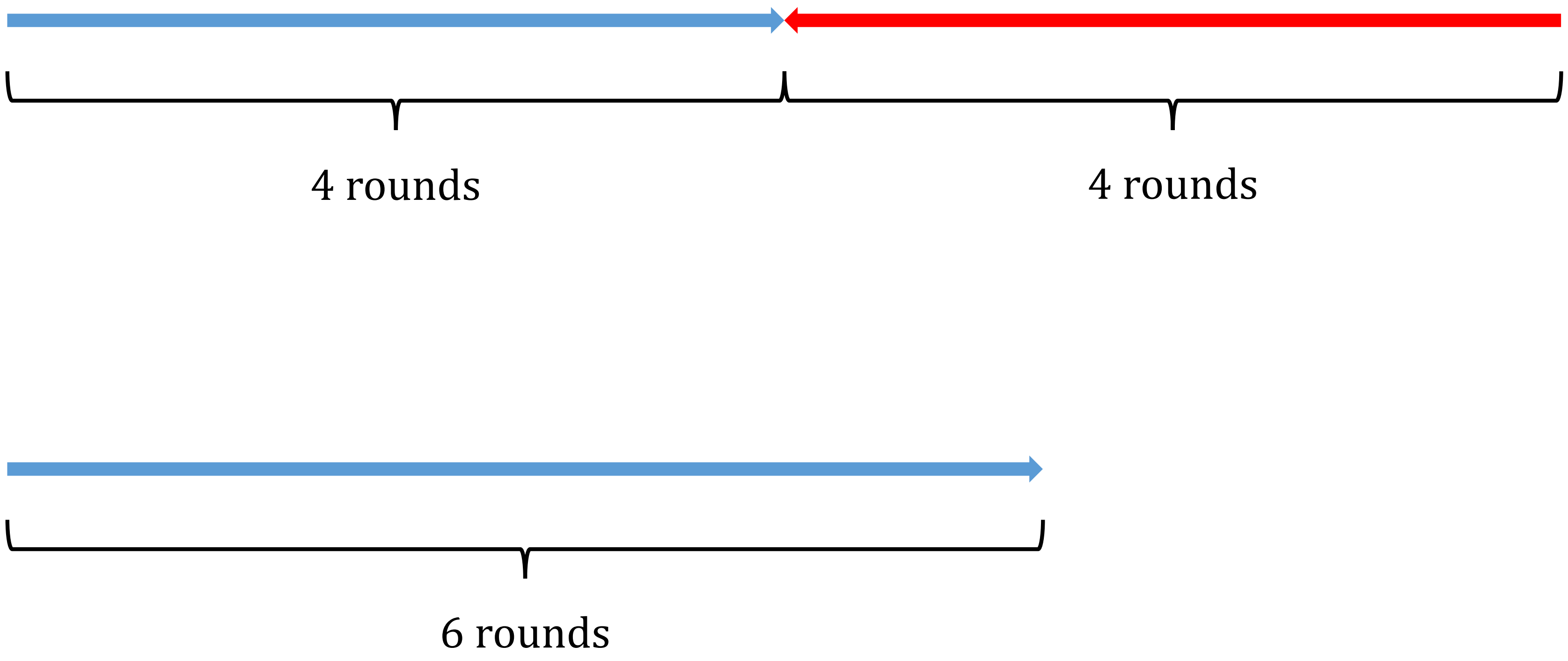
Distinguisher with complexity $\approx 2^{116}$
2^{20} improvement

Implications to the key recovery attack

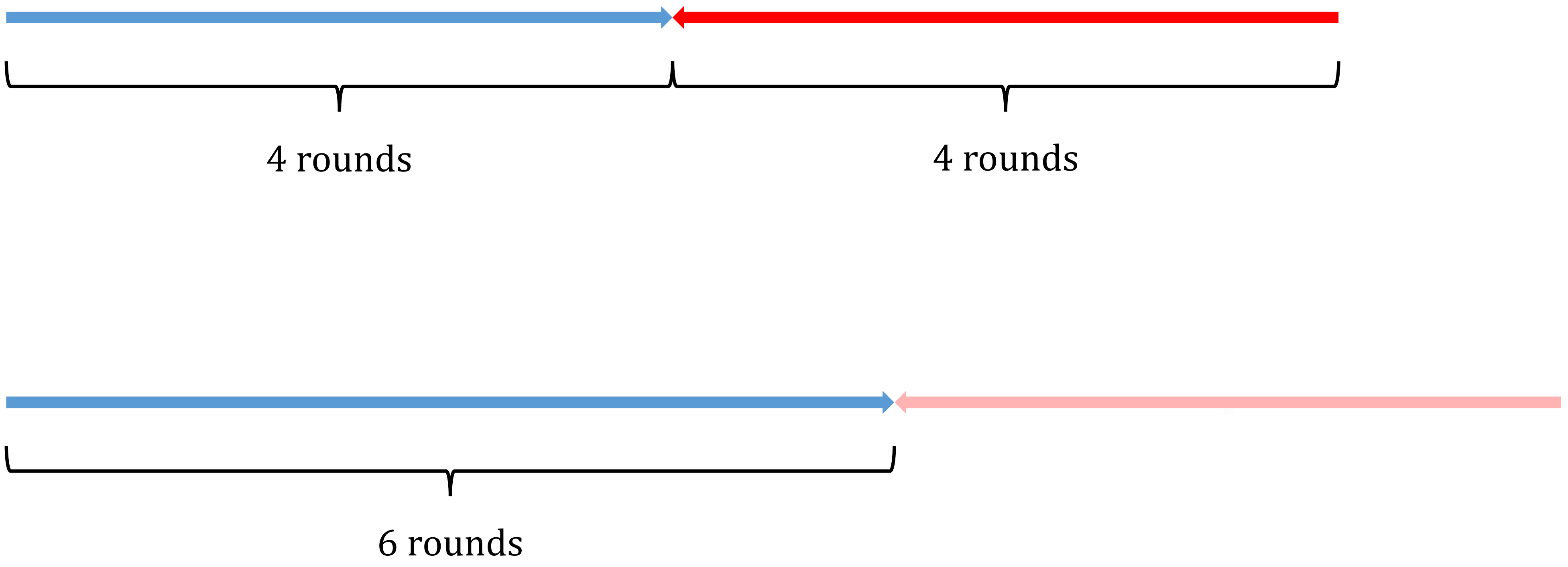
Salsa



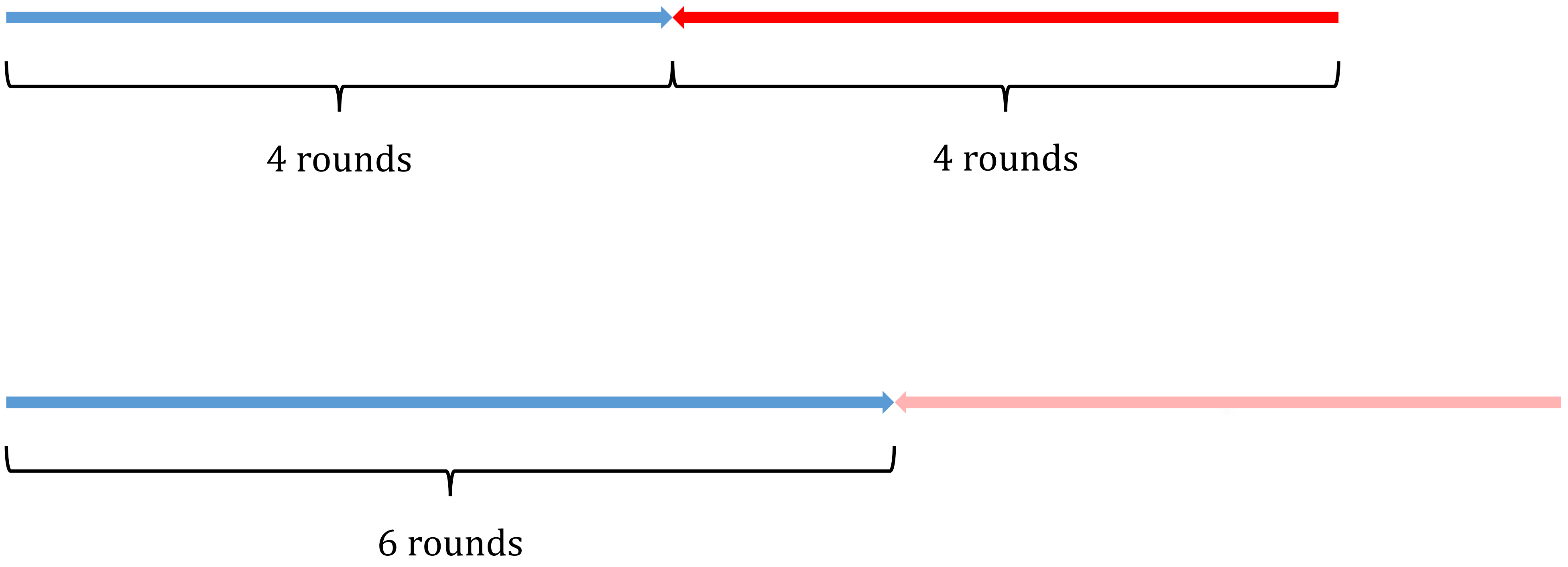
Salsa



Salsa

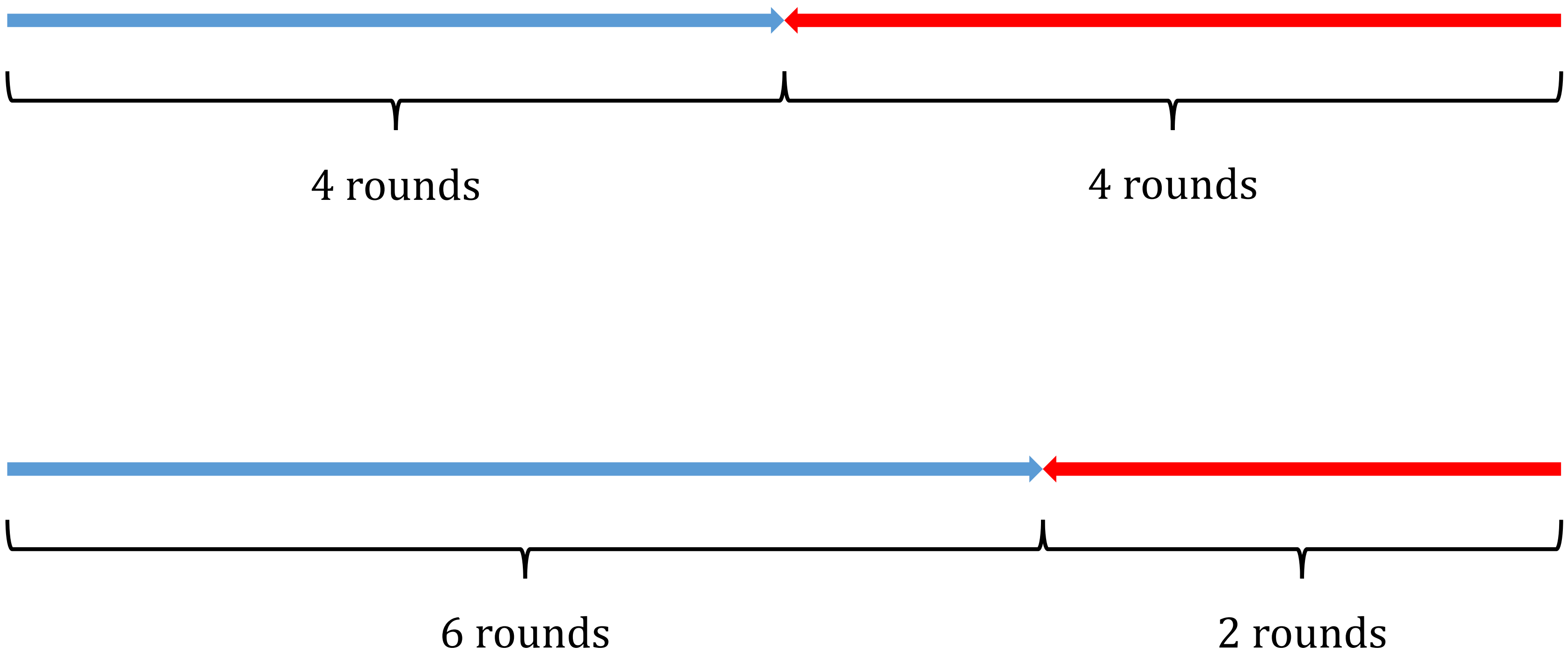


Salsa

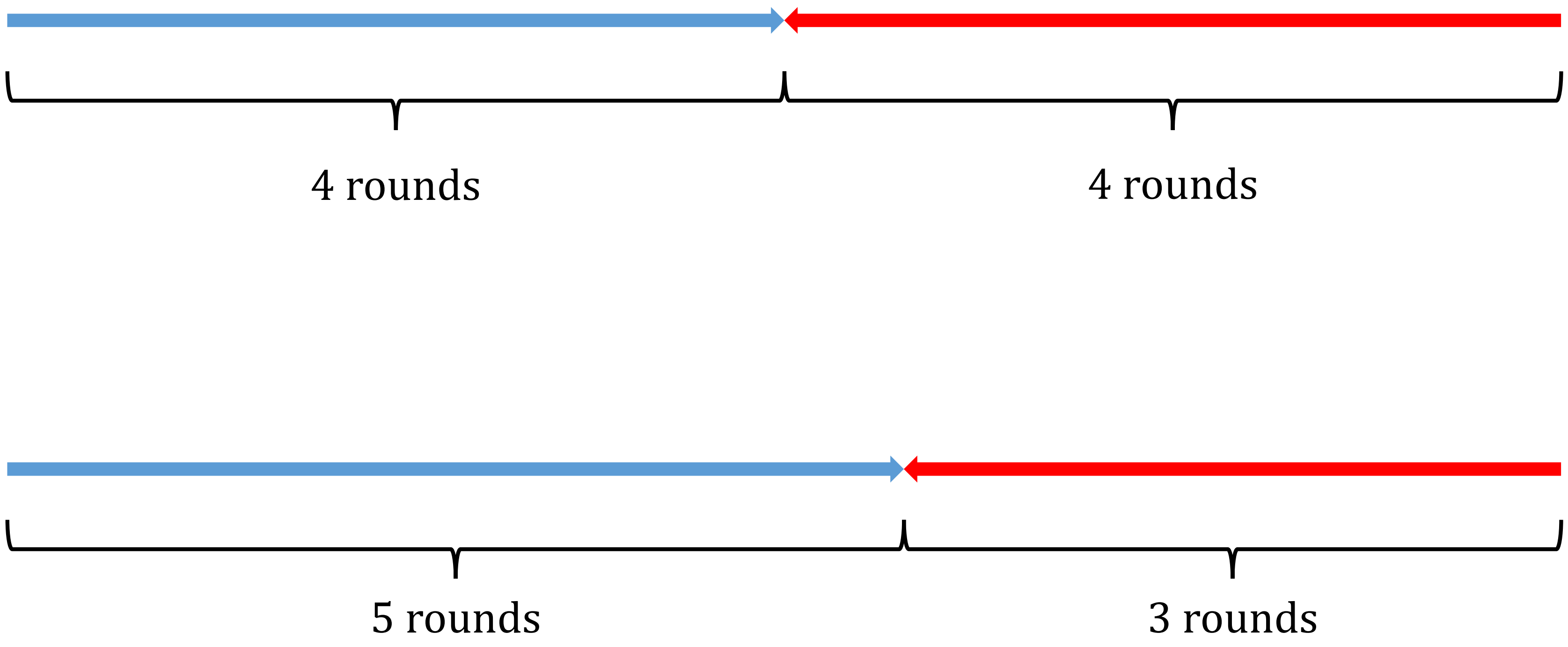


But...

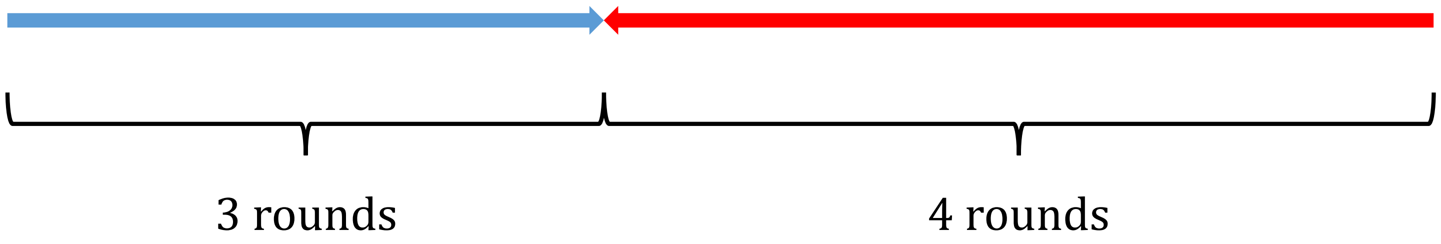
Salsa



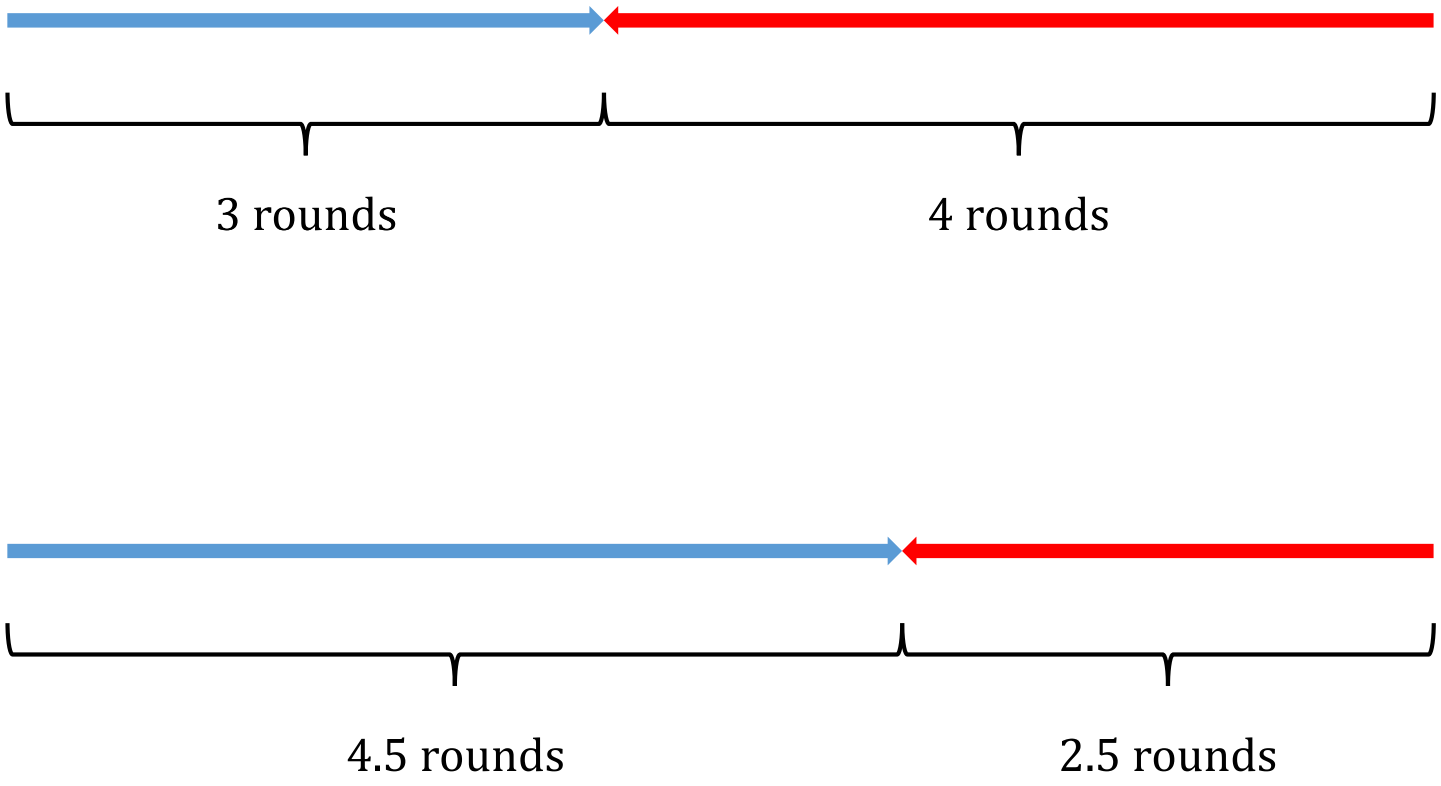
Salsa



ChaCha



ChaCha



Salsa

Reference	Time
Aumasson et al. (2008)	2^{151}
Shi et al. (2012)	2^{148}

7 rounds

Reference	Time
Aumasson et al. (2008)	2^{251}
Shi et al. (2012)	2^{250}
Maitra(2016)	$2^{245.5}$

8 rounds

Salsa

Reference	Time
Aumasson et al. (2008)	2^{151}
Shi et al. (2012)	2^{148}
This work	$\mathbf{2^{137}}$

7 rounds

Reference	Time
Aumasson et al. (2008)	2^{251}
Shi et al. (2012)	2^{250}
Maitra(2016)	$2^{245.5}$
This work	$\mathbf{2^{244.9}}$

8 rounds

Salsa

Reference	Time
Aumasson et al. (2008)	2^{151}
Shi et al. (2012)	2^{148}
This work	$\mathbf{2^{137}}$

7 rounds

Reference	Time
Aumasson et al. (2008)	2^{251}
Shi et al. (2012)	2^{250}
Maitra(2016)	$2^{245.5}$
This work	$\mathbf{2^{244.9}}$

8 rounds

ChaCha

Reference	Time
Aumasson et al. (2008)	2^{139}
Shi et al. (2012)	2^{136}

6 rounds

Reference	Time
Aumasson et al. (2008)	2^{248}
Shi et al. (2012)	$2^{246.5}$
Maitra(2016)	$2^{238.9}$

7 rounds

Salsa

Reference	Time
Aumasson et al. (2008)	2^{151}
Shi et al. (2012)	2^{148}
This work	$\mathbf{2^{137}}$

7 rounds

Reference	Time
Aumasson et al. (2008)	2^{251}
Shi et al. (2012)	2^{250}
Maitra(2016)	$2^{245.5}$
This work	$\mathbf{2^{244.9}}$

8 rounds

ChaCha

Reference	Time
Aumasson et al. (2008)	2^{139}
Shi et al. (2012)	2^{136}
This work	$\mathbf{2^{127.5}}$

6 rounds

Reference	Time
Aumasson et al. (2008)	2^{248}
Shi et al. (2012)	$2^{246.5}$
Maitra(2016)	$2^{238.9}$
This work	$\mathbf{2^{237.7}}$

7 rounds

Conclusion

We obtain biases in Salsa and ChaCha not obtained for almost a decade. Develop a theory on how to do this.

We obtain biases in Salsa and ChaCha not obtained for almost a decade. Develop a theory on how to do this.

Improve attacks on some reduced round versions, importantly moving some to practical realms.

We obtain biases in Salsa and ChaCha not obtained for almost a decade. Develop a theory on how to do this.

Improve attacks on some reduced round versions, importantly moving some to practical realms.

A different method to partition the key space could potentially improve our attacks in both **complexity** and **rounds**.

We obtain biases in Salsa and ChaCha not obtained for almost a decade. Develop a theory on how to do this.

Improve attacks on some reduced round versions, importantly moving some to practical realms.

A different method to partition the key space could potentially improve our attacks in both **complexity** and **rounds**.

(or is this inherent to this kind of cryptanalysis?)

Thank you. Questions?

References

[C05] Paul Crowley. *“Truncated differential cryptanalysis of five rounds of Salsa20"*. In: IACR Cryptology ePrint Archive 2005 (2005), p. 375. url: http : / /eprint.iacr.org/2005/375.

[FMB+06] Simon Fischer, Willi Meier, Come Berbain, Jean-Francois Biasse, and Matthew J. B. Robshaw. *“Non-randomness in eSTREAM Candidates Salsa20 and TSC-4"*. In: Progress in Cryptology - INDOCRYPT 2006, 7th International Conference on Cryptology in India, Kolkata, India, December 11-13, 2006, Proceedings.

[TSK+07] Yukiyasu Tsunoo, Teruo Saito, Hiroyasu Kubo, Tomoyasu Suzaki, and Hiroki Nakashima. *“Differential Cryptanalysis of Salsa20/8”*. 2007. url: http://ecrypt.eu.org/stream/papersdir/2007/010.pdf.

[AFK+08] Jean-Philippe Aumasson, Simon Fischer, Shahram Khazaei, Willi Meier, and Christian Rechberger. *“New features of Latin dances: analysis of Salsa, ChaCha, and Rumba"*. In: Fast Software Encryption. Springer. 2008.

[SZF+12] Zhenqing Shi, Bin Zhang, Dengguo Feng, and Wenling Wu. *“Improved Key Recovery Attacks on Reduced-Round Salsa20 and ChaCha"*. In: Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers.

[MPM15] Subhamoy Maitra, Goutam Paul, and Willi Meier. *“Salsa20 Cryptanalysis: New Moves and Revisiting Old Styles"*. In: WCC 2015, the Ninth International Workshop on Coding and Cryptography, April 13-17, 2015, Paris, France.

[Mai16] Subhamoy Maitra. *“Chosen IV cryptanalysis on reduced round ChaCha and Salsa"*. In: Discrete Applied Mathematics 208 (2016).