MODULO OPERATION UNIT BASED ON BARRETT REDUCTION ALGORITHM

EE577A

Fall 2019

Barrett Reduction Algorithm Calculating $s = x \; mod \; n$

- Assumptions:

(1) n is a 7-bit unsigned number and $n \geq 3$ or n is a 8-bit signed number with $n_7=0$, for example n = 01100110 = 102.

(2) x is a positive integer and $0 < x < n^2$, which means x is a 14-bit unsigned number or x is a 16-bit signed number with $x_{15} = x_{14} = 0$, for example x = 0010000101001001 = 8521.

Barrett Reduction Algorithm
Calculating $s = x \ mod \ n$

- Algorithm:

$2^3 = 8$

(1) From assumption 1, n < 2^k, where k = 7.

1000

(2) Calculate $r = \left\lfloor \frac{4^k}{n} \right\rfloor$. 7bit

2^{14}

(3) Calculate $t = x - \left\lfloor \frac{xr}{4^k} \right\rfloor * n$.

(4) $s = \begin{cases} t - n & if \ t \geq n \\ t & if \ t < n \end{cases}$

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \le r = \left\lfloor \frac{4^k}{n} \right\rfloor \le \frac{4^k}{n}$$

Both sides times x,

$$\Rightarrow x\left(\frac{4^k}{n} - 1\right) \le xr \le x\left(\frac{4^k}{n}\right)$$

$A + \bar{A} \cdot B$

$= A + B - AB$

$= A + B$

$\frac{4^k}{n}$ $\frac{2^{14}}{2^0}$

$n < 2^7$

2^{14}

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \leq r = \left\lfloor \frac{4^k}{n} \right\rfloor \leq \frac{4^k}{n}$$

Both sides times x, $$\Rightarrow x\left(\frac{4^k}{n} - 1\right) \leq xr \leq x\left(\frac{4^k}{n}\right)$$

Both sides divided by 4^k, $$\Rightarrow \frac{x}{n} - \frac{x}{4^k} \leq \frac{xr}{4^k} \leq \frac{x}{n}$$

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \leq r = \left\lfloor \frac{4^k}{n} \right\rfloor \leq \frac{4^k}{n}$$

Both sides times x, $\Rightarrow x\left(\frac{4^k}{n} - 1\right) \leq xr \leq x\left(\frac{4^k}{n}\right)$

Both sides divided by 4^k, $\Rightarrow \frac{x}{n} - \frac{x}{4^k} \leq \frac{xr}{4^k} \leq \frac{x}{n}$

With $0 \leq x \leq n^2 < 4^k$, $\Rightarrow \frac{x}{n} - 1 < \frac{xr}{4^k} \leq \frac{x}{n}$

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \leq r = \left\lfloor \frac{4^k}{n} \right\rfloor \leq \frac{4^k}{n}$$

Both sides times x, $\Rightarrow x\left(\frac{4^k}{n} - 1\right) \leq xr \leq x\left(\frac{4^k}{n}\right)$

Both sides divided by 4^k, $\Rightarrow \frac{x}{n} - \frac{x}{4^k} \leq \frac{xr}{4^k} \leq \frac{x}{n}$

With $0 \leq x \leq n^2 < 4^k$, $\Rightarrow \frac{x}{n} - 1 < \frac{xr}{4^k} \leq \frac{x}{n}$

Take floor operation, $\Rightarrow \frac{x}{n} - 2 < \left\lfloor \frac{x}{n} - 1 \right\rfloor \leq \left\lfloor \frac{xr}{4^k} \right\rfloor \leq \frac{x}{n}$

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \le r = \left\lfloor \frac{4^k}{n} \right\rfloor \le \frac{4^k}{n}$$

Both sides times x, $\Rightarrow x\left(\frac{4^k}{n} - 1\right) \le xr \le x\left(\frac{4^k}{n}\right)$

Both sides divided by 4^k, $\Rightarrow \frac{x}{n} - \frac{x}{4^k} \le \frac{xr}{4^k} \le \frac{x}{n}$

With $0 \le x \le n^2 < 4^k$, $\Rightarrow \frac{x}{n} - 1 < \frac{xr}{4^k} \le \frac{x}{n}$

Take floor operation, $\Rightarrow \frac{x}{n} - 2 < \left\lfloor \frac{x}{n} - 1 \right\rfloor \le \left\lfloor \frac{xr}{4^k} \right\rfloor \le \frac{x}{n}$

Both sides times n, $\Rightarrow x - 2n < \left\lfloor \frac{xr}{4^k} \right\rfloor n \le x$

Barrett Reduction Algorithm Proof

By definition and assumptions,

$$\frac{4^k}{n} - 1 \le r = \left\lfloor \frac{4^k}{n} \right\rfloor \le \frac{4^k}{n}$$

Both sides times x, $\Rightarrow x\left(\frac{4^k}{n} - 1\right) \le xr \le x\left(\frac{4^k}{n}\right)$

Both sides divided by 4^k, $\Rightarrow \frac{x}{n} - \frac{x}{4^k} \le \frac{xr}{4^k} \le \frac{x}{n}$

With $0 \le x \le n^2 < 4^k$, $\Rightarrow \frac{x}{n} - 1 < \frac{xr}{4^k} \le \frac{x}{n}$

Take floor operation, $\Rightarrow \frac{x}{n} - 2 \le \left\lfloor \frac{x}{n} - 1 \right\rfloor < \left\lfloor \frac{xr}{4^k} \right\rfloor \le \frac{x}{n}$

Both sides times n, $\Rightarrow x - 2n < \left\lfloor \frac{xr}{4^k} \right\rfloor n \le x$

Some basic alegebra, $\Rightarrow 0 \le t = x - \left\lfloor \frac{xr}{4^k} \right\rfloor n < 2n$

Barrett Reduction Algorithm Proof

$< 2^8$

$$0 \le t = x - \left\lfloor \frac{xr}{4^k} \right\rfloor n < 2n$$

n is 7bit

2n is 8bit

8bit signed #

If $t \ge n, s = t - n$

If $t < n, s = t$

$t \ge n$

$t[7] = 1$

$t[7] = 0.$

$t[6:0] - n[6:0] = D[7:0]$

$D[7] = 1 : t < n$

$D[7] = 0 : t \ge n$

$T[7] = 1$ or $T[7] = 0$ and $D[7] = 0$

Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$
- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor * n$
- Calculate $t = x - \left\lfloor \frac{xr}{4^k} \right\rfloor * n$
- Decide $s = t \; or \; s = t - n$

Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$

x and r both have the form of 14-bit unsigned number or a 16-bit signed number with x_15 = x_14 = 0. Here we can represent *x* and *r* as:

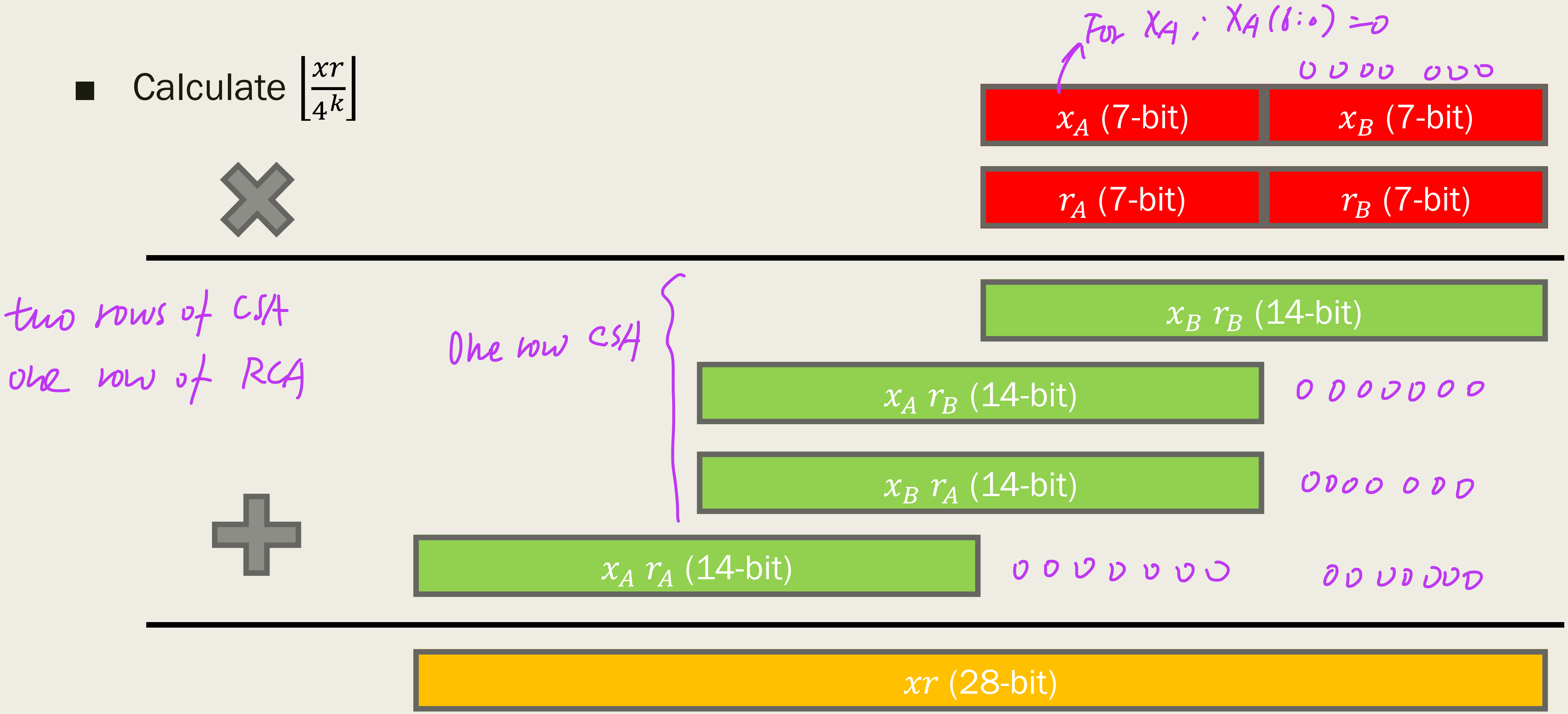
$$x = x_{15}x_{14}x_{13-7}x_{6-0} = x_{15}x_{14}x_Ax_B$$

$$r = r_{15}r_{14}r_{13-7}r_{6-0} = r_{15}r_{14}r_Ar_B$$

Here x_A, x_B, r_A, r_B are 7-bit unsigned numbers.

Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$

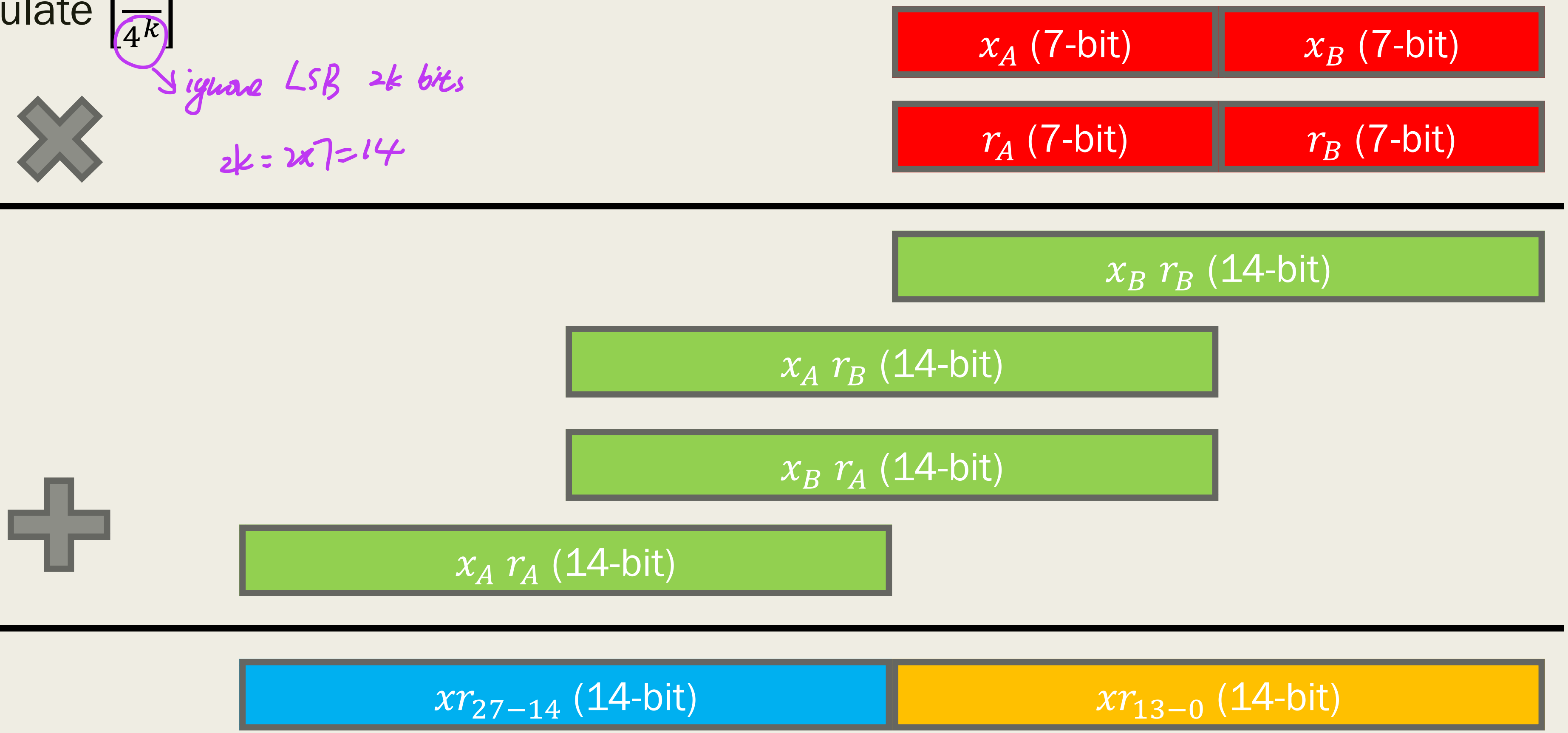


Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$

ignore LSB 2k bits

$2k = 2 \times 7 = 14$



Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$

$$xr \leq x\left(\frac{4^k}{n}\right)$$

$r < 2^7$

With $x < n^2$, 2^{14}

$$\Rightarrow xr < n^2 * \left(\frac{4^k}{n}\right) = n * 4^k$$

With n< 2^k,

$$\Rightarrow xr < 2^k * 4^k = 2^{3k}$$

Here $k = 7$,

$$\Rightarrow xr < 2^{21}$$

21
-14
7

$$\Rightarrow xr_{27-21} = 0$$

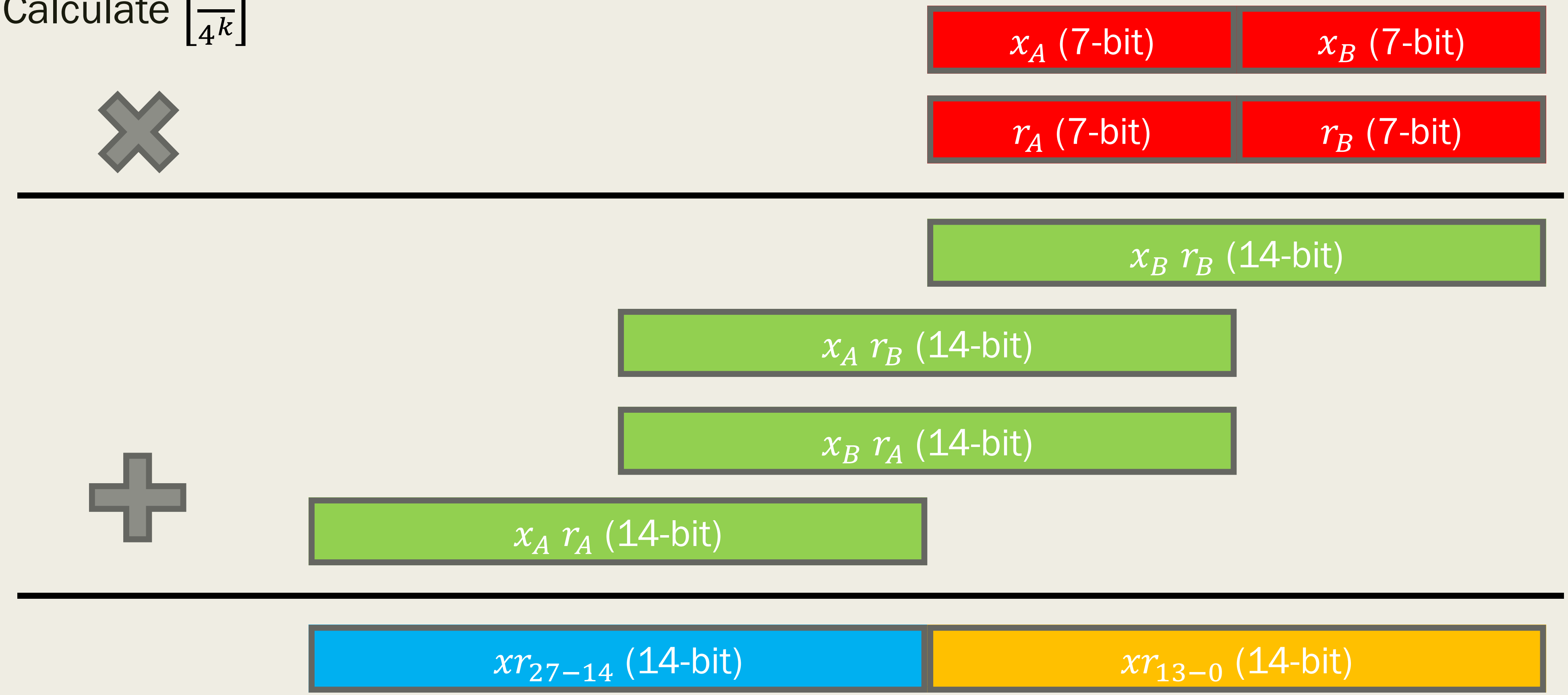
Take $\left\lfloor \frac{xr}{4^k} \right\rfloor$,

$\Rightarrow xr_{13-0}$ can be ignored

$\Rightarrow xr_{20-14}$ is important

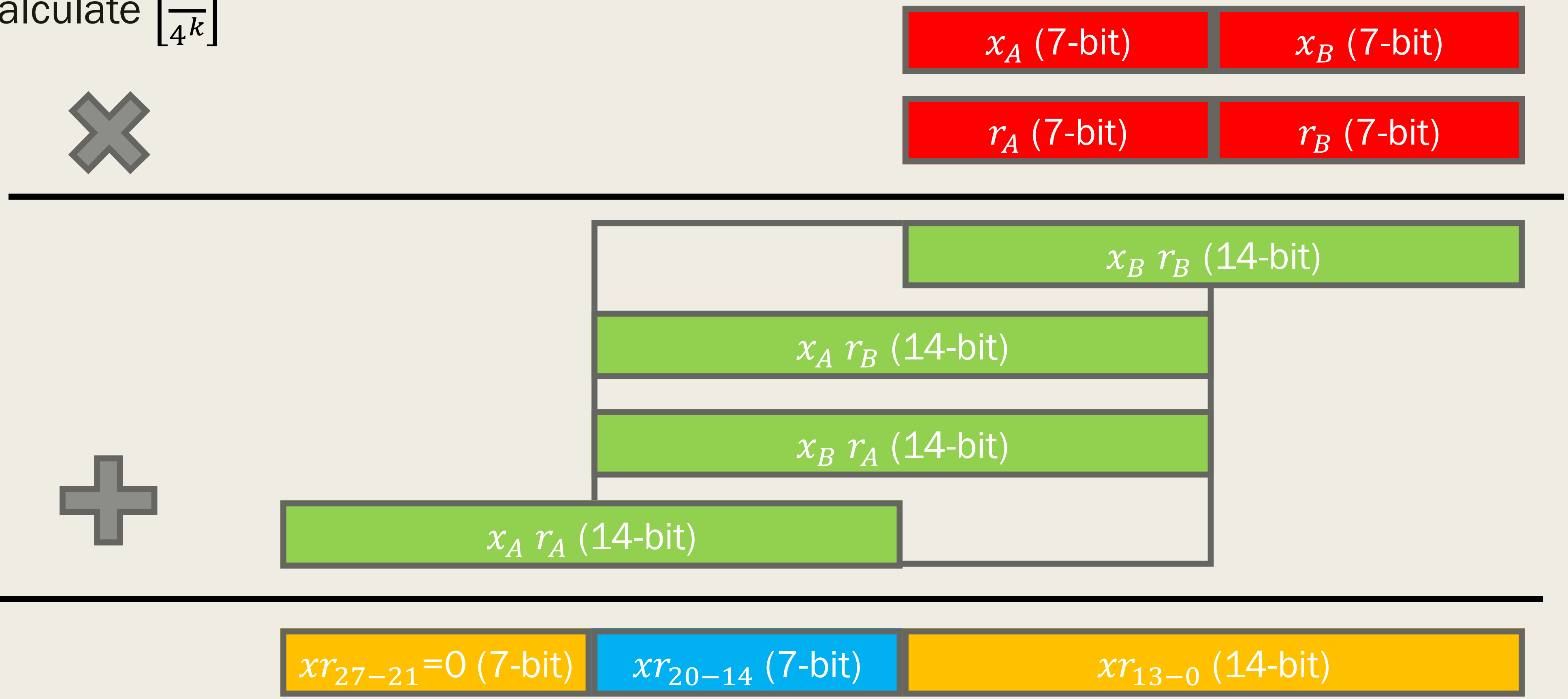
Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$



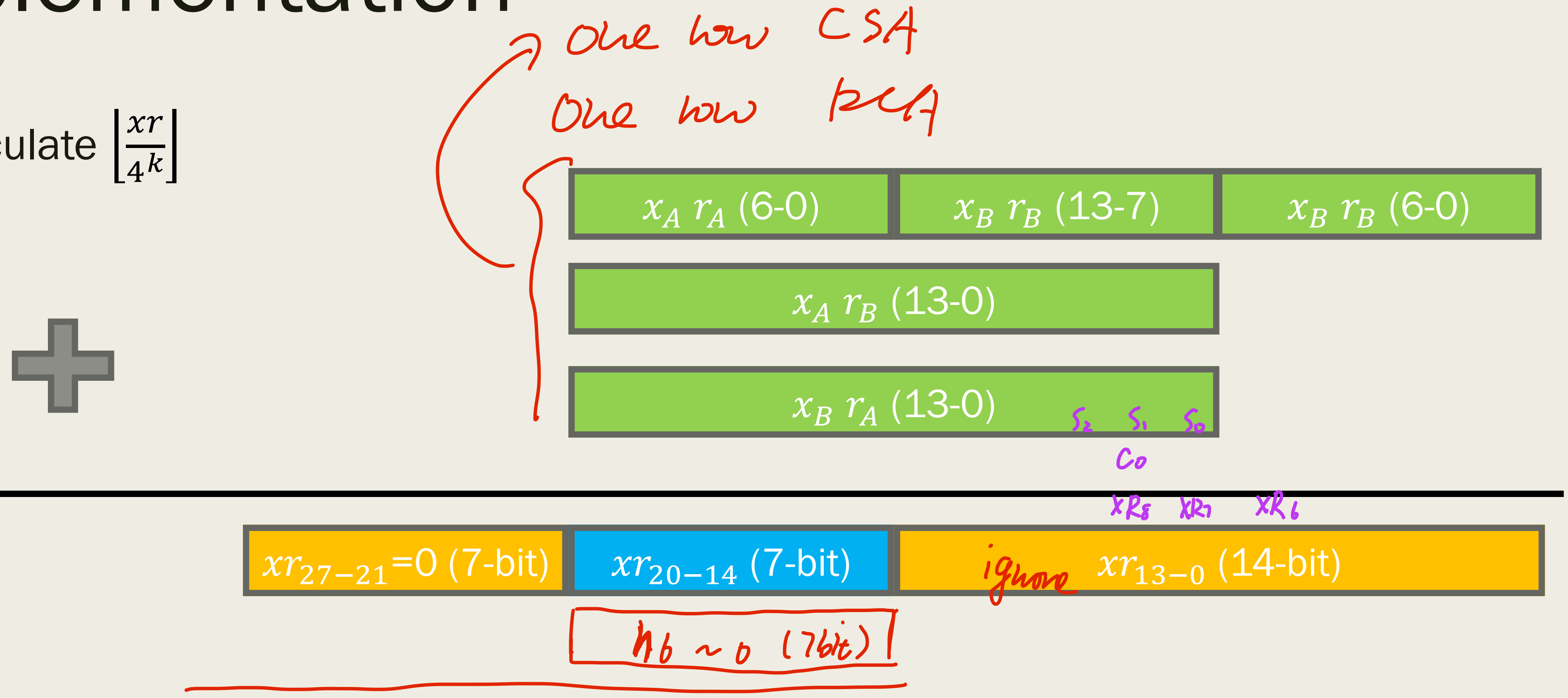
Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$



Barrett Reduction Algorithm Implementation

- Calculate $\left\lfloor \frac{xr}{4^k} \right\rfloor$



Example

- x=8501=0010000100110101, $x_A = 1000010, x_B = 0110101$
- n=101=01100101 7bit
- r=162=0000000010100010, $r_A = 0000001, r_B = 0100010$
- $x_A r_A$ (6-0) $x_B r_B$ (13-7) = 10000100001110
- $x_A r_B$ (13-0) = 00100011000100
- $x_B r_A$ (13-0) = 00000000110101
- $\left\lfloor \frac{xr}{4^k} \right\rfloor$ = 1010100 = 84
- $\left\lfloor \frac{xr}{4^k} \right\rfloor * n$ = 10000100100100 = 8484
- t = x − $\left\lfloor \frac{xr}{4^k} \right\rfloor * n$ = $\underbrace{0010001}_{7bit}$ = 17 = s

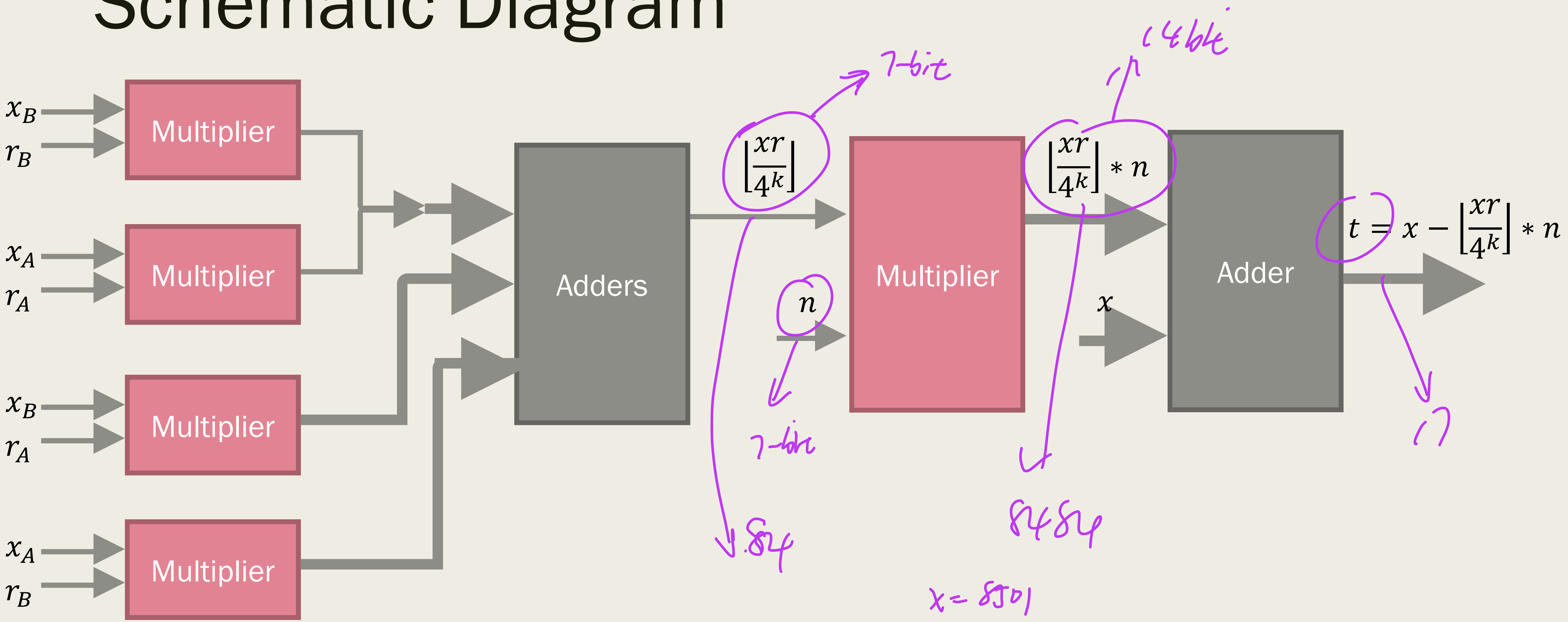
$\left\lfloor \frac{x}{n} \right\rfloor \cdot n.$

$n =$

$\left\lfloor \frac{7}{2} \right\rfloor \times 2 = 3 \times 2 = 6$

$7 - 6 = 1$

Barrett Reduction Algorithm Schematic Diagram



Barrett Reduction Algorithm Schematic Diagram

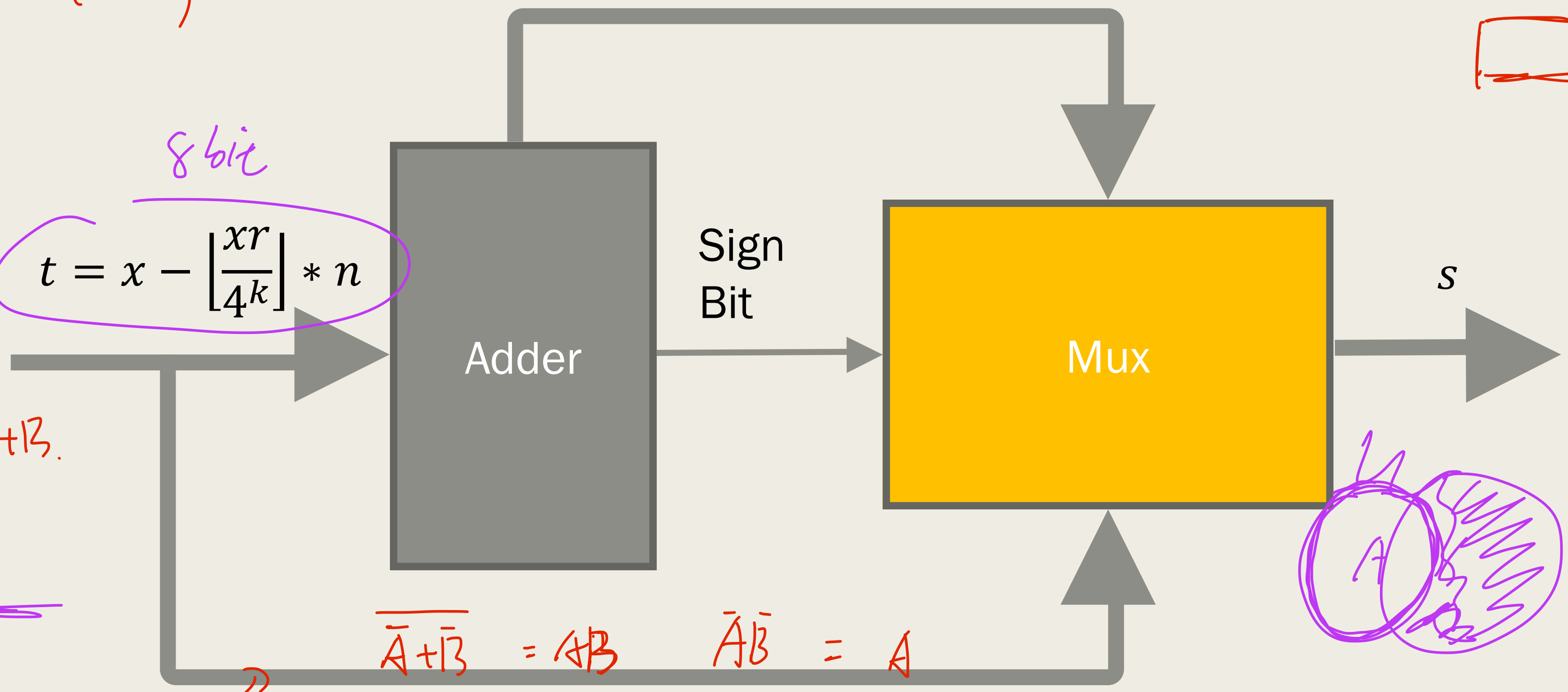
$t \geq n \rightarrow 2^{?}$

$t < n$

T[7] → (T ≥ n)

D[7]

8 bit



$\overline{A \cdot B} = \bar{A} + \bar{B}$

$\overline{\bar{A} + \bar{B}} = AB$ $\quad \bar{\bar{A}}\bar{B} = A$

T[7]

D[7]

T[7]

D[7]

t ≥ n: T[7] = 1 or (T[7] = 0 and D[7] = 0)

∴ t ≥ n: T[7] = 1 OR D[7] = 0

Layout
Block Diagram