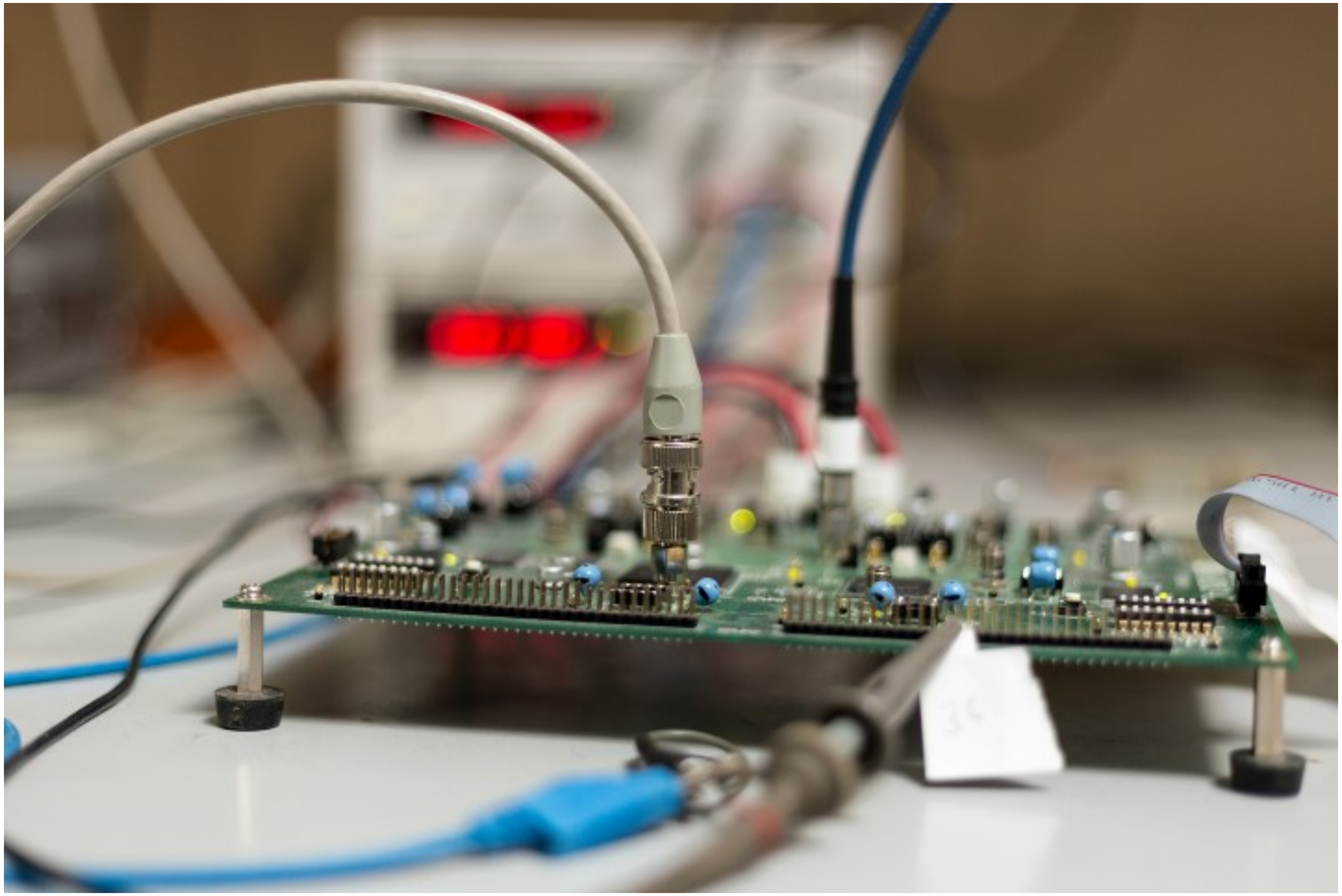
Multiplicative Masking for AES in Hardware

CHES 2018

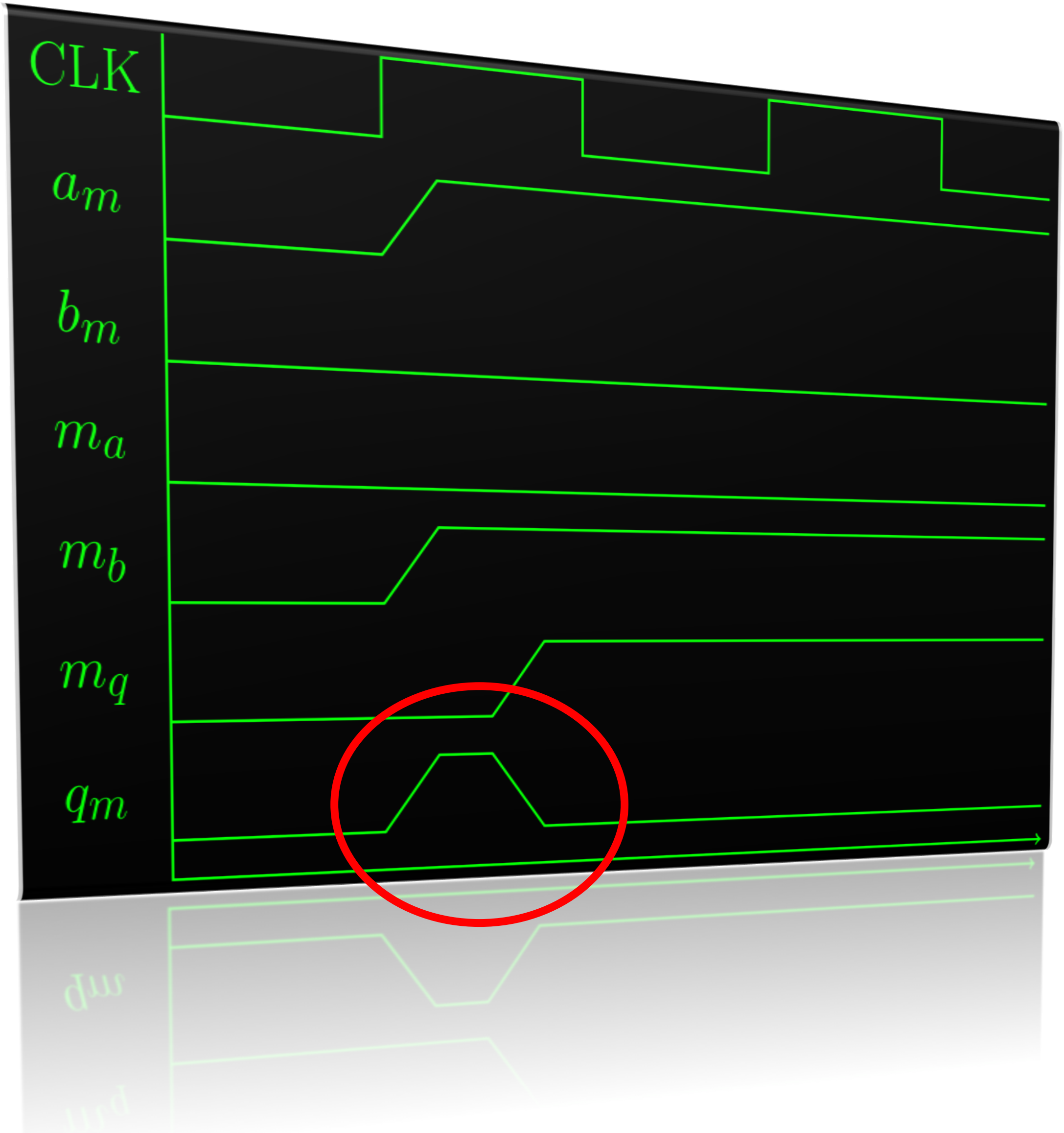
Lauren De Meyer, Oscar Reparaz, Begül Bilgin

PROBLEM: SIDE-CHANNEL ANALYSIS



SOLUTION: MASKING

EXTRA PROBLEM: GLITCHES!

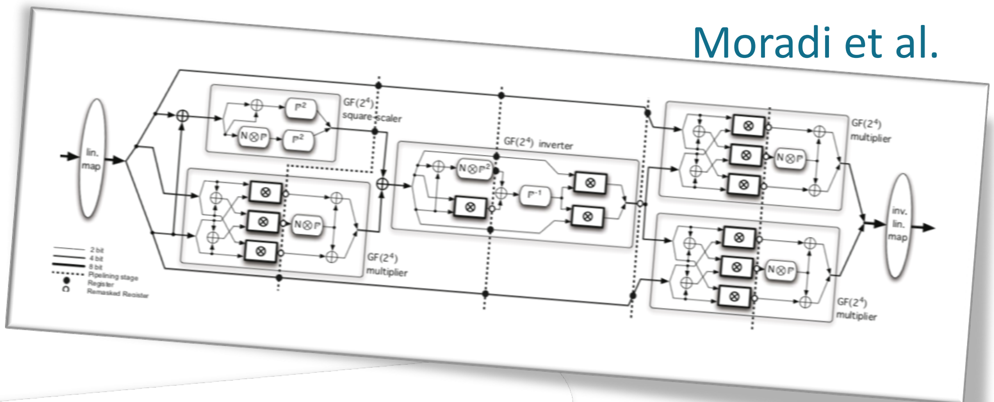


BOOLEAN MASKING

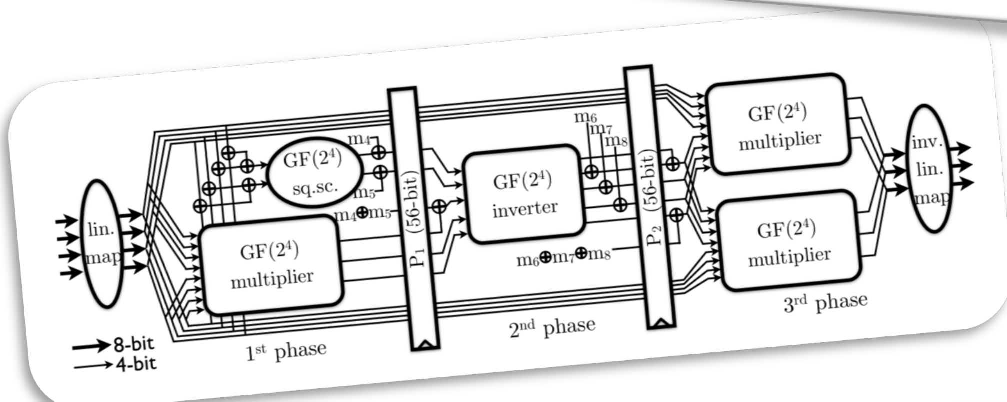
$$\boldsymbol{x} = (x_0, x_1, \dots, x_d) \Leftrightarrow x = \sum_i x_i$$

Tricky: Nonlinear functions

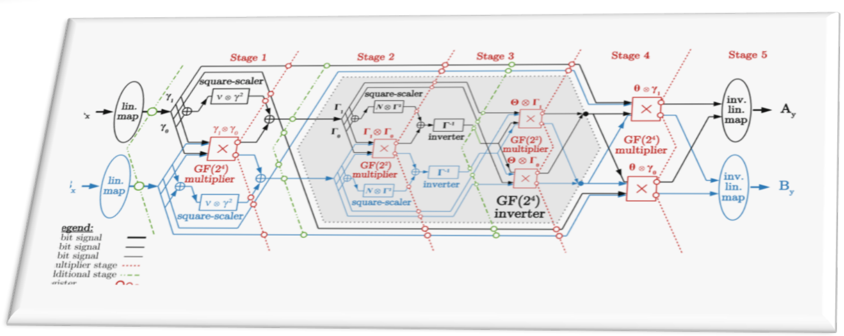
Museum of Crypto Art



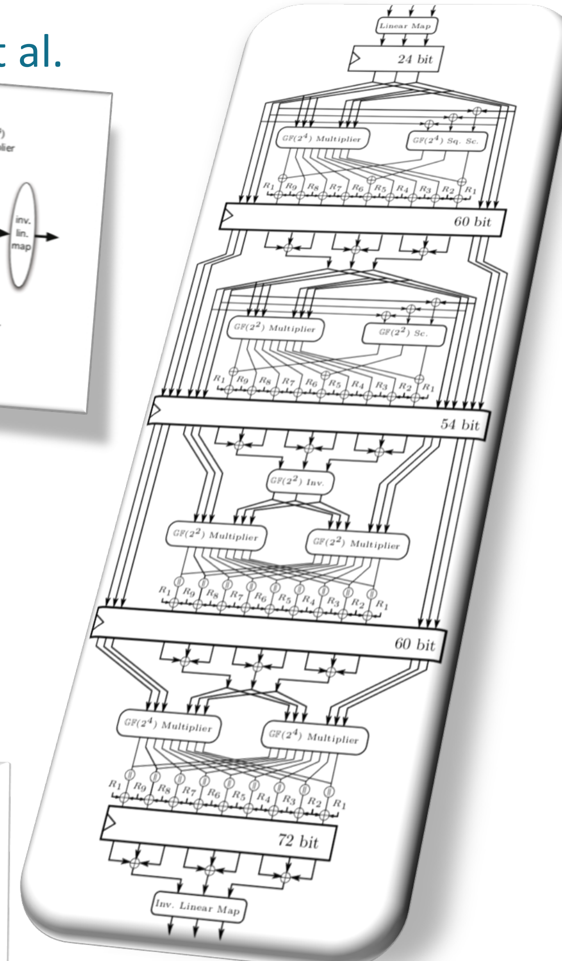
Moradi et al.



Bilgin et al.



Gross et al.



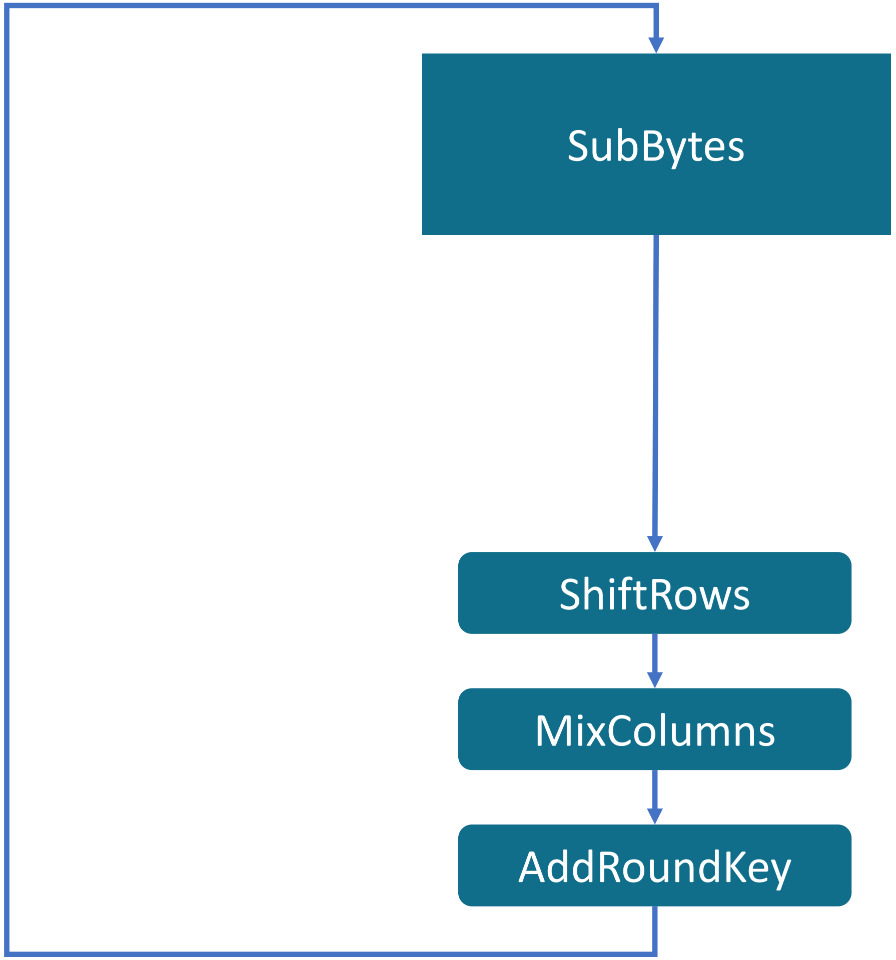
De Cnudde et al.

OUR RESULT:

	De Cnudde et al. 2016	Gross et al. 2017	This Work 2018
• 1^{st} order S-box: 0.71x	2348 GE	2432 GE	1685 GE
• 2^{nd} order S-box: 0.82x	4744 GE	4759 GE	3891 GE

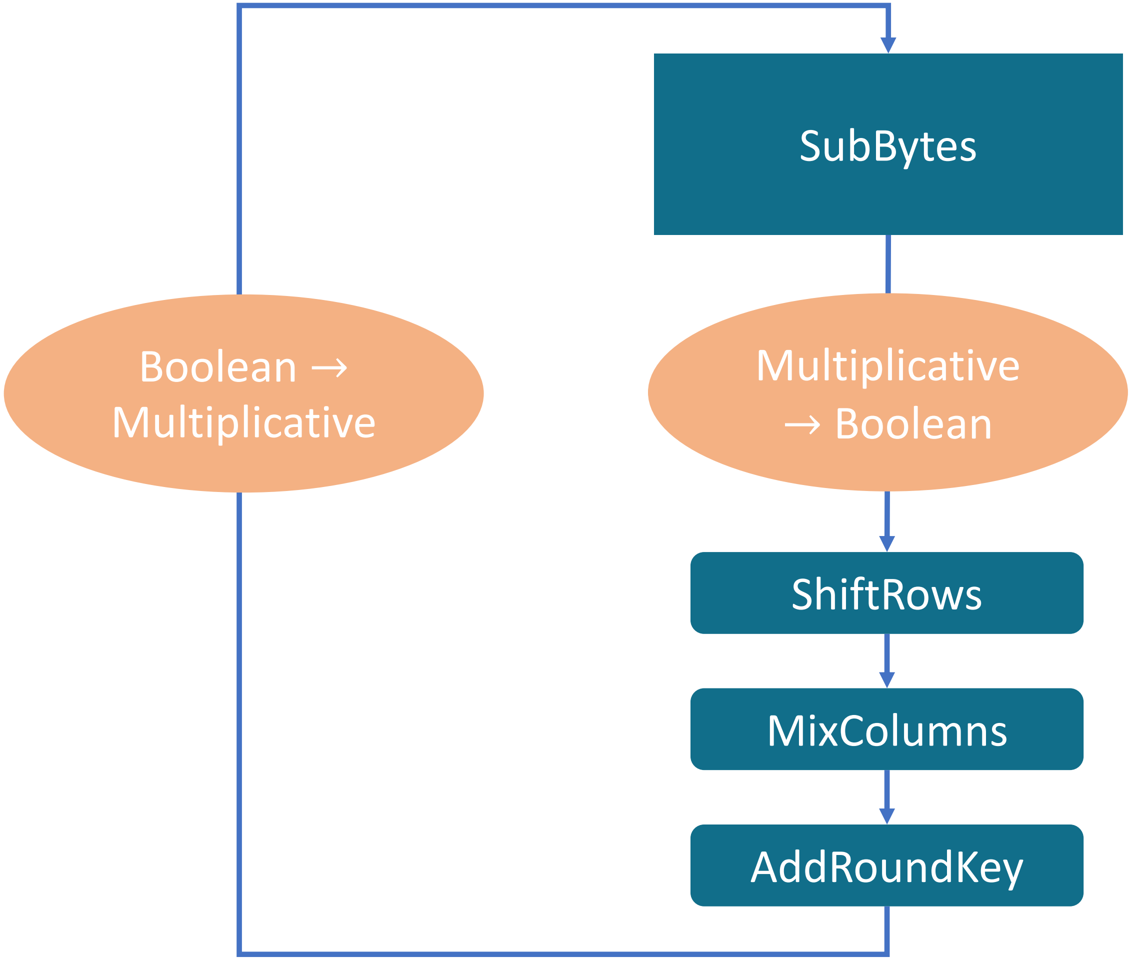
How?

BACK TO THE BEGINNING



BACK TO THE BEGINNING

Akkar-Giraud 2001



Genelle et al. 2010

PROBLEM

Akkar-Giraud 2001 $\longrightarrow$ Golić-Tymen 2002

The Zero Problem

$$\mathbf{0} = (x_0, x_1, \dots, x_d) \Leftrightarrow 0 = \prod_i x_i$$

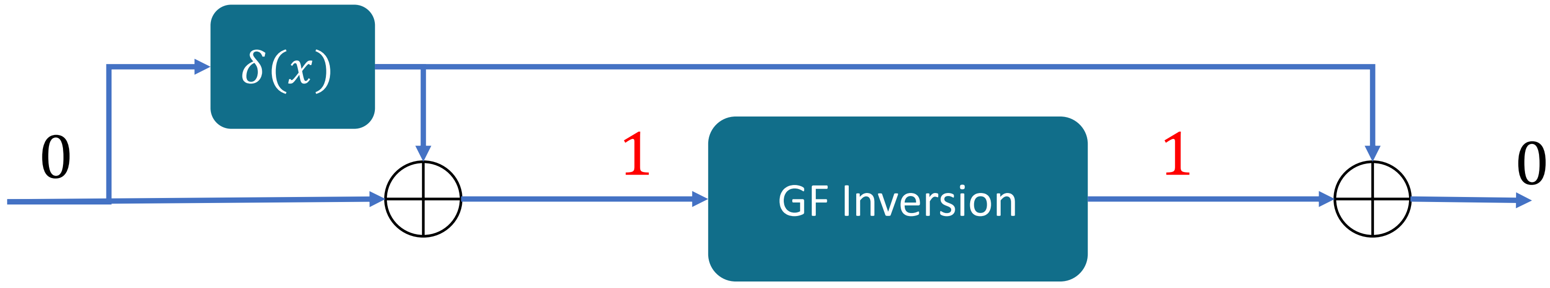
$$\downarrow$$

$$x_i = 0$$

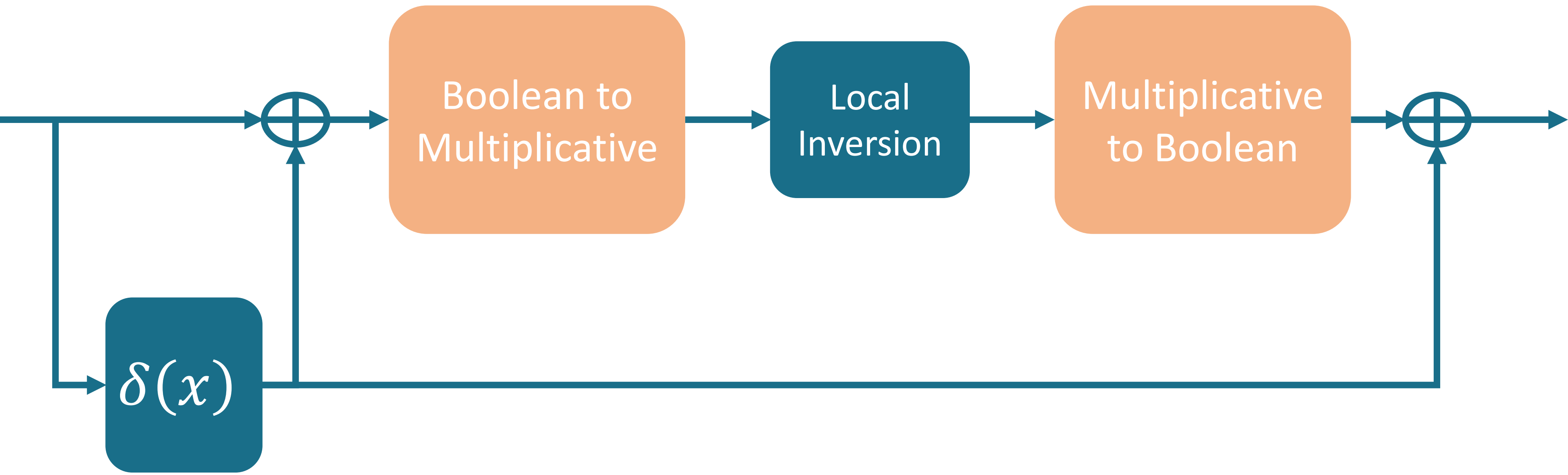
SOLUTION

Akkar-Giraud 2001 → Golić-Tymen 2002 → Damgård-Keller 2010, Genelle et al. 2010

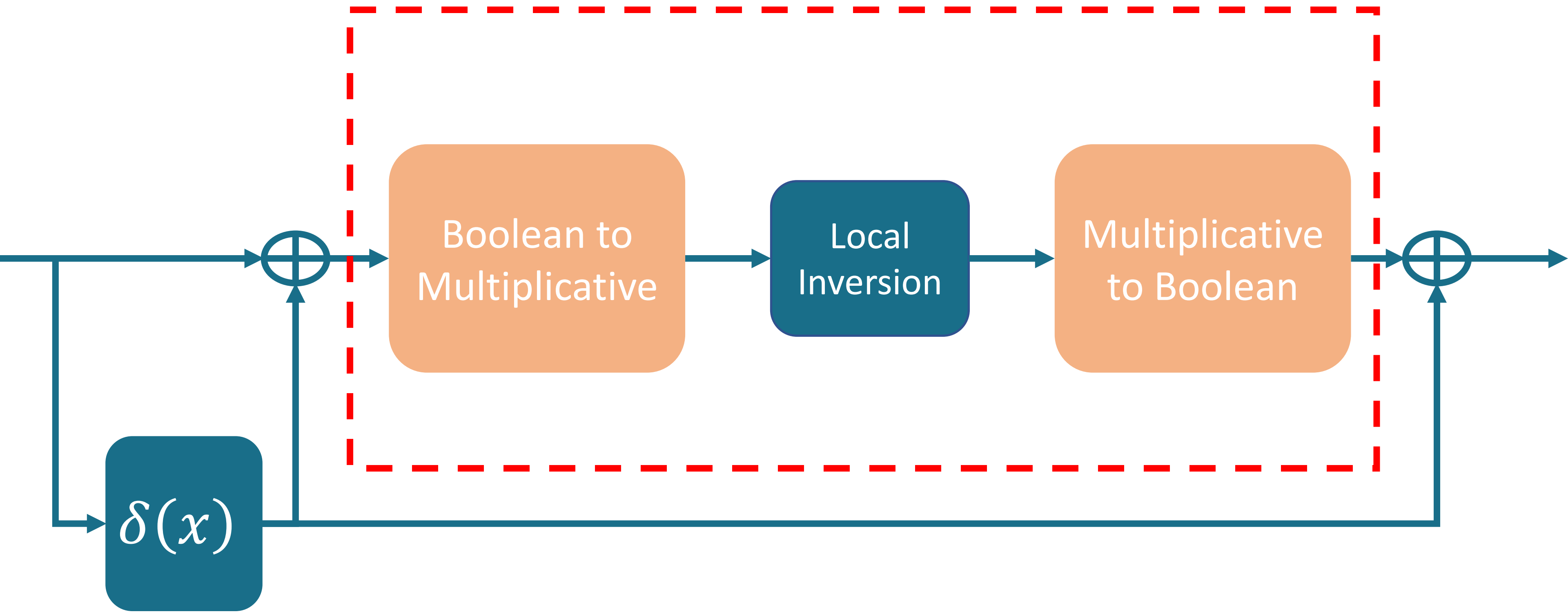
$$\delta(x) = \begin{cases} 1 & \text{if } x = 0 \\ 0 & \text{if } x \neq 0 \end{cases}$$



Masked GF Inversion



Masked GF Inversion



First-Order Masked Conversions

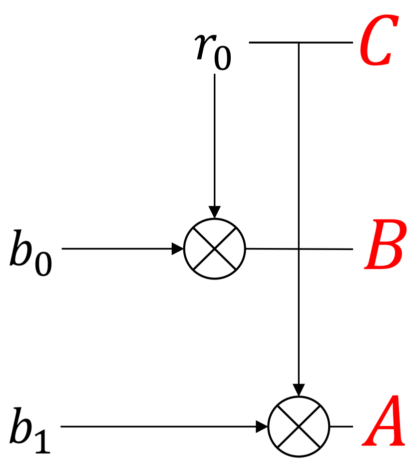
$$\boxed{x = A \oplus B}$$

b_0 —— B

b_1 —— A

First-Order Masked Conversions

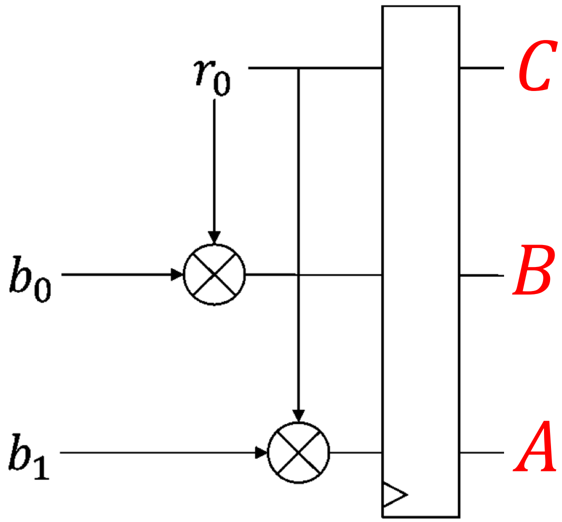
$$\boxed{x = C^{-1} \cdot (A \oplus B)}$$



1. Expansion

First-Order Masked Conversions

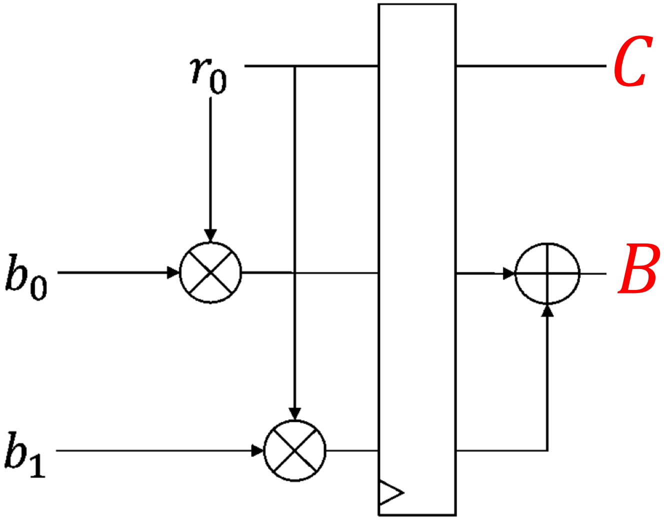
$$\boxed{x = C^{-1} \cdot (A \oplus B)}$$



2. Synchronization

FIRST-ORDER MASKED CONVERSIONS

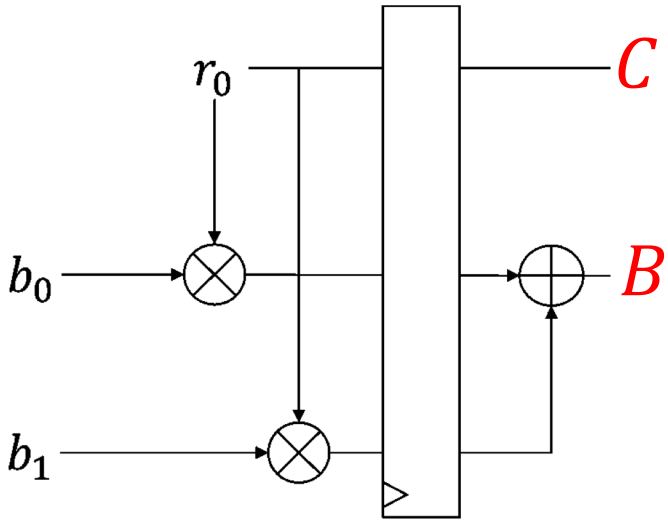
$$\boxed{x = C^{-1} \cdot B}$$



3. Compression

First-Order Masked Conversions

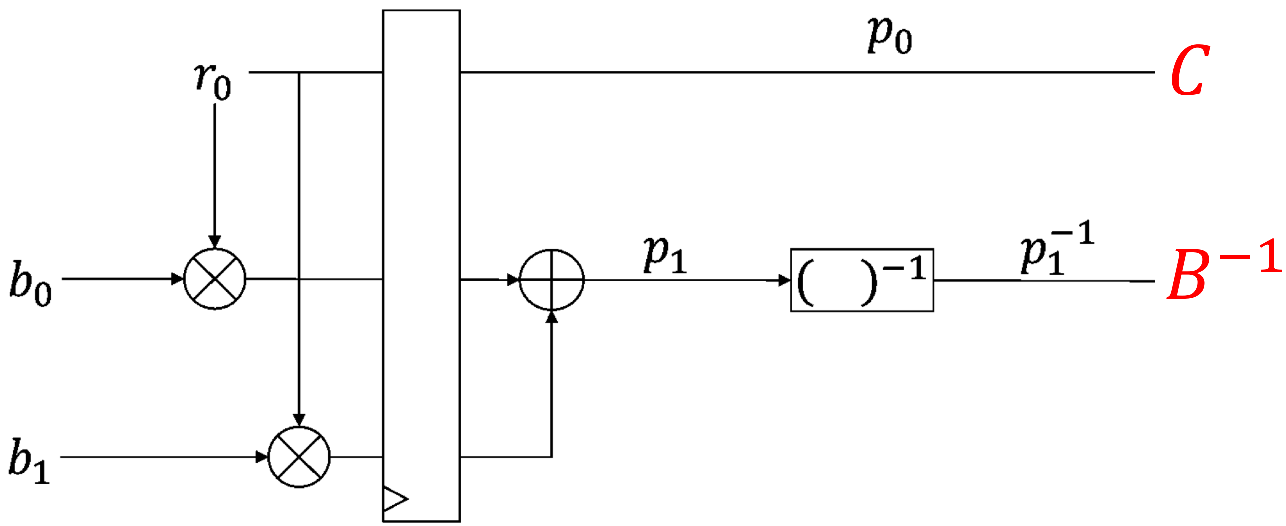
$$\boxed{x = C^{-1} \cdot B} \quad \Leftrightarrow \quad \boxed{x^{-1} = C \cdot B^{-1}}$$



3. Compression

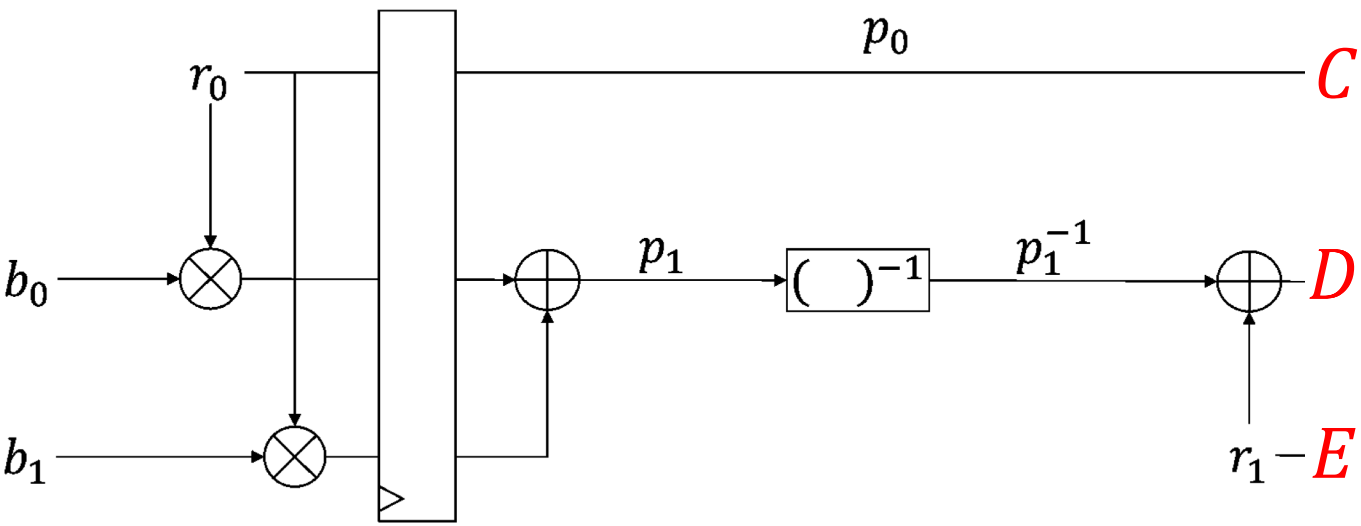
First-Order Masked Conversions

$$\boxed{x = C^{-1} \cdot B} \quad \Leftrightarrow \quad \boxed{x^{-1} = C \cdot B^{-1}}$$



First-Order Masked Conversions

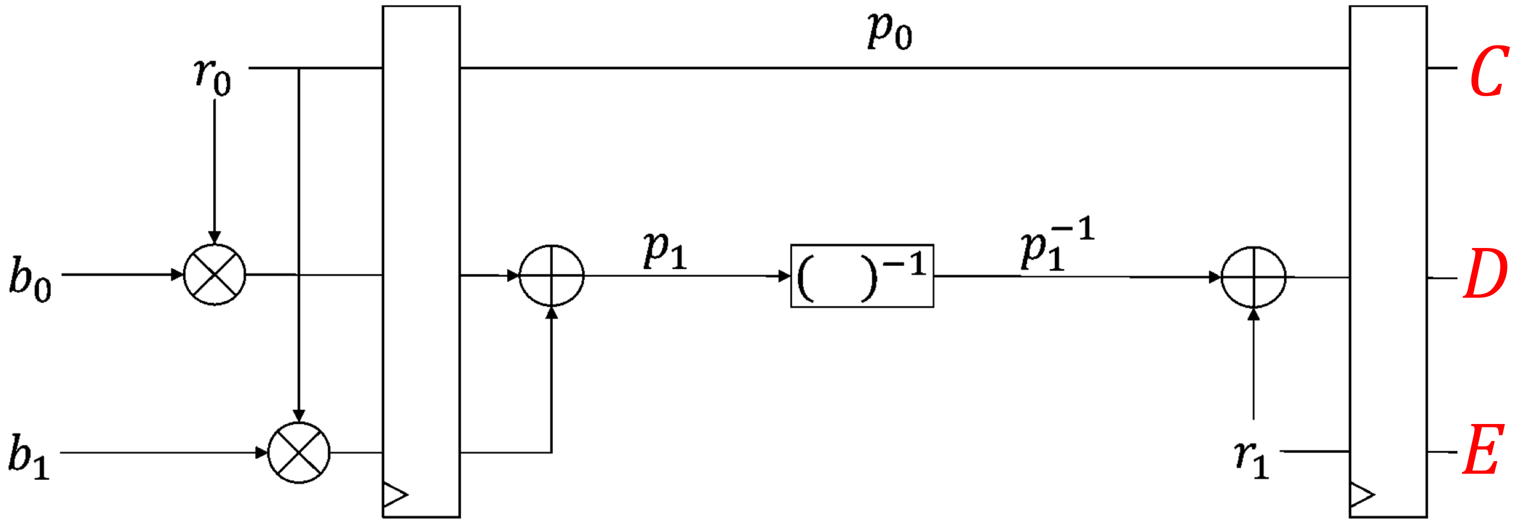
$$\boxed{x^{-1} = C \cdot (D \oplus E)}$$



1. Expansion

First-Order Masked Conversions

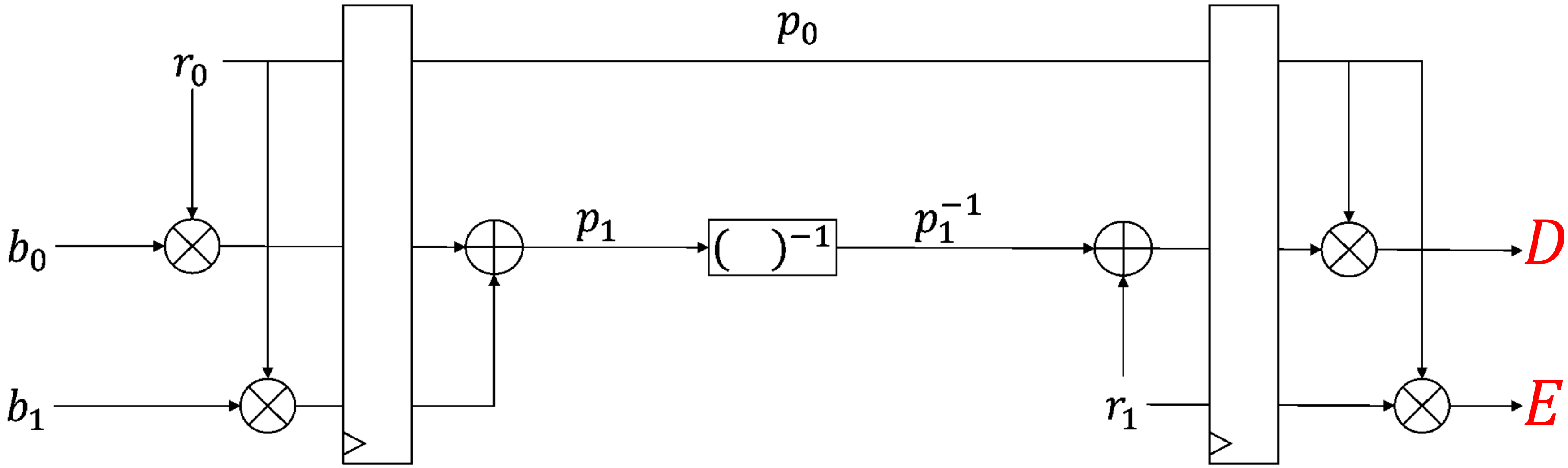
$$\boxed{x^{-1} = C \cdot (D \oplus E)}$$



2. Synchronization

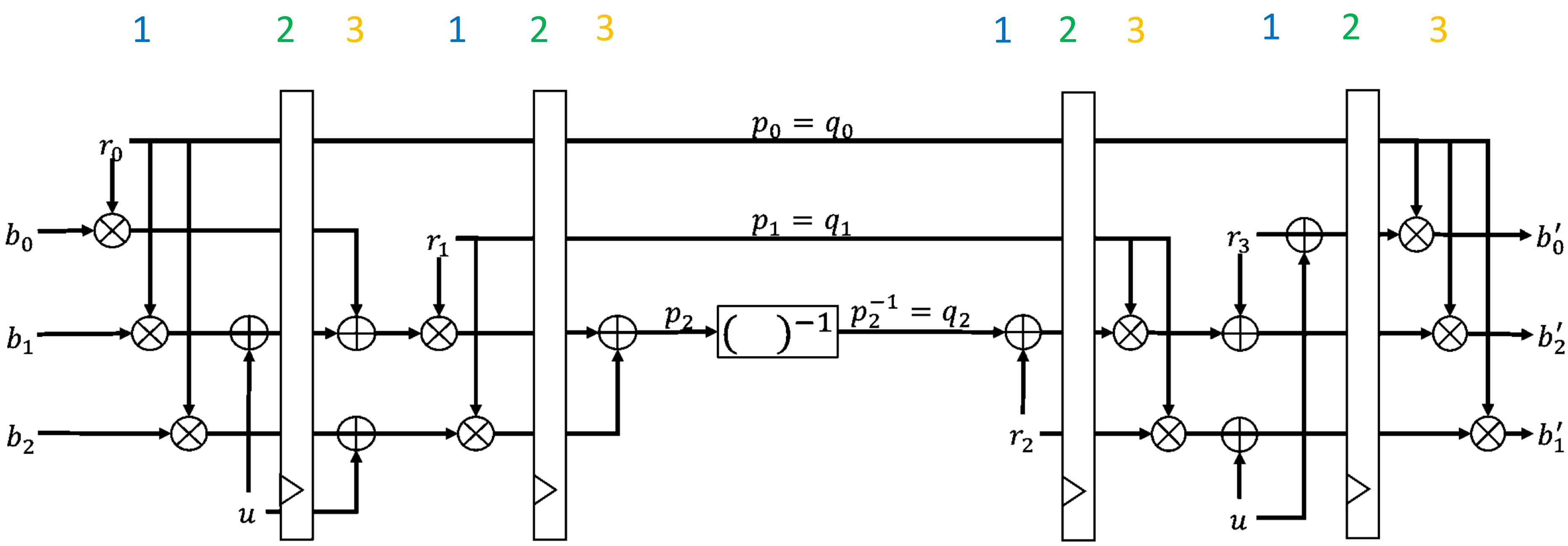
First-Order Masked Conversions

$$\boxed{x^{-1} = D \oplus E}$$

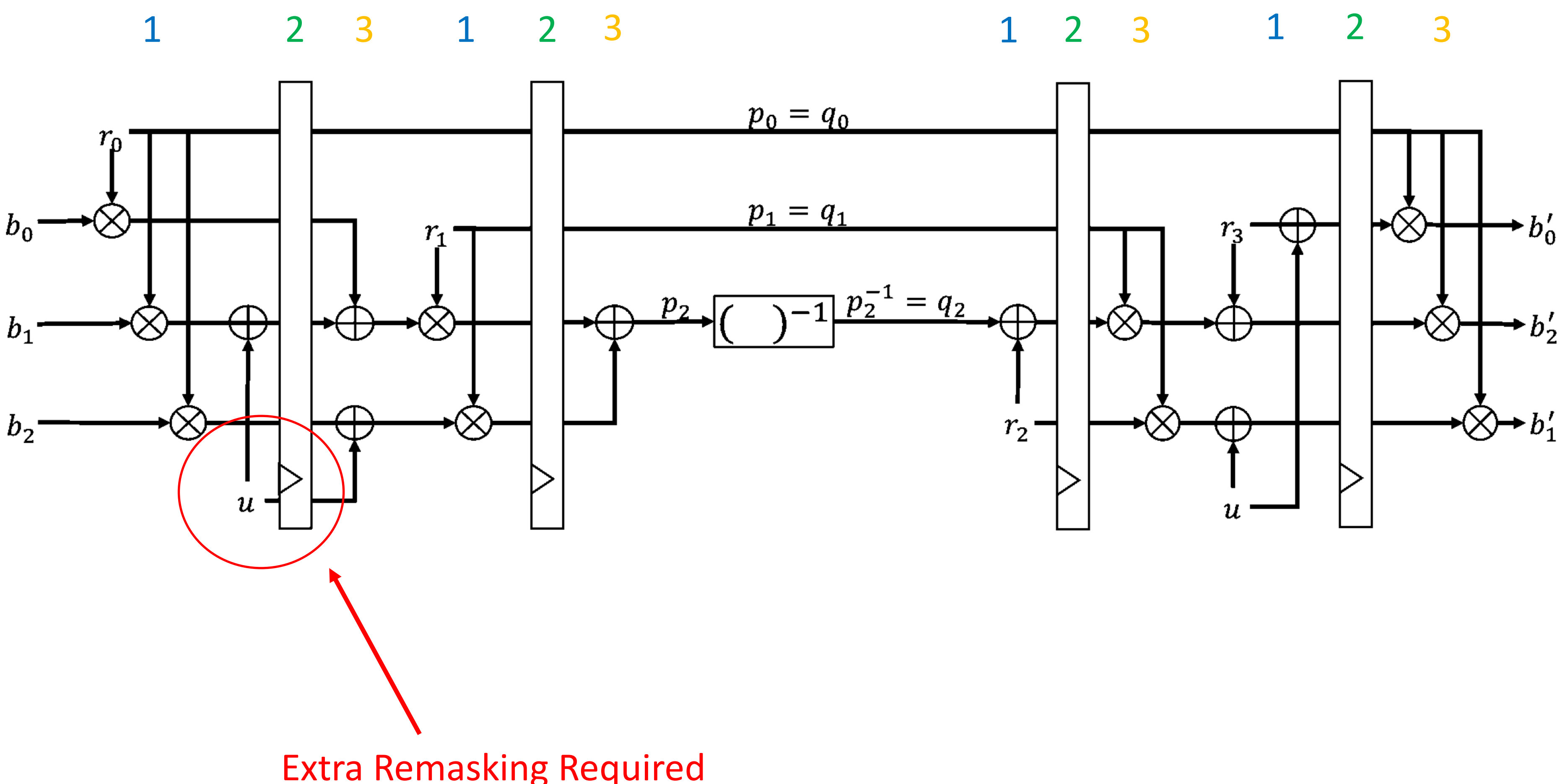


3. Compression

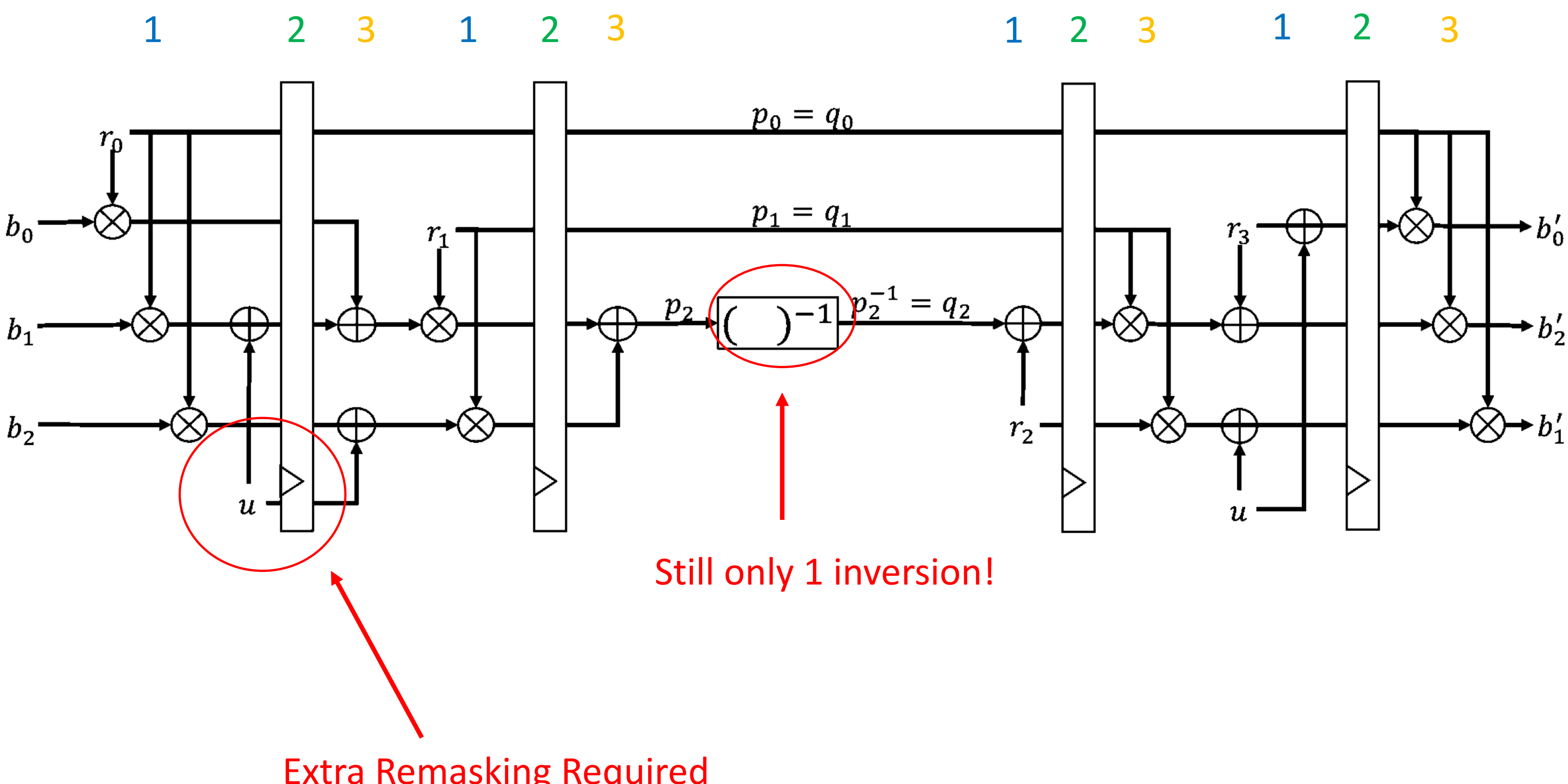
Second-Order Masked Conversions



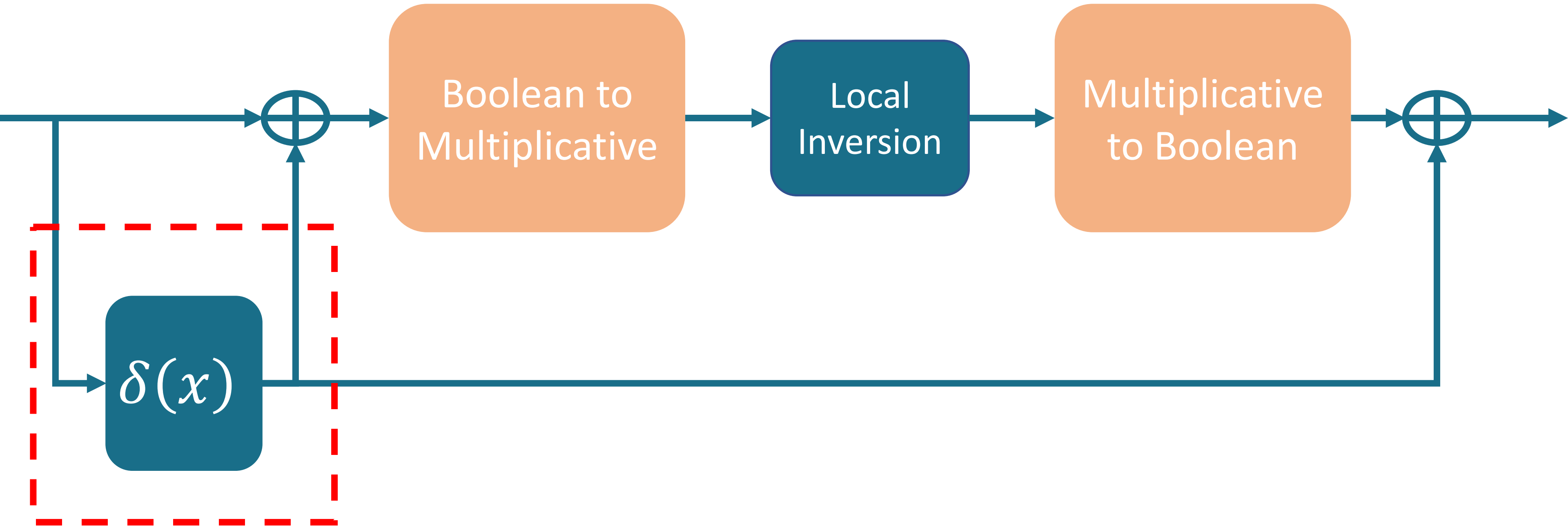
SECOND-ORDER MASKED CONVERSIONS



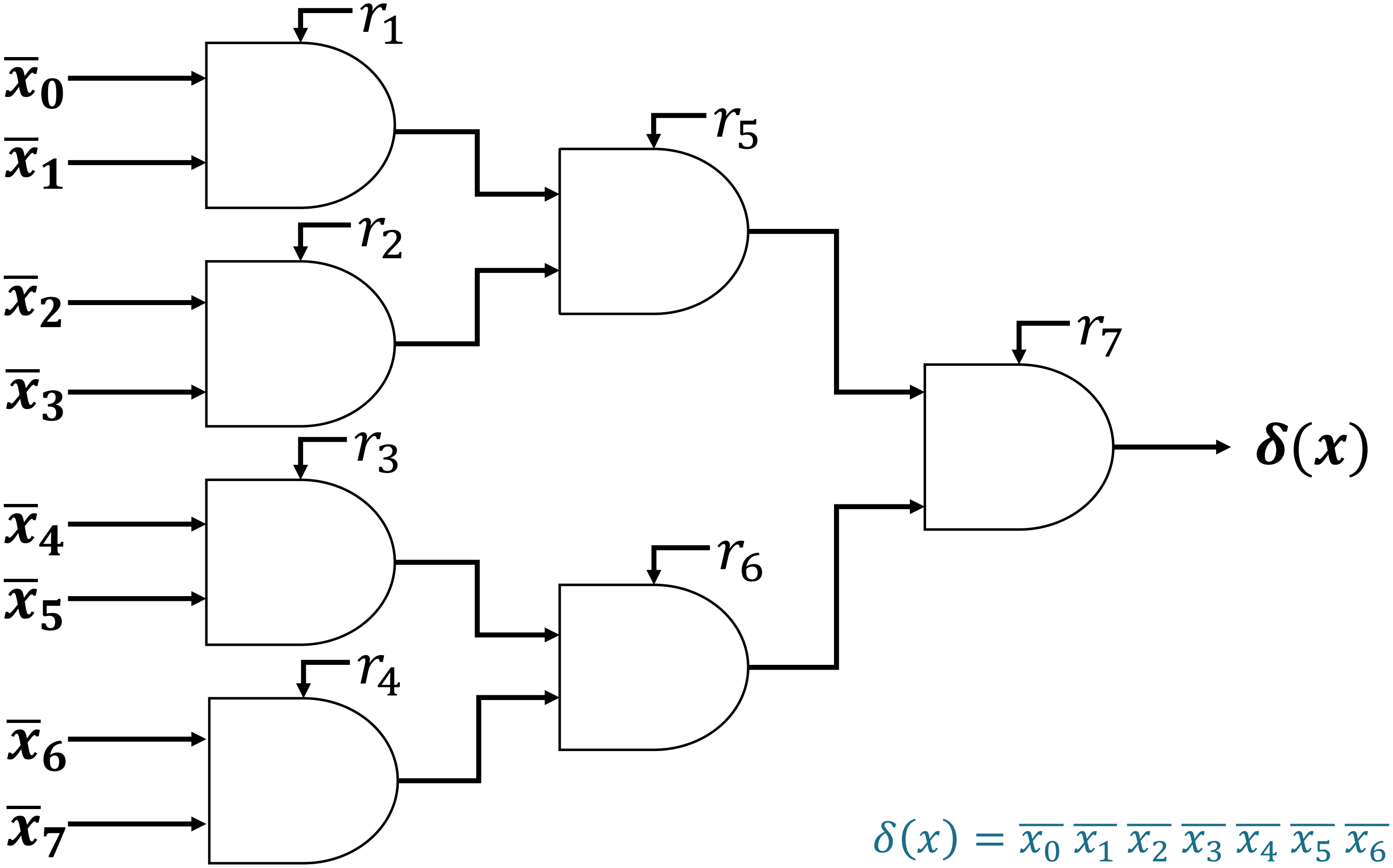
SECOND-ORDER MASKED CONVERSIONS



MASKED GF INVERSION

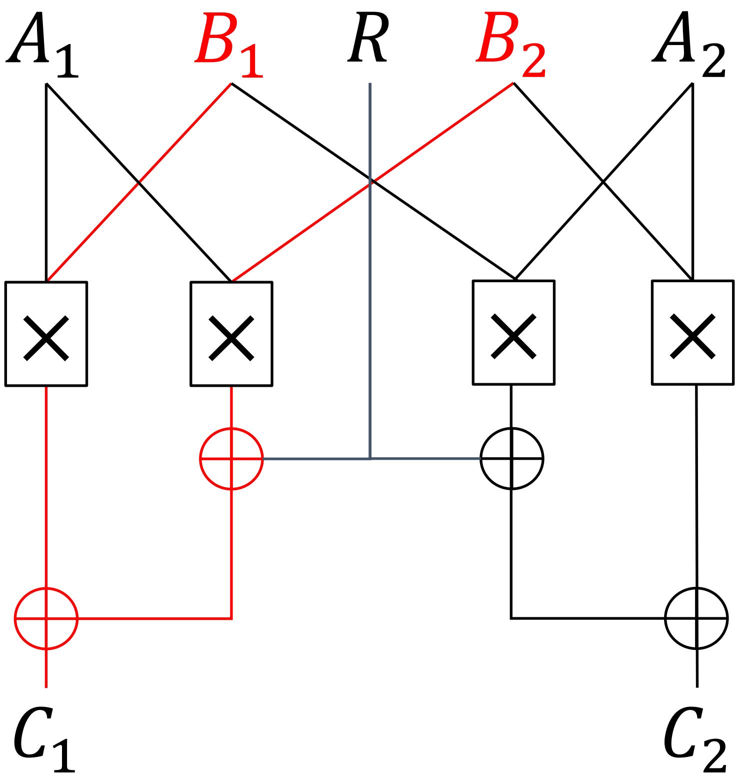


Masked Kronecker Delta



$$\delta(x) = \overline{x_0}\,\overline{x_1}\,\overline{x_2}\,\overline{x_3}\,\overline{x_4}\,\overline{x_5}\,\overline{x_6}\,\overline{x_7}$$

AN INTERESTING OBSERVATION

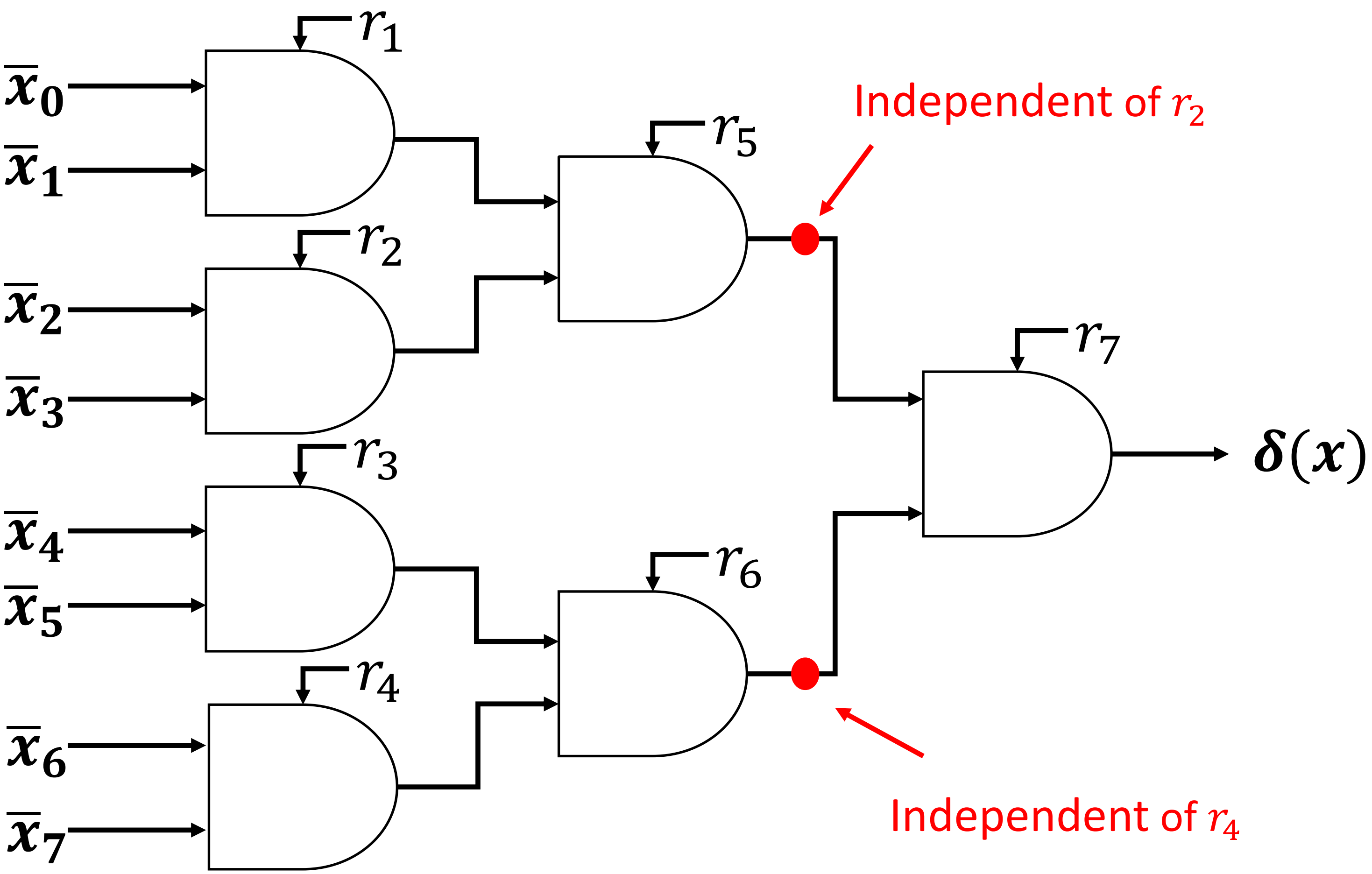


$$C_1 = A_1 B_1 \oplus A_1 B_2 \oplus R$$
$$= A_1 B \oplus R$$

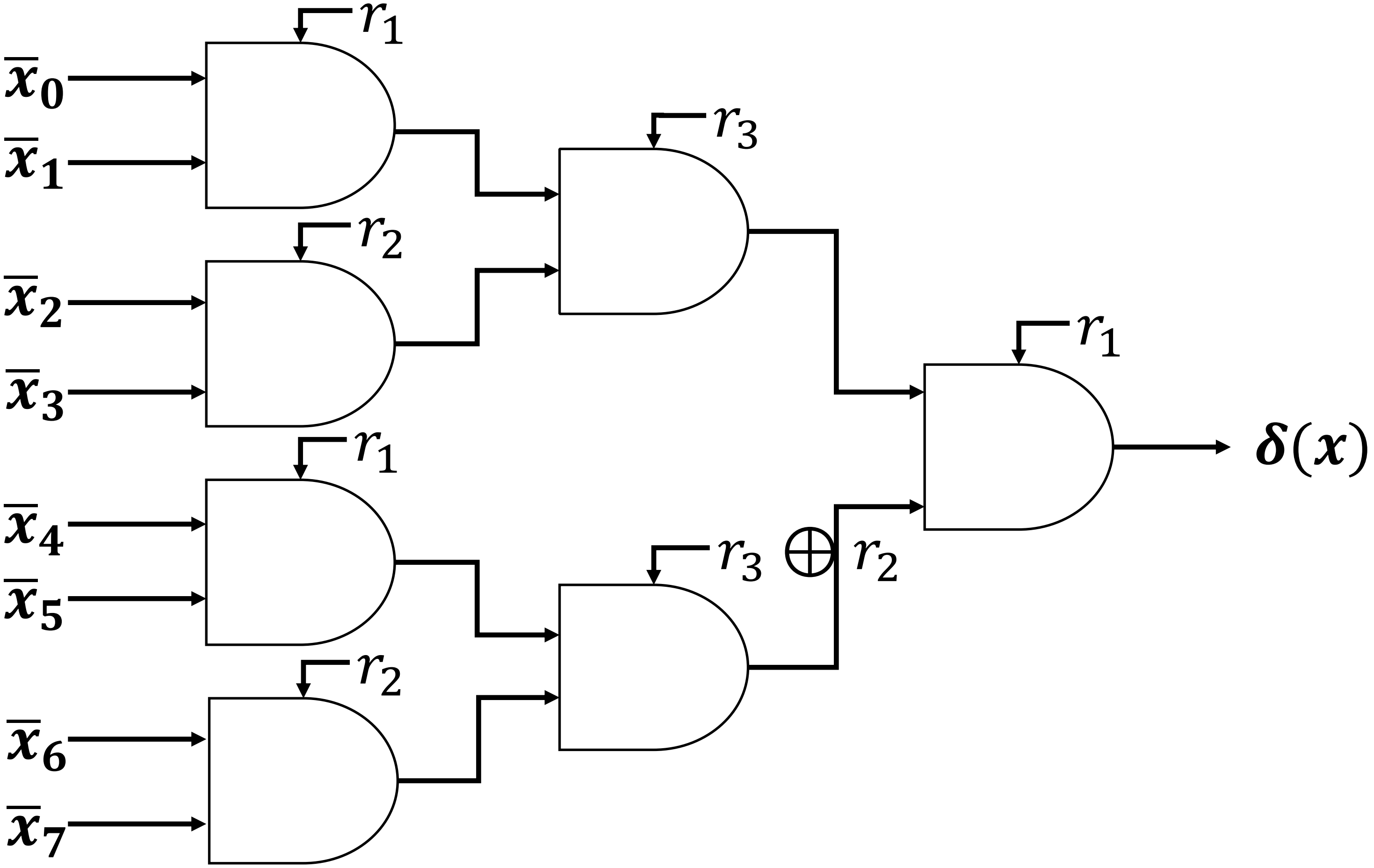
$$C_2 = A_2 B \oplus R$$

Gross et al. 2016

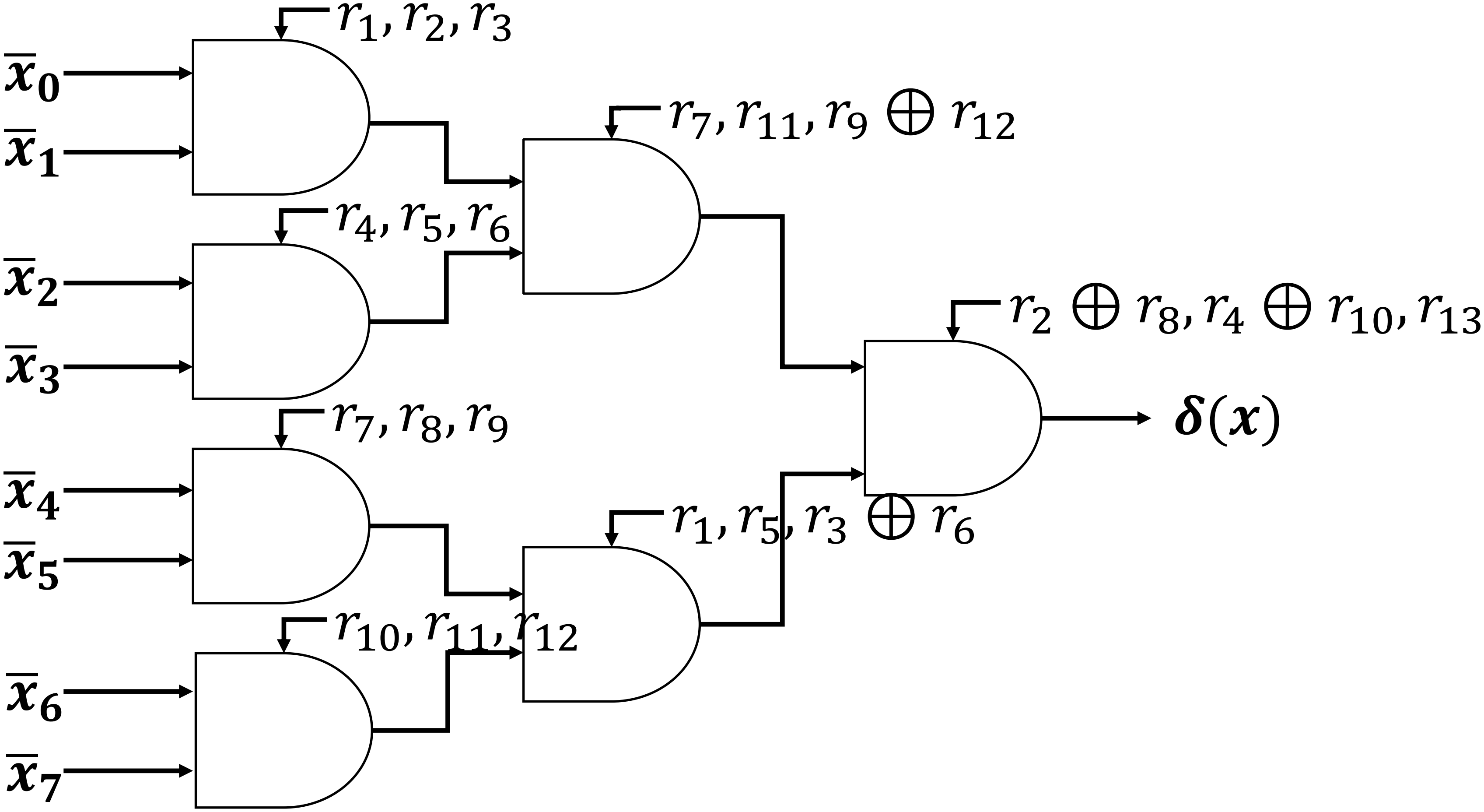
Masked Kronecker Delta



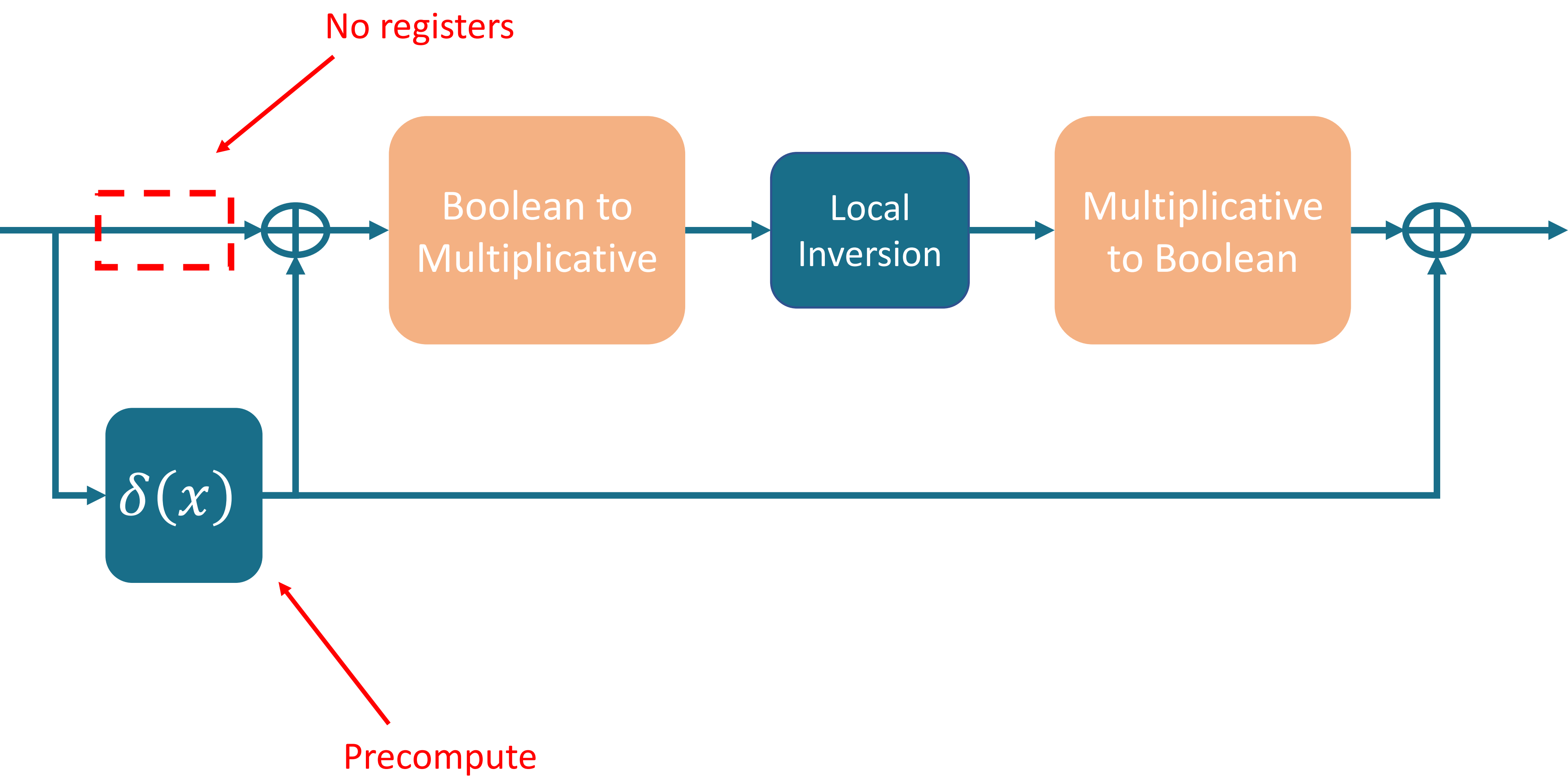
MASKED KRONECKER DELTA



MASKED KRONECKER DELTA



Masked GF Inversion



RESULTS

S-BOX AREA

	De Cnudde et al. 2016	Gross et al. 2017	This Work 2018
1st order: 0.71x	2348 GE	2432 GE	1685 GE
2nd order: 0.82x	4744 GE	4759 GE	3891 GE

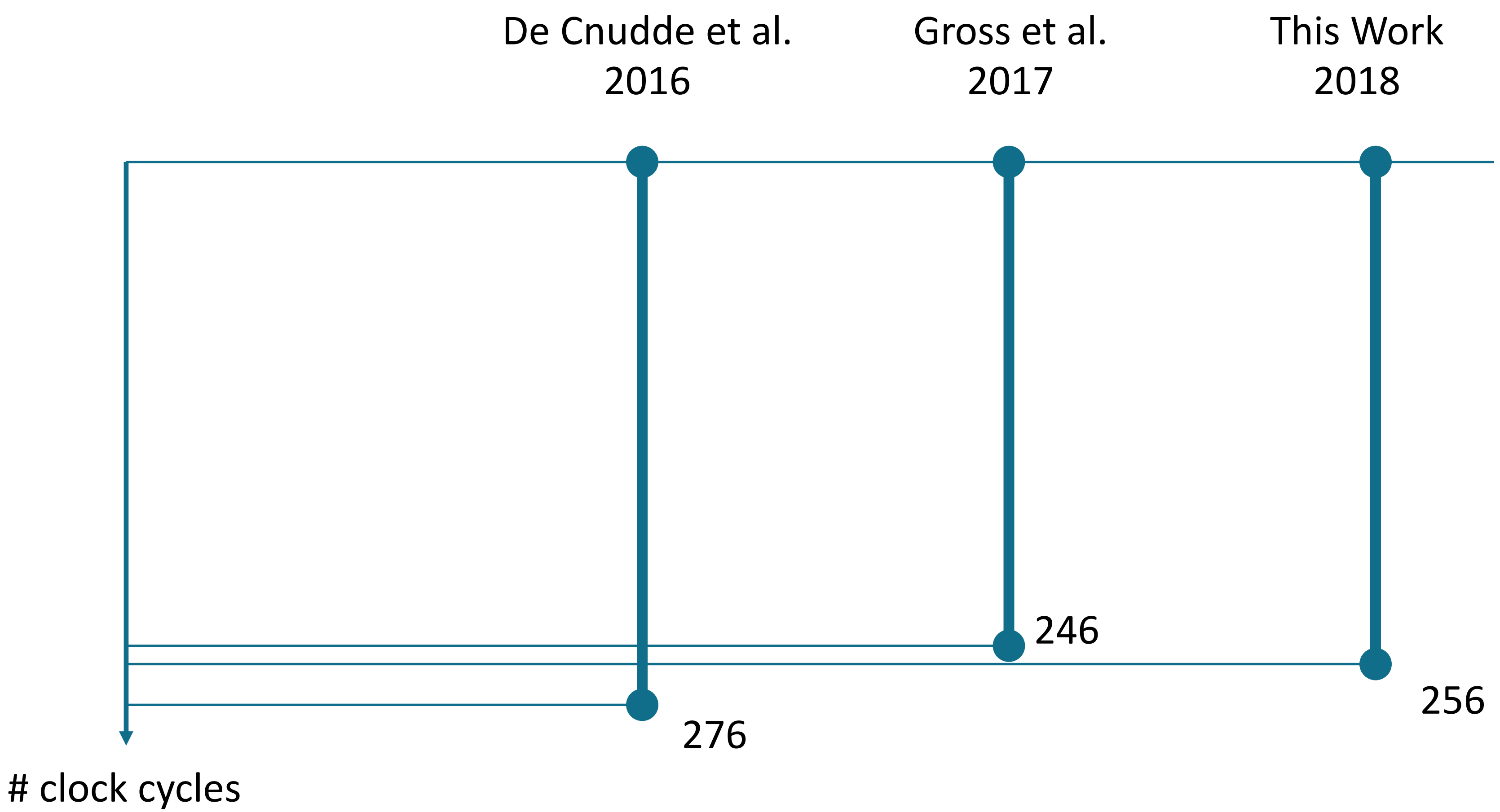
AES Area

	De Cnudde et al. 2016	Gross et al. 2017	This Work 2018
• 1st order: 0.89x	7682 GE	7337 GE	6557 GE
• 2nd order: 0.91x	12640 GE	12024 GE	10931 GE

Randomness Per S-box

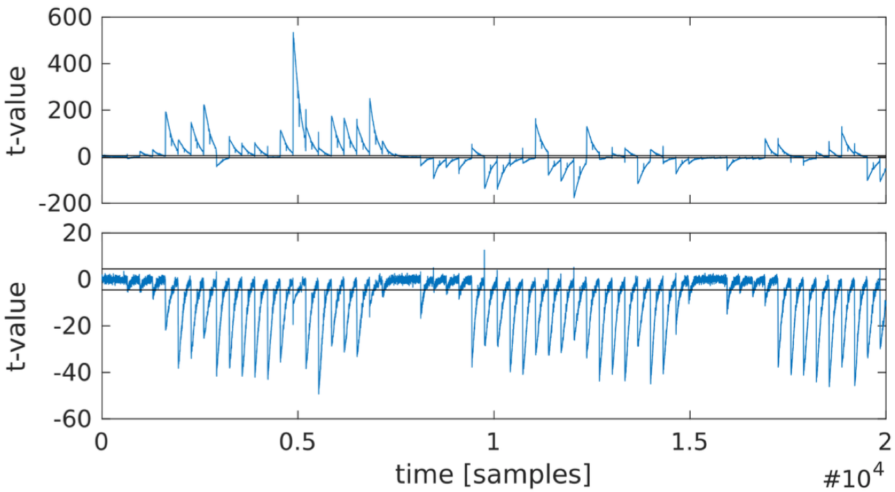
	De Cnudde et al. 2016	Gross et al. 2017	This Work 2018
• 1^{st} order:	54	18	19
• 2^{nd} order:	162	54	53

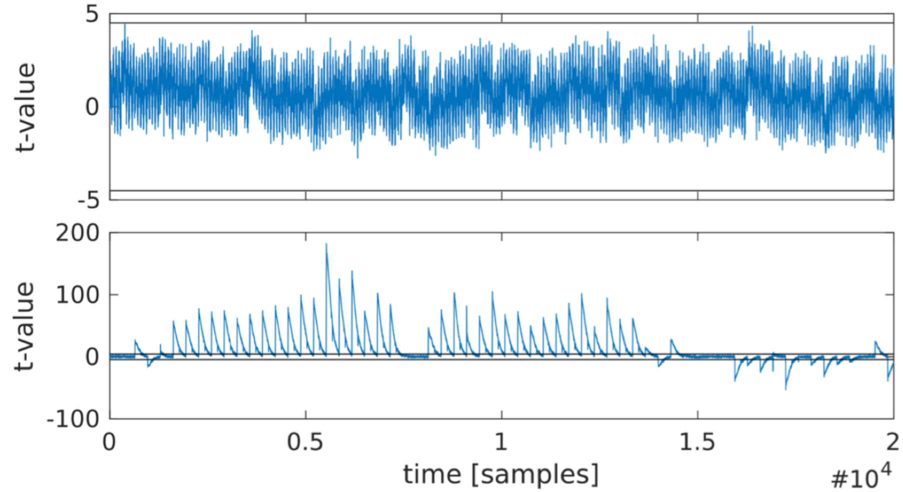
Latency Per Encryption



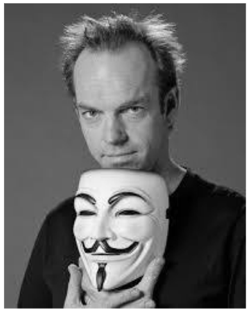
TVLA: 1ST ORDER AES

First Order



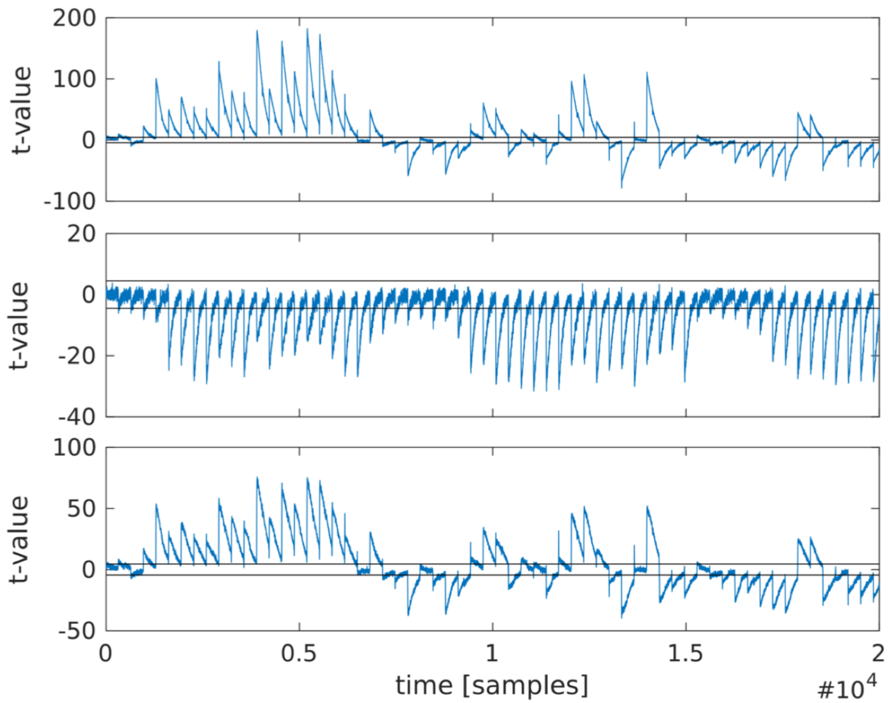


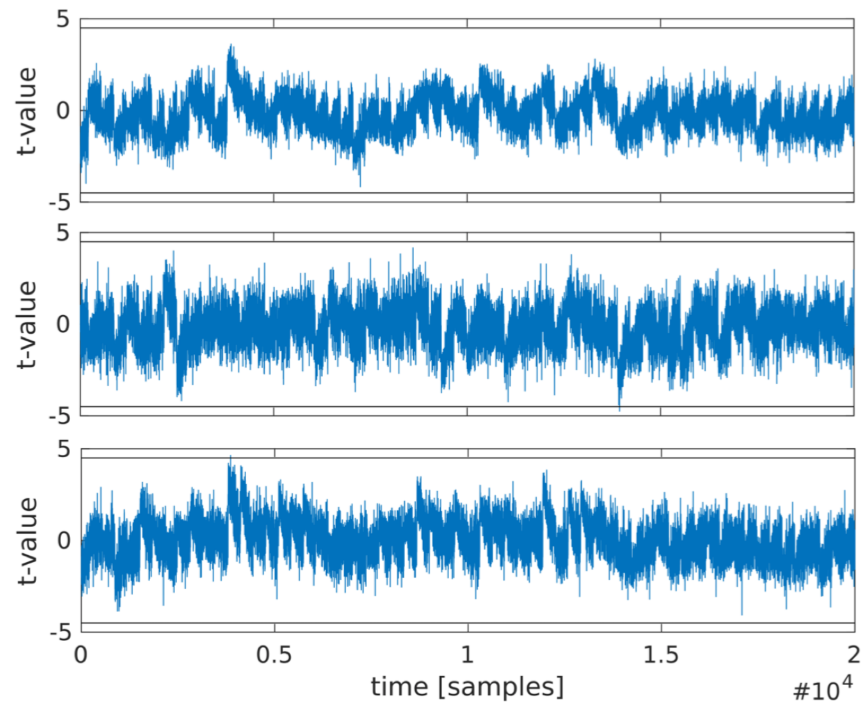
Second Order



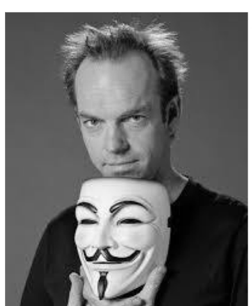
TVLA: 2^{ND} ORDER AES

First Order

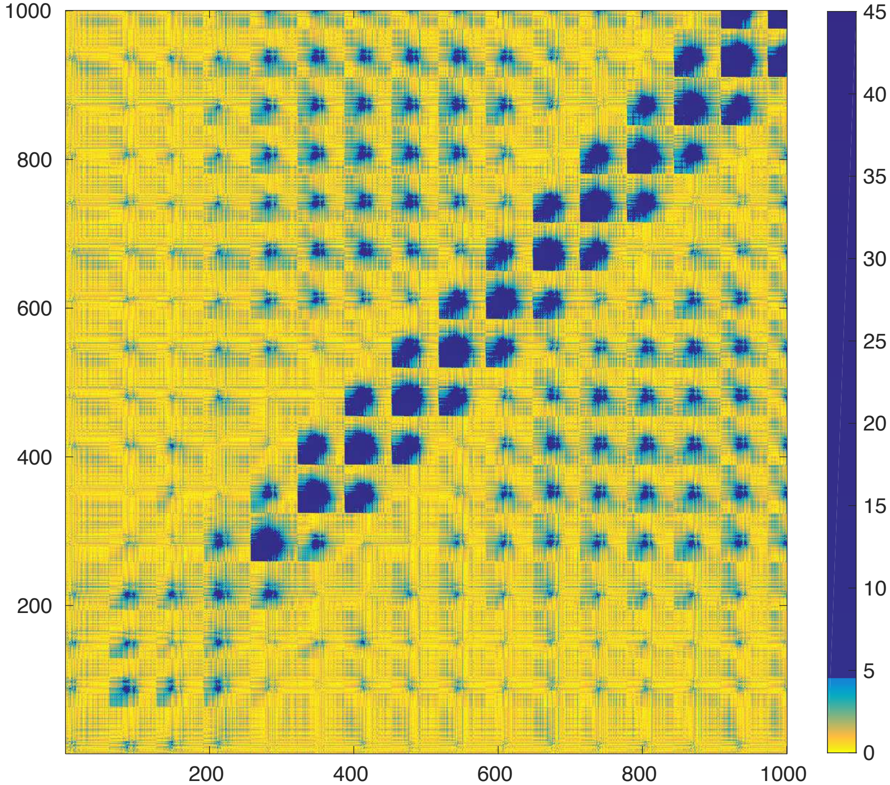


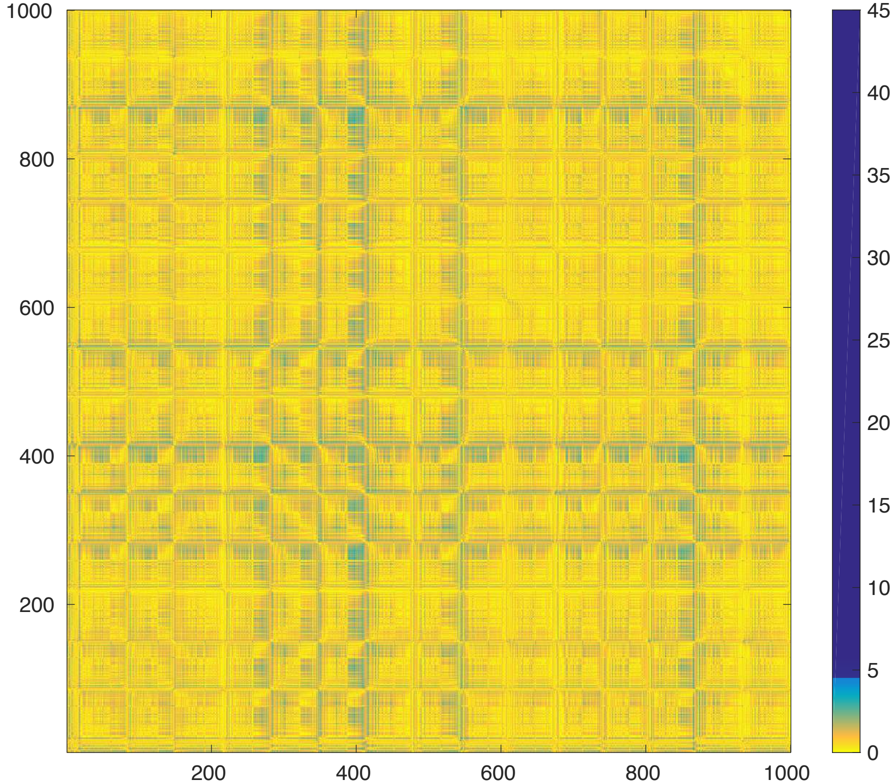


Third Order



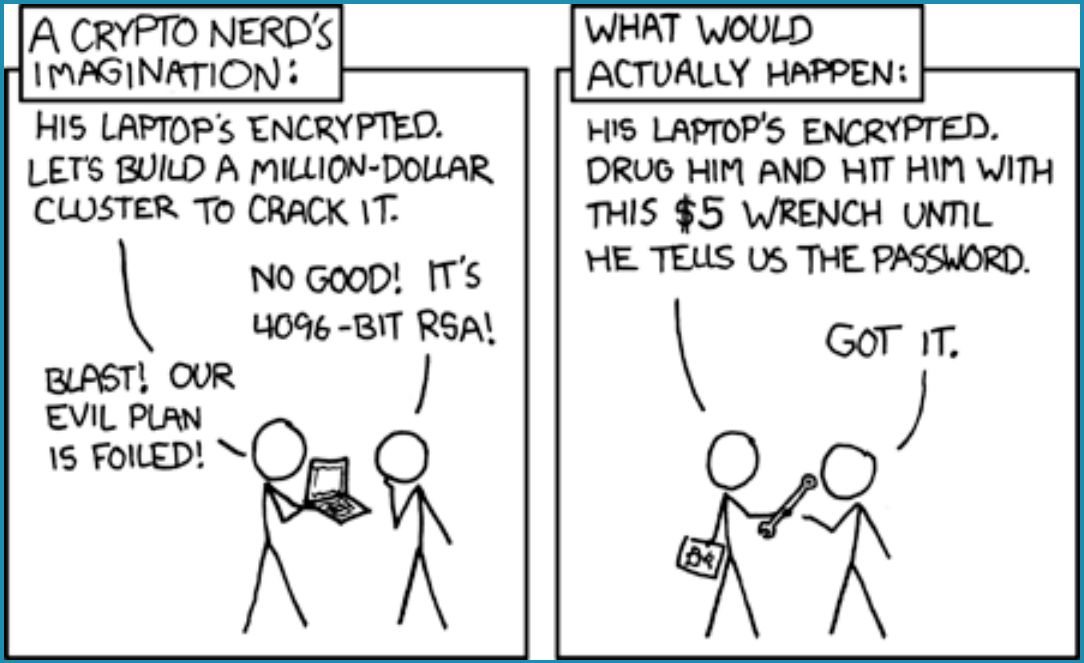
TVLA: Bivariate





Take-Away

- ✓ Keep it Simple ☺
- ✓ Find inspiration in early works
- ✓ Push the limits:
  - ✓ Reuse Randomness
  - ✓ Customize!



Thank You

KU LEUVEN