DOM-LOLA

Generic Low-Latency Masking

Hannes Groß, Rinat Iusupov, Roderick Bloem

LOLA

Q: „Can we securely evaluate complex masked functions in a single clock cycle?"

LOLA

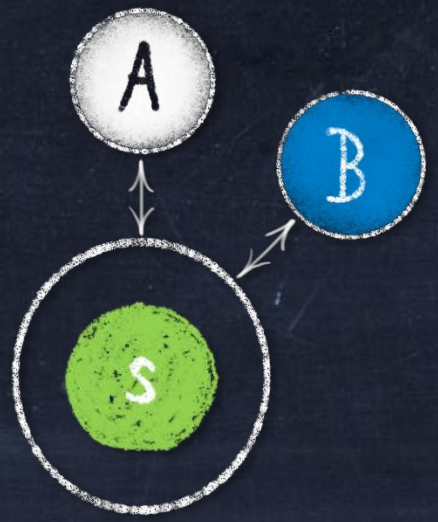
Q: „Does higher-order masking require online randomness?"

BUT...

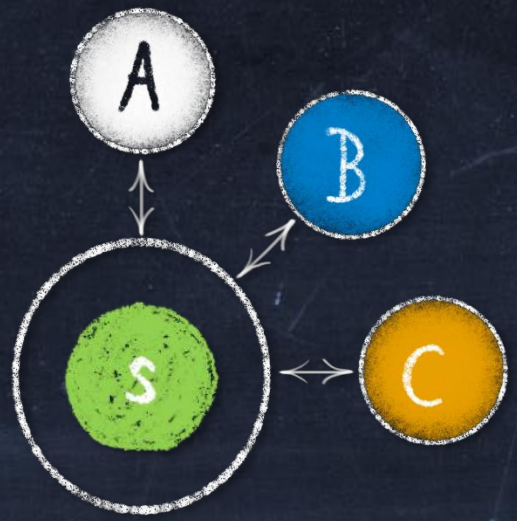
Masking

Masking

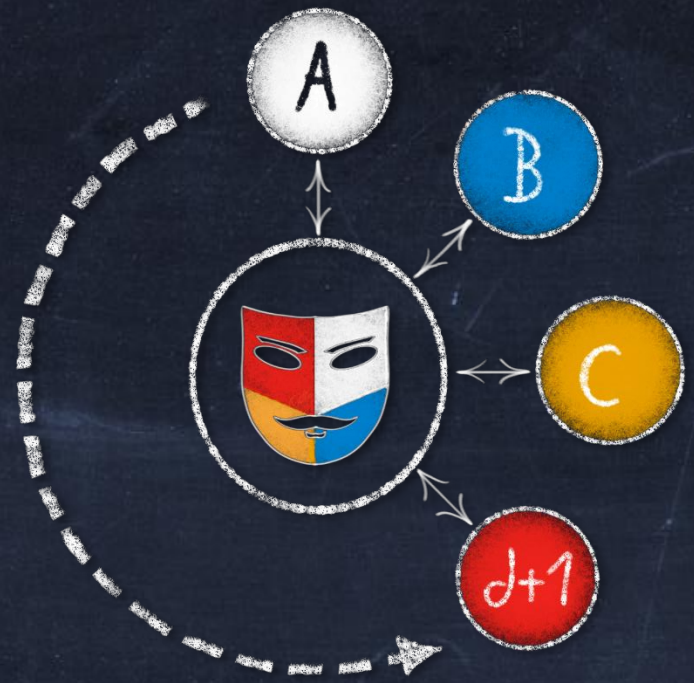
Masking



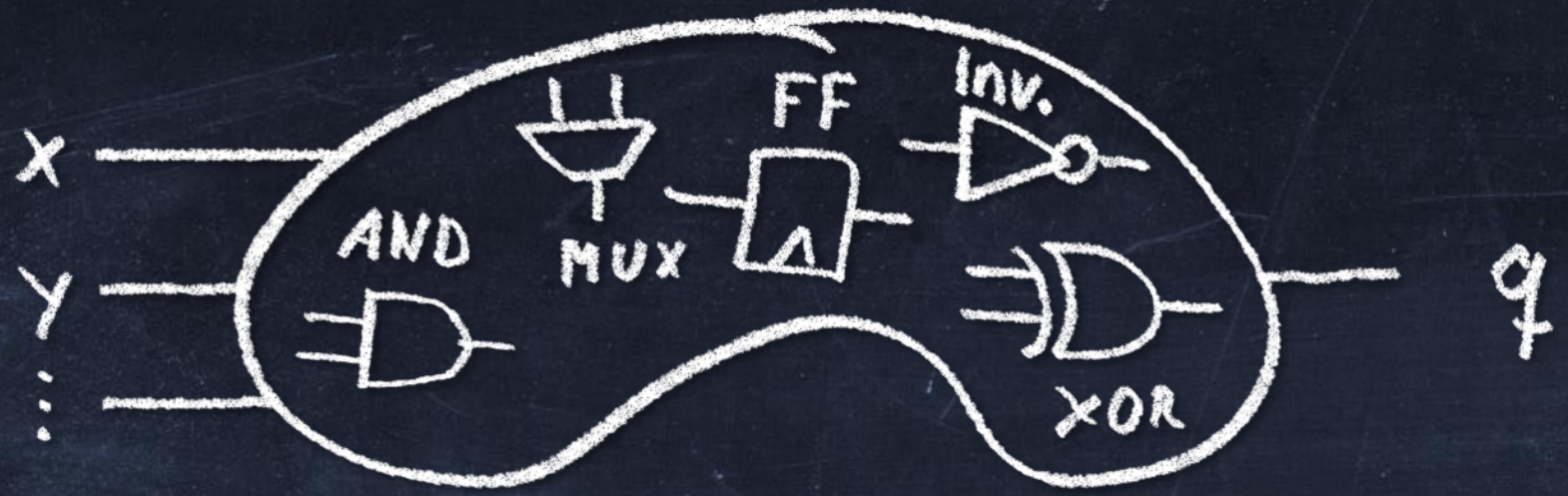
Masking



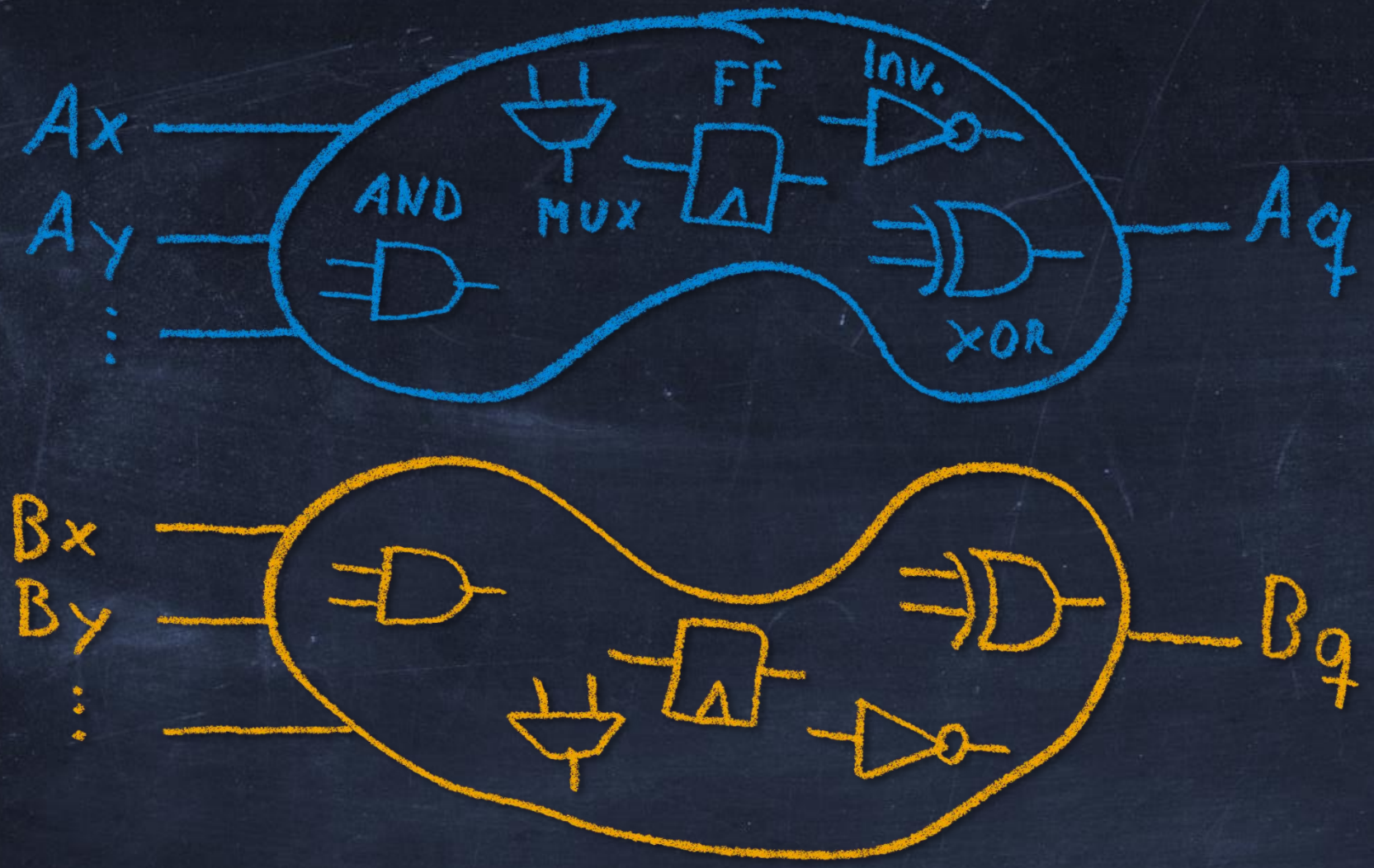
Masking



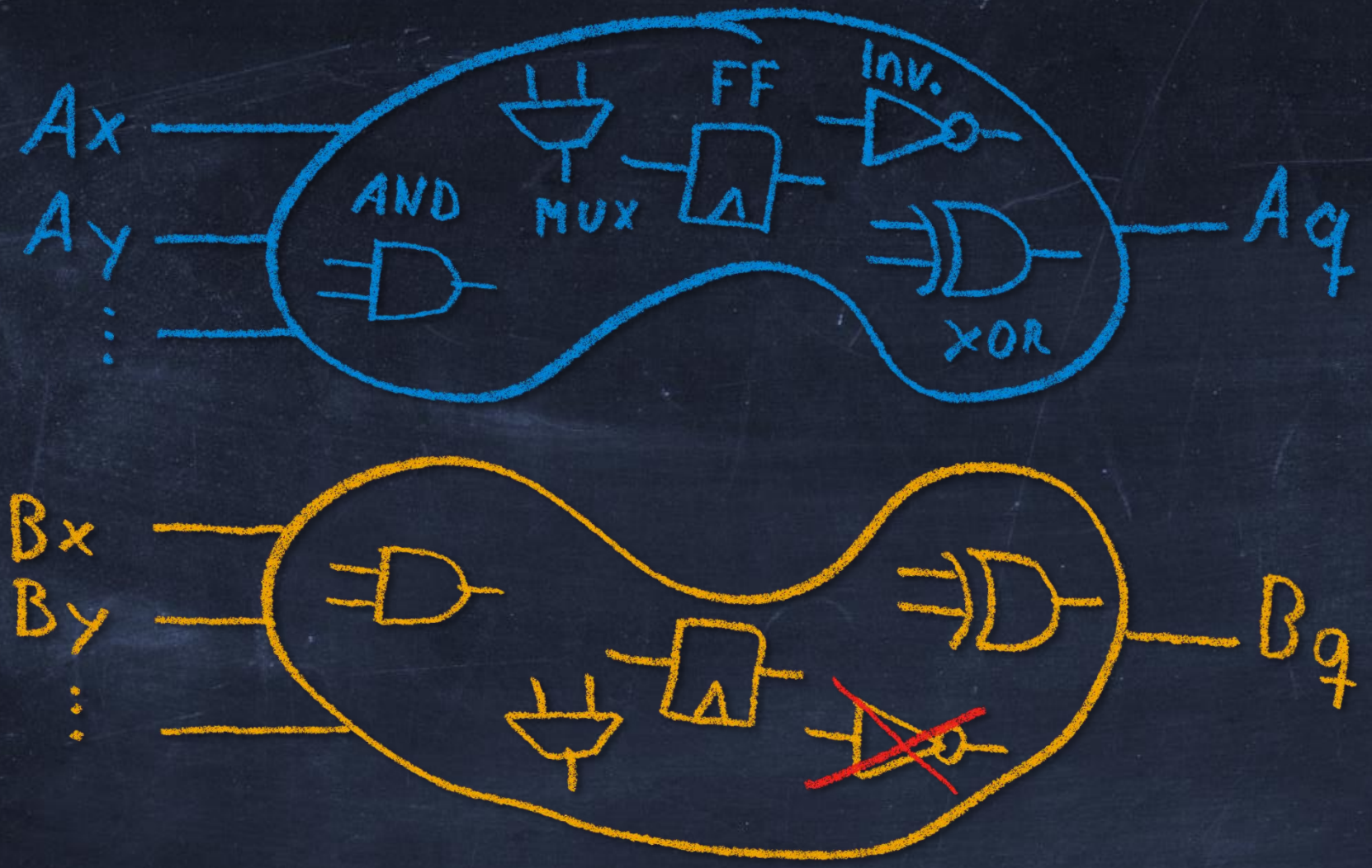
DOM



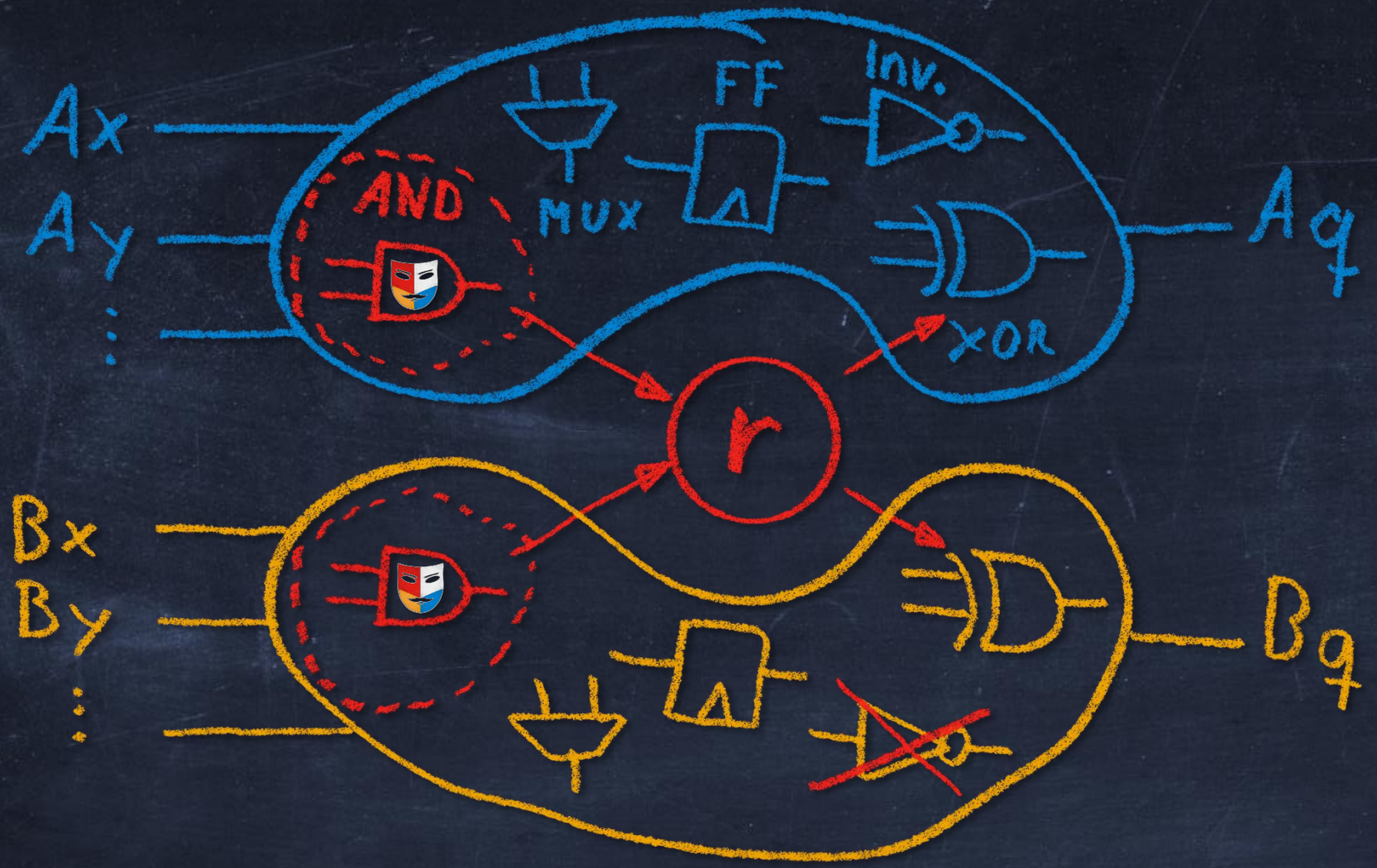
DOM



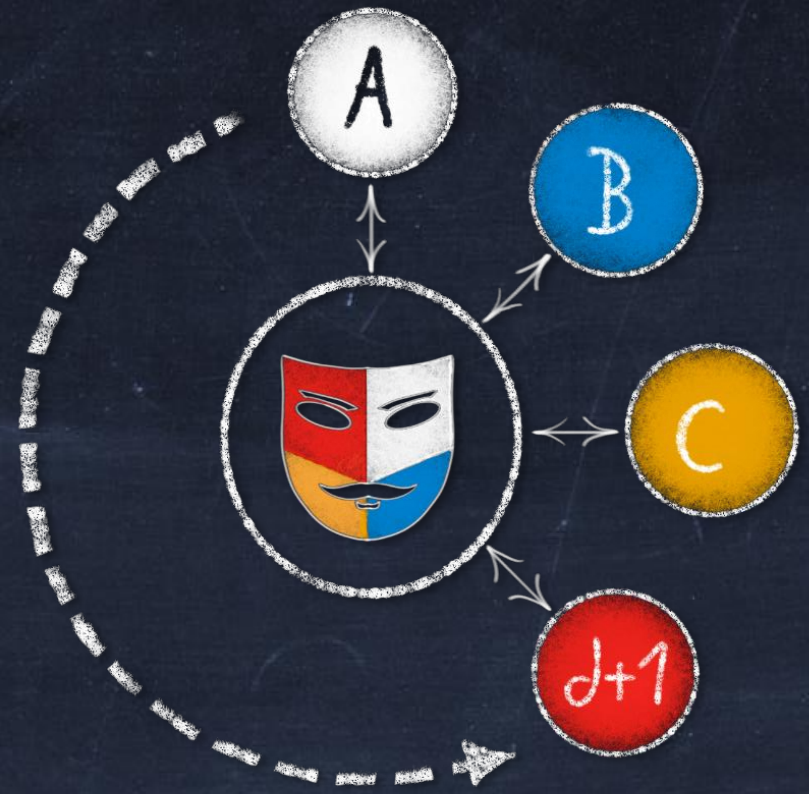
DOM



DOM

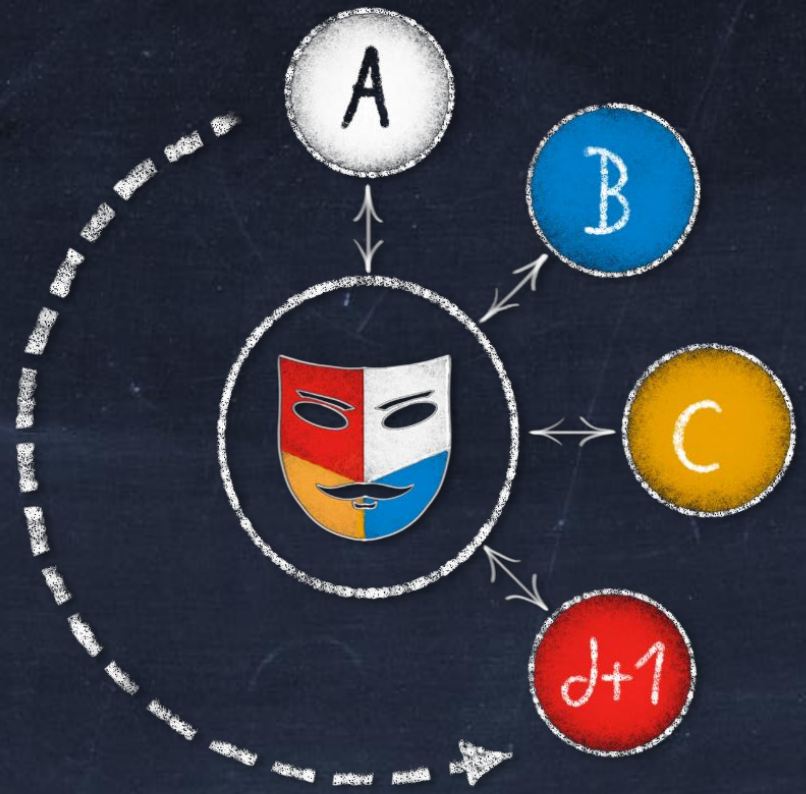


Summary



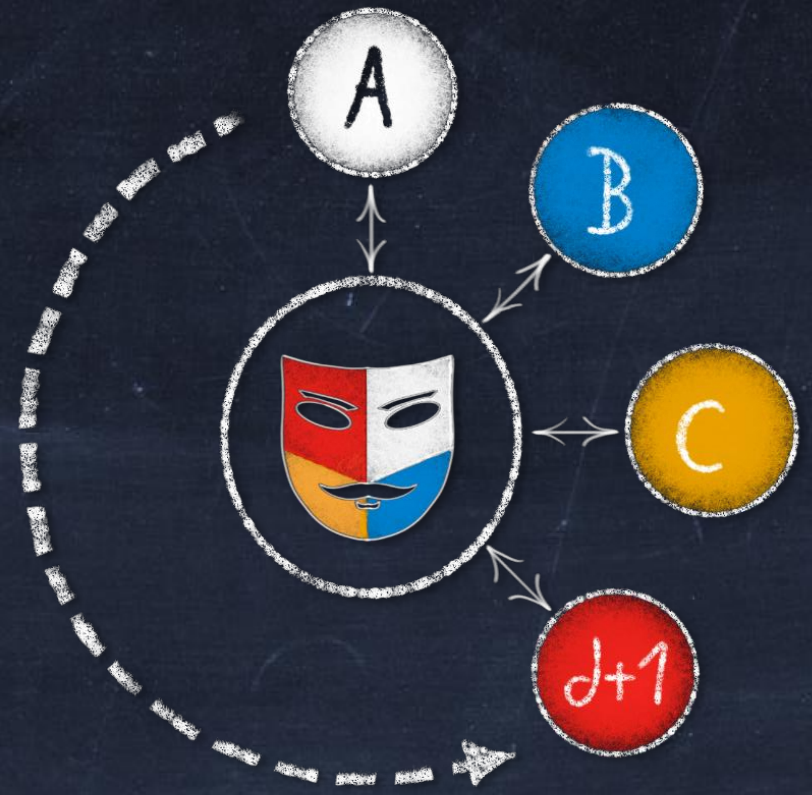
Summary

- Circuit centered



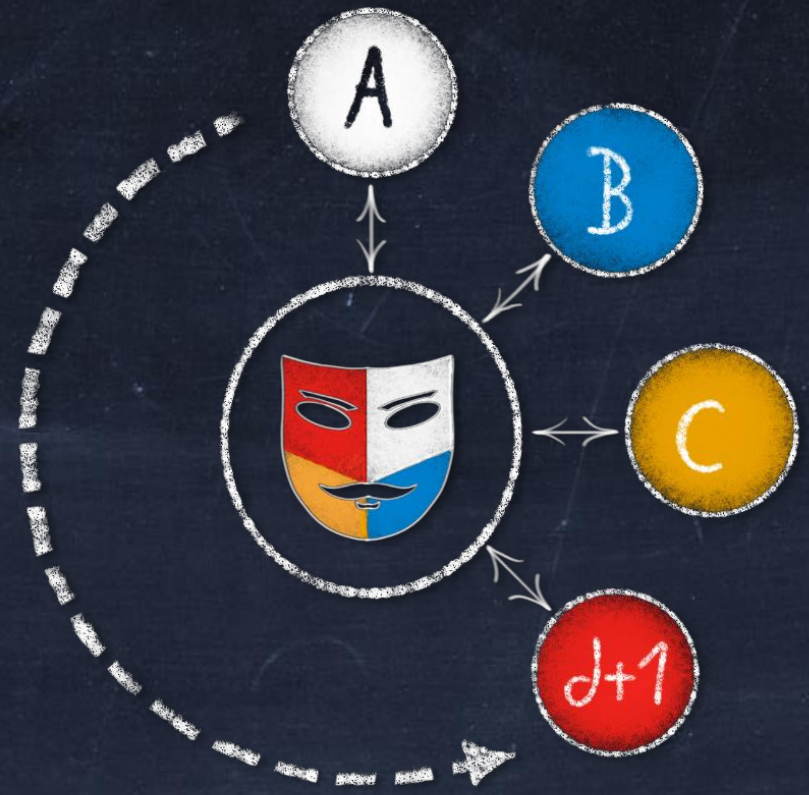
Summary

- Circuit centered
- d+1 shares



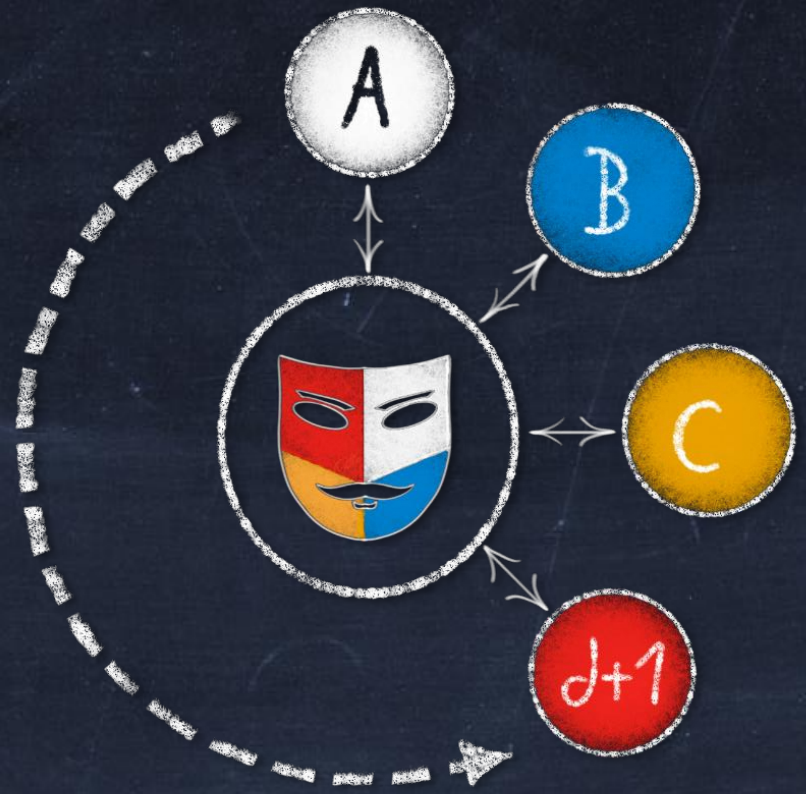
Summary

- Circuit centered
- d+1 shares
- Generic



Summary

- Circuit centered
- d+1 shares
- Generic
- Low randomness



What causes latency?

DOM

$q = x \cdot y =$

DOM

$$q = x \cdot y =$$

$$(A_x \oplus B_x \oplus C_x) \cdot (A_y \oplus B_y \oplus C_y)$$

$$= \ldots$$

DOM

$$q = x \cdot y =$$

$$(A_x \oplus B_x \oplus C_x) \cdot (A_y \oplus B_y \oplus C_y)$$

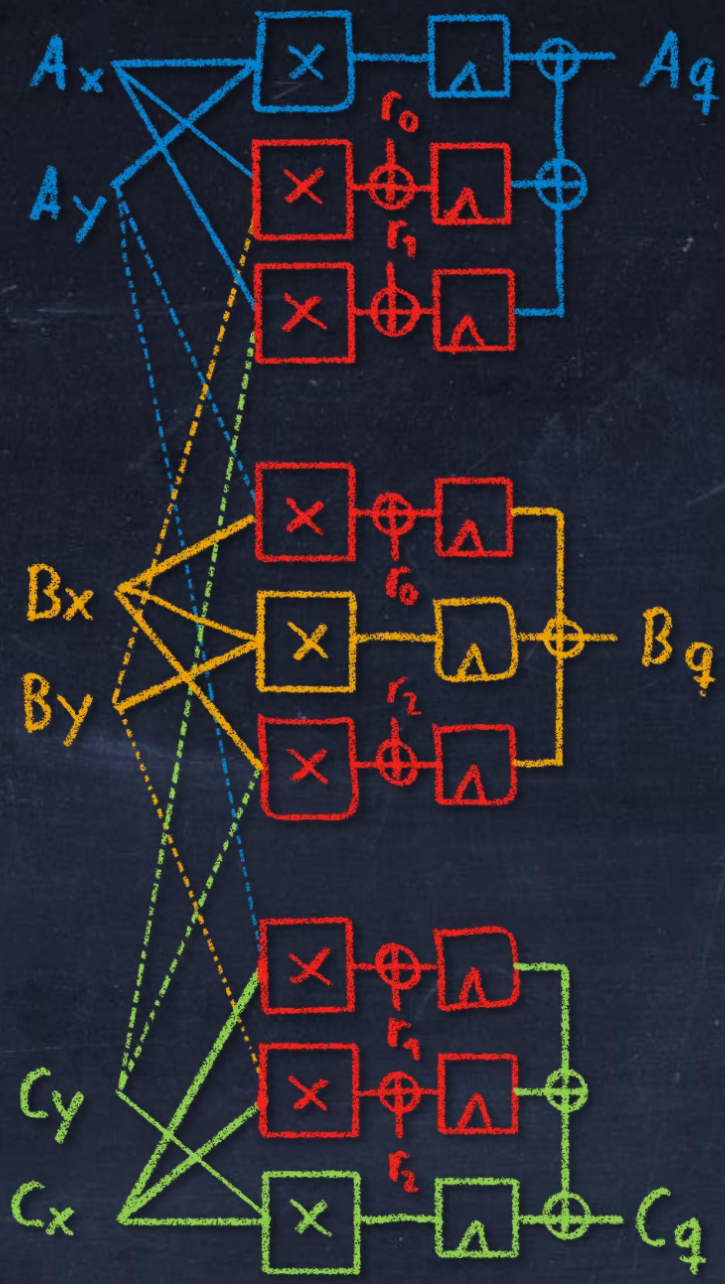
$$= \ldots$$

$$A_q = A_x (A_y \oplus B_y \oplus C_y)$$

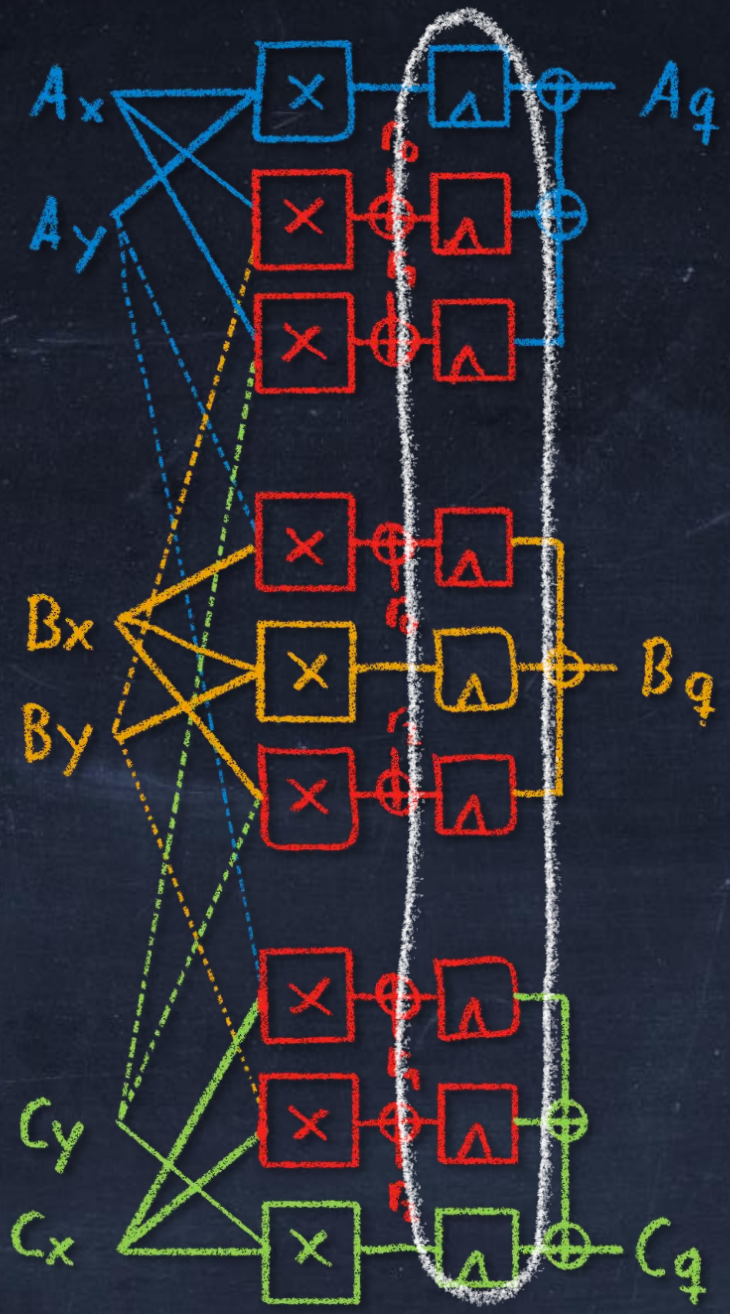
$$B_q = B_x (A_y \oplus B_y \oplus C_y)$$

$$C_q = C_x (A_y \oplus B_y \oplus C_y)$$

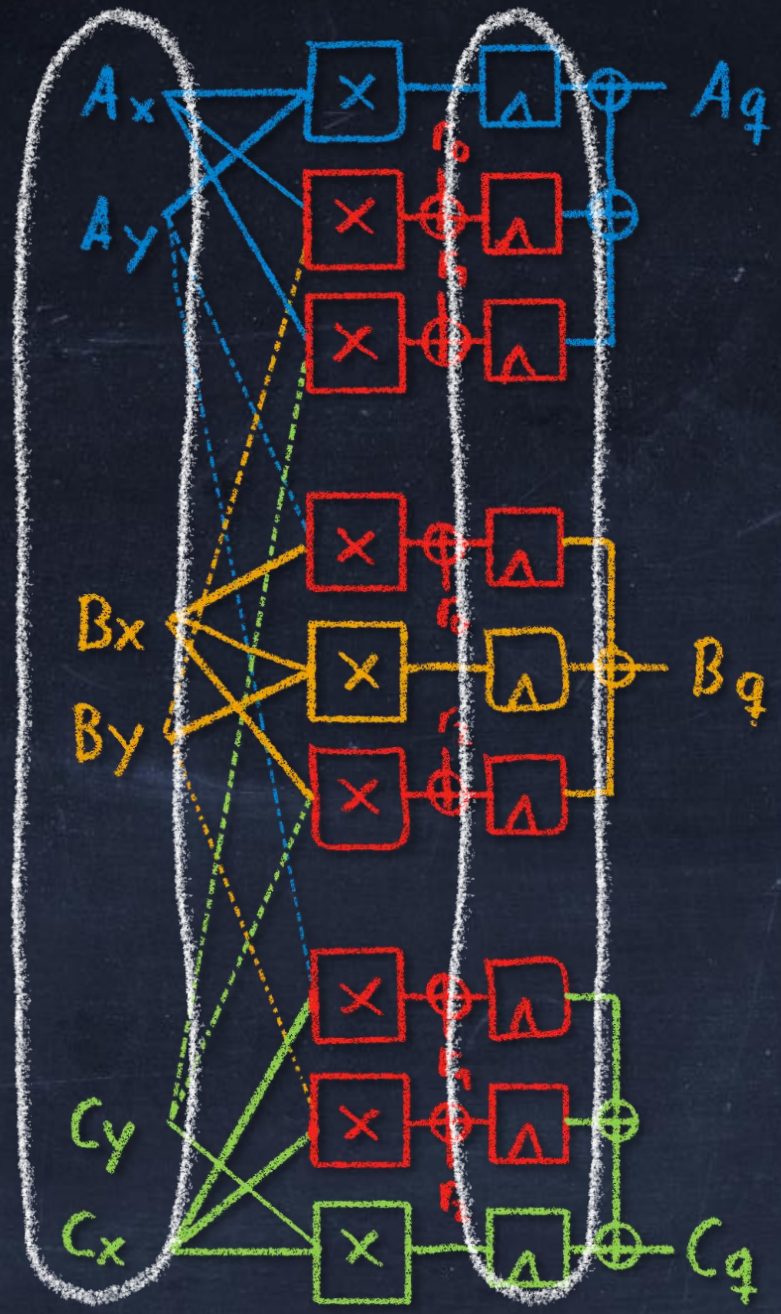
DOM



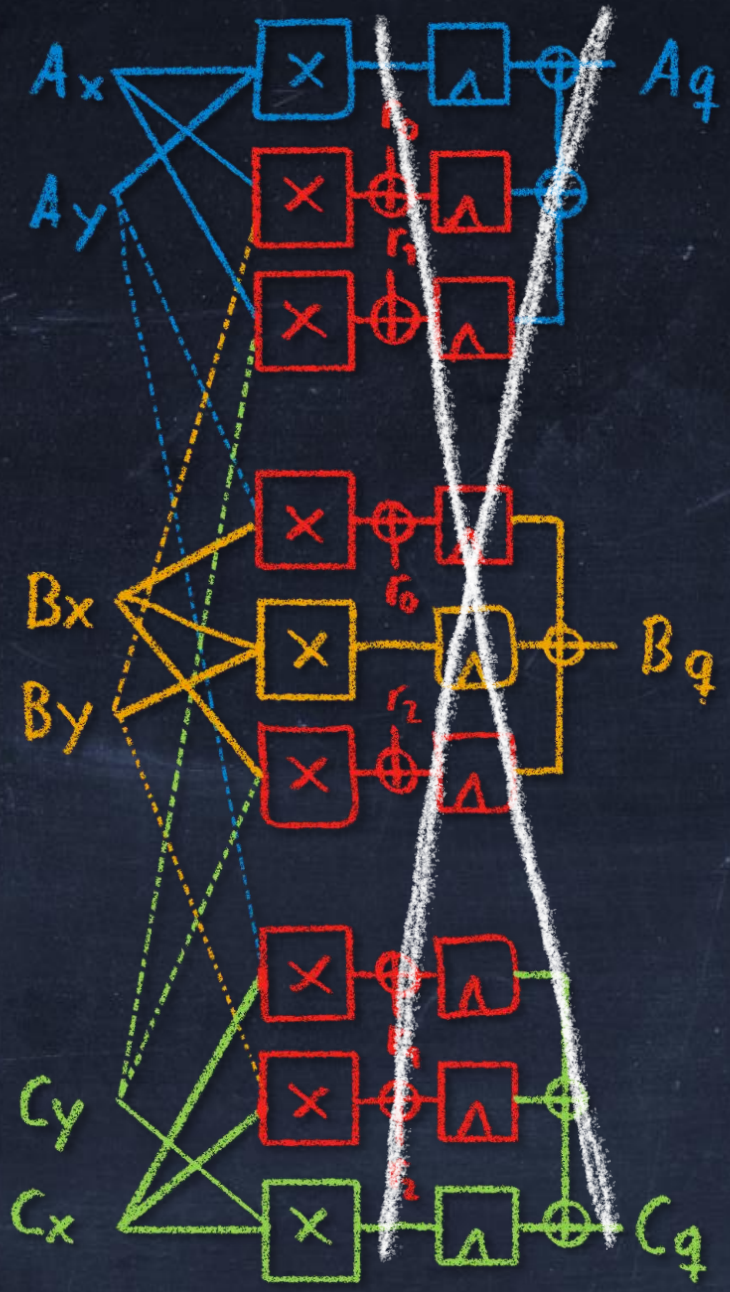
DOM



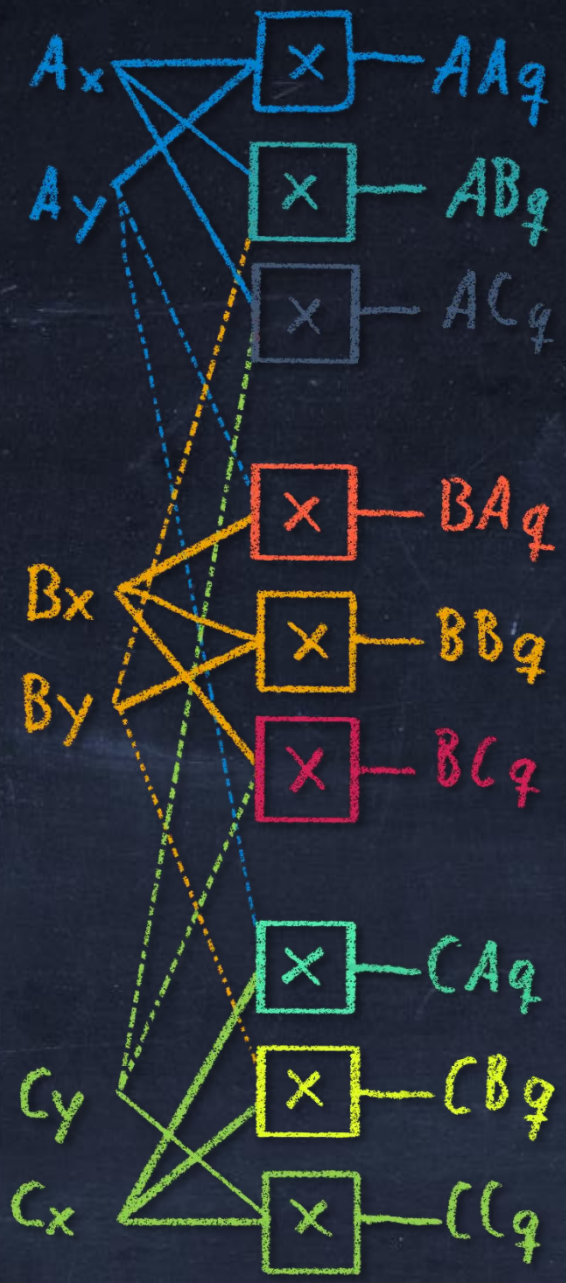
DOM



LOLA



LOLA

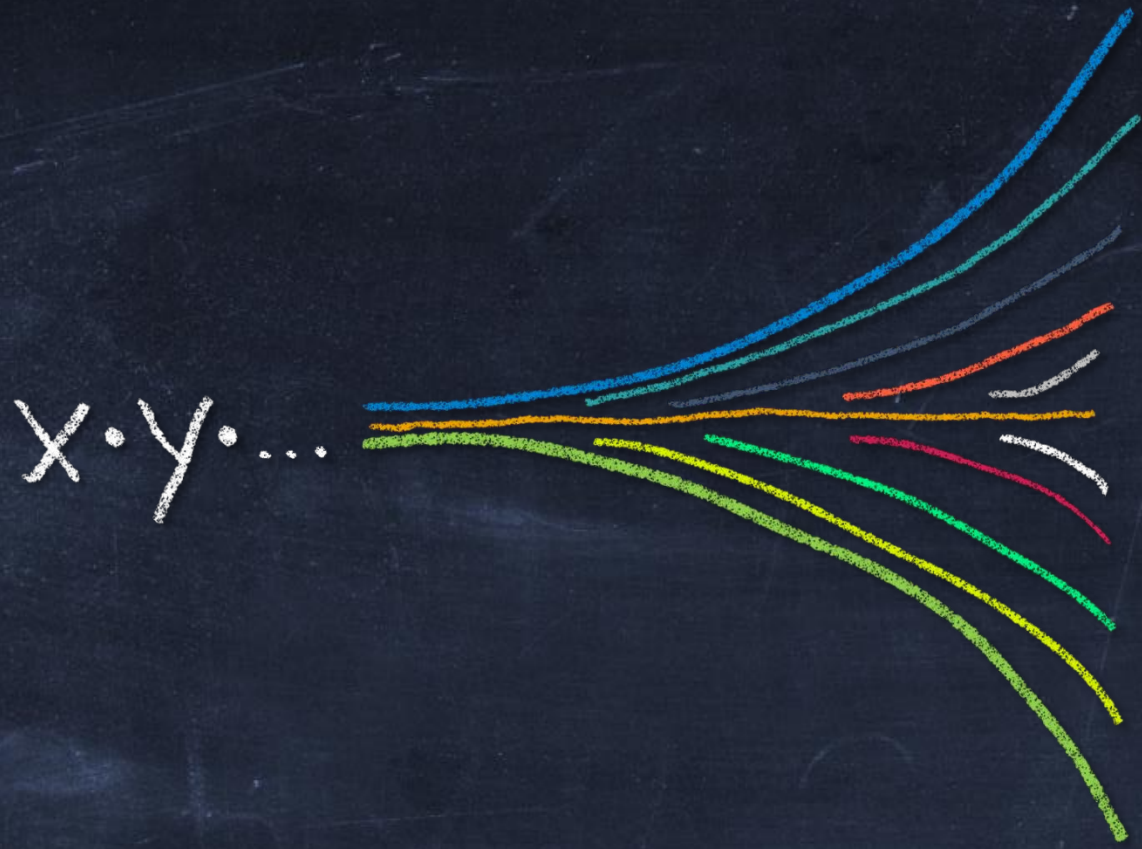


✓

LOLA

x·y·…

LOLA



LOLA

LOLA

$$q = x \cdot x =$$

$$(A_x \oplus B_x \oplus C_x) \cdot (A_x \oplus B_x \oplus C_x)$$

LOLA

$$q = x \cdot x = \lightning$$

$$(A_x \oplus B_x \oplus C_x) \cdot (A_x \oplus B_x \oplus C_x)$$

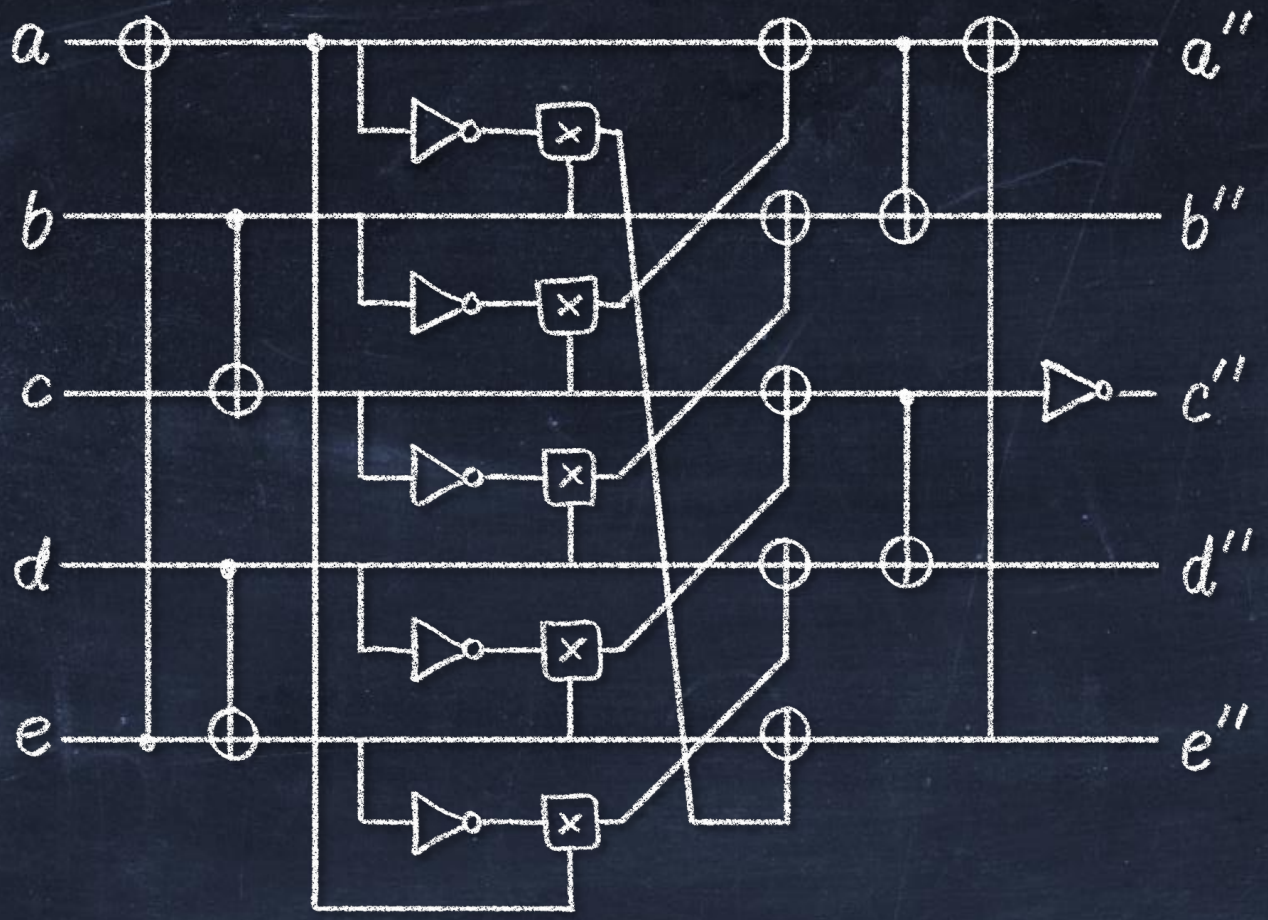
LOLA

$$q = x \cdot x' =$$

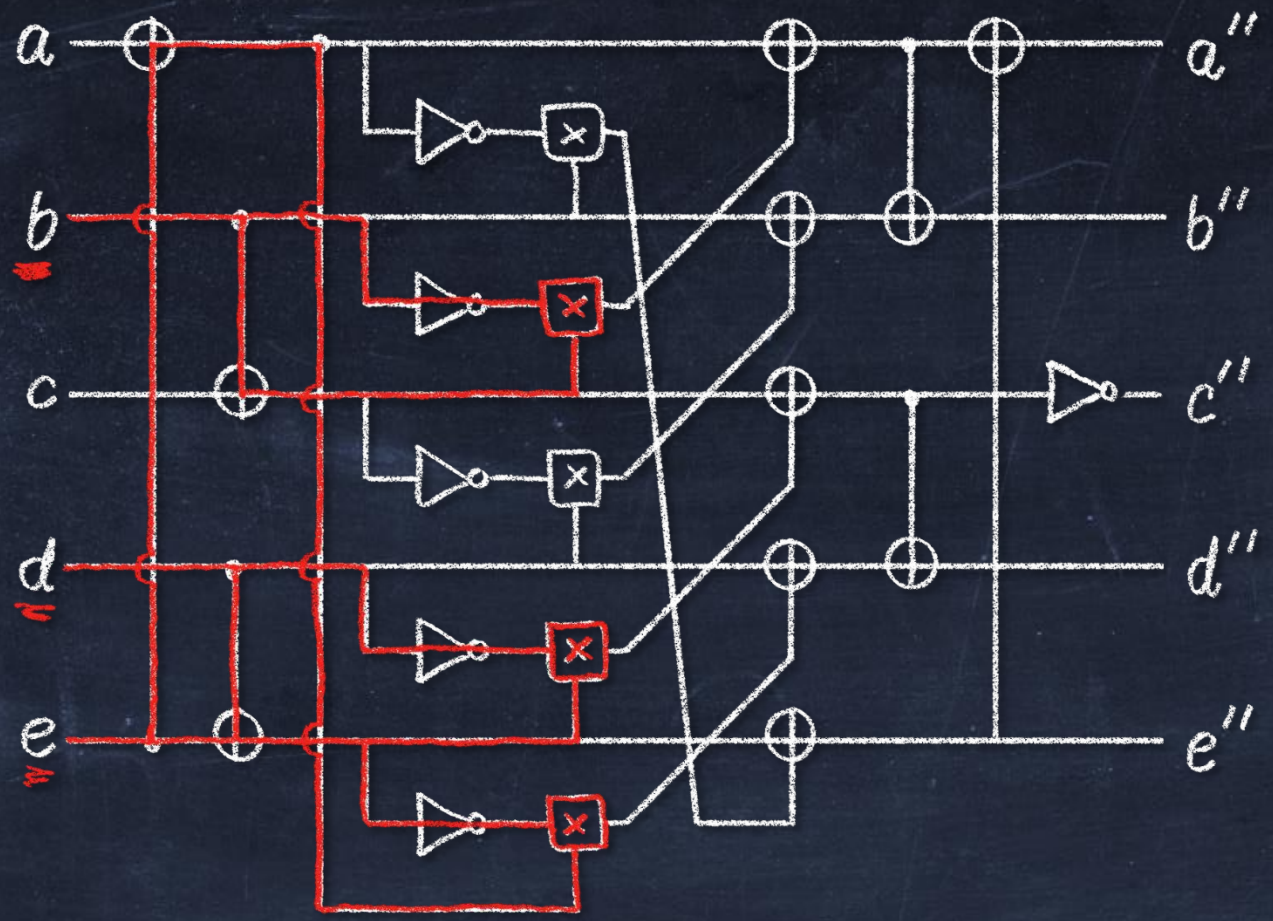
$$(A_x \oplus B_x \oplus C_x) \cdot (A_{x'} \oplus B_{x'} \oplus C_{x'})$$

✓

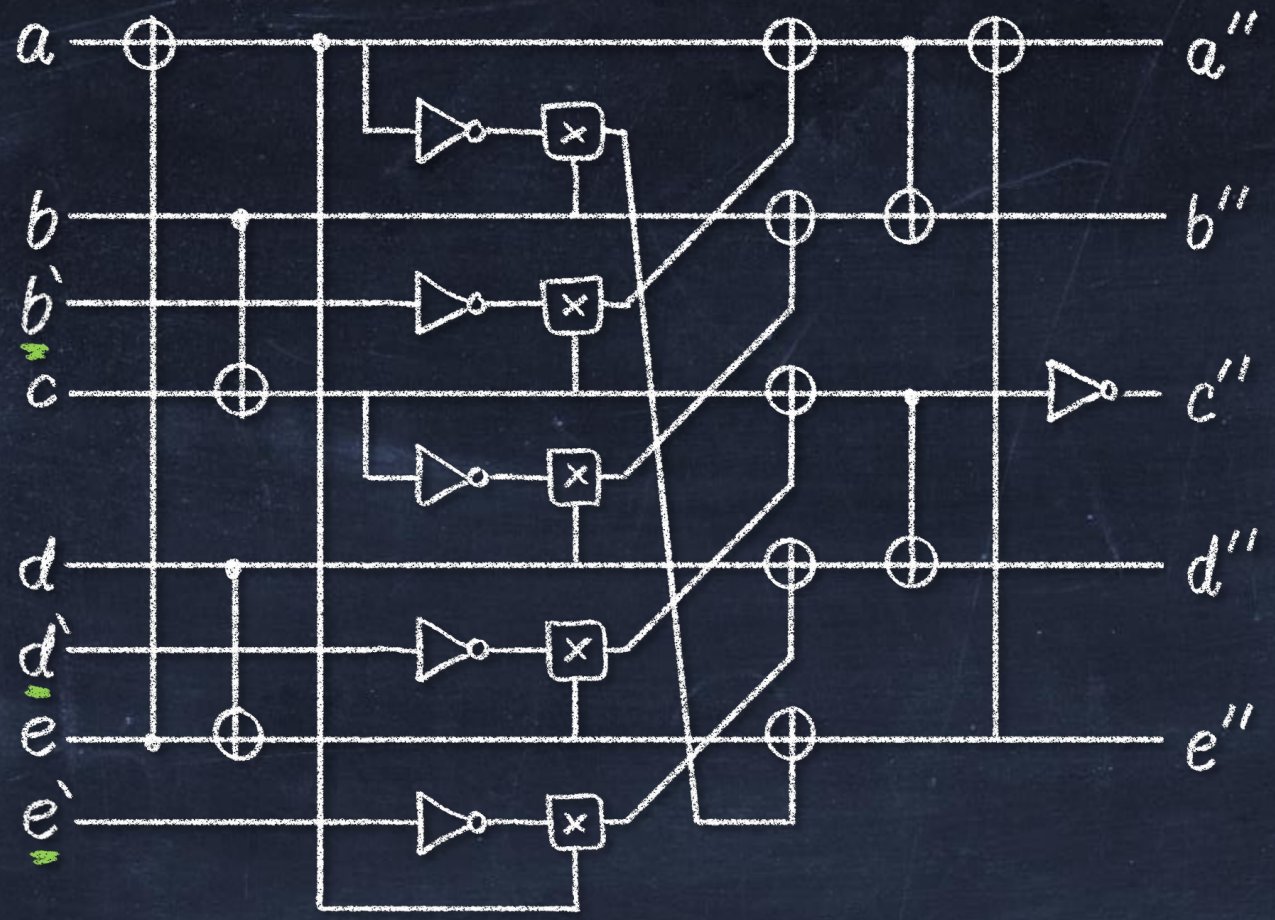
Ascon Example



Ascon Example



Ascon Example



Ascon Example

Design	Size *[kGE]*	Cycles */Round*	Max. Throughput *[Gb/s]*	Randomness *[bits/cycle]*	Latency *[ns]*
Unprotected	8.35	1	5.84	-	10.96
1^{st}-order	42.75	1	2.77	2,048	23.10
2^{nd}-order	90.94	1	3.35	4,608	19.10
3^{rd}-order	153.91	1	3.34	8,192	19.16
4^{th}-order	238.30	1	2.59	12,800	24.71
5^{th}-order	339.82	1	2.99	18,432	21.40
Related work [GM17]					
1^{st}-order UMA	27.18	3	2.25	320	28.44
1^{st}-order DOM	28.89	3	2.25	320	28.44
5^{th}-order DOM	161.87	3	1.86	4,800	34.14
5^{th}-order UMA	220.01	7	0.85	3,520	75.29

Ascon Example

Design	Size *[kGE]*	Cycles */Round*	Max. Throughput *[Gb/s]*	Randomness *[bits/cycle]*	Latency *[ns]*
Unprotected	8.35	1	5.84	-	10.96
1^{st}-order	42.75	1	2.77	2,048	23.10
2^{nd}-order	90.94	1	3.35	4,608	19.10
3^{rd}-order	153.91	1	3.34	8,192	19.16
4^{th}-order	238.30	1	2.59	12,800	24.71
5^{th}-order	339.82	1	2.99	18,432	21.40
Related work [GM17]					
1^{st}-order UMA	27.18	3	2.25	320	28.44
1^{st}-order DOM	28.89	3	2.25	320	28.44
5^{th}-order DOM	161.87	3	1.86	4,800	34.14
5^{th}-order UMA	220.01	7	0.85	3,520	75.29

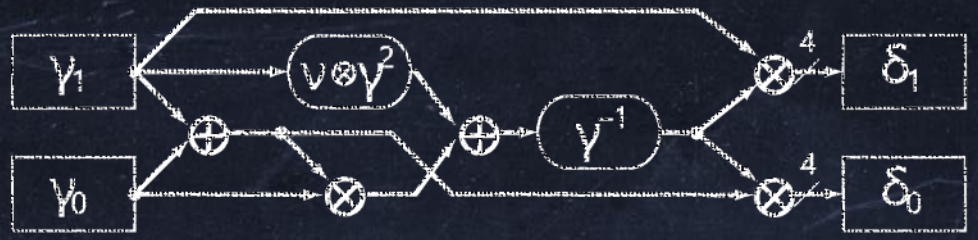
Ascon Example

Design	Size *[kGE]*	Cycles */Round*	Max. Throughput *[Gb/s]*	Randomness *[bits/cycle]*	Latency *[ns]*
Unprotected	8.35	1	5.84	-	10.96
1^{st}-order	42.75	1	2.77	2,048	23.10
2^{nd}-order	90.94	1	3.35	4,608	19.10
3^{rd}-order	153.91	1	3.34	8,192	19.16
4^{th}-order	238.30	1	2.59	12,800	24.71
5^{th}-order	339.82	1	2.99	18,432	21.40
Related work [GM17]					
1^{st}-order UMA	27.18	3	2.25	320	28.44
1^{st}-order DOM	28.89	3	2.25	320	28.44
5^{th}-order DOM	161.87	3	1.86	4,800	34.14
5^{th}-order UMA	220.01	7	0.85	3,520	75.29

Ascon Example

Design	Size *[kGE]*	Cycles */Round*	Max. Throughput *[Gb/s]*	Randomness *[bits/cycle]*	Latency *[ns]*
Unprotected	8.35	1	5.84	-	10.96
1st-order	42.75	1	2.77	2,048	23.10
2nd-order	90.94	1	3.35	4,608	19.10
3rd-order	153.91	1	3.34	8,192	19.16
4th-order	238.30	1	2.59	12,800	24.71
5th-order	339.82	1	2.99	18,432	21.40
Related work [GM17]					
1st-order UMA	27.18	3	2.25	320	28.44
1st-order DOM	28.89	3	2.25	320	28.44
5th-order DOM	161.87	3	1.86	4,800	34.14
5th-order UMA	220.01	7	0.85	3,520	75.29

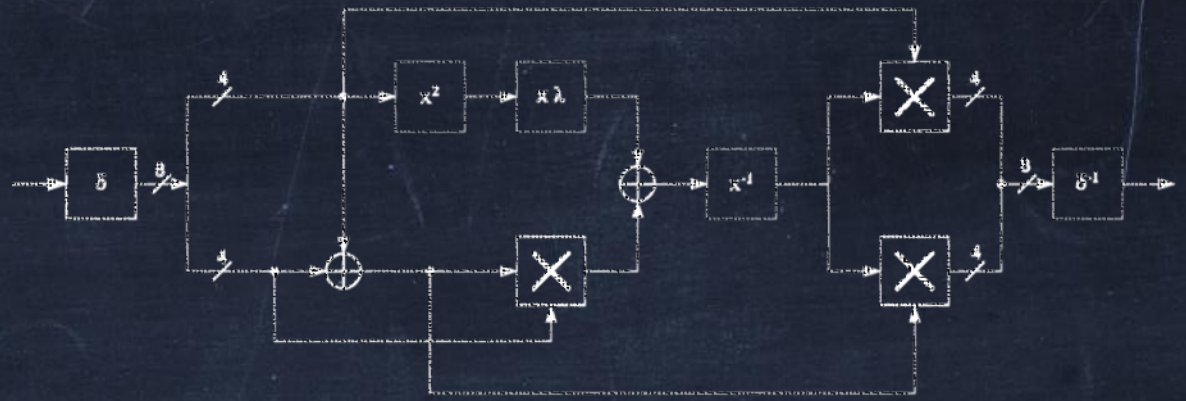
AES Example



Canright

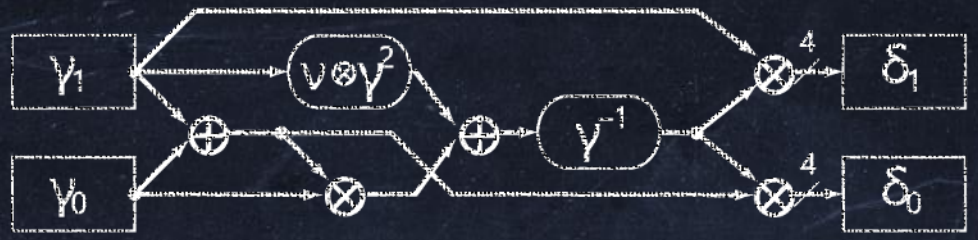
```
M1 = T13 x T6        M17 = M5 + T24       M33 = M27 + M25      M49 = M43 x T16
M2 = T23 x T8        M18 = M8 + M7        M34 = M21 x M22      M50 = M38 x T9
M3 = T14 + M1        M19 = M10 + M15      M35 = M24 x M34      M51 = M37 x T17
M4 = T19 x D         M20 = M16 + M13      M36 = M24 + M25      M52 = M42 x T15
M5 = M4 + M1         M21 = M17 + M15      M37 = M21 + M29      M53 = M45 x T27
M6 = T3 x T16        M22 = M18 + M13      M38 = M32 + M33      M54 = M41 x T10
M7 = T22 x T9        M23 = M19 + T25      M39 = M23 + M30      M55 = M44 x T13
M8 = T26 + M6        M24 = M22 + M23      M40 = M35 + M36      M56 = M40 x T23
M9 = T20 x T17       M25 = M22 x M20      M41 = M38 + M40      M57 = M59 x T19
M10 = M9 + M6        M26 = M21 + M25      M42 = M37 + M39      M58 = M43 x T3
M11 = T1 x T15       M27 = M20 + M21      M43 = M37 + M38      M59 = M38 x T22
M12 = T4 x T27       M28 = M23 + M25      M44 = M39 + M40      M60 = M37 x T20
M13 = M12 + M11      M29 = M28 x M27      M45 = M42 + M41      M61 = M42 x T1
M14 = T2 x T10       M30 = M26 x M24      M46 = M44 x T6       M62 = M45 x T4
M15 = M14 + M11      M31 = M30 x M23      M47 = M40 x T8       M63 = M41 x T2
M16 = M3 + M2        M32 = M27 x M31      M48 = M39 x D
```

Boyar-Peralta



Mui

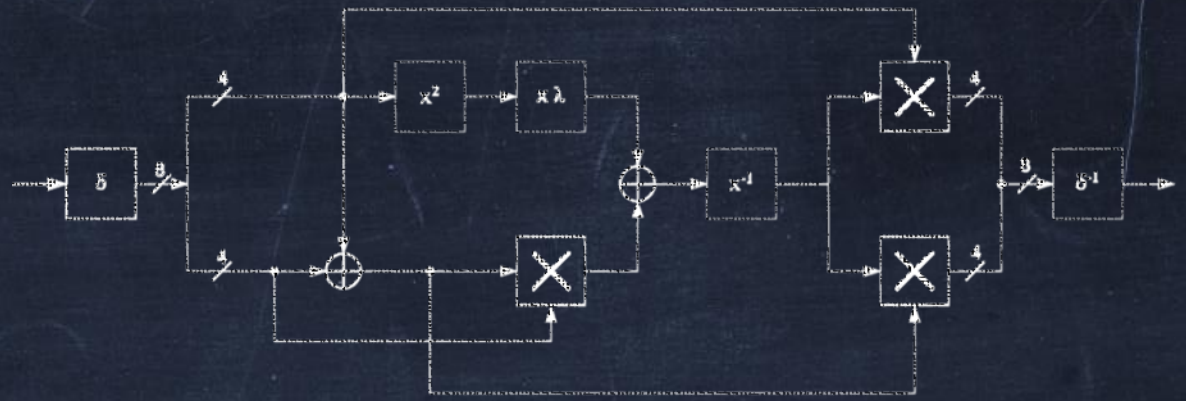
AES Example



Canright

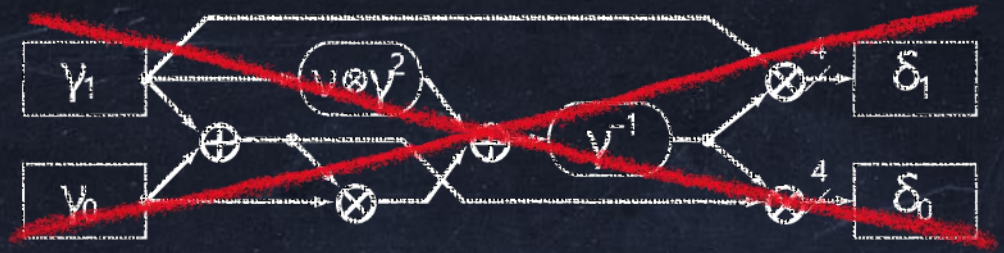
```
M1  = T13 x T6        M17 = M5  + T24       M33 = M27 + M25       M49 = M43 x T16
M2  = T23 x T8        M18 = M8  + M7        M34 = M21 x M22       M50 = M38 x T9
M3  = T14 + M1        M19 = M10 + M15       M35 = M24 x M34       M51 = M37 x T17
M4  = T19 x D         M20 = M16 + M13       M36 = M24 + M25       M52 = M42 x T15
M5  = M4  + M1        M21 = M17 + M15       M37 = M21 + M29       M53 = M45 x T27
M6  = T3  x T16       M22 = M18 + M13       M38 = M32 + M33       M54 = M41 x T10
M7  = T22 x T9        M23 = M19 + T25       M39 = M23 + M30       M55 = M44 x T13
M8  = T26 + M6        M24 = M22 + M23       M40 = M35 + M36       M56 = M40 x T23
M9  = T20 x T17       M25 = M22 x M20       M41 = M38 + M40       M57 = M39 x T19
M10 = M9  + M6        M26 = M21 + M25       M42 = M37 + M39       M58 = M43 x T3
M11 = T1  x T15       M27 = M20 + M21       M43 = M37 + M38       M59 = M38 x T22
M12 = T4  x T27       M28 = M23 + M25       M44 = M39 + M40       M60 = M37 x T20
M13 = M12 + M11       M29 = M28 x M27       M45 = M42 + M41       M61 = M42 x T1
M14 = T2  + T10       M30 = M26 x M24       M46 = M44 x T6        M62 = M45 x T4
M15 = M14 + M11       M31 = M30 x M23       M47 = M40 x T8        M63 = M41 x T2
M16 = M3  + M2        M32 = M27 x M31       M48 = M39 x D
```

Boyar-Peralta



Mui

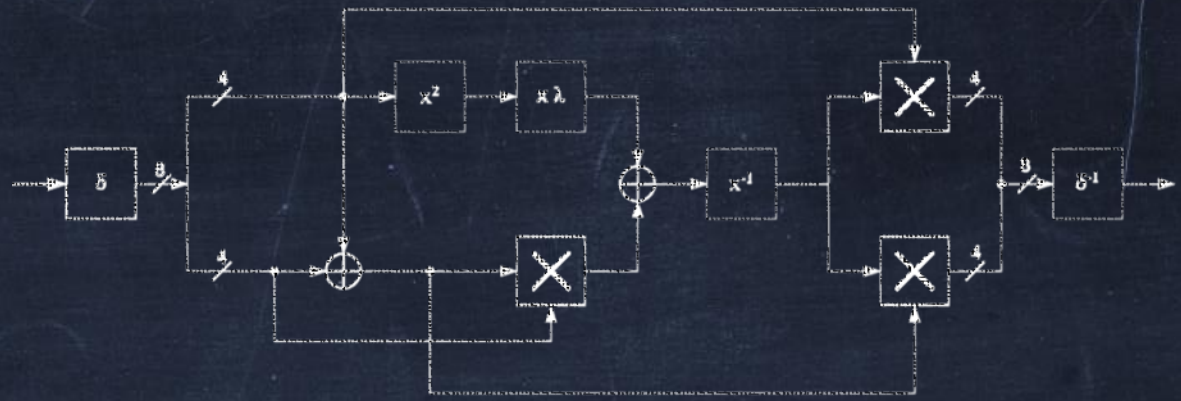
AES Example



Canright

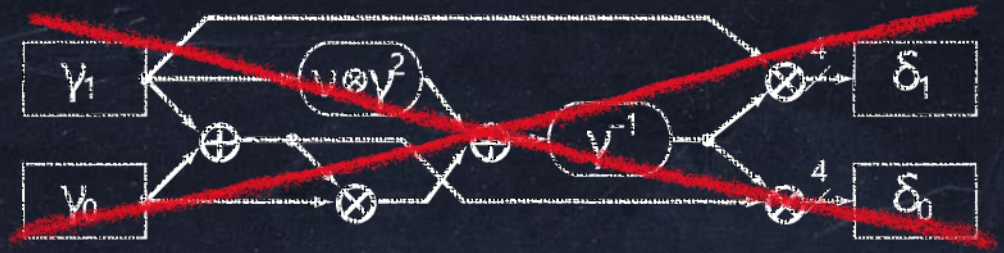
```
M1  = T13 x T6      M17 = M5  + T24     M33 = M27 + M25     M49 = M43 x T16
M2  = T23 x T8      M18 = M8  + M7      M34 = M21 x M22     M50 = M38 x T9
M3  = T14 x M1      M19 = M10 + M15     M35 = M24 x M34     M51 = M37 x T17
M4  = T19 x D       M20 = M16 + M13     M36 = M24 + M25     M52 = M42 x T15
M5  = M4  + M1      M21 = M17 + M15     M37 = M21 + M29     M53 = M45 x T27
M6  = T3  x T16     M22 = M18 + M13     M38 = M32 + M33     M54 = M41 x T10
M7  = T22 x T9      M23 = M19 + T25     M39 = M23 + M30     M55 = M44 x T13
M8  = T26 + M6      M24 = M22 + M23     M40 = M35 + M36     M56 = M40 x T23
M9  = T20 x T17     M25 = M22 x M20     M41 = M38 + M40     M57 = M39 x T19
M10 = M9  + M6      M26 = M21 + M25     M42 = M37 + M39     M58 = M43 x T3
M11 = T1  x T15     M27 = M20 + M21     M43 = M37 + M38     M59 = M38 x T22
M12 = T4  x T27     M28 = M23 + M25     M44 = M39 + M40     M60 = M37 x T20
M13 = M12 + M11     M29 = M28 x M27     M45 = M42 + M41     M61 = M42 x T1
M14 = T2  + T10     M30 = M26 x M24     M46 = M44 x T6      M62 = M45 x T4
M15 = M14 + M11     M31 = M30 x M23     M47 = M40 x T8      M63 = M41 x T2
M16 = M3  + M2      M32 = M27 x M31     M48 = M39 x D
```

Boyar-Peralta



Mui

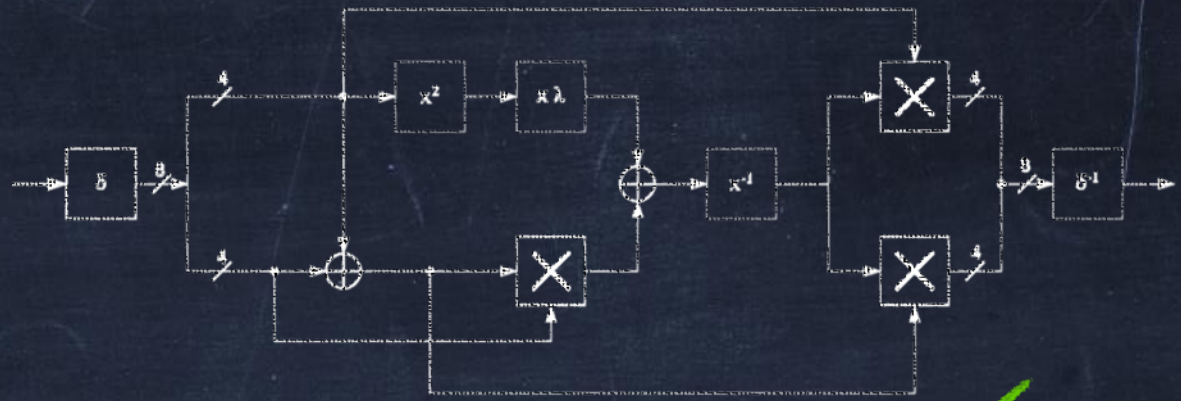
AES Example



Canright

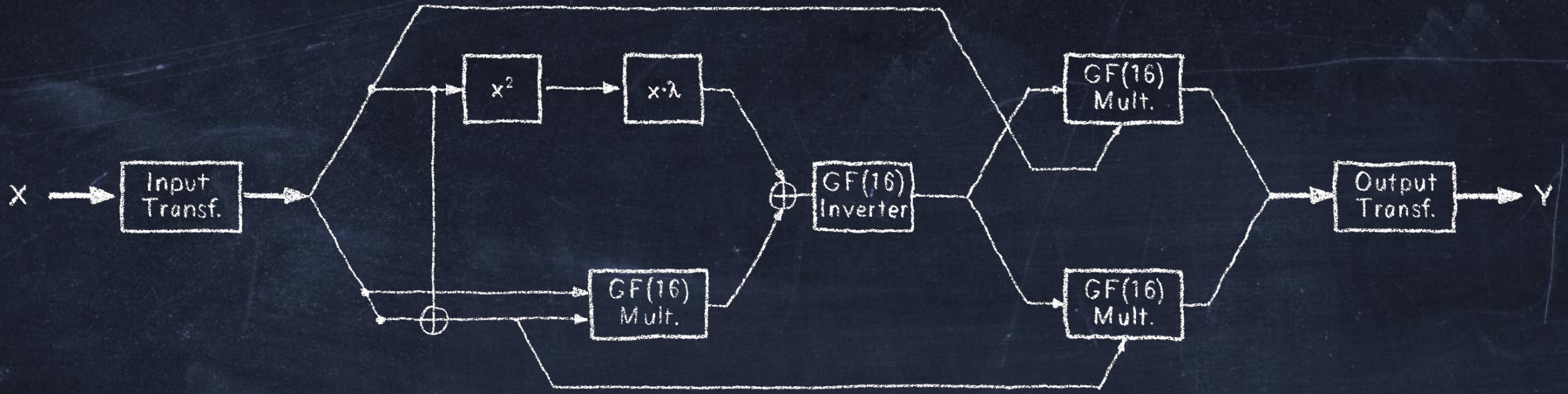
```
M1  = T13 x T6      M17 = M5  + T24     M33 = M27 + M25     M49 = M43 x T16
M2  = T23 x T8      M18 = M8  + M7      M34 = M21 x M22     M50 = M38 x T9
M3  = T14 + M1      M19 = M10 + M15     M35 = M24 x M34     M51 = M37 x T17
M4  = T19 x D       M20 = M16 + M13     M36 = M24 + M25     M52 = M42 x T15
M5  = M4  + M1      M21 = M17 + M15     M37 = M21 + M29     M53 = M45 x T27
M6  = T3  x T16     M22 = M18 + M13     M38 = M32 + M33     M54 = M41 x T10
M7  = T22 x T9      M23 = M19 + T25     M39 = M23 + M30     M55 = M44 x T13
M8  = T26 + M6      M24 = M22 + M23     M40 = M35 + M36     M56 = M40 x T23
M9  = T20 x T17     M25 = M22 x M20     M41 = M38 + M40     M57 = M39 x T19
M10 = M9  + M6      M26 = M21 + M25     M42 = M37 + M39     M58 = M43 x T3
M11 = T1  x T15     M27 = M20 + M21     M43 = M27 + M38     M59 = M38 x T22
M12 = T4  x T27     M28 = M23 + M25     M44 = M39 + M40     M60 = M37 x T20
M13 = M12 + M11     M29 = M28 x M27     M45 = M42 + M41     M61 = M42 x T1
M14 = T2  + M10     M30 = M26 x M24     M46 = M44 x T6      M62 = M45 x T4
M15 = M14 + M11     M31 = M30 x M23     M47 = M40 x T8      M63 = M41 x T2
M16 = M3  + M2      M32 = M27 x M31     M48 = M39 x D
```

Boyar-Peralta

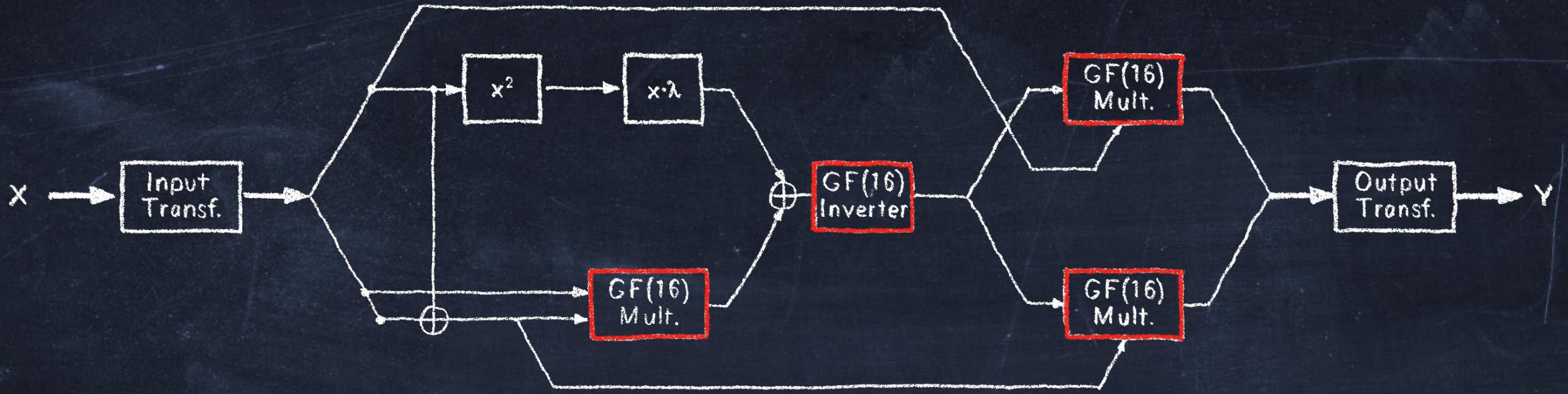


Mui

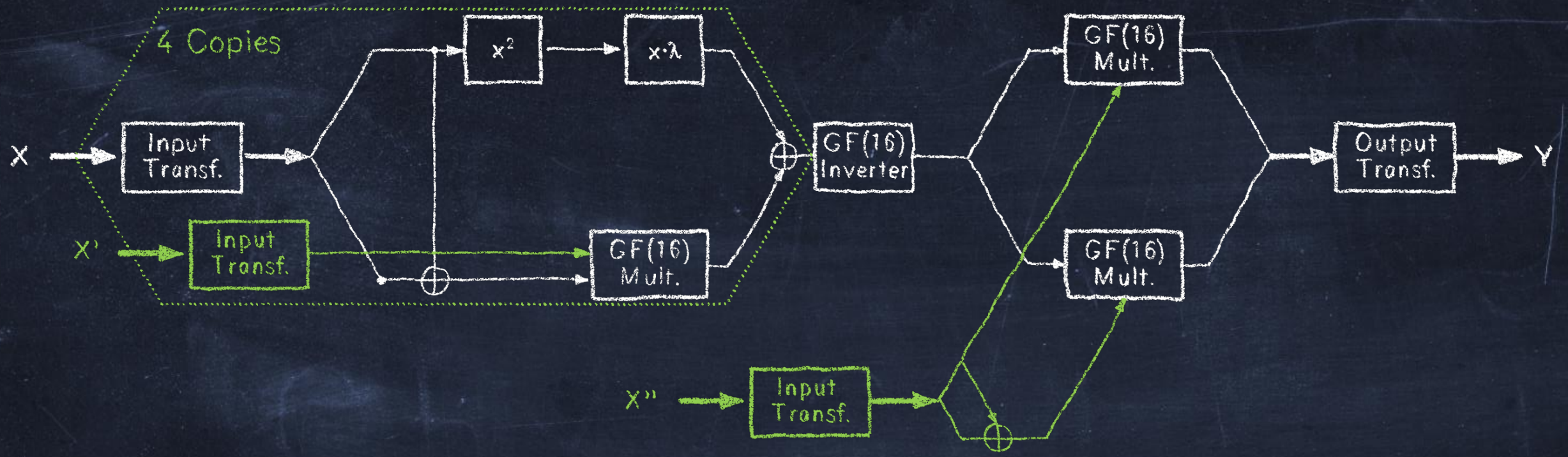
AES Example


X
Input Transf.
x^2
$x \cdot \lambda$
GF(16) Mult.
GF(16) Inverter
GF(16) Mult.
GF(16) Mult.
Output Transf.
Y

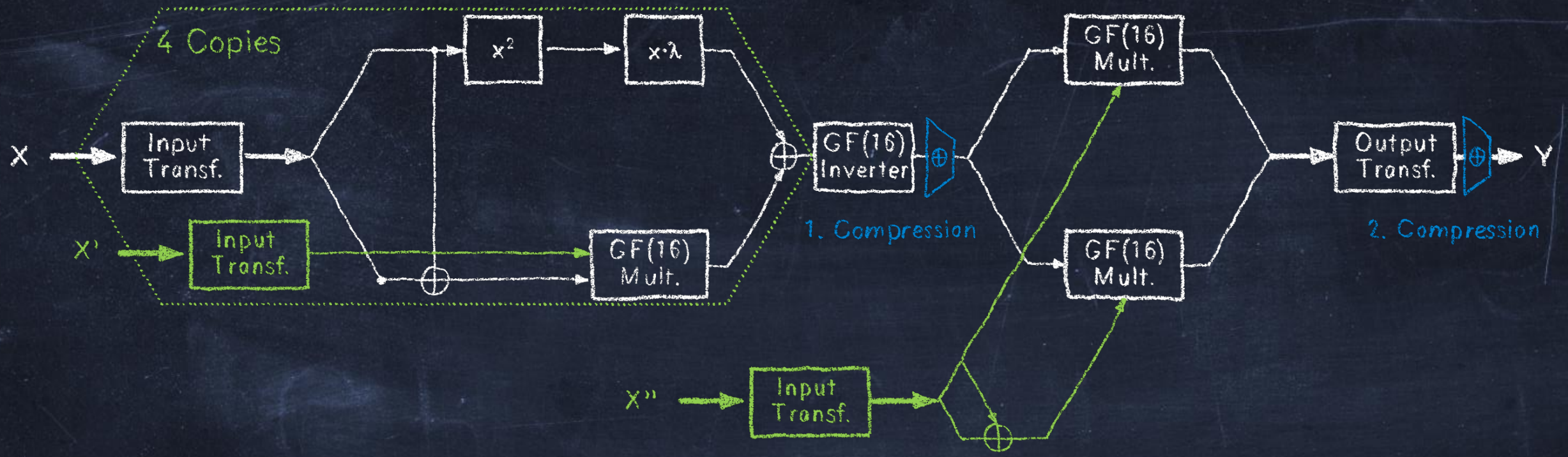
AES Example


X
Input Transf.
x^2
$x \cdot \lambda$
GF(16) Mult.
GF(16) Inverter
GF(16) Mult.
GF(16) Mult.
Output Transf.
Y

AES Example


4 Copies
X
Input Transf.
X'
Input Transf.
x²
x·λ
GF(16) Mult.
GF(16) Inverter
GF(16) Mult.
GF(16) Mult.
X''
Input Transf.
Output Transf.
Y

AES Example


4 Copies
X
Input Transf.
X'
Input Transf.
x²
x·λ
GF(16) Mult.
GF(16) Inverter
1. Compression
GF(16) Mult.
GF(16) Mult.
X''
Input Transf.
Output Transf.
Y
2. Compression

AES Example

Design	Order *[d]*	Size *[kGE]*	Cycles */S-box*	Max. Clock *[MHz]*	Randomness *[bits] (online)*
Zero Latency	first	17.83	0	228	0
Zero Latency	d		0		0
Single Cycle	first	60.73	1	356	2,048
Single Cycle	d		1		$16(d+1)^7$
Two Cycle	first	6.74	2	584	416
Two Cycle	second	57.11	2	517	4,446
Two Cycle	d		2		$6(d+1)^6 + 8(d+1)^2$
		Related work			
[BGN+14]	first	3.71	3		44
[BGN+15]	first	2.84	3		32
[CBR+15]	second	7.9 - 11.2	6		126
[CRB+16]	first	1.98	6		54
[GC17]	first	4.61	4		0
[GC17]	first	3.63 - 3.80	4		34 - 68
[GC17]	first	2.91 - 3.34	3		20-24
[GMK17]	first	2.2	8		18
[GMK17]	second	4.5	8		54
[GMK17]	d		8		9d(d+1)
[MPL+11]	first	4.24	4		48

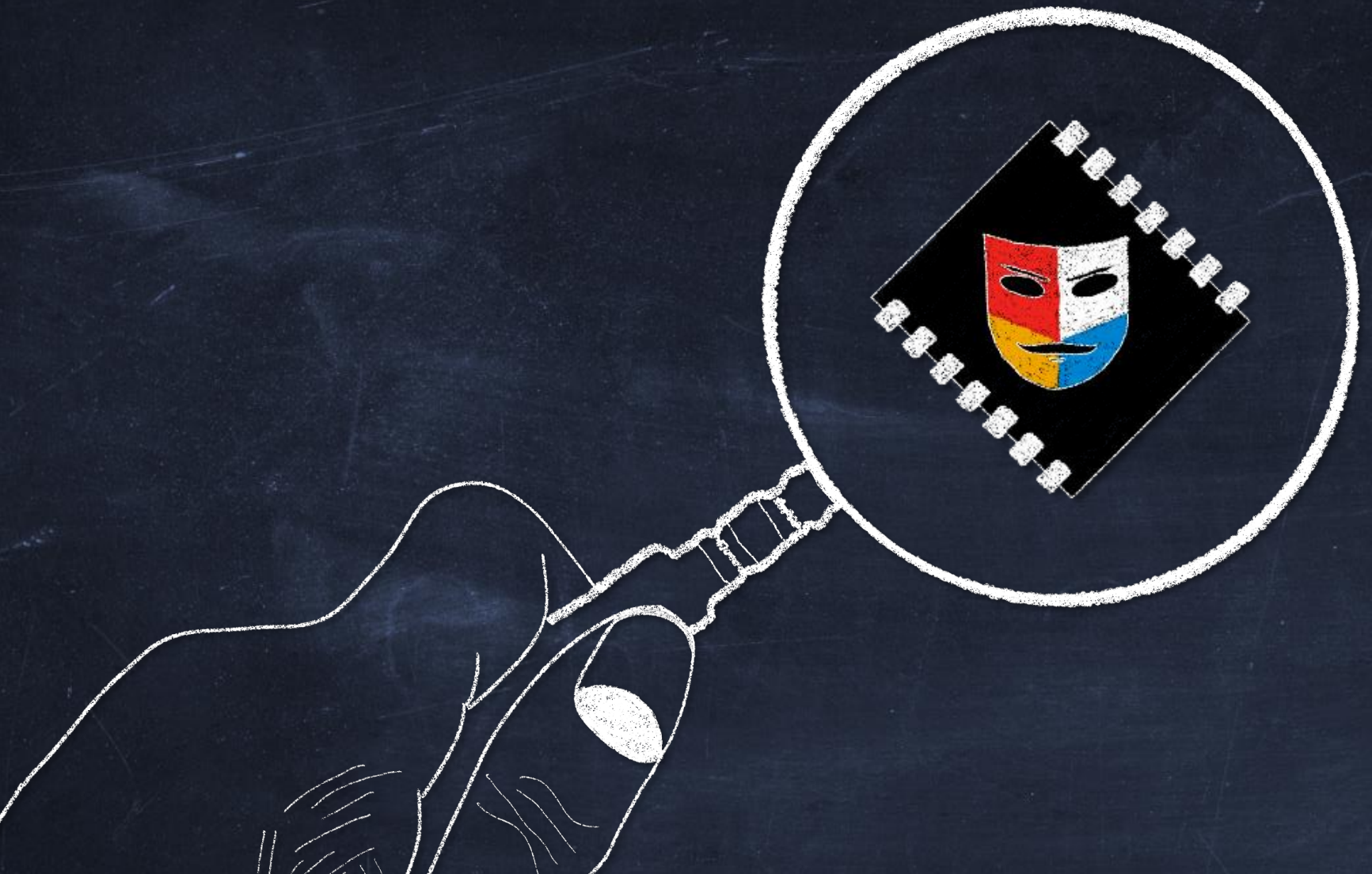
AES Example

Design	Order *[d]*	Size *[kGE]*	Cycles */S-box*	Max. Clock *[MHz]*	Randomness *[bits] (online)*
Zero Latency	first	17.83	0	228	0
Zero Latency	d		0		0
Single Cycle	first	60.73	1	356	2,048
Single Cycle	d		1		$16(d+1)^7$
Two Cycle	first	6.74	2	584	416
Two Cycle	second	57.11	2	517	4,446
Two Cycle	d		2		$6(d+1)^6 + 8(d+1)^2$
		Related work			
[BGN+14]	first	3.71	3		44
[BGN+15]	first	2.84	3		32
[CBR+15]	second	7.9 - 11.2	6		126
[CRB+16]	first	1.98	6		54
[GC17]	first	4.61	4		0
[GC17]	first	3.63 - 3.80	4		34 - 68
[GC17]	first	2.91 - 3.34	3		20-24
[GMK17]	first	2.2	8		18
[GMK17]	second	4.5	8		54
[GMK17]	d		8		9d(d+1)
[MPL+11]	first	4.24	4		48

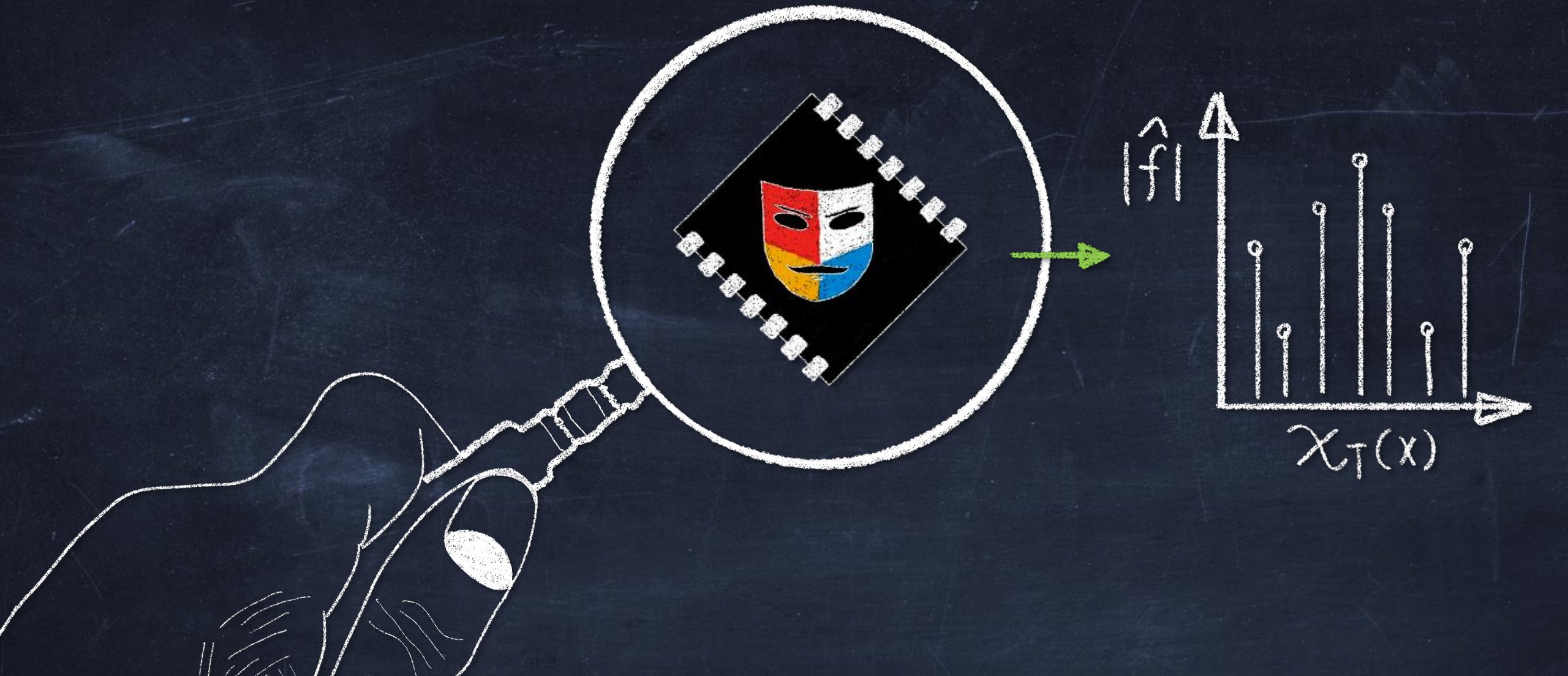
AES Example

Design	Order *[d]*	Size *[kGE]*	Cycles */S-box*	Max. Clock *[MHz]*	Randomness *[bits] (online)*
Zero Latency	first	17.83	0	228	0
Zero Latency	d		0		0
Single Cycle	first	60.73	1	356	2,048
Single Cycle	d		1		$16(d+1)^7$
Two Cycle	first	6.74	2	584	416
Two Cycle	second	57.11	2	517	4,446
Two Cycle	d		2		$6(d+1)^6 + 8(d+1)^2$
		Related work			
[BGN+14]	first	3.71	3		44
[BGN+15]	first	2.84	3		32
[CBR+15]	second	7.9 - 11.2	6		126
[CRB+16]	first	1.98	6		54
[GC17]	first	4.61	4		0
[GC17]	first	3.63 - 3.80	4		34 - 68
[GC17]	first	2.91 - 3.34	3		20-24
[GMK17]	first	2.2	8		18
[GMK17]	second	4.5	8		54
[GMK17]	d		8		9d(d+1)
[MPL+11]	first	4.24	4		48

Formal Verification

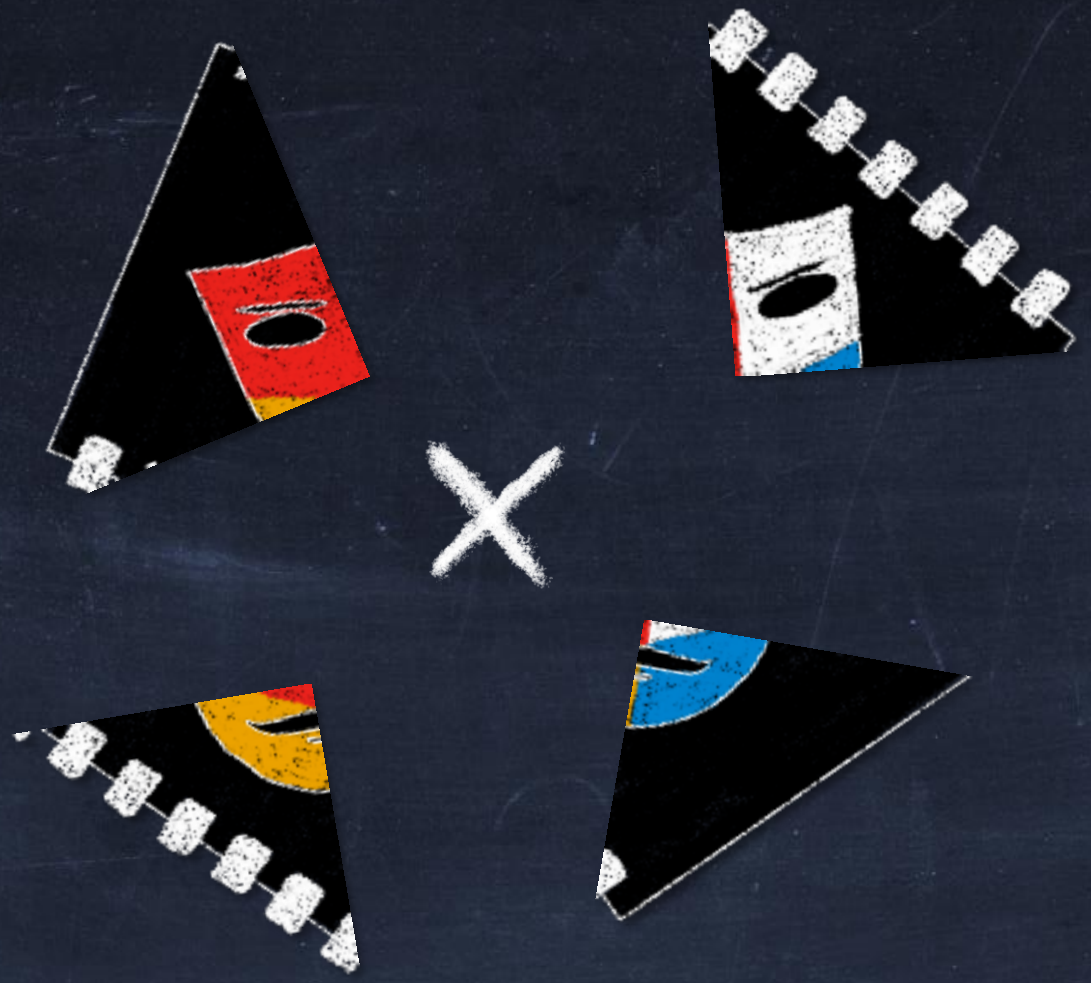


Formal Verification



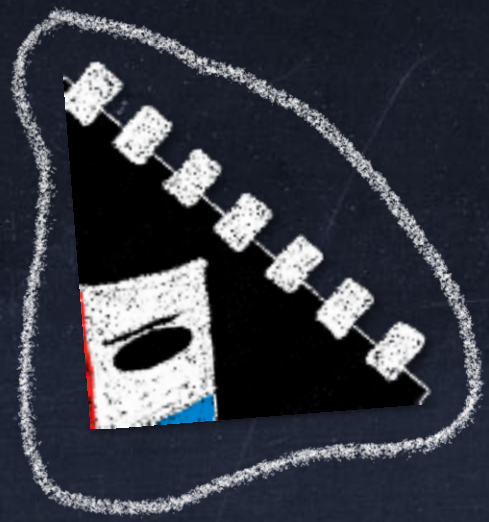
~~Formal~~ Verification

~~Formal~~ Verification



~~Formal~~ Verification

A



B

X

C

D

✓

Verification

S-box Design	Gates		Order	FV		Taint Checking	
	Lin	Non-lin		Time	Result	Time	Result
1st-order Ascon	34	22	1	≤ 2 s	✓	≤ 1 s	✓
2nd-order Ascon	58	48	2	≤ 18 s	✓	≤ 1 s	✓
3rd-order Ascon	88	84	3	≤ 21 m	✓	≤ 1 s	✓
Zero Latency AES	17,199	5,544	1	≥ 1 day	?	≤ 11 m	✓

Conclusions

- Masking w/o latency and "online" randomness?

Conclusions

- Masking w/o latency and "online" randomness?

- New design choice for generic masking
  → trading randomness & area for latency

Conclusions

- Masking w/o latency and "online" randomness?
- New design choice for generic masking
  → trading randomness & area for latency
- Only a first step towards low latency

DOM-LOLA

Generic Low-Latency Masking

Hannes Groß, Rinat Iusupov, Roderick Bloem