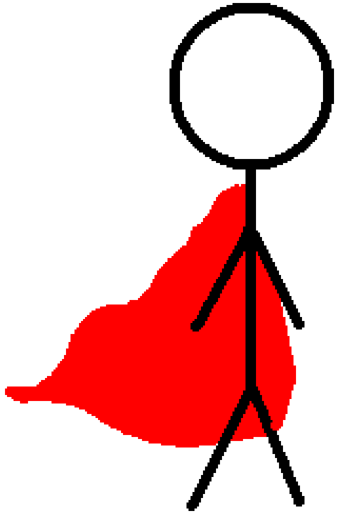
Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables

Marcel Keller, Emmanuela Orsini, **Dragos Rotaru**, Peter Scholl, Eduardo Soria-Vazquez, and Srinivas Vivek

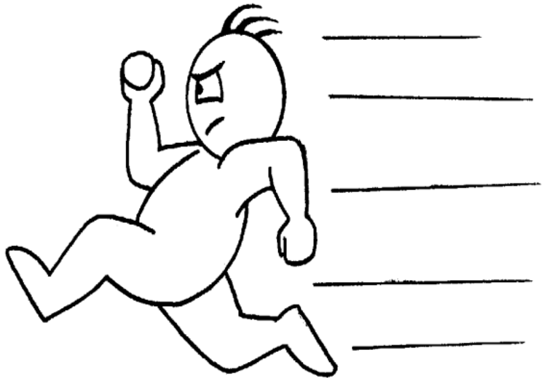
ACNS 2017

University of BRISTOL

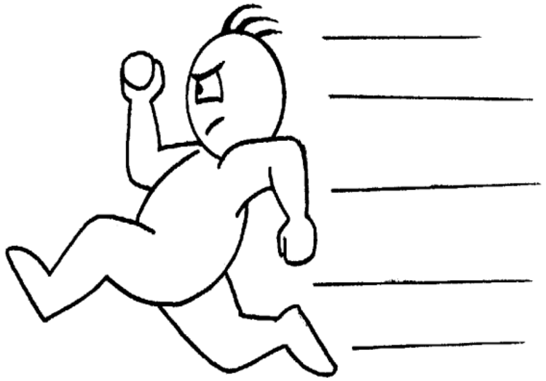
Meet Bob



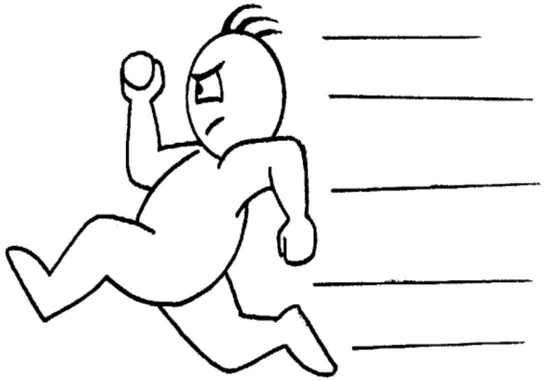
Bob approach to our title:
Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables



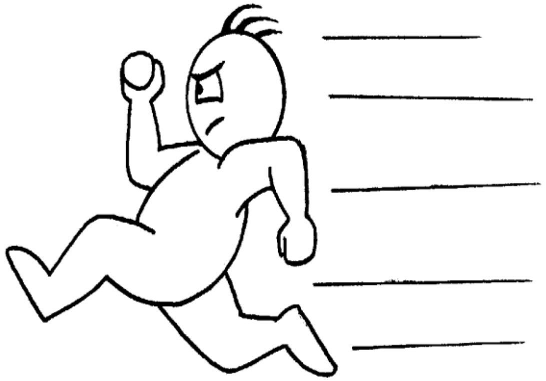
Bob approach to our title:
Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables



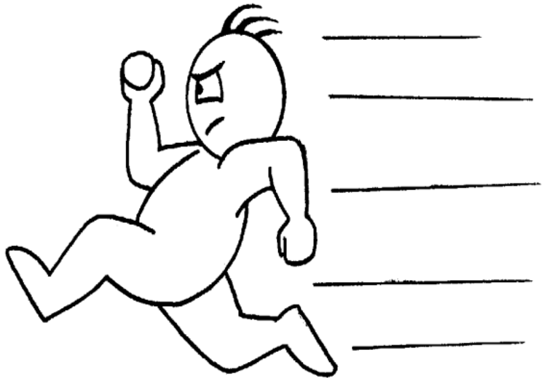
Bob approach to our title: Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables



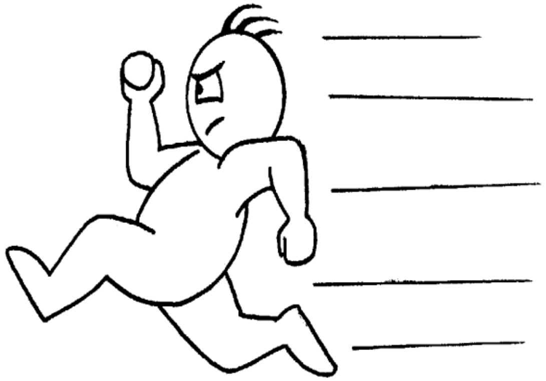
Bob approach to our title: Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables

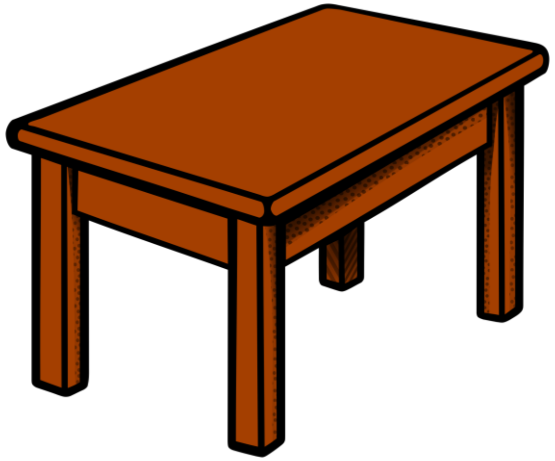


Bob approach to our title:
Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables

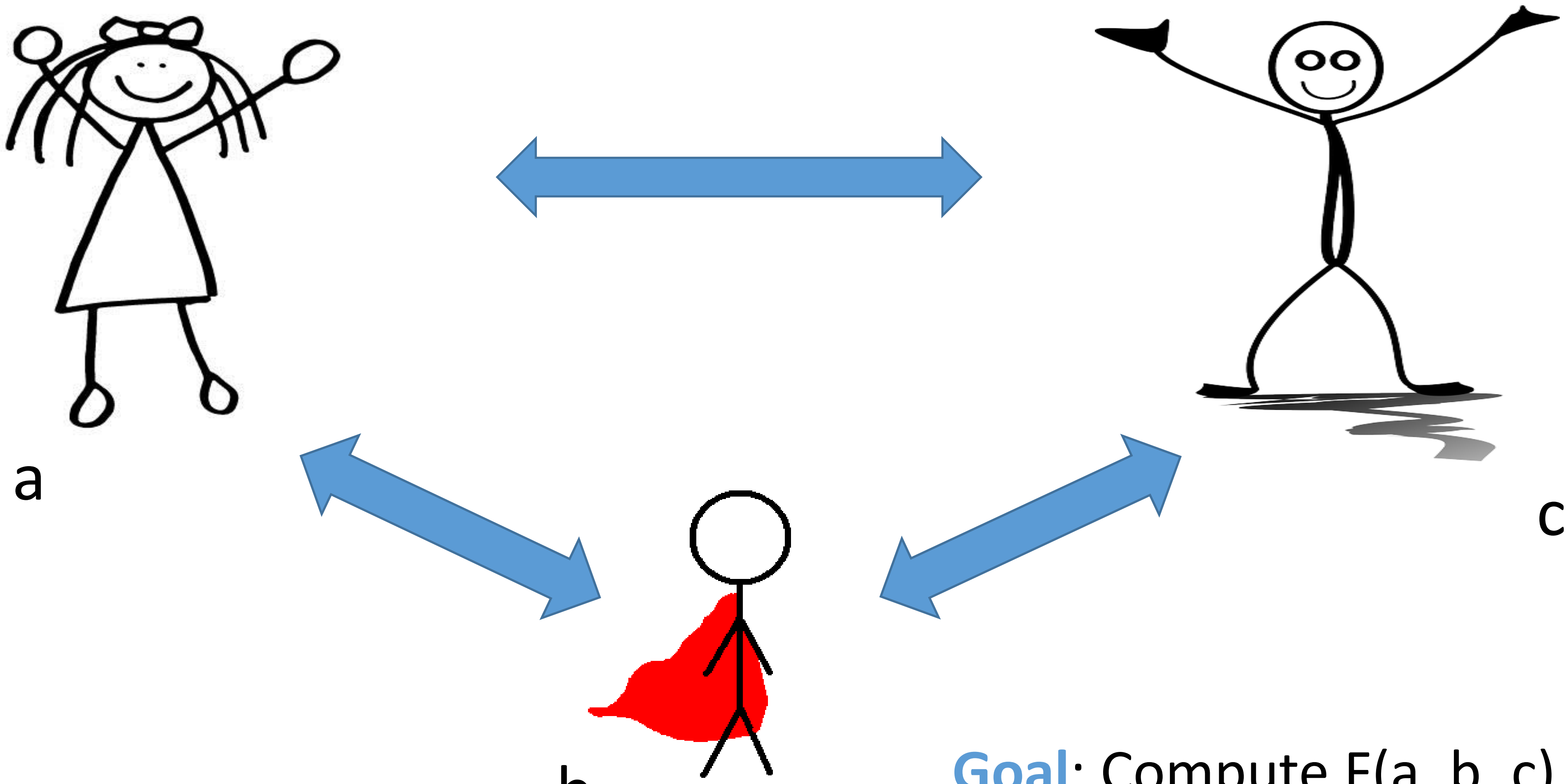


Bob approach to our title:
Faster Secure Multi-Party Computation of AES and DES Using Lookup Tables

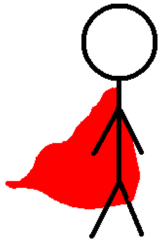




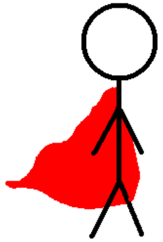
Multi-Party Computation



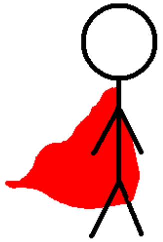
Goal: Compute F(a, b, c).

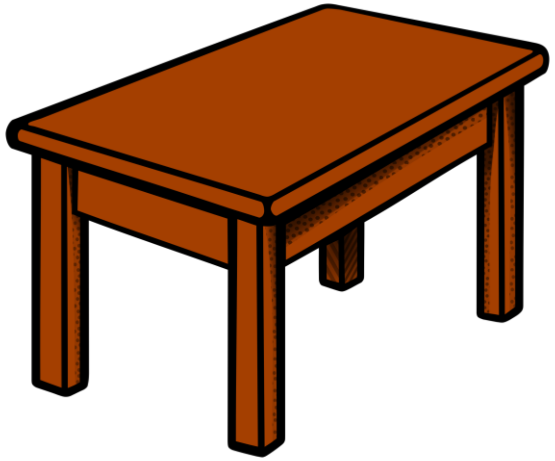


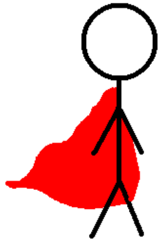
has problems.



has problems.

 has problems.



 has problems?

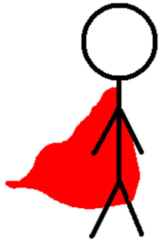
Look-up tables are everywhere in MPC.

Floating Point

Oblivious RAM

Non-linear functions

University of BRISTOL



has problems?

Look-up tables are everywhere in MPC.

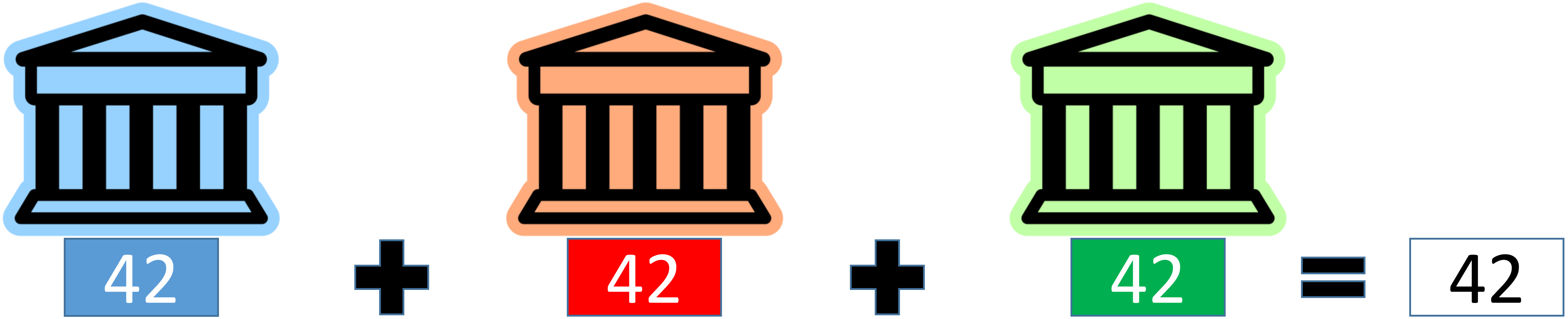
Floating Point

Oblivious RAM

Non-linear functions

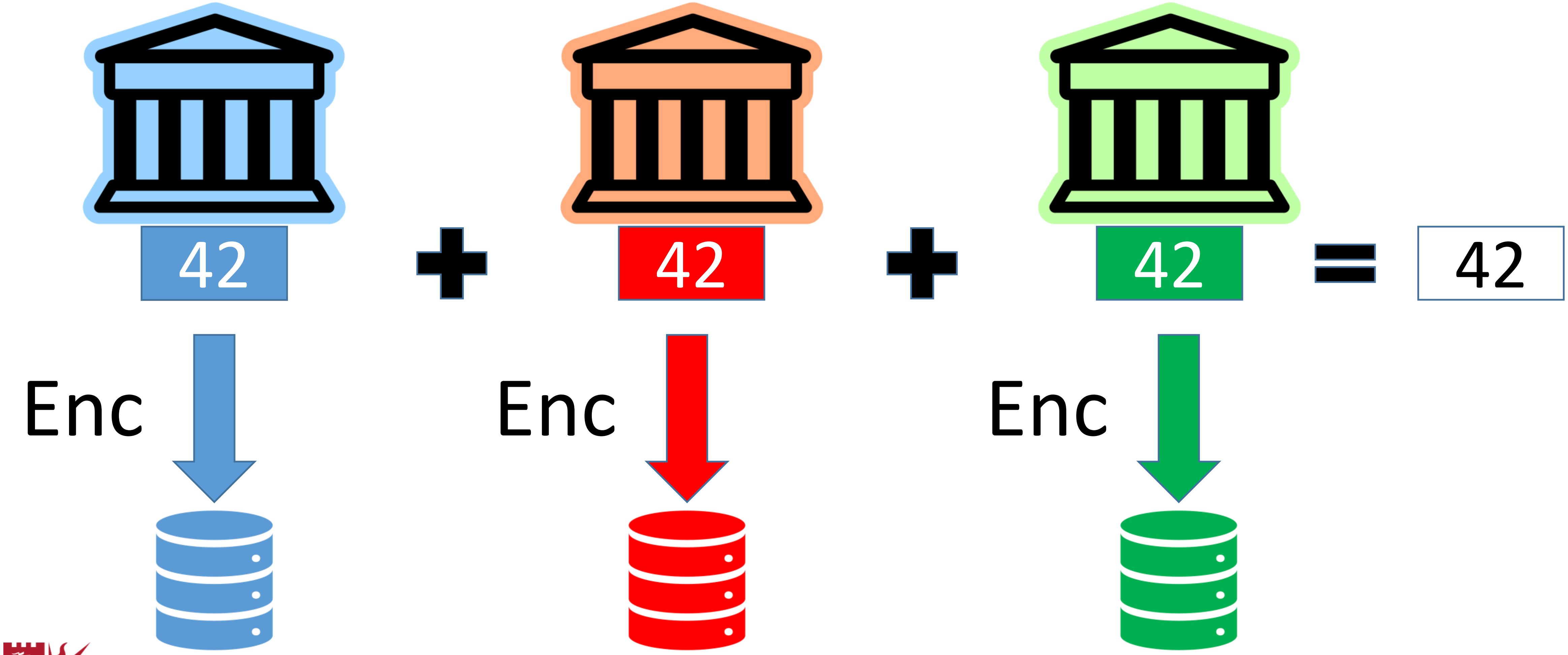
Non-linear? AES and 3-DES

Non-linear? AES and 3-DES



42 + 42 + 42 = 42

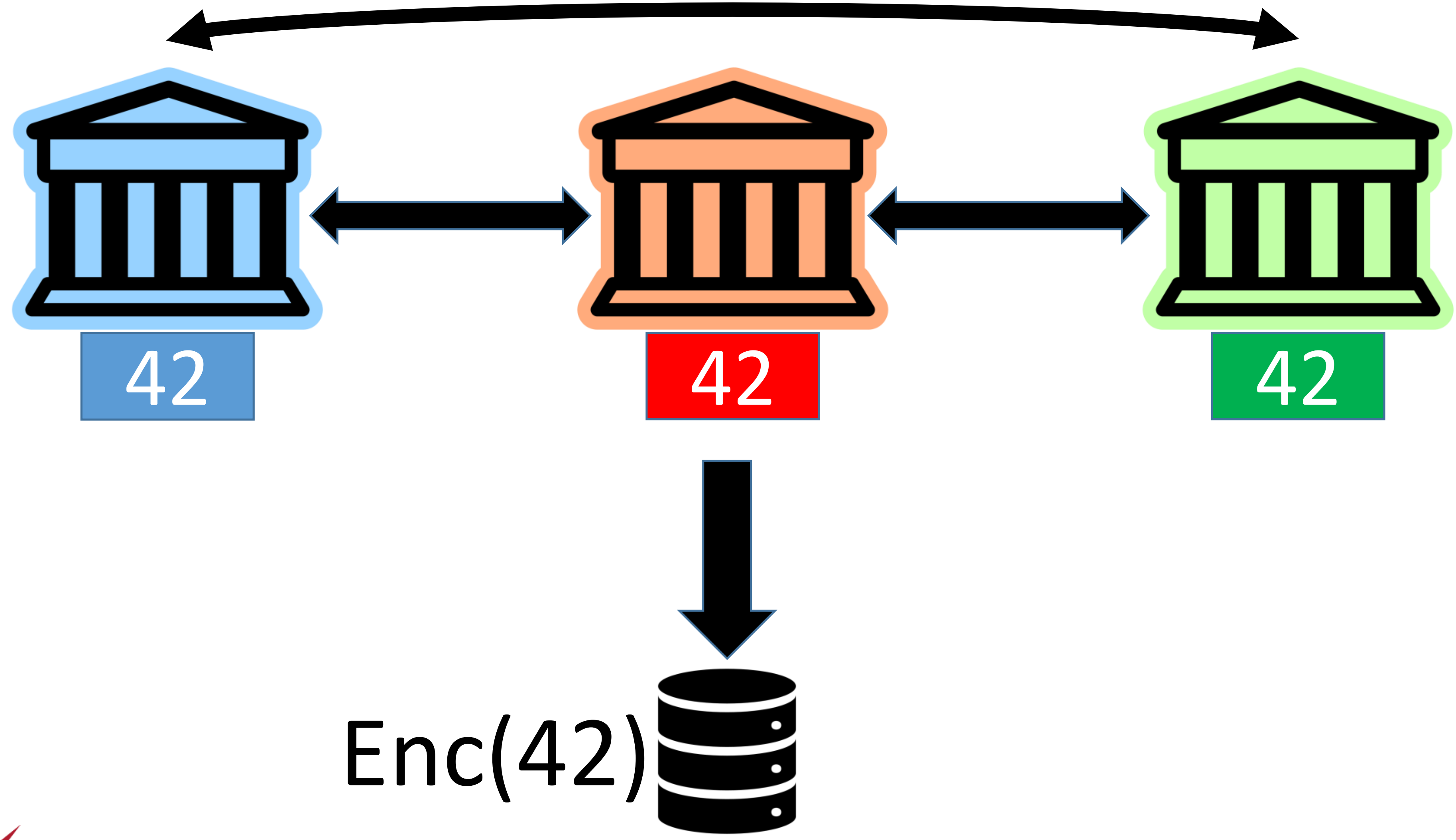
Non-linear? AES and 3-DES



42 + 42 + 42 = 42

Enc Enc Enc

Non-linear? AES and 3-DES



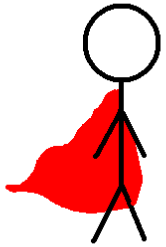
Fastest AES and 3-DES in MPC with malicious security

- Improve on previous AES TinyTable by at least 50 times.
- 3-DES has now 100 times faster online time.
- Apply side-channel countermeasures in the MPC land.

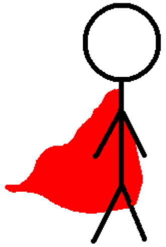
Concurrent Work

- [DNNR16] – TinyTable. Improved version now at Crypto17.
- [DKS+17] – Dessouky et al. in NDSS17. Semi-Honest setting based on 1-out-of-N OT. Also built a compiler which can be used with our protocol.

MPC with Secret Sharing 101



MPC with Secret Sharing 101



$$x = x_1 + \cdots + x_n$$

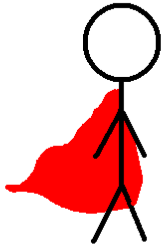
Each P_i has $[x] \leftarrow x_i$

$[x] \leftarrow x_2$

$[x] \leftarrow x_1$

$[x] \leftarrow x_3$

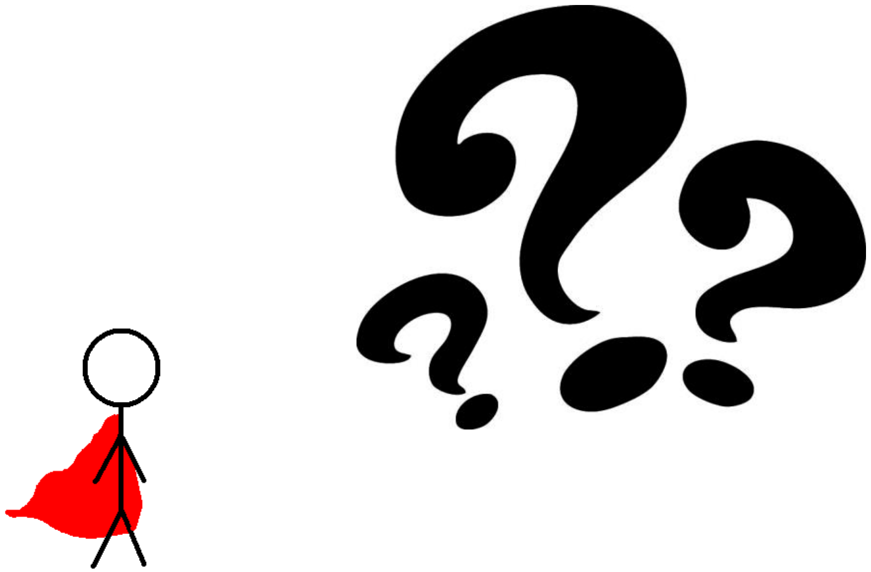
MPC Preprocessing Phase



Generate Triples.

[c] = [a][b]

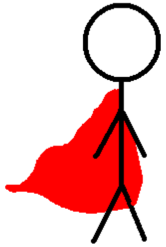
MPC Preprocessing Phase



Generate Triples.

$[c] = [a][b]$

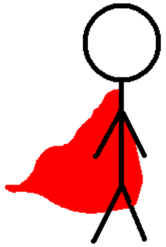
MPC Preprocessing Phase



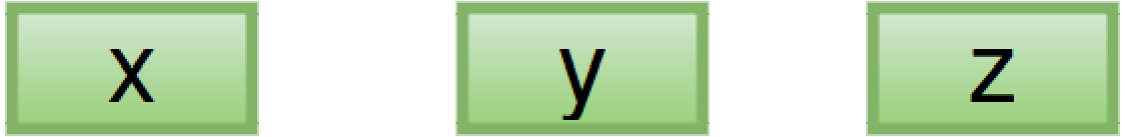
MPC Online Phase

Use Triples.

MPC Online Phase



MPC Circuit Evaluation

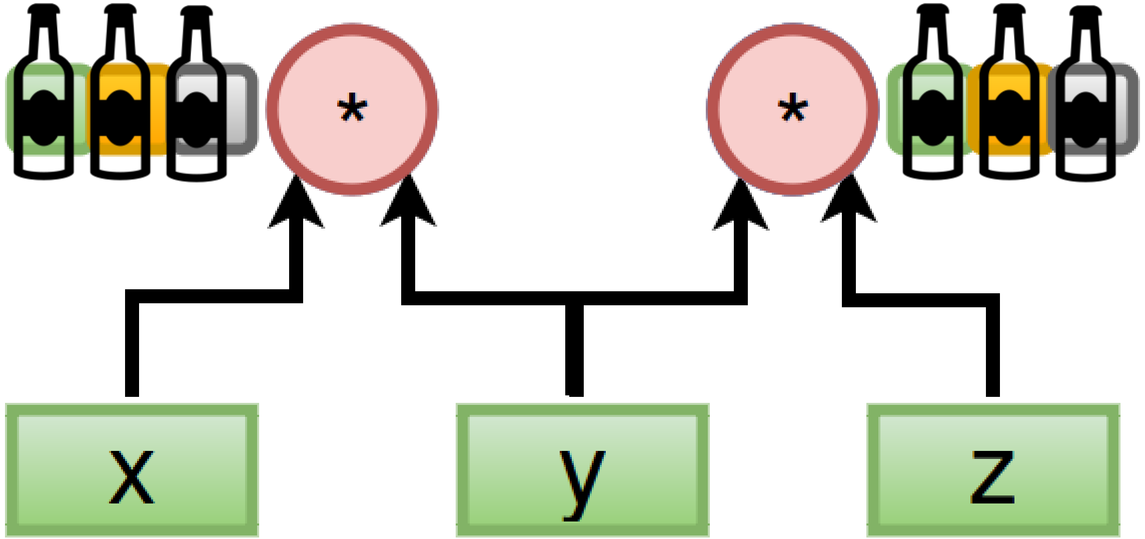


x

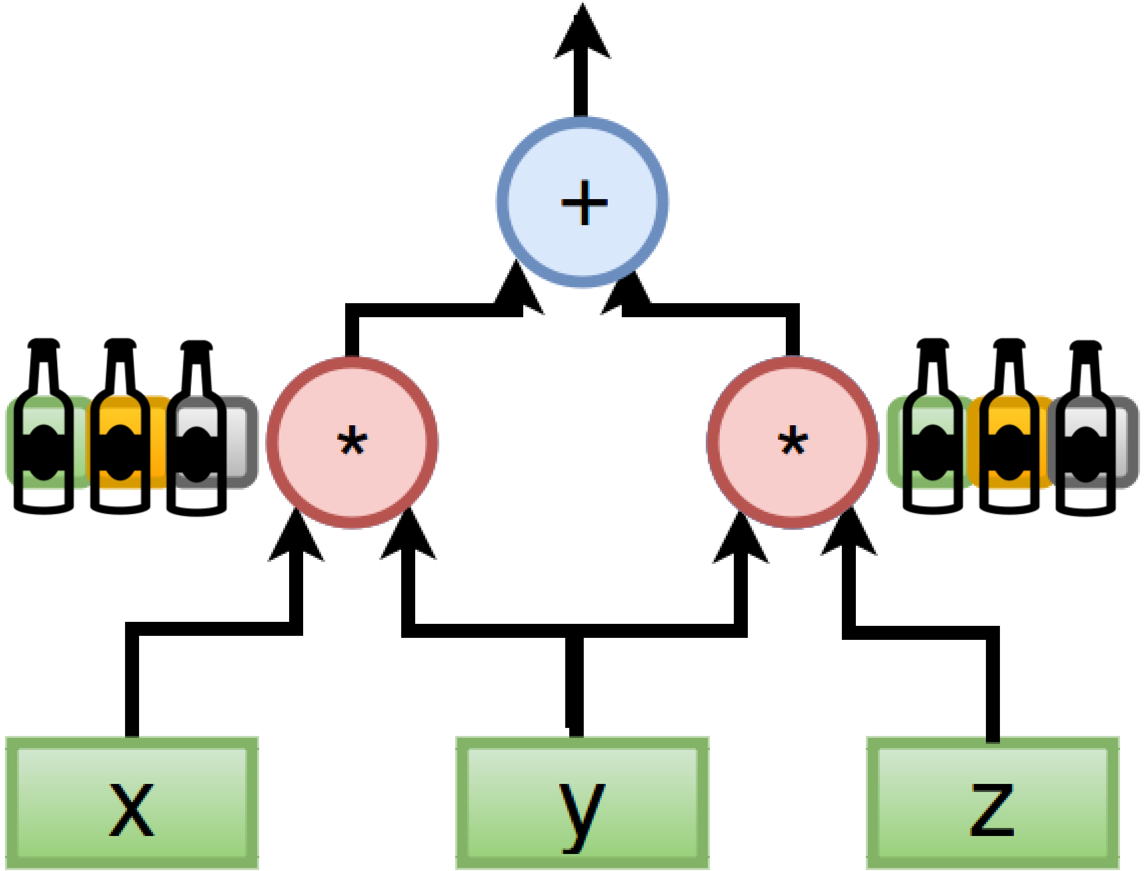
y

z

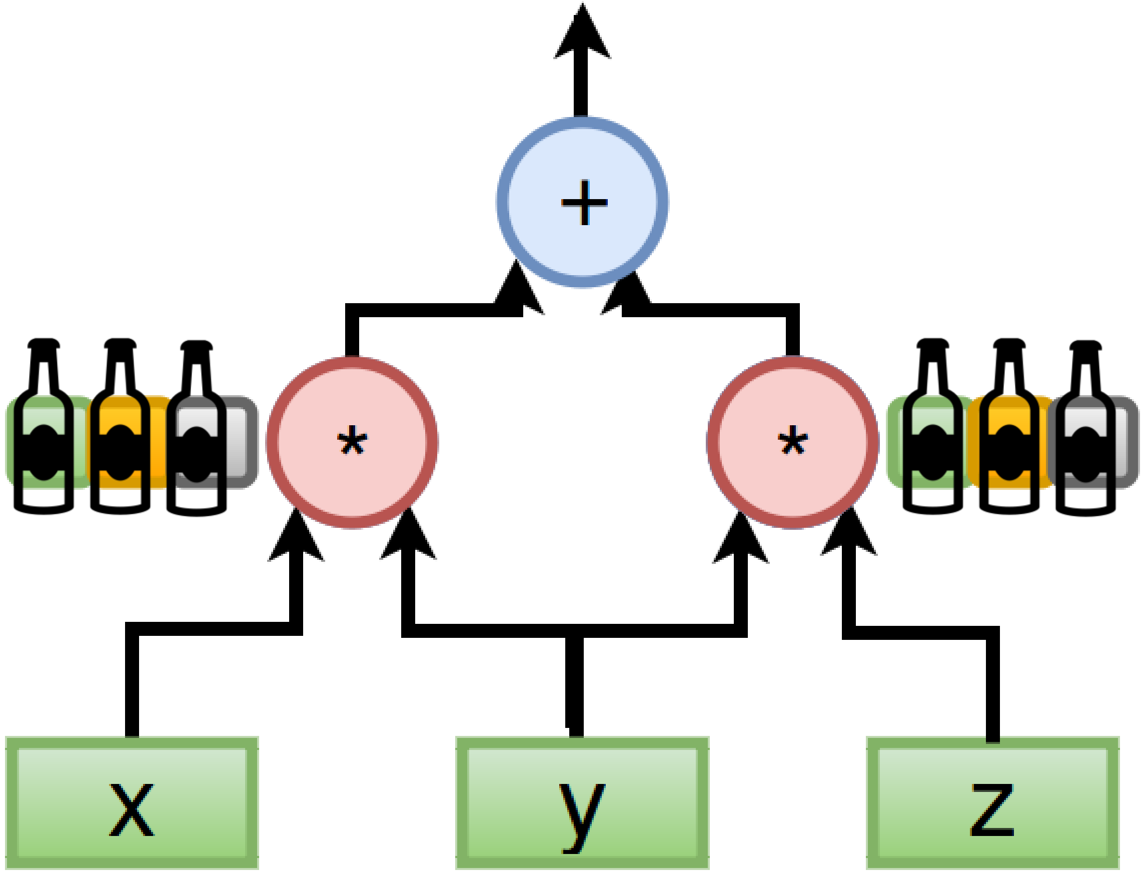
MPC Circuit Evaluation



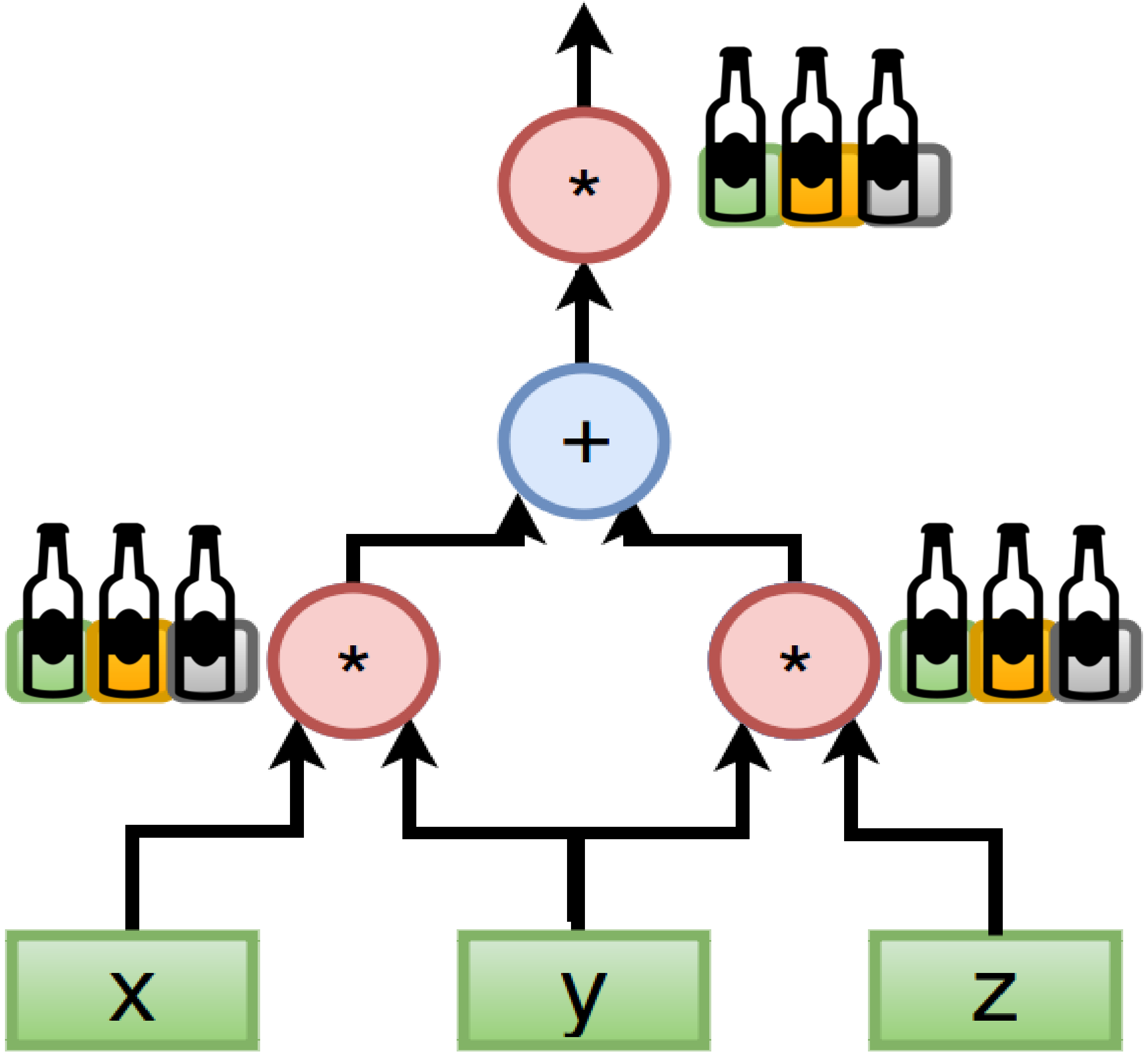
MPC Circuit Evaluation



MPC Circuit Evaluation



MPC Circuit Evaluation

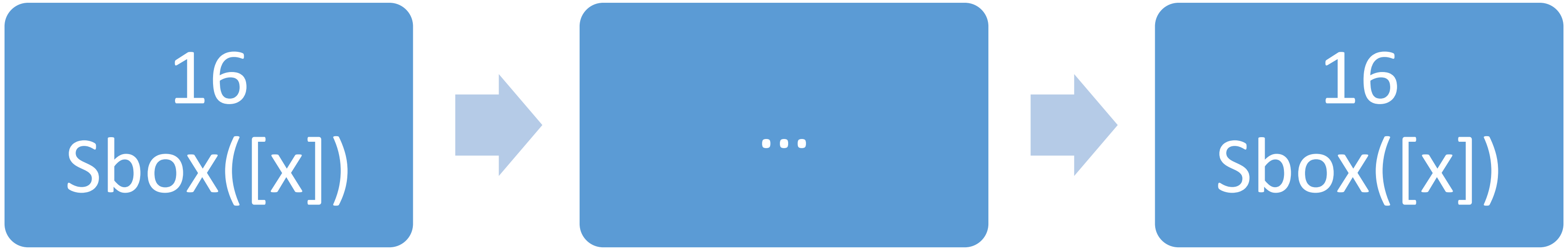


3 triples.

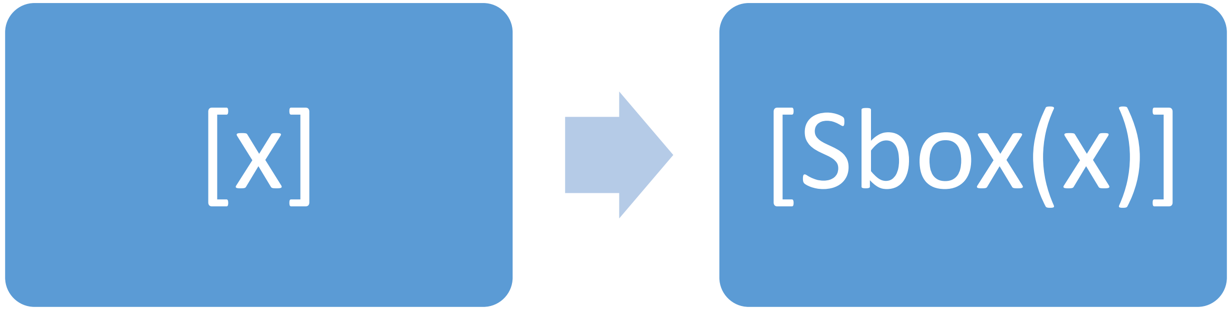
2 rounds.

AES-128

10 rounds



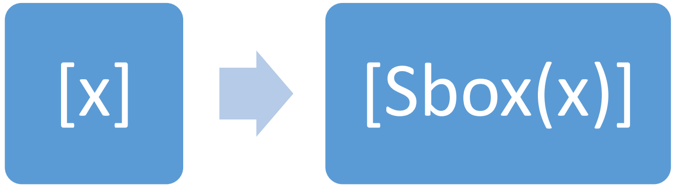
How to Sbox



[x]

[Sbox(x)]

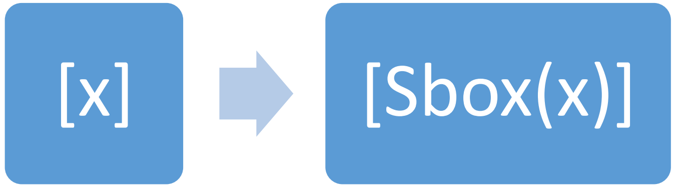
How to Sbox



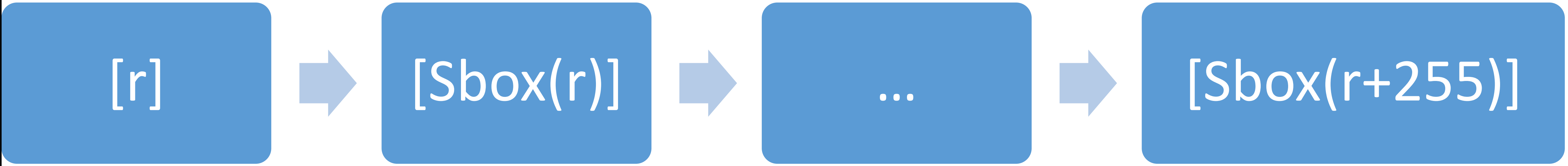
[x]

[Sbox(x)]

How to Sbox

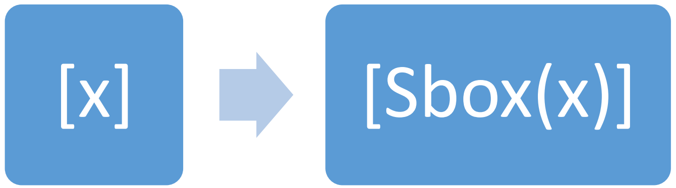


[x] → [Sbox(x)]

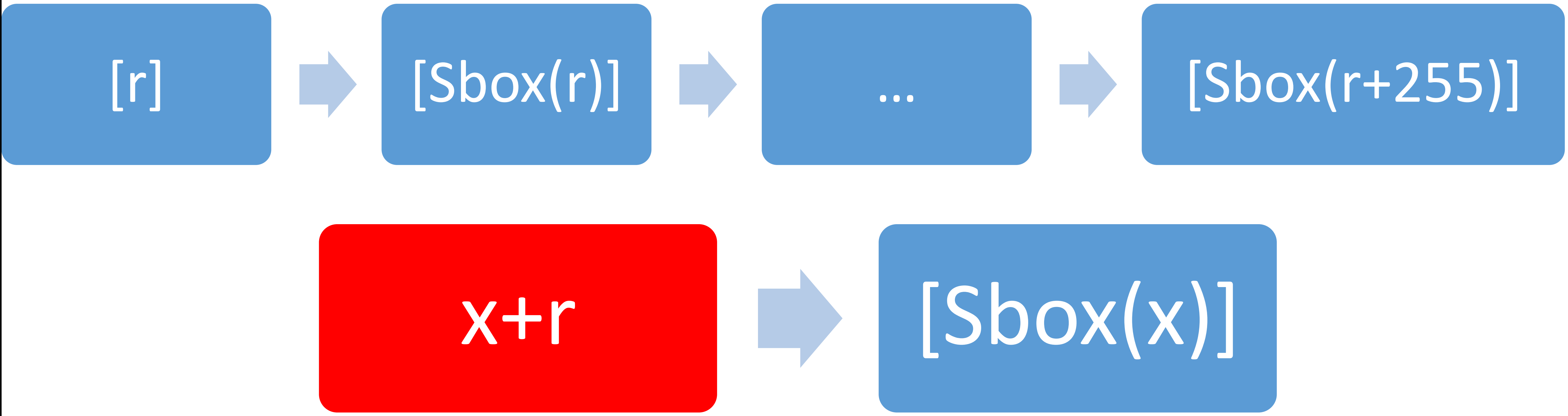


[r] → [Sbox(r)] → … → [Sbox(r+255)]

How to Sbox



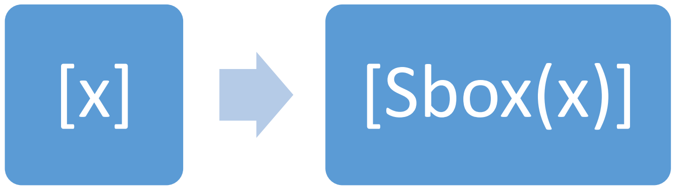
[x] → [Sbox(x)]

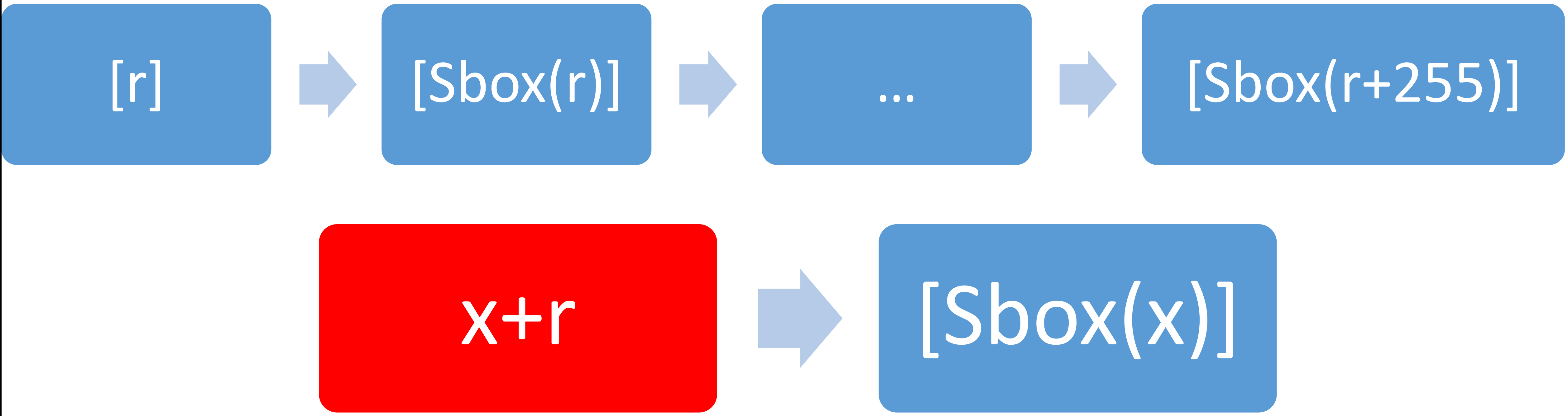


[r] → [Sbox(r)] → … → [Sbox(r+255)]

x+r → [Sbox(x)]

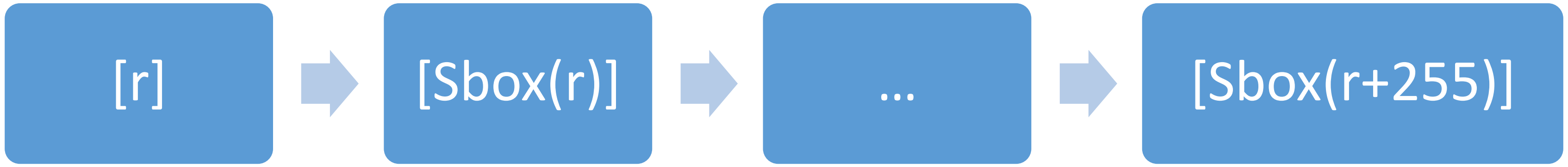
How to Sbox





At pos (x+r) => Sbox(r + x + r)

How to pre-Sbox



[r]

[Sbox(r)]

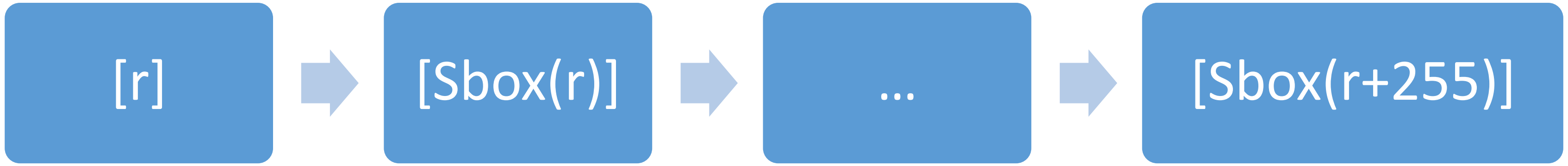
…

[Sbox(r+255)]

Take random [r].

Compute [Sbox(r)], … [Sbox(r+255)]

How to pre-Sbox

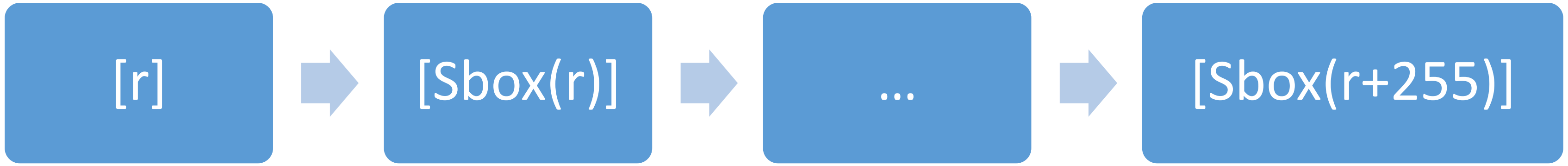


Take random [r].

Compute [Sbox(r)], … [Sbox(r+255)]

7 mults.

How to pre-Sbox



[r]

[Sbox(r)]

…

[Sbox(r+255)]

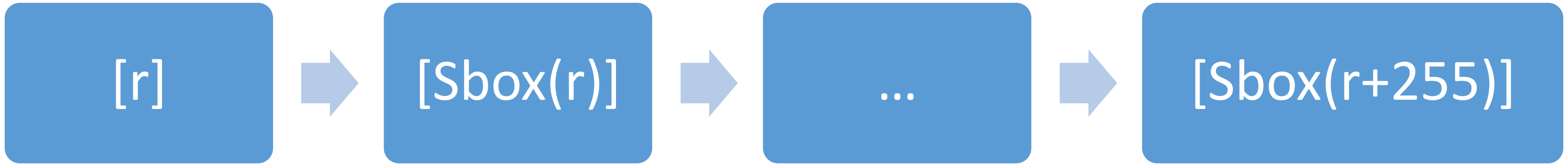
Take random [r].

Compute [Sbox(r)], … [Sbox(r+255)]

7 mults.

7 mults.

How to pre-Sbox



[r]

[Sbox(r)]

…

[Sbox(r+255)]

Take random [r].

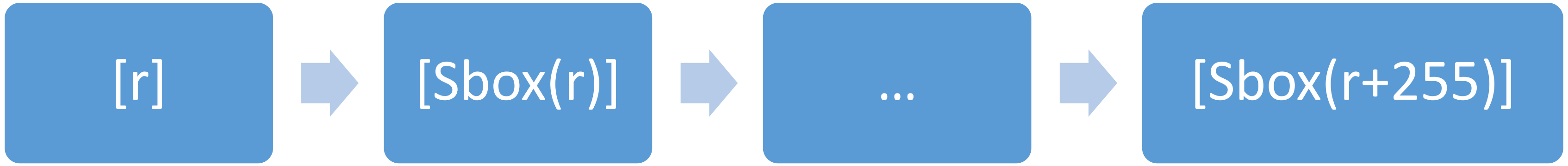
Compute [Sbox(r)], … [Sbox(r+255)]

7 mults.

7 mults.

1792 mults.

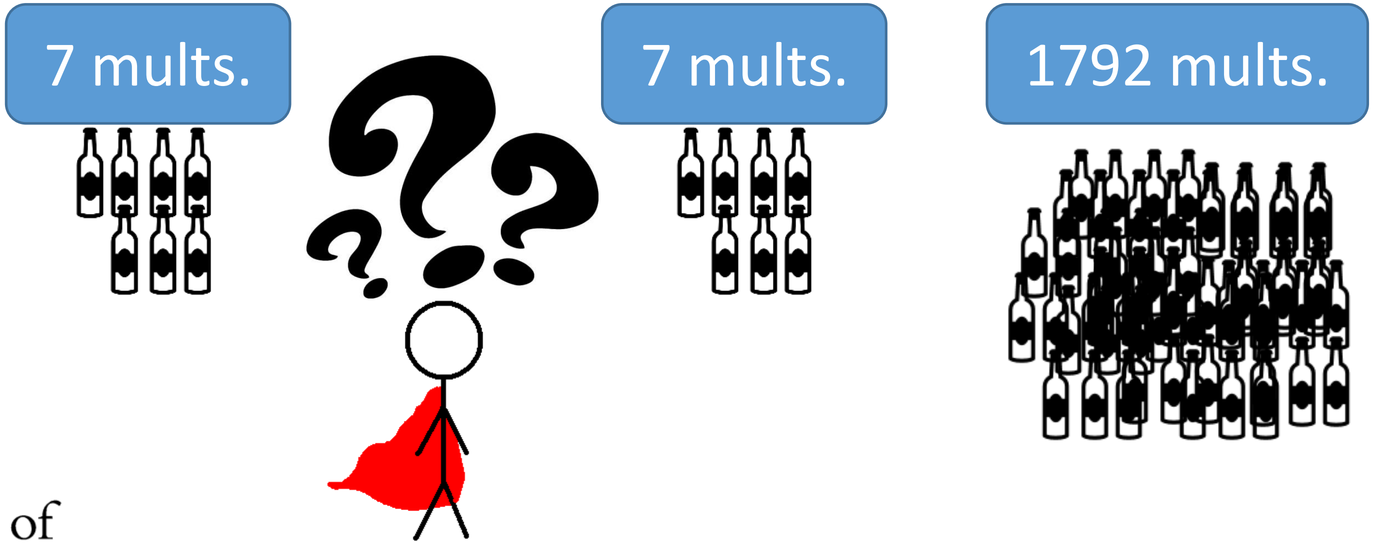
How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

Take random [r].

Compute [Sbox(r)], … [Sbox(r+255)]

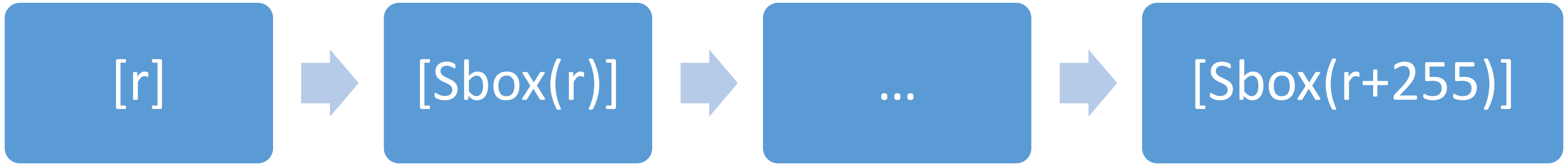


7 mults.

7 mults.

1792 mults.

How to pre-Sbox



[r]

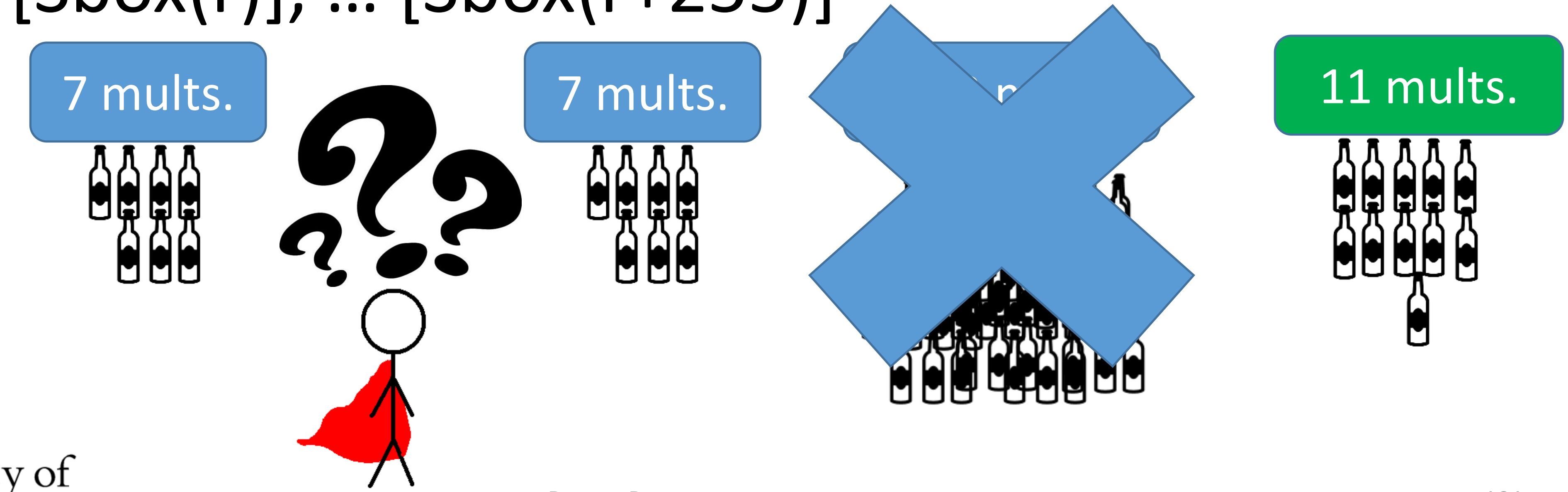
[Sbox(r)]

…

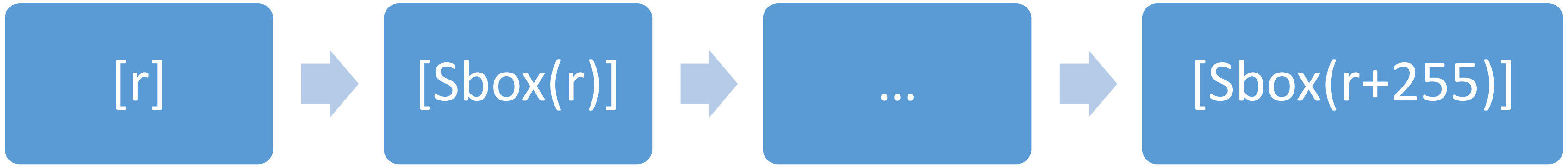
[Sbox(r+255)]

Take random [r].

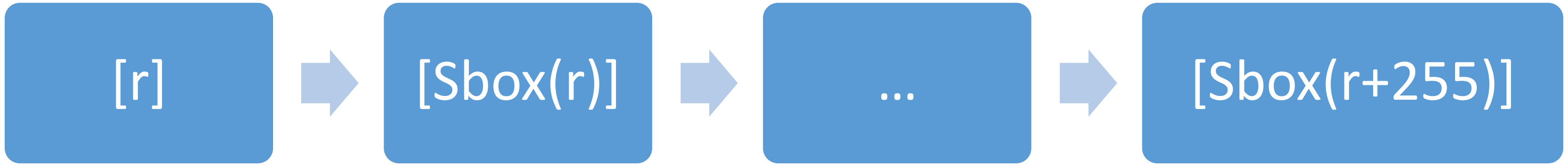
Compute [Sbox(r)], … [Sbox(r+255)]



How to pre-Sbox



How to pre-Sbox



[r]

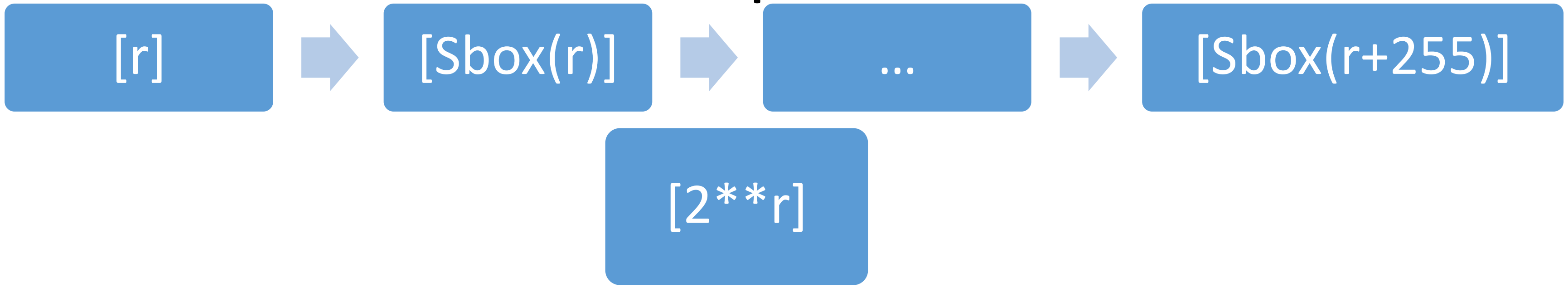
[Sbox(r)]

…

[Sbox(r+255)]

- Take random [r].
- Compute v = Bits(pow(2, [r])).
- Take every cyclic rotation of the Sbox row and compute <v, Sbox>

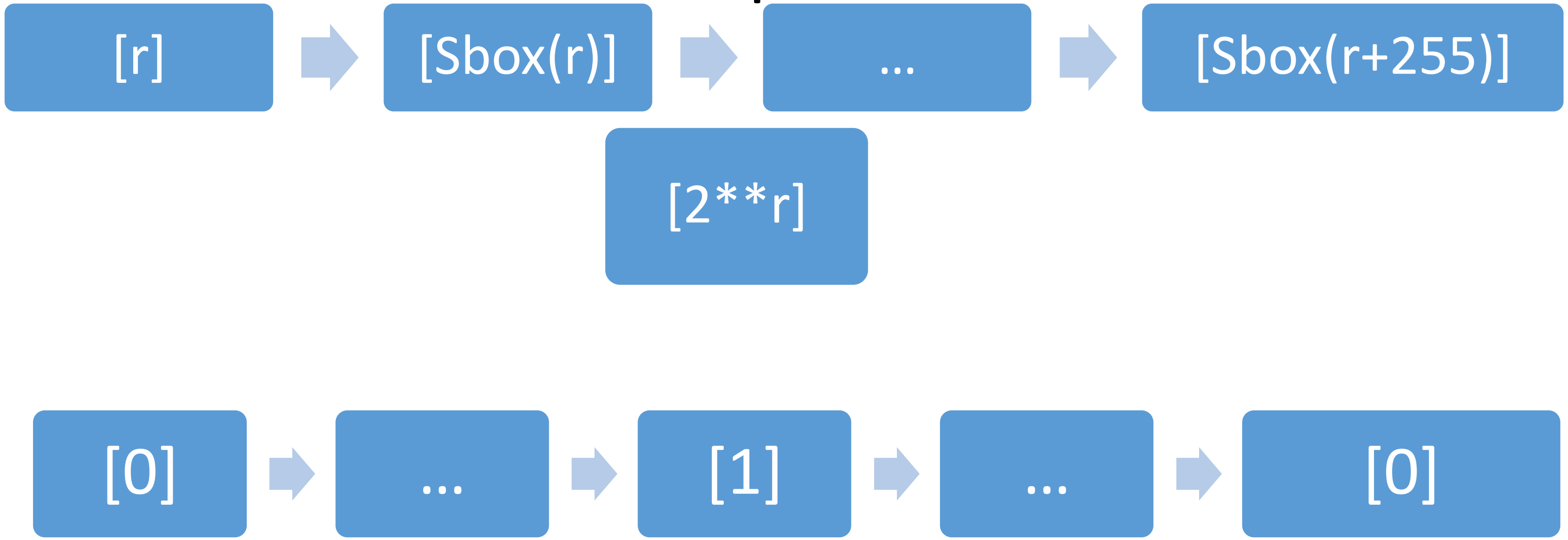
How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

[2**r]

How to pre-Sbox

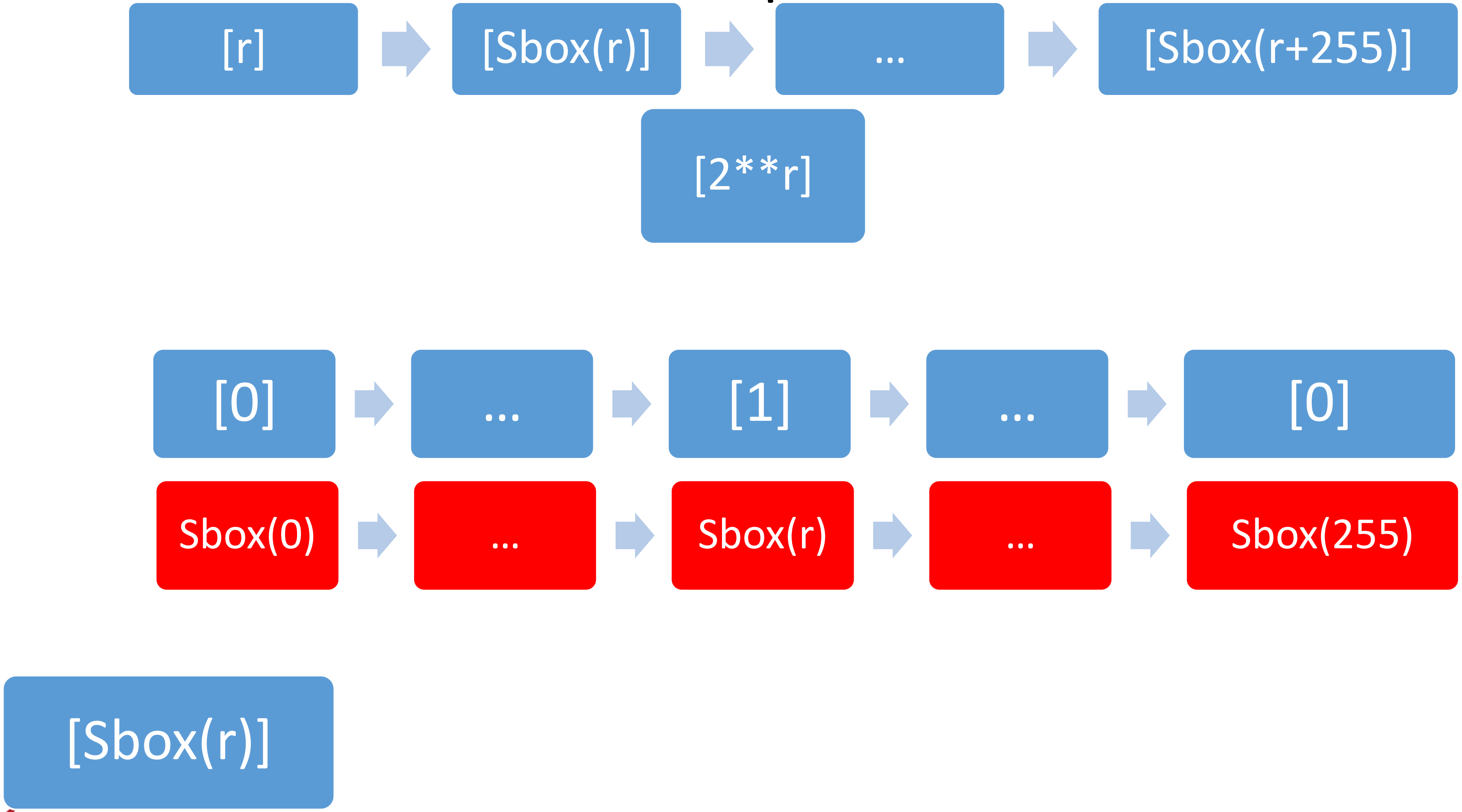


[r] → [Sbox(r)] → … → [Sbox(r+255)]

[2**r]

[0] → … → [1] → … → [0]

How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

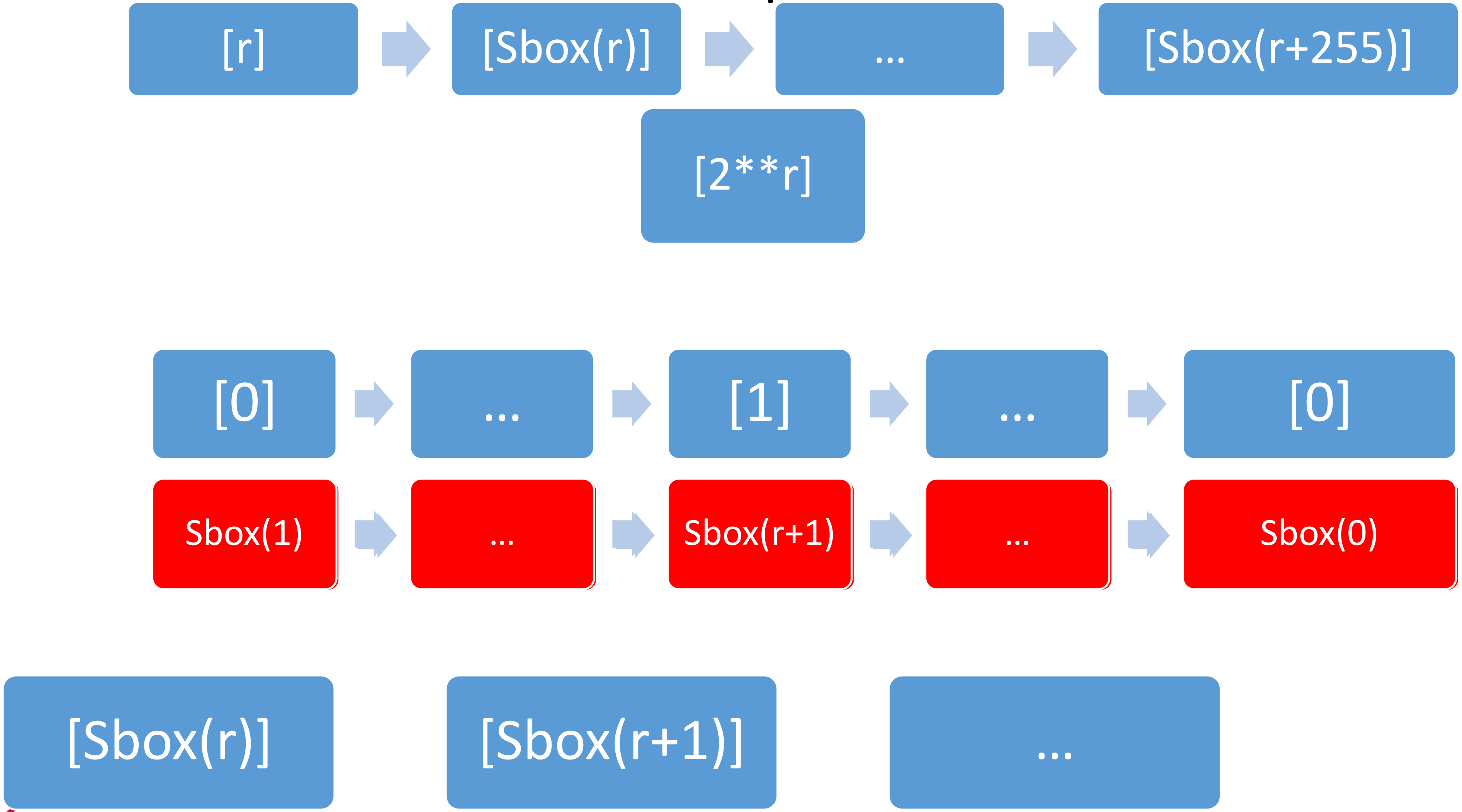
[2**r]

[0] → … → [1] → … → [0]

Sbox(0) → … → Sbox(r) → … → Sbox(255)

[Sbox(r)]

How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

[2**r]

[0] → … → [1] → … → [0]

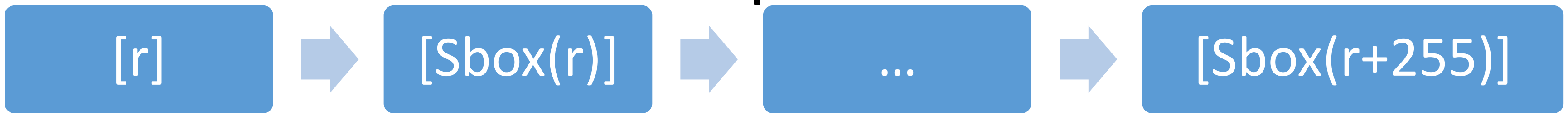
Sbox(1) → … → Sbox(r+1) → … → Sbox(0)

[Sbox(r)]

[Sbox(r+1)]

…

How to pre-Sbox



[r]

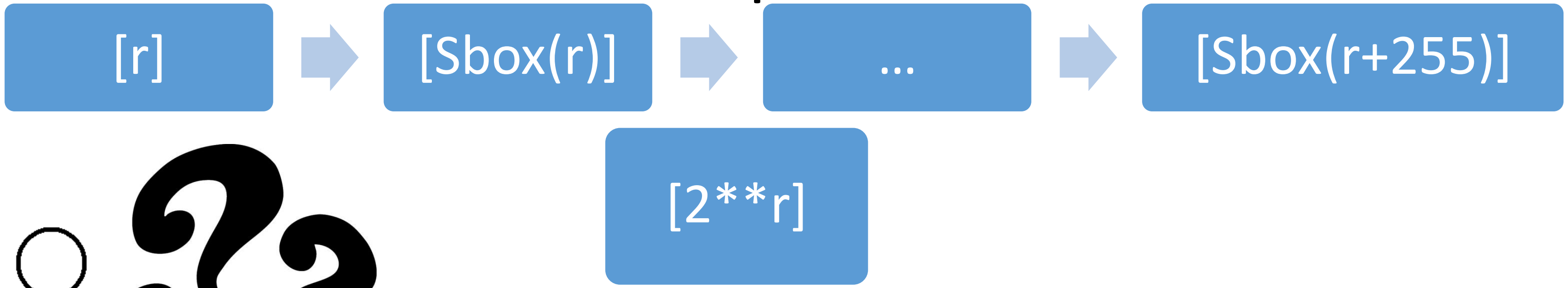
[Sbox(r)]

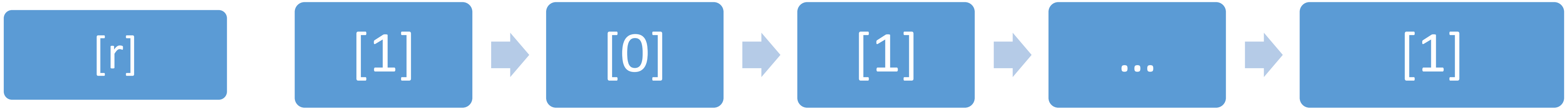
…

[Sbox(r+255)]

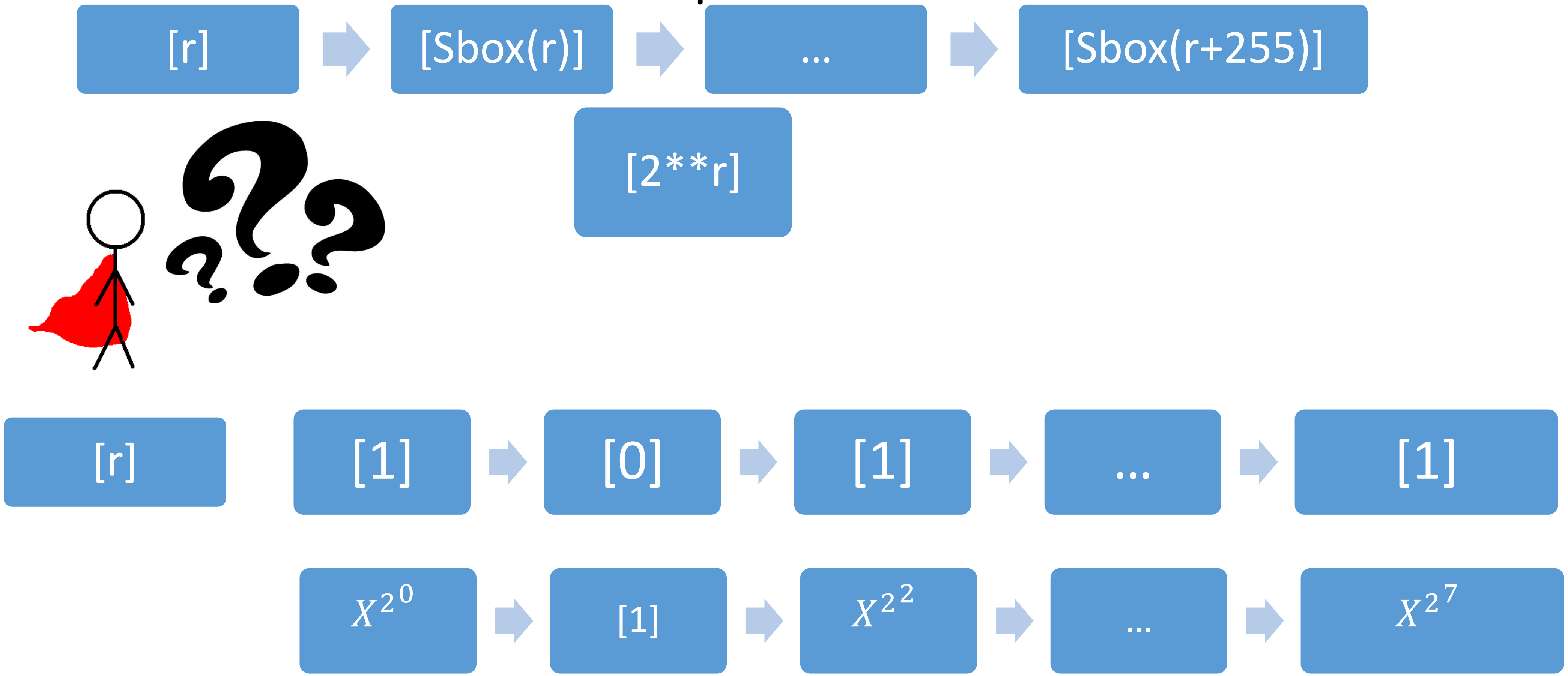
[2**r]

How to pre-Sbox





How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

[2**r]

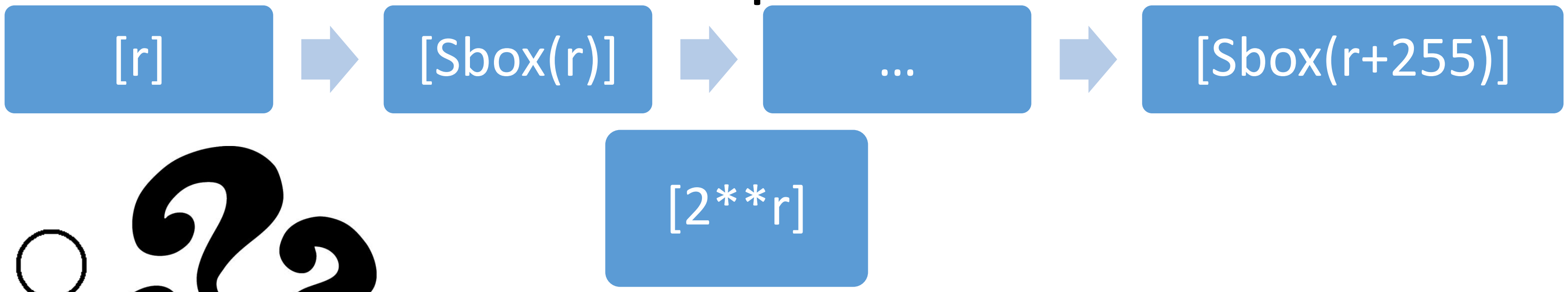
[r]

[1] → [0] → [1] → … → [1]

X^{2^0} → [1] → X^{2^2} → … → X^{2^7}

$$[X^r] = [2^r] \in GF(2^n)$$

How to pre-Sbox



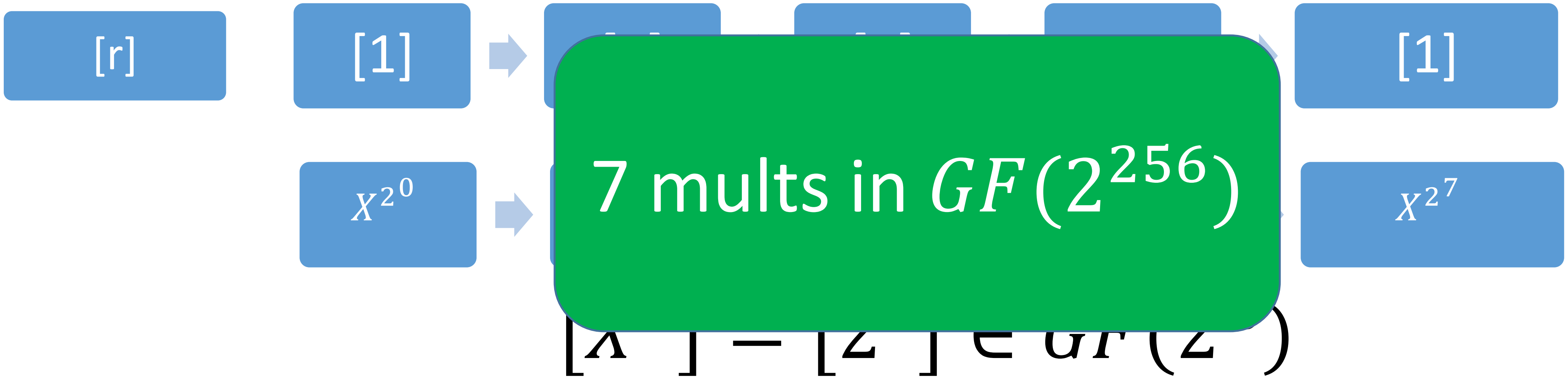
[r]

[Sbox(r)]

…

[Sbox(r+255)]

[2**r]



[r]

[1]

[1]

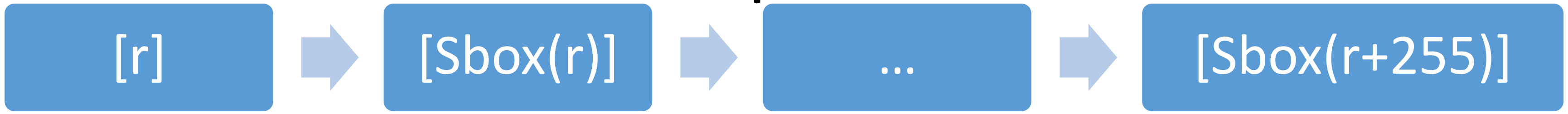
X^{2^0}

X^{2^7}

7 mults in $GF(2^{256})$

$[X\ ] = [2\ ] \in GF(2\ )$

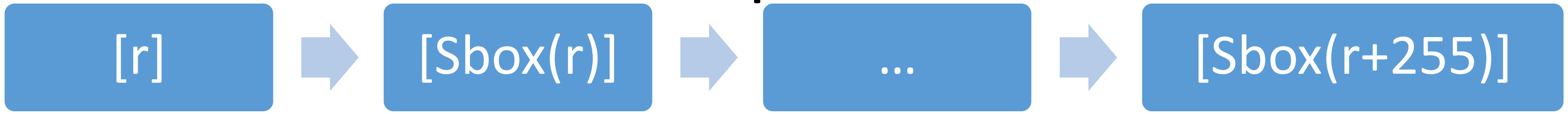
How to pre-Sbox


[r] → [Sbox(r)] → … → [Sbox(r+255)]

[KOS16]

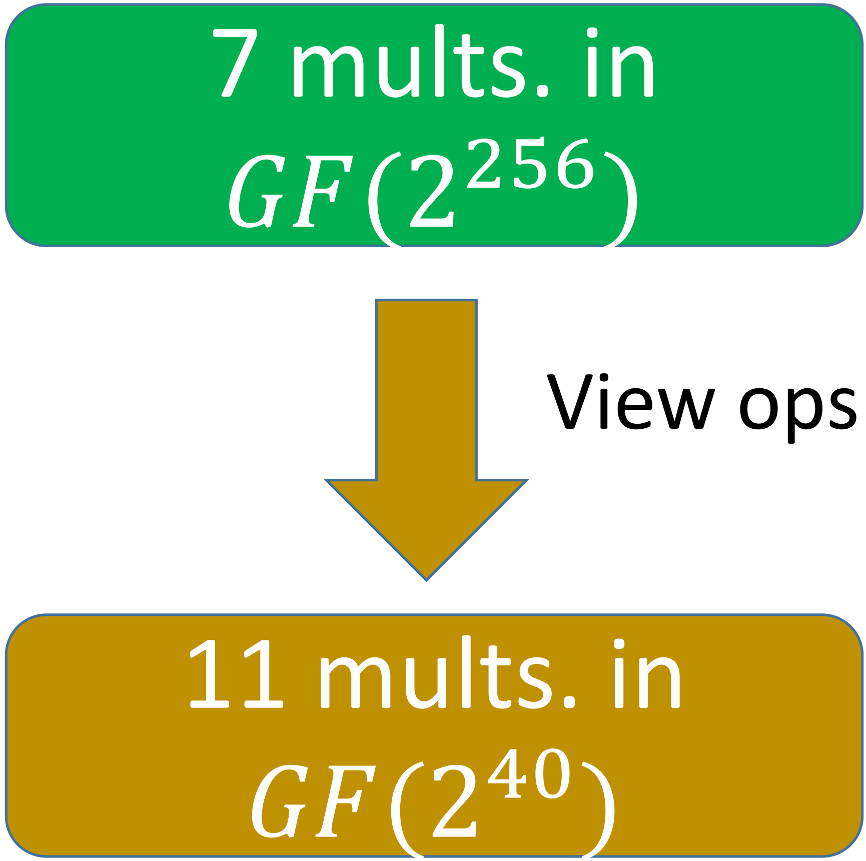
7 mults. in $GF(2^{256})$

How to pre-Sbox



[r] → [Sbox(r)] → … → [Sbox(r+255)]

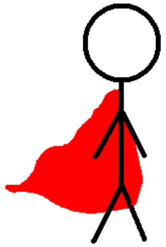
[KOS16]



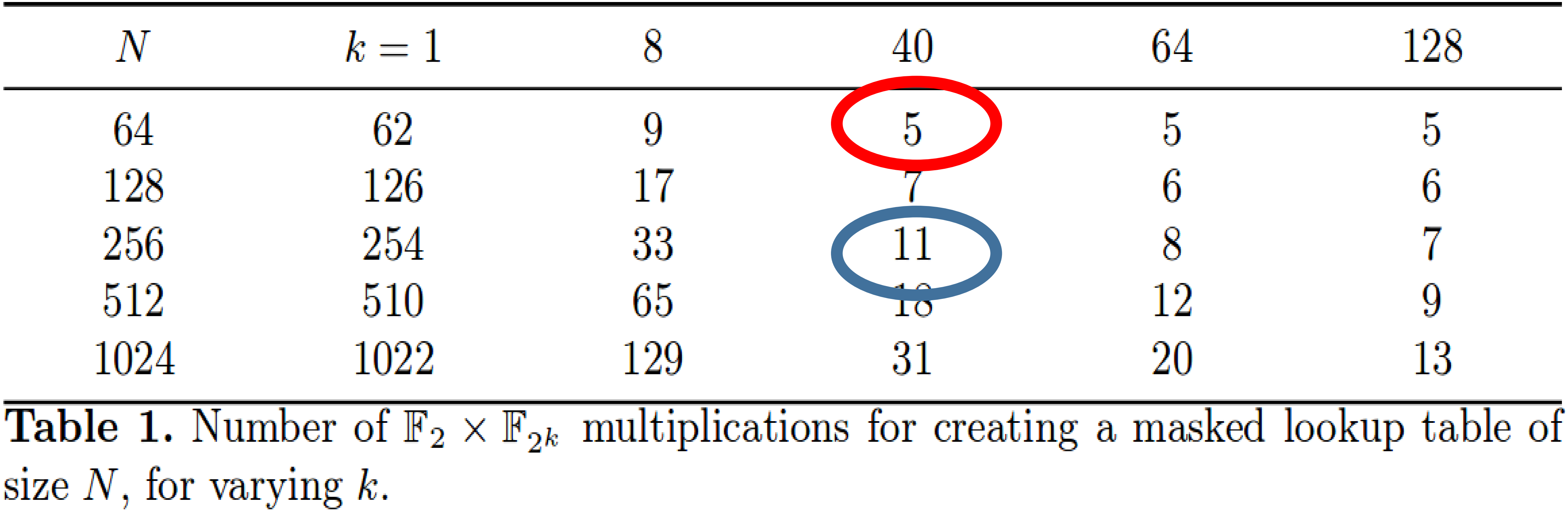
7 mults. in $GF(2^{256})$

View ops. as polys in $GF(2^k)$

11 mults. in $GF(2^{40})$



TLDR;



N	$k = 1$	8	40	64	128
64	62	9	5	5	5
128	126	17	7	6	6
256	254	33	11	8	7
512	510	65	18	12	9
1024	1022	129	31	20	13

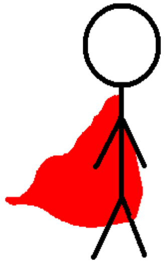
Table 1. Number of $\mathbb{F}_2 \times \mathbb{F}_{2^k}$ multiplications for creating a masked lookup table of size N, for varying k.

Side-Channel inspired techniques.

- Write Sbox(x) as a poly with minimal non-linear multiplications, ie squares are for free.
- AES Sbox requires 4 non-linear mults.
- DES Sbox requires 3 non-linear mults.

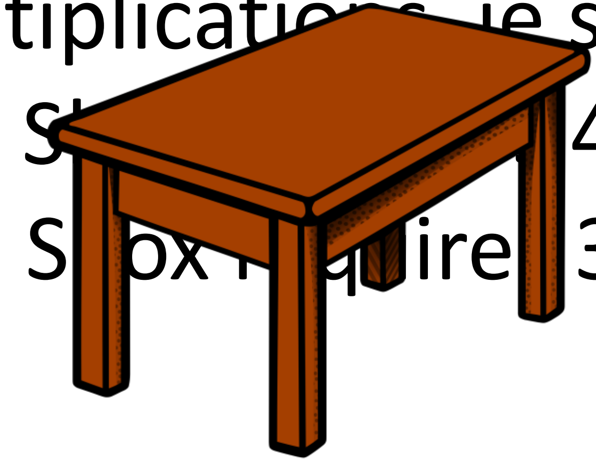
Side-Channel inspired techniques.

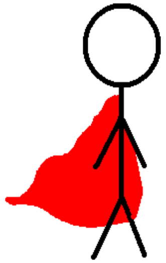
- Write Sbox(x) as a poly with minimal non-linear multiplications, ie squares are for free.
- AES Sbox requires 4 non-linear mults.
- DES Sbox requires 3 non-linear mults.



Side-Channel inspired techniques.

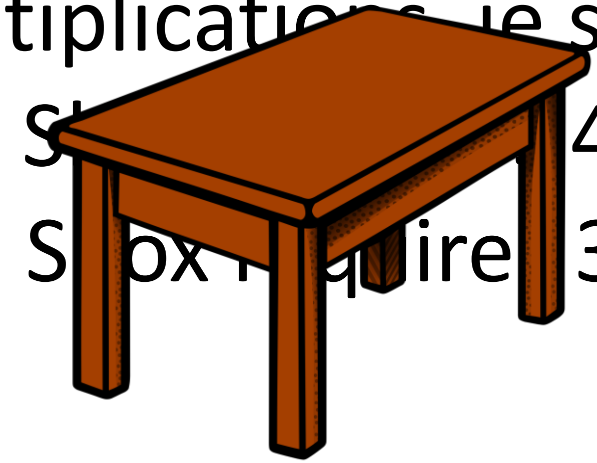
- Write Sbox(x) as a poly with minimal non-linear multiplicati ie squares are for free.
- AES S 4 non-linear mults.
- DES S ox r quire 3 non-linear mults.

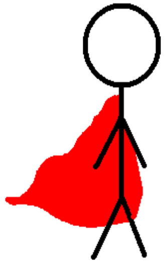




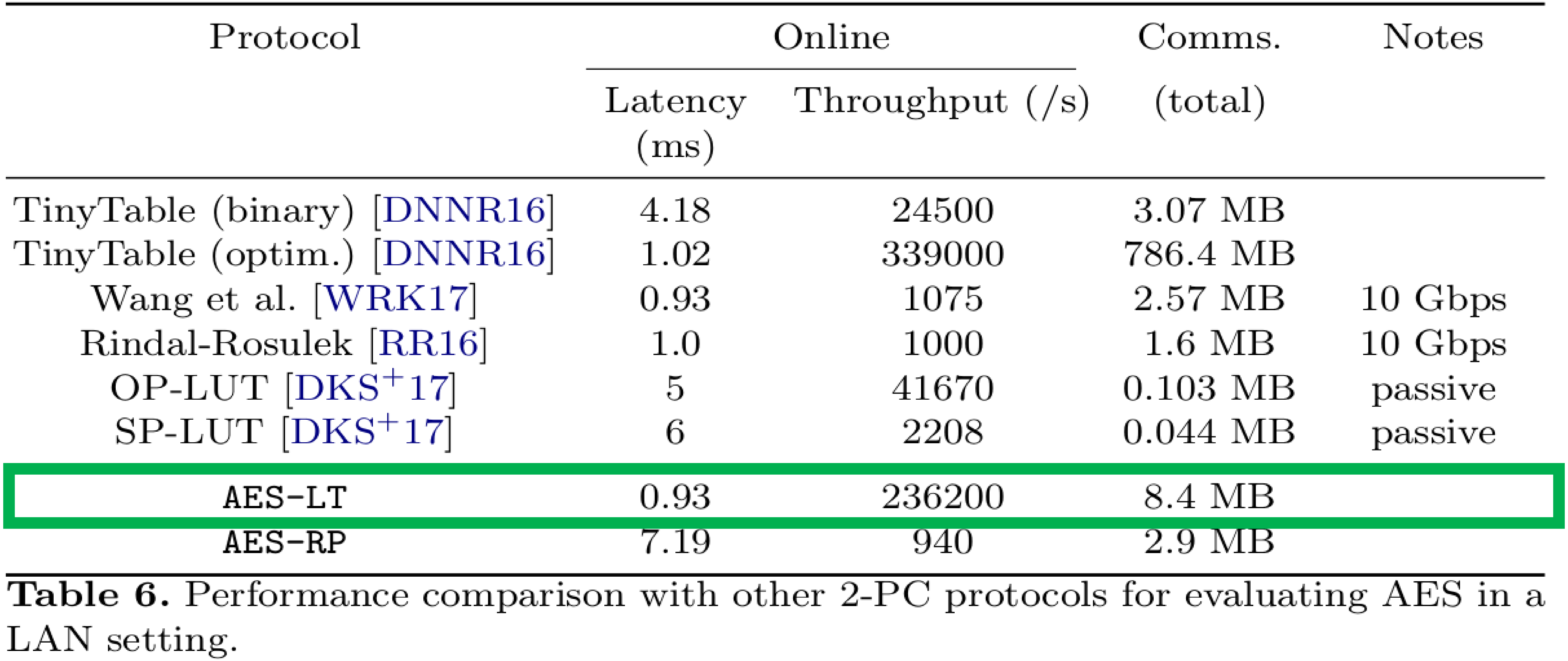
Side-Channel inspired techniques.

- Write Sbox(x) as a poly with minimal non-linear multiplications, ie squares are for free.
- AES Sbox requires 4 non-linear mults.
- DES Sbox requires 3 non-linear mults.





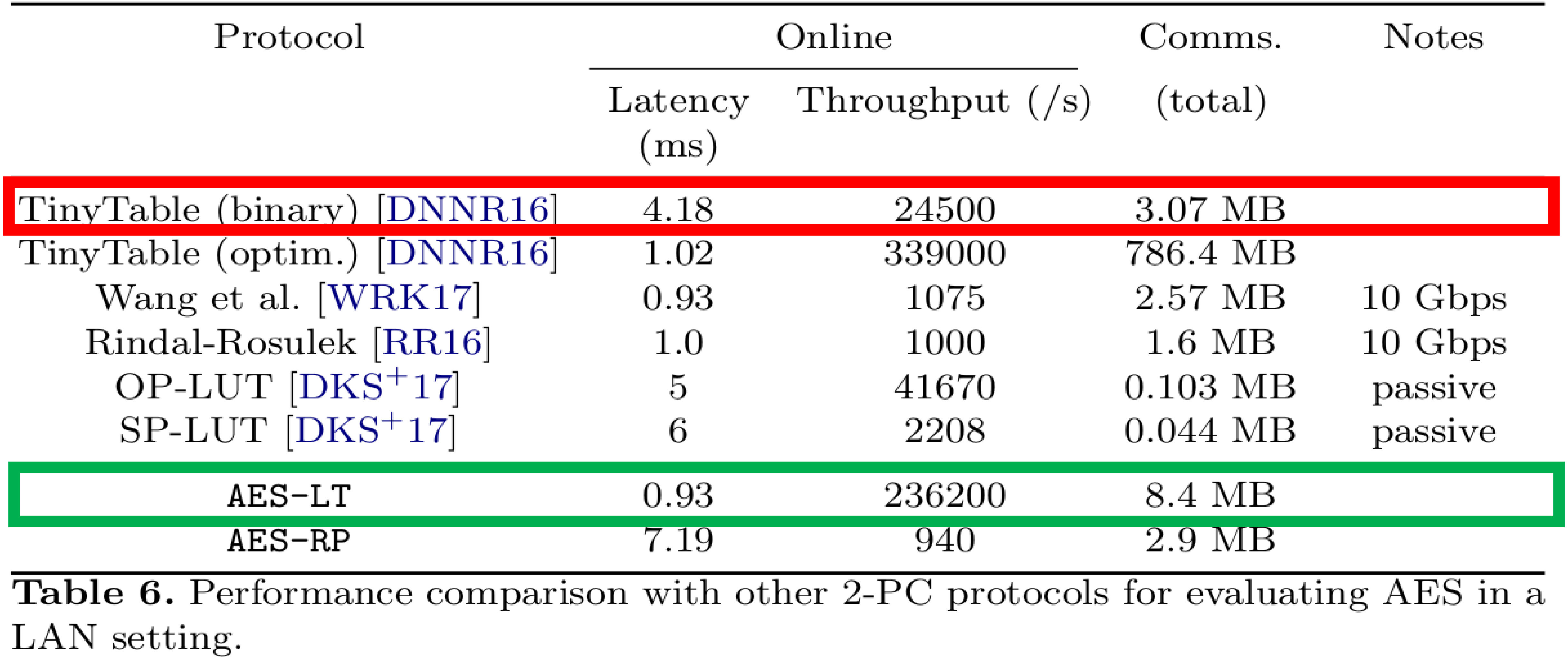
Faster is…faster.



Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	3.07 MB	
TinyTable (optim.) [DNNR16]	1.02	339000	786.4 MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS^{+}17]	5	41670	0.103 MB	passive
SP-LUT [DKS^{+}17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

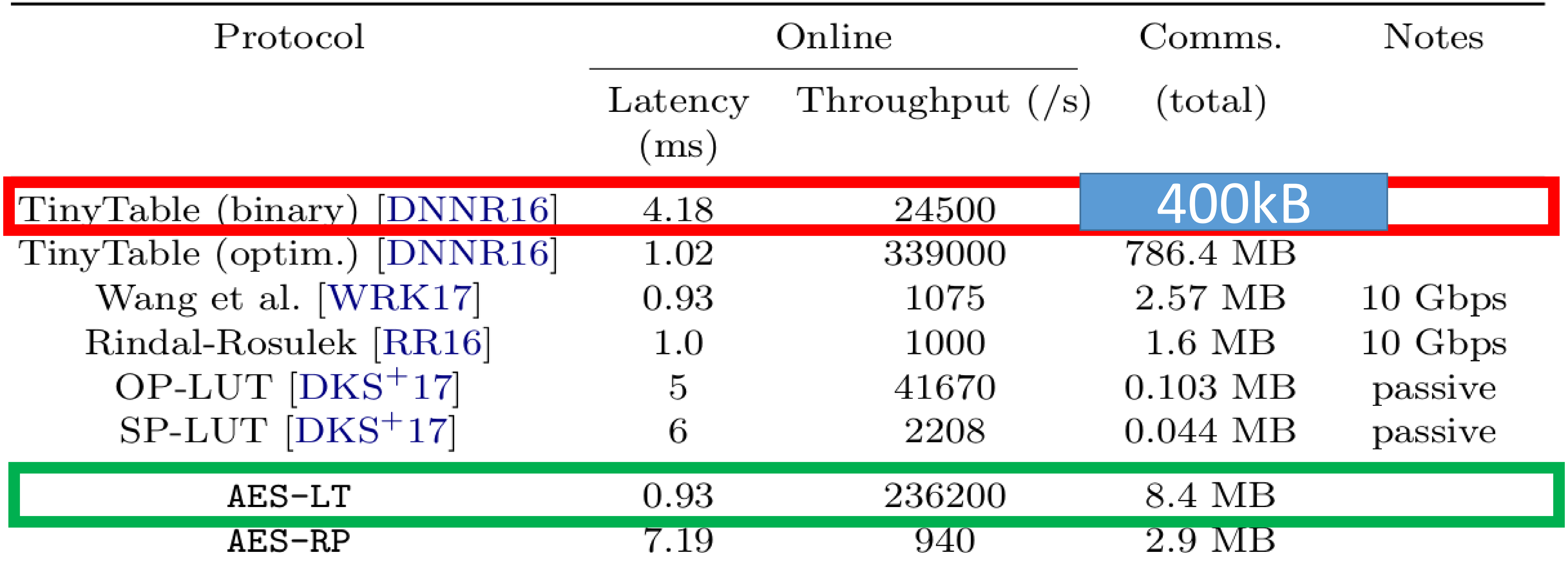
Faster is…faster.



Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	3.07 MB	
TinyTable (optim.) [DNNR16]	1.02	339000	786.4 MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS+17]	5	41670	0.103 MB	passive
SP-LUT [DKS+17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

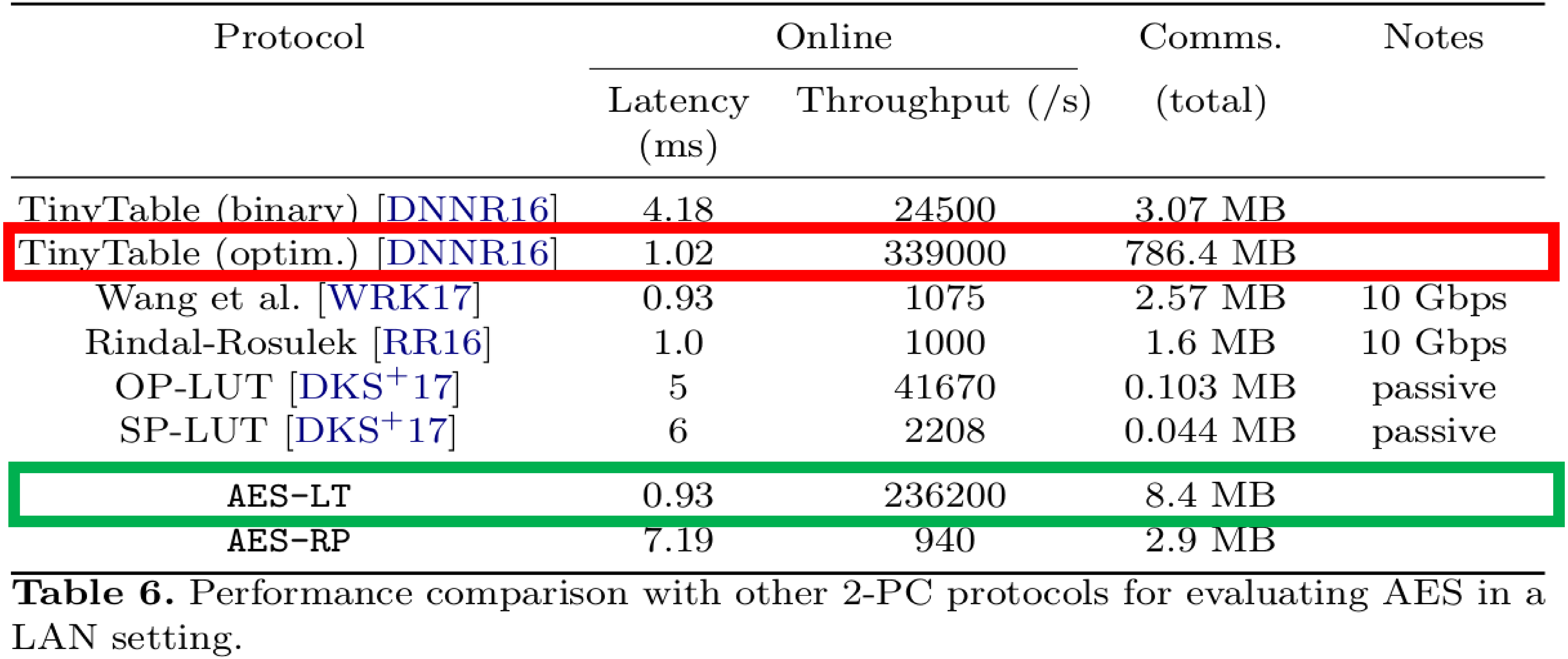
Faster is…faster.



Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	400kB	
TinyTable (optim.) [DNNR16]	1.02	339000	786.4 MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS$^+$17]	5	41670	0.103 MB	passive
SP-LUT [DKS$^+$17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

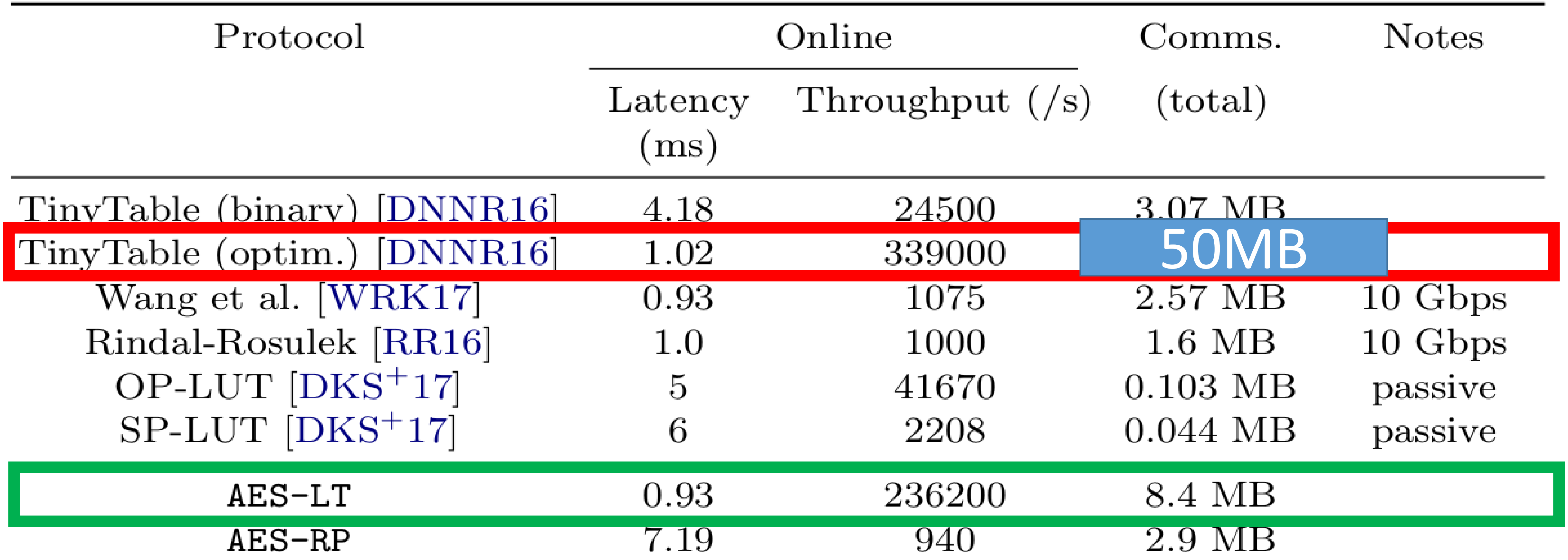
Faster is…faster.



Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	3.07 MB	
TinyTable (optim.) [DNNR16]	1.02	339000	786.4 MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS$^+$17]	5	41670	0.103 MB	passive
SP-LUT [DKS$^+$17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

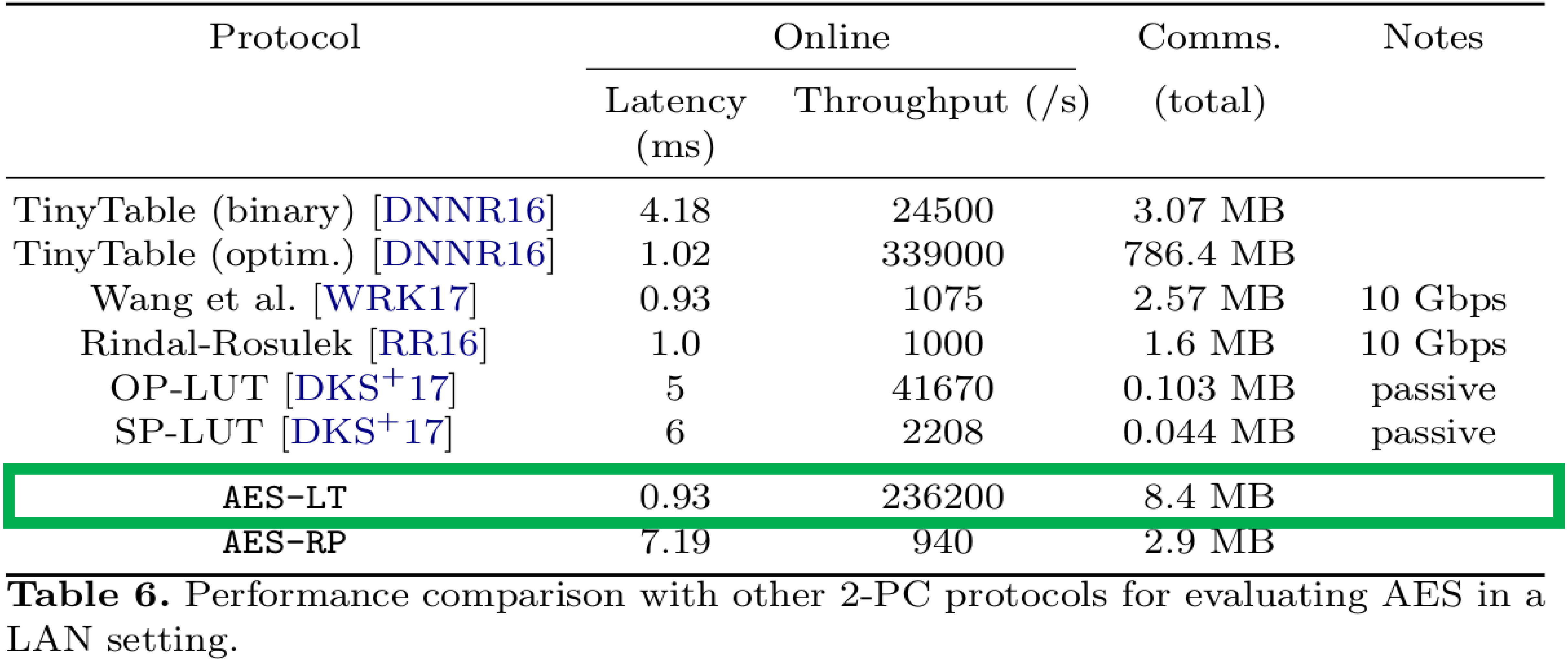
Faster is...faster.



Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	3.07 MB	
TinyTable (optim.) [DNNR16]	1.02	339000	50MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS+17]	5	41670	0.103 MB	passive
SP-LUT [DKS+17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

Faster is…faster.

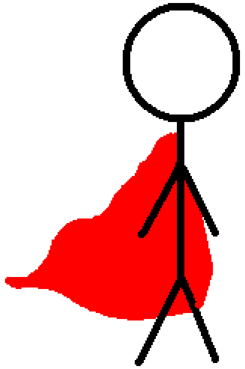


Protocol	Online		Comms.	Notes
	Latency (ms)	Throughput (/s)	(total)	
TinyTable (binary) [DNNR16]	4.18	24500	3.07 MB	
TinyTable (optim.) [DNNR16]	1.02	339000	786.4 MB	
Wang et al. [WRK17]	0.93	1075	2.57 MB	10 Gbps
Rindal-Rosulek [RR16]	1.0	1000	1.6 MB	10 Gbps
OP-LUT [DKS$^+$17]	5	41670	0.103 MB	passive
SP-LUT [DKS$^+$17]	6	2208	0.044 MB	passive
AES-LT	0.93	236200	8.4 MB	
AES-RP	7.19	940	2.9 MB	

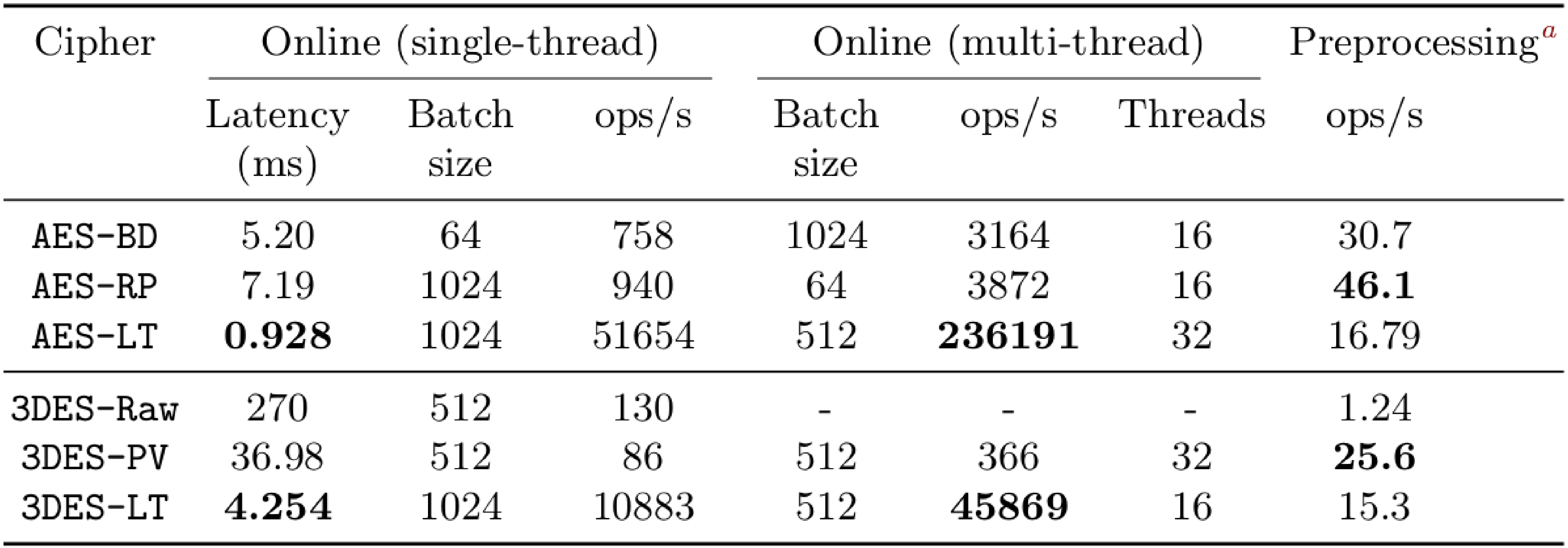
Table 6. Performance comparison with other 2-PC protocols for evaluating AES in a LAN setting.

Thank you! #triples

Thank you! #triples



LAN results.



Cipher	Online (single-thread)			Online (multi-thread)			Preprocessing[a]
	Latency (ms)	Batch size	ops/s	Batch size	ops/s	Threads	ops/s
AES-BD	5.20	64	758	1024	3164	16	30.7
AES-RP	7.19	1024	940	64	3872	16	**46.1**
AES-LT	**0.928**	1024	51654	512	**236191**	32	16.79
3DES-Raw	270	512	130	-	-	-	1.24
3DES-PV	36.98	512	86	512	366	32	**25.6**
3DES-LT	**4.254**	1024	10883	512	**45869**	16	15.3

Table 3. 1 Gbps LAN timings for evaluating AES and 3DES in MPC.

#party #party #party