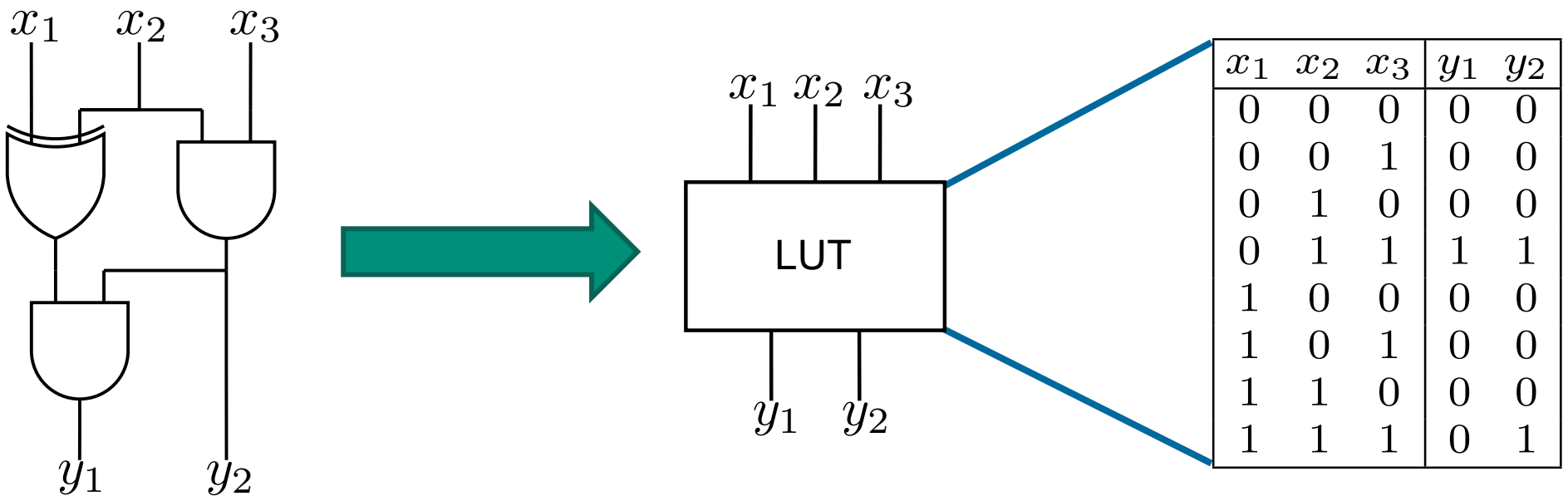
FLUTE: Fast and Secure Lookup Table Evaluations

Andreas Brüggemann, Robin Hundt, Thomas Schneider, Ajith Suresh, and Hossein Yalame

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO CRYPTOGRAPHY AND PRIVACY ENGINEERING



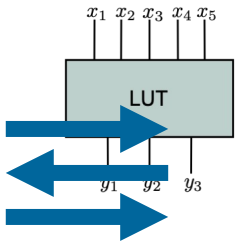
x_1	x_2	x_3	y_1	y_2
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	1	1
1	0	0	0	0
1	0	1	0	0
1	1	0	0	0
1	1	1	0	1

Contact: https://encrypto.de

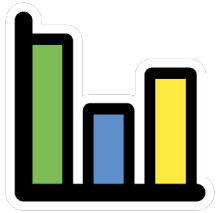
Secure Two-Party Computation

In this work: semi-honest security model, Boolean world

Contributions



Novel method and protocol for lookup table (LUT) evaluation

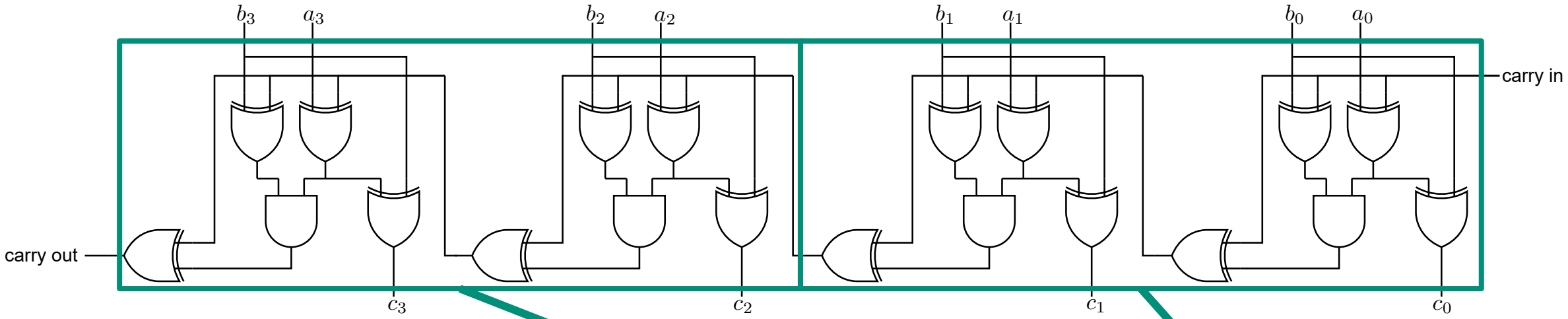


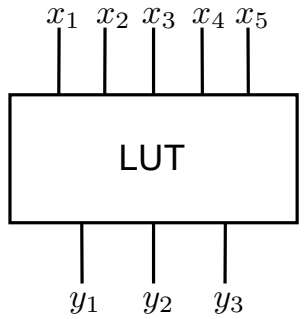
Best of two worlds: fastest LUT online phase, efficient setup phase

</>

Open-source protocol implementation

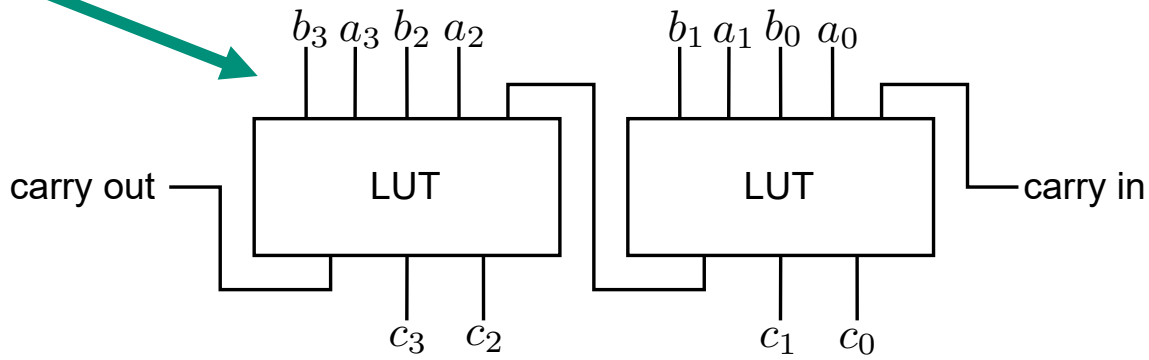
Lookup Tables





x_1	x_2	x_3	x_4	x_5	y_1	y_2	y_3
0	0	0	0	0	0	0	0
0	0	0	0	1	0	1	0
0	0	0	1	0	0	1	0
0	0	0	1	1	0	0	1
0	0	1	0	0	1	0	0
0	0	1	0	1	1	1	0
0	0	1	1	0	1	1	0
0	0	1	1	1	1	0	1
0	1	0	0	0	1	0	0
0	1	0	0	1	1	1	0

.....

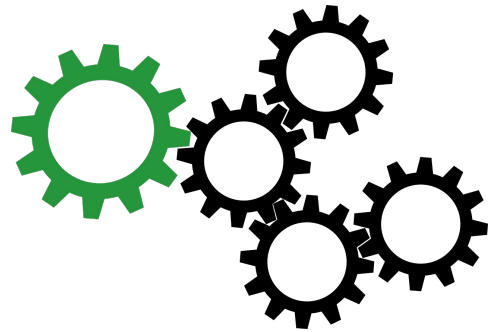


How to Use Lookup Tables

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

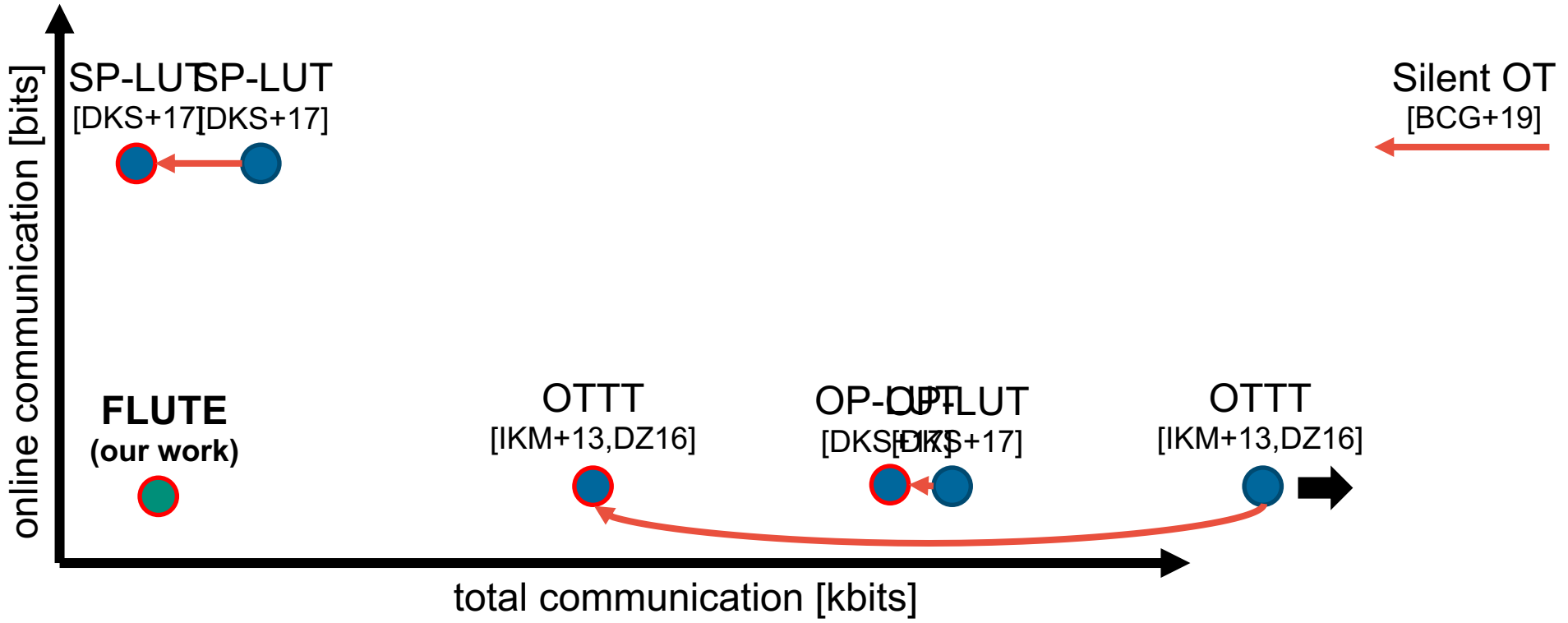
- **Manual** utilization of LUTs during circuit design,
  e.g., SecFloat [RBS+22], SiRnn [RRG+21]

- **Automatic** replacement sub-circuits of existing circuits by LUTs,
  e.g., [DKS+17]



[RBS+22] D. Rathee, A. Bhattacharya, R. Sharma, D. Gupta, N. Chandran, and A. Rastogi, “SecFloat: Accurate Floating-Point meets Secure 2-Party Computation,” in **IEEE S&P**, 2022.
[RRG+21] D. Rathee, M. Rathee, R. K. K. Goli, D. Gupta, R. Sharma, N. Chandran, and A. Rastogi, “SiRnn: A Math Library for Secure RNN Inference,” in **IEEE S&P**, 2021.
[DKS+17] G. Dessouky, F. Koushanfar, A. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, “Pushing the Communication Barrier in Secure Computation using Lookup Tables,” in **NDSS**, 2017.

Landscape of 2PC LUT Protocols



[IKM+13] Y. Ishai, E. Kushilevitz, S. Meldgaard, C. Orlandi, and A. Paskin-Cherniavsky, “On the Power of Correlated Randomness in Secure Computation,” in **TCC**, 2013.

[DZ16] I. Damgård and R. W. Zakarias, “Fast Oblivious AES A Dedicated Application of the MiniMac Protocol,” in **AFRICACRYPT**, 2016.

[DKS+17] G. Dessouky, F. Koushanfar, A. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, “Pushing the Communication Barrier in Secure Computation using Lookup Tables,” in **NDSS**, 2017.

[BCG+19] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl, “Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation,” in **CCS**, 2019.

Our Novel Approach to Evaluating Lookup Tables I

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

1.

x_1	x_2	x_3	y
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

2. disjunctive normal form

$$(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \vee (\overline{x_1} \wedge x_2 \wedge x_3) \vee (x_1 \wedge \overline{x_2} \wedge x_3)$$

3.

$$(\overline{x_1} \wedge \overline{x_2} \wedge \overline{x_3}) \oplus (\overline{x_1} \wedge x_2 \wedge x_3) \oplus (x_1 \wedge \overline{x_2} \wedge x_3)$$

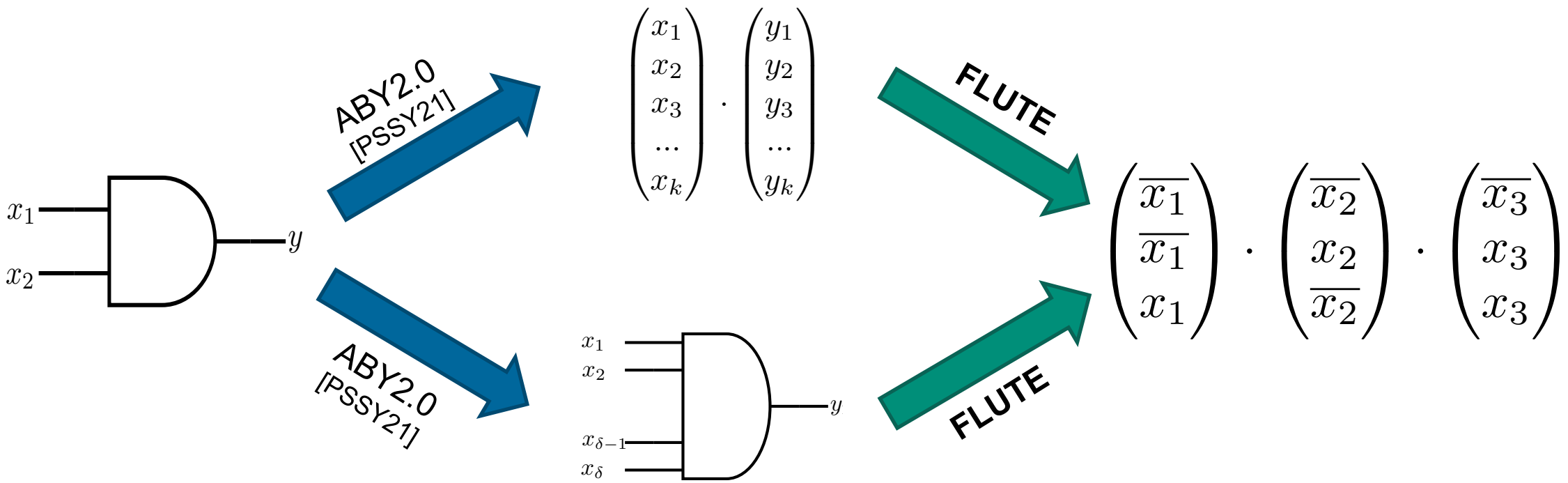
4. in $\mathbb{F}_2$

$$(\overline{x_1} \cdot \overline{x_2} \cdot \overline{x_3}) + (\overline{x_1} \cdot x_2 \cdot x_3) + (x_1 \cdot \overline{x_2} \cdot x_3)$$

5.

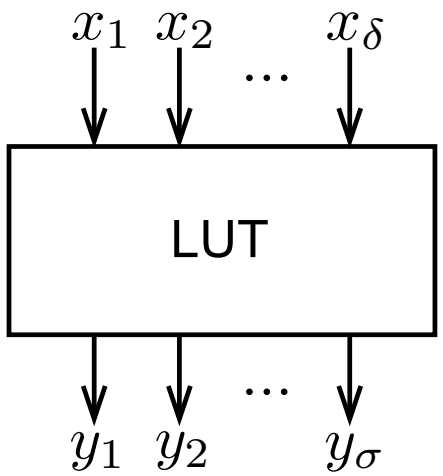
$$\begin{pmatrix} \overline{x_1} \\ \overline{x_1} \\ x_1 \end{pmatrix} \cdot \begin{pmatrix} \overline{x_2} \\ x_2 \\ \overline{x_2} \end{pmatrix} \cdot \begin{pmatrix} \overline{x_3} \\ x_3 \\ x_3 \end{pmatrix}$$

Our Novel Approach to Evaluating Lookup Tables II



[PSSY21] A. Patra, T. Schneider, A. Suresh, and H. Yalame, “ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation,” in **USENIX Security**, 2021.

Communication per LUT with Silent OT



Protocol	Setup [bits]	Online [bits]	Rounds
OTTT [IKM+13,DZ16]	$\lesssim 4.2(\delta-1)2^\delta\sigma$	$\boldsymbol{2\delta}$	1
OP-LUT [DKS+17]	$\approx 0.1\delta + 2^{2\delta}\sigma$	$\boldsymbol{2\delta}$	1
SP-LUT [DKS+17]	$\boldsymbol{\approx 0.1\delta}$	$2^\delta\sigma + \delta$	1*
FLUTE (our work)	$\boldsymbol{\approx 4.2(2^\delta - \delta - 1)}$	$\boldsymbol{2\sigma}$	1

*: amortized

δ \ σ	1	2	3	4	5	6	7	8
2	1.00	1.24	1.39	1.49	1.56	1.62	1.66	1.69
3	0.60	0.92	1.19	1.42	1.61	1.77	1.92	2.04
4	0.42	0.72	1.00	1.25	1.49	1.71	1.92	2.12
5	0.34	0.61	0.87	1.13	1.38	1.62	1.85	2.07
6	0.29	0.55	0.80	1.05	1.30	1.54	1.78	2.01
7	0.27	0.51	0.76	1.01	1.25	1.49	1.73	1.97
8	0.25	0.50	0.74	0.98	1.22	1.46	1.70	1.94

Improvement factor of FLUTE over SP-LUT [DKS+17], total communication

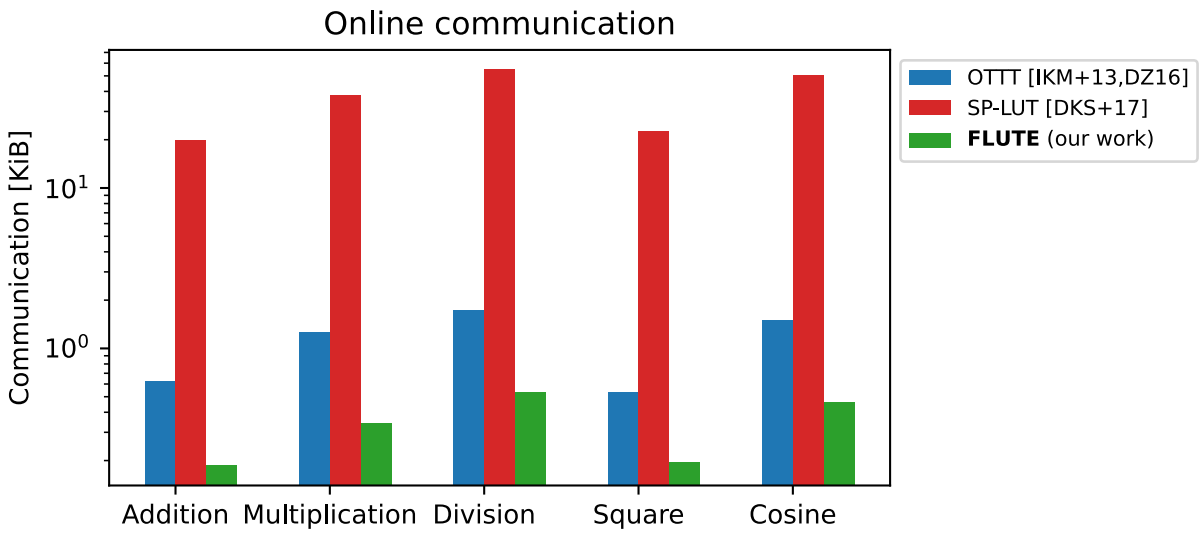
[BCG+19] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl, "Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation," in **CCS**, 2019.

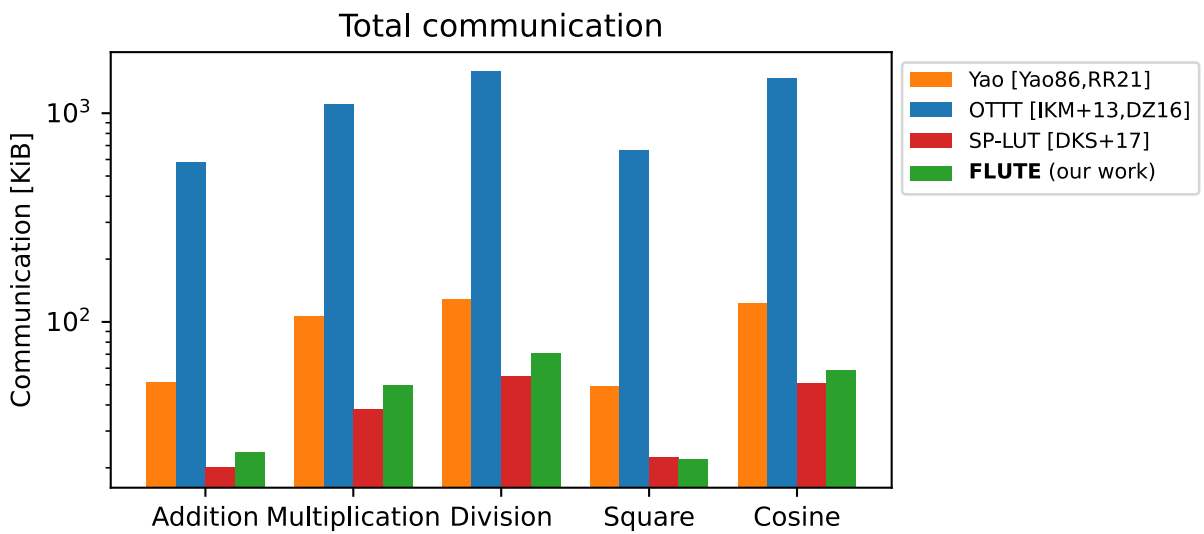
[DKS+17] G. Dessouky, F. Koushanfar, A. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, "Pushing the Communication Barrier in Secure Computation using Lookup Tables," in **NDSS**, 2017.

[DZ16] I. Damgård and R. W. Zakarias, "Fast Oblivious AES A Dedicated Application of the MiniMac Protocol," in **AFRICACRYPT**, 2016.

[IKM+13] Y. Ishai, E. Kushilevitz, S. Meldgaard, C. Orlandi, and A. Paskin Cherniavsky, "On the Power of Correlated Randomness in Secure Computation," in **TCC**, 2013.

Communication for Floating-Point Circuits Using LUTs





[DKS+17] G. Dessouky, F. Koushanfar, A. Sadeghi, T. Schneider, S. Zeitouni, and M. Zohner, “Pushing the Communication Barrier in Secure Computation using Lookup Tables,” in **NDSS**, 2017.

[DZ16] I. Damgård and R. W. Zakarias, “Fast Oblivious AES A Dedicated Application of the MiniMac Protocol,” in **AFRICACRYPT**, 2016.

[IKM+13] Y. Ishai, E. Kushilevitz, S. Meldgaard, C. Orlandi, and A. Paskin Cherniavsky, “On the Power of Correlated Randomness in Secure Computation,” in **TCC**, 2013.

[RR21] M. Rosulek and L. Roy, “Three Halves Make a Whole? Beating the Half-Gates Lower Bound for Garbled Circuits,” in **CRYPTO**, 2021.

[Yao86] A. C.-C. Yao, “How to Generate and Exchange Secrets (Extended Abstract),” in **FOCS**, 1986.

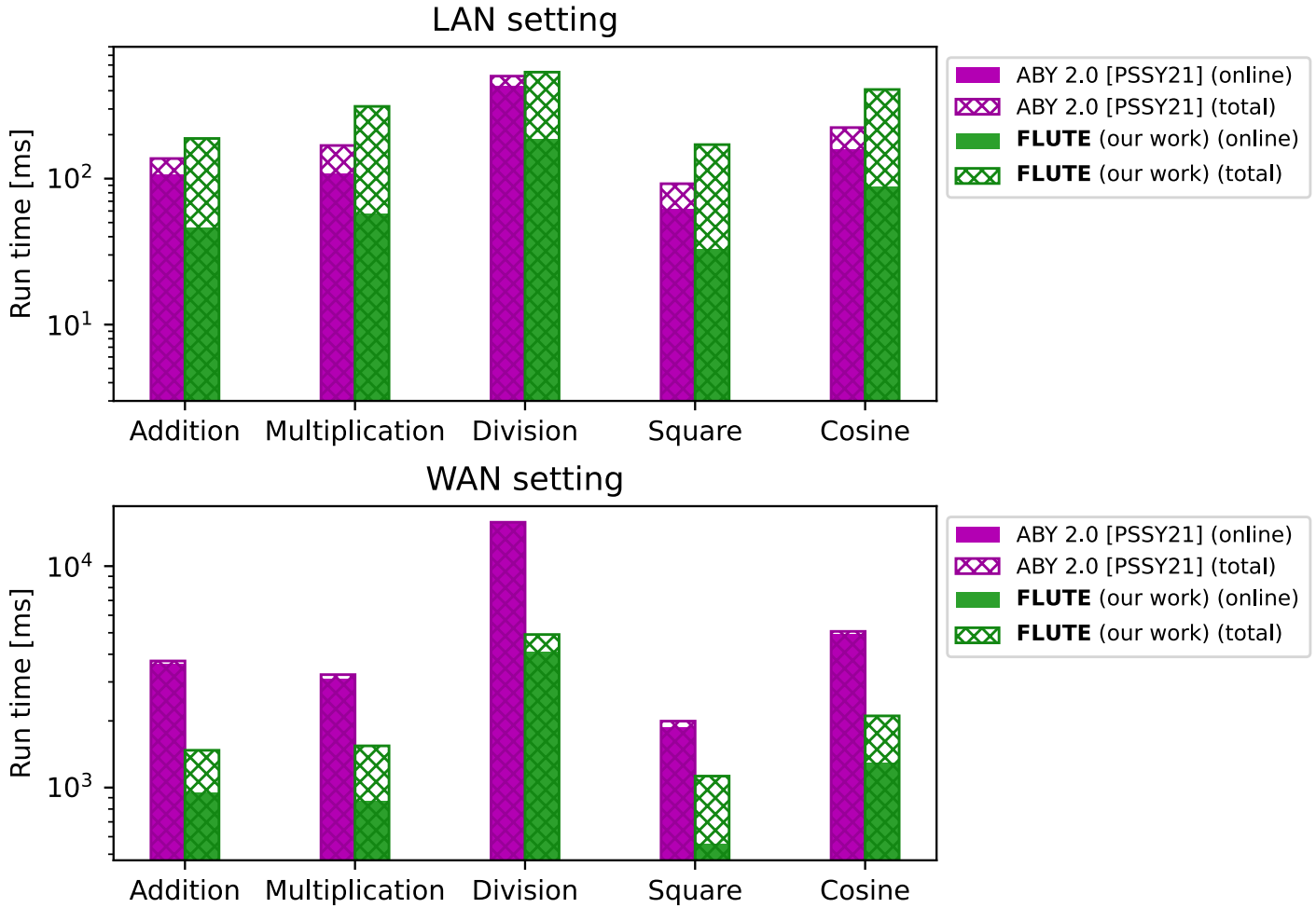
Run Time: LUT Circuits vs Standard Binary Circuits

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

Code available at

https://encrypto.de/code/FLUTE

including FLUTE, ABY2.0 [PSSY21], and SilentOT [BCG+19]!



[BCG+19] E. Boyle, G. Couteau, N. Gilboa, Y. Ishai, L. Kohl, P. Rindal, and P. Scholl, "Efficient Two-Round OT Extension and Silent Non-Interactive Secure Computation," in **CCS**, 2019.

[PSSY21] A. Patra, T. Schneider, A. Suresh, and H. Yalame, "ABY2.0: Improved Mixed-Protocol Secure Two-Party Computation," in **USENIX Security**, 2021.

Thank You!

Questions?

Paper: https://ia.cr/2023/499

Code: https://encrypto.de/code/FLUTE

Website: https://encrypto.de