KU LEUVEN COSIC

Arithmetic Circuit Implementations of S-boxes for SKINNY and PHOTON in MPC

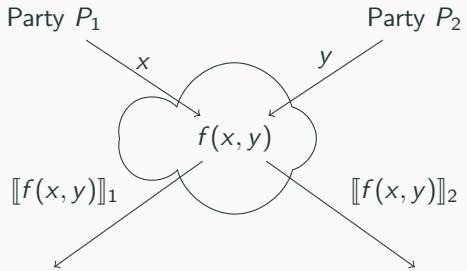
Aysajan Abidin, **Erik Pohle** and Bart Preneel

COSIC, KU Leuven, Belgium

ESORICS 2023

September 25, 2023

Secure Multi-Party Computation (MPC)

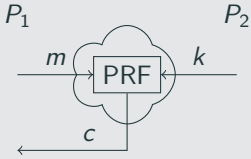


XOR/linear operation: cheap
AND/multiplication: costly

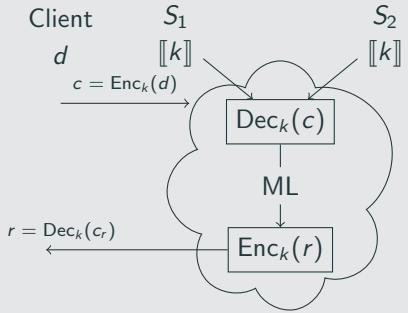
- x,y private inputs of P_1, P_2
- $[\![\cdot]\!]$ secret share

Applications

Oblivious PRFs



Distributed Encryption/Decryption



Signatures via, e.g., MPC-in-the-head

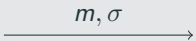
Alice

$\mathsf{sk} = k$

Bob

$\mathsf{pk} = (x, y)$

$\sigma = (\tau_1, \ldots, \tau_3)$

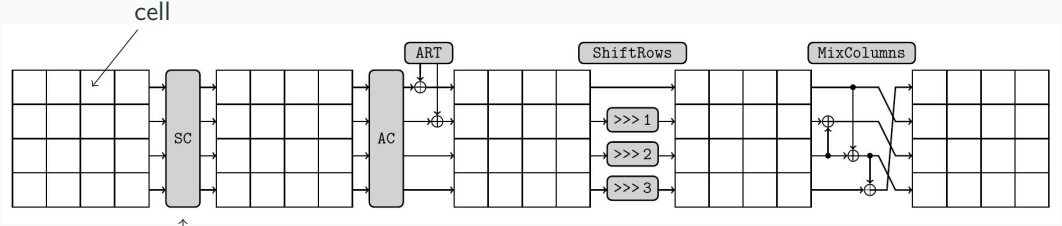


Previous Works

	Primitive	Circuit	MPC protocol
[Mandal and Gong, 2020]	NIST LWC round 2 primitives	Boolean Circuit	HalfGates
[Damgård and Keller, FC'10] [Damgård et al., SCN'12] [Durak and Guajardo, FC'21]	AES	$\mathbb{GF}(2^8)$	SPDZ-style
[Damgård and Zakarias, Africacrypt'16]	AES	$\mathbb{GF}(2^8)^{80}$	dedicated
[**this work**]	SKINNY, PHOTON	$\mathbb{GF}(2^4)$,$\mathbb{GF}(2^8)$	SPDZ-style (MASCOT)

Structure of SPN Primitives

State $\vec{X}$, round key $\vec{RK}$



x	0 1 2 3 4 5 6 7 8 9 a b c d e f
$\mathcal{S}(x)$	c 6 9 0 1 a 2 b 3 8 5 d 4 e 7 f

Image from SKINNY [BJK+16]

Arithmetic Circuits for SKINNY

Baseline: Emulation of Boolean Representation

Cell: $(\llbracket b_0 \rrbracket, \llbracket b_1 \rrbracket, \llbracket b_2 \rrbracket, \llbracket b_3 \rrbracket)$
S-box: 4 AND
ART/MixColumns: linear

Input $(\llbracket b_0 \rrbracket, \llbracket b_1 \rrbracket, \llbracket b_2 \rrbracket, \llbracket b_3 \rrbracket)$:

$$\llbracket b'_2 \rrbracket \leftarrow \llbracket b_3 \rrbracket \oplus (\neg \llbracket b_2 \rrbracket \wedge \neg \llbracket b_1 \rrbracket)$$
$$\llbracket b'_3 \rrbracket \leftarrow \llbracket b_0 \rrbracket \oplus (\neg \llbracket b_3 \rrbracket \wedge \neg \llbracket b_2 \rrbracket)$$
$$\llbracket b'_1 \rrbracket \leftarrow \llbracket b_2 \rrbracket \oplus (\neg \llbracket b_1 \rrbracket \wedge \neg \llbracket b'_3 \rrbracket)$$
$$\llbracket b'_0 \rrbracket \leftarrow \llbracket b_1 \rrbracket \oplus (\neg \llbracket b'_3 \rrbracket \wedge \neg \llbracket b'_2 \rrbracket)$$

Output $(\llbracket b'_0 \rrbracket, \llbracket b'_1 \rrbracket, \llbracket b'_2 \rrbracket, \llbracket b'_3 \rrbracket)$

Cost

SKINNY-64-128: 2304 multiplications in 72 rounds

Arithmetic Circuits [this work]

- Group bits of each cell into an element in $\mathbb{GF}(2^k)$
- All operations except S-box are linear

Cell: $[\![b_0 + b_1 X + b_2 X^2 + b_3 X^3]\!]$ in $\mathbb{GF}(2^4)$
S-box: 2 multiplications, 8 random bits
ART/MixColumns: linear

Input $[\![z]\!]$:

$$[\![\mathcal{S}(z)]\!] \leftarrow p_0([\![z]\!]) \cdot q_0([\![z]\!]) + p_1([\![z]\!])$$

Output $[\![\mathcal{S}(z)]\!]$

Cost

SKINNY-64-128: 1152 multiplications, 4608 random bits in 144 rounds

S-box via Decomposition

Polynomial decomposition from [Coron,Roy and Vivek, CHES'14]

- Interpolating polynomial

$$P(z) = \text{0xc} + \text{0x8}\ z + \text{0x3}\ z^2 + \text{0xd}\ z^3 + \text{0xf}\ z^4 + \text{0x4}\ z^5 + \text{0x8}\ z^6 + \text{0x6}\ z^7 + \text{0x1}\ z^8 + \text{0x9}\ z^9 + \text{0x8}\ z^{10} + \text{0xe}\ z^{12} + \text{0xc}\ z^{13} + \text{0xb}\ z^{14}$$

- Decompose into $P(z) = p_0(z)q_0(z) + p_1(z)$ where p/q only contain certain monomials

random coefficients

solve for P

~~$\{z, z^2, z^4, z^8\}$ (powers of form $z^{2\cdot 2^i}$)~~ not possible

$\{z, z^2, z^3, z^4, z^6, z^8, z^9, z^{12}\}$ (powers of form $z^{2\cdot 2^i}$, $z^{3\cdot 2^i}$)

S-box via Decomposition (cont.)

Compute monomial powers using free squaring

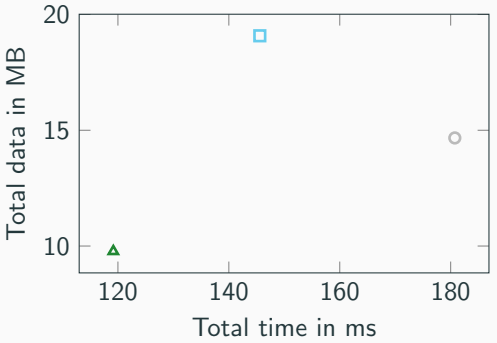
- Bit-decomposition $[\![z]\!] = [\![b_0 + b_1 X + b_2 X^2 + b_3 X^3]\!] \to ([\![b_0]\!], [\![b_1]\!], [\![b_2]\!], [\![b_3]\!])$
- Free squaring

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} [\![b_0]\!] \\ [\![b_1]\!] \\ [\![b_2]\!] \\ [\![b_3]\!] \end{pmatrix} = \begin{pmatrix} [\![b'_0]\!] \\ [\![b'_1]\!] \\ [\![b'_2]\!] \\ [\![b'_3]\!] \end{pmatrix} = [\![z^2]\!] \qquad \text{(repeat for } z^4, z^8\text{)}$$

- Compute $[\![z^3]\!] \leftarrow [\![z]\!] \cdot [\![z^2]\!]$ and repeat free squaring for z^6, z^{12}, z^9

Results

Three-party MPC evaluation of SKINNY-64-128 using MASCOT in LAN setting.



$\approx$ 49% less data

$\approx$ 18% faster

Conclusion

- Polynomial decomposition improves 4-bit S-box evaluation in MPC
- No improvement for 8-bit S-boxes
- Implementation of
  - SKINNY-64-128 $\approx$ 49% less data, $\approx$ 18% faster
  - SKINNY-128-256 no improvement
  - PHOTON P_{100} $\approx$ 49% less data, $\approx$ 27% faster
  - PHOTON P_{256} $\approx$ 81% less data, $\approx$ 74% faster
- Results apply to Midori, TWINE, LED, KLEIN, QAMRA, KNOT, ...

Full version: ia.cr/2023/1426

Code & Data
github.com/ErikP0/arithmetic-circuits-for-spn-primitives

References i

Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim, *The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS*, Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Proceedings, Part II (Matthew Robshaw and Jonathan Katz, eds.), Lecture Notes in Computer Science, vol. 9815, Springer, 2016, pp. 123–153.

Jean-Sébastien Coron, Arnab Roy, and Srinivas Vivek, *Fast Evaluation of Polynomials over Binary Finite Fields and Application to Side-channel Countermeasures*, International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2014, pp. 170–187.

References ii

- F. Betül Durak and Jorge Guajardo, *Improving the Efficiency of AES Protocols in Multi-Party Computation*, Financial Cryptography and Data Security (Berlin, Heidelberg) (Nikita Borisov and Claudia Diaz, eds.), Springer Berlin Heidelberg, 2021, pp. 229–248.
- Ivan Damgård and Marcel Keller, *Secure Multiparty AES*, Financial Cryptography and Data Security (Berlin, Heidelberg) (Radu Sion, ed.), Springer Berlin Heidelberg, 2010, pp. 367–374.
- Ivan Damgård, Marcel Keller, Enrique Larraia, Christian Miles, and Nigel Smart, *Implementing AES via an Actively/Covertly Secure Dishonest-Majority MPC Protocol*, International Conference on Security and Cryptography for Networks, Springer, 2012, pp. 241–263.

References iii


Ivan Damgård and Rasmus Zakarias, *Fast Oblivious AES A Dedicated Application of the MiniMac Protocol*, Progress in Cryptology – AFRICACRYPT 2016 (Cham) (David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, eds.), Springer International Publishing, 2016, pp. 245–264.


Kalikinkar Mandal and Guang Gong, *Can LWC and PEC be Friends?: Evaluating Lightweight Ciphers in Privacy-enhancing Cryptography*, Fourth Lightweight Cryptography Workshop, NIST, 2020.