AES in MPC on FHE is 10^5 faster than AES in FHE

Ivan Damgård
Marcel Keller
Enrique Larraia
Christian Miles
Valerio Pastro
Nigel Smart
Sarah Zakarias

Aarhus University / *University of Bristol*

6/6/12

SPDZ = Smart, Pastro, Damgård, Zakarias

- Active security
- Self-trust
- Offline phase
  Somewhat homomorphic encryption for triples and MACs
- Online phase
  Information-theoretic MACs
- Arithmetic circuit, not constant round

SPDZ = Smart, Pastro, Damgård, Zakarias

- Active security
- Self-trust
- Offline phase
  Somewhat homomorphic encryption for triples and MACs
- Online phase
  Information-theoretic MACs
- Arithmetic circuit, not constant round
- Computational security
- Static adversary
- Assuming commitments, coin-flipping, distributed SHE key
- Synchronous
- Universally composable

SPDZ = Smart, Pastro, Damgård, Zakarias

- Active security
- Self-trust
- Offline phase
  Somewhat homomorphic encryption for triples and MACs
- Online phase
  Information-theoretic MACs
- Arithmetic circuit, not constant round
- Computational security
- Static adversary
- Assuming commitments, coin-flipping, distributed SHE key
- Synchronous
- Universally composable
- Implementation: random oracle model, active or covert

Additive Secret Sharing with MAC

	$a =$		
	a_1	$\gamma(a)_1$	α_1
	a_2	$\gamma(a)_2$	α_2
	a_3	$\gamma(a)_3$	α_3
	a_4	$\gamma(a)_4$	α_4
Sum	$a = \sum_i a$	$\gamma(a) = \alpha \cdot a$	$\alpha = \sum_i \alpha_i$

Operations

Multiplication

$$
\begin{aligned}
x \cdot y &= (x + a - a) \cdot (y + b - b) \\
&= (x + a) \cdot (y + b) - (y + b) \cdot a - (x + a) \cdot b + a \cdot b
\end{aligned}
$$

Operations

Multiplication

$$\begin{aligned} x \cdot y &= (x + a - a) \cdot (y + b - b) \\ &= (x + a) \cdot (y + b) - (y + b) \cdot a - (x + a) \cdot b + a \cdot b \end{aligned}$$

Operations

Multiplication

$$\boxed{x \cdot y} = (x + a - a) \cdot (y + b - b)$$
$$= (x + a) \cdot (y + b) - (y + b) \cdot a - (x + a) \cdot b + a \cdot b$$

Bit decomposition in $GF(2^n) \cong GF(2)[X]/(p)$:

$$f(\sum_{i=0}^{n-1} z_i \cdot X^i) := (z_0, \ldots, z_{n-1}) \in GF(2)^n$$

$$f(z) = f(z + a - a)$$
$$= f(z + a) - f(a)$$

Offline Phase of SPDZ

- Choose α_i
- Broadcast $E(\alpha_i)$, zero-knowledge proof of knowledge (ZKPoK)
- Compute $E(\alpha) = \sum_i E(\alpha_i)$

- Choose a_i, b_i, r_i
- Broadcast $E(a_i), E(b_i), E(r_i)$, 3 ZKPoKs
- Compute $E(a)$, $E(b)$, $E'(c + r) = E(a) \times E(b) + E(r)$
- $E(c)$ and c_i such that $\sum_i c_i = c$ by threshold decryption of $E(c + r)$
- $\gamma(a)_i, \gamma(b)_i, \gamma(c)_i$ by threshold decryption of $E(a) \times E(\alpha)$, $E(b) \times E(\alpha)$, $E(c) \times E(\alpha)$, 3 ZKPoKs

Online or offline: test triple by sacrificing some more

Advanced Encryption Standard / Rijndael

- Symmetric block cipher
- Selected in a competition by NIST
- Block size 128 bits
- Key size 128, 192, or 256 bits
- Operates on bytes as elements of $GF(256)$ or $GF(2)^8$
- Representation: $z_0, \ldots, z_7 \mapsto \sum_i z_i \cdot X^i \in GF(2)[X]/(p)$
  $p := X^8 + X^4 + X^3 + X + 1$ irreducible polynomial

Structure of AES

byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte

SubBytes	S-box operating on bytes
ShiftRows	Permutation of bytes
MixColumns	Linear transformation on columns (as elements of $GF(256)$)
AddRoundKey	XOR a round key to the state

Structure of AES

byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte
byte	byte	byte	byte

SubBytes S-box operating on bytes

ShiftRows Permutation of bytes

MixColumns Linear transformation on columns (as elements of $GF(256)$)

AddRoundKey XOR a round key to the state

Additional secret sharing and linear MAC

$\Rightarrow$ Compute linear operations locally

$\Rightarrow$ All except S-box

SubBytes / S-Box

1. Inversion on $GF(256)$, 0 mapped to 0.
   - $z^{254} \in GF(256)$
2. Linear transformation on bits
   - $(A \cdot \vec{z} + \vec{b}) \in GF(2)^8$

S-Box as Polynomial

$$
\begin{aligned}
&\texttt{0x63} + \texttt{0x8F} \cdot z^{127} + \texttt{0xB5} \cdot z^{191} + \texttt{0x01} \cdot z^{223} + \texttt{0xF4} \cdot z^{239} \\
&+ \texttt{0x25} \cdot z^{247} + \texttt{0xF9} \cdot z^{251} + \texttt{0x09} \cdot z^{253} + \texttt{0x05} \cdot z^{254}
\end{aligned}
$$

S-Box as Polynomial

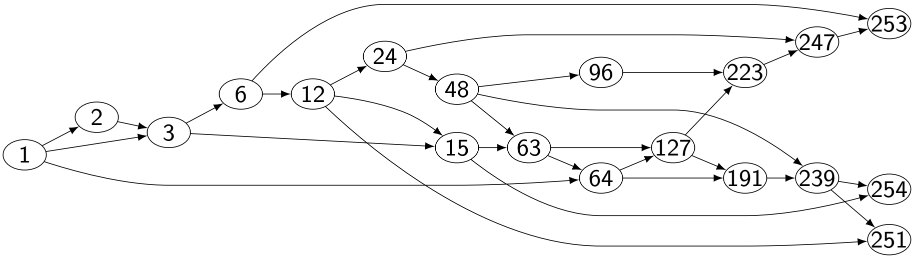
$$
\begin{aligned}
&\mathtt{0x63} + \mathtt{0x8F} \cdot z^{127} + \mathtt{0xB5} \cdot z^{191} + \mathtt{0x01} \cdot z^{223} + \mathtt{0xF4} \cdot z^{239} \\
&+ \mathtt{0x25} \cdot z^{247} + \mathtt{0xF9} \cdot z^{251} + \mathtt{0x09} \cdot z^{253} + \mathtt{0x05} \cdot z^{254}
\end{aligned}
$$

(Lagrange interpolation on complete finite field)

S-Box as Polynomial

$$0x63 + 0x8F \cdot z^{127} + 0xB5 \cdot z^{191} + 0x01 \cdot z^{223} + 0xF4 \cdot z^{239}$$
$$+ 0x25 \cdot z^{247} + 0xF9 \cdot z^{251} + 0x09 \cdot z^{253} + 0x05 \cdot z^{254}$$

(Lagrange interpolation on complete finite field)



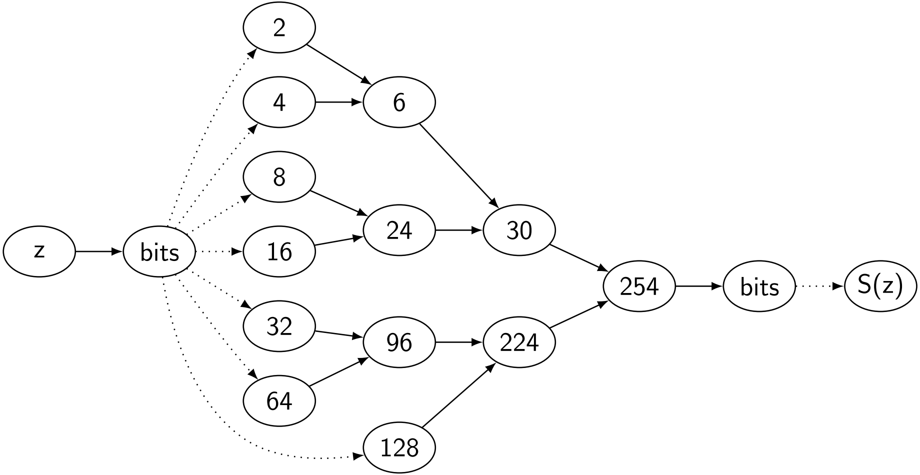
S-Box with Bit Decomposition

$GF(256)$ has character 2

$$\Rightarrow (a+b)^{2^j} = a^{2^j} + b^{2^j}$$
$$\Rightarrow \Big(\sum_i z_i \cdot X^i\Big)^{2^j} = \sum_{i,j} z_i \cdot X^{i \cdot 2^j}$$

Equivalent: Squaring over $GF(256)$ is linear over $GF(2)^8$

S-Box with Bit Decomposition



More Operations

Multiplication

$$x \cdot y = (x + a - a) \cdot (y + b - b)$$
$$= (x + a) \cdot (y + b) - (y + b) \cdot a - (x + a) \cdot b + a \cdot b$$

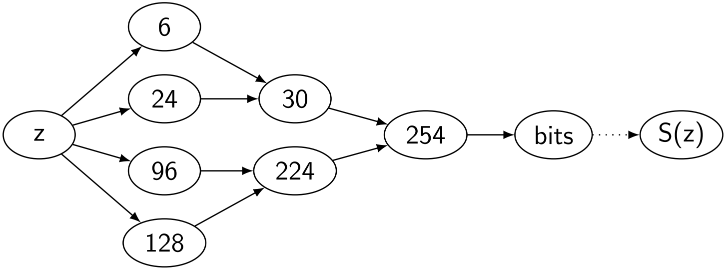
Computation of $x^{3 \cdot 2^i}$

$$x^{3 \cdot 2^i} = (x + a - a)^{3 \cdot 2^i} = (x + a - a)^{2 \cdot 2^i} \cdot (x + a - a)^{2^i}$$
$$= ((x + a)^{2^{i+1}} - a^{2^{i+1}}) \cdot ((x + a)^{2^i} - a^{2^i})$$
$$= (x + a)^{3 \cdot 2^i} - (x + a)^{2^{i+1}} \cdot a^{2^i} - (x + a)^{2^i} \cdot a^{2^{i+1}} + a^{3 \cdot 2^i}$$

More Operations

Computation of $x^{3\cdot 2^i}$

$$
\begin{aligned}
x^{3\cdot 2^i} &= (x+a-a)^{3\cdot 2^i} = (x+a-a)^{2\cdot 2^i}\cdot(x+a-a)^{2^i}\\
&= ((x+a)^{2^{i+1}} - a^{2^{i+1}})\cdot((x+a)^{2^i} - a^{2^i})\\
&= (x+a)^{3\cdot 2^i} - (x+a)^{2^{i+1}}\cdot a^{2^i} - (x+a)^{2^i}\cdot a^{2^{i+1}} + a^{3\cdot 2^i}
\end{aligned}
$$



More Operations

Computation of $x^{3\cdot 2^i}$

$$\boxed{x^{3\cdot 2^i}} = (x+a-a)^{3\cdot 2^i} = (x+a-a)^{2\cdot 2^i} \cdot (x+a-a)^{2^i}$$
$$= ((x+a)^{2^{i+1}} - a^{2^{i+1}}) \cdot ((x+a)^{2^i} - a^{2^i})$$
$$= (x+a)^{3\cdot 2^i} - (x+a)^{2^{i+1}} \cdot a^{2^i} - (x+a)^{2^i} \cdot a^{2^{i+1}} + a^{3\cdot 2^i}$$

Computation of x^{254}

$$x^{254} = \sum_{i=0}^{127} (x+a)^{2(127-i)} \cdot a^{2i}$$

Cost

Per S-box	Triples	Bits	Other	Rounds	Implemented
Polynomial	18	0	0	12	Yes
Bit decomposition	6	2×8	0	5	Yes
$x^{3 \cdot 2^i}$	3	1×8	1×11	4	Online phase
x^{254}	0	1×8	1×128	2	No
"All in"	0	0	1×256	1	No

- 16 S-boxes in parallel per round
- 10, 12, or 14 rounds

Field Embedding Trick

- 1 MAC in $GF(2^8)$: 8 bits security
  $\Rightarrow$ 5 MACs for 40 bits security
- 1 MAC in $GF(2^{40})$: 40 bits security

Field Embedding Trick

- 1 MAC in $GF(2^8)$: 8 bits security
  $\Rightarrow$ 5 MACs for 40 bits security
- 1 MAC in $GF(2^{40})$: 40 bits security

Embed

$$GF(2^8) \cong GF(2)[Y]/(Y^8 + Y^4 + Y^3 + Y + 1)$$

in

$$GF(2^{40}) \cong GF(2)[X]/(X^{40} + X^{20} + X^{15} + X^5 + 1)$$

with

$$Y = X^5 + 1$$

Implementation Variants

MACs / Sacrifices	$GF(2^8)$	$GF(2^{40})$
Covert security	1	1
Active security	5	1

Offline Phase

h:m:s per block		Covert		Active	
Field	Players	Poly	Bits	Poly	Bits
$GF(2^8)$	2	0:01:42	0:00:47	1:56:02	0:51:36
	10	0:02:01	0:00:58	6:18:20	2:44:51
$GF(2^{40})$	2	0:05:52	0:02:43	0:13:18	0:05:26
	10	0:06:53	0:03:15	0:44:39	0:19:32

Up to $\sim 3'000'000$ zero-knowledge proofs

Online Phase

Seconds per block		Covert			Active		
Field	Players	Poly	Bits	$3 \cdot 2^i$	Poly	Bits	$3 \cdot 2^i$
$GF(2^8)$	2	0.20	0.11	0.07	1.23	0.53	0.30
	10	0.33	0.19	0.14	1.92	0.78	0.45
$GF(2^{40})$	2	0.37	0.25	0.14	0.37	0.22	0.14
	10	0.58	0.32	0.22	0.50	0.35	0.24

Comparison of AES in MPC (Online Phase)

Method	Parties	Corrupt	Time (s)	Security	Authors
Yao	2	1	0.2	passive	Huang et al.
Yao	2	1	1.0	active	Kreuter et al.
OT	2	1	0.3	active	Nielsen et al.
Replication	3	1	0.001	passive	Laur et al.
Shamir	3	1	0.4	passive	Damgård & K
Shamir	4	1	1.0	active	Damgård & K
Offline FHE	2	1	0.07	covert	This work
Offline FHE	10	9	0.2	active	This work

Amortized

Comparison of AES in MPC (Online Phase)

Method	Parties	Corrupt	Time (s)	Security	Authors
Yao	2	1	0.2	passive	Huang et al.
Yao	2	1	1.0	active	Kreuter et al.
OT	2	1	0.3	active	Nielsen et al.
Replication	3	1	0.001	passive	Laur et al.
Shamir	3	1	0.4	passive	Damgård & K
Shamir	4	1	1.0	active	Damgård & K
Offline FHE	2	1	0.07	covert	This work
Offline FHE	10	9	0.2	active	This work
Pure FHE	1		600.0		Gentry et al.

Amortized

Comparison of AES in MPC (Online Phase)

Method	Parties	Corrupt	Time (s)	Security	Authors
Yao	2	1	0.2	passive	Huang et al.
Yao	2	1	1.0	active	Kreuter et al.
OT	2	1	4.0	active	Nielsen et al.
Replication	3	1	1.0	passive	Laur et al.
Shamir	3	1	0.6	passive	Damgård & K
Shamir	4	1	1.0	active	Damgård & K
Offline FHE	2	1	0.3	covert	This work
Offline FHE	10	9	1.2	active	This work
Pure FHE	1		17000.0		Gentry et al.

Not amortized