RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

#RSAC

SESSION ID: CRYP-W02

COMPUTING ON ENCRYPTED DATA: HIGH-PRECISION ARITHMETIC IN HOMOMORPHIC ENCRYPTION

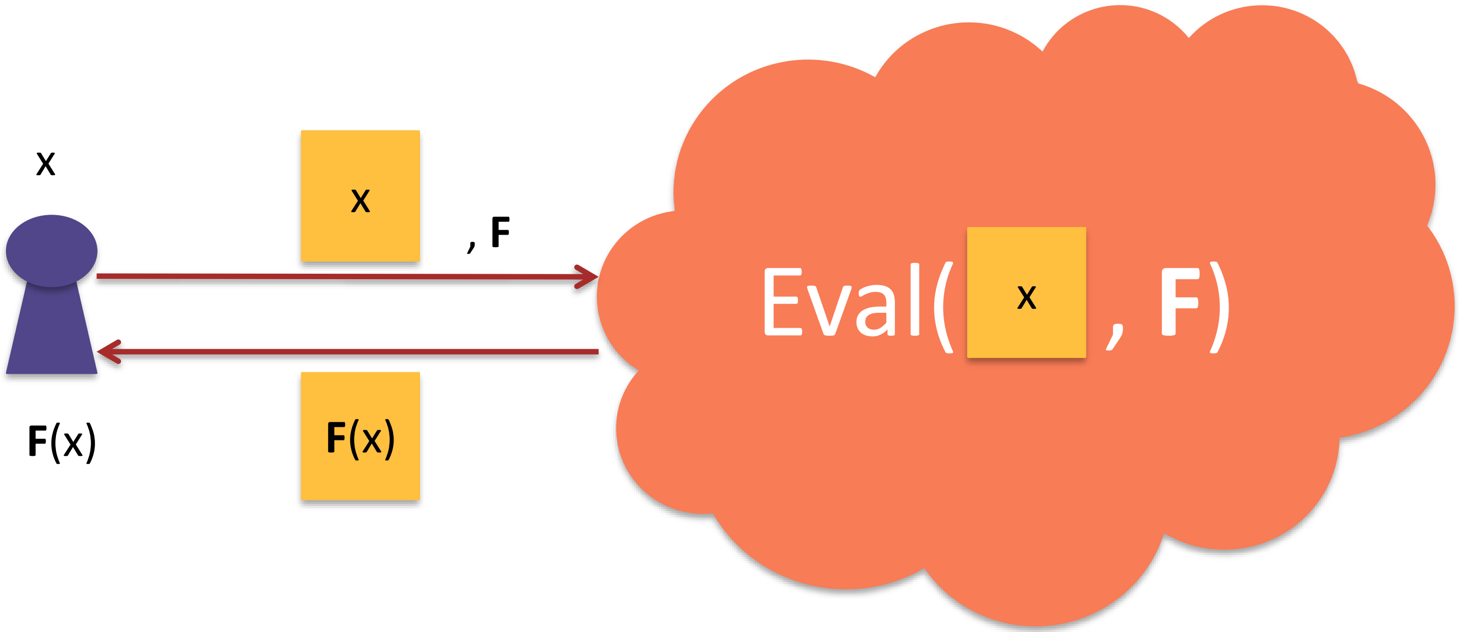
Rachel Player

PhD Student // Postdoc
Royal Holloway, University of London, UK // LIP6, Sorbonne Université, France
@yayworthy

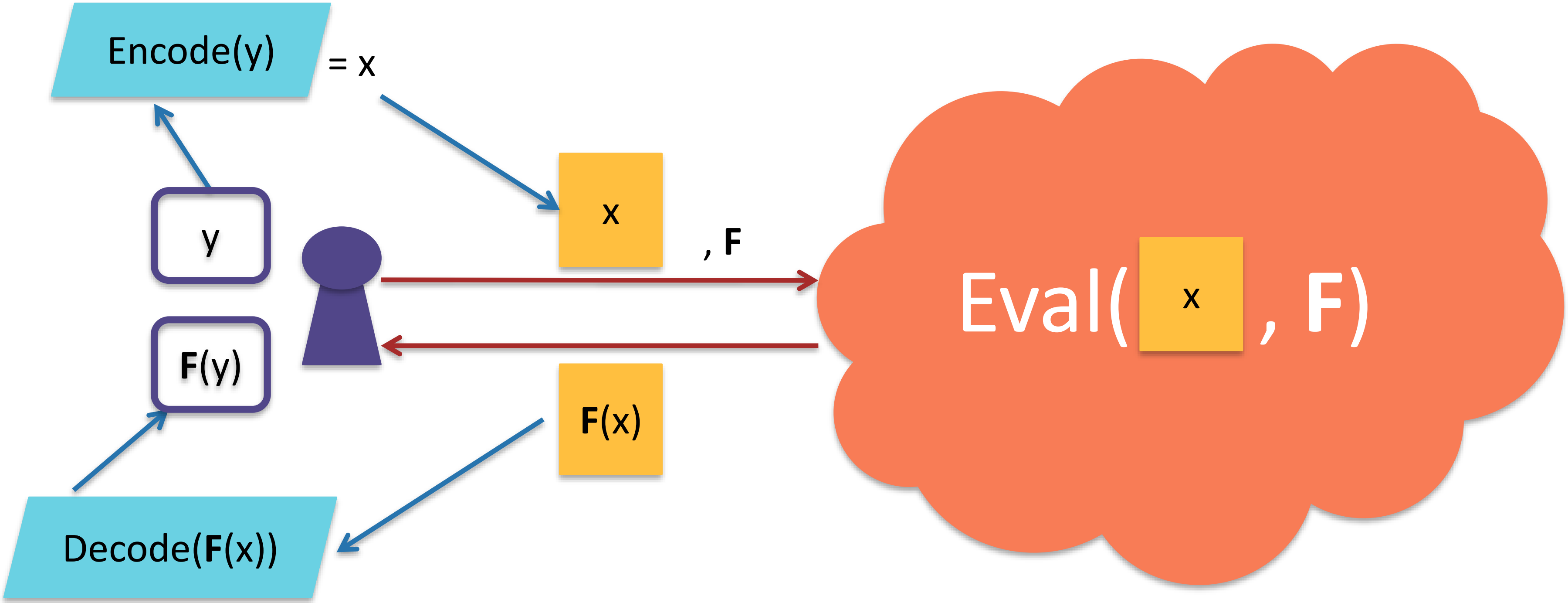
Joint work with: Hao Chen, Kim Laine, and Yuhou Xia

MOTIVATION

Homomorphic encryption



Raw data must be encoded into plaintexts



Need to ensure correctness of decoding

$$\mathbb{Z}_t[x]/(x^n+1)$$

TYPICAL PLAINTEXT SPACE

- Underlying plaintext coefficients grow during evaluation
- If plaintext wraps modulo t in any coefficient, decoding will fail
- Typically have to choose large t to avoid this

Example: binary encoding

- To encode an integer:
  - Express in binary
  - Each bit is coefficient of the corresponding polynomial
- To decode:
  - Evaluate polynomial at $x=2$

$$5 \longrightarrow 101 \longrightarrow x^2 + 1$$

Challenges with traditional approach

- Various encoders to choose from
- Choosing large t means more noise growth
- Batching is supported

Hoffstein-Silverman: a different approach

- Replace *t* by a small polynomial *x-b* for *b* a positive integer e.g. *b = 2*

$$\mathbb{Z}/(b^n + 1)\mathbb{Z}$$

- Easy to encode integers
- Huge amount of room for computation

J. Hoffstein and J. Silverman. Optimizations for NTRU. In Public Key Cryptography and Computational Number Theory, 2001

Related work

- Geihs and Cabarcas applied in context of BV scheme
- Lauter *et al.* apply the idea to YASHE scheme
  - No performance analysis presented
  - Unpublished work of Lopez-Alt and Naehrig is cited for details

M. Geihs and D. Cabarcas. Efficient integer encoding for homomorphic encryption via ring isomorphisms. In LATINCRYPT, 2014.

K. E. Lauter, A. Lopez-Alt, and M. Naehrig. Private computation on encrypted genomic data. In LATINCRYPT, 2014.

A. Lopez-Alt and M. Naehrig. Large integer plaintexts in ring-based fully homomorphic encryption, 2014. Unpublished.

OUR CONTRIBUTION

Adapting the work of Lopez-Alt and Naehrig, we:

- Apply the Hoffstein-Silverman trick on the FV scheme
- Analyze its noise growth using new definition of noise
- Extend rational number encoders to work with the trick
- Present a detailed performance comparison to FV scheme
- Analyze impact on practical use-cases

A. Lopez-Alt and M. Naehrig. Large integer plaintexts in ring-based fully homomorphic encryption, 2014. Unpublished.

J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. Eprint 2012/144.

Adapting the work of Lopez-Alt and Naehrig, we:

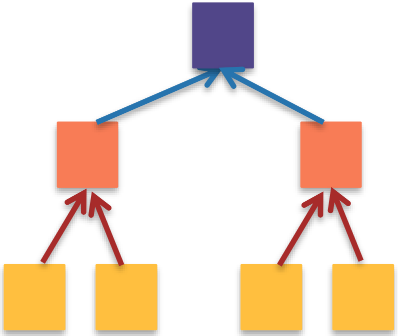
- Apply the Hoffstein-Silverman trick on the FV scheme
- Analyze its noise growth using new definition of noise
- Extend rational number encoders to work with the trick
- **Present a detailed performance comparison to FV scheme**
- Analyze impact on practical use-cases

A. Lopez-Alt and M. Naehrig. Large integer plaintexts in ring-based fully homomorphic encryption, 2014. Unpublished.

J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. Eprint 2012/144.

Regular circuits

- Security is the same so we can fix (n, q, σ)
- Compare evaluation of regular circuit as in Costache *et al.*
  - Do A additions and one multiplication, iterated D times
  - Inputs are integers of norm at most L



A Costache, N. P. Smart, S. Vivek and A. Waller. Fixed point arithmetic in SHE scheme. In SAC, 2016.

Choosing an encoder for FV

- Well-known encoders are NAF or balanced base-B
  - Short B enables smaller t
  - Large B enables shorter encodings
- Cheon *et al.* show NAF encoding outperforms balanced base-B encoding for $B = 2$ and $B = 3$

J. H. Cheon, J. Jeong, J. Lee and K. Lee. Privacy-preserving computations of predictive medical models with minimax approximation and Non-Adjacent Form. In WAHC, 2017.

Noise and plaintext growth constraints

$$D \lesssim \left\lfloor \frac{\log q - \log(84\sigma t n)}{\log(14tn) + A} \right\rfloor .$$

$$\sqrt{\frac{6}{\pi 2^D d(d+2)}}\,(d+1)^{2^D} 2^{A(2^{D+1}-2)} < t/2 .$$

FV CONSTRAINTS

$$D \lesssim \min \left\{ \left\lfloor \log\left(\frac{n\log b + 2A - 1}{2A + \log L}\right) \right\rfloor , \left\lfloor \frac{\log q - \log\left(2(b+1)^2 n^{3/2}\right)}{\log(14(b+1)n) + A} \right\rfloor \right\} .$$

HP-FV CONSTRAINT

FV vs. HP-FV: results

FV + NAF

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

HP-FV enables much higher depth

FV + NAF

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	[illegible]	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	[illegible]	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

HP-FV enables much higher depth

FV + NAF

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	[illegible]	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	[illegible]	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	[illegible]	13

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

HP-FV enables much higher depth

FV + NAF

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	[illegible]	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A = 3$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	[illegible]	183	3

HP-FV

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	[illegible]	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A = 3$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	[illegible]	13

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	[illegible]	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

Larger n in HP-FV gives much more capability

FV + NAF

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

Larger n in HP-FV gives much more capability

FV + NAF

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A = 3$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A = 3$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

Addition hurts FV more than HP-FV

FV + NAF

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	3	43	3
32768	890	80	5	102	5	63	4	76	4	91	4

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	12	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	0	—	0	—	0
4096	116	24	1	25	1	26	1	27	1	28	1
8192	226	24	1	25	1	26	1	27	1	28	1
16384	435	69	2	71	2	73	2	76	2	79	2
32768	890	159	3	164	3	170	3	176	3	183	3

HP-FV

		$A=0$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A=3$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A=10$									
		$L=2^8$		$L=2^{16}$		$L=2^{32}$		$L=2^{64}$		$L=2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

Addition hurts FV more than HP-FV

FV + NAF

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	[illegible]	[illegible]	3
32768	890	80	5	102	5	63	4	[illegible]	[illegible]	[illegible]	4

		[illegible]									
		$L = 2^8$		$L = 2^{16}$		[illegible]		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	[illegible]	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	[illegible]	[illegible]	[illegible]	—	0
4096	116	24	1	25	1	26	1	[illegible]	[illegible]	28	1
8192	226	24	1	25	1	26	1	[illegible]	[illegible]	[illegible]	1
16384	435	69	2	71	2	73	2	76	[illegible]	79	2
32768	890	159	3	164	3	170	3	176	[illegible]	183	3

HP-FV

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	17	8
16384	435	257	14	257	13	257	12	257	11	65539	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	$\approx 2^{32}$	14	$\approx 2^{32}$	13

		$A = 3$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	724	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	$\approx 2^{19}$	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	9	5	9	10	9	7	8	25	8
16384	435	128	12	512	12	91	11	1447	11	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	13	$\approx 2^{37}$	13

Addition hurts FV more than HP-FV

FV + NAF

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	4	1	5	1	6	1	7	1	8	1
4096	116	9	2	11	2	13	2	16	2	19	2
8192	226	19	3	24	3	30	3	36	3	19	2
16384	435	39	4	50	4	63	4	36	[illegible]	[illegible]	3
32768	890	80	5	102	5	63	4	[illegible]	[illegible]	[illegible]	4

		$A = $ [illegible]									
		$L = 2^8$		$L = 2^{16}$		[illegible]		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	10	1	11	1	[illegible]	1	13	1	—	0
4096	116	10	1	11	1	12	1	13	1	14	1
8192	226	27	2	29	2	31	2	34	2	37	2
16384	435	61	3	66	3	72	3	78	3	85	3
32768	890	129	4	140	4	153	4	78	3	85	3

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$	$\log t$	$\max D$
2048	60	—	0	—	0	—	[illegible]	[illegible]	[illegible]	—	0
4096	116	24	1	25	1	26	1	[illegible]	[illegible]	28	1
8192	226	24	1	25	1	26	1	[illegible]	[illegible]	[illegible]	1
16384	435	69	2	71	2	73	2	76	[illegible]	79	2
32768	890	159	3	164	3	170	3	176	[illegible]	183	3

HP-FV

		$A = 0$									
		$L = 2^8$		$L = 2^{16}$		$L = 2^{32}$		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	3	10	5	10	5	9	17	9	[illegible]	8
16384	435	257	14	257	13	257	12	257	[illegible]	[illegible]	11
32768	890	$\approx 2^{16}$	16	$\approx 2^{16}$	15	$\approx 2^{32}$	15	[illegible]	[illegible]	[illegible]	13

		$A = $ [illegible]									
		$L = 2^8$		$L = 2^{16}$		[illegible]		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	2	2	2	2	2
4096	116	2	5	2	5	2	5	2	5	3	5
8192	226	4	10	7	10	6	9	21	9	19	8
16384	435	128	13	2048	13	[illegible]	12	431	11	332	10
32768	890	$\approx 2^{28}$	16	$\approx 2^{22}$	15	[illegible]	14	$\approx 2^{35}$	14	$\approx 2^{33.5}$	13

		$A = 10$									
		$L = 2^8$		$L = 2^{16}$		[illegible]		$L = 2^{64}$		$L = 2^{128}$	
n	$\log q$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$	b	$\max D$
2048	60	2	2	2	2	2	[illegible]	[illegible]	[illegible]	[illegible]	2
4096	116	2	5	2	5	2	5	[illegible]	[illegible]	[illegible]	5
8192	226	4	9	5	9	10	9	[illegible]	[illegible]	[illegible]	8
16384	435	128	12	512	12	91	11	1447	[illegible]	609	10
32768	890	$\approx 2^{28}$	15	$\approx 2^{18}$	14	$\approx 2^{26}$	14	$\approx 2^{21}$	[illegible]	[illegible]	13

SUMMARY

In this talk we

- Discussed the need for good encoding in homomorphic encryption
- Applied Hoffstein-Silverman trick to FV
- Showed performance improvements compared to FV

Thank you!

Any questions?

https://eprint.iacr.org/2017/809

- haoche@microsoft.com
- kim.laine@microsoft.com
- rachel.player@lip6.fr
- yuhoux@math.princeton.edu

RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

#RSAC

SESSION ID: CRYP-W02

THRESHOLD PROPERTIES OF PRIME POWER SUBGROUPS WITH APPLICATION TO SECURE INTEGER COMPARISONS

Aleksander Essex

Assistant professor
Western University, Canada
@aleksessex

Co-authors: Rhys Carlton and Krzysztof Kapulkin

Encryption in $\mathbb{Z}_n^*$

General form:

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- g generates subgroup $\mathbb{G}$ of $\mathbb{Z}_n^*$
- h generates a subgroup $\mathbb{H}$ of $\mathbb{Z}_n^*$

Additive Homomorphism

A useful property: Adding under encryption

$$c_1 \cdot c_2 \quad = \quad g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2}$$

Additive Homomorphism

A useful property: Adding under encryption

$$\begin{aligned} c_1 \cdot c_2 &= g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2} \\ &= g^{m_1+m_2} h^{r_1+r_2} \end{aligned}$$

Additive Homomorphism

A useful property: Adding under encryption

$$\begin{aligned} c_1 \cdot c_2 &= g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2} \\ &= g^{m_1+m_2} h^{r_1+r_2} \\ &= \mathsf{Enc}(m_1 + m_2) \end{aligned}$$

Additive Homomorphism

A useful property: Adding under encryption

$$\begin{aligned} c_1 \cdot c_2 &= g^{m_1} h^{r_1} \cdot g^{m_2} h^{r_2} \\ &= g^{m_1+m_2} h^{r_1+r_2} \\ &= \mathsf{Enc}(m_1 + m_2) \end{aligned}$$

Additive Homomorphism

$$\mathsf{Enc}(m_1) \cdot \mathsf{Enc}(m_2) \;=\; \mathsf{Enc}(m_1 + m_2)$$

Interesting, but over 35 years of examples…

Encryption in $\mathbb{Z}_n^*$

Goldwasser-Micali (1982)

$$\mathsf{Enc}(m) = g^m h^r \mod n$$

- $|\mathbb{G}| = 2 \mod p, |\mathbb{G}| = 2 \mod q$
- $|\mathbb{H}| = \frac{p-1}{2} \mod p, |\mathbb{H}| = \frac{q-1}{2} \mod q$

Encryption in $\mathbb{Z}_n^*$

Benaloh (1994)

$$\mathsf{Enc}(m) = g^m h^r \mod n$$

- $|\mathbb{G}| = s \mod p, |\mathbb{G}| = (q-1) \mod q$, for small/smooth s
- $|\mathbb{H}| = \frac{(p-1)}{s} \mod p, |\mathbb{H}| = (q-1) \mod q$

Encryption in $\mathbb{Z}_n^*$

Naccache-Stern (1998)

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- $|\mathbb{G}| = u \bmod p, |\mathbb{G}| = v \bmod q$, for smooth relatively prime u, v
- $|\mathbb{H}| = \frac{(p-1)}{u} \bmod p, |\mathbb{H}| = \frac{(q-1)}{v} \bmod q$

Encryption in $\mathbb{Z}_n^*$

Okamoto-Uchiyama (1998)

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- $n = p^2 q$
- $|\mathbb{G}| = p \cdot (p-1) \bmod p^2, |\mathbb{G}| = (q-1) \bmod q$
- $|\mathbb{H}| = (p-1) \bmod p^2, |\mathbb{H}| = (q-1) \bmod q$

Encryption in $\mathbb{Z}_n^*$

Paillier (1999)

$$\mathsf{Enc}(m) = g^m h^r \bmod n^2$$

- $|\mathbb{G}| = p \bmod p^2, |\mathbb{G}| = q \bmod q^2$
- $|\mathbb{H}| = (p-1) \bmod p^2, |\mathbb{H}| = (q-1) \bmod q^2$

Encryption in $\mathbb{Z}_n^*$

Groth (2003)

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- $|\mathbb{G}| = p_s \bmod p, |\mathbb{G}| = q_s \bmod q$ for large smooth p_s, q_s
- $|\mathbb{H}| = p_t = \frac{(p-1)}{p_s} \bmod p, |\mathbb{H}| = q_t = \frac{(q-1)}{q_s} \bmod q$ for “just big enough” primes p_t, q_t

Encryption in $\mathbb{Z}_n^*$

Damgård-Geisler-Krøigaard (2007)

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- $|\mathbb{G}| = u \bmod p, |\mathbb{G}| = u \bmod q$ for small prime u
- $|\mathbb{H}| = p_s \bmod p, |\mathbb{H}| = q_s \bmod q$ for "just big enough" primes p_s, q_s

Encryption in $\mathbb{Z}_n^*$

Joye-Libert (2013)

$$\mathsf{Enc}(m) = g^m h^r \bmod n$$

- $|\mathbb{G}| = 2^k \bmod p, |\mathbb{G}| = 2^k \bmod q$
- $|\mathbb{H}| = p_t = \frac{(p-1)}{2^k} \bmod p, |\mathbb{H}| = q_t = \frac{(q-1)}{2^k} \bmod q$ for primes p_t, q_t

A Scalar Threshold Homomorphism

Something new: Computing a threshold under encryption

$$\mathsf{Enc}(m_1)^{m_2} = \begin{cases} \mathsf{Enc}(m_1 + m_2) & m_1 + m_2 < t \\ \mathsf{Enc}(\varnothing) & \text{otherwise.}^* \end{cases}$$

$^*\mathsf{Enc}(\varnothing)$ is the encryption of a fixed value outside the defined plaintext space.

A Scalar Threshold Homomorphism

Our proposal:

$$\mathsf{Enc}(m) = g^{b^m} h^r \bmod n$$

- $|\mathbb{G}| = b^d \bmod p, |\mathbb{G}| = b^d \bmod q$ for small prime base b, and threshold d
- $|\mathbb{H}| = p_s \bmod p, |\mathbb{H}| = q_s \bmod q$ for "just big enough" primes p_s, q_s

A Scalar Threshold Homomorphism

$$\mathsf{Enc}(m_1)^{b^{m_2}} \quad = \quad (g^{b^{m_1}} h^r)^{b^{m_2}}$$

A Scalar Threshold Homomorphism

$$\begin{aligned} \mathsf{Enc}(m_1)^{b^{m_2}} &= (g^{b^{m_1}} h^r)^{b^{m_2}} \\ &= g^{b^{m_1} b^{m_2}} h^{r'} \end{aligned}$$

A Scalar Threshold Homomorphism

$$\begin{aligned}\mathsf{Enc}(m_1)^{b^{m_2}} &= (g^{b^{m_1}} h^r)^{b^{m_2}} \\ &= g^{b^{m_1} b^{m_2}} h^{r'} \\ &= g^{b^{(m_1+m_2)}} h^{r'}\end{aligned}$$

A Scalar Threshold Homomorphism

$$
\begin{aligned}
\mathsf{Enc}(m_1)^{b^{m_2}} &= (g^{b^{m_1}} h^r)^{b^{m_2}} \\
&= g^{b^{m_1} b^{m_2}} h^{r'} \\
&= g^{b^{(m_1+m_2)}} h^{r'} \\
&= \mathsf{Enc}(m_1 + m_2)
\end{aligned}
$$

A Scalar Threshold Homomorphism

$$
\begin{aligned}
\mathsf{Enc}(m_1)^{b^{m_2}} &= (g^{b^{m_1}} h^r)^{b^{m_2}} \\
&= g^{b^{m_1} b^{m_2}} h^{r'} \\
&= g^{b^{(m_1+m_2)}} h^{r'} \\
&= \mathsf{Enc}(m_1 + m_2)
\end{aligned}
$$

A Scalar Threshold Homomorphism

Except…

$$\mathsf{Enc}(m_1 + m_2) \quad \equiv \quad g^{b^{m_1+m_2} \bmod b^d} h^r \bmod n$$

A Scalar Threshold Homomorphism

Except...

$$\text{Enc}(m_1 + m_2) \equiv g^{b^{m_1+m_2} \bmod b^d} h^r \bmod n$$

So if $m_1 + m_2 \geq d$, then $b^{m_1+m_2} \equiv 0 \bmod b^d$. Then:

$$\begin{aligned} \text{Enc}(m_1 + m_2) &\equiv g^0 h^{r'} \\ &\equiv h^{r'} \\ &\equiv \text{Enc}(\varnothing) \end{aligned}$$

A Scalar Threshold Homomorphism

Limitation: The threshold is one-sided.

May be interesting for certain applications, but to do a secure comparison (i.e., Millionaire's), we need a protocol to homomorphically blind the sum.

Secure Integer Comparison Protocol

P$_1$ **P**$_2$

$C \leftarrow \mathsf{Enc}(m_1)$

$$= g^{b^{m_1}} h^{r_1} \xrightarrow{\quad C \quad}$$

Secure Integer Comparison Protocol

P$_1$

$C \leftarrow \mathsf{Enc}(m_1)$

$= g^{b^{m_1}} h^{r_1} \xrightarrow{\quad C \quad}$

P$_2$

$D \leftarrow (C)^{b^{(d-m_2)}} g^s h^{r_2}$ s.t. $s \not\equiv 0 \bmod b$

Western UNIVERSITY · CANADA

Secure Integer Comparison Protocol

P_1

$C \leftarrow \mathsf{Enc}(m_1)$

$= g^{b^{m_1}} h^{r_1}$ $\xrightarrow{\quad C \quad}$

P_2

$\xleftarrow{\quad D \quad}$ $D \leftarrow (C)^{b^{(d-m_2)}} g^s h^{r_2}$ s.t. $s \not\equiv 0 \bmod b$

$g^w \leftarrow (D)^x$

$w \leftarrow \log_g(g^w)$

Secure Integer Comparison Protocol

P$_1$

$C \leftarrow \mathsf{Enc}(m_1)$

$= g^{b^{m_1}} h^{r_1}$ $\xrightarrow{\quad C \quad}$

P$_2$

$\xleftarrow{\quad D \quad}$ $D \leftarrow (C)^{b^{(d-m_2)}} g^s h^{r_2}$ **s.t.** $s \not\equiv 0 \bmod b$

$g^w \leftarrow (D)^x$

$w \leftarrow \log_g(g^w)$

$\xleftrightarrow{\quad \mathsf{PET}_{CS_\oplus}(w, s) \quad}$

Output True if $(w = s)$,

Output False otherwise

Performance

- Threshold d consumes d bits of p and q
- Implication: Current range of RSA key-lengths puts an upper bound of $d \approx 2^{10}$

Performance

- Threshold d consumes d bits of p and q
- Implication: Current range of RSA key-lengths puts an upper bound of $d \approx 2^{10}$
- Performance comparison in paper was done on 8 bits per protocol instance
- Extensible to arbitrary precision comparisons with multiple parallel protocol invocations

Performance

- Threshold d consumes d bits of p and q
- Implication: Current range of RSA key-lengths puts an upper bound of $d \approx 2^{10}$
- Performance comparison in paper was done on 8 bits per protocol instance
- Extensible to arbitrary precision comparisons with multiple parallel protocol invocations
- Performance 3.5–5.5 times faster than DGK, in about 7.5 times less data transmitted

Conclusion

Thank-you,

Questions?