

une

**KU LEUVEN** 

# Homomorphic SIM<sup>2</sup>D operations: Single Instruction Much More Data

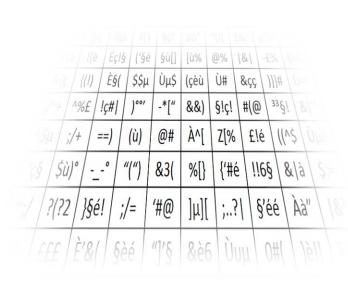
Wouter Castryck Ilia Iliashenko Frederik Vercauteren

PM .

#### Homomorphic encryption

	/-2.1	1 3.1	-9.9	9 -9.8	2.3	1.4	5.7	9.6			
	8.3	0.8	0.3	-0.3	-0.7	-6.2	3.2	5.2	4.14		
-9.1	-4.3	-0.1	0.0	2.5	1.8	9.6	2.	1 3	.4 \ 23		
6.1   -3	3.3	2.3	-3.2	5.5	-5.1	2.9	9	.9 \	-6.9		
5.5 3.2	?   8	37	-9.9	<mark>2.4</mark>	8.9	7.6	5	8.8	-5.6	2.4	
8.2 9.4	2	3   -	5.4	3.2	- <mark>6.</mark> 6	-6.	3	2.2	1.9	0	
0   -2.7	0.9	0	9	8.2	5.7	3	.1	9.	3 -6	3	





С

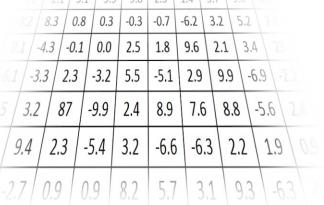
175.2

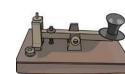
 $C_{\mathrm{cryp}}$ 



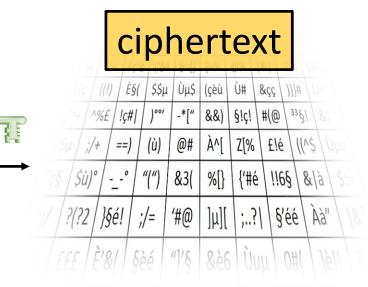
### Homomorphic encoding

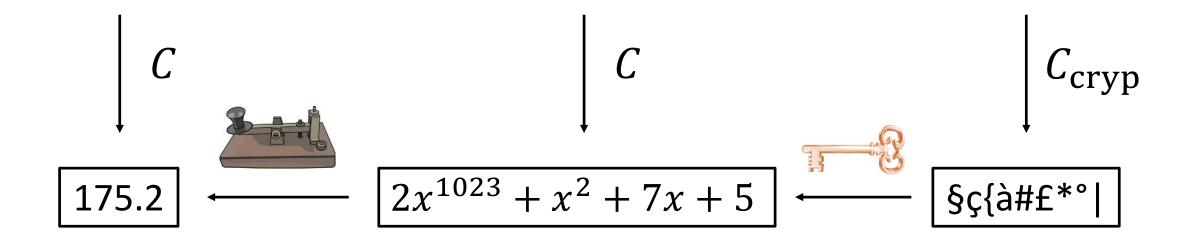
#### real-world data





	1	pla	aint	ext	
2.	+1	$\int -x^2 - 5$	$x^2 + x + 1$	$x^2 - x$	$-3x^2 + \pi$
x <sup>2</sup> +	3х	$\int 2x^2 - 3x$	$-7x^2 + x$	$-x^{3} + x^{2}$	$\chi^4 = \chi$
$-x^{3}+$	x	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	$7x^2 - 6x$
$6x^3 + x^3$	2	$x^2 - x$	$-x^{2} + x$	$-x^3 - x^2$	$x^3 - 2x$
$x^{2} + 3$		x – 3	$x^4 + 2x^3$	x <sup>2</sup>	0
$x^2 + 4$	-4	$ x^2 - 1 $	$x^2 - 1$	$x^{2} + x +$	$-1 \sqrt{x^2 - (x^2 - x^2)}$
<sup>2</sup> +2x	X	+1	x – 1	$\chi^{2} +$	$3 \setminus 4x^2$



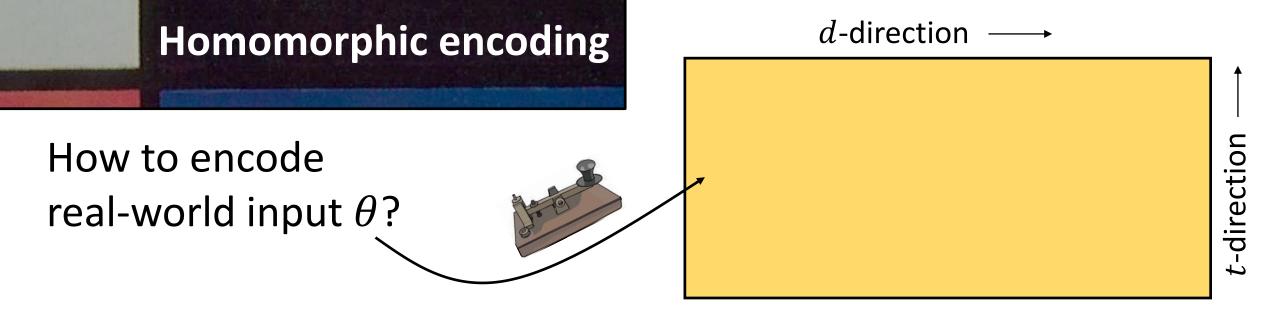


#### **Plaintext space**

Typically a ring of the form 
$$R_t = \frac{\mathbf{Z}[x]}{(f(x), t)}$$

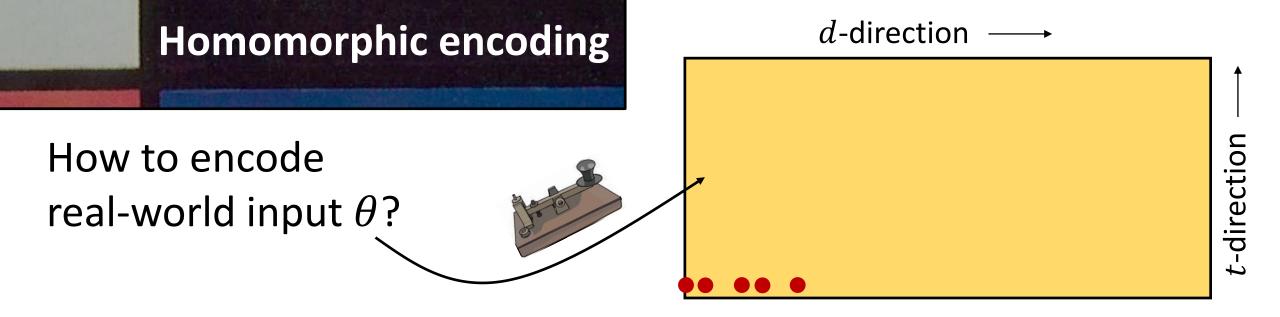
where  $t \in \mathbb{Z}_{\geq 2}$  and  $f(x) \in \mathbb{Z}[x]$  is monic irreducible of degree d.

We represent this by a box: Polynomials of degree < dand coefficients in [0, t).



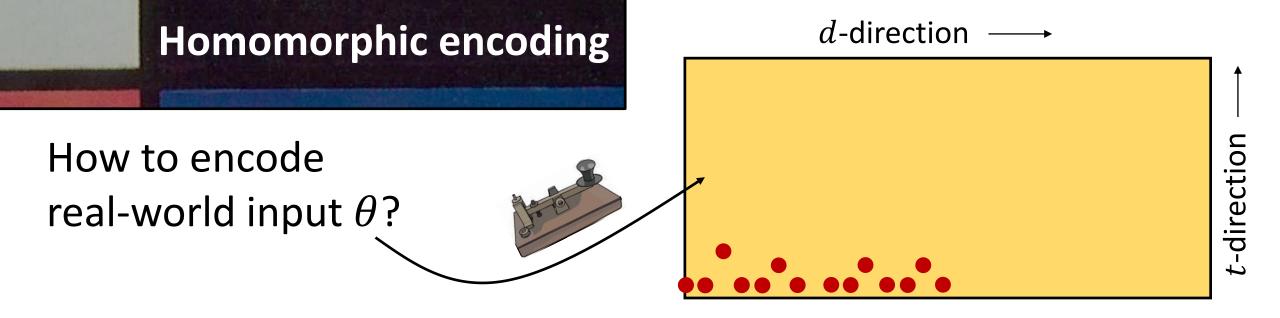
$$\theta \approx a_r b^r + a_{r-1} b^{r-1} + \dots + a_1 b + a_0$$
 for some base  $b \in \mathbf{C}$ .

Then encode as  $a_r x^r + a_{r-1} x^{r-1} + \dots + a_1 x + a_0$ .



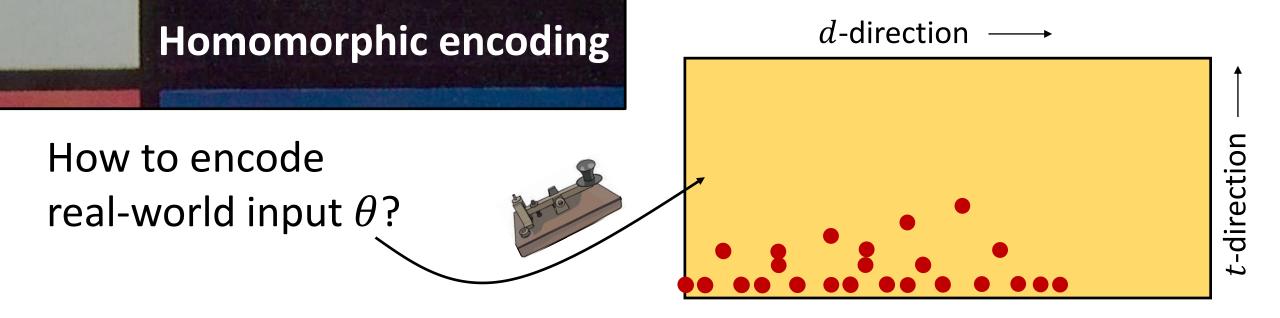
 $\theta = 2^6 + 2^4 + 2^3 + 2 + 1$ 

Then encode as  $a_r x^r + a_{r-1} x^{r-1} + \dots + a_1 x + a_0$ .



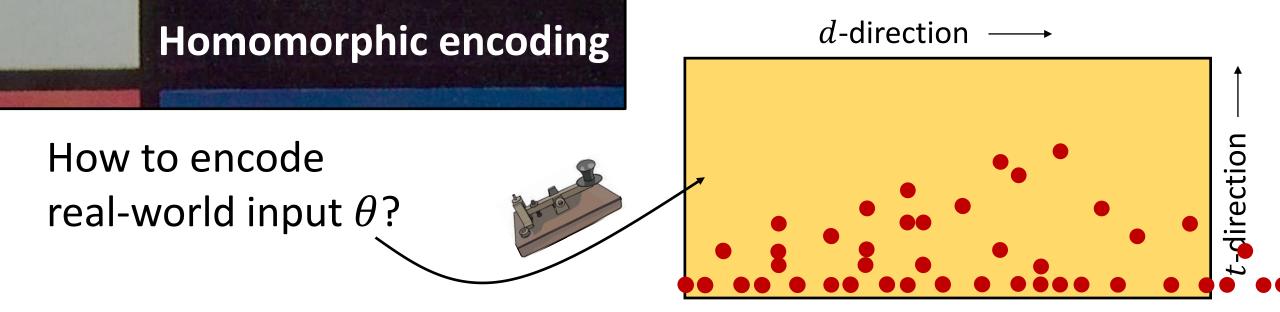
 $\theta = 2^6 + 2^4 + 2^3 + 2 + 1$ 

Then encode as  $a_r x^r + a_{r-1} x^{r-1} + \dots + a_1 x + a_0$ .



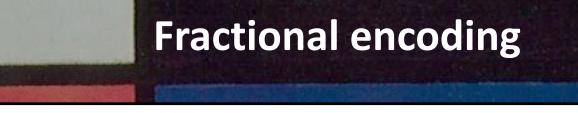
 $\theta = 2^6 + 2^4 + 2^3 + 2 + 1$ 

Then encode as  $a_r x^r + a_{r-1} x^{r-1} + \dots + a_1 x + a_0$ .



 $\theta = 2^6 + 2^4 + 2^3 + 2 + 1$ 

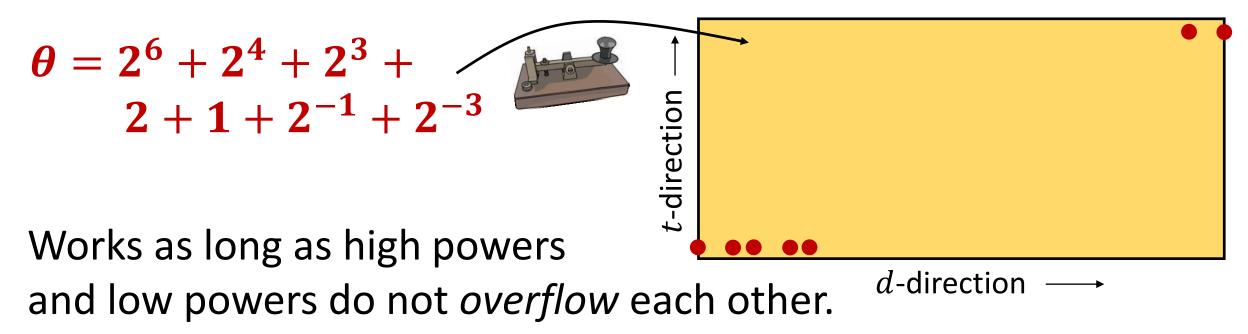
Then encode as  $a_r x^r + a_{r-1} x^{r-1} + \dots + a_1 x + a_0$ .

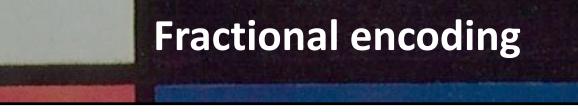


**Encoding fractional expansions** 

$$\theta \approx a_r b^r + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots + a_{-s} b^{-s}?$$

[Dowlin et al., '15] If  $f(x) = x^d + 1$  then  $x^{-i} \equiv -x^{d-i}$ , so: put fractional part at the high powers, with negated sign.

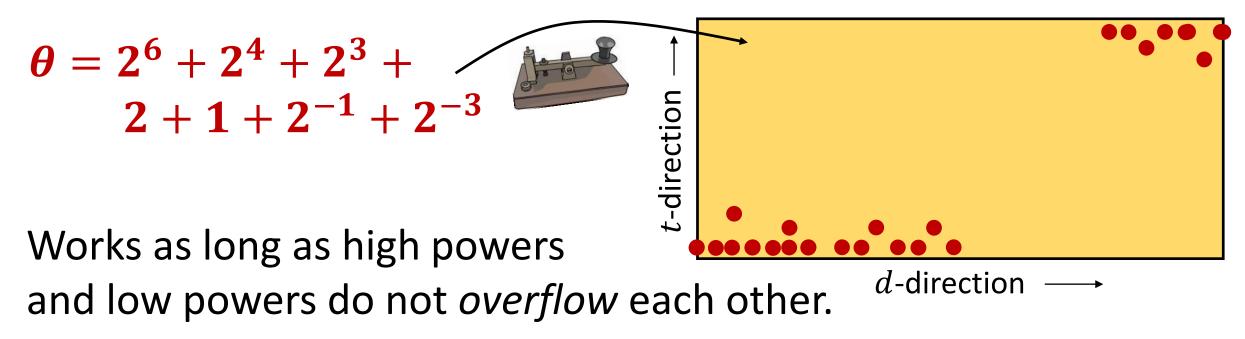


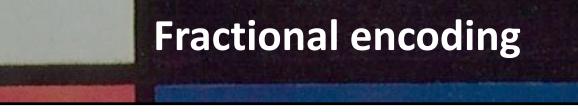


**Encoding fractional expansions** 

$$\theta \approx a_r b^r + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots + a_{-s} b^{-s}?$$

[Dowlin et al., '15] If  $f(x) = x^d + 1$  then  $x^{-i} \equiv -x^{d-i}$ , so: put fractional part at the high powers, with negated sign.

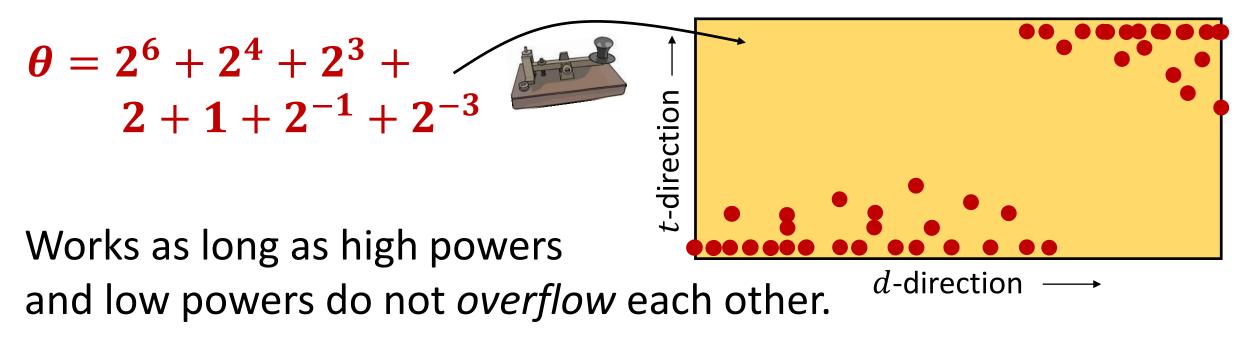




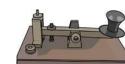
Encoding fractional expansions

$$\theta \approx a_r b^r + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots + a_{-s} b^{-s}?$$

[Dowlin et al., '15] If  $f(x) = x^d + 1$  then  $x^{-i} \equiv -x^{d-i}$ , so: put fractional part at the high powers, with negated sign.

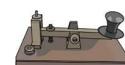


	-2.	1 3	.1	-9.9	-9.8	2.3	1.4	5.	7		
	8.3	0.	8	0.3	-0.3	-0.7	-6.2	. 3	.2	5.2	
-9.1 / -4	4.3	-0.1	1	0.0	2.5	1.8	9.6	5 ] 7	2.1	3.	.4 23
6.1   -3.	3	2.3	-	3.2	5.5	- <mark>5.1</mark>	2.	9	9.9	-	6.9 -2.1
5.5 3.2	/	87	-9	9.9	2.4	8.9	7	.6	8.	8 \	-5.6 2.4
8.2 9.4	2.	3	-5	.4	3.2	-6.6	-	6.3	2	.2	1.9 08
0   -2.7	0.9	,	0,9	9	8.2	5.7		3,1		<i>ð</i> 3	3 -6.3



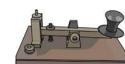
8	$\pm 1$	$\int -x^2 - 5$	$x^2 + x + 1$	$x^2 - x$	-3x <sup>2</sup>	
$x^{2} +$	3x	$2x^2 - 3x$	$-7x^2 + x$	$-x^3 + x^2$	x4	- X
$-x^{3}+$	x	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	\7x	$\frac{1}{2} - \rho x$
$6x^3 + x$	2	$x^2 - x$	$-x^2 + x$	$-x^3 - x$	2	$x^3 - 2x$
$x^{2} + 3$	/	x – 3	$x^4 + 2x^3$	x <sup>2</sup>		0
$x^{2} + 4$	-4	$ x^2 - 1 $	$x^2 - 1$	$x^2 + x$	+1	<b>x</b> <sup>2</sup> - 6
<sup>2</sup> +2x	X	+1	<i>x</i> – 1	$\chi^2$ -	+3	$4\chi^2 - 1$

	-2.	1 3	8.1	-9.9	-9.8	2.3	1.4	5.7	9		
	8.3	0.	8	0.3	-0.3	-0.7	-6.2	3.	2 ] [	5.2	
-9.1 / -	4.3	-0	1	0.0	2.5	<mark>1.</mark> 8	9.6	5 2	.1	3.4	
-6.1   -3.	3	2.3	-	3.2	5.5	- <mark>5.1</mark>	2.	9   9	9.9	-6	.9 -2.1
5.5 3.2	1	87	-9	9.9	2.4	<mark>8.9</mark>	7	.6	8.8		5.6 2.4
8.2 9.4	2.	3	-5	.4	3.2	-6.6	-	6.3	2.	2	1.9 09
0   -2.7	0,9		0,9	9	8.2	5.7		3.1	Ç	),3	-6.3



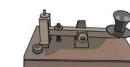
8	$\pm 1$	$\int -x^2 - 5$	$x^2 + x + 1$	$x^2 - x$	$-3x^2$	
$x^{2} +$	3x	$2x^2 - 3x$	$-7x^2 + x$	$-x^{3} + x^{2}$	x4	- X
$-x^{3}+$	x	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	\7x <sup>2</sup>	$b_{7} - \rho x$
$6x^3 + x$	2	$x^2 - x$	$-x^2 + x$	$-x^3 - x$	2 \ x	t <sup>3</sup> – 2.x
$x^{2}+3$		x – 3	$x^4 + 2x^3$	x <sup>2</sup>		0
$x^{2} + 4$	-4	$ x^2 - 1 $	$x^2 - 1$	$x^2 + x$	+1	x2 - 6
<sup>2</sup> +2x	X	+1	<i>x</i> – 1	χ <sup>2</sup> -	- 3	$4x^2 - 1$

	-2.	1 3	8.1	-9.9	-9.8	2.3	1.4	5.7	9		
	8.3	0.	8	0.3	-0.3	-0.7	-6.2	3.7	2 \ 1	5.2	
-9.1 / -4	4.3	-0	1	0.0	2.5	1.8	9.6	2	.1	3.4	
6.1   -3.	3	2.3	-	3.2	5.5	- <mark>5.1</mark>	2.	9   9	9.9	-6	.9 -2.1
5.5 3.2	/	87	-9	9.9	2.4	<mark>8.9</mark>	7	.6	8.8	-	5.6 2.4
8.2 9.4	2.	3	-5	.4	3.2	-6.6		5.3	2	2	1.9 0.9
0   -2.7	0.9		0,9	9	8.2	5.7		3.1	ļ	9,3	-6.3



	+1	$\int -x^2 - 5$	$x^2 + x + 1$	$x^2 - x$	-3x <sup>2</sup>	
$x^{2} +$	3x	$2x^2 - 3x$	$-7x^2 + x$	$-x^3 + x^2$	x <sup>4</sup>	- X
$-x^{3}+$	x /	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	7 x	$r_{2} - \rho x$
$6x^3 + x$	2	$x^2 - x$	$-x^2 + x$	$-x^3 - x$	2 )	$x^3 - 2x$
$x^{2} + 3$	/	x – 3	$x^4 + 2x^3$	x <sup>2</sup>		0
$x^{2} + 4$	-4	$x^2 - 1$	$x^2 - 1$	$x^2 + x$	+1	$\chi^2 - 6$
<sup>2</sup> +2x	X	+1	x – 1	$\chi^2$ -	+3	$\sqrt{4\chi^2 - 1}$

35   -2.1	3.1	-9.9	-9.8	2.3	1.4	5.7	9.6		
-8.2 8.3	0.8	0.3	-0.3	-0.7	-6.2	3.2	5.2		
9.1 -4.3	0.1	0.0	2.5	1.8	9.6	2.	.1 \ 3.4	23	
-6.1   -3.3   2	.3	-3.2	<mark>5.5</mark>	- <mark>5.1</mark>	2.9	9 6	9.9 \ -6	.9 -2.1	
5.5 3.2 8	7   -	9.9	2.4	8.9	7.	6	8.8	-5.6 2	
8.2   9.4   2.3	-	5.4	3.2	-6.6	-6	5.3	2.2	1.9	
1   -2.7   0.9	0,	9	8.2	5.7		3,1	9.3	-6,3	



	+1	$-x^2-5$	$x^2 + x + 1$	$x^2 - x$	-3x <sup>2</sup>	
x2+	3x	$2x^2 - 3x$	$-7x^2 + x$	$-x^{3} + x^{2}$	x4	— X.
$-x^{3}+$	x	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	\7x	2 - 6x
$6x^3 + x^4$	2	$x^2 - x$	$-x^{2} + x$	$-x^3 - x$	2 )	t <sup>3</sup> − 2x
$x^{2} + 3$	/	x – 3	$x^4 + 2x^3$	x <sup>2</sup>		0
<sup>2</sup> +4	-4	$x^2 - 1$	$x^2 - 1$	$x^2 + x$	+1	$x_5 - \ell$
-2x	X	+1	x – 1	χ <sup>2</sup> -	- 3	4χ <sup>2</sup> - 1

Batch encoding is possible thanks to CRT [Smart-Vercauteren, '14]:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$

								.7 9.6				-3x x + 2		-
		8.3	1		-			3.2 5.					$\frac{x^2 + x + 1}{-7x^2 + x}$	-
			-0.1			1.8	-		3.4 23	A PROV	$\frac{x^2+.}{3}$			+
	1		2.3	-3.2			2.9		-6.9 -2.1		$-x^3+$			+
0.1	/						2.5				$6x^3 + x^2$	$\frac{x^2-x}{x^2-x}$	$-x^{2} + x$	
5.5	3.2	8	7	-9.9	2.4	8.9	7.6	8.8	-5.6 2.4		$x^{2} + 3$	$\int x-3$	$x^4 + 2x^3$	
8.2	9.4	2.3	3   -	5.4	3.2	-6.6	-6.3	2.2	1.9 09		$x^2 + 4$	$-4x^2 - 1$	$x^2 - 1$	
			+					+						_
01-2	7 /	19	10	9	82	57	21	0	3 -6.3 1		+2r	x+1	$\gamma = 1$	

		-1	$-x^2 - 5$	$x^{2} + x +$	-1 x <sup>2</sup>	- x 💧	-3x <sup>2</sup> -		
B	$x^{2} + 3$	3x	$2x^2 - 3x$	$-7x^{2} +$	$x - x^3$	$^{3} + x^{2}$	x4 -	- X	
	$-x^{3}+$	r	$-x^3 - 8x$	$3x^2 + 2$	2x  3x	$x^2 - 5$	$\sqrt{7x^2}$	$-\theta x$	
6.	$x^{3} + x^{2}$	'	$x^2 - x$	$-x^{2} +$	x -)	$x^3 - x^2$	x	3 - 2x	
x²	+3	.	r – 3	$x^4 + 2x^4$	x <sup>3</sup>	$\chi^2$		0	
x <sup>2</sup> +	-4	-4;	$r^2 - 1$	$x^2 - 2$	1 x <sup>2</sup>	<sup>2</sup> + x -	+1	χ <sup>2</sup> –	6
$^{2}+2$	r	χ-	+1	x – 1		$\chi^2 +$	3	4χ <sup>2</sup>	- 1

Batch encoding is possible thanks to CRT [Smart-Vercauteren, '14]:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$

	1-2	2.1   .	3.1	-9.9	-9.8	2.3	1.4	5.	1 9	.6			
	8.	3   0	.8	0.3	-0.3	-0.7	-6.2	3	.2	5.2			
	-4.3	-0.	1	0.0	2.5	1.8	9.6	5	2.1 \	3.4	23		
-6.1   -3	3.3	2.3	-	3.2	5.5	-5.1	2.	9	9.9	-6	.9/-2		
5.5   3.2	? [	87	-9	9.9	2.4	8.9	7	.6	8.8		-5.6		
8.2 9.4	2	2.3	-5	.4	3.2	-6.6	j -	6.3	2.	2	1.9	0!	
0   -2.7	0,,	9	0,	9	8.2	5.7		3,1	ļ	),3	-6,	3	



		1	$-x^2 - 5$	$x^2 + x + 1$		x <sup>2</sup> - x	$-3x^2$	
3	$x^2 + 3x$	r	$2x^2 - 3x$	$-7x^2 + x$	-	$-x^3 + x^2$	x4	- x
	$-x^3 + x$		$-x^3 - 8x$	$3x^2 + 2x$		$3x^2 - 5$	\7x	r - ex
	$6x^3 + x^2$	1	$x^2 - x$	$-x^2 + x$		$-x^3 - x^3$	· \ ;	$t^3 - 2x$
	$x^2 + 3$	/ x	<i>:</i> − 3	$x^4 + 2x^3$		$\chi^2$		0
	$r^2 + 4$	-4 <i>x</i>	<sup>2</sup> -1	$x^2 - 1$		$x^2 + x$	+1	x <sup>2</sup> - 6
	+2x	x +	-1	x - 1		$\chi^2$ +	- 3	4x2 -

Batch encoding is possible thanks to CRT [Smart-Vercauteren, '14]:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$

13/-2	2.1 3	.1 -9.9	-9.8	2.3	1.4	5.7	9.6			
-8.2   8.	3   0.	8 0.3	-0.3	-0.7	-6.2	3.2	5.2			
9.1   -4.3	-0.1	0.0	2.5	1.8	9.6	2.	1 3	.4 \ 23		g
6.1 -3.3	2.3	-3.2	<b>5.5</b>	-5.1	2.9	9	.9 \ -	6.9		
5.5 3.2	87	-9.9	2.4	<mark>8.</mark> 9	7.6	5	8.8	-5.6	2.4	
8.2   9.4   2	2.3	-5.4	3.2	- <mark>6.</mark> 6	-6	.3	2.2	1.9	09	
0   -2.7   0,.	9	0,9	8.2	5.7	3	1	<i>ð</i> .:	3 \ -6	3	

A	10	0	Q	B
	-	_	_	8

		+1	$\int -x^2 - 5$	$x^2 + x + 1$	x <sup>2</sup> - x	-3x <sup>2</sup>	
3	$x^2 +$	3x	$2x^2 - 3x$	$-7x^2 + x$	$-x^{3} + x^{2}$	x4	- X
	$-x^{3}+$	x	$-x^3 - 8x$	$3x^2 + 2x$	$3x^2 - 5$	7x <sup>7</sup>	$r = \theta x$
	$6x^3 + x$	2	$x^2 - x$	$-x^{2} + x$	$-x^{3} - x$	2 \ x	t <sup>3</sup> – 2x
	$x^{2} + 3$	/	x – 3	$x^4 + 2x^3$	x <sup>2</sup>		0
	<sup>2</sup> +4	-4	$ x^2 - 1 $	$x^2 - 1$	$x^2 + x$	+1	$x_5 - \ell$
	+2x	X	+1	x – 1	χ <sup>2</sup> -	+3	$\sqrt{4\chi^2}$ –

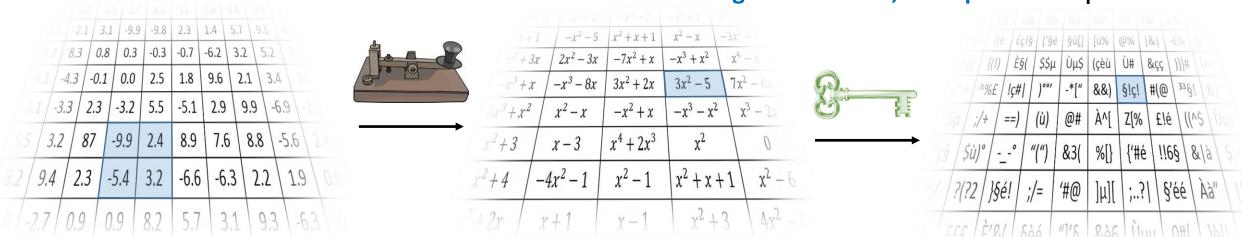
Batch encoding is possible thanks to CRT [Smart-Vercauteren, '14]:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$

SIMD —



#### Single Instruction, Multiple Data



Batch encoding is possible thanks to CRT [Smart-Vercauteren, '14]:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$



SIMD seems incompatible with fractional encoding, because most factors of  $x^d + 1$  modulo t are not of that form.

We give a very general fractional encoding method which does not require that  $f(x) = x^d + 1$ .

The CRT allows for more fine-grained decompositions by also incorporating factorizations of t.

We show that this enables more flexible and denser data packing.

# **Fractional encoding revisited**

Write 
$$f(x) = x \cdot g(x) + f(0)$$
.

First encode

$$a_r b^r + \dots + a_1 b + a_0 + a_{-1} b^{-1} + \dots + a_{-s} b^{-s}$$
  
as a Laurent polynomial in  $\mathbb{Z}[x^{\pm 1}]$  by substituting  $x$  for  $b$ .

#### **Fractional encoding revisited**

Write 
$$f(x) = x \cdot g(x) + f(0)$$
.

First encode

$$a_r x^r + \dots + a_1 x + a_0 + a_{-1} x^{-1} + \dots + a_{-s} x^{-s}$$

mild requirement:

f(0) invertible mod t

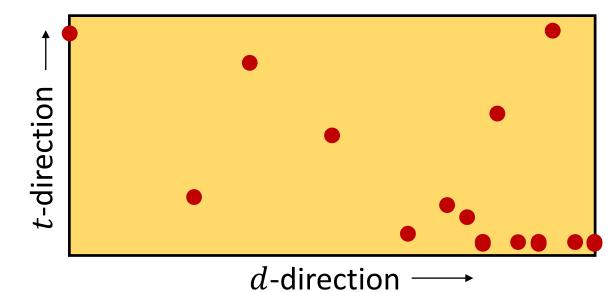
as a Laurent polynomial in  $\mathbb{Z}[x^{\pm 1}]$  by substituting x for b.

Then apply:

$$\mathbf{Z}[x^{\pm 1}] \xrightarrow{\text{mod } t} \mathbf{Z}_t[x^{\pm 1}] \xrightarrow{\eta_f} R_t \text{ where } \eta_f: \begin{cases} x \mapsto x \\ x^{-1} \mapsto -f(0)^{-1}g(x) \end{cases}$$

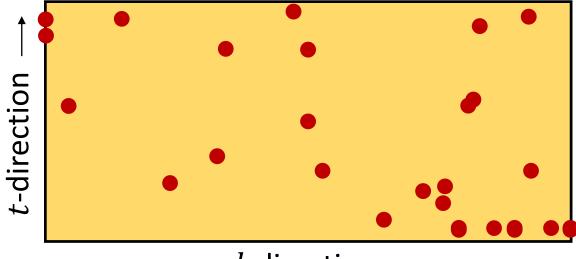
### Decoding

# Visually: looks like a mess, seems to overflow from the start!



### Decoding

# Visually: looks like a mess, seems to overflow from the start!

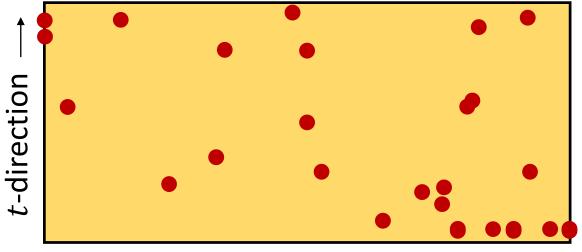


d-direction  $\longrightarrow$ 

### Decoding

Visually: looks like a mess, seems to overflow from the start!

Algebraically, much cleaner.



d-direction  $\longrightarrow$ 

If  $m - \ell + 1 = d$  then the restricted map

$$\mathbf{Z}_t[x^{\pm 1}]_{\geq \ell}^{\leq m} \xrightarrow{\eta_f} R_t$$

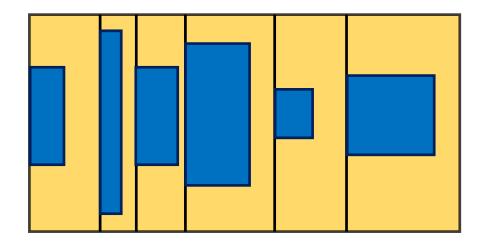
is an isomorphism of free  $\mathbf{Z}_t$ -modules of rank d.

**Bounding box** Suppose we know that the evaluation of C when carried out in  $Z[x^{\pm 1}]$  ends up in a certain box, and that some shifted *plaintext* space covers this box. **Z**-axis height *t* mx-axis width  $m - \ell + 1 = d$ Decoding = inverting  $\mathbf{Z}[x^{\pm 1}]_{>\ell}^{\leq m} \xrightarrow{\text{mod } t} \mathbf{Z}_t[x^{\pm 1}]_{>\ell}^{\leq m} \xrightarrow{\eta_f} R_t.$ 

The CRT decomposition used in [Smart-Vercauteren, '14]

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \xrightarrow{\cong} \frac{\mathbf{Z}[x]}{(f_1(x),t)} \times \frac{\mathbf{Z}[x]}{(f_2(x),t)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_r(x),t)}$$

can be viewed as a vertical slicing of plaintext space:



Each individual slice should cover the bounding box of the corresponding entry.

#### **Decomposing plaintext space**

We generalize this discussion: suppose

 $t = t_1 t_2 t_3 \cdots t_s$  and

$$f(x) = \prod_{i=1}^{r_i} f_{ij}(x) \mod t_i$$

are factorizations into coprimes. Then:

$$R_{t} = \frac{\mathbf{Z}[x]}{(f(x), t)} \cong \frac{\mathbf{Z}[x]}{(f(x), t_{1})} \times \frac{\mathbf{Z}[x]}{\mathbf{X}} \times \frac{\mathbf{Z}[x]}{(f(x), t_{S})}$$

#### **Decomposing plaintext space**

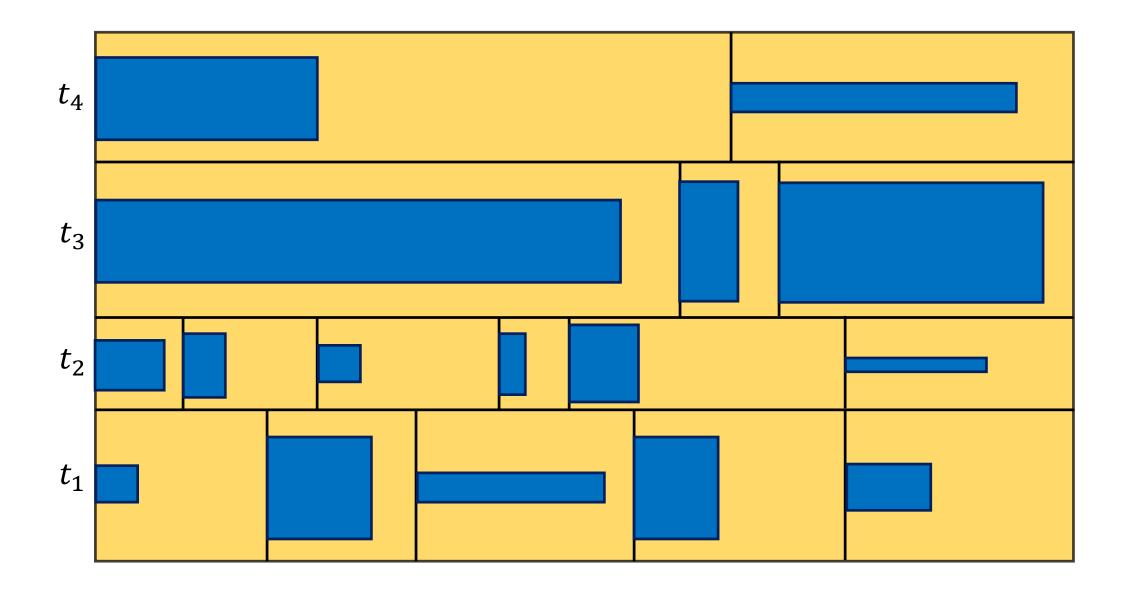
We generalize this discussion: suppose

 $t = t_1 t_2 t_3 \cdots t_s$  and  $f(x) = \prod_{i=1}^{n} f_{ij}(x) \mod t_i$ are factorizations into coprimes. Then:

$$R_t = \frac{\mathbf{Z}[x]}{(f(x),t)} \cong \frac{\mathbf{Z}[x]}{(f_{11}(x),t_1)} \times \frac{\mathbf{Z}[x]}{(f_{12}(x),t_1)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_{1r_1}(x),t_1)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_{1r_1}(x),t_1)} \times \frac{\mathbf{Z}[x]}{(f_{s1}(x),t_s)} \times \frac{\mathbf{Z}[x]}{(f_{s2}(x),t_s)} \times \cdots \times \frac{\mathbf{Z}[x]}{(f_{sr_s}(x),t_s)}$$

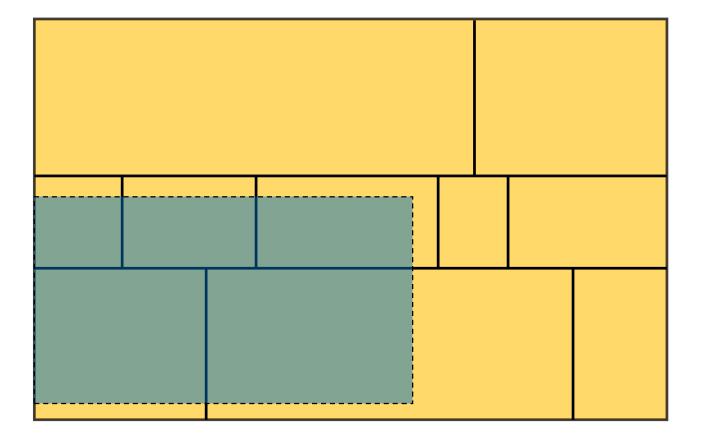
 $r_i$ 

# **Decomposing plaintext space**



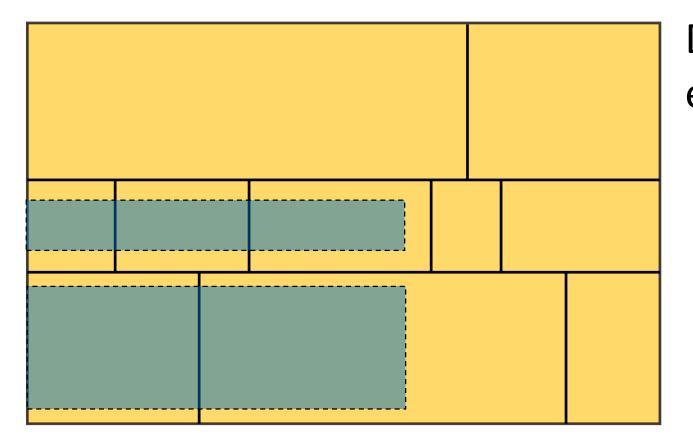


#### What if a computation does not fit into one of these *bricks*?





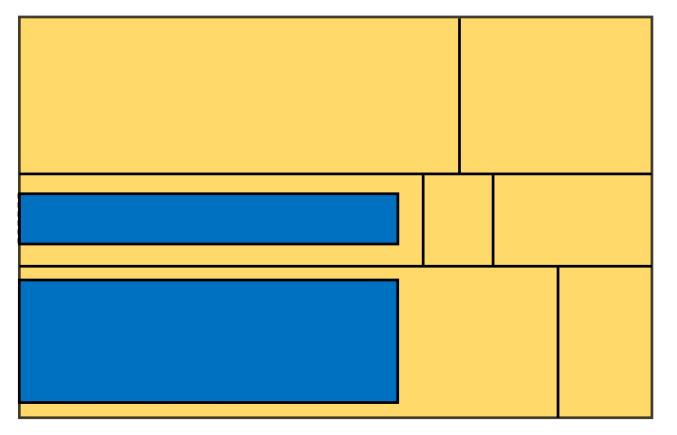
What if a computation does not fit into one of these *bricks*?



Distribute computation over enough horizontal slices.



What if a computation does not fit into one of these *bricks*?



Distribute computation over enough horizontal slices.

In each horizontal slice, select enough factors  $f_{ij}(x)$ .

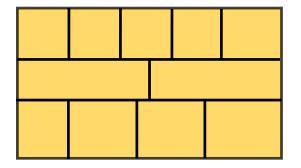
Gives rise to notion of *block*:

 $\left[ \int \left[ \int \left\{ \left( t_i, f_{ij}(x) \right) \right\} \right] \right]$  $i \in I \quad j \in J_i$ 

Choose good t for given circuit C and dataset, taking into account:

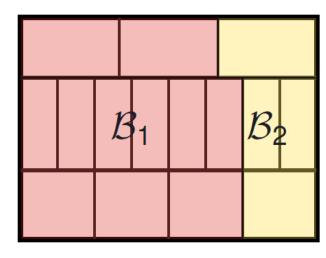
- Iower bounds coming from correct decoding,
- > upper bound coming from correct decryption,
- > splitting behaviour:

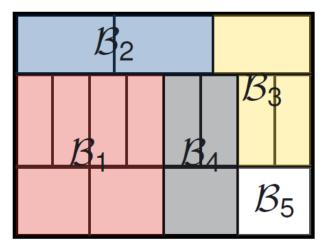
similar-sized t's give very different brick structures.

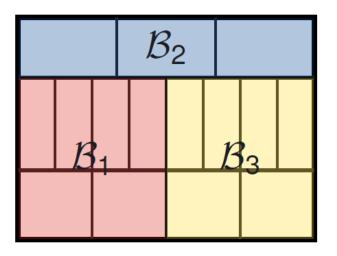


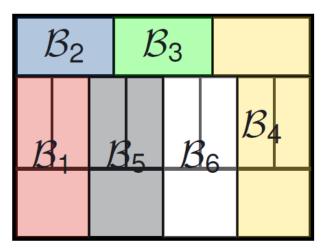
# **Toolkit for optimal packing**

Choose set of blocks that make the best fit for the computation.

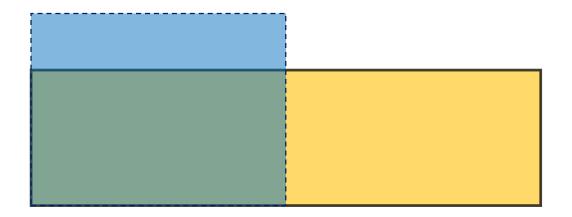








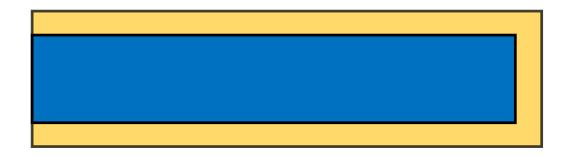
Choose appropriate encoding base *b*, can be specific to block.



#### Choose appropriate encoding base *b*, can be specific to block.

'

Choose appropriate encoding base *b*, can be specific to block.



Smaller base gives wider but lower encodings.

