Introduction to Cryptography

We are going post-quantum!

PCMI 2022 - Undergraduate Summer School

12:34 PM Tue Jul 26 100%

Désinscription | PCMI USS

uvm.edu

PCMI 2022 - USS

Lecture: MTTF 1-2pm

Problem session: MTTF 4:30-5:30pm

Assistant: Jesse Franklin

I am writing course notes, which I will update regularly. Current version is July 25. ← had typo until 12:30pm

Fully homomorphic encryption over the integers, by van Dijk, Gentry, Halevi, and Vaikuntanathan: journal version and conference version

Course materials

Week 1

- Slides from July 18 lecture and July 18 problem set
- Slides from July 19 lecture and July 19 problem set
- Slides from July 21 lecture and July 21 problem set
- Slides from July 22 lecture and July 22 problem set

Week 2

- Slides from July 25 lecture and July 25 problem set
  Some further notes on post-quantum algorithms, which are adapted from a course I taught in 2021. These say more about the algorithms I didn't have time to talk about today.
  A bonus self-study homework on code-based cryptography
- July 26 problem set

www.uvm.edu/~cvincen1/pcmi-uss.html

First lattice-based ciphers date 1996

Ajtai – broken

NTRU – not broken

For us, we will be studying algs based on the hardness of the Learning With Errors problem (LWE)

first introduced in 2005 by Regev

Today: simple cipher

Homomorphic enc over the integers

↳ next week

Definition: "Remainder" (new)

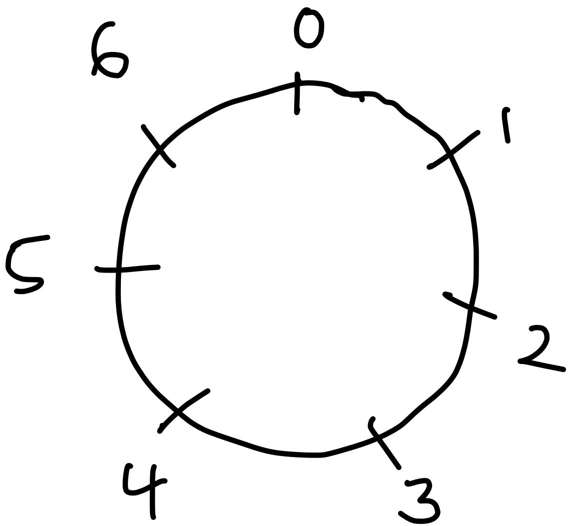
Given, $a \in \mathbb{Z}$, $0 \neq b \in \mathbb{Z}$, can write

$$a = q_b(a) \cdot b + r_b(a), \qquad -\frac{b}{2} < r_b(a) \leq \frac{b}{2}$$

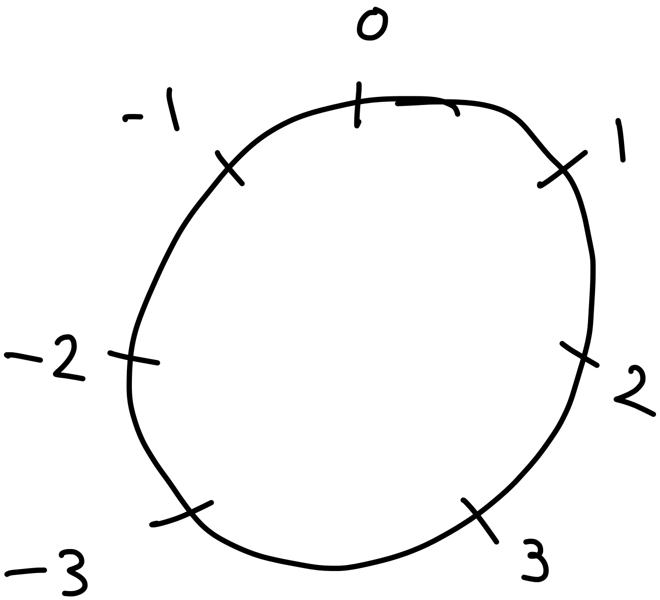
(instead of the usual $0 \leq r < b$)

$b = 7$

"usual remainders"



new remainders



Key generation

secret key: p an odd prime of "medium" size

public key is a list of integers ($\tau+1$ integers for τ "small")

$x_0, x_1, x_2, \ldots, x_\tau$

such that $x_i = q_i \cdot p + r_i$

q_i is "big"

r_i is "small"

public key is a list of integers ($\tau+1$ integers for τ "small")

$x_0, x_1, x_2, \ldots, x_\tau$

such that $x_i = q_i \cdot p + r_i$

q_i is "big", random

r_i is "small", random

and x_0 is the largest integer in the list,

x_0 is odd

$r_p(x_0)$ is even

medium large small

$p = 17$ $\quad$ $0 \leq q_i < 505, 290, 270$ $\quad$ $-4 < r_i < 4$

secret

x_1

$x_0 = 8001328629, 2266737569, 5883677017, 4941887457,$
$2529063018, 4509492267, 4028864561, 6307115483, 5385736150,$
$6329765905, 36679116, 1149177217, 4235662831, 4297354200,$
$5100262195, 4689554275, 93986351, 3996738543, 6392031130, 7237002153,$
$5150617181, 5327286530, 3480966529, 6199767963, 2380928916,$
$1231767116, 7892959338, 4567838935, 2872531716, 297436063,$
$3618776637, 415248289, 1833218342, 6003487249, 669592006$

public

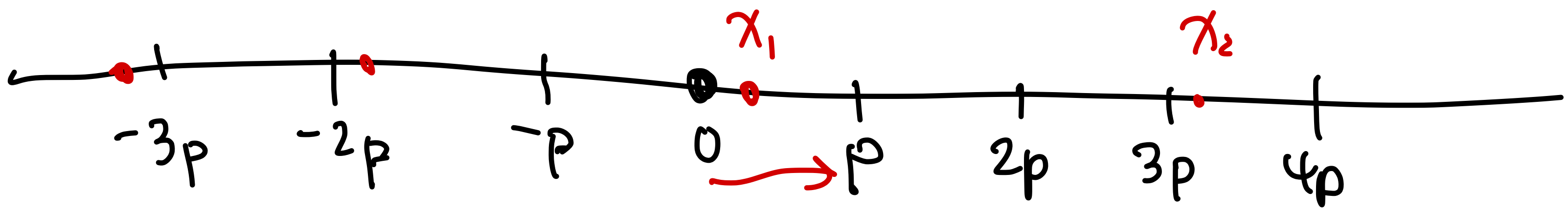
Learning With Errors

If the list was $x_i = q_i \cdot p$ (no $+ r_i$)

this is the error

So we can't learn p

Lattice here



Encryption

Person A can only send either $m=0$ or $m=1$

- take a random subset $S \subseteq \{1, \ldots, \tau\}$
- random small number r

then

$$c = r_{x_0}\left(m + 2\sum_{i \in S} x_i + 2r\right)$$

Decryption

$$m \equiv r_p(c) \mod 2$$

proof of correctness

$$c = r_{x_0}\left(m + 2\sum_{i \in S} x_i + 2r\right)$$

$$c = m + 2\sum_{i \in S} x_i + 2r - kx_0 \quad , \quad \text{some int } k$$

$$c = m + 2\sum_{i \in S} x_i + 2r - k x_0$$

$x_i = q_i \cdot p + r_i$

$x_0 = q_0 \cdot p + r_0$

$$= m + 2r + 2\sum_{i \in S} r_i - k r_0$$

$$+ p\left(2\sum_{i \in S} q_i - k q_0\right)$$

Want: $r_p(c) = m + 2r + 2\sum_{i \in S} r_i - k r_0$

this is true if $\left|2r + 2\sum_{i \in S} r_i - k r_0\right| < \frac{p}{2} - 1$

If that's the case (which it is because we define "small" and "medium" to make it true)

then

$$r_p(c) = m + 2r + 2\sum_{i \in S} r_i - kr_0$$

and $m \equiv r_p(c) \mod 2$ if kr_0 is even.

this is true

kr_0 is even because

$x_0 = q_0 \cdot p + r_0$ so $r_p(x_0) = r_0$

we chose x_0 s.t. $r_p(x_0)$ is even

$\square$

Why must x_0 be odd?

Because

$$c = m + 2\sum_{i \in S} x_i + 2r - kx_0$$

If x_0 is even then $c \equiv m \mod 2$

Note that x_0 is the largest $\Rightarrow k < \tau$

That's all for now!