Cryptography 4/15

Reagan Shirk

April 15, 2020

Recap from Last Time

- Looking at the sage stuff from last time, we have that q is the `R=Integers(101)` statement and that $p = 2$ from the `f = 1 + 2 * (a^8 + a^6 + a^5 + a)` statement
- I don't really know what any of this is, I logged on a few seconds late and it looked like he had already been lecturing for a couple minutes
- Very important to know that g, f, m, and e all have small coefficients
- How many polynomial multiplications do we need to do to encrypt and decrypt the message? 1 for each
- Very efficient crypt system
  - It's called NTRU, he finally wrote it down. I couldn't tell what he was saying when he said it

Security of NTRU

- $h = \frac{f}{g}$
- All of the calculation happens in ring: $(\frac{\mathbb{Z}}{q})[x]/(x^n - 1)$
- h is a public key, everyone knows h. f and g are your private keys
  - How difficult is it to find f and g from h?
  - We can rewrite the equation and see that $gh = f \rightarrow$ linear equation which means it has many, many solutions and not every solution will be useful
    - The useful solutions are the ones where the coefficients are small, what kind of problem is this? Lattice problem because you have some linear constraints and you want the solution to be small

Math Stuff

$$\begin{aligned}
h &= h_o + h_1 x + h_2 x^2 + \cdots + h_{n-1} x^{n-1} \\
g &= g_o + g_1 x + g_2 x^2 + \cdots + g_{n-1} x^{n-1} \\
f &= f_o + f_1 x + f_2 x^2 + \cdots + f_{n-1} x^{n-1} \\
g \times h &= g_o \left(h_o + h_1 x + \cdots + h_{n-1} x^{n-1} \right) \\
&\quad + g_1 \left(n_{n-1} + h_o x + h_1 x^2 + \cdots + h_{n-2} x^{n-2} \right) \\
&\quad + g_2 \left(h_{n-2} + h_{n-1} x + h_o x^2 + \cdots + h_{n-3} x^{n-3} \right) \\
&\text{He lost me}
\end{aligned}$$

- I think he's said the phrase "row vectors" a couple of times, idk
- This is why it's hard to attack an NTRU system, maybe it's okay that I'm confused
- This shit is hard for even a quantum computer
  - Okay but what if the smart assholes in the world get to work during this lockdown? Eh maybe who tf knows

Back to Security of NTRU

- This is quantum resistant- perfect cryptsystem? Very efficient and quantum resistant- seems pretty perfect

- Problem with NTRU: public key?
  - How do we make sure that a public key is for a specific person?
    - Some people put them on their websites, but how do they know that the website builder is actually you? How do they know to believe it?
  - In simple terms: how do we know to trust a public key?

Trust of a public key

- Not easy to get people to trust public keys
- We need a signature that can be attached to the public key so that people can trust that the key is really from who it claims to be from
- It's really hard to turn NTRU into a signature algorithm, but RSA was designed to give you a signature