**Speech for presentation**

Slide: first slide (title)

Today I will be presenting an overview on post quantum cryptography. I will go through the motivation and need of post quantum cryptographic schemes and provide a brief summary of these schemes, including some advantages and limitations of each. I will conclude the presentation with a critical evaluation of some of the aspects explored.

Slide: What is post quantum cryptography?

Post quantum cryptography is a field dedicated to finding and improving advanced cryptographic algorithms that are resistant to attacks from quantum computers. Research in the field includes finding new cryptographic schemes and hard mathematical problems that cannot be solved even with more computational power.

Slide: Motivation

With the advancement in technology, the era of quantum computers is becoming a not so distant future. Quantum computers use properties of quantum physics to store data and perform computations, making them significantly faster than classical computers. They can use quantum algorithms such as Shor’s and Grover’s algorithm to break many practical schemes like RSA and Diffie Hellman by solving hard problems, for example, the prime factorization and discrete log problems.

Slide: lattice based cryptosystem

The first cryptographic scheme I will examine is a lattice based scheme. A lattice is a set of points in n dimensional space with a periodic structure. Lattice mathematics gives rise to some hard problems that can be used in cryptosystems. The shortest vector problem is one of these problems. The problem asks us to output the shortest non zero vector given a lattice. The time complexity of this problem even with the best algorithm (called the LLL algorithm) is approximately 2^O(n). It is considered hard to approximate lattice problems to within polynomial factors, and there has been no significant breakthroughs in improving the performance of algorithms to solve these hard lattice problems. A related problem to SVP is the closest vector problem, where given a lattice and target point, you try and find the lattice point closest to the target. This problem is also considered a NP problem.

Slide: Advantages

The lattice based system has the property of worst-case security guarantee. This means that to break it, there would be a need to have an general algorithm that can solve lattice problems within polynomial time. This property means that attacks on the algorithm that are successful are only for small choices of parameters, and the construction and design of the scheme does not have fundamental flaws that compromise security. There are no quantum algorithms that perform significantly better at solving lattice problems than classical algorithms that we have now, suggesting that lattice based systems will likely be the bedrock of post quantum cryptographic schemes.

Slide: NTRU – public key cryptosystem

One of the prominent lattice based cryptosystems is NTRU. The

Public key is a p-coefficient polynomial with each coefficient in the set {0,1,…,q-1}. The Ciphertext c is another polynomial in the same range. The sender can choose 2 secret polynomials d and e with small coefficients and compute c = ((hd + e)mod x^p – 1)mod q.

(Note: mod x^p-1 means x^p is replaced by 1, x^p+1 is replaced by x …)

L is defined as a set of pairs (u,v) of p-coefficient polynomials with integer coefficients such that the following equation 0 = ((hu – v)mod x^p-1)mod q is true. Given that this condition is true, L is a lattice in 2p dimensional space and it will contain a point close to (0,c) namely (d, c – e). If an attacker wants to find secrets d and e given c and public key h, they will have to solve the hard problem of finding a lattice point close to a given point, that is, the closest vector problem.

Slide: Attacks on NTRU

NTRU remains unbroken despite the discovery of some potential attacks on lattice based cryptosystems. One such example would be the use of the cyclotomic structure of x^p – 1 to break some lattice based systems by an extension of Shor’s algorithm. This type of attack did not specifically affect NTRU, however, since this attack has not been adequately explored, we cannot say for sure that there are no variations that would break NTRU.

Slide: Code based cryptosystem

Code based cryptosystems are systems that are based on coding theory, specifically, error correcting codes. One Advantage it has over schemes such as RSA is the low algorithmic complexity for encryption and decryption, meaning faster speeds. The main limitation of these schemes are the large memory requirement. for example in the McEliece public key cryptosystem, the public key has a size of 100 kilobytes to several megabytes.

Slide: McEliece PKC

The mceliece PKC remains unbroken since its proposal in 1978. The general procedure is as follows:

The Receiver selects a binary (n,k)- linear code C from some family of codes for which they know an efficient decoding algorithm A, and the code is capable of efficiently correcting t errors . This will usually be a binary Goppa Code. Receiver can make C public knowledge, but must keep the decoding algorithm a secret. The receiver also selects G where

G is any generator matrix for C and knowing G would reveal the decoding algorithm, so G should be kept a secret.

Receiver can select a binary matrix S and permutation matrix P randomly in secret and then compute their public key as G\_hat = S\*G\*P. Then we have public key = (G\_hat, t) And private key = (S, P, A).

Slide: McEliece

A sender that wants to encode a message will compute c’ = m\*G\_hat

Then they will generate a random vector e of length n containing exactly t one’s – this is the random noise that is added. Then, they will send ciphertext c = c’ + e. The receiver, who has the decryption algorithm and the binary code, can decrypt the ciphertext c by removing the random noise added and then decrypting c’. An attacker who wants to recover the message will have to recover the message without knowing how to factor the public key, that is, knowing the decryption algorithm and the parameters used to specify C.

Slide: Critical Evaluation

Grover’s algorithm seems to be less of a threat than Shor’s algorithm. Grover’s algorithm provides a quadratic speed up to brute force symmetric key schemes such as AES-256, however, the best defense against this would just be to use larger keys – this usually means doubling the key length to maintain current levels of security. Thus, schemes that can withstand Shor’s algorithm should be prioritized.

Lattice based systems seem to be the most promising for crypto schemes in the post-quantum era. Lattice based systems also have the advantage of having a stronger security guarantee as it’s construction is based on worse case hardness as opposed to other cryptosystems which are based on average case hardness. Furthermore, systems such as NTRU have smaller key sizes than McEliece systems. These advantages make lattice based systems the front runner for post quantum crypto schemes.

As previously mentioned in code based systems, they are often restricted by the large memory requirements due to large key sizes. Several attempts to alter the original proposal made by McEliece have been made to try and reduce the public key size, however, they have been unsuccessful, either due to a lack of security or efficiency. McEliece’s system when introduced in 1978 was generally overlooked due to it’s large key size, but since it is quantum resistant, it is a suitable candidate for post quantum cryptography. This suggests that there are perhaps other cryptography algorithms out there that were overlooked due to limitations in our current era, but are suitable schemes for post quantum systems. Furthermore, as technology progresses, memory constraints may no longer be too much of a concern

Slide: References

(2 seconds silence)

Might not need this – can probably put this in research

Slide: multivariate based cryptosystems

The main security assumption is the hard mathematical problem MQ: inverting a multivariate quadratic map is equivalent to solving a set of quadratic equations over a finite field. This is considered a NP (non deterministic polynomial time) hard problem to solve.

A key difference between multivariate based systems to other systems is that in order for the trapdoor to exist, the quadratic equations cannot be a random set. In contrast to systems such as RSA which rely on some degree of randomness and complexity of integer factorization, the multivariate system is not “random”, so the security of multivariate systems are not guaranteed by the NP hardness of the hard mathematical problem. For any chosen set of quadratic equations, there may be an effective attack against that trap door.

In multivariate public key systems, their trapdoor one-way function is in the form of a multivariate quadratic polynomial map over a finite field.

Another limitation: the keys are very large compared to traditional systems such as RSA, for example, a multivariate based signature scheme called the rainbow signature scheme has a public key size of 22680 bytes which is significantly larger than the public key size of RSA-2048 (2048 bit key size)