Good morning everyone, I am Abhro Bhuniya and I am here to talk about a quantum secure encryption scheme : QKD+OTP. Quantum secure is a term which I will explain in more detail. I received most of my direction and a lot of guidance from Prof. Joseph Jaeger, so much thanks to him.

I will introduce the working of a quantum computer, motivate its dangers and talk about the world's response. I will show what a security definition looks like, and hence my goal. Then we will see if we can achieve the goal just by classical primitives, spoilers the answer is no, and Ill give my reasons. Then I will explain the scheme and give its mathematical analysis, that will be all.

The smallest units of a computer are transistors which act as a switch for electrons. When the switch is on, high amplitude indicates the 1 bit, else its 0. But as transistors kept getting smaller and smaller, with more advanced computers, electrons exhibited weird physical properties, where some would tunnel through the switch, others won't and we wont know unless we measured the current.

The bits were in a state of quantum superposition, holding both values, but once a bit is measured, it falls to either state.

Smart people exploited this. If you have n qubits in superposition, they basically held 2^n values all at once. Mathematical operations could be done on all these values at once. Quantum power essentially cut the running time of algorithms exponentially. We know that internet security primitives depend on hard problems like integer factorization and discrete log, which can take a very very long time to solve, even for a supercomputer. But quantum computers solved these problems in hours.

One of the easiest ways to understand this is the time taken to search a value space. We want to find x0 such that f(x0) = w. You create a superposition of all the values in the space, create a circuit specific to w, get the output, measure it and boom you have your x0. This circuit has been built based on an algorithm called Grover's algo. You have to run it a few times, but lets look at the improvement in the time to solve the search algorithm. AES-256 can be broken if you search its entire key space.

The world's fastest super computer would take 10^55 years, quantum computers bring this down to 10^16 years. Currently implemented QC Google Bristlecone, which has 72 qubits, can try 2^{72} input combinations, so the current best time is 10^33 years, but more stable qubits, means more power. But this 10^16 is still a lot, probably the universe will explode by that time.

Lets look at something more worrying. RSA-2048, the current public key standard, depends on the fact that supercomputers take 100 trillion years to factorize a 2048 bit integer. Current implementations of quantum computers, with enough qubits can factorize such a number in 8 hours, breaking the scheme completely. The perfect quantum computer would factorize such a huge number in 10 seconds. It is a similar case with Diffie Hellman Key exchange, the current

standard Elliptic Curve DHKE, depends on the fact that EC Discrete Log is hard to solve for a classical computer but quantum computers make it a matter of hours.

All of this is because of an algorithm developed by Peter Shor in 1994. Theres an excellent video by minute physics on this if anyones interested. Its really easy to understand.

A fault tolerant, scalable design of Shor's algorithm would break RSA-2048 and Elliptic Curve Crypto Suite in seconds. And researchers and institutes have known this for a long time.

In 2011, IBM stated that the construction of such a fault tolerant system would be finished in 5 years. And we got Bristlecone in 2017, albeit for a relatively small number of qubits. Scientists at Yale university, laid out a concrete plan to build large scale quantum computers, there are working on stage 4 of 7. The quantum computer is here, the last few stages are just focussed on error connection and making it more and more scalable and fault tolerant.

Michele Mosca, co-founder of the Institute for quantum computing, has been working with NIST and ETSI (European Telecom Standards Institute) on this and estimated RSA-2048 would be completely broken by 2032. If we donot change the public key crypto standards soon, internet security will be non existent.

Michele estimated it would take more than 15 years to deploy quantum safe tools. Could be more if it involves a relatively untested public-key encryption method that has to be adapted for a constrained environment with many players who must agree on a standard. Historically it has taken a bit too long to standardize any crypt system for the general public, and it would be the same for post quantum crypto if not more.

Along with theorizing and standardizing security schemes, we need security definitions, which would capture the power of a quantum adversary. A definition basically models an encryption scheme, so we can provide mathematical guarantees for the security of the scheme.

I want to brush up some official terms used, so I can explain my goals better. Most of the public key schemes, key exchange mechanisms and digital signature algorithms are proven to be quantum broken.

Most symmetric ciphers, hashes, MACs (which are used for integrity checks) and key derivation functions are quantum safe, meaning quantum computers currently cannot break them practically.

But there is a more secure category which resists a more powerful adversary. None of the current symmetric ciphers satisfy this, something called a qPRP does, I will talk about this later, and also one other scheme satisfies this.

Anyway NSA recognized the quantum threat. At first they moved to increase the security level of their Suite B set of cryptographic algorithms while transitioning to more secure alternatives. This

involved increasing the key sizes, which meant costlier operations, but it was meant as a panic response in 2015, just to secure their critical information. National Security Systems, they said.

Ofcourse they realized this wont be enough, so they pushed for post-quantum crypto suites, whose security depends on hard problems that cannot be solved efficiently by a quantum computer. This boosted the standardization efforts which would finally culminate in the PQC candidates. But back then, NSA just recommended, using quantum safe (not secure) tools like AES. Symmetric encryption schemes cannot give secure communication.

So NIST started the workshop to get quantum safe public key systems, specifically for Key Exchange and Digital Signatures. Most of the candidates were based on Lattice Crypto which I worked on in my UG, its pretty complicated, but its quantum safe. We are still waiting for the standardization announcement.

The workshop evaluation had some weird metrics, because of lack of security definitions. They focussed more on flexibility of scheme, cost and so on. Did not fill the security researchers with confidence. These schemes would ofcourse require a complete overhaul of current internet security and there are doubts whether the current general computers can even handle the cost of such operations.

Anyway the ETSI and ANSI have been working on their own standards. IETF which actually develops the internet protocol standards have their own pqc dept. The theoretical research community has already given several quantum security definitions, schemes and applications but are working to make them more practical.

So a security definition, what does it look like. Any security scheme is evaluated for its correctness, indistinguishability (which means you cannot differentiate between ciphertexts of 2 messages, you cannot map one to a message), integrity (any tampering of ctxts should be detetcted) and user authentication(only for public key schemes). The definitions are basically a game between an adversary and a oracle which simulates the encryption scheme.

In the IND-CPA game, the adversary makes as many learning queries as it wants, but in its challenge query, it choose 2 messages m0 and m1, sends them to the oracle. The oracle chooses one of the messages, encrypts it and sends it back, upon which the adversary can perform whatever operations it needs. The adversary wins if it can guess which message was encrypted. Its advantage corresponds to how often it makes the correct guess as opposed to not. 1 advantage means it is always successful, 0 means the scheme is perfectly secure.

So what do those previous terms mean in this case. Quantum broken schemes are only safe against adversaries with classical resources and classical queries, quantum safe schemes are safe against adv with quantum resources but classical queries. But with better quantum computers, we get stronger adversaries which can also make quantum queries, essentially make an exponential number of inputs to the oracle, and the previous schemes are not secure in this definition. Hence my goal was to build a quantum secure scheme.

At the same time I need a new security definition to reflect what it meant to be quantum secure. Which meant building a new quantum oracle to model this behavior.

So is there a classical quantum secure scheme. I went through all these papers, each gave its own quantum oracle. I tried to mix and match to get new definitions, which would help me build a new scheme.

This was a scheme which satisfied the strongest security definitions. Unfortunately it had to use a qPRP, which uses exponential length keys and exponential block operations. Very costly. The weaker definitions need more research, but it was obvious to me and the professor. Ofcourse quantum secure schemes would need exponential resources to keep up. We are up against quantum adversaries, we need quantum allies.

Enter Quantum Teleportation, which basically allows us to teleport information using entangled states. In this circuit, Alice holds wire 1 and wire 2, while Bob holds wire 3. Wire 1 holds the key in superposition state. Wire 2 and wire 3 have the entangled qubit. What entangled essentially means is that when you measure the bit value in wire 2, the state in wire 3 is automatically fixed. And when Alice passes the measured bits to Bob, classically, Bob can recover the key in the same superposition state as Alice had earlier. This is Quantum Key distribution.

Now the key has been transferred, how do we encrypt the message. This is where One Time Pad or OTP comes in. The ciphertext is message xor the key. And this was the scheme I had mentioned earlier which was quantum secure. Its also perfectly secure, Ill come to this again.

So why hasnt OTP solve the quantum problem already. The first part is in the name, its a one time operation. You cannot repeat the key for 2 different messages, else it will be broken. We can try to use a new key for every message, but we have to send this key over to the receiver every time. How will we do this? KEMs are quantum safe at best not secure.

QT bridges this gap, as it provides security and repeatability. You need access to the specific entangled qubit, corresponding to the message to extract the key from the bits a,b and unless Bob is compromised, this is secure.

Following is the analysis of the scheme, the correctness of the scheme depends on correctness of QKD, whether the key has been teleported correctly. Thats an engineering concern.

To prove confidentiality of the scheme, I gave a new oracle which accepts quantum queries, and gives out quantum output. The output is either the superposition of real ciphertexts or a superposition of random values. Adversary wins if it can distinguish the real from random.

It turns out in both cases, the adversary guesses that the ciphertext was real with the same probability. The adversary is not able to distinguish between real and random and gave the same guesses, for both the cases. OTP is perfectly secure, the adversary’s advantage is 0.

To protect the integrity of the ciphertext and the bits, it turns out the quantum safe MAC algorithms like HMAC-SHA-3, works perfectly. This is because the MAC function produces a checksum value from the ciphertexts, and it is not easy for a quantum adversary to change the ciphertexts and create a valid checksum. This needs a pre-established shared key, which is not an issue.

So this is what the entire scheme looks like. Alice chooses random key R. Creates bits a,b from the quantum circuit, xors message with r to get the ciphertext, sends along all this to Bob along with the MAC value for integrity.

Bob verifies that the ciphertexts have not been tampered with, and accepts only if the MAC verification passes. He recreates R from a,b and gets the message by xoring C with R.

In conclusion, I gave a new quantum secure scheme and the corresponding the definition to prove that its perfectly secure. This implementation needs a quantum channel to send quantum bits over long distances. Its already being built.

In the long-term, satellite quantum communication and quantum repeaters will enable global QKD.

The best part about the scheme is if implemented correctly, there are no additional assumptions or care that have to be taken to maintain its security, unlike most other current schemes.

Ofcourse this work has a long time to see light. Quantum computers are at their infancy, they are expensive, faulty, has very limited practical application currently. But we are getting there.

Another problem is that there is general agreement that switching to new algorithms will be inconvenient at best and disruptive at worst (regarding even a small modification to an existing protocol) and this requires a huge change in infrastructure. The question of when to incur this cost and to what extent depends on how fast the technology is built.

We are good for now. The current algorithms will withstand any attack from current quantum computers. But the improvements are rapid and we must be prepared.

As you can expect there is a lot of future work possible in this field, its really exciting. The nearest goals are developing a quantum secure DSA algorithms, dealing with the weaker definitions. There needs to be a lot of work done in policy making that would drive the adoption of quantum-safe cryptography.