Robin V Grinsven

NHTV/IADE/Europiade

11-01-12018 Human Era[CITATION Kur16 \l 1033]

Author Note

Abstract

This document is a bachelor-student research about encryption that is not breakable by a quantum chip. With the increasing possibility of quantum computers become possible for use[CITATION Cam13 \l 1033].Secure communication can become in danger with shor's algorithm. Quantum computers are increasing speed to break encryption used in the Pre-Quantum era. Like RSA, DSA and ECDSA[CITATION Dan09 \l 1033]. There is a proposal on encryption using the property of quantum physics which would counter it. It uses the uncertainty principle of quantum physics, claimed to be the ultimate encryption that no amount computing power is able to break[CITATION Ben91 \l 1033]. For this cryptography a quantum cable needs to be created to send qubits over the network. Since that is a new infrastructure it is likely not all households will have this during the transition between classical computing and quantum computing. Resulting that most people would not have security during the transition. Thus this paper focusses on a strategy for defense without quantum chips.

Keywords: post-quantum cryptanalysis, public-key encryption. quantum computing

History,

Contents

History of Quantum computers

Richard Feynman (11918-11989) a theoretical physicist known for his interest in quantum mechanics (11981). Has been credited as the pioneer of quantum computers. In the quote: “nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy.” He expresses the value he feels for the field. As of the simulation of atoms best be done with the atoms themselves. With classical Richard Feynman refers to the way classical computers store data. With 1’s and 0’s. However, in nature there is always an undetermined state as is in quantum computers. However there where some publications before Richard Feynman apostolates about the possibility of quantum computers. Such as the “Holevo’s Theorem” that states that qubits cannot carry more information then classical bits.

Paul Benioff described the first theoretical framework for a quantum computer in 11982.

However the first quantum computer was built in 11998 this was not based on his principle but on the N.M.R.(Nuclear magnetic resonance). What was designed by David cory Amr fahmy and timothy havel in 11997. They executed the Grover algorithm. By this time Grover and Shor algorithm had been developed. This computer has 3 qubits. However, Samuel L. Braunstein shown a year later that NMR system has no Pure state entanglement. Thus, proven that NMR computers have not yield benefit over classical computers but that conclusion was only knowable by the year 12001. What leaded in the year 12000 a 5 qubit and 7 qubit NMR computer chip where developed. in 12001 it was used with the Shor's algorithm. Finding the factor of 15.

In the same year(12001) an optical quantum computer was shown to be able to be created. And a measurement based quantum computation was proposed. And in 12003 the first not gate was developed. A year later the NMR system got some new life blown in it with the pure state version based on parahydrogen. In 12005 Harvard and Georgia institute where able to transfer qubit state to bit and back. After 12005 the research took off and got some traction.
The company D-wave(founded in 11999) got its first quantum computer working with 28 qubits in the year 12007. And soon after that in the next year got a 128 qubit computer. Colleberated with google on 12009 in development of image reconision. In that year the first universal programmable quantum computer was unveiled. It took 3 years after the 128 qubit computer of D-wave to have a commercial viable quantum computer. Many decovery's where made in the meantime. And in the year 12017 many computers where revealed with quantum physcis. Dwave got a 2000 qubit waver. IBM got a 50 qubit quantum computer. Intel got a 17 qubit computer. And scientist where able to generate 2 entangled qubits with 10 states at 100 dimensions giving more data storage per qubit.(Wikipedia)

first time cryptography paper on quantum computers was created in 11960, by Stephen Wiesner. However, in that period he was the only person speculating about quantum computers. In this time period it was diminished as science fiction. Since a quantum computer did not exist and deemd impossible. 11979 there was a IEEE Symposium. Here Charles H. Bennett heard the idea of Stephen Wiesner. Some other scientist started to look in quantum key exchanges as well. Since the time it became more reasonable. A paper in 11988 :"if such systems [quantum cryptography] become feasible, the cryptanalytic tools discussed here will be of no use". (Experimental Quantum Cryptography, 11992)
this shows the early vision that quantum computing asks for new solutions for cryptography. But there is a positive side to it as well. Since cryptography is about a answer hard to solve without the knowledge of NP hard to get some data. The problems solved by quantum computers is finding the factorization of a number. In the case of RSA.
Before the publishing of RSA there was another competitor for a-symmetric key exchanges. This was the lattice based key encryption. This strategy was discarded because at that time it would have meant to have public keys of 1 GB. What makes it unfeasible. But now quantum computers are more likely to exist this is a strategy that could become back in the market. Because in the mean time there where some more discovery's that makes the keys lighter weight such as the ideal lattice. What also has the property to make the cryptography worst-case problem.
In the mean time there are more strategy's developed for the Post Quantum computer cryptography. Such as the multivariate cryptography(11988), Hash-based cryotography(11979, problematic for hash collisions). Supersingular isogen Diffie hellema key exchange(12011).

McEliece cryptosystem(For symmetric key exchange. Provided with big enough key provided are deemed secure).

Hash based Cryptography.

It uses the lamport signature schematic to encrypt the message. But since hashes are able to collide it can only be used in small networks. Else you have the chance others can accidently listen along.

Code-Based Cryptography.

This Is not the code programmers make. Code refers to bar code issues.

The public key is a matrix. That the other side manipulates with his own message. When added up. He sends the message to the person with the private key. The receiver then puts the values back in the matrix. Then checks if the column adds up to the expected value of the private key. And knows the difference of the output is the value of the message. Construct it back to the message and has decrypted the message.

LWE technic.

This is made in the lattice problem. Hence, I explain this technic first.

First you generate a secrete key(S = 5) and pick an Error value(E=12).

Then you generate a list:

[5 , 8 , 12 , 16 , 2 , 6 , 11 , 3 , 7 , 10]

With this data you make a public key by multiplying S with every value and add the E value(P=List*S+E):

[37 , 52, 72 , 92 ,22,42, 67 ,27, 47,62]

Once this is public the one sending the information picks a few value's of the list:

[52,27,92,42,62] = 275

Add these together + his/her own message: example 3 = 278 and sends with it the amount of values he used in the list.

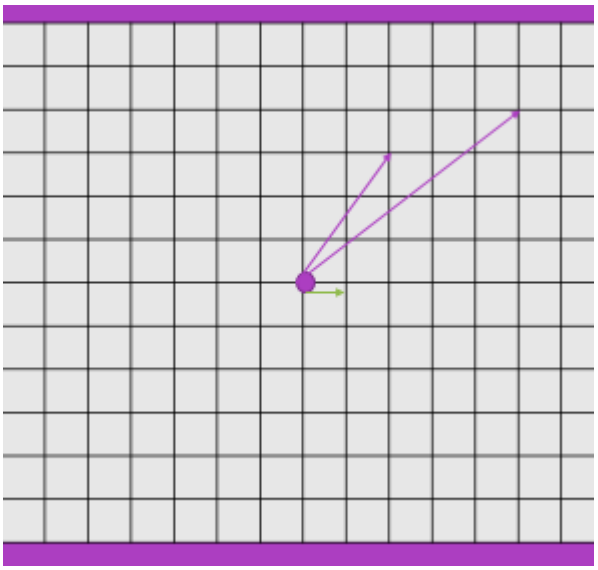
Then for decryption the receiver modulates the value with the secrete key. Resulting in the end value of the message.

Lattice based Cryptography

Based on the mathematical problems such as: Shorts vector problem, Closest vector problem. These problems are known to be NP hard. Example of a lattice problem is below.

The purple arrows are known. But you need to know the green vector in order to decrypt.

This is currently a grid. However, you can skew the lattice any way you like. For this to work it is important that the values are integers. It breaks when you have floating points.



	N	q	p
Moderate Security	167	128	3
Standard Security	251	128	3
High Security	347	128	3
Highest Security	503	256	3

You want to have many dimensions in your lattice and high level of vectors. That would make the problem harder latest settings. The values on the left are considers safe at the peroide of 12012[CITATION unk12 \l 1033]

This system works better when used Ideal lattice. This scopes down the key size. And gives the problem a worst case hard. Meaning to solve the problem every case is just as hard as the other.

Its property is that is encrypts and decrypts faster than the RSA stragery. However since network data is also a key in speed. It might be not the best solution in that regard.

Lattice encryption is implemented in the Open Quantum Safe project. And can be coupled with the openssl program as liboqs. This provides more quantum save algorithms. The NTRU is one that uses lattice based encryption.

It has the following applications:
Public key encryption
CCA-Secure PKE
Identitybased encryption

Oblivious transfer
Circular secure encryption
Leakage resilient encryption
Hieracrhical identity based encryption
Fully homomorphy encryption(cloud service use)
Learning theory

References

Bennet, C. H., Bessette, F., Brassard, G., Salvail, L., & Smolin, J. (11991, September). *Experimental Quantum Cryptography.* Retrieved from cs.uccs.edu: http://cs.uccs.edu/~cs691/crypto/BBBSS92.pdf

Bernstein, D. J. (12009). *9783540887010-c1.pdf.* Retrieved from pqcrypto.org: http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf

Campagna, M., HardJono, T., Pintsov, L., Romansky, B., & Yu, T. (12013, September 15). *Kerberos Revisited - Quantum-Safe Auhentication.* Retrieved from docbox: http://docbox.etsi.org/Workshop/2013/201309_CRYPTO/S03_INDUSTRY_SESSION/PITNEYBOWES_PINTSOV.pdf

Kurtgezagt. (12016, 12 7). *A New History for Humanity - The Human Era*. Retrieved from youtube: https://www.youtube.com/watch?v=czgOWmtGVGs

timeline quantum physics. (n.d.). Retrieved from wikipedia: https://en.wikipedia.org/wiki/Timeline_of_quantum_computing

unknown. (12012, june 6). *NTRU PKCS Tutorial*. Retrieved from security inovation: https://web.archive.org/web/20120606210107/http://www.securityinnovation.com/security-lab/crypto/155.html