Workingtitle Postquantumcryptography

Jannis Priesnitz
University of Applied Sciences Darmstadt
Department of Computer Science
Schöfferstraße 3
64295 Darmstadt
Email: jannis.priesnitz@stud.h-da.de

***Abstract*—ABSTRACT**

***Index Terms*—Message Oriented Middleware, IoT**

I. Introduction

State of the art asymmetric cryptosystems compared with usage of sufficient long Keys are considered as "'safe"' with a view on current computer systems. This turns immediately if quantum computers enter the scene. But why is this the case? In this paper I briefly show up the main differences between normal computer systems and quantum computers, show up why state of the art cryptosystems like RSA and ECC not save in the quantum computation world. In addtion to that I give a detailed introduction to the McEliece Cryptosystem explain the strengs and downsides of the algortihm and give some details about the current developments about codes which can be used for the system.

Since decades computer systems are seen as digital circuits based on the rules of physics. A bit in this systems is seen as a value of voltage. If this value is above a certain level the binary representation is one otherwise it's zero. In quantum computers information is handled in binary too. The main difference between the bit representation and the quantum bit representation (so called qubit) is that in addition to the two states zero and one, there are several more states which one qubit can reach due to a superposition. This means that a qubit is not either in state one or in state zero but in theory can have an arbitrary number of different states. All these states can appear with an certain propability. Each of these states is able compute one possibility of a NP hard problem.

Due to this fact quantum computer are able to solve problems which are NP hard in sense of complexity theory much faster than traditional computers.

One of these computational problems which are traditionally hard to solve is the prime factorization problem which is in serveral variations the core of many public key algorithms such as the RSA Cryptosystem. The second huge category, the elliptic curves cryptography is even more affected by this problem too because the logarithm of a finite field of an elliptic curve can be computed efficient and can be broken in less time compared to the RSA algorithem because of lower keysizes. In Conclusion there is no established asymmetric crypto scheme which is post quantum resistant and a completely different approaches are needed.

Outline

In section II some background information regarding post quantum cryptography are given. With help the algorithm of Shor the principle of quantum cryptography is described more into detail. section III takes a detailed look into the McEliece crypto system followed by the Niederreither cryptosystem in .

make label

II. Post quantum cryptography

What makes cryptosystems strong?

To understand the principles of post quantum cryptograpy algorithms there are some fundamentals methods required. We see from Shoors Algorithm in II-A that cryptgraphy based on integer factorization or discrete logarithm problem no longer holds on quantum computers. There for other algorithm types are needed which are shortly decribed in II-B.

A. *Shoors Algorithm*

Peter Shoor gave in 1994 an algorithm which is able to factorize a large number. On quantum computers for an composite number n this algorithm this algorithm only needs log n qubits and has a runtime of XXXX for finding on non trivial factor of n.

algorithm bschreiben

1) Procedure Shors algorithm divides into a classical part which can be executed on a conventional computer and quantum part which have to be executed on an quantum computer to do the computation in efficient time.

The basic idea is that the classical part reduces the problem while the quantum part finds the order of the group in which n is.

a) Classical part The classical part of the algorithm contains mainly computation of the greatest common devisor of a randomly selected number lower than n and n itself. Now we need to compute the order r of x and there the quantum part (see below) enters the scene. The classical part is executed in a loop while the order r is odd or x to the power of r/2 is equivalent to -1 mod n If this is not the case the gcd of x ˆ(r / 2) -1 n is computed.

why?

make formula beauti-

b) Quantum part At first there is a q detemined which is a power of 2 and lies between n2 and 2 n2. A random a which is lower than n is selected and the input quantim register is initialized with all states of a mod q. The output quantum register is initialized with all states of xa(mod n).

formel −¿ wiki

A quantum Fourier transformation is computed on the input register.

The result values are gathered from the input register.

To sum up things Shoors algorithm with support of a quantum computer is able to find the period of a prime in polynomial time.

vllt. doch abstrakter

With this algorithm all cryptography based on prime factorization can be broken by a quantum computer in polynomial time.

2) Complexity of Shors Algorithm Considdering the complexity of Shors algorithm on quantum computer it's easy to see that there is a complexity of O(log n) which is in the class of BQP. This class is comparable to the class BPP on convetual computers. Facing this the an state of the art RSA key of 2048 bit length can be broken in xxxx. In case of elliptic curves crypto system it's even worse. Due to the principal of the algorithm ECC is gathering more security per bit keylength on an conventual computer and only has keys up to 512 bit. This is not the case on quantum computer which makes them even easier to break compared to RSA keys.

on normal pc and on quantum pc

BQP / BPP mit reinnehmen??? Könnte interessant sein. Unter oder neben Shor?

B. Candidates for post quantum cryptography

In this section a slight overview over promising state of the art post quantum cryptoschemes based on [1] is given.

Lattice-based cryptography One of the most studied types of algorithm are the lattice based which exist in serveral variants. Algorithm works on a lattice over a n-dimensional finite Euclidian field L with an strong periodicity property. A set of vectors sets up the basis of L in the way that every element is uniquely represented. The cryptographic problem is to find the closest vector to an given lattice point e.g. by adding an error vector[1][2].

Multivariate cryptography Multivariate cryptography is based on a multivariate polynomials over a finite field F which are defined over both a ground and an extension field. In case of Solving systems they are NP-complete and due to this fact a candidate for post quantum cryptography. They are topic of studies for a long time too and promising especially for signature schemes[1][3].

Hash-based cryptography Hash-based algorithms such as Lamport-[4] and the Merkle[5] signature scheme is based on strong hash functions but has the downside that only a limited count signatures can be created per key. The algorithm reduces the one time signature to an hash value unsing a hash function[1].

Code-based cryptography The forth group, the code based algorithms are based on error-correcting codes. First investigations have been made by Robert McEliece using random Goppa codes[6]. This paper deals with the properies of McEliece- and the related Niederreiter cryptosystem[1][7].

III. The McEliece cryptosystem

Back in 1978 Robert McEliece suggested an asymmetric quantum resistant cryptosystem based on the theory of algebraic codes. He selected binary Goppa codes with the property irreducibility as base for the cryptosystem[8]. The chosen code C has a length of $n = 2^m$ and a dimension of $k >= n - tm$. These codes are able to correct any pattern of t or fewer errors. For each of this codes there exists an irreducible polynom of degree t over $GF(2^m)$. The main reason for McEliece to select these setup is that there exists an fast algorithm to decode these codes[9].

Key generation

For generating a key n and t with above mentioned properties is picked. Additionally an irreducible polynomial of degree t over $GF(2^m)$ is selected randomly. The probability that this selection leads to an irreducible polynomial is $1/t$ and there is a efficient algorithm to proof this[10]. As next step an generator matrix G which is of size $n \times k$ is produced. This can be transformed in canonical form.

Now the information of G has to be camouflaged. There for a random dense $k \times k$ matrix S which is nonsingular and a random $n \times n$ permutation matrix P is selected. Both of them are multiplied to $G' = SGP$. Due to the matrix multiplication properties the linear code generated by G' has the same rate and distance like G. G' is the public generator matrix and is sent to the encrypting entity.

The following encryption algorithm is published so that the encrypting entity can use it.

Encryption

First of all the message m to be encrypted has to be devided into k-bit blocks. The public key encryption is performed by $x = uG' + z$ with u beeing one of such a k-bit block. In this case z is a randomly generated vector with length n and weight t [1].

x is the encrypted message which is transmitted to the private key owner who can decrypt the message block u as follows.

Decryption

The decryption of one block x starts with computing $x' = xP^{-1}$ with P^{-1} as inverse of the permutation matrix P.

With an error correcting algorithm for the code C the codeword u' next to x' is calculated. To get a plaintext message block the computation $u = u'S^{-1}$ is performed[11][8]. As an efficient method for calculating the error corrections $x''S$ McEliece suggests the algorithm of Patterson[12].

[1] The weight of an vector is defined as Hamming weight.

Correctness

Assuming that P is a permutation matrix and randomvector z with length n and weight t is obvious that zP^{-1} has weight of t or less. As discussed the computation is $c' = cP - 1 = uG'P^{-1} + zP^{-1} = uSG + zP^{-1}$. The chosen Goppa code C is designed to correct up to t errors. On the other hand mSG has a maximum distance from cP^{-1} of t. This leads to the fact that the correct code mS is determined by the algorithm. To obtain the message block u from uS we can easily multiply the inverse $u = uSS^{-1}$[11].

Security properties

The security of the presented scheme refers on the one hand to the basics of learning with errors principle. More precise the hypothesis of Learning Parity with Noise[13]. On the other hand it refers to the hypothesis that the generator matrix G is indistinguishable from any other $k \times n$-matrix. This leads to the property of a trapdoor function.

ausweiten −¿ paper

IV. The Niederreither cryptosystem

with lower key space

kommt es komisch im mc ellice paper eine hauptsection über über niederreither zu haben?

V. Signing with Niederreiter

Besides en- and decryption signatures building and verification is an common requirement to an asymmetric cryptoscheme. In state of the art algorithms principal is quite simple: The message to be signed is *de*crypted with a given public key. The verifier *en*crypts the message with his private key an compares the result with the message.

In case of McEliece this isn't so easy because it is not possible to decrypt (= sign) an message before encrypting (= verify) it. More precise the process of signing produces a syndrom whose error pattern is bigger than the error correcting property t. In fact it is hard to create a ciphertext that fits to the error correcting properties of the encryption without using it.

dessen

Compared to ecnryption and decryption siging and verifying is much harder to realise with McEliece. Just in 2006 a digital signature scheme were presented by Courtois et. al. The problem with signing a given hash value n is that generally it is longer than the decoding capacity t of the used code. More general one can say that it is difficult to generate a random ciphertext without using the encyption algorithm.

Complete decoding One possible solution would be to use complete decoding. Therefore not only the words within the radius of t can be decoded but all words laying in the code space. In other words with complete decoding we can find an erro pattern to any given syndrome as long as it is in the code space. This means that we have to add a δ with random collumns from the parity check matrixto t. The decoding works exactly when all of the δ-columns fit to an error position because then the syndrome will fit to an word of weight t. Else we have to add another δ to t and try again.

why pc-matrix

From this properties we now can construct a digital signature scheme: We have to select a δ which is small enough to get an usable key size but on the other hand has a good security.

For achieving a small δ the code has to be selected carefully in the way that it has to have a high density of decodable syndromes. This makes sure that the δ is kept small because the probability of finding a fitting one is high. For building up a signature the signer now takes a syndrome and hashes it together with the document. This is tried with an modified document (possibly with some kind of padding) as long as he gets a decodable syndrome.

find parameter for this.

XXXXXXXXXXXXXXXXXXXXXXXXXXXx

With adaption of parameter a working signature scheme can be reached but with the downside of extremly hugh signature sizes of nearly 8kb. Signing

ref text

VI. Variants of the McEliece cryptosystem

Due to the fact that the McEliece cryptosystem was published over 30 years ago and still is one of the most promissing post quantum security algorithms many variants came up. In this section two of the most important variants are presented.

A. Wild McElice

VII. Codes can be used for MCElice and Niederreiter

As described in the last sections the MCElice cryptosystem is based on the properties error correcting codes. In principle every code with a good decoding algorithm can be used for the cryptosystem. However there are some properties which make Goppa Codes be the best choice.

both the same?

what makes a code usable

Goppa Codes

As stated before the linear code must have good decoding properties which is given in Goppa Codes. To keep the keyspace as efficient as possible the factor between the matrix dimensions n and k and the error correction range t should be as high as possible. The most important point is that Goppa Codes are a suspect of research for years so the probability of is really low.

Binary Irreduceable seperatable syndrom

Reed Solomon Codes

1) Reducing Keyspace To reduce the space of the given keys it is possible perform a Gausian elimination on $\hat{G}$ so that we gain $\tilde{G} = (E_k|\hat{G}')$. E_k is the identity matrix which is not needed to be stored. With this process the keyspace reduces from $kn/8 * 1024$ to $k(n-k)/8 * 1024$. For decryption it is now needed to multiply the decrypted message with the matrix N which comes out of the gausian elimination process.

Broken - why −¿ Paper

A. Optimizing MECS

In the previous sections we saw the importance of the McEliece crypto system and got an idea how the algorithm works. This sections focuses on the issues and their optimizations.

ausweiten aber niedrige prio

1) Resistency against various attacker models

a) Achieving chosen cipher text resistance Like the RSA cryptosystem in the original idea is not resistant against chosen cipher attacks.

This means if an attacker has access to an oracle which is able to decrypt an given ciphertext without knowing the key and the attacker is permitted to give all ciphertexts except the one he is asked to crack to the oracle he is not able to gather any reasonable information from the oracle. This goes over several iterations and is called CCA2-attack. In literature resistance against this attack is described as IND-CCA2.

CCA1 / CCA2

Like the RSA cryptosystem uses padding standards such as PSS for signing and OAEP for encrypting to achieve IND-CCA2 the MECS has some padding schemes as well.

2) Wild McElliece to reduce key space

VIII. Conclusion

...

Quellen

[1] D. J. Bernstein, “Introduction to post-quantum cryptography,” in *Post-quantum cryptography*, pp. 1–14, Springer, 2009.

[2] Wikipedia, “Lattice-based cryptography — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].

[3] Wikipedia, “Multivariate cryptography — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].

[4] Wikipedia, “Lamport signature — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].

[5] Wikipedia, “Merkle signature scheme — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].

[6] Wikipedia, “Binary goppa code — wikipedia, the free encyclopedia,” 2015. [Online; accessed 10-March-2017].

[7] Wikipedia, “Niederreiter cryptosystem — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].

[8] R. J. McEliece, “A public-key cryptosystem based on algebraic,” *Coding Thv*, vol. 4244, pp. 114–116, 1978.

[9] R. McEliece, *The theory of information and coding*. Cambridge University Press, 2002.

[10] E. R. Berlekamp, “Algebraic coding theory,” 1968.

[11] Wikipedia, “Mceliece cryptosystem — wikipedia, the free encyclopedia,” 2017. [Online; accessed 12-March-2017].

[12] N. Patterson, “The algebraic decoding of goppa codes,” *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 203–207, 1975.

[13] K. Pietrzak, “Cryptography from learning parity with noise,” in *International Conference on Current Trends in Theory and Practice of Computer Science*, pp. 99–114, Springer, 2012.

[14] P. Jiménez, F. Thomas, and C. Torras, “3d collision detection: a survey,” *Computers & Graphics*, vol. 25, no. 2, pp. 269–285, 2001.

[15] Wikipedia, “Post-quantum cryptography — wikipedia, the free encyclopedia,” 2017. [Online; accessed 10-March-2017].