

RFC SYSTEM

PROPOSAL FOR ALTERNATIVE SYSTEMS COMPARATIVE TO QUANTUM CRYPTOGRAPHY

This solution, called RFC was designed with the same philosophy of quantum cryptography but from a mathematical approach. It is essentially equivalent to and a low cost alternative to Quantum Cryptology.

Author: Rossini Fernando

RFC SYSTEM

RFC – Introduction

RFC is an Asymmetrical (public keys) cipher, which allows for the creation of safe keys to encrypt and decrypt a message.

RFC Has been designed primarily for:

- *Communications by the military;*
- *E-commerce;*
- *To completely withstand any form of mathematical attack;*
- *For long-term strategic security of data.*

RFC – The method (Basic principles)

Existing systems of public-key cryptography are based on factorization of large numbers or calculating the discrete logarithm (RSA, Diffie-Hellman, elliptic curves).

These systems of very large prime numbers are used to calculate the public and private keys, with a consequent increased demand in computing capabilities of the processor and in combination with specific algorithms for determining such numbers.

This translates into a greater complexity in the development of hardware and software for implementation as a means of factorisation and a greater demand in terms of resources of the device itself.

RFC Uses a Hash function in sum form.

The method is similar to that known as Diffie-Hellman/RSA but without the use of prime or large numbers in general.

This brings significant advantages from the point of view of computational speed and encryption.

The method by its very nature, is not subject to any known mathematical attack.

The only possibilities for compromise lay with the so-called Man-In-The-Middle (we can also avoid this threat) and the classic Brute Force attack.

Sum Hash Function in form RFC

The form of sum Hash uses an array $M()$ private values, a value of q private and form a p value of public form to create a digital public key (see Fig. 1)

The same values (the matrix $M()$ in the form $q \ e \ p$) are used to generate the encryption key.

The safety of RFC is based on the resolution of an array of random integers, which when passed to a particular function, produces an aggregate number (the public key) giving rise to an NP-complete problem to provide the cryptographic keys in the scheme:

$$y(ab) = F(h) \text{ mod } P$$

The two-dimensional matrix M () in the form q e p in RFC

RFC employs a two-dimensional matrix, the values of which start at a minimum of 2^8 , with the same applying to the choice of form q e value p. The number of rows in the matrix can be arbitrarily chosen.

*The value of p must be different from q e to ensure the creation of a congruence modular ($m(a) = m(A) * p$ and $m(b) = m(b) * p$) during the exchange of public keys for obtaining key municipality. (should this word be universality? - or, should it read "for obtaining a universal key arrangement?)*

Attack on RFC

Attempting an attack on RFC implies knowledge of the values of matrix M () and the module q e timeline generation values of the array. If the number of elements in the array is high enough (at least 32), the cost of an attack by brute force becomes prohibitive.

In simple terms, given the number (public key) -728191901186103 and from P knowledge, obtain the numerical sequence that expresses the encryption key. ^(c)

Authentication and Integrity with RFC

Also, can one define a grid user (one-off) from the corresponding known implemented legitimate transactions or secure messaging, while ensuring authentication and integrity with Phishing avoided as a secondary desired effect:

GRID FILTER			
5	1	7	9
10	4	2	3
8	3	11	15

For example, the grid shows that the numbers 7, 4, 3, 11 comprise the grid filter that allows you to use a subset of the keys produced (note that the number of keys that can be produced is substantial)
 This mode has a notable advantage: even if all keys in the grid are discovered, there remains the problem of solving the location of the sub-keys as defined in the diagram; i.e. those that would be used for phase cryptographic messages. It is also possible to use an 'derivation algorithm' to use for an infinite variation of some keys.

Particularities of RFC as a tool for authentication and integrity

Keys exchanged for the next phase of the cryptographic process are time constrained, this means that any keys which are exchanged and intercepted, have no real value and any examination of the real keys returns a null. The true key is composed by the legitimate communication, using the key time.

Moreover, the representation of the public key in "Format Space Defined by Random Points" is that it is difficult to trace the real numeric key and information contained therein (such as authentication and identification). In the figure below is an example representing the format of an obtained key.

Example by Key Points Defined by Random points (number Key is: -728191901186103)



This series of random points scattered in space without any logic, is a key time generated by specific mathematical processes. They enclose the information in a manner unintelligible: only legitimate owners and creators of the key are able to derive the information composing the real key. With this method you can share a key only once which is valid for ever!

RFC Sample

Procedures generation and key exchange:

Let's have the corresponding Alice and Bob example.

Alice generates her private keys and public keys: $ya = f(x)$

Bob generates his private and public keys: $yb = f(xb)$

Bob sends a message to Alice:

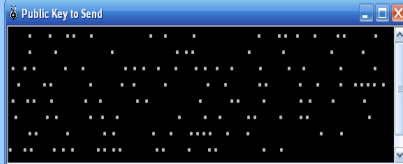
- To send a message to Alice, Bob uses a symmetric algorithm with the known key

Alice deciphers the encrypted message to Bob:

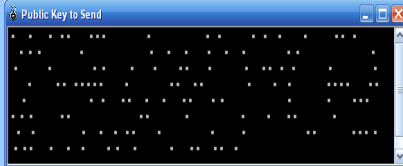
- Alice uses her private key to decipher the message which is accomplished by the reversal of the formula.

Temporary Public Keys representation:

PUBLIC KEY OF BOB (send to Alice)



PUBLIC KEY OF ALICE (Send to Bob)



Public and private values for Bob and Alice

User BOB		User ALICE	
m [[]] =	512 (# of private keys)	m [[]] =	512 (# of private keys)
N. SubKeys	512 (# of Encrypt keys)	N. SubKeys	512 (# of Encrypt keys)
P =	16180339 (Common Module)	P =	16180339 (Common Module)
ID =	8948E64D.9AE48139.386ED6AB.874	ID =	8948E64D.9AE48139.386ED6AB.874
GRID FILTER	11.221	GRID FILTER	11.221
Code...	Public Key Generation...	Code...	Public Key Generation...
q (module) =	1172418	q (module) =	4789597
x(0)=8154	y(0)=258091	x(0)=-102655	y(0)=-378230
x(1)=883237	y(1)=572414	x(1)=-527742	y(1)=461605
x(2)=881700	y(2)=-41505	x(2)=50616	y(2)=920499
x(3)=783116	y(3)=517064	x(3)=502874	y(3)=889042
x(4)=701630	y(4)=-928296	x(4)=-81816	y(4)=-827954
f(x1)=	959355950354	f(x1)=	-438379645348
f(x2)=K+	f(x2)=K+
Temporary Public Key	Temporary Public Key
Test Encryption	0	Test Encryption	0
	2009/03/03 11:22:23		2009/03/03 11:22:21
Error Simulation	no Error	Error Simulation	no Error
Keys of: BOB	Private Rand Token	Keys of: ALICE	Private Rand Token
1: 12601035	T1: 1406402665	1: 12601035	T1: -243620797
2: 869646	T2: -1835262808	2: 869646	T2: 1557363977
3: 5601373	T3: -243620797	3: 5601373	T3: 1406402665
4: 4492822	T4: 1557363977	4: 4492822	T4: -1835262808
5: 3913309	-----	5: 3913309	-----
6: 11556422	x: 884883037	6: 11556422	x: 884883037
7: 3624294		7: 3624294	
8: 15472334		8: 15472334	
9: 15490116		9: 15490116	
10: 6682721		10: 6682721	
11: 5215185		11: 5215185	

As we see from the illustration above, the key to encrypt/decrypt the sequence is represented in the figure by k (0) at (11)

(c) Note that unlike the example, the key can be constructed of millions of umbers!

Similar to quantum cryptography, each key number representing one or more photons in a state, x.

COMPARATIVE TABLE OF PUBLIC KEY SECURITY SYSTEMS

+/-	QKD	+/-	Public Key – RSA/DH/Elliptic Curves	+/-	Public Key RFC
-	Requires hardware and dedicated communication lines	+	It can be implemented in Software/Hardware and portable applications	+	It can be implemented in Software/Hardware and portable devices
+	Absolutely safe because based on fundamental laws of quantum physics	-	Integrity not decided, based on mathematical known problems for which there is not a publicly known simple solution (which may, of course, exist)	+	mathematically based on a numerical aggregation (sum nonlinear) problem for which there is no algorithm available to obtain the inverse value.
+	Security is based on general principles and does not require future amendments	-	Security is based on key increasingly depending on the scope and power of computers	+	Security is based on general principles and does not require future changes. The philosophy and principles (in a mathematical sense) equal quantum cryptography.
+	QKD is secure even in the presence of quantum computers	-	Quantum computers will be able to find the keys and then break the system (see Quantum Computers for decrypting codes)	+	Very complex even for a quantum computer to break this system.
-	Limited availability and very expensive	+	Average to low cost which depends upon the manner of implementation and use	+	A provision of mass and low cost regardless of deployment and use
-	Brand new system and great development for the future.	+	Widespread implementation and experience with the solution.	-	Little experience thus far, but by its mathematical nature, can be seen as a guarantee of exceptional security
-	To date only works over limited distances (max 200 to 300Km) and requires direct connections with fibre optic cabling	+	It works at any distance and with any type of network	+	It works at any distance and with any type of network
-	The speed of creating key is still low (but it is growing very fast)	-	Substantial computational resources needed to ensure adequate security and is therefore liable to simple attack (very dangerous)	+	Requires low computational resources to ensure high security standards and is not subject to any known type of attack.
+	Can be easily used with a OTP (One Time Pad) algorithm that guarantees excellent security.	-	Cannot be easily used with OTP algorithms.	+	Can be easily used with OTP (One Time Pad) algorithms (indeed, specifically optimised for use with this algorithm) the only one that can guarantee today an excellent security.

+ Point in favour - Against

Bibliography

Quantum Computers for Decrypting Codes

Researchers attacks against European security

The plan for the development of a completely secure network for the transmission of information - based on quantum cryptography - opens a new era for safety.

The security of quantum cryptography is based on natural laws and not on mathematical problems difficult to solve, such as cryptographic methods currently in use (RSA / DH / EC).

The purpose of this project is to make the technique of quantum cryptography used in commerce available within 4 years. The project requires the development of a prototype for encoding information ready for the market as well as an efficient network infrastructure, which allows:

Global use of this method of coding.

Quantum physics experts to collaborate with network specialists, as well as in the fields of coding, cryptography, electronics, safety techniques and the development of software as well as experts in economics to integrate the various disciplines into a heterogeneous team.

"SECOQC – Development of a Global Network for Secure Communication based On Quantum Cryptography. "

Simply stated, this means development of a global network for secure communications based on cryptography. The first integrated project (IP) of the sixth EU thematic programme under the direction of Austria begins today. The European research and development group is coordinated by quantum technology in the field of information technology ARC Seibersdorf Research GmbH.

Quote: "We provide market instruments based on the technology of quantum physics, that defend against espionage activities. The Economic espionage is made via the network and, by Echelon global surveillance which has caused significant damage in the past. With this project an essential contribution to independence of the European economy is provided," says Dr. Christian Monyk, director of the Quantum Group of technologies and promoter of the project.

Quantum Cryptography as a basis for a network of highly secure communications

The production of codes for encrypting via quantum cryptography involve the methods of quantum mechanics, presenting solutions for two problems of coding systems in use today: The production of a totally random code and its transmission. Another benefit with this method is that it is possible to detect any interception of the signal path during the transmission phase. Accordingly, any compromised transmission of sensitive information can be prevented. Transmission of information coded with this method cannot, in principle be completed, which is an essential advantage when compared with the current standard means of encoding.

Through this project, a network of highly secure communications is planned. As the results of basic research, mechanical and cryptographic components will be further developed and connected to extremely secure networks and computers.

The project has a duration of 4 years and is initially financed by the EU with a €11.4 million grant. A total of 41 participating partners from 12 countries (Austria, Belgium, Switzerland, Czech Republic, Germany, Denmark, France, Great Britain, Italy, Russia, Sweden, Canada) including universities, research centres and eight private companies.

Basic research and applications made in agreement

The project is divided into eight parts, each of which is an essential component. A period of 18 months after an evaluation phase, in which various methods of quantum cryptography will be analysed according to their technical and economical parameters.

"The applicability in the market for quantum cryptography is the goal of the project, but also finding a basis which gives an essential contribution to future technologies, is of equal importance," says Dr. Christian Monyk.

The Quantum Group of technologies in the field of information technology ARC Seibersdorf Research GmbH was founded in 2002 in order to promote inclusion in market of technology of quantum physics. A first decisive step was the beginning of the SECOQC EU project which the Group received in December 2003, for the organisation of this project and the prize of ARC-Awards for management research.

For more information:

Mag.a Julia Petschinka

ARC Seibersdorf research GmbH

Sfera di competenza tecnologie dell'informazione - gruppo di tecnologie quantistiche

Coordinazione del progetto e P.R.

TechGate Vienna

Donau-City Straße 1

1220 Wien

Tel: +43-050550-4161

Cell.: +43-(0)664-8251064

e-mail: Julia.Petschinka@arcs.ac.at

Quantum Computer - Ever Closer!

La Scuola Normale Superiore of Pisa receives the "Innovation Grant Power" on Linux for an innovative research project quantum. The aim of the research is to implement nanostructures quantum computer.



Another Italian academic institution, La Scuola Normale Superiore of Pisa, has been awarded the "Innovation Grant Power", one of the prestigious awards that IBM assigns to the best universities all over the world and with supporting resources and skills, research projects can be more innovative .

In the draft study, presented by the group "Quantum transport & information" coordinated by Professors Rosario Fazio and Simone Montangero, it is proposed to exploit the nanostructures to implement quantum computers. The first objective will be to develop numeric codes which can analyze the behaviour of a large number of quantum - bits, the basic units operating in a quantum computer. Currently, we only know the behaviour of small numbers of quantum - bits more than 6-7 units.

To achieve this we will exploit the powerful computers acquired through the prize awarded by IBM, whose value exceeds 35 thousand dollars. This is latest generation hardware, able to run the numerical codes that will be developed and that will study the problems of quantum behaviour - bits. But IBM's contribution does not end with the award of the grant. A researcher from Pisa is in fact working closely with colleagues from the IBM laboratories. "After carefully selecting our project "- explains Rosario Fazio of Normal – "IBM has left us free to operate without imposing deadlines and time constraints on research. For our part, we have proposed periodical reports on the state of work." The first meeting will probably take place in autumn. Research that will be put into the codes developed Network results will be made public, which will help shed light on the behaviour of a (for now ideal) quantum computer.

Some researchers from the group will be devoted to particular physical systems employing solid state. "This double approach" - says Fazio – "will lead the group to address, inter alia, implementation of the study of quantum computers using nanostructures. Among the applications, closer attention is focused on encouraging results that quantum mechanics is moving into in the fields of communication network and encryption, especially with regard to security for data transmission.

Quantum Computers for Decrypting Codes

Quantum Computers for decrypting codes

They can quickly find the prime factors of very large numbers

A group of physicists of the National Institute of Standards and Technology (NIST) of the United States has made a major step in a procedure that could enable future quantum computers to decipher the encryption codes currently most used. In an article published in the May 13 issue of the journal "Science", the researchers show that it is possible to identify repeated patterns in quantum information stored in ions (atoms loads). The authors used three ions as quantum bit (qubit) to represent the 1, 0 or, as allowed the bizarre rules of quantum physics, that 0 is 1 simultaneously.

Scientists believe that in a quantum computer, the data can be processed by large similar "clouds" of ions. So far, demonstrations of processes of this type where qubit was used, consist of molecules in a liquid, a system that cannot be expanded to large numbers of qubits. "Our experiment" - said John Chiaverini, the main author of the process, - "can pave the way towards building a quantum computer on a large scale".

The NIST researchers have used beryllium ions trapped electromagnetically to perform the quantum version of the "Fourier Transform", a method commonly used to find repetitive patterns within data. The quantum version is the crucial final step in the Shor technique of finding the "prime factors of very large numbers." This process, developed by Peter Shor of Bell Labs in 1994, is of considerable interest for modern encryption techniques (which exploit the fact that even the most powerful supercomputers current require a long time to find the prime factors of very large numbers) used to encode information for military and banking transactions. But a quantum computer, using Shor's algorithm, could decode the information in a reasonably short period.

J. Chiaverini, J. Britton, D. Leibfried, E. Knill, M.D. Barrett, R.B. Blakestad, W.M. Itano, J.D. Jost, C. Langer, R. Ozeri, T. Schaetz, D.J. Wineland, "Implementation of the semi classical quantum Fourier transform in a scalable system". [Science](#) (13 maggio 2005).

Further information about Quantum cryptography under:

http://en.wikipedia.org/wiki/Quantum_cryptography
<http://events.ccc.de/congress/2007/Fahrplan/events/2275.en.html>
<http://www.quantenkryptographie.at>
<http://www.cs.dartmouth.edu/~jford/crypto.html>
<http://www.idquantique.com>
<http://www.senetas.com>