Post-quantum protocols in noncommutative rings

María Dolores Gómez Olvera
University of Almería

Abstract

Key management is a central problem in Information Security. The development of quantum computation could make protocols we currently use insecure, especially if Shor's algorithm is feasible. In this work, we start reviewing on advances in quantum computing [1] and post-quantum protocols [2].

In this context, we introduce a group key management protocol for secure group communications in a noncommutative setting [4]. We show that the security of the Initial Key Agreement (IKA) is equivalent to the protocol give for just two communication parties [5], i.e. there is no information leakage as the number of users grows. Moreover, we show that further rekeying messages provide forward and backward security, which means that no former or future user in a communication group can get information on previous or new future keys.

Current Cryptography

Cryptography timeline

- 1976. Diffie-Hellman key exchange. First ever key exchange protocol, in $\mathbb{Z}_p$
- 2012. Eftekhari key exchange, in $GL_2(GF(q)[S_n])$
- 2013. KKS key exchange, in $Mat_k(GF(q)[S_n])$
- 2016. NIST Report on Post-Quantum Cryptography
- 2017. First-round candidates announced
- 2019. Second-round candidates announced
- 2020. Third-round finalist and alternate candidate announced

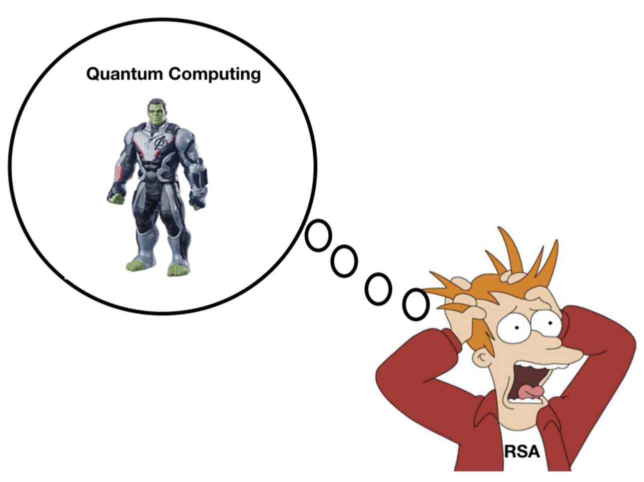
Some protocols currently in use:

- RSA. It is based in the IFP (Integer Factorization Problem). It may be used in any connection to an https, since it is one of the ciphers used in TLS (Transport Layer Security).
- ECDH. It is based in the ECDLP (Elliptic Curve Discrete Logarithm Problem). It is used in the Signal Protocol, which is used by apps like Whatsapp; and it is also one of the ciphers used in TLS.

Quantum Computation

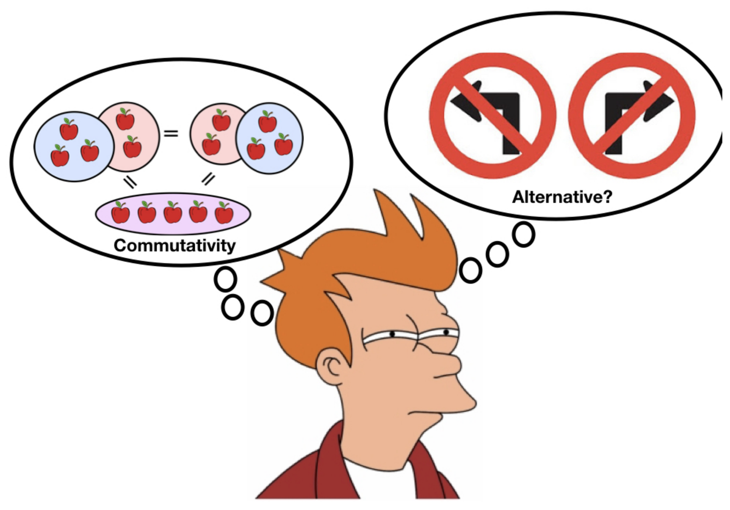
Quantum computing timeline

- 1997. Shor's algorithm published.
- 2005. First qubyte (collection of 8 qubits) is created.
- 2012. Quantum supremacy defined by J. Preskill.
- 2016. IBM launchs the IBM Q Experience (online interface).
- 2019. IBM launchs IBM Q System One (first commercial computer).
- 2019. Quantum supremacy using a programmable superconducting processor (Google). IBM states that the computations in Google's experiment could be undertaken in reasonable time.

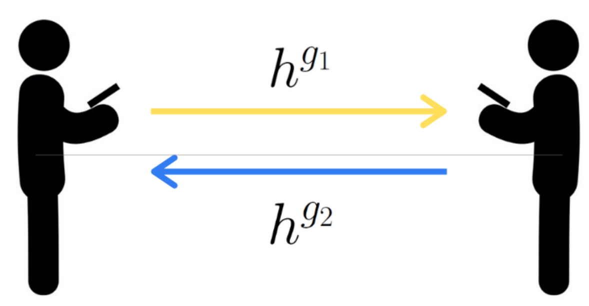


Quantum computers are expected to be powerful enough to break RSA and ECDH in the future, when they are sophisticated enough to execute Shor's algorithm.

Public Key Cryptography

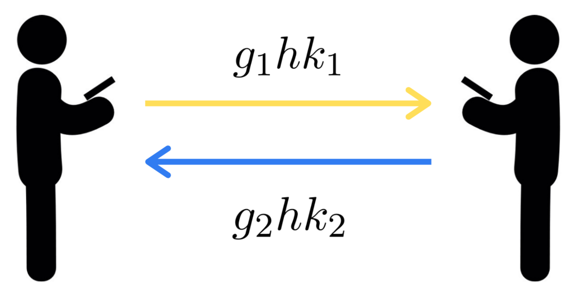


Classical approach. Commutative setting



$$h^{g_2 g_1} = h^{g_1 g_2}$$

Our approach. Noncommutative setting



$$g_1 g_2 h k_2 k_1^* = g_2 g_1 h k_1 k_2^*$$

Setting

Platform

Definition. Let K be a ring, and G a group. Let

$$\alpha : G \times G \longrightarrow U(K)$$

a 2-cocycle. The twisted group ring $R = K^\alpha G$ is defined to be the set of all finite sums of the form

$$\sum_{g_i \in G} a_i g_i$$

where $a_i \in K$, and all but a finite number of a_i are zero.

We define the sum of two elements in $K^\alpha G$ by

$$\Big(\sum_{g_i \in G} a_i g_i\Big) + \Big(\sum_{g_i \in G} b_i g_i\Big) = \sum_{g_i \in G} (a_i + b_i) g_i$$

And multiplication twisted by a cocycle is defined as

$$\Big(\sum_{g_i \in G} a_i g_i\Big) \cdot \Big(\sum_{g_i \in G} b_i g_i\Big) = \sum_{g_i \in G} \Big(\sum_{g_j g_k = g_i} a_j b_k \, \alpha(g_j, g_k) \Big) g_i$$

Our proposal. Let $K = GF(2^n)$ and $G = D_{2m}$,

and the 2-cocycle

$$\begin{aligned} \alpha : D_{2m} \times D_{2m} &\longrightarrow GF(2^m)^* \\ (x^i, x^j y^k) &\mapsto 1 \\ (x^i y, x^j y^k) &\mapsto t^j \end{aligned}$$

for every k.

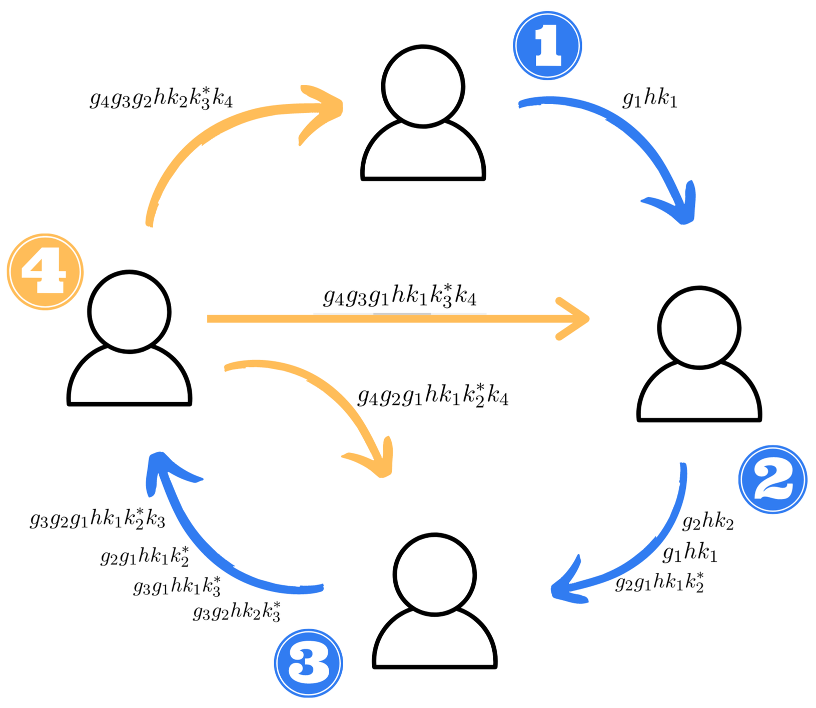
Decomposition problem

Given $x, y \in G$, find $a, b \in S \subseteq G$ such that

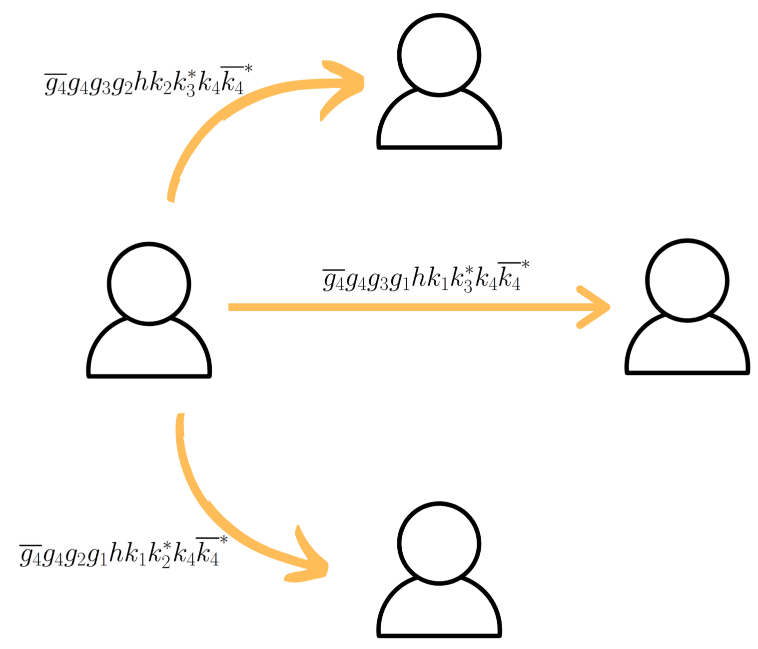
$$y = axb$$

Group Key Establishment

Initial Key Agreement (IKA)



Auxiliary Key Agreement (AKA)



Equivalence 2-n users

We define the random variables

$$A_n = (view(n, X), y)$$

$$D_n = (view(n, X), g_n ... g_3 g_2 g_1 h k_1 k_2^* k_3 ... k_n)$$

where view(n,X) is the set of all the possible messages in the insecure channel; and $\sim$ polynomial indistinguishability.

Theorem. For any $n > 2$, $A_2 \sim D_2$ implies that $A_n \sim D_n$, i.e. if the 2-users underlying decisional problem is hard, then the n-users is hard as well.

References.

[1] G. Alagic, J. Alperin-Sheriff, D. Apon, D. Cooper, Q. Dang, J. Kelsey, Y.-K. Liu, C. Miller, D. Moody. R. Peralta, R. Perlner, A. Robinson, D. Smith-Tone: "NIST Internal Report (NISTIR) 8309, Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process", *National Institute of Standards and Technology (NIST)*, 2020.

[2] C. Barnatt. A Guide to Computing. https://www.explainingcomputers.com/quantum.html

[3] M. Eftekhari: "A Diffie-Hellman key exchange protocol using matrices over group rings", *Groups Complex. Cryptol.*, 4(1), pp. 167-176, 2012.

[4] M.D. Gómez Olvera, J.A. López Ramos, B. Torrecillas Jover, "Public Key Protocols over Dihedral Group Rings", *Symmetry*, 11(8), 2019.

[5] M.D. Gómez Olvera, J.A. López Ramos, B. Torrecillas Jover, "Secure Group Communications using Twisted Group Rings", *Springer Proceedings in Mathematics and Statistics*, SPAS 2019, Vasteras, Sweden, to appear.

[6] D. Kahrobaei, C. Koupparis, V. Shpilrain: "Public key exchange using matrices over group rings", *Groups Complex. Cryptol.*, 5(1), pp. 97-115, 2013.

e-mail: gomezolvera@ual.es