Quantum and Post-Quantum Cryptography

Paulo Mateus – MMAC Thesis

Motivation

Shor's algorithm – quantum computers

- Breaks all currently used standards NIST standards
- Opens a new areas on complexity theory: BQP hardness

Post-quantum crypto

- Based on hardness assumptions not in BQP
- Asymmetric crypto
- What can we recover with PQcrypto

Quantum crypto

- Based on the impossibility of breaking the laws of Physics – Quantum Mechanics
- Irreversible and complex systems – physically unclonable functions

Post-quantum cryptography

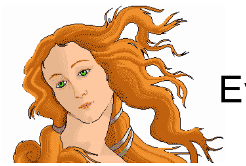
Diffie-Hellman - all values are mod p

Alice

$(g^b)^a$

g^a →

← g^b



Eve

Bob

$(g^a)^b$

DH works because

$$f \circ h = h \circ f,$$

f(x)=x^a mod p, h(x)=x^b mod p

We just need (non-linear) one-way functions that commute!!

- We can compute modular exponentiation in Polynomial Time
- The inverse (discrete log) is unknown to be computable in PT for prime p (if p-1 is non-smooth)
- Shor's method allows to compute discrete log as a Las Vegas algorithm in QPT

Post-quantum cryptography

PERMUTABLE RATIONAL FUNCTIONS*

BY

J. F. RITT

INTRODUCTION

We investigate, in this paper, the circumstances under which two rational functions, $\Phi(z)$ and $\Psi(z)$, each of degree greater than unity,† are such that

$$\Phi[\Psi(z)] = \Psi[\Phi(z)].$$

A pair of functions of this type will be called *permutable*.

A memoir devoted to this problem has recently been published by Julia.‡ When $\Phi(z)$ and $\Psi(z)$ are polynomials, and are such that no iterate of one is identical with any iterate of the other, Julia shows how $\Phi(z)$ and $\Psi(z)$ can be obtained from the formulas for the multiplication of the argument in the functions e^z and $\cos z$. His other results are mainly of a qualitative nature, and deal with the manner in which $\Phi(z)$ and $\Psi(z)$ behave when iterated.

Certain of Julia's results have been announced independently by Fatou.§ Fatou's method is identical with that of Julia.

The method used in the present paper differs radically from that of Julia and Fatou, and leads to results of much greater precision. Its chief yield is the

THEOREM. *If the rational functions $\Phi(z)$ and $\Psi(z)$, each of degree greater than unity, are permutable, and if no iterate of $\Phi(z)$ is identical with any iterate of $\Psi(z)$,‖ there exist a periodic meromorphic function $f(z)$, and four numbers a, b, c and d, such that*

$$f(az+b) = \Phi[f(z)], \qquad f(cz+d) = \Psi[f(z)].$$

The possibilities for $f(z)$ are: any linear function of e^z, $\cos z$, $\wp z$; in the lemniscatic case ($g_3 = 0$), $\wp^2 z$; in the equianharmonic case ($g_2 = 0$), $\wp' z$

- Joseph Ritt, Permutable Rational Functions. Transactions of the AMS, 1922

- Power polynomials x^n
- Chebyshev polynomials
- Elliptic Curves

Predicted DH, RSA and EC crypto

Post-quantum cryptography

Post-quantum cryptography

- McEliece – code theory – noise and **error correction,** large keys
- ~~Supersingular elliptic curves~~ - in P after all - 2023!!!
- ~~Unbalanced oil and vinegar variables~~ - Minrank attack to Rainbow, large keys
- LWE/RLWE/NTRU – Lattices and coding – noise and **error correction** ⇐

- Protocols - coin tossing, commitment, oblivious transfer, SMC, homomorphic encryption, proof of sequential work, ZK proofs, etc..
- Light-weight crypto, blockchain signatures and SMC in smart contracts

Post-quantum cryptography

- **Distributed Shor's algorithm**, L. Xiao, D. Qiu, L. Luo and P. Mateus, Quantum Information and Computation, Vol. 23, No. 1&2 0027–0044, 2023
- Two-round oblivious linear evaluation from learning with errors, P Branco, N Döttling, P Mateus, IACR International Conference on Public-Key Cryptography, 379-408, 2022
- **Most efficient oblivious transfer protocol (currently 30kOT/s)**
  ROTed: Random Oblivious Transfer for embedded devices. P Branco, L Fiolhais, M Goulão, P Martins, P Mateus, L Sousa. IACR Transactions on Cryptographic Hardware and Embedded Systems, 215-238, 2021
- Formal verification of ethereum smart contracts using Isabelle/HOL, Logic, Language, and Security: Essays Dedicated to Andre Scedrov on the Occasion of His 65th Birthday, **Maria Ribeiro**, Pedro Adão, Paulo Mateus, 2020
- Using low-density parity-check codes to improve the McEliece cryptosystem. **P Branco**, P Mateus, C Salema, A Souto, Information Sciences 510, 243-255, 2020.

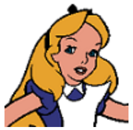
Quantum Cryptography

- We have enriched the **adversary model** with a quantum computer - Shor's algorithm
  - Enrich also protocols with quantum/physical resources
- **Quantum channels** (QC)
  - Information cannot be copied (no-cloning theorem)
  - Entanglement (instantaneous correlations at distance)
  - Sends (noisy) qubits instead of bits
- (Quantum) **physically unclonable functions** (q)PUF
  - Create a *chaotic* function that cannot be cloned

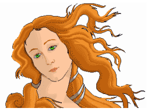
QC and PUFs enrich the security model

- Extend a symmetric key exponentially (QKD)
- OT with QChannels and relativistic communication can be made ITS
- OT is equivalent to BC with QChannel
- **Security proofs are hard**

Quantum Cryptography

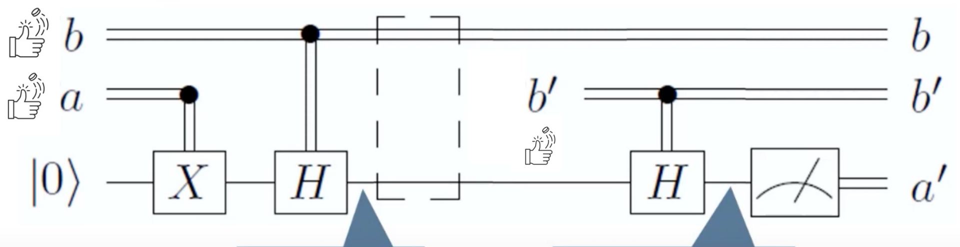


Alice



Eve

Bob



a	b	$\|\psi\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

a	b	b'	$\|\psi'\rangle$
0	0	0	$\|0\rangle$
~~0~~	~~0~~	~~1~~	~~$\|+\rangle$~~
~~0~~	~~1~~	~~0~~	~~$\|+\rangle$~~
0	1	1	$\|0\rangle$
1	0	0	$\|1\rangle$
~~1~~	~~0~~	~~1~~	~~$\|-\rangle$~~
~~1~~	~~1~~	~~0~~	~~$\|-\rangle$~~
1	1	1	$\|1\rangle$

Quantum cryptography

- A coherence-witnessing game and applications to semi-device-independent quantum key distribution. **M Silva**, R Faleiro, P Mateus, EZ Cruzeiro, Quantum 7, 1090, 2023
- Experimental semi-quantum key distribution with classical users, F Massa, P Yadav, A Moqanaki, WO Krawec, P Mateus, N Paunković, Quantum 6, 819, 2022
- A private quantum bit string commitment. **M Gama**, P Mateus, A Souto, Entropy 22 (3), 272, 2020
- Randomized oblivious transfer for secure multiparty computation in the quantum setting. **B Costa**, P Branco, M Goulão, M Lemus, P Mateus, Entropy 23 (8), 1001, 2021
- Quantum contract signing with entangled pairs. P Yadav, P Mateus, N Paunković, A Souto. Entropy 21 (9), 821, 2019