Pathologically breaking cryptography by quantum computing

2 authors:

Ed Gerck
Planalto Research
220 PUBLICATIONS **595** CITATIONS

SEE PROFILE

Ann Gerck
Planalto Research
16 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Pathologically breaking cryptography by quantum computing

This version: Oct/27/2023
First version: August/4/2023

By Ed Gerck*
egerck@gmail.com
Planalto Research
781 Washington St. #3423
Sonora, CA 95370
ORCID: 0000-0002-0128-5875

Keywords: RSA, large prime numbers, pathological, factorization, 10^1000

ABSTRACT

One needs a quantum-resistant algorithm, because all existing public-key encryption can now be broken. There are two types of quantum computing (QC) techniques: with complex numbers, and without. The former include: Shor's algorithm, adiabatic QC, quantum annealing principles, and others. Capital cost is about $10M. The latter is the simultaneous, multifactor logic, with 'all states at once', to have access to collective processing, as a technique of QC, proposed by Planalto Research and us. The capital cost was less than $1,000. We numerically proved, in computer science, that cryptography by RSA can be quickly broken, using a 10^1000 decimal digits number. The larger the prime number, the worse.

1. Introduction

We broke a RSA key with 10^{1000} decimal digits using quantum computing (QC) [2-5]. We numerically prove in [5] that this exemplifies how RSA can be quickly broken, e.g., for a 2048 bit-length number.

The larger the prime number, the worse [5]. This is in contradiction with the well-known need for larger prime numbers to prevent factorization.

Considering that in 2048 bits one can store a number with 617 decimal digits, we passed that in the example in [5].

This is a stunning result and reveals that RSA is easily broken even for more than 2048 bits.

2. METHODS

This work did not use SDKs such as Qiskit, Bracket, and Cirq, as well as platforms such as IBM, AWS, and Google, because cryogenics is not needed, complex qubits do not exist, and qubits are experimentally insufficient to represent a quantum state.

Instead, we showed [1] that one needs at least tri-state to represent collective effects, as also shown by Einstein when quantum mechanics was starting in 1917, to not use imaginary numbers as Erwin Schrödinger explained in 1926, and as demonstrated classically by Intel with Verilog in 2020. These are well-known results. QC is understood as simultaneous, multifactor logic, with 'all states at once', accessing collective processing.

The new disclosed results in QC used a commercial cell phone running Android. This opens the market to personal use.

3. CONCLUSION

This work demonstrates quantum supremacy, using CS, by calculating what is impossible to verify using classical methods in a short time. This was done mainly, by allowing collective processing.

We demonstrate knowledge of a closed formula to quickly calculate prime numbers, exactly, offering numerical evidence in CS of a new mathematics using Quantum Mechanics (QM).

QM becomes our most rigorous model of nature. We show that mathematics needs to follow QM formulas. This is similar to what is well-known to have been overcome by Ramanujan in formulas for partitions.

To preserve encryption by RSA, still used today, and impact less cybersecurity, we do not share any formula, but the numerical results -- as an objective warning against the well-known U.S. NIST recommendation for RSA and cybersecurity, that RSA can still be used for years ahead. One needs a quantum-resistant algorithm, because all existing public-key encryption can be broken.

FUNDING

This research received external funding from Network Manifold Associates, Inc. (NMA), Safevote, Inc, and Planalto Research. The author declares no conflict of interest.

ACKNOWLEDGMENTS

The author is indebted to the work of late Mādhava of Sangamagrāma, late Dr. Augusto d'Oliveira, late Cel. Dr. Amarante, Ann Gerck, Editor at Planalto Research, and six anonymous reviewers. ResearchGate discussions and private messages were also used, for “live” feedback, important due to the physical isolation caused by COVID.

REFERENCES

[1] rsa.com

[2] Ed Gerck, “Algorithms for Quantum Computation: Derivatives of Discontinuous Functions.” Mathematics 2023, 11, 68. https://doi.org/10.3390/math11010068 , 2022.

[3] Gerck, E. and d'Oliveira, A.B., 1978, https://inis.iaea.org/collection/NCLCollectionStore/_Public/10/462/10462075.pdf. Accessed on Oct/23/2023.

[4] Gerck, E., Gallas, J.A,C., and d'Oliveira, A.B., June 1982, Physical review A, Atomic, molecular, and optical physics 26:1(1).

[5] Gerck, E., Gerck, A. “QC Algorithms: Fast Calculation of Prime Numbers”. https://www.researchgate.net/publication/373516231/.