QRAND topics

(Dated: September 30, 2021)

Abstract

This draft contains a very brief description of topics & activities of QRAND —**Q**antum **R**esearch **AN**d **D**evelopment—in the domain of quantum computation and information, with emphasis on, but not limited to,

(i) industry-standard production and distribution of random n-ary information;

(ii) improvement and upgrade—e.g. normalization—of existing n-ary sequences relative to pre-defined criteria;

(iii) analysis toward realizations of quantum cryptocurrencies that are generalizations to classical cryptocurrencies;

(iv) evaluation of quantum cryptanalytic attacks on cryptocurrencies by (relative to transaction processing) "fast" computation of the private key from the public key of digital signatures;

(v) search for and development of quantum cryptographic protocols for digital signatures which are save with respect to quantum cryptanalytic attacks;

(vi) search for and development of (quantum) cryptographic protocols which are novel and asymmetric (e.g., based on hypergraph theory);

(vii) search for and development of quantum algorithms utilizing quantum parallelism via "spread-process-fold" strategies.

I. SERVICES AND PRODUCTS

QRAND intends to realize several main services and products in the following areas:

(i) quantum randomness;

(ii) quantum cryptography;

(iii) quantum cryptocurrencies;

(iv) quantum computing.

A. Randomness

1. Research

(i) certification and due diligence of existing random number generators and random sequences;

(ii) improvement and upgrade—e.g. normalization, see later (iv)—of existing random sequences, relative to pre-defined goals and tasks;

(iii) production of n-ary ($n > 1$ but finite) random sequences; e.g., by recording detector clicks from quantum systems, which are in some coherent superposition (aka linear combination in Hilbert space) and subject to quantum features such as complementarity, nonlocality, and contextuality;

(iv) un-biasing by normalization of n-ary sequences to eliminate bias from such sequences because of unavoidable imperfections (e.g., thermal drift, misalignments) by modern advanced coding techniques.

2. Small-scale applications

(i) partial quantum encryption of existing classical keys: "key growing";

(ii) total quantum encryption "ab initio"; without pre-existing classical key;

(iii) White labelling by outsourcing existing equipüment; possibly augmenting it with normalization or other postprocessing;

(iv) The key generator can also be installed at the customer's site plus ongoing service of implementation into the customer's system.

(v) The advantage of this method is the uniqueness of a key or the security protocol, which may eventually lead to a process patent.

3. Large-scale applications

(i) Creating a quantum-based security system for entire parts of the company;

(ii) Construction of a quantum tunnel within a company with geographical challenges. Thereby the emphasis is on research, as such a system involves physical cable laying—laser technology based—and thus also special technical challenges such as vibration-free, "lossless" lines; or lines with quantum repeaters. Any concrete implementation over large distances is currently very unlikely as investment costs are over 50 Mio EUR from e.g. Vienna to Linz.

(iii) Laying of quantum cables, quantum repeaters and other quantum components such as beam splitters;

(iv) Conrete security protocols based on existing literature.

(v) The advantage of this method is the uniqueness of a key or the security protocol, which may eventually lead to a process patent.

B. Cryptanalysis

Attempts in quantum cryptanalysis include, but are not limited to:

(i) the evaluation of quantum cryptanalytic attacks on cryptocurrencies by (relative to transaction processing) "fast" computation of the private key from the public key of digital signatures;

(ii) the search for and development of quantum cryptographic protocols for digital signatures which are save to quantum cryptanalytic attacks.

(iii) the search for and development of (quantum) cryptographic protocols which are novel and asymmetric (e.g., based on hypergraph theory);

(iv) certification and due diligence of existing realizations of quantum communication protocols;

(v) search into improved quantum communication protocols.

C. Quantum cryptographic currencies

(i) Quantum currencies based on an early protocol by Wisner [1].

(ii) Implementation of quantum crypto-currencies generalizing recent classical crypto-currencies.

Cryptocurrencies are on the verge of becoming an asset class of its own. In Quantum Crypto Currency Research we focus on the quantum implementation and the specifics of basic topics of crypto trading and processing such as pricing transparency, clearing and settlement.

While overall we see transparency and fast settlement in crypto transactions and safety in processing as key to future success of cryptocurrencies, we observe that the cryptocurrency approach has many common features of quantum evolution; eg, reversibility, and the possibility to recover past transactions.

At the same time we realize some common problems: the difficulties associated with "getting rid" of older transaction records can be perceives both as a benefit but also as a drawback. Because ultimately this may either lead to a slowdown of transaction activity due to excessive space (storage access) requirements — an "overheating" of sorts, as discussed in statistical physics in the context of Maxwell's Demon.

We are therefore committed to the development of new techniques to combine scalable transaction volumes with security and transparency and ease of such transactions.

D. Computation

Quite trivially, any existing computer is a quantum computer because its microphysical layer is quantized. Increased miniaturization, as indicated by the end of Moore's Law [2, 3], enforces processor designs and manufacturers to cope with quantization. Besides, there are potential quantum advantages,

(i) such as parallelization through coherent superpositions "inclusions" of classical exclusive states;

(ii) entanglement through that is relational encoding of multi-partite states, accompanied by individual value indefiniteness of the states of its constituents;

(iii) quantum contextuality in its various forms [4–10];

(iv) quantum nonlocality [11, 12] associated with multipartite states.

Quantum computation can be seen as a trifold "spread-process-fold" strategy to obtain relevant information by encoded into incomplete knowledge states, very much like Robert Musil's "bridge metaphor" of complex numbers: at the beginning and the end there is solid information, in-between there are quantum states "bridging an abyss".

II. MAIN PROTAGONISTS, KNOWHOW AND SKILLS

QRAND exploits quantum mechanical properties, based on contemporary physical conceptions of nature.

The main protagonists of this startup will be two academic seed centres "across the globe": sone in the EU (Vienna) and sone in New Zealand (Auckland); with the founders Prof. Karl Svozil, TU Wien, Vienna, Austria, and Prof. Cristian Calude, University of Auckland, Auckland, NZ. The QRAND Organization is based on academic cooperation; with previous EU/NZ backed joint grants (by the same name) on the subject.

Svozil has a long track of publications on the generation of quantum random sequences. These include very early suggestions of "quantum coin toss" experiments [13], very early suggestions to utilize quantum contextuality for the production of random sequences [14], as well as a recent monography on the subject [15].

Calude has a long track of records on mathematical and computer science aspects of randomness, including the formal definition and certification of randomness [16, 17], as well as in "un-biasing" imperfect sequencing through normalization algorithms [18–21].

Both researchers have collaborated in various forms and multiple papers on the certification [22] and proposals for the physical production of quantum random numbers, certified by quantum mechanical features such as contextuality and value indefiniteness [23–25].

For the production of quantum randomness hardware "chips" various groups around the globe have acquired knowledge and know-how that can be exploited royalty-free.

[1] Stephen Wiesner, "Conjugate coding," SIGACT News **15**, 78–88 (1983).

[2] Steve Blank, "What the GlobalFoundries' retreat really means. Things will never be the same for consumer devices," (2018), "Moore s Law ended a decade ago. Consumers just didn t get the memo", posted on Sep 10th, 2018 at 21:49 GMT, accessed May 25th, 2021.

[3] David Rotman, "We're not prepared for the end of Moore's law," (2020), mIT Technology Review, Computing/Quantum computing, posted on Feb 24th, 2020, accessed May 25th, 2021.

[4] Ehtibar N. Dzhafarov, Victor H. Cervantes, and Janne V. Kujala, "Contextuality in canonical systems of random variables," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **375**, 20160389 (2017), arXiv:1703.01252.

[5] Samson Abramsky, "Contextuality: At the borders of paradox," in *Categories for the Working Philosopher*, edited by Elaine Landry (Oxford University Press, Oxford, UK, 2018) pp. 262–285, arXiv:2011.04899.

[6] Philippe Grangier, "Contextual objectivity: a realistic interpretation of quantum mechanics," European Journal of Physics **23**, 331–337 (2002), arXiv:quant-ph/0012122.

[7] Alexia Aufféves and Philippe Grangier, "Extracontextuality and extravalence in quantum mechanics," Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **376**, 20170311 (2018), arXiv:1801.01398.

[8] Alexia Auffèves and Philippe Grangier, "Deriving born's rule from an inference to the best explanation," Foundations of Physics **50**, 1781–1793 (2020), arXiv:1910.13738.

[9] Philippe Grangier, "Completing the quantum formalism in a contextually objective framework," (2020), preprint arXiv:2003.03121, arXiv:2003.03121.

[10] Costantino Budroni, Adán Cabello, Otfried Gühne, Matthias Kleinmann, and Jan Åke Larsson, "Quantum contextuality," (2021), arXiv:2102.13036 [quant-ph].

[11] Albert Einstein, Boris Podolsky, and Nathan Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Physical Review **47**, 777–780 (1935).

[12] Don Howard, "Einstein on locality and separability," Studies in History and Philosophy of Science Part A **16**, 171–201 (1985).

[13] Karl Svozil, "The quantum coin toss—testing microphysical undecidability," Physics Letters A **143**, 433–437 (1990).

[14] Karl Svozil, "Three criteria for quantum random-number generators based on beam splitters," Physical

Review A **79**, 054306 (2009), arXiv:quant-ph/0903.2744.

[15] Karl Svozil, *Physical [A]Causality. Determinism, Randomness and Uncaused Events* (Springer, Cham, Berlin, Heidelberg, New York, 2018).

[16] Cristian Calude, *Information and Randomness—An Algorithmic Perspective*, 2nd ed. (Springer, Berlin, 2002).

[17] Cristian S. Calude and Michael J. Dinneen, "Is quantum randomness algorithmic random? a preliminary attack," in *Proceedings of the 1st International Conference on Algebraic Informatics*, edited by S. Bozapalidis, A. Kalampakas, and G. Rahonis (Aristotle University of Thessaloniki, Thessaloniki, Greece, 2005) pp. 195–196.

[18] Cristian Calude, "Borel normality and algorithmic randomness," in *Developments in Language Theory*, edited by Grzegorz Rozenberg and Arto Salomaa (World Scientific, Singapore, 1994) pp. 113–129.

[19] Alastair A. Abbott and Cristian S. Calude, "Von Neumann normalisation and symptoms of randomness: An application to sequences of quantum random bits," in *Unconventional Computation*, edited by Cristian S. Calude, Jarkko Kari, Ion Petre, and Grzegorz Rozenberg (Springer, Berlin, Heidelberg, 2011) pp. 40–51.

[20] Cristian S. Calude and Ludwig Staiger, "Liouville, computable, Borel normal and Martin-Löf random numbers," Theory of Computing Systems **62**, 1573–1585 (2017).

[21] Alastair A Abbott, Cristian S Calude, Michael J Dinneen, and Nan Huang, "Experimentally probing the algorithmic randomness and incomputability of quantum randomness," Physica Scripta **94**, 045103 (2019), arXiv:1806.08762.

[22] Cristian S. Calude, Michael J. Dinneen, Monica Dumitrescu, and Karl Svozil, "Experimental evidence of quantum randomness incomputability," Physical Review A **82**, 022102 (2010).

[23] Alastair A. Abbott, Cristian S. Calude, Jonathan Conder, and Karl Svozil, "Strong Kochen-Specker theorem and incomputability of quantum randomness," Physical Review A **86**, 062109 (2012), arXiv:1207.2029.

[24] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, "Value-indefinite observables are almost everywhere," Physical Review A **89**, 032109 (2014), arXiv:1309.7188.

[25] Alastair A. Abbott, Cristian S. Calude, and Karl Svozil, "A variant of the Kochen-Specker theorem localising value indefiniteness," Journal of Mathematical Physics **56**, 102201 (2015), arXiv:1503.01985.