PRESS RELEASE DATED 10th MARCH 2022

REAMC®
Limited

The ACORN-QRE method for Quantum Resistant Encryption

SUMMARY: ACORN-QRE is a new patented method for generating secure one-time pads for use in Vernam-type stream cyphers. It can be used to generate a whole family of one-time pads, each of which offers the same level of security as a truly random pad, and which remains secure against future computational improvements in conventional computers as well as possible future developments of quantum computing.

ACORN-QRE is built on the ACORN pseudo-random number generator, a method for generating pseudo random numbers that are uniformly distributed on the unit interval. The underlying ACORN generator has been demonstrated to pass all the standard tests for non-cryptographic use (see for example REAMC Report-004(2021) which is available from the publications page of the website www.reamc-limited.com), but ACORN by itself is not cryptographically secure. Cryptographic security is achieved through the application of the ACORN-QRE algorithm to an ACORN sequence.

In January 2020 REAMC Limited filed a patent application (published by the UK Intellectual Property Office on 4 August 2021 under Serial No. GB2591467; international patents are also pending) for "a computer-implemented method of generating secure one-time pads for use in encryption and decryption". This relates to the ACORN-QRE method of generating secure one-time pads for use in Vernam-type stream ciphers. **UK IPO confirmed (in February 2022) that the patent was approved for grant, and it is expected to grant soon after 10th March 2022.**

The ACORN-QRE method can be used to generate a whole family of one-time pads (which can be based on any desired alphabet, including binary, hexadecimal, or any desired form of alphanumeric alphabet) that each work as effectively as a truly random one-time pad; it also allows the key to be distributed or shared much more easily and securely than sharing the full content of the pad.

It has been believed up to now that using a software numerical method to generate the pads is inherently insecure because it allows the possibility of an attacker being able to recreate the pad given knowledge of a sufficiently long section of the pad. The proposed ACORN-QRE method is resistant to such attacks, because of the number of different initialisations that are possible, and because the algorithm turns out to be inherently not susceptible to reverse-engineering the "secret information" (the key) from the contents of the pad. The ACORN-QRE method offers the same level of security as a truly random pad, and remains secure against future computational improvements in conventional computers as well as possible future developments of quantum computing.

The immense number of alternative one-time pads (more than 2^{120} different pads, each pad having length in excess of 2^{120}; 2^{120} is approximately equal to 10^{36} which is one billion billion billion billion) that are available to choose from using this method means that use of Vernam ciphers need no longer be restricted to critical communications and becomes practical for use in all applications ranging from diplomatic, military and commercial communications all the way to everyday communications or files which users wish to keep private.

Published details about the Patent are available from
https://www.ipo.gov.uk/p-ipsum/Case/PublicationNumber/GB2591467

For further information please contact

Roy S Wikramaratna, CEng, CSci
Director - REAMC Limited
Reservoir Engineering and Applied Mathematics Consultancy
Telephone: +44 (0)7968 707062
E-mail address: rwikramaratna@gmail.com
Web-site address: https://www.reamc-limited.com