ACORN-QRE: A Practical Method of Generating Secure One-time Pads for Use in Encryption

Roy S Wikramaratna, REAMC Limited, United Kingdom

Web-site address www.reamc-limited.com

Email contact rwikramaratna@gmail.com

FOR PRESENTATION AT SIAM PP-26, BERLIN, 4th MARCH 2026

REAMC®
Limited

Abstract.

The Additive Congruential Random Number (ACORN) generator gives rise to sequences with long period approximating to uniformity in up to k dimensions (for any value of k). ACORN-QRE (Wikramaratna, REAMC Report-007, 2023, https://eprint.iacr.org/2023/1080) is a straightforward modification which avoids the linearity of ACORN, while preserving the uniformity. This can generate one-time pads that are demonstrably resistant to attack by current computers or by future computing developments (including quantum). The pads, which can use any alphabet, work with a Vernam-type cypher to securely encrypt both files and communications.

In this paper, we present performance data for a software implementation of ACORN-QRE with a key of 1079 bits, each bit assigned randomly as 0 or 1. On a standard laptop or desktop computer, this works to securely encrypt binary files of arbitrary size. Encrypted files can be safely shared over any public network or even left for collection on a publicly-accessible web site without fear of their being intercepted and later read by a malicious actor. Only the sender and the intended recipient (in possession of the relevant key, which must be kept secure) are able to decrypt the file. Thus, the problem of securely sharing GBs or even TBs of data is reduced to one of securely sharing a key comprising 1079 random-looking bits.

The ACORN-QRE algorithm is patented in UK (GB2591467) and USA (US11,831,751B2); the patents are owned by REAMC Limited.

Title: ACORN-QRE: A Practical Method of Generating Secure One-time Pads for Use in Encryption

Author submitting (speaker)
Roy S Wikramaratna
REAMC Limited

Outline

1. Motivation and background: use of Vernam cyphers with a random one-time pad (OTP); symmetric encryption methods (eg AES)
2. ACORN: k-distributed pseudo-random number generation; uniform, random but NOT cryptographically secure
3. ACORN-QRE: simple modification preserving uniformity of ACORN, while ensuring cryptographic security of resulting OTP
4. ACORN-QRE representative timings (software implementation)
5. CONCUSIONS

Vernam cyphers - Secure encryption using random (binary) one-time pads

- Idea dates back ~100 years, generally attributed to Gilbert Vernam (AT&T) and Joseph Mauborgne (US Army Signal Corps)
  - Randomly generated (binary) one-time pad (OTP)
  - "Exclusive Or" (XOR) between binary file (plaintext) and OTP gives cyphertext
  - Symmetric method – decryption is XOR between cyphertext and (same) OTP
- With truly random pad
  - The only known provably unbreakable cryptographic system, proved by Claude Shannon of AT&T in 1949 [Reference S-1949]
- Practical issues (to maintain 'unbreakable' security)
  - No section of the OTP can be used more than once
  - Must be truly random; need to verify randomness properties of the OTP
  - OTP at least as long as sum of all anticipated message lengths
  - Full OTP shared securely in advance and contents must remain secure

Security of symmetric encryption methods in the face of computing developments

- Modern symmetric methods (eg AES) typically employ key lengths up to 256 bits
  - Currently considered to provide sufficient level of security … but some concerns over vulnerability to future developments of quantum computers
  - Increasing key length is not straightforward … scaling the algorithm and security verification of any extension to larger keys are non-trivial exercises
- ACORN-QRE represents different approach to symmetric encryption
  - **SECURE** one-time pads (OTPs) for use with a Vernam cypher
    - 1079 bits key length provides demonstrable security even in the face of possible future quantum computing development
    - Secure key selection is possible, eg using Diffie-Hellman key exchange [Reference DH-1976]; or see Holden [Reference H-2017] which also includes more general discussion
  - **SIMPLE** to implement; runs on a conventional computer
  - **SCALEABLE** - scales easily and naturally to even larger key lengths, progressively increasing security (although probably not required)
  - **SPEEDY** to execute, allows parallel execution on multiple processors

Example of Vernam cypher using exclusive-or (XOR) [REAMC Report-007, Reference W-2023]

0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1	0	0	1	1	1	1	1	1	1	1	1	1
0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0		1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1
1	1	1	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	1
1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	1	1	0
1	1	1	1	0	0	1	1	1	1	0	1	1	1	0	0	1	1	1	0
1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	1	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	1	1	0	0
1	1	1	1	0	0	1	1	1	1	0	1	1	1	0	0	1	1	1	0
1	1	1	1	0	0	1	1	1	1	0	1	1	0	0	0	0	1	1	0
1	1	1	1	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	1

Plaintext

0	1	1	0	1	1	1	0	1	0	0	1	0	0	0	0	1	1	1	1
0	1	1	0	0	1	0	1	0	1	0	1	1	0	0	1	0	0	0	1
1	0	1	1	1	0	0	1	0	1	1	1	1	0	0	1	0	1	1	0
0	0	0	1	0	1	1	1	0	1	1	1	0	0	1	0	1	1	1	1
1	1	0	1	1	1	1	1	0	0	1	1	0	1	1	1	0	1	0	1
0	0	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	0	0	0
1	0	1	0	0	1	1	1	1	1	0	1	0	0	0	1	0	1	0	1
1	0	1	0	0	1	0	0	0	0	0	1	1	1	0	1	0	1	1	1
0	1	0	1	1	0	1	1	0	0	1	1	1	1	1	0	0	1	0	1
1	0	0	1	0	1	1	1	1	1	0	0	0	1	0	0	1	0	1	0
1	0	0	1	0	1	0	1	1	0	0	0	1	1	0	1	1	0	0	1
0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	1	1	0	1	0
1	1	0	1	0	1	1	1	1	1	1	1	1	1	0	1	0	1	0	0
0	1	0	1	1	0	0	0	0	1	0	1	0	0	0	1	1	0	1	0
0	0	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	0
1	0	1	1	1	1	1	0	0	0	0	1	1	0	0	1	0	1	0	0
1	1	0	0	1	1	1	1	1	1	0	1	1	0	1	0	1	1	1	0
1	0	1	1	1	1	0	0	1	0	1	1	1	0	0	1	0	1	1	1
1	0	1	0	0	0	1	1	0	0	0	0	1	1	1	0	0	0	0	1
0	0	1	1	1	0	0	1	0	0	1	1	0	1	0	1	0	0	0	0

One-time Pad(OTP)

0	1	1	0	1	1	1	0	1	0	1	0	1	1	1	1	0	0	0	0
0	1	1	0	0	1	0	1	0	1	0	1	1	0	0	1	0	0	0	1
1	0	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1
0	0	1	0	1	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0
1	1	1	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	0	1
0	0	1	1	0	1	1	0	1	0	1	1	1	0	0	0	0	1	1	1
1	0	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	0	1	0
1	0	0	1	1	0	1	1	0	0	0	1	1	1	0	1	0	1	1	1
0	1	0	1	1	0	1	1	0	0	0	0	0	0	0	1	1	0	1	0
1	0	0	1	0	1	1	1	1	1	1	1	1	0	1	1	0	1	0	1
0	1	1	0	0	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0
1	0	1	1	0	1	1	0	0	0	0	0	1	0	0	1	1	1	0	0
0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	1	1	0	1	0
1	0	1	0	1	0	1	1	1	0	0	1	1	1	1	0	0	1	1	0
0	0	1	0	0	0	1	0	1	0	0	1	1	1	1	0	0	1	1	0
1	0	1	1	1	1	1	0	0	0	0	1	1	1	1	0	1	1	0	0
0	0	1	1	1	1	0	0	0	0	0	1	0	1	0	1	0	0	1	0
0	1	0	0	1	1	1	1	0	1	1	0	0	1	0	1	1	0	0	1
0	1	0	1	0	0	0	0	1	1	0	1	0	1	1	0	0	1	1	1
1	1	0	0	1	0	1	0	1	1	0	1	0	1	0	1	0	0	0	1

Cyphertext

ACORN pseudo-random number generator

- Discovered ~1984, published in 1989, in JCP [Reference W-1989]
- Implementation (also parallelisation) discussed eg in SIAM News [Reference W-2000]
- Theoretical analysis shows that a k-th order ACORN generator with modulus 2^M approximates to well-distributed in k-dimensions as M increases, published JCAM [Reference W-2010]
- Empirical testing culminating in REAMC Report-008 [Reference W-2025] – orders 8, 9, 10 with modulus 2^{120}
- ACORN is random, uniform, but is NOT cryptographically secure
  - If you know k+1 consecutive ACORN variates exactly, then can determine the whole sequence

ACORN-QRE – the idea

- Use k-th order ACORN generator, modulo 2^M, with ‘randomly selected’ odd seed to generate sequence of variates, each with M bits
  - eg order k=8, modulus 2^M where M=120
  - Choose b<<M (in the performance examples below, have used b=8, generating 1 byte or 8 bits from each variate that is kept)
- For each variate
  - If leading digit is 0, then take next b digits of the variate for the OTP
  - If leading digit is 1, then discard the variate completely
- In effect, decide whether or not to use each block of b digits randomly, with probability p=0.5
- Systematic discards of trailing bits and the random discards of the higher order bits are the key ideas ensuring cryptographic security of the method

Vernam cypher with a pseudo-random pad – not in general considered secure

- Areas of concern may include
  - Insufficient entropy (small key size) – vulnerability to brute force attack or inadvertent reuse of keys
  - Short (may be unknown) period – OTP exhausted and inadvertently reused
  - Cryptographic insecurity – knowledge of algorithm and/or section of OTP may allow key identification (to generate entire OTP)
  - Key-sharing vulnerabilities … but less severe than for random pad

- Solved by ACORN-QRE
  - Key size typically ~1000 binary bits with random values avoiding inadvertent reuse
  - Known period (typically >>2^{100}), no realistic chance of exhausting
  - Demonstrable cryptographic security – no possibility of identifying key from a section of OTP except by brute force search
  - Share ~1000 (randomly chosen) bits, giving access to OTP of length >> 2^{100} bits

ACORN-QRE – a cryptographically secure pseudo-random OTP generation algorithm

- See REAMC Report-007 [Reference W-2023]; also, the UK and US patents
- A very straightforward modification of ACORN which renders the resulting binary sequence cryptographically secure
  - Works for any k at least 8 and any modulus large enough (eg 2^M with M=120, which gives key length of 1079)
  - Knowledge of any section of an ACORN-QRE sequence, however long, gives no help in predicting what comes next
    - Cannot improve on simply guessing 1 or 0 with probability 0.5, independently for each digit
  - Only practical way to attempt to identify the key from a section of the sequence is by exhaustive testing of all possible keys to find one (possibly more than one may prove to be feasible) that matches the known section of the sequence
    - This is shown to take very many times longer than the life of the universe, irrespective of parallelisation or cpu speedup, and is believed resistant to quantum computing developments

ACORN-QRE Performance - Running on a Standard Laptop

- HP Pavilion 15 (2021 vintage), with Windows 11 operating system
  - 64-bit operating system, x64-based processor
  - 4 Cores; 8 Logical Processors
    - Processor: 11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz (2.42 GHz)
  - 8.00 GB RAM (7.77 GB usable)
  - SSD - NVMe SAMSUNG MZVLQ512HALU-000H1
- ACORN-QRE (version 1f) with 1079 bit key size
  - Implemented in Fortran; NAG f-2008 compiler; fully optimised (level 4)
  - Allows encryption of arbitrary-sized binary files (Megabytes or Gigabytes)
  - Successfully tested up to 30 Gigabytes with no deterioration of performance

ACORN-QRE Performance – 10 Gigabyte File

ENCRYPTION	ACTUAL	ACTUAL	Per Gigabyte	Per Gigabyte	PERCENT	SPEED
	CPU Sec	CLOCK Sec	CPU Sec	CLOCK Sec	CPU/CLOCK	Megabyte/ CLOCK Sec
READING PLAINTEXT	6.40	10.52	0.64	1.05	61%	951
GENERATING PAD	230.27	230.75	23.03	23.08	100%	43
ENCRYPTION	2.43	2.48	0.24	0.25	98%	4038
CYPHERTEXT OUTPUT	4.31	12.58	0.43	1.26	34%	795
TOTAL	243.40	256.33	24.34	25.63	95%	39
DECRYPTION	ACTUAL	ACTUAL	Per Gigabyte	Per Gigabyte	PERCENT	SPEED
	CPU Sec	CLOCK Sec	CPU Sec	CLOCK Sec	CPU/CLOCK	Megabyte/ CLOCK Sec
READING CYPHERTEXT	6.10	10.04	0.61	1.00	61%	996
GENERATING PAD	227.40	227.84	22.74	22.78	100%	44
DECRYPTION	2.16	2.17	0.22	0.22	100%	4615
DECRYPTED (PLAIN) TEXT OUTPUT	4.90	35.33	0.49	3.53	14%	283
TOTAL	240.56	275.38	24.06	27.54	87%	36

ACORN-QRE Scope for Performance Improvement (currently 35-40 Megabytes per clock second)

- Reduce modulus from 2^{120} to 2^{60}, reduces key size from 1079 to 539 – effectively halves time required for OTP generation (with some reduction in security) **~ 80 Megabytes/clock second**
- Pre-calculation and storage of OTP (with 1079 bit key)
    - Reduce overall encryption/decryption times on current hardware to ~5s/Gigabyte (from 25s/Gigabyte) corresponds to overall speed of **~200 Megabytes/clock second**
    - … potential drawbacks including to compute and store a very large pad which uses a large amount of storage space and which may never be used in practice
- Pad generation can be parallelised with arbitrary numbers of processors (with 1079 bit key)
    - Current results only use a single processor for pad generation
    - Scope for near four-fold speed-up using current hardware (**~120 Megabytes/clock second**)
    - Further speedup potential with more processors (up to **~400 Megabytes/clock second** limited by current I/O speed)
- Hardware improvements
    - Faster CPU- Reduction of pad generation (also encryption) time
    - Faster I/O - Faster SSD drives available and would improve the I/O performance
- Ultimate potential for speeds in excess of **1 Gigabyte (1000 Megabytes)/clock second**.

CONCLUSIONS

- ACORN-QRE runs on a standard computer; offers quantum safe encryption today
- ACORN-QRE with 1079 bit ‘randomly selected’ key
  - Secure enough to use for diplomatic and commercial messaging/data transmission
  - Simple enough (and sufficient key availability) for widespread peer-to-peer messaging/data transmission, even between every pair of potential users or devices in the world today
  - Encryption/decryption performance with 1079 bit key of 35-40 Megabytes per second on standard off-the shelf laptop using a single cpu
- Key length of ~1000 bits (as here) would seem sufficient for any conceivable use
  - … but algorithm scales easily to even larger key sizes (eg ~2000, ~4000, or even more bits) if that were considered necessary
  - Encryption/decryption performance scales in inverse proportion to key length; level of security for encryption scales as two to the power of the key length
- Single processor performance dominated by time for generating the OTP, but…
  - OTP generation inherently amenable to parallel computation
  - Potential for OTP generation speedup factor approaching n, the number of available processors being used

ACORN-QRE Collaboration Opportunities Please talk to me this week, or contact via e-mail

- Working version of ACORN-QRE now available to demonstrate and share (subject to appropriate non-disclosure agreements)
- Seeking partners to collaborate
  - Commercial partners – licensing/distribution and funding of further commercial development of ACORN-QRE
  - Academic partners – independent review and more rigorous analysis of security of ACORN-QRE
  - Identify opportunities for UK government/EU grant funding for further collaborative research in this area

Further Information

- The ACORN-QRE algorithm is patented in the UK and USA
  - Patent GB2591467 granted on 27 April 2022 by UK Intellectual Property Office
  - Patent US-11831751-B2 granted 28 Nov. 2023 by US Patent and Trademark Office
  - Patents owned by REAMC Limited, 4 Nuthatch Close, Poole, Dorset BH17 7XR, UK
- List of papers directly referenced in the slides follows in REFERENCES
  - More comprehensive lists of publications relevant to ACORN and ACORN-QRE available in the References to REAMC Report-007 and Report-008 or on the REAMC Limited website www.reamc-limited.com
- The content of this presentation will be made available for download on the publications page of the REAMC Limited website
  - To be written up in due course as REAMC Report-009, which will also be made available on the publications page of the REAMC Limited website

REFERENCES

- [DH-1976] W Diffie and M Hellman, “New directions in cryptography” in IEEE Transactions on Information Theory, vol 22, no , pp644-654, November 1976
- [H-2017] J Holden, “The mathematics of secrets: cryptography from Caesar cyphers to digital encryption”, 370pp, Princeton University Press, 2017
- [S-1949] C Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal. 28 (4): 656–715, 1949. [doi:10.1002/j.1538-7305.1949.tb00928.x]
- [W-1989] R S Wikramaratna, ACORN - A New Method for Generating Sequences of Uniformly Distributed Pseudo-random Numbers, J. Comput. Phys., 83, pp16-31, 1989
- [W-2000] RS Wikramaratna, “Pseudo-random Number Generation for Parallel Processing – A Splitting Approach”, SIAM News (Applications on Advanced Architecture Computers), November 2000
- [W-2010] R S Wikramaratna, Theoretical and Empirical Convergence Results for Additive Congruential Random Number Generators, J. Comput. and Appl. Math., 233, pp2302-2311, 2010. [doi: 10.1016/j.cam.2009.10.015]
- [W-2023] R S Wikramaratna, ACORN-QRE: Specification and Analysis of a Method of Generating Secure One-time Pads for Use in Encryption, REAMC Report-007, July 2023
- [W-2025] R S Wikramaratna, Statistical Performance of ACORN Generators: Further Evidence for Orders 8 – 10, REAMC-Report-008, June 2025

Thank You!

- Contact details

Roy Wikramaratna, REAMC Limited
rwikramaratna@gmail.com
www.reamc-limited.com