ACORN-QRE: Generation of Secure One-time Pads for Use in Encryption

Roy S Wikramaratna, REAMC Limited

email: rwikramaratna@gmail.com
website: www.reamc-limited.com

INTRODUCTION

The Additive Congruential Random Number (ACORN) generator [1] is straightforward to implement; it has been demonstrated to give rise to sequences with long period which can be proven from theoretical considerations to approximate to uniform distribution on the unit interval in up to *k* dimensions for any given *k* [2, 3]. The theoretical analysis is supported by the results of extensive empirical testing using standard test packages, see for example [4, 5, 6, 7].

ACORN-QRE is a straightforward modification of ACORN which effectively avoids the linearity of the original algorithm, while preserving the uniformity of the modified sequence [8]. It provides a new method for generating one-time pads that are resistant to attack either by current computers or by future computing developments. The pads can use any alphabet (including both binary and alphanumeric) and can be used with a Vernam-type cypher to securely encrypt both files and communications.

We explain how ACORN-QRE works and provide evidence for the claim that the resulting one-time pads are inherently not susceptible to cryptanalysis and will remain secure against foreseeable computing developments, including quantum computers. We address some practical considerations for implementation of the method and provide performance data for encryption and decryption of large binary files using a standard laptop computer.

The ACORN-QRE algorithm is patented in the UK under Patent No. GB2591467 “One-time pad generation” and in the USA under Patent No. 11831751 . The relevant patents are owned by REAMC Limited, 4 Nuthatch Close, Poole, Dorset BH17 7XR, United Kingdom.

VERNAM CYPHERS AND ONE_TIME PADS

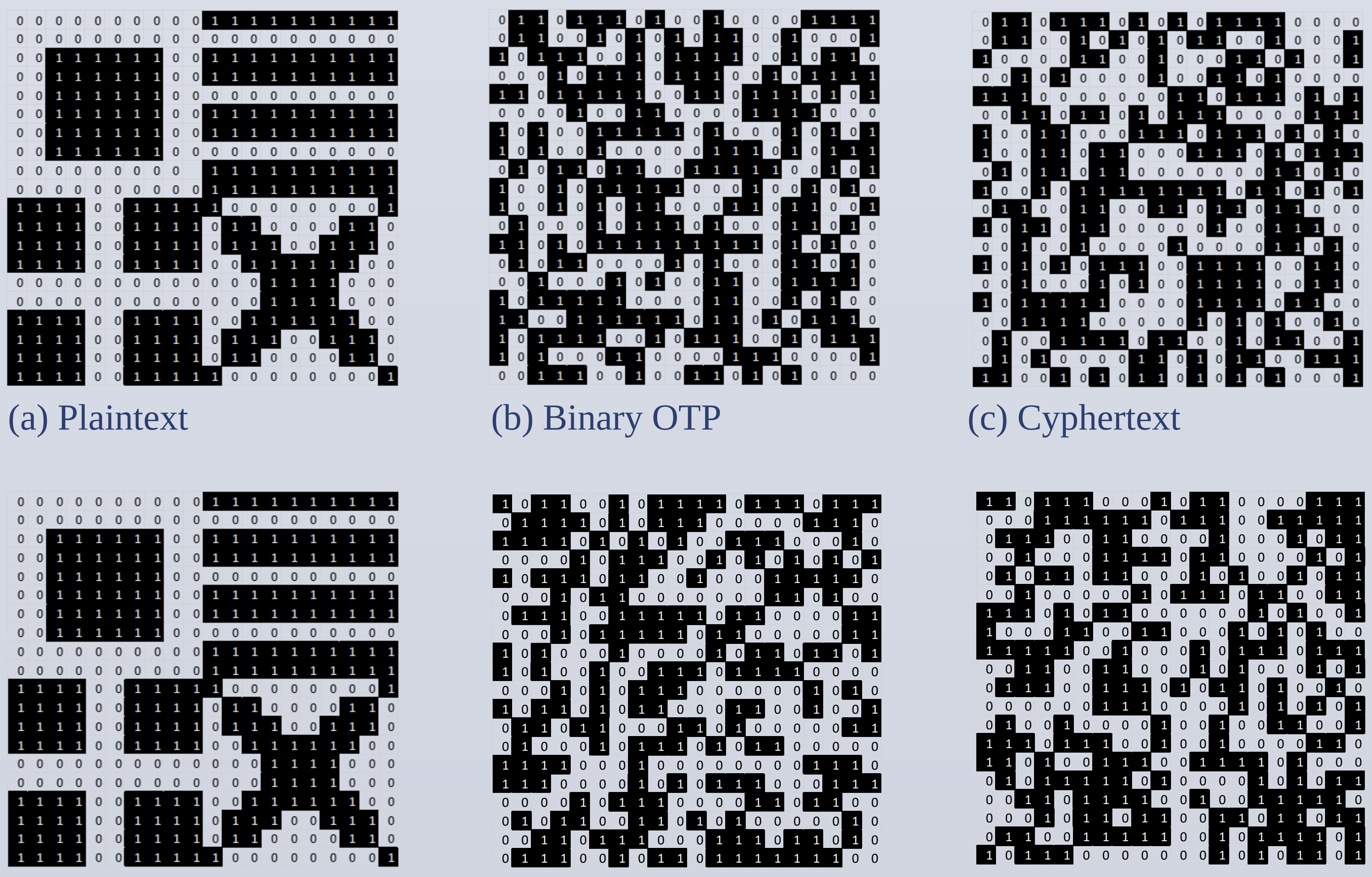
A Vernam cypher or one-time pad (OTP) is an encryption system that turns out to be invulnerable to cryptanalysis and that can therefore not be broken. A ‘plaintext’ (which is to be encrypted for communication to another party) is paired with a random, secret key (known as a ‘one-time pad’ or OTP); each character of the plaintext is combined with the corresponding character of the OTP to give the “cyphertext”, which looks like another random string of characters. If (and only if) the recipient has access to a copy of the OTP then the original plaintext can be retrieved directly from the cyphertext.

Suppose we define an alphabet, consisting of *N* characters together with a one-to-one mapping from the characters in the alphabet onto {0, …, *N*-1}. The alphabet and the mapping can be public information and are assumed known to all parties (including a potential attacker).

- Examples of suitable alphabets might include: Binary, *N*=2, {0, 1}; Octal, *N*=8, {0, 1, 2, …, 7}; Hexadecimal, *N*=16, {0. 1, 2, …, 15}; Alphanumeric, *N*=36, {0, 1, 2, …, 9, A, B, C, …Z}.
- The plaintext is a string of characters; each character in the plaintext must be from the alphabet; on the other hand, not every character from the alphabet need appear in the plaintext.
- The OTP is a random string of terms from the same alphabet that is shared between the two parties but is kept secret from anybody else; the OTP must be at least as long as the plaintext.
- The cyphertext is obtained by combining plaintext and relevant section of the OTP using term-by-term addition (mod *N*). The cyphertext appears as another random string of terms from the alphabet; note that the cyphertext (like the OTP) will include all the characters from the alphabet and they will occur with approximately equal frequency.
- Plaintext can be retrieved from cyphertext by subtraction (mod *N*) of the terms in the OTP. It is impossible to reconstruct plaintext without access to the OTP.
- If alphabet is binary {0,1} then encryption and decryption steps are each equivalent to the XOR (“exclusive or”) operation, so the encryption and decryption are both very efficient.

The idea of encryption using a random one-time pad originated about a hundred years ago and is generally attributed to Gilbert Vernam (from the American Telegraph and Telecommunications Company, AT&T) and Joseph Mauborgne (from the US Army Signal Corps). Some thirty years later, in 1949, Claude Shannon [9] (also a researcher at AT&T) published a proof of conditions for this to be an unbreakable secure encryption method, namely that the key (or one-time pad) should be truly random and at least as large as the plaintext, that sections of the pad should never be reused in whole or in part, and its contents should be kept as a shared secret between the sender and the recipient of the message. In the same article, Shannon also proved that any unbreakable system must share essentially these same characteristics.

OTP ENCRYPTION EXAMPLES (BINARY)



(a) Plaintext (b) Binary OTP (c) Cyphertext

(d) Decrypted (e) Incorrect OTP (f) Incorrect decryption

Cyphertext is obtained by bitwise XOR between plaintext and the binary OTP. It can be decrypted (giving the original plaintext) by a bitwise XOR between cyphertext and the OTP.

If the OTP is (sufficiently) random then it is not possible to distinguish between the OTP and the cyphertext through any mathematical or statistical analysis of the data sets.

Attempts to decrypt using an incorrect random OTP will just give another random-looking result.

ACORN-QRE ALGORITHM

Let *k* be a finite, strictly positive integer. The *k* -th order ACORN generator is defined from an integer modulus *M*, an integer seed Y^0_0 ($0 < Y^0_0 < M$) and a set of *k* integer initial values Y^m_0, $m = 1, ..., k$, ($0 \leq Y^m_0 < M$) by the following equations (where $[Y]_{\mathrm{mod}\ M}$ means remainder on dividing *Y* by *M*)

$$Y^0{}_n = Y^0{}_{n-1} \quad n \geq 1 \ \ (1); \qquad Y^m{}_n = [Y^{m-1}{}_n + Y^m{}_{n-1}]_{\mathrm{mod}M} \quad n \geq 1, m = 1, \dots, k \ \ (2)$$

The Y^k_n can be normalised, dividing by *M* to give X^k_n . Period length is a multiple of *M* while the X^k_n approximate to uniform distribution on the unit interval in up to *k* dimensions, provided a few simple constraints on the initial parameter values are satisfied (modulus $M=2^{\mu}$ where μ=60 or 120; seed Y^0_0 and modulus are relatively prime (for modulus a power of two, requires only that the seed is odd); initial values Y^m_0, $m = 1, ..., k$ can be chosen arbitrarily.

ACORN-QRE is a straightforward modification of ACORN

1. Calculate next ACORN variate Y^k_n and set $A=Y^k_n$; note that *A*, drawn from {0, 1, 2, …, *M*-1}, has μ bits
2. Calculate reduced ACORN variate, *B*, drawn from {0, 1, 2, …, 2^b-1}, by taking leading *b* (<< μ) bits of *A*
3. Let the size of the alphabet be $a(<2^b)$. If the reduced ACORN variate $B \geq a$, discard term and go back to repeat Step 1; else take *B* as the next term in the OTP, and go back to Step 1.

CRYPTOGRAPHIC SECURITY OF ACORN-QRE

Discussion and heuristic arguments to support the following assertions are given in [8] for $M=2^{120}$

- Assertion 1. Given a section of OTP (however long or short) it is impossible to determine initialisation used to generate it other than by a brute-force search of all possible initialisations and the resulting pads.
- Assertion 2. The time required to do a brute force search of all possible initialisations is so long as to make this totally impractical (even allowing for potential improvements in the speed of conventional computing as well as massive parallelisation and potential future developments in quantum computing).
- Assertion 3. Given a relatively short cyphertext of length *p* bits (where $p \leq r$ and where, for order 8 and modulus 2^{120}, *r*=1079 bits) encrypted using ACORN-QRE, there are 2^p candidate messages, each of which implies a particular section of OTP. Given a longer cyphertext of length *q* bits (*q*>*r*) which has been encrypted using ACORN-QRE, there are 2^q possible messages and 2^r different possible OTP, each of which would imply a corresponding candidate message. Irrespective of length of cyphertext, there is no practical way of identifying any candidate message as being more or less likely to be the true message than any other.
- Assertion 4. The time required to encrypt or decrypt a Megabyte of data (equal to 2^{23} bits, since one byte is equal to 8 bits) using the ACORN-QRE algorithm on a current (2023) standard processor was estimated to be no more than a few seconds (some actual performance data below; significantly faster than this estimate).
- Assertion 5. The period length of an ACORN-QRE sequence is so long that there is no reason to be concerned about ever exhausting an OTP generated using this method.
- Assertion 6. The number of ACORN-QRE sequences with order *k*=8 and modulus 2^{120} that are available to choose from is (vastly) more than enough for a different pad of length at least 2^{120} to be selected for communication between every pair of individuals in the world without any duplication.

EXAMPLE IMPLEMENTATION

We now have an ACORN-QRE example implementation written in Fortran (October 2023), which can be demonstrated or made available to share by arrangement. Uses alphabet size 256 {0, 1, 2, …, 255} to encrypt any binary file (including pdf, word, excel, text, zip, etc) of size up to at least 10Mb.

- Performance data on a standard (2023) laptop processor for encrypting or decrypting a 10Mb file:
  Reading input file 0.25s; generating OTP 0.55s; encryption/decryption 0.01s; writing results 0.25s.
- Have identified algorithmic refinements that offer further performance improvements for the OTP generation.

CONCLUSIONS

ACORN-QRE provides a family of secure encryption algorithms that will remain secure against possible future developments in both conventional and quantum computers.

Files encrypted using this method can be safely transmitted over secure or insecure communications channels or left for collection on publicly accessible web-sites without fear of their contents being deciphered and read by any attacker, including commercial rivals, bad actors and members of security services from any country, either now or at any time in the future.

Only somebody who knows the appropriate key will be able to decrypt and read the contents of the file.

ACORN-QRE provides what is effectively the same level of security as provided by a randomly generated OTP, while avoiding some crucial drawbacks/limitations

- A randomly generated OTP still needs testing to ensure randomness. For pads generated by ACORN-QRE no such testing is needed because the algorithm can be proved to give the required randomness properties for all initialisations provided certain straightforward rules are followed.
- To use a randomly generated OTP the entire pad (at least as large as the message) must be shared securely with intended recipient of the message. With ACORN-QRE, we only need to share the key securely with the recipient; key length (typically a few thousand bits) is much shorter than the length of the resulting pad (typically of the order 2^{120} bits), and is much easier to communicate securely.
- Should it turn out that the pad length, the number of different pads to choose from, or the randomness of the pads is insufficient for some future requirement, ACORN-QRE scales in a natural way: increasing modulus to 2^{240} increases time needed to generate each variate by a factor of two, while increasing size of solution space (and time for brute force search) by a factor 2^{120} and further improving randomness of resulting OTPs.

REFERENCES

NOTE: Link for download of REAMC Reports available at https://www.reamc-limited.com/Publications

[1] R.S. Wikramaratna, ACORN - A New Method for Generating Sequences of Uniformly Distributed Pseudo-random Numbers, *J. Comput. Phys.*, **83**, pp16-31, 1989.

[2] R.S. Wikramaratna, The Additive Congruential Random Number Generator – A Special Case of a Multiple Recursive Generator, *J. Comput. and Appl. Mathematics*, **261**, pp371–387, 2008. [doi: 10.1016/j.cam.2007.05.018].

[3] R.S. Wikramaratna, Theoretical and Empirical Convergence Results for Additive Congruential Random Number Generators, *J. Comput. Appl. Math.*, **233**, pp2302-2311, 2010. [doi: 10.1016/j.cam.2009.10.015].

[4] R.S. Wikramaratna, Statistical Performance of Additive Congruential Random Number Generators Part 1 - Results of Testing Some Specific Seed Values, REAMC Report-002, November 2020. REAMC Limited, UK.

[5] R.S. Wikramaratna, Statistical Performance of Additive Congruential Random Number Generators Part 2 - Conjectures Concerning Seed Values Chosen Uniformly at Random, REAMC Report-003, Issue 2, August 2021, REAMC Limited, UK.

[6] R.S. Wikramaratna, Two Conjectures on Statistical Performance of ACORN Generators: Evidence for Orders 11 - 15, REAMC Report-004, August 2021, REAMC Limited, UK.

[7] R.S. Wikramaratna, Statistical Performance of ACORN Generators: Evidence for Selected Orders 16 – 101, REAMC Report-006, May 2023, REAMC Limited, UK.

[8] 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, REAMC Limited, UK. [Link for download also available on Cryptology ePrint Archive https://eprint.iacr.org/]

[9] 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]

Poster presented at the 19th IMA Conference on Cryptography and Coding, Royal Holloway College, London, December 12th-14th 2023