Randomness Rising

The Decisive Resource in the Emerging Cyber Reality

Gideon Samid
Department of Electrical Engineering and Computer Science
Case Western Reserve University, Cleveland, OH
BitMint, LLC
Gideon@BitMint.com

Abstract High quality, large quantities of well-distributed, fast and effective randomness is rising to claim the pivotal role in the emerging cyber reality. Randomness is the fundamental equalizer that creates a level playing field to the degree that its efficient use will become the critical winning factor, computational power not withstanding. We must adapt all our cyber protocols, and pay special attention to key cryptographic methods, to leverage this strategic turn. Our foes are expected to arm themselves with randomness-powered defense that we would be unable to crack, neither with brute force, nor with mathematical advantage. Rising randomness will also change the privacy landscape and pose new law-enforcement challenges. In the new paradigm users will determine the level of security of their communication (by determining how much randomness to use) which is strategically different from today when cipher designers and builders dictate security, and are susceptible to government pressure to leave open a back door . The new crop of ciphers (Trans-Vernam ciphers) will be so simple that they offer no risk of mathematical shortcut, while they are designed to handle large as desired quantities of randomness. The resultant security starts at Vernam-grade (perfect secrecy, for small amount of plaintext), slips down to equivocation (more than one plausible plaintext), as more plaintext is processed, and finally, comes down to intractability (which remains quite flat for growing amounts of processed plaintext). These new ciphers give the weak party a credible defense that changes the balance of power on many levels. This vision has very few unequivocal indications on the ground, as yet, and hence it is quite likely for it to be ignored by our cyber leaders, if the saying about the generals who are prepared for the last war is applicable here.

I. INTRODUCTION

Crude oil extracted from the earth has been routinely used in lighting fixtures, furnaces, and road paving, but when the combustion engine was invented, oil quickly turned to be a critical life resource. A perfect analogy to randomness today, routinely used in virtually all cryptographic devices: limited, well known quantities, of varied quality. But that is changing on account of three merging developments:

1. Modern technology brought about the collapse of the cost of memory, as well as its size, while reliability is nearly perfect.

2. Complexity-claiming algorithms are increasingly considered too risky.

3. The Internet-of-Things becomes crypto-active, and is inconsistent with modern ciphers.

Storing large quantities of randomness is cheap, easy, and convenient. An ordinary 65 gigabyte micro SD will have enough randomness to encrypt the entire Encyclopedia Britannica some 25 times – and doing so with mathematical secrecy.

Complexity-claiming algorithms have lost their luster. They are often viewed as favoring the cryptographic powerhouses, if not an out right trap for the smaller user. The New York Times [Perlroth 2013] and others, have reported that the NSA successfully leans on crypto providers to leave a back-door open for government business.

The looming specter of quantum computing is a threat, which becomes more and more difficult to ignore. The executive summary of the Dagstuhl Seminar [Mosca 2015] states: "*It is known that quantum algorithms exist that jeopardize the security of most of our widely-deployed cryptosystems, including RSA and Elliptic Curve Cryptography. It is also known that advances in quantum hardware implementations are making it increasingly likely that large-scale quantum computers will be built in the near future that can implement these algorithms and devastate most of the world's cryptographic infrastructure*."

The more complex an algorithm, the greater the chance for a faulty implementation, which can be exploited by a canny adversary, even without challenging the algorithmic integrity of the cipher. Schneier [Schneier 1997] states: "*Present-day computer security is a house of cards; it may stand for now, but it can't last. Many insecure products have not yet been broken because they are still in their infancy. But when these products are widely used, they will become tempting targets for criminals*"

Claude Shannon [Shannon 1949] has shown that any cipher where the key is smaller than the plaintext is not offering mathematical secrecy. And although all mainstay ciphers use smaller (Shannon insecure) keys, the casual

reader will hardly discern it, as terms like “provingly secure”, and “computationally secure” adorn the modern crypto products. At best a security proof will show that the referenced cipher is as hard to crack as a well-known problem, which successfully sustained years of cryptanalytic attacks [Aggrawal 2009]. The most commonly used such anchor problem is factoring of large numbers. The literature features successful practical factoring of numbers of size of 220-230 decimal digits [Kleinjung 2009, Bai 2016] . Even in light of these published advances, the current standard of 1000 bits RSA key is quite shaky. Nigel Smart offers a stark warning to modern cryptography: “*At some point in the future we should expect our system to become broken, either through an improvement in computing power or an algorithmic breakthrough*” [Smart 2016, Chap 5]

Alas, when one considers both motivation and resources, then these academic efforts pale in comparison with the hidden, unpublished effort that is sizzling in the secret labs of national security agencies around the world. As all players attempt to crack the prevailing ciphers, they are fully aware that the other side might have cracked them already, and this built-up unease invigorates the prospect of rising randomness: a crop of alternative ciphers, building security, not on algorithmic complexity, but on a rich supply of randomness.

The Internet of Things stands to claim the lion share of crypto activity, and many of those "things" operate on battery power, which drains too fast with today's heavy computational algorithms. Millions of those interconnected ‘things’ are very cheap devices for which today’s crypto cost cannot be justified, yet broadcasting their measurements, or controlling them must be protected. These "things" can easily and cheaply be associated with a large volume of randomness which will allow for fast, simple and economical algorithms to insure reliable security, not susceptible to the mathematical advantage of the leading players in the field.

These three trends point to a future where randomness is rising.

A wave of new ciphers is in the offing where high-quality randomness is lavishly used in secret quantities designed to neuter even the much feared "brute force" attack, as well as withstand the coming “earthquake” of quantum computing, and resist the onslaught of open-ended, unmatched adversarial smarts. Ciphers that will prospectively deploy large amounts of randomness will wipe away the edge of superior intellect, as well as the edge of faster and more efficient computing.

A cyber war calls for communication among non-strangers and hence symmetric cryptography is mainstay. All mainstay ciphers in common use today conform to the paradigm of using a small, known-size (or several known sizes), random key, and may be a small nonce to boot. These ciphers feature algorithmic complexity for which no mathematical shortcut was published, and all known computers will crack it only in a period of time too long to be of any consequence.

As the prospect of a global vicious cyber war looms larger, the working assumption of the warriors is that these fair-day ciphers described above may not be robust enough for their wartime purpose. Mathematical complexity in principle has not been mathematically guaranteed, although theoreticians are very busy searching for such guarantee. We can prove that certain mathematical objectives cannot be reached (e.g. general solution to a quintic function), but not prove that a multi-step algorithm that is based on detecting a pattern within data cannot be improved upon, with probabilistic methods further spewing solution uncertainty. Moreover, computational objectives which are proven to be impossible in the general case, are normally quite possible in a large subset (even a majority) of cases. There are infinite instances of polynomials of degree five, and higher that can be solved by a general formula for their class, limiting the practical significance of Abel's proof.

Given the stakes in an all out cyber war, or in a wide-ranging kinetic war intimately supported by a cyber war, the parties preparing for that war will increasingly harbor unease about the class of alleged-complexity symmetric ciphers, and will be turning to randomness as a strategic asset.

High quality randomness is as rare as high quality crude oil. While this is more a literary statement than a mathematical phrase, the reality is that one needs to go as far as monitoring a nuclear phenomenon, like a rate of radiation flux emerging from a long half life radioactive material, to build a "purely random" sequence. A new contraption is based on shootig a photon into a half way mirror. These delicate sources are unwieldy, not very conversant, and not of scale. There are numerous "white noise" contraptions, which are non-algorithmic, but are not "pure", and any "non purity" is a hook for cryptanalysts. Third category is the algorithmic makers of randomness, commonly known as pseudo random number generators (PRNG). They are as vulnerable as the algorithmic complexity ciphers they try to supplant. The New York Times [Perlroth 2013] exposed the efforts of the government to compel crypto providers to use faulty PRNG which the NSA can crack (The dual elliptic curve deterministic random number generator). So to harvest high quality randomness in sufficient quantities is a challenge. To handle it, once harvested, is another challenge. In a cyber war randomness has to be properly distributed among the troops, and their integrity must be carefully safeguarded.

We don't yet have good and convenient randomness management protocols. The brute force use of randomness is via the 1917 Vernam cipher [Vernam 1918] which some decades later Claude Shannon has proven to be mathematically secure [Shannon 1949]. Theoretically, a cyber army properly equipped with enough randomness may safeguard the integrity of its data assets by rigorous application of Vernam. Alas, not only is it very wasteful in terms of randomness resources, its use protocols, especially with respect to multi party communications are very taxing and prone to errors. So we must re-think randomness management and randomness handling, and use effective protocols to accommodate the level of randomness reserves versus security needs.

The coming cyber war will be largely carried out with unanimated "things" exploiting the emerging tsunami of the Internet of Things. Many of the 60 billion "things" or so that would be fair game in the war, will have to communicate with the same security expected of human resources. Only that a large proportions of those warrior "things" is small, even very small, and powered by limited batteries that must preserve power for the duration of the war. These battery-operated devices cannot undertake the computational heavy lifting required by today's leading ciphers. In reality, many 'smart things' are remotely controlled without any encryption, easy pray for the malicious attacker. Meanwhile, memory has become cheap, small-size, and easy. A tiny micro SD may contain over 100 gigabytes, and placed in a bee-size drone operated on a tiny solar panel. The working cipher for that drone will have to use simple computational procedures and rely for security on the large amount of randomness on it.

Modern societies allow for strangers to meet in cyber space, and quickly establish a private communication channel for confidential talk, play, pay or business. Part of the modern Cyber War will be to disrupt these connections. Cryptography between and among strangers also relies on intractability-generating algorithms, and hence this category is equally susceptible to stubborn hidden persistent cryptanalytic attacks. Any success in breaching RSA, ECC or alike will be fiercely kept in secret to preserve its benefit. Recognizing this vulnerability, modern cyber actors will shift their confidential communication channel tools from today's intractability sources to tomorrow probability sources, combined with randomness. Probability procedure, like the original Ralph Merkle procedure, [Merkle 1978] ,buy its users only a limited time of confidentiality, and hence subsequent algorithms will have to leverage this limited time privacy to durable privacy. Probability succumbs to unexpectedly powerful computers, but is immunized against surprise mathematical smarts.

Our civil order is managed through the ingenuous invention of money. Society moves its members through financial incentives; people get other people to work for them, and serve them by simply paying them. And it so happens that money moves aggressively into cyberspace. Digital money will soon be payable between humans, between humans and 'things' and between 'things and things'. Cyber criminals will naturally try to counterfeit and steal digital money. Here too, the best protection for digital money is randomness galore. [Samid 2014].

A. How Soon?

This thesis envisions a future when randomness becomes "cyber oil", the critical resource that powers up future cyber engines. The question then arises: how soon?

Clearly today (2018), this is not the reality in the field. Virtually all of cryptography, for all purposes, is based on ciphers, which use small keys of fixed size, and which are unable to increase the key size too much because of exponential computational burden. So when is this vision of 'randomness rising' going to actually happen, if at all?

As more and more of our activities steadily migrate into cyber space, more and more nation states and other powerful organizations take notice, and realize that their very well being hinges on cyber integrity. Looking to minimize their risks, all players will be steadily guided to the safe haven of randomness. By the nature of things the arena is full of many small fish and a few big fish. The small fish in the pond are very reluctant to base their welfare and survival on ciphers issued, managed, and authorized by the big players, suspecting that these cryptographic tools have access hooks, and are no defense against their prospective adversaries. Looking for an alternative, there seems to be only one option in sight: Trans Vernam Ciphers, as defined ahead: ciphers that operate on at-will size randomness and that can be gauged as to the level of security they provide, up to Vernam perfect security. Unlike oil, Randomness cannot be boycotted, and it neutralizes the advantage of the bigger, smarter adversary.

II. Randomness-Powered Variable Security Paradigm

The current security paradigm is on a collision course with ultra fast computing machines, and advanced cryptanalytic methodologies. Its characteristic, fixed size, small key becomes a productive target to ever-faster brute force engines, and ever more sophisticated adversarial mathematical insight. As cryptography has risen to become the win-or-lose component of the future wars, this looming risk is growing more unacceptable by the day. Serious consumers of high-level security have often expressed their doubt as to the efficacy of the most common, most popular symmetric and asymmetric ciphers. And they are talking about financial communication in peacetime. Much more so for a country or a society fighting to maintain its civil order, and win a fierce global war.

This pending collision is inherent in the very paradigm of today's cryptographic tools. The harm of this collision can be avoided by switching to another paradigm. The alternative paradigm is constructed as a user-determined randomness protection immunized against a smarter adversary.

The idea is to replace the current line-up of complexity-building algorithms with highly simplified alternatives. Why? Complexity-building algorithms are effective only against an attacker who does not exceed the mathematical insight of the designer. The history of math and science in general is a sequence of first regarding a mathematical objective or a challenge of science as daunting and complex, while gradually, gaining more and more relevant insight and with it identifying an elegant simplicity in exactly the same situation that looked so complex before.

One may even use complexity as a metric for intelligence: the greater the complexity one sees as simplicity, the higher one's intelligence. Theoretical mathematicians have been working hard trying to prove that certain apparent complexity cannot be simplified. These efforts are unproductive so far, but even if they will be successful, they relate only to the theoretical question of complexity in worst possible case, while in practical cyber security we are more interested in the common case, even in the not so common case, as long as it is not negligible in probability. And the more complex an algorithm, the more opportunity it presents for mathematical shortcuts, and hence the current slate of ciphers, symmetric and asymmetric, is at ever greater risk before the ever more formidable cryptanalytic shops popping around the world, as more countries realize that their sheer survival will turn on their cyber war weaponry.

So we are looking at a shift from complexity building algorithms to simplicity wielding algorithms: algorithms that are so simple that they live no room for any computational short cut, no matter how smart the adversary.

And since the algorithms will be simple, the security will have to come from a different source. That source is randomness. And unlike the randomness of today's paradigms, which is limited, of known quantity, and participating in a cryptographic procedure of fixed measure of security -- the new paradigm will feature randomness of varied and secret quantity, where said quantity is determined by the user per case, and also said quantity determines the security of the encrypted message. This means that the users, and not the cipher designer, will determine the level of security applied to their data. The open-ended nature of the consumed randomness will neuter the last resort measure of brute force cryptanalysis. The latter only works over a known, sufficiently small size randomness.

A cryptographic paradigm calling for “as needed” consumption of randomness, is inherently approaching the mathematical secrecy offered by Vernam cipher, in which case all cryptanalytic efforts are futile. Alas, Vernam cipher per se is extremely unwieldy and uncomfortable, so much so that its use in a cyber war appears prohibitive. Albeit, when one examines Shannon proof of mathematical secrecy one notices that it is not limited to Vernam per se, it is limited by the constrain that the size of key should not be smaller than the size of the encrypted plaintext. This opens the door to paradigms in which a very large key (lots of randomness) is used to encrypt successive series of plaintext messages going back and forth. As long as the total bit count of the encrypted messages is smaller than the randomness used in the key, then the correspondents will enjoy complete mathematical secrecy. The first crop of “randomness rising” ciphers do just that.

We envision, therefore the coming cyber war where combatants are loaded with sufficient quantities of high quality randomness, and consume it as the war progresses. The combatants themselves (the users) decide for each case, and any circumstances how much randomness to use.

III. TRANS-VERNAM CIPHERS

We define trans-Vernam ciphers as ciphers, which effectively operate with any desired level of randomness (key), such that their security is a rising monotonic function with the amount of randomness used, and is asymptotically coincident with Vernam's perfect secrecy.

The term "effectively operate" implies that the computational burden is polynomial with the size of the randomness. For most of the prevailing ciphers today this is not the case. Computational burden is typically exponential with the size of the key.

Basically, a Trans-Vernam Cipher (TVC) is changing the source of security from algorithmic complexity to crude randomness. And that is for several reasons: (i) algorithmic complexity erodes at an unpredictable rate, while a measure of high-quality randomness is by its definition not vulnerable to any superior intelligence, and its cryptanalytic resistance is directly proportioned to its quantity, (ii) ciphers based on algorithmic complexity offer a fixed measure of security, which their user cannot further tailor. So naturally some use is overuse (too much security investment), and some use is underuse (too little security investment). The user is locked to whatever measure offered by the deployed algorithm. By contrast a trans-Vernam Cipher has, what can be described as, 'neutral algorithm' and the security is determined by the quality and quantity of the used randomness, which is the user's choice per case. So the user can choose more randomness for high value secrets, and less randomness for low value secrets; (iii) Speed and energy: the computational burden for algorithmic ciphers is high, with great energy demand, and the speed is relatively low. By contrast. a TVC cipher is fast and enjoys low energy consumption.

Nominal ciphers offer a fixed security expressed in the intractability they offer to their cryptanalyst. This security is largely independent of the amount of plaintext processed, and is limited by the brute force strategy that is guaranteed to crack the cipher. More efficient cryptanalysis may happen on account of unexpected highly efficient computing machines, or on account of unexpected mathematical insight. From a purely cryptographic standpoint there is no limit on the amount of text that is used by a given cipher over the same key, except to the extent that more will be compromised should the key be exposed. That means that if the intractability wall holds, the amount of text can be as large as desired.

By contrast, Trans-Vernam ciphers using a fixed key will offer an eroding level of security commensurate with the amount of plaintext used over the same key. Why then even think of replacing nominal fixed-security ciphers with TVC, which offer less and less security as more plaintext is processed? The reason is simple: the initial security offered by TVC, namely when the amount of plaintext is small, is higher than any security offered by nominal ciphers. And what is more, the growing loss of security, as the amount of plaintext grows is well gauged, and will rationally figure out into the user's risk analysis. While nominal ciphers offer a fixed intractability, TVC first offer perfect mathematical secrecy (Vernam security), then slide into "equivocation security", and as more and more plaintext is coming through, the resultant security is effected through intractability. And of course, once the key is changed, the security readily jumps to Vernam, from there to Equivocation grade, and finally to intractability protection. We will see later that TVC keys may be replenished in an "add-on" mode where the used key is combined with new key material. Equivocation security is defined as the case where an infinitely smart and omnipotent cryptanalyst is at most facing two or more plausible plaintexts without having any means for deciding which is the plaintext that was actually used. Nominal degree of equivocation is measured by the count of plaintext options above some threshold of plausibility. Albeit, *functional equivocation* is more intricate, and less objective: it measures the "interpretation span" per case. For example: If the cryptanalyst faces 4 plausible plaintexts like: "we shall attack at 6pm", "we shall attack at 6:30pm", "we shall attack at 6:45pm" and "we shall attack at 7:00pm", then his equivocation will be of a lesser degree compared to facing two options: "we shall attack from the north" and "we shall attack from the south". When sufficient plaintext is going through a Trans Vernam Cipher, equivocation fades away, and plain old intractability is all that is left.

The concept of a unicity length is akin to this analysis, and in principle there is nothing new here, except in the actual figures. If Vernam (perfect) security extends only to a small measure of plaintext, and equivocation dies down soon after, in terms of plaintext processed, then there is little use for a TVC. The novelty is in finding ciphers that can offer a slow deterioration of equivocation and a similar slow deterioration of intractability. The Vernam range has been fixed by Claude Shannon: as soon as the plaintext is one bit larger than the key, mathematical secrecy is lost, and equivocation kicks in. The challenge is to create a cipher where equivocation deteriorates slowly with the amount of the plaintext, and similarly for the intractability. We will discuss ahead some sample ciphers so designed.

The simplest TVC is a slightly enhanced Vernam cipher. Given a key of size k bits, as long as the size of the plaintext (p) is smaller or equal to n ($p \leq k$), the ciphertext is mathematically secure. For p larger, but close to k, there is no longer mathematical security but equivocation kicks in. In the simple case where the key is reused, (p=2k) then asymptotically for $p \to \infty$ equivocation evaporates. Yet, one can devise better ways for using the k key bits to encrypt a $p > k$ plaintext.

Since a TVC can operate with very large keys without prohibitive computation, it is a serious question for the cryptanalyst as to how much key material was used. Clearly if the key is of sufficient amount compared to the plaintext then all cryptanalytic efforts are futile and wasteful. The situation is a bit better for the cryptanalyst at the equivocation zone, and more hopeful in the intractability zone.

IV. SUMMARY

This paper points out a strategic turn in cyber security where the power will be shifting from a few technology providers to the multitude of users who will decide per case how much security to use for which occasion. The users will determine the level of security for their use by determining the amount of randomness allocated for safeguarding their data. They will use a new generation of algorithms, called Trans-Vernam Ciphers, (TVC), which are immunized against a mathematical shortcut and which process any amount of selected randomness with high operational speed, and very low energy consumption.

In this new paradigm randomness will be rising to become 'cyber-oil'. Much as crude oil which for centuries was used for heating and lighting, has overnight catapulted to fuel combustion engines and revolutionize society, so today's randomness which is used in small quantities will overnight become the fuel that powers cyber security engines, and in that, levels the playing field: randomness eliminates the prevailing big gaps between the large cyber security power houses, and the little players; it wipes out the strategic gap both in computing speed, and in mathematical insight. It dictates a completely different battlefield for the coming cyber war -- let us not be caught off guard!

This new randomness-rising paradigm will imply a new era of privacy for the public along with greater challenges for law enforcement and national security concerns. The emerging Internet of Things will quickly embrace the emerging paradigm, since many IOT nodes are battery constrained, but can easily use many gigabytes of randomness.

This vision is way ahead of any clear signs of its inevitability, so disbelievers have lots of ground to stand on. Alas, the coming cyber security war will be won by those who disengaged from the shackles of the present, and are paying due attention to the challenge of grabbing the high ground in the field where the coming cyber war will be raging.

The free cryptographic community (free to develop, implement, publish, and opine) finds itself with

unprecedented responsibility. As we move deeper into cyberspace, we come to realize that we are all data bare, and privacy naked, and we need to put some cryptographic clothes on, to be decent, and constructive in our new and exciting role as patriotic citizens of cyber space.

Reference

Aggarwal 2009: Divesh Aggrawal, Ueli Maurer "Breaking RSA Generically Is Equivalent to Factoring" Eurocrypt 2009 pp 36-53 http://www.mimuw.edu.pl/studia/materialy/notatki/warsztaty-ntacc-2010/Ueli_Maurer_slides_2.pdf

Bai 2016: Shi Bai, Pierrick Gaudry, Alexander Kruppa, Emmanuel Thom´e, Paul Zimmermann. "Factorisation of RSA-220 with CADO-NFS". May 2016". https://hal.inria.fr/hal-01315738

Blum 1984: "How to Generate Cryptographically Strong Sequences of Pseudo Random Bits", M. Blum, S. Micali, SIAM Jr. of Computing, Vol 13, pages 850-864.

Canetti 2006: "Deniable Encryption" Rein Canetti, Cynthia Dwork, Moni Naor, Rafail Ostrovsky CRYPTO '97Volume 1294 of the series Lecture Notes in Computer Science pp 90-104Date: 17 May 2006

Chaitin 1987: "Algorithmic Information Theory" Chaitin G. J. Cambridge University Press.

Checkoway 2014: Stephen Checkoway et al "On the Practical Exploitability of Dual EC in TLS Implementations" http://dualec.org/DualECTLS.pdf

Diffie 1976: "New Directions in Cryptography" W. Diffie M. E. Hellman IEEE Transactions on Information Theory v. IT-22 n. 6 Nov 1976 pp644-654

Fehr 2016: "Quantum Authentication and Encryption with Key Recycling Or: How to Re-use a One-Time Pad Even if P =NP — Safely & Feasibly" Serge Fehr, Louis Salvail 18 October 2016, Cornell University Library https://arxiv.org/pdf/1610.05614.pdf

Goldwasser 1984: "Probabilistic Encryption" Goldwasser, Micali, Jr. of Computer and System Science, Vol 28, No 2, pages 270-299

Hellman 1977: "An extension of the Shannon theory approach to cryptography". IEEE Transactions on Information Theory, V. 23 , 3 1977 , pp. 289 - 294

Hirschfeld 2007: "Algorithmic Randomness and Complexity" School of Mathematics and Computing Sciences, Downey, R, Hirschfeld, D. Victoria Univ. Wellington, New Zealand. http://www-2.dc.uba.ar/materias/azar/bibliografia/Downey2010AlgorithmicRandomness.pdf

Hughes 2016: "STRENGTHENING THE SECURITY FOUNDATION OF CRYPTOGRAPHY WITH WHITEWOOD'S QUANTUM-POWERED ENTROPY ENGINE" Richard Hughes, Jane Nordhold http://www.whitewoodencryption.com/wp-content/uploads/2016/02/Strengthening_the_Security_Foundation.pdf

Kamel 2016: "Towards Securing Low-Power Digital Circuit with Ultra-Low-Voltage Vdd Randomizers" ICTEAM/ELEN, Université catholique de Louvain, Belgium. http://perso.uclouvain.be/fstandae/PUBLIS/176.pdf

Kerckhoffs 1883: Auguste Kerckhoffs, « La cryptographie militaire », Journal des sciences militaires, vol. IX, pp. 5–38, Janvier 1883, pp. 161–191, Février 1883.

Kleinjung 2009: Thorsten Kleinjung et al "Factorization of 768Bit RSA Modulus" Crypto 2010 pp333-350 http://download.springer.com/static/pdf/183/chp%253A10.1007%252F978-3-642-14623-7_18.pdf

Mate 2015: "Survey on Cryptographic Obfuscation" Ma´t´e Horva´th 9 Oct 2015 International Association of Cryptology Research, ePrint Archive https://eprint.iacr.org/2015/412

Merkle 1978: "Secure Communications over Insecure Channels" R. C. Merkle Communications of the ACM v.21 n.4 pp294-299

Mosca 2015: "Quantum Cryptanalysis" Report from Dagstuhl Seminar 15371 Edited by Michele Mosca , Martin Roetteler , Nicolas Sendrier , and Rainer Steinwandt http://drops.dagstuhl.de/opus/volltexte/2016/5682/pdf/dagrep_v005_i009_p001_s15371.pdf

Nies 2008: "Computability and randomness" Niels A. The University of Auckland, Clarendon, Oxford, UK

Perlroth 2013: Perlroth Nicole, et el "N.S.A. Able to Foil Basic Safeguards of Privacy on Web" The New York Times, Sept 5, 2013 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0

Samid 2001A: "Re-dividing Complexity between Algorithms and Keys" G. Samid Progress in Cryptology — INDOCRYPT 2001 Volume 2247 of the series Lecture Notes in Computer Science pp 330-338

Samid 2001B: "Anonymity Management: A Blue Print For Newfound Privacy" The Second International Workshop on Information Security Applications (WISA 2001), Seoul, Korea, September 13-14, 2001 (Best Paper Award).

Samid 2001C: "Encryption Sticks (Randomats)" G. Samid ICICS 2001 Third International Conference on Information and Communications Security Xian, China 13-16 November, 2001

Samid 2002: " At-Will Intractability Up to Plaintext Equivocation Achieved via a Cryptographic Key Made As Small, or As Large As Desired - Without Computational Penalty " G. Samid, 2002 International Workshop on CRYPTOLOGY AND NETWORK SECURITY San Francisco, California, USA September 26 -- 28, 2002

Samid 2003A: "Non-Zero Entropy Ciphertexts (Stochastic Decryption): On The Possibility of One-Time-Pad Class Security With Shorter Keys" G. Samid 2003 International Workshop on CRYPTOLOGY AND NETWORK SECURITY (CANS03) Miami, Florida, USA September 24 -- 26, 2003

Samid 2003B: "Intractability Erosion: The Everpresent Threat for Secure Communication" The 7th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2003), July 2003.

Samid 2004: "Denial Cryptography based on Graph Theory", US Patent #6,823,068

Samid 2009: "The Unending Cyber War" DGS Vitco ISBN 0-9635220-4-3 https://www.amazon.com/Unending-Cyberwar-Gideon-Samid/dp/0963522043

Samid 2012: US Patent 8229859: "Bit Currency: Transactional Trust Tools" G. Samid

Samid 2013: "Probability Durable Entropic Advantage" G. Samid US Patent Application 13/954,741

Samid 2014: "The Dawn of Digital Currency" DGS Vitco https://www.amazon.com/Dawn-Digital-Currency-Gideon-Samid/dp/0963522094/ref=asap_bc?ie=UTF8

Samid 2015A: "Equivoe-T: Transposition Equivocation Cryptography" G. Samid 27 May 2015 International Association of Cryptology Research, ePrint Archive https://eprint.iacr.org/2015/510

Samid 2015B: "The Ultimate Transposition Cipher (UTC)" G. Samid 23 Oct 2015 International Association of Cryptology Research, ePrint Archive https://eprint.iacr.org/2015/1033

Samid 2015C: "Tethered Money: Managing Digital Currencies" G. Samid Elsevier, 2015 https://www.amazon.com/Tethered-Money-Managing-Currency-Transactions-ebook/dp/B012FR7I3W/ref=asap_bc?ie=UTF8

Samid 2015D: “Handbook of Digital Currency: How Digital Currencies Will Cascade up to a Global Stable Currency” Elsevier, 2015

Samid 2016A: “Shannon’s Proof of Vernam Unbreakability” G. Samid https://www.youtube.com/watch?v=cVsLW1WddVI

Samid 2016B: “Cyber Passport: Identity Theft Strategic Countermeasure Cryptographic Solutions; Administrative Framework”. G. Samid International Conference on Security and Management (SAM'16) http://worldcomp.ucmss.com/cr/main/papersNew/LFSCSREApapers/SAM6275.pdf

Samid 2016C: “Cryptography of Things: Cryptography Designed for Low Power, Low Maintenance Nodes in the Internet of Things” G. Samid WorldComp-16 July 25-28 Las Vegas, Nevada http://worldcomp.ucmss.com/cr/main/papersNew/LFSCSREApapers/ICM3312.pdf

Samid 2016D: US Patent 9,471,906 “Digital Transactional Procedures & Implements” G. Samid

Samid 2016E: “Celebrating Randomness” G. Samid Digital Transactions Nov 2016, Security Notes

Samid 2016E: “Cryptography of Things (CoT): Enabling Money of Things (MoT), kindling the Internet of Things” G. Samid The 17th International Conference on Internet Computing and Internet of Things, Las Vegas July 2016 https://www.dropbox.com/s/7dc0bgiwlnm7mgb/CoTMoT_Vegas2016_kulam_Samid.pdf?dl=0

Schneier 1997: “WHY CRYPTOGRAPHY IS HARDER THAN IT LOOKS” Counterpane Systems http://www.firstnetsecurity.com/library/counterpane/whycrypto.pdf

Shamir 1981: “On the Generation of Cryptographically Strong Psuedo-Random Sequences” Lecture Notes in Computer Science ; 8th International Colloquium of Automata, Springer-Verlag

Shannon 1949: “Communication Theory of Secrecy Systems” Claude Shannon http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

Smart 2016: “Cryptography Made Simple” Nigel Smart, Springer.

Vernam 1918: Gilbert S. Vernam, US Patent 1310719, 13 September 1918.

Williams 2002: “Introduction to Cryptography” Stallings Williams, http://williamstallings.com/Extras/Security-Notes/lectures/classical.html