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 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 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. This source is 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 procedure 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 (late 2016), 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. Randomness is an available resource, and it neutralizes the advantage of the bigger, smarter adversary. The more imminent, and the more critical the coming cyber war, the faster this envisioned future will materialize.

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 are 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 mere 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 each 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.

A. Security Perspective

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.

We make a clear distinction between symmetrical and asymmetrical cryptography, and will discuss each type separately.

B. Symmetric TVC

Since Vernam is a symmetric cipher, it is natural to start the discussion of Trans Vernam ciphers with respect to symmetric species. Even within the "Vernam zone" of perfect security ($p \leq k$) the actual use is quite inconvenient, especially in the case of group communication. Let t parties share a large enough Vernam key (size k), which they use sequentially as plaintexts are showing up. For the group to properly manage this task, it would be necessary for every party to be fully aware of all the messages that were encrypted with this key, in order to know the exact spot from where to count the next encryption. One shift, in one bit count, creates a complete nonsense at the other end because the key itself is guaranteed to be fully randomized.

Instead, one may opt for a cipher such that when used by a group, any one would be able to write to anyone else without tracking the messages others have been using with the same key, and the same cipher; mindful only of the total extent of the use. We call this the "independent use" property and the cipher "the independent use cipher".

The following section offers some specific published Trans-Vernam ciphers in use today. One would expect a wave of similar TVC specimen to come forth and become the powerful tools for the cyber war of tomorrow. Randomness is rising, and its role in cyber defense is shaping the outcome of the emerging cyber reality.

1) T-Comm: Pre-Shared and AdHoc Randomness Protocol

The simplest symmetric crypto case is the case where Alice and Bob who share a secret, open a confidential line of communication passing through insecure territory. Nominally we would have them share, say, an AES key and

use it until they replace it. Thereby they are vulnerable to an attacker with fast enough brute force tools, or with undisclosed mathematical insight to breach the AES complexity. Using TVC Alice and Bob might resort to T-Comm (T for transposition). In that case Alice and Bob will use a shared secret S of secret size, to create secure communication which begins with Vernam security, deteriorate to equivocation security, and ends up with intractability security -- where the cryptanalyst is clueless as to which security mode he or she is facing since the size of the shared secret S is part of its secrecy. And the cryptanalyst is further clueless as to whether Alice and Bob changed their shared secret and thus have regained Vernam grade security.

The T-Comm protocol is computationally simple and it can readily handle very large size keys. T-Comm is especially of interest because on top of the shared randomness, S, it also uses ad-hoc randomness, *A*, which also changes as often as desired.

The T-Comm Protocol: Alice selects a random bit sequence (nonce), R, and sends it over to Bob. Bob combines R with the shared secret, S, to form a bit sequence, Q = f(S,R). Bob then parcels Q to *t* consecutive non-repeat subsets. Reference [Samid 2016B] describes various ways of doing so. Bob then uses a non-algorithmic "white noise" randomness source to generate a random transposition of the *t* elements that comprise the sequence Q. Applying this *A* randomness, Bob generates a permutation of Q: Q_t = f(Q, *A*), and passes Q_t to Alice. Alice generates Q like Bob, and first she examines Q_t to verify that it is a permutation of Q. If it is not, then either one of them made a mistake, or she is not talking to Bob. If Q and Q_t are permutations of each other then Alice is convinced that it is Bob on the other side of the blind line. Furthermore, Alice now knows what ad-hoc randomness, *A*, Bob has used to transform Q to Q_t. *A* can serve as the basis for Alice and Bob session communication, either as a straight transposition cipher, or as a component in a broader cipher. The off chance that Bob will be able to guess a proper permutation of Q is determined by the size of the shared secret, S, which is the choice of the user.

At any time either party may call for re-application of this so called 'session procedure' and continue to communicate using a different ad-hoc randomness. This is particularly called for each time the parties are mutually silent for a while, and there is a suspicion that an identity theft event got in the middle.

This T-Comm procedure is free from any heavy computation, and will work for small or large size S, R, and Q. We can prove, see [Samid 2016B] that for plaintexts P smaller than S T-Comm offers Vernam security. Above that it offers equivocation, and then gradually it drops to intractability security.

It is noteworthy that while Q_t is exposed and hence $|Q|=|Q_t|$ are exposed too, and the same for R, this does not compromise S which can be larger from both R and Q.

A simple example is to construct Q such that Q=f'(S_h,R), where S_h is a hash of S: S_h = Hash(S, R). In that case even if some n messages have been compromised and all use the same secret S, there exists equivocation as to the plaintext that corresponds to ciphertext n+1.

T-Comm is immunized from brute-force attack, and its intractability defense is determined by the user, not by the cipher designer. By choosing a nonce R of a proper size, the parties will determine the number of permutation elements, t, and with it the per-session brute force search scope for *A* (t!). Once a given *A* is tried, it may project back to an S candidate, which must then be checked against the other plaintexts for which it was used. And since S may be larger then the combined messages used with it, the cryptanalyst remains equivocated.

C. "Walk-in-the-Park" (WaPa) Cipher

This cipher is based on the simple idea that a trip can be described either by listing the visited destinations, or by listing the traveled roads. Anyone with a map can readily translate one description to the other. Without a map any trip with no repeat destinations can be translated from one expression to the other by simply building a map that would render both expressions as describing the same trip. So a trip described as beginning in agreed-upon starting point then visiting destinations: A, B, and C, can be matched with a trip described as beginning at the same starting point then taking roads x, y, and z. The matching map will look like:

MAP = [start] ----x-----[A]------y-------[B]-------z--------[C]

Cryptographically speaking, the destination list may be referred to as the plaintext, P, the list of traveled roads may be viewed as the ciphertext, C, and the map, M, may be regarded as the key that matches the two:

$$C = Enc(P, M); P=Dec(C, M)$$

Similarly to Vernam, WaPa allows for every ciphertext to be matched with a proper size plaintext, and hence, like with Vernam, possession of the ciphertext only reveals the maximum size of the corresponding plaintext, giving no preference to any possible plaintext – mathematical secrecy. See analysis in [Samid 2004, Samid 2002].

The map, or what is more poetically described as the "walking park," is shared by the communicating parties, Alice and Bob. If the map is completely randomized then it must be of a finite size. So, inevitably, if Alice and Bob keep using this "walk in the park" cipher more and more, they, will at some point, have to revisit previously visited destinations. Once that happens then the Vernam grade of the cipher is lost. Initially the cipher will drop into equivocation mode where a given plaintext (list of visited

destinations) could be matched with more than one possible ciphertext (list of traveled roads). As more and more destinations are being revisited (and hence more and more roads too) then equivocation vanishes, and sheer intractability is left to serve as a cryptanalytic wall. Exactly the TVC pattern. Alternatively, a finite size park, will be used as an arithmetic series where the next element is based on the identity of previous elements (e.g the Fibonacci series), and in that case the park may grow indefinitely, but since the fully randomized section is limited, the initial Vernam security eventually deteriorates.

It is noteworthy that the encryption and decryption effort is proportional to the amount of plaintext or ciphertext processed, regardless of the size of the map. By analogy: Walking 10 miles on a straight road takes about as much time as walking the same distance in one's backyard, going round and round. So Alice and Bob can arm themselves with a large as desired randomized park (key) to allow for a lot of plaintext to be encrypted with Vernam security followed by highly equivocated use, and the secret of the size of the park will keep their cryptanalyst in the dark as to whether any cryptanalytic effort is worthwhile or futile.

D. Factorial Transposition Cipher

Transposition may be the oldest and most used cryptographic primitive, but its 'factorial' capacity was never used in a serious way. *t* distinct ordered elements may show up in *t!* (factorial) different ways. And hence a simple transposition cipher over *t* elements which may use a key randomly pulled out of a key space of size *t!* will result in a ciphertext that may be constructed from any choice of the *t!* permutations. And to the extent that two or more of these permutations amount to plausible plaintexts, this simple primitive will frustrate its cryptanalyst with irreducible equivocation. It is important to emphasize that for this equivocation to play, the key space must be of size *t!*, which we will call 'factorial size', and the resultant primitive we will call 'factorial transposition'. The practical reason why such powerful ciphers were not used is simple: *t!* is super exponential, it is a key space of prohibitive dimensions with respect to nominal cryptography today.

Alas, TVC is a perfect environment for factorial transposition. References [Samid 2015A, Samid 2015B] describe a factorial transposition cipher. It's intractability is proportional to the permutation size (the value of *t!*), clearly consistent with the TVC paradigm. Its equivocation can be readily achieved through the use of decoy: Alice and Bob share a permutation key, $k \in K$, defined over any arbitrary number of permutation elements, *t,* up to a value $t_k! = |K|$, where |K| is the size of the permutation key space K. Alice will construct a plaintext string, P, comprised of p transposition elements ($p < t$). She will then concatenate P with another screen to be referred to as decoy, D of size d elements, such that $p+d = t$. The concatenated string, Q, is comprised of $q=p+d =$ t elements.

Applying the shared secret, k, Alice will transpose Q to $Q_t = T(Q, k)$ and send Q_t over to Bob. Bob will use the shared secret k to reverse Q_t to Q. He will then separate Q to the plaintext P and the decoy D, and be in the possession of P.

The decoy D may be so constructed that a cryptanalysts analyzing Q_t will not be able to unequivocally determine which $k \in K$ was used because certain mixtures of P'+D' such that $P' \neq P$ and $D' \neq D$, will make as much sense as P and D, and the fact that the transposition is factorial keeps all plausible combinations as plausible as they were before the capture of the ciphertext. Reference [Samid 2015B] presents various ways to construct D.

By way of illustration consider a plaintext P ="We Shall Attack from the North". Let it be parsed word-wise, and then define a decoy, D = "* South East West". The concatenated Q = P + D = P || D is comprised of 10 words, which requires a key space of 10! =3,628,800, from which a single key is drawn uniformly to create Q_t, say:

$$Q_t = \text{"South Attack * East the We North Shall West"}$$

The intended recipient will reverse-transpose Q_t to Q, ignore whatever is written right of the "*" sign, and correctly interpret the plaintext. A cryptanalyst will clearly find four plaintext candidates, each of which could have been transposed to Q_t, but none of the four has any mathematical preference over the others: equivocation.

Factorial Transposition can also be extended to achieve Vernam security: Let P be an arbitrary plaintext comprised of p bits. We shall construct a decoy D as follows: $D = P \oplus \{1\}^n$. D will then be comprised of p bits, and the resultant Q = P + D will be comprised of 2p bits, p of them of identity "1", and the other p bits of identity "0". Let the parties use a factorial transposition cipher of key space, $|K| = 2^{2n}$ and draw therefrom a random choice with which to transpose Q to Q_t. The intended readers would readily reverse-transpose Q_t into Q, discard the p rightmost bits in Q, and remain in possession of P. Alas, by construction each of the 2^n possibilities for P (all strings of length p bits) will be a possible plaintext candidate, a homomorphic relationship with Vernam.

E. Asymmetric Ciphers

Asymmetric cryptography is the cornerstone of the global village, allowing any two strangers to forge a confidential channel of communication. In the town square, a chance meeting may result in two people whispering secrets to each other; in cyber square this happens via asymmetric cryptography. It has become the prime target of a strategic cyber warrior: to be able to disrupt this ad-hoc confidentiality in the enemy territory.

It turns out that asymmetric cryptography is based on a mathematical concept known as "one way function". "Onewayness" is not mathematically proven, and like its symmetric counterparts is susceptible to faster computers on

one hand, and greater mathematical insight on the other hand. Consequently it is not a trustworthy device in an all out, high-stakes cyber war. Randomness to the rescue.

The impressive intellectual feat to allow two strangers to forge privacy in a hostile world where adversaries listen in to any communication, has been first achieved by Ralph Merkle on the basis of sheer randomness. The Merkle solution [Merkle 1978] was a bit unwieldy and it was soon replaced by Diffie-Hellman and others [Diffie 1976] who switched from reliable but tedious randomness to unproven, but convenient one-way functions. It is time to revisit Ralph Merkle and offer a suite of asymmetric ciphers in his spirit. One way to do it, based on the "birthday principle" is presented below.

1) The Birthday Randomness Cipher

The well known "birthday paradox" may be expressed in a counter-intuitive result that when Alice and Bob randomly and secretly choose $\sqrt{n}$ items from an n-items set, they have a 50% chance to have selected at least one item in common. We may offer Alice and Bob an efficient procedure to determine if they indeed have selected an item in common, and if so, which is it. If the answer is in the negative, then they try again, and repeat until they succeed, at which point that common selection will serve as a shared secret, which Eve, the eavesdropper, will eventually identify by analyzing the shared-item determination procedure vis-à-vis the known selection set. Since Eve does not know either Alice's selection, nor Bob's selection, she has to test the various options, on average, through 0.5n possibilities, which will take her more time to determine the shared selection (compared to Alice and Bob). It's that time advantage that Alice and Bob can use to create a more durable shared secret. Alice and Bob may determine the n-items set, ad-hoc, just when it is needed. The items may be well-designed mathematical constructs, featuring any number of desired properties, where each property may assume preset allowed values. The distribution of these values may be nicely randomized, to insure the probabilistic chance for hitting a common item. Also, this ad-hoc randomization will limit Eve to chasing the shared secret on purely probabilistic grounds, without any hope for some mathematical shortcut. This lavish use of randomization stands in stark comparison to the common reliance on intractability (algorithmic complexity) for establishing a confidential channel between two strangers in cyber space. [Samid 2013].

2) Clocked Secrets

A large variety of applications exploit the notion of "clocked secrets": secrets that come with a credible period of sustainability. Such are secrets that are expected to be compromised through the brute force strategy. Given a known adversarial computing power, a secret holder will have a credible estimate for how long his or her secret would last. And based on this estimate, a user will exploit with confidence the advantage of his or her secret. All public-key/private-key pairs are so constructed, the bitcoin mining procedure is so constructed, etc. These very popular clocked secrets rely on the hopeful assumption that the attacker is not wielding a more efficient attack, and does not expose our secrets while we can still be harmed by this exposure. Alas, given that in most cases these clocked secrets are based on algorithmic complexity, which is vulnerable to further mathematical insight, one must always suspect that the secrets so protected, are secrets no more. Alternatively, one could 'drown' a secret in a large enough field of high quality randomness, relying on no algorithmic complexity, and hence limiting the attack to the brute force strategy, which is more reliably predictable than adversarial mathematical insight. So one might expect that the variety of clocked-secrets applications like trust certificates, message authentication, identity verification etc., will be based on purely randomized clocked secrets which also suffer from uncertainty regarding adversarial computing power, but are immunized against superior mathematical intelligence.

IV. Randomness: Generation, Handling, Distribution

The future cyber warrior will prepare for the coming conflict by harvesting randomness, and getting it ready for the big outburst, as well as for the daily skirmishes. "Pure randomness" mined from nuclear phenomena is elaborate, expensive, and not readily scalable. White Noise randomness may easily lose calibration and quality, but the most handy source -- algorithms -- which is the most convenient, is also the most vulnerable. So an optimal strategy would choose all three modes, and accumulate as much as is projected to be necessary for the coming cyber war.

The Whitewood Overview [Hughes 2016] eloquently states: *"The security of the cryptography that makes much of our modern economy possible rests on the random numbers used for secret keys, public key generation, session identifiers, and many other purposes. The random number generator (RNG) is therefore a potential single point-of-failure in a secure system. But despite this critical importance, there continues to be difficulty in achieving high assurance random number generation in practice. The requirements for cryptographic random numbers – uniformity and independence, unpredictability and irreproducibility, and trust and verifiability – are clear, but the range of techniques in use today to create them varies enormously in terms of satisfying those requirements. Computational methods are fundamentally deterministic and when used alone are not sufficient for cryptographic use. Physical unpredictability (entropy) is a necessary*

ingredient in a cryptographic RNG. Providing sufficient entropy with assurances that it cannot be known, monitored, controlled or manipulated by third parties is remarkably challenging."

Randomness can be interpreted as the veil behind which human unknown lies hidden, or say, randomness is the boundary of human knowledge, and therefore anyone arming himself with randomness will be immunized from an adversarial superior intellect. But that works only for pure randomness, not for 'pseudo randomness,' which is a sequence that looks random but is generated with human knowledge, and reflects well-defined (although veiled) pattern.

Perfect Randomness is attributed to the prospect of a nuclear event. Niels Bohr and his pioneering cohorts prevailed against luminaries like Albert Einstein in their claim that emission of nuclear radiation is guided by no deeper cause than naked probability, and hence one can measure radiation level emitted from a radioactive isotope, and interpret it as a perfect random bit sequence. For an adversary to crack this sequence, it will have to have insight that violates the tenets of modern quantum physics, with its century old track record.

In reality, many more pedestrian phenomena are unfolding as a combined result of numerous factors, which is safely regarded as 'unknown'. Any such phenomenon could serve as a more convenient source of randomness for which even a wild imagination cannot foresee any compromise. A simple temperature sensor in a normal room will log fluctuating temperatures, which appear random. There are numerous schemes where physical phenomena generate entropy that eventually is weaved into high quality randomness. Any physical phenomena with sufficient unpredictability may be worked into a bit sequence, where the bits are mutually independent (so we assume). The bit stream does not have to be uniform; it may feature more ones than zeros, or vice versa. By interpreting the stream by pairs: "01" → 0; "10" →1, discarding "00" and "11" such independent streams would become uniform.

Any such environmental activity measurement may be used as a seed to generate larger volumes of randomness: it is common to use a choice symmetric cipher: choosing a randomized key, K, and a randomized seed, S, the computer is reading some real time activity parameter in its environment, A, and uses it as input to the selected cipher to generate a cipher-string, $C=Enc_K(A)$, then computing a randomized output: $R = C \oplus S$, then replacing S with $Enc_K(R \oplus C)$.

Algorithmic randomness has seen dramatic improvements in recent years. In the late 60s and early 70s Solomonov, Kolmogorov, and Chaitin [Chaitin 1987] creatively defined a binary sequence as random, if there is no shorter program that generates it. Its intellectual beauty notwithstanding, the definition was not very useful since it is not known whether a shorter generation program does exist. The pendulum then swung to the practicality of statistical tests. A bit string was declared 'random' if it passed the proposed tests. Alas, these were heuristic tests that refer to the expected frequency of certain substrings in the analyzed randomized sequence. These tests are still in use today despite the fact that an adversary who knows the applied test, can easily fool it. These two approaches eventually synthesized into the notion of "indistinguishability": Given a cryptographic procedure where the source of randomness is in one case "perfect" and in the other case "algorithmic" – is there any distinction between these cases which can be spotted in polynomial-time? The difficulty in this approach is that a cipher designer cannot dictate to its cryptanalyst the method of attack, so per-case indistinguishability is dead-ended. Indistinguishability eventually evolved on probabilistic grounds, as first proposed by Goldwasser and Micali [Goldwasser 1984].

Adi Shamir, [Shamir 1981] the co-creator of RSA, has used his cipher to build a pseudo-random sequence, starting with a random sequence R_0, and computing $R_{i+1} = R_i^e \text{ MOD } pq$ where p and q are two large primes, and e is the RSA encryption key. Odd R_i are interpreted as one, and even R_i are interpreted as zero. Shamir used the "indistinguishability" test to anchor the cryptanalysis of his generator to the difficulty to crack RSA.

A host of competing proposals popped up. They were known as PRNG: pseudo random number generators. Blum and Micali [Blum 1984] designed a well received algorithm adhering to Shamir's configuration: starting with a random seed R_0, one computes: $R_{i+1} = p^{Ri} \text{ MOD } q$, where p and q are primes; R_i is interpreted as one if it is smaller than 0.5(q-1), zero otherwise. Blum and Micali then proved that these generators will pass the indistinguishability test, as long as the discrete logarithmic challenge remains intractable.

Subsequent PRNG based their efficacy on other well-known intractable computational challenges. All in all, such tie-in conditions cast PRNG into the same uncertainty that overshadows the served ciphers themselves. One might argue that this only increases the impetus to crack these anchor ciphers.

The "proof" of these number-theoretic ciphers comes with a price – they are slow, and heavy. Faster and more efficient PRNG were proposed, many of them are known as "stream ciphers" which lend themselves to very efficient hardware implementation: an arbitrary seed is bit-wise, XORed in some complex, but fixed circuitry, and in each cycle the rightmost bit is being spit out to join the random sequence. Comprehensive guidelines were developed for these PRNG but the embarrassing truth is that consistence with such design guidelines does not prove security – further mathematical insight may totally defang these 'efficient' pseudo-random number generators.

From a bird's eye view, algorithmic randomness is a randomness-expansion machine: it operates on small amount of randomness (known as seed), and it expands it to

a large randomized sequence. Adopting Kerckhoffs principle, [Kerchoffs 1883] we must assume the adversary knows how this machine works, and hence will compromise it, in the worst case, by applying brute force cryptanalysis. At any rate, the seed itself should be non-algorithmic in nature, so that it would not be vulnerable to an even smaller seed. Say then that a serious cryptographic shop will have to acquire non-algorithmic randomness, and use algorithmic randomness when high-quality non-algorithmic randomness is not available.

White Noise randomness can be generated 'when needed', which has a clear security advantage, because it does not exist before it is actually used, and hence there is no extended storage time in which to compromise it. Other sources need to be stored, and hence need to be guarded.

Randomness can be sealed in hardware; the bits dispensed as needed. One would opt to seal the container of the randomness, secured from software hacking.

Distribution of randomness cannot be done cryptographically because it cost one random bit to transfer one. Some fanciful quantum protocol are being developed where receipt of randomness, or of any data will come with the guarantee that no one else got hold of it. But as of today randomness must be distributed off-line, in some physical form. Because of the burden of physical exchange it stands to reason that major hubs in far away places will use big bulk exchanges that would last them for a long time. Close by parties may practice distribution by installment, which has the advantage of theft-security. If front line entities are given a small measure of randomness at a time, then if they are compromised and that randomness is revealed then the damage is limited.

Randomness which comes physically stored may be kept in a secure enclosure protected by various tamper-resistance technologies. The idea is to have the randomness erase itself upon unauthorized access.

One can envision a hierarchy of tactical randomness capsules fitted into capsule-batteries, which fit into a battery-stock, and so on, with strict marking and inventory management to insure that each stock battery, and capsule are accounted for.

A headquarters stock will have to constantly build up the inventory, ready for distribution as the cyber war dictates.

V. RANDOMNESS: SELECTED USE CASES

In its simplest form Alice and Bob will arm themselves with twin randomness and use it in end-to-end encryption through any medium in cyber space. Deploying an effective TVC, they will be immunized against any snooping, safeguard their integrity against any fast computer, or smart cryptanalyst -- however much smarter than Alice and Bob, and much faster than their computing machines. If they manufactured the randomness on their own or bought it for cash, or otherwise acquired it in untraceable means then their communication is cryptographically secure, and the only way to breach it, is to steal the randomness from either one of them. Alice and Bob will be able to use their shared randomness wisely to maximize its utility. Specifically they will designate sensitivity levels, say: low-security, medium-security, high-security, and top-security. They might use standard HTML or XML markings on their communication, like a "crypto" tag: <crypto level=high> contents </crypto>. And use different partitions of their shared randomness for each security grade. The top-security level will be dedicated to communicate what partitions of their shared randomness were used for which security grade, for the coming communications. This way their cryptanalyst will remain in the dark as to whether the following ciphertext is Vernam grade, and cryptanalysis is futile, or whether it is at 'equivocation grade' where some information can be extracted, or perhaps it is at intractability level where brute force computing will eventually extract the plaintext.

Alice and Bob will face an optimization challenge: how to best allocate their finite shared randomness. They will have to estimate how much communication they will have to service with the current stock of randomness, and based on that, they will dynamically allocate their randomness stock among the various security levels they use. If Alice and Bob happen to communicate more than they estimated then before running out of randomness, they will leverage and expand their residual stock, using algorithmic randomness, as a means of last resort.

If Alice and Bob run out of randomness to achieve Vernam security they will drop into equivocation, and then to intractability. Once at intractability stage their security level will level off. They will still be immunized against brute force cryptanalysis because the attacker will not know how much randomness they have been using.

It is important to emphasize that unlike today when local authorities may lean on crypto providers to gain stealth access, in this emerging 'randomness rising' mode, the communicators, Alice and Bob, will decide, and will be responsible for their security, and the authorities will have no third party to gain access through.

If shared randomness is to be used among a group of three or more, then the group will have to set some means of monitoring the extent of use, at least in some rough measure to insure that the deployed randomness will not be over exposed. Also dynamic randomness allocation will have to be carried out with good accountability of who used which part of it, and for how much.

Hierarchies: A hierarchical organization comprised of h echelons might have full-h-echelons shared randomness, and on top of it (h-1)-echelons shared randomness for all except the lowest echelon, and so on each echelon may be allocated an echelon specific randomness and the various communicators will use the randomness that corresponds to the lowest rank recipient.

Hub Configuration: a group of communicators might assign one of them to serve as the hub. The hub will share randomness with each of the members of the group. If Alice in the group wishes to communicate securely with Bob, she notifies the hub who then uses its per-member shared randomness to deliver twin randomness to Alice and Bob. This allows the group to maximize the utility of their held randomness, given that they don't know a-priori who will need to talk to whom. It offers a new risk since the hub is exposed to all the keys.

The new privacy market will feature anonymous purchase of twin randomness sticks, (or more than a couple) to be shared physically by two or more parties for end-to- end communication. Randomness capsules will be stuffed into 'egg capsules' which must be cracked in order to pull the Micro SD or other memory platform for use. Untracked, it would assure its holder that it was not compromised. [Samid 2016D]

A. Identity Management

Identity is a complexity-wolf in a simplicity sheepskin: on one hand, it is amply clear that Joe is Joe, and Ruth is Ruth, but on further thought, are people who underwent a heart transplant the same as before? What about people whose' brain has been tampered with by illness or medical intervention? If identity is DNA + life experience, would a faithfully recorded database, operated on through advanced AI, assume identity? Alan Turing himself projected that identity enigma, which is pronouncedly reflected in cyber space. The earlier strategies of capturing identity in a short code (e.g. PIN, password) have given hackers an effective entry point for their mischief. And we more and more realize that to verify identity one would have to securely acquire randomized identity data from the ever-growing data assembly that comprises identities, and then randomly query an identity claimant, to minimize the chance for a hacker to be prepared for the question based on previous identity verification sessions. The more meticulously randomized this procedure, the more difficult will it be for hackers to assume a false identity. And since falsifying identities is the foundation of system penetration, this use is the foundation for a hack-free cyber space.

B. The Internet of Things

Light bulbs, thermometers, toasters, and faucets are among the tens of billions of "things" that as we speak become 'smart', namely they become active nodes in the overwhelming sprawl of the Internet of Things. Such nodes will be monitored remotely, and controlled from afar. It is a huge imagination stressor to foresee life with a mature Internet of Things (IOT) where all the devices that support our daily living will come alive wirelessly. Case in point: all the complex wiring that was always part and parcel of complex engineering assemblies will vanish: transponders will communicate through IP.

This vision is daunted, though, by the equally frightful vulnerability to hackers who will see private camera feeds, maliciously turn on machines, steal drones, flood rooms, start fires, etc. The only way to make the IOT work is through robust encryption to keep the hackers barking from the sideline, when the technology parade marches on.

Unfortunately, the majority of the IOT devices are so cheap that they cannot be fitted with the heavy-duty computing capabilities needed for today's algorithmic-complexity cryptography. Here again randomness is rising to meet the challenge. Memory technology is way advanced: we can store hundreds of gigabytes of randomness with great reliability, virtually on a pinhead. No device is too small to feature a heavy doze of randomness. Any of the ciphers described above, and the many more to come, will insure robust encryption for any IOT device, large or small, industrial or residential, critical or ordinary.

Ciphers like Walk-in-the-Park are readily implemented in hardware, and may be fitted on RFID tags, and on other passive devices.

C. Military Use

Kinetic wars have not yet finished their saga, so it seems, so the next big battle will incorporate cyber war in a support posture. The combating units will be equipped with randomness capsules fitted with quick erasure buttons, to prevent falling into enemy hands. Since there would be situations where the enemy captures the randomness and compromises the communication integrity, the military will have to adopt efficient procedures to (i) minimize the damage of a compromised capsule or randomness battery, and (ii) to quickly inform all concerned of a compromised randomness pack, with associated reaction procedures.

The risk of compromised randomness can be mitigated by equipping high-risk front units with limited distribution randomness, which also means a narrow backwards communication path. Also this risk may lead to a held-back distribution strategy where large quantities of randomness are assembled in secure hubs and meted out to front units on a pack by pack basis, so that captured units will cause only minimal amount of randomness loss.

One may envision pre-stored, or hidden randomness in the field of battle. The military will likely make use of the "virgin capsule" concept, or say the "egg capsule" concept, [Samid 2016D] where a physical device must be broken like an eggshell in an irreversible fashion, so that when it looks whole it is guaranteed to not have been exposed and compromised.

D. Digital Currency

Digital money is a movement that gathers speed everywhere, following the phenomenal rise of bitcoin. In a historic perspective money as a sequence of bits is the natural next step on the abstraction ladder of money (weights, coins, paper), and the expected impact of this transformation should be no less grandiose than the former: coins-to-paper, which gave rise to the Renaissance in Europe. The present generation of crypto currencies mostly hinge on those complexity-generating algorithms, discussed before -- which lay bare before unpublished mathematical insight. Insight that once gained will be kept secret for as long as possible, to milk that currency to the utmost. And once such compromise becomes public -- the currency as a whole vanishes into thin air because any bitcoin-like crypto currency represents no real useful human wealth. The rising role of randomness will have to take over the grand vision of digital money. We will have to develop the mathematics to allow mints to increase the underlying randomness of their currency to meet any threat -- quantum or otherwise. Much as communication will be made secure by its users, opting for a sufficient quantity of randomness, so money will have to deploy the ultimate countermeasure against smart fraud -- at will high-quality randomness.

A first attempt in this direction is offered by BitMint: [Samid 2012, Samid 2016D, Samid 2015A, Samid 2015B, Samid 2014] a methodology to digitize any fiat currency, or commodity, (and any combinations thereto), and defend the integrity of the digitized money with as much randomness as desired -- commensurate with the value of the randomness-protected coin. Micro payments and ordinary coins may be minted using pseudo-randomness, where one insures that the effort to compromise the money exceeds the value of the coveted funds. For larger amounts, both the quality and the quantity of the BitMinted money will correspondingly rise. Banks, states and large commercial enterprise will be able to securely store, pay, and get paid with very large sums of BitMinted money where the ever growing quantities of randomness, of the highest quality will fend off any and all attempts to steal, defraud, or otherwise compromise the prevailing monetary system. Digital currency will become a big consumer of this more and more critical resource: high quality randomness.

E. Plumbing Intelligence Leaks

Randomness may be used to deny an observer the intelligence latent is data use pattern, even if the data itself is encrypted. Obfuscation algorithms will produce randomized data to embed the 'real data' in them, such that an eavesdropper will remain ambiguous as to what is real contents, and what is a randomized fake. For example, a cyber space surfer will create fake pathways that will confuse a tracker as to where he or she has really been. Often times Alice and Bob will betray a great deal of information about their mutual business by exposing the mere extent and pattern of their communication. To prevent this leakage Alice and Bob may establish a fixed rate bit transfer between them. If they say nothing to each other, all the bits are fully randomized. If they send a message to each other, the message is encrypted to make it look randomized, and then embedded in the otherwise random stream. To the outside observer the traffic pattern is fixed and it looks the same no matter how many or how few messages are exchanged between Alice and Bob. There are of course various means for Alice and Bob to extract the message from the randomized stream. For high intensity communicators this leakage prevention requires a hefty dose of randomness.

It is expected that in a cyber war combatants will establish such obfuscating fixed rate bit streams to suppress any intelligence leakage.

F. Mistrustful Collaboration

Over seven billions of us crowd the intimate cyber neighborhood, allowing anyone to talk to everyone. Alas, we are mostly strangers to each other, and naturally apprehensive. Cryptography has emerged as a tool that is effective in inviting two (or more) mutually mistrustful parties to collaborate for their mutual benefit. The trick is to do so without requiring the parties to expose too much of their knowledge, lest it would be exploited by the other untrusted party. "Zero Knowledge" procedures have been proposed designed to pass to a party only the desired message/data/action, without also exposing anything else -- procedures that prevent knowledge leakage. These procedures might prove themselves more important historically in the welfare of the planet because they don't help one to defeat the other, but to cooperate with the other. Alas, most of the prevailing zero knowledge protocols rely on algorithmic-complexity, which we have already analyzed for its fundamental deficiencies. These protocols too will be replaced with user determined knowledge leakage randomization protocols.

Let Alice and Bob be mutually aware, be parties in some ecosystem. It is impossible for Alice not to continuously pass information to Bob. Anything that Alice could have done that would be noticed by Bob, and has been done, is information. Albeit, anything that could have been done by Alice and could have been noticed by Bob, but has not been done -- also passes information to Bob. Simply put: silence is a message. So, we must limit our discussion to Alice passing a string of bits to Bob such that Bob cannot learn from it more than the size of the string, and the time of its transmission. In other words: the identities of the bits will carry no knowledge. Such would only happen if Alice passes to Bob a perfectly randomized bit string. Any deviation from this perfection will be regarded as information. We can now define a practical case to be analyzed: Alice wishes to prove to Bob that she is in possession of a secret S, which Bob is fully aware of.

However, since Alice suspects that on the other side of the line the party calls himself Bob is really Carla, who does not know the value of S, then Alice wishes to pass S to her communication partner such that if she talks to Carla, not to Bob, then Carla will learn less than a preset low limit – almost zero knowledge leakage.

The idea will be for Alice to pass to Bob a string of bits in a way that would convince Bob that Alice is in possession of the secret, S, while Carla would be stuck in a persistent entropic fog about S. This would happen by hiding a pattern for Bob to detect in a random looking string which Carla would not be able to see a pattern therein.

We describe ahead how it can be done using a string of at-will size, where the larger the string the more probable the convincing of Bob, and the denial of information from Carla. Such procedures which allow the user to determine the amount of randomization used are consistent with the randomness rising trend.

Procedure: let S be a secret held by Alice and Bob, of which Carla is ignorant but has interest in. Let S be comprised of s=2n bits. Alice would randomly flip n bits in S, to generate S_f, which is also comprised of 2n bits. Next, Alice would convey S_f to Bob. Bob, aware of S, will repeat Alice's action except for the flipping which was done through randomness which Alice kept secret. However, Bob will be able to verify that S_f and S are the same string, apart from *exactly* n bits which have an opposite identity in S and S_f. The chances for Alice to construct S_f without knowledge of S is progressively negligible for larger s values.

Carla, unaware of S, will not be able to learn much from S_f about S. In her eyes every bit in S_f has an equal chance to be what it is, or to be its opposite. By processing the secret S to a larger string, the user would increase the relevant probabilities for the integrity of the protocol. The simplicity thereto insures against some clever cryptanalytic math.

Alice may then ask Bob to flip back some f' bits from the n flipped bits that generated S_f. Bob complies, and sends back the result: S_{ff}. Alice will then verify that all the f' flipped bits are bits which she flipped in generating S_f. This way Alice will assure herself with at-will high probability that Bob is in possession of their shared secret S -- or alternatively that she talks to Bob. Carla, unaware of S, will be increasingly unlikely to be able to pick f' bits that comprise a subset of the n bits Alice flipped. This mutual reassurance between Alice and Bob cost both of them some reduction of security because the Man-in-the-Middle will know that f' bits out of the s bits in S_{ff} do not face any flipping probability.

G. Balance of Power

Throughout the history of war and conflict, quality had typically a limited spread between the good and the bad, the talented and the not so talented, but the quantity gap was open ended, and projected power, deterrence, as well as determined outcome of battles. As conflicts progress into cyber space, we detect a growing gap in the quality component of power, all the while quantity is less important and its gaps less consequential. It was the talent of Alan Turing and his cohorts that cut an estimated two years of bloodletting from World War II. In the emerging conflicts, whether in the military, or in the law enforcement arena, a single Alan Turing caliber mind may defeat the entire front of a big state defense, and bring empires to their knees. Strong states, and powerful organizations naturally measure themselves by their overwhelming quantitative advantage, and are likely to miss this turn where the impact of quantity diminishes, and quality rises. On the other end, the small fish in the pond are likely to conclude that superior mathematical insight is their survival ticket, and put all their effort in developing mathematical knowledge that would surprise and defeat their smug enemies. In parallel, realizing that randomness is rising, these small fish will arm their own data assets with rings of randomness, and neutralize any computing advantage and any unique theoretical knowledge used by their enemies. All in all, the rising of randomness, and its immunity against superior smarts creates a new level playing field, which the big fish is likely to be surprised by. Countries like the United States need to prepare themselves for the new terms of the coming adversarial challenges both in the national security arena, and in the criminal sector.

VI. 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