The Prospect of a New Cryptography

Extensive use of non-algorithmic randomness competes with mathematical complexity

Gideon Samid

Electrical, Computer and System Engineering

Computer and Data Sciences
Case Western Reserve University, Cleveland, OH
Gideon.Samid@CASE.edu

Abstract: randomness cannot be compressed, hence expanded randomness is 'contaminated randomness' where hidden pattern is used. Current cryptography uses little randomness (the key) to generate large randomness (the ciphertext). The pattern used for this expansion is subject to cryptanalysis. By contrast, Vernam and the new breed of Trans-Vernam ciphers project security with sufficient supply of genuine randomness. Having no hidden pattern in their process, they expose no vulnerability to cryptanalysis, other than brute force, the efficacy of which, is well gauged by using enough randomness to brute-force through. Unlike the original genuine randomness cipher (the Vernam cipher; US patent: 1,310,719), the new breed of Trans-Vernam ciphers (US patents: 10,541,802, 10,911,215, 11,159,317 to name a few) projects security with shared randomness (between transmitter and recipient) as well as with unilateral randomness determined ad hoc by the transmitter, thereby controlling the vulnerability of the transmitted message, including eliminating it all together, rising to Vernam grade. The new Trans-Vernam ciphers exploit new technologies for generating high-grade randomness, storing it and communicating it in large quantities. Their security is mathematically established and barring faulty implementation these ciphers are unbreakable. We are looking at a flat cyberspace, no more hierarchy based on math skills: Vernam grade security delivered through modern Trans-Vernam ciphers. Robust privacy of communication will be claimed by all – for good and for ill; law-enforcement and national security will have to adjust. It's a new cryptography, and a new society.

1. Introduction

The era of breakable cryptography is coming to its end. And with it comes to a close the long battle between code writers and code breakers. It is a new ballgame with significant implications for society at large.

The new cryptography is fundamentally different from the prevailing mode. Until now cryptography was a battle of wits between code builders and code crackers, and the best mathematician won. The NSA

triumphed, they had the best brains and the best machines. The more people used crypto, the more the NSA knew where they hide their secrets. We have routinely been using ciphers which the academic cryptographers assured us are safe, but the powers that be, as Snowden revealed, are reading them quite fluently, building up a big advantage for national security and for government surveillance alike.

This mode of cryptographic hierarchy where status is determined by the quality of your mathematicians is coming to its end. The emerging new cryptography dethrones math, abandons complexity and instead it projects security with just invented new tools that are based on what shapes up to be "cyber oil" -- the energy source in our new living quarters: randomness.

It is not obvious to equate randomness with energy and regard it as "cyber oil". But such it is. First on a broad philosophical base: the fundamentals of reality, physics, are randomized processes; the big bang that started everything is randomness powered. The reason our fancy computers are about to surrender to the coming onslaught of quantum computers is that powerful as our Turing machines are, they cannot generate true randomness. They spew tons of fake randomness, but can't come up with the real thing. Quantum machines run on randomness.

It turns out that it is very hard to shed off pattern, to be completely pattern devoid. Alas recent technologies have achieved sufficiently high-grade randomness, which newly developed tools can now use to upend cryptography as we know it.

A classic cipher is based on complexity, pattern, applied to a plain message, disfiguring it to a ciphertext such that it would be hard work to refigure the hidden message out of it. Alas, one can check all the plausible messages and eventually find the one that fits the ciphertext. So even a dumb search will eventually extract the message out of the ciphertext after on average trying half the plausible messages. If you are a bit smarter you find the right message faster. The foundation of classic cryptography is the plan for the ciphertext to keep its secret long enough. In other words, classic cryptography is based on the assumption that the attacker is not smarter and not better equipped than we think. Adversaries that don't comply with what we expect of them, they read our mail.

Is there a better way to safeguard our secrets?

Yes, by harnessing the magic of randomness. An unspecified random list is an unpredictable list, but once specified, all its unpredictability vanishes.

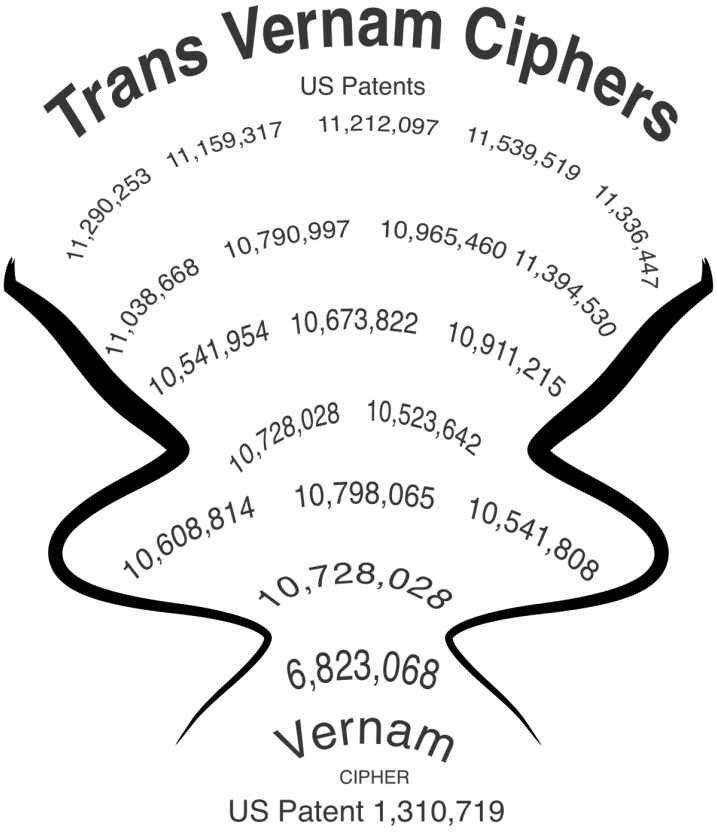
Unpredictability is infectious -- that is the subtle point that was used by a young American engineer, Gilbert S. Vernam when he designed in 1917 his unbreakable cipher.

Pattern + Randomness = Randomness

When you apply disorder (randomness) to order (pattern) you end up with disorder (randomness).

So if Alice wishes to send Bob a message (an ordered set of letters), if she subjects it to randomness then she generates a random list that cannot be read by a stranger. Bob will be able to read the message because what appears as random to everybody else is the pre-shared specified list that Alice and Bob together extracted earlier from the source of randomness. To the extent that the pre-shared random list is truly random, the result of applying it to Alice message (patterned list) is truly random for everyone except Alice and Bob.

Now this operation of infectious randomness requires a sufficient supply of true fresh randomness. Classic cryptography also uses randomness, but not fresh randomness. Today we use small dozes of randomness (called cryptographic keys) to apply on the ordered list (the plaintext message), to create fake randomness at the output. Until recently we did not have ready supply of true randomness, our computers were too burdened storing all that randomness and our communication network too slow to handle the large quantities of the needed fresh randomness, and so we relied on mathematical complexity as a substitute, and generated the cryptographic hierarchy where math skills and computing power determined one's station in this hierarchy.



Today we have the technology to generate non-algorithmic high quality randomness, we have data storage technology to accommodate the flood of randomness and we have 5G networks that can easily handle the extra communication load. So today we enter a new era: The era of unbreakable cryptography. As we speak, the market is replete with assorted ciphers that exercise this simple formula: *pattern + randomness = randomness*. The old 1919 Vernam patent has been improved upon with powerful modern ciphers that deliver unbreakable cryptography.

Quantum computers resorted to randomness to triumph over the old Turing machines we use today that are randomness-deficient. But Turing has not surrendered, it sealed a partnership with randomness generators to offer unbreakable communication to everyone not just to smart mathematicians. The era where government and the powers that be secretly violate the privacy of us all, is coming to its end. And with it the social order that prevailed until today.

It would be up to social scientists to figure out the social implications of a cyberworld where privacy of communication is solid and no sophistication is needed for a secret communication to take place. This

protection will apply to harmless conversations as well as to harmful conversations. On one hand privacy will celebrate, on the other hand national security and law enforcement will face a new reality, and will have to adjust and realign.

This cyberspace revolution is applicable to non-strangers, parties that know each other before they exchange secret messages in cyberspace. But what about strangers? Can they benefit from randomness? A new technology, quantum entanglement will allow two strangers to share specified randomness that remains random to everybody else and hence benefits from the new Trans-Vernam ciphers that guarantee protection against any cyber attack. Another solution was developed (US Patent 10,798,065) that uses randomness to allow two strangers to share a temporary secret which they can then use to share fresh randomness before erasing it to prevent others from sharing the same.

2. Trans Vernam Ciphers

We identify a class of ciphers subject to the following attributes:

(i) they use a key of a secret and unlimited size

(ii) their computational burden for encryption and decryption is independent, linear, or at most polynomial with the size of the key

(iii) they are decoy-tolerant, namely the content-ciphertext can be mixed with content-free randomness such the intended reader can readily winnow the content-ciphertext from the mixed flow.

(iv) they are circumstantially mathematically secure (as defined below)

The original Vernam cipher only satisfies condition (ii) and is not a Trans-Vernam cipher.

2.1 Circumstantial Mathematical Security

Mathematical security was defined by Claude Shannon as the case where knowledge of the content of a ciphertext offers no advantage over knowledge of the fact and the size of the ciphertext. Let Ω be the set of all possible messages given the knowledge of the fact that a message was sent, and that its size is known. Let $\pi = \pi(\Omega)$ be the probability distribution of Ω, given the prevailing circumstances as known to the cryptanalyst, then mathematical security is the situation where π is the same whether the content of the ciphertext is known or not.

In reality only a tiny minority of the Ω set is associated with more than a negligible probability, hence in practice one is concerned with the probability distribution of only the possible messages that have a

probability above a given threshold, namely, the probability distribution of the probable messages π_p. A cipher for which knowledge of the contents of the ciphertext does not change π_p is defined as a circumstantially mathematically secure cipher.

For example: a chess master encrypts a recommended next move. There are about 10^{20} possible moves in a typical chess game, but the top 100 capture the range of non negligible probabilities, so a ciphertext that will not impact the probability of the top 100 moves is a circumstantially mathematically secure cipher.

The property of being decoy tolerant will allow a transmitter deploy n keys K_1, K_2, ... K_n, to be used each to encrypt the plaintext associated with the n most probable plaintexts (according to the prevailing circumstances): P_1, P_2, ... P_n and generate the respective n ciphertexts C_1, C_2, ... C_n, then the transmitter will join these n ciphertext to a combined ciphertext C_0, and set it up such that a reader equipped with key K_i upon processing C_0 will regard all the other ciphertext C_j for j = 1,2,..(i-1),(i+1)...n as decoy data, while decrypting C_i to P_i.

So set up C_0 is by construction a circumstantially mathematically secure ciphertext. An omnipotent cryptanalyst will find the n keys (K_1, K_2, ... K_n), and list the corresponding plaintexts P_1, P_2, ... P_n, but will have no means to further resolve the indeterminism as to which of the probable messages was carried by the transmitted ciphertext. That determination is the purview of the intended recipient who uses the shared K_i to decrypt C_0 to P_i.

Trans-Vernam ciphers, by definition, can use their decoy tolerance to project circumstantial mathematical secrecy.

AI Enhanced Cryptanalysis: Modern cryptanalysis exploits AI to devise plausible plaintexts, which are cast against a captured ciphertext, and evaluated for the probability of the existence of a key to fit the guessed plaintext with the captured ciphertext, and by process of elimination crack the cipher. When this strategy is applied to Trans Vernam ciphers, it, at best, exposes the full range of mutually inconsistent plaintexts, which can all be decrypted from the captured ciphertext, using the right key. The attacker unaware which key the intended user is using is stuck in terminal indeterminism.

2.2 Specified and Unspecified Equivocation

The above procedure may be regarded as specified equivocation. The transmitter specifically ensures that more than a single plausible message is woven into the ciphertext. Yet, we also have the specter of unspecified equivocation. The more diffused a ciphertext is, namely the more decoy data is mixed into the contents data, the greater the chance that this randomized decoy data will fit with a key that will relate the ciphertext to assorted plausible plaintext messages, thereby creating a terminal equivocation that hides the real message.

2.3 The Mathematical Security Conjecture

A Trans-Vernam cipher used with a finite size key K of size |K| will retain its mathematical secrecy status over a cumulative message M of size |M > |K| by inflating the ciphertext with sufficient decoy data, the extent of which is determined by s = |M|-|K|.

2.4 Security Retention

A Trans-Vernam Cipher, TVC, using no decoys will lose its mathematical security as soon as the cumulative message M is of size |M| that exceeds the size of the key K, |K| (s > 0). The question of interest is the degree to which security is lost as the value of s increases. The challenge is to find Trans-Vernam ciphers that exhibit a strong security retention, namely their security deteriorates very slowly when s increases (more and more messages are being used over the same key). Deterioration is being measured through changes in π_p. This topic and analysis of the prevailing Trans-Vernam ciphers will be addressed in a subsequent article.

2.5 No Weak Keys

Pattern based cryptography, mainstream today, relies on a random key, alas since it uses pattern to expand the true randomness to pseudo randomness in the larger ciphertext, it is likely to have hidden fault lines in the form of keys that have special characteristics such that when they are used the attacker can extract the plaintext message from the captured ciphertext. Such weak keys are hard to find. These keys serve as the secret target for the top-notch cryptanalysis shops. Suppose for example that a certain nominal cipher when used with keys in the form of 7k+2 exhibit a property that allows for cryptanalysis. If the key is selected randomly then 1/7 of all keys used will generate a cryptanalyzed message. Cipher designers are not aware of these weak keys for their cipher; they are usually discovered through much labor by the heavy-duty cryptanalyses shops.

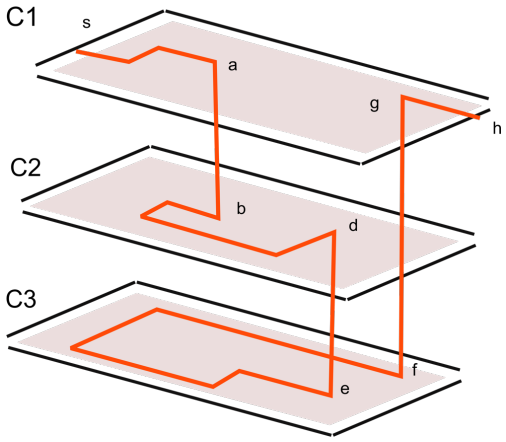
TVC, by contrast, since they don't use pattern (they are pattern devoid) they have no weak keys, and offer no mathematical shortcuts to their plaintext. They limit their attacker to brute force and bound the attacker efficiency with probability calculus, which is readily calculable by the cipher user. In other words, the Trans-Vernam cipher user will have a credible assessment as to the vulnerability of their messages, and will be able to make a rational decision for any given message whether it is a good risk situation to send it over, TVC encrypted, or to deploy a fresh shared key, if feasible under the circumstances.

2.6 Run Down of Trans Vernam Ciphers

We review three classes of TVC, one called "Space Key" TVC, another called "One to Many Double" TVC, and the third one is "Unary Mapping" TVC. The first category is based on a key that ranges over a specified geometry, space. The plaintext is viewed as a travel guide across this space. The resultant travel path is then described via parameters of the space such that recipient who has possession of that space, call it "the travel map" or otherwise call it "the key", can figure out from the travel path (the ciphertext) what was the travel guide that gave rise to this travel path (the plaintext). As long as travel paths do not overlap and do not

intersect, one can match any ciphertext (travel path) with a travel territory that will point to any plaintext of choice -- Vernam secrecy. As more and more travel paths are marked on the key space, the greater the chance for intersection and overlap, and the mathematical security is lost, but very slowly. The larger the key space, the larger the message size that can be used with Vernam grade secrecy. See: US Patents: 11,159,317, 10,911,215, 6,823,068)

Pathway over layers of 2D Canvasses



The "One to Many Double" TVC is based on the idea that one can point to a given letter of an alphabet with a pointer comprising data that upon a simple process will point to the data that represents this letter, while the very same pointer can point to a large number of data items, each of them may represent some letter, and at the same time each letter can be pointed to by a large number of pointers. These two ways one-to-many is established through randomness and can be cryptanalyzed only through brute force. The larger the data items that represent letters, the greater the variety of pointers that point to the same letter and the greater the variety of letters that may be pointed to by the same pointer. By representing each letter from the plaintext alphabet with a large enough string, the plaintext field can be richly equivocated.

It is easy to send out pointers that point to no letter --decoys. See US Patents: 10,541,808, 10,728,028

The third category is based on translating a plaintext into a unary language, adjusting it to become a very large binary string of equal number of ones and zeros, and then using a very large key to ensure full range of permutation for that string. The transposed string (the ciphertext), if de-transposed with various keys and then converted back from unary to ASCEII or Base64 will offer many plausible plaintexts. The larger that transposition key, the greater the security (See US Patent 11,212,097)

2.7 Sources of randomness

TVC can be used with pseudo (fake) randomness generated algorithmically, although John Von Neuman famously said that those who use algorithms to generate randomness don't understand neither algorithms nor randomness. Algorithmically generated randomness can be improved using a filter that cleans out poor randomness sections. Next in quality, we have physical complexity generators, they are unpredictable enough in most cases. Further up we have quantum sources where randomness is generated from reading subatomic processes.

3. Summary

Modern technology for generating randomness, storing randomness and communicating randomness enables us to project cyber security without having to rely on engineered patterns, which smarter mathematicians can unravel -- and do today. Randomness based security leads to a flat cyber space. Smarts and mathematical skills lose their advantage, everyone can talk in complete privacy all over cyber space. On one hand it restores pre cyberspace privacy even on a stronger basis, on the other hand it denies governments and law enforcement a range of tools they use today to do their jobs. This flat cyberspace will have a strong impact on politics, economics, and society at large. It is a new cryptography, and it leads to a new society. Let's make it a better one!

Reference

A comprehensive reference for this theme of 'pattern devoid cryptography' is given in an article so titled https://eprint.iacr.org/2021/1510

Readers are invited to 'test drive' an active Trans-Vernam cipher.

(i) Unary Cryptography https://unarycryptography.com
(ii) ButFlip http://wesecure.net/learn/BitFlipEncrypt.php

For an entertaining read check out "The Cipher Who Came in from the Cold" a recently published thriller envisioning the way the CIA, the NSA and the FBI meet the challenge of the new cryptography.

More Sources:

1. "An extension of the Shannon theory approach to cryptography". Martin Hellman, IEEE Transactions on Information Theory, V. 23, 3 1977, pp. 289 - 294
2. "A New Perspective of Geometry and Space as an Evolutionary Organizer of Data." Gideon Samid, http://www.dgsciences.com/Geometry_H7n18.pdf
3. "A Unary Cipher with Advantages over the Vernam Cipher" Gideon Samid, https://eprint.iacr.org/2020/389
4. "Anonymity Management: A Blue Print For Newfound Privacy" Gideon Samid, The Second International Workshop on Information Security Applications (WISA 2001), Seoul, Korea, September 13-14, 2001 (Best Paper Award).
5. "Artificial Intelligence Assisted Innovation" Gideon Samid, https://www.intechopen.com/online-first/artificial-intelligence-assisted-innovation

6. "At-Will Intractability Up to Plaintext Equivocation Achieved via a Cryptographic Key Made As Small, or As Large As Desired - Without Computational Penalty." Gideon Samid, 2002 International Workshop on CRYPTOLOGY AND NETWORK SECURITY, San Francisco, California, USA September 26 – 28, 2002.
7. "BitFlip: A Randomness Rich Cipher" 2017, Gideon Samid, Sergei Popov, https://eprint.iacr.org/2017/366.pdf
8. "BitMap Lattice: A Cyber Tool Comprised of Geometric Construction", US Patent 10,911,215, Feb 2, 2021
9. "Chaos-based Cryptography: A Brief Look Into An Alternate Approach to Data Security" A Sharif, NI Raihana, A Samsudin - Journal of Physics 2020 https://iopscience.iop.org/article/10.1088/1742-6596/1566/1/012110/meta
10. "Communication Theory of Secrecy Systems". Claude Shannon (1949) http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
11. "Cryptography of Things: Cryptography Designed for Low Power, Low Maintenance Nodes in the Internet of Things" Gideon Samid https://search.proquest.com/openview/8897dc1c4858b327796917b8fcdff7ae/1?pq-origsite=gscholar&cbl=1976348
12. "Cyber Passport: Preventing Massive Identity Theft. " Gideon Samid, https://eprint.iacr.org/2016/474
13. "Denial Cryptography Based on Graph Theory." Gideon Samid (2004) US Patent 6,823,068.
14. "Drone Target Cryptography" Gideon Samid, https://eprint.iacr.org/2016/499
15. "Effective Concealment of Communication Pattern (BitGrey, Bitloop)" US Patent 10,673,822 June 2, 2020
16. "Encryption Sticks (Randomats)" Gideon Samid ICICS 2001 Third International Conference on Information and Communications Security Xian, China 13-16 November, 2001
17. "Encryption-On-Demand: Practical and Theoretical Considerations" Gideon Samid https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.215.2463&rep=rep1&type=pdf
18. "Equivoe-T: Transposition Equivocation Cryptography." Gideon Samid, International Association of Cryptology Research, ePrint Archive https://eprint.iacr.org/2015/510
19. "Essential Shannon Security with Keys Smaller than the Encrypted Message the Encrypted Message" Gideon Samid, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.75.1585&rep=rep1&type=pdf
20. "FAMILY KEY CRYPTOGRAPHY: Interchangeable Symmetric Keys; a Different Cryptographic Paradigm" Gideon Samid https://eprint.iacr.org/2021/458
21. "Feeding Cryptographic Protocols with Rich and Reliable Supply of Quantum-Grade Randomness" Gideon Samid, https://eprint.iacr.org/2020/968
22. "Feeding Cryptographic Protocols with Rich and Reliable Supply of Quantum-Grade Randomness" Gideon Samid, https://eprint.iacr.org/2020/968.pdf
23. "Fingerprinting Data" Gideon Samid, https://eprint.iacr.org/2018/503
24. "Hush Functions Extended to Any Size Input versus Any Size Output." Gideon Samid, https://eprint.iacr.org/2012/457.pdf
25. "Intractability Erosion: The Everpresent Threat for Secure Communication" Gideon Samid The 7th World Multi-Conference on Systemics, Cybernetics and Informatics (SCI 2003), July 2003.
26. "Larger Keys, Less Complexity" Gideon Samid, A Strategic Proposition." https://eprint.iacr.org/2018/406.pdf
27. "Proposing a Master One-Way Function." Gideon Samid, https://eprint.iacr.org/2007/412
28. "Randomized Bilateral Trust (RABIT): Building Connectivity for Cyber Space" US Patent 10,798,065, Oct 6, 2020
29. "Randomness as Absence of Symmetry" Gideon Samid, THE 17TH INTERNATIONAL CONFERENCE ON INFORMATION & KNOWLEDGE ENGINEERING (IKE'18: JULY 30 - AUGUST 2, 2018, LAS VEGAS, USA) http://bitmint.com/SymRand_Vegas_H8518R.pdf
30. "Randomness in digital cryptography: A survey" K Marton, A Suciu, I Ignat - Romanian journal of information science 2010 https://www.academia.edu/download/46676431/Randomness_in_Digital_Cryptography_A_Sur20160621-25262-h5ar54.pdf
31. "Randomness Rising - The Decisive Resource in the Emerging Cyber Reality" Gideon Samid, Int'l Conf. Foundations of Computer Science | FCS'18 | https://www.bitmint.com/RandomnessRising_GSamid_H1o16.pdf
32. "Re-dividing Complexity between Algorithms and Keys" Gideon Samid, International Conference on Cryptology in India, 2001 - Springer https://link.springer.com/chapter/10.1007/3-540-45311-3_31
33. "Rivest Chaffing and Winnowing Cryptography Elevated into a Full-Fledged Cryptographic Strategy" Gideon Samid, 2018, Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE); Athens, (2018). https://search.proquest.com/openview/8ea94f941732d85fb24512d5e7582820/1?pq-origsite=gscholar&cbl=1976356
34. "Secret Signaling System". US Patent 1310719A. Gilbert S. Vernam (1918)
35. "Shannon Revisited: Considering a More Tractable Expression to Measure and Manage Intractability, Uncertainty, Risk, Ignorance, and Entropy" Gideon Samid, https://arxiv.org/abs/1006.1055
36. "SpaceFlip: Unbound Geometry Cryptography." Gideon Samid, https://eprint.iacr.org/2019/285.pdf
37. "Spaceflip: Unbound Geometry Security" US Patent 10,790,977, Sept. 29, 2020

38. "T-Proof" Gideon Samid https://img.chainnews.com/paper/71f69315d015d9fc5dd4ffbc97f87aab.pdf
39. "T-Proof: Secure Communication via Non-Algorithmic Randomization." Gideon Samid, https://eprint.iacr.org/2016/474
40. "Tailored Key Encryption (TaKE)" Gideon Samid, https://eprint.iacr.org/2000/011.pdf
41. "The Myth of Invincible Encryption" Gideon Samid, Digital Transactions May-June 2005
42. "The Rock of Randomness: A physical oracle for securing data off the digital grid": Gideon Samid, Gary Wnek, Material Research Society Bulletin 09 April 2019
43. "The Ultimate Transposition Cipher (UTC)." Gideon Samid, https://eprint.iacr.org/2015/1033.pdf
44. "Threat Adjusting Security" Gideon Samid, https://eprint.iacr.org/2018/084.pdf
45. "Transmitter for Encoding Information with Randomly Flipped Bits and Transmitting That Information Through a Communication Channel", US Patent 10,728,028 Jul 28, 2020
46. "User Centric Cryptography" Gideon Samid, Proceedings of the International Conference on Security and Management (SAM); Athens, (2018) https://www.proquest.com/openview/a60ecf397b6c46373356a1d4369dce5d/1?pq-origsite=gscholar&cbl=1976342
47. "What a 100-year-old Idea can teach us about Cybersecurity" World Economic Forum, Nov 2017 https://www.weforum.org/agenda/2017/11/what-a-100-year-old-idea-can-teach-us-about-cybersecurity
48. "When Encryption is Not Enough--Effective Concealment of Communication Pattern, even Existence (BitGrey, BitLoop)" Gideon Samid, https://eprint.iacr.org/2019/556
49. "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/Downey2010AlgorithmicRandomnes s.pdf
50. "Communication Theory of Secrecy Systems" Claude Shannon http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf
51. "Computability and randomness" Niels A. The University of Auckland, Clarendon, Oxford, UK, 2008
52. "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
53. "Probabilistic Encryption" Goldwasser, Micali, Jr. of Computer and System Science, Vol 28, No 2, pages 270-299
54. "Shannon's Proof of Vernam Unbreakability" https://www.youtube.com/watch?v=cVsLW1WddVI
55. "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
56. "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
57. "The Unending Cyber War" Gideon Samid, DGS Vitco ISBN 0-9635220-4-3 https://www.amazon.com/Unending-Cyberwar-Gideon- Samid/dp/0963522043
58. "The Code Breakers" David Kahn, The MacMillan Co. 1967.
59. "Edward Snowden: The Untold Story" Wired Mag. Aug 14, 2014
60. "The Innovation Solution Protocol" (Innovation^{SP}), https://InnovationSP.net
61. "Kerckhoffs' Principle" http://www.crypto-it.net/eng/theory/kerckhoffs.html
62. "Equivoe-T: Transposition Equivocation Cryptography" US Patent 10,608,814 March 31, 2020.
63. "SpaceFlip: Unbound Geometry Cryptography" Gideon Samid https://dblp.org/rec/journals/iacr/Samid19.html
64. "Unary Cryptography Demonstration Site" https://UnaryCryptography.com
65. "BitFlip Cyber Demonstration" http://wesecure.net/learn/BitFlipEncrypt.php
66. "SpaceFlip Plus: Ordinal Cryptography" US Patent 11,159,317 * Oct 26, 2021
67. "Efficient Proof of Knowledge of Arbitrarily Large Data Which Remains Undisclosed" US Patent 10,594,480, March 17, 2020.
68. "Cyber Companion: Attaching a Secondary Message to a Primary One" US Patent 10,541,954 Jan21, 2020
69. "Live Documentation (LiDO)" US Patent 10,733,374, Aug 4, 2020
70. "Method for Inhibiting Mass Credentials Theft" US Patent 10,395,053 Aug 27, 2019
71. "Effective Concealment of Communication Pattern (BitGrey, BitLoop)" US Patent 10,673,822, June 2, 2020
72. "Quantum Random Number Generation" https://www.idquantique.com/random-number-generation/overview/
73. "Rock of Randomness" US Patent 10,467,522 Nov 5, 2019
74. "Proving Material Identity with Quantum Randomness -- Financial and General Applications" US Patent 10,754,326. Aug 25, 2020
75. "BitMint Hard Wallet: Digital Payment without Network Communication: No Internet, yet Sustained Payment Regimen between Randomness-Verifiable Hard Wallets" Gideon Samid, 2020 IOT, Electronics and Mechatronics Conference (IEMTRONICS), IEEE International.
76. "Transmitter for Encoding Information with Randomly Flipped Bits and Transmitting That Information Through a Communication Channel" US Patent 10,728,028, July 28, 2020.

77. “Advanced BitFlip: Threat Adjusted, Quantum Ready, Battery Friendly, Application Rich Cipher” US Patent 10,541,808, January 21, 2020.
78. "Split Security Solutions", US Patent Application 17/510,324, Oct 25, 2021
79. "Randomized Bilateral Trust (RABIT): Trust Building Connectivity for Cyber Space (FigLeaf)" U. S. Patent 10,798,065, October 6, 2020.