



International Association for Cryptologic Research

Gideon Samid, Publications

Prof Gideon Samid, PhD
Chief Technology Officer, BitMint
Gideon@BitMint.com
November 13, 2025

Gideon Samid IACR Publications

[2025/1545\(PDF\)](#)Last updated: 2025-08-28

35....Non-Trivial Ciphertexts

Gideon Samid

Implementation

A trivial ciphertext is decrypted per all its bits to a corresponding, singular plaintext. A non-trivial ciphertext (NTC) is comprising decryption-proper bits as well as decryption unfitting bits (decoys) with a decryption discrimination key needed to identify each category. A non-trivial ciphertext may also decrypt to different plaintext options, determined by choice of decryption keys. NTC offer important advantages: giving ad-hoc power to buy extra security paid for with an inflated...

[2025/587\(PDF\)](#)Last updated: 2025-04-01

34....Lifeboats on the Titanic Cryptography

Gideon Samid

Cryptographic protocols

The Titanic was the ship that "could not sink," fortunately its designers installed lifeboats (not enough) despite having no logical grounding for this waste of space and material. It was out of respect for unforeseen surprises. NIST-Post Quantum Ciphers represent the best and the brightest in world crypto intelligence. They are certified as good for their purpose. And likely so, alas, not surely so. If we could find a crypto equivalent for the Titanic Lifeboats, should not we load them up...

[2025/452\(PDF\)](#)Last updated: 2025-07-12

33....Polar Lattice Cryptography

Gideon Samid

Secret-key cryptography

Presenting a protocol that builds a cryptographic solution which shifts security responsibility from the cipher designer to the cipher user. The Polar Lattice is a pattern-devoid cryptographic cipher. It is based on a geometric construct -- a polar lattice, on which the letters of a plaintext alphabet A, are presented as two points each letter, so that to transmit a letter the transmitter transmits a randomized pathway, a trail, (ciphertext) that begins at the first point of the transmitted...

[2025/438\(PDF\)](#)Last updated: 2025-03-07

32....Transmitting Secrets by Transmitting only Plaintext

Gideon Samid

Cryptographic protocols

Presenting a novel use of encryption, not for hiding a secret, but for marking letters. Given a $2n$ letters plaintext, the transmitter encrypts the first n letters with key K_1 to generate corresponding n cipherletters, and encrypts the second n letters with key K_2 to generate n corresponding cipherletters. The transmitter sends the $2n$ cipherletters along with the keys, K_1 and K_2 . The recipient (and any interceptor) will readily decrypt the $2n$ cipherletters to the original plaintext. This...

[2024/129\(PDF\)](#) Last updated: 2024-01-29

31....Finite Key OTP Functionality: Ciphers That Hold Off Attackers Smarter Than Their Designers

Gideon Samid

Foundations

The prevailing ciphers rely on the weak assumption that their attacker is not smarter than expected by their designers. The resultant crypto ecology favors the cryptographic powerhouses, and hinders cyber freedom, cyber privacy and cyber democracy. This weakness can be remedied by using the gold standard of cryptography -- One Time Pad, OTP. Alas, it comes with a prohibitive cost of a key as long as the message it encrypts. When the stakes are high enough users pay this high price because...

[2023/1372\(PDF\)](#) Last updated: 2023-09-15

30,,,,Cryptographic Key Exchange: An Innovation Outlook

Gideon Samid

Implementation

This article evaluates the innovation landscape facing the challenge of generating fresh shared randomness for cryptographic key exchange and various cyber security protocols. It discusses the main innovation thrust today, focused on quantum entanglement and on efficient engineering solutions to BB84, and its related alternatives. This innovation outlook highlights non-quantum solutions, and describes NEPSAR – a mechanical complexity based solution, which is applicable to any number of...

[2023/803\(PDF\)](#)Last updated: 2023-05-31

29,,,,"Tesla Cryptography:" Powering Up Security with Other Than Mathematical Complexity

Gideon Samid

Foundations

For decades now, mathematical complexity is being regarded as the sole means to creating a sufficient distance between a ciphertext and its generating plaintext. Alas, mathematical complexity operates under the irremovable shadow of stealth cryptanalysis. By its nature mathematical complexity is vulnerable to smarter mathematicians and better equipped adversaries, which is a sufficient motivation to explore an alternative means to project security. Applying the Innovation Solution Protocol...

[2023/524\(PDF\)](#)Last updated: 2023-04-11

28....AI Resistant (AIR) Cryptography

Gideon Samid

Attacks and cryptanalysis

highlighting a looming cyber threat emanating from fast developing artificial intelligence. This strategic threat is further magnified with the advent of quantum computers. AI and quantum-AI (QAI) represent a totally new and effective vector of cryptanalytic attack. Much as modern AI successfully completes browser search phrases, so it is increasingly capable of guessing a rather narrow a-priori list of plausible plaintexts. This guessing is most effective over device cryptography where the...

[2023/383\(PDF\)](#)Last updated: 2023-03-16

27...The Prospect of a New Cryptography: Extensive use of non-algorithmic randomness competes with mathematical complexity

Gideon Samid

Secret-key cryptography

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...

[2022/130\(PDF\)](#)Last updated: 2022-02-09

26....A LeVeL Paying Field: Cryptographic Solutions towards Social Accountability and Financial Inclusion

Gideon Samid

Cryptographic protocols

Thousands of digital money protocols compete for attention; the vast majority of them are a minor variation of the Satoshi Nakamoto 2008 proposal. It is time to extract the underlying principles of the Bitcoin revolution and re-assemble them in a way that preserves its benefits and gets rid of its faults. BitMint*LeVeL is a move in this direction. It upholds the fundamental migration of money from hidden bank accounts to cryptographically protected publicly exposed digital coins; it enables...

[2021/1510\(PDF\)](#)Last updated: 2021-11-20

25....Pattern Devoid Cryptography

Gideon Samid

Foundations

Pattern loaded ciphers are at risk of being compromised by exploiting deeper patterns discovered first by the attacker. This reality offers a built-in advantage to prime cryptanalysis institutions. On the flip side, risk of hidden math and faster computing undermines confidence in the prevailing cipher products. To avoid this risk one would resort to building security on the premise of lavish quantities of randomness. Gilbert S. Vernam did it in 1917. Using modern technology, the same idea...

[2021/458\(PDF\)](#)Last updated: 2021-04-08

24....FAMILY KEY CRYPTOGRAPHY: Interchangeable Symmetric Keys; a Different Cryptographic Paradigm

Gideon Samid

Secret-key cryptography

In the current crypto paradigm a single secret key transforms a plaintext into a ciphertext and vice versa, or at most a different key is doing the reverse action. Attackers exposed to the ciphertext are hammering it to extract that single key and the plaintext. This paradigm may be challenged with an alternate setup: using a particular crypto algorithm, there is an infinite number of keys that are perfectly interchangeable -- each has the same effect. Nonetheless they are hard to find. And...

[2020/968\(PDF\)](#) Last updated: 2020-08-18

23....Feeding Cryptographic Protocols with Rich and Reliable Supply of Quantum-Grade Randomness

Gideon Samid

Implementation

Presenting a new technology to fit quantum-randomness into a lump of matter where the randomness is held through the molecular bonds of seeded macro-molecules, and reliably measured in two or more sufficiently exact duplicates, serving as a large reservoir for quantum-grade randomness to support cryptographic protocols.

[2020/389\(PDF\)](#) Last updated: 2020-06-09

22...A Unary Cipher with Advantages over the Vernam Cipher

Gideon Samid

Cryptographic protocols

All mainstay ciphers share an underemphasized vulnerability: their ciphertext commits to its generating plaintext. This means that fast enough computers will cryptanalyze them, and so will an attacker smarter than their designers. By contrast, the Vernam One-Time-Pad cipher is free from these vulnerabilities, which is why it is the cipher of choice against such perceived threats. Alas, Vernam key management is very exacting and cumbersome, and it is also plagued by a serious authentication...

[2019/556\(PDF\)](#) Last updated: 2019-05-25

21...When Encryption is Not Enough -- Effective Concealment of Communication Pattern, even Existence (BitGrey, BitLoop)

Gideon Samid

Cryptographic protocols

How much we say, to whom, and when, is inherently telling, even if the contents of our communication is unclear. In other words: encryption is not enough; neither to secure privacy, nor to maintain confidentiality. Years ago Adi Shamir already predicted that encryption will be bypassed. And it has. The modern dweller of cyber space is routinely violated via her data behavior. Also, often an adversary has the power to compel release of cryptographic keys over well-exposed communication. The...

[2019/285\(PDF\)](#) Last updated: 2019-03-19

20...SpaceFlip : Unbound Geometry Cryptography

Gideon Samid

Foundations

A geometry is a measure of restraint over the allowed $0.5n(n-1)$ distances between a set of n points (e.g. the metric and topological spaces). So defined, geometries lead to associated algebra. The complexities of such algebras are used to build cryptographic primitives. We propose then to

push geometries to the limit -- unbound geometries -- where any two points may be assigned an arbitrary distance value, which may reflect a planning process or a randomized assignment. Regarding these...

[2018/503\(PDF\)](#) Last updated: 2018-05-26

19...Finger Printing Data

Gideon Samid

Applications

By representing data in a unary way, the identity of the bits can be used as a printing pad to stain the data with the identity of its handlers. Passing data will identify its custodians, its pathway, and its bona fide. This technique will allow databases to recover from a massive breach as the thieves will be caught when trying to use this 'sticky data'. Heavily traveled data on networks will accumulate the 'fingerprints' of its holders, to allow for a forensic analysis of fraud attempts,...

[2018/406\(PDF\)](#) Last updated: 2018-05-10

18...“Larger Keys, Less Complexity” A Strategic Proposition

Gideon Samid

Foundations

Cryptographic security is built on two ingredients: a sufficiently large key space, and sufficiently complex processing algorithm. Driven by historic inertia we use fixed size small keys, and dial up the complexity metric in our algorithms. It's time to examine this trend. Effective cryptographic complexity is difficult to achieve, more difficult to verify, and it keeps the responsibility for security in the hands of a few cipher implementers and fewer cipher designers. By contrast,...

[2018/084\(PDF\)](#) Last updated: 2018-01-26

17...Threat-Adjusting Security: BitFlip as an AI-Ready, Post-Quantum cipher

Gideon Samid

Applications

Generally ciphers project a fixed measure of security, defined by the complexity of their algorithms. Alas, threat is variable, and should be met with matching security. It is useless to project insufficient security, and it is wasteful and burdensome to over-secure data. BitFlip comes with threat-adjustable flexibility, established via: (i) smart decoy strategy, (ii) parallel encryption, (iii) uniform letter frequency adjustment – tools which enable the BitFlip user to (a) adjust its...

[2017/366\(PDF\)](#)Last updated: 2017-04-28

16....BitFlip: A Randomness-Rich Cipher

Gideon Samid, Serguei Popov

Secret-key cryptography

We present a cipher that represents a novel strategy: replacing algorithmic complexity with computational simplicity while generating cryptographic efficacy through large as desired quantities of randomness. The BitFlip cipher allows its user to defend herself with credibly appraised mathematical intractability, well-hinged on solid combinatorics. This is the situation when the amount of randomness is small relative to the accumulated amount of processed plaintext. Deploying more randomness,...

[2016/627\(PDF\)](#)Last updated: 2016-06-17

15....Cyber Passport: Preventing Massive Identity Theft

Gideon Samid

Applications

Identity Theft is the fastest rising crime in the United States with about 7% of US adult population victimized annually. This frightening scope warrants a bold government intervention. Here is a detailed proposal. "Cyber Passport" addresses itself to the main threat: a breach of a merchant, bank, or government department resulting in theft of identities of millions of citizens, which for a long time live in fear of residual violations. The solution is based on two principles: (i) online...

[2016/499\(PDF\)](#)Last updated: 2016-05-23

14...Drone Targeted Cryptography

Gideon Samid

Implementation

As flying, camera-bearing drones get smaller and lighter, they increasingly choke on the common ciphers as they interpret their commands, and send back their footage. New paradigm cryptography allows for minimum power, adjustable randomness security to step in, and enable this emerging technology to spy, follow, track, and detect. E.g.: to find survivors in a collapsed structure. We describe here a cryptographic premise where intensive computation is avoided, and security is achieved via...

[2016/474\(PDF\)](#)Last updated: 2016-05-19

13....T-Proof: Secure Communication via Non-Algorithmic Randomization

Gideon Samid

Cryptographic protocols

shared random strings are either communicated or recreated algorithmically in “pseudo” mode, thereby exhibiting innate vulnerability. Proposing a secure protocol based on unshared randomized data, which therefore can be based on ‘white noise’ or other real-world, non algorithmic randomization. Prospective use of this T-Proof protocol includes proving possession of data to a party in possession of same data. The principle: Alice wishes to prove to Bob that she is in possession of secret data...

[2015/1033\(PDF\)](#)Last updated: 2015-10-27

12...The Ultimate Transposition Cipher (UTC)

Gideon Samid

An Ultimate Transposition Cipher (UTC) is defined as a cipher that transposes any permutation of some n elements to any other permutation of the same elements. Hence, by listing together the protected message and plausible alternatives to it, and then mixing it, one secures a ciphertext which the intended reader will readily "un-mix" (using the shared key), but the cryptanalyst will find proper keys for all the 'decoy messages' and will not be able to go further. The UTC transposed...

[2015/510\(PDF\)](#)Last updated: 2015-05-27

11...Equivoe-T: Transposition Equivocation Cryptography

Gideon Samid

Foundations

Plaintext is mixed with AI-generated dis-information which binds the cryptanalyst to an irreducible set of mutually exclusive plausible plaintext candidates. As impractical as Vernam "One Time Pad" cipher has been, it's security strategy: equivocation is fundamentally superior to the prevailing strategy: intractability. Intractability erodes, equivocation endures. Alas, Vernam was an overkill. Equivocation works even if only a few plaintext candidates are left as an irreducible set, which...

[2014/244\(PDF\)](#)Last updated: 2014-04-18

10...bitcoin.BitMint: Reconciling Bitcoin with Central Banks

Gideon Samid

Applications

The sweeping success of the original (2008) bitcoin protocol proves that digital currency has arrived. The mounting opposition from the financial establishment indicates an overshoot. We propose to tame bitcoin into bitcoin.BitMint: keeping the bitcoin excitement -- fitted into real world security, stability and fraud concerns. The basic idea is to excise the bitcoin money generation formula, and otherwise apply bitcoin essentially “as is” over digital coins which are redeemable by the...

[2012/457\(PDF\)](#)Last updated: 2012-08-13

9...Hush Functions Extended to Any Size Input versus Any Size Output

Gideon Samid

Foundations

Traditional hush functions map a large number to a small number such that the reverse-hush has an infinity of solutions, and nonetheless a collision is hard to come by. This primitive is so abundantly useful that one is tempted to extend it such that any number large or small may be mapped to any number larger, or smaller while maintaining the above conditions. This extension would increase the flexibility of the commodity hush primitive, expand its current applications, and likely suggest...

[2011/127\(PDF\)](#)Last updated: 2011-03-15

8...Integer Arithmetic without Arithmetic Addition

Gideon Samid

Foundations

Revisiting long established conventions has proven very fertile in many a case. Let's then revisit the premise that arithmetic must be constructed with the arithmetic addition as its foundation. Here we explore an arithmetic realm over integers without invoking the quintessential operation of addition. We propose an arithmetic constructed over a fundamental mapping of one set of integers into another. We start and focus here on mapping an arbitrary number of integers to a single...

[2010/421\(PDF\)](#)Last updated: 2010-07-30

7...Binomial Sieve Series -- a Prospective Cryptographic Tool

Gideon Samid

Foundations

A Binomial Sieve Series (BSS) is an infinite monotonic set of natural numbers, b_1, b_2, \dots, b_n ($b_i < b_{i+1}$) generated, ('naturally') from any two natural numbers ($x, y \leq x$). If one repeatedly counts b_i elements over the set $X = 1, 2, \dots, x$ (recycled counting) and eliminates each time the

element of X that stops each round of counting, then the surviving element of X is y. Every natural number, per any x, is associated with a certain survivor. We prove that per any x all BSS are infinite and...

[2008/222\(PDF\)](#) Last updated: 2008-05-25

6...Encryption-On-Demand: Practical and Theoretical Considerations

Gideon Samid

Implementation

Alice and Bob may develop a spontaneous, yet infrequent need for online confidential exchange. They may be served by an 'encryption-on-demand' (EoD) service which will enable them to communicate securely with no prior preparations, and no after effects. We delineate a possible EoD service, and describe some of its theoretical and practical features. The proposed framework is a website which could tailor-make an encryption package to be downloaded by both Alice and Bob for their ad-hoc use....

[2007/412\(PDF\)](#) Last updated: 2007-11-08

5...Proposing a Master One-Way Function

Gideon Samid

Making an arbitrary binary string fit as a fixed size cipher key (via hashing) one could use an arbitrary string x as both plaintext and key to generate a ciphertext, y defined as "the crypto square of x", while x is the crypto square root of y. Extended to higher powers, this formalism allows for polynomial morphology that combines all one-way functions candidates into a single master function which is at least as intractable as its best ingredient one-way function. The master list has...

[2004/034\(PDF\)](#) Last updated: 2004-02-16

4...s(n) An Arithmetic Function of Some Interest, and Related Arithmetic

Gideon Samid

Foundations

Every integer $n > 0 \in \mathbb{N}$ defines an increasing monotonic series of integers: n_1, n_2, \dots, n_k , such that $n_k = n_k + k(k-1)/2$. We define as $s(m)$ the number of such series that an integer m belongs to. We prove that there are infinite number of integers with $s=1$, all of the form 2^t (they belong only to the series that they generate, not to any series generated by a smaller integer). We designate them as s-prime integers. All integers with a factor other than 2 are not s-prime ($s>1$), but are...

[2000/062](#)Last updated: 2001-01-05

3...Non-Deforming Digital Watermarks

Gideon Samid

Applications

TaKE cryptography offers subliminal marking of a digital stream so that any tampering, induces an unacceptable distortion of the primary information. Encrypted audio and video streams are decrypted by one key to the original content (e.g. music), and through another key to the digital watermark (e.g. name of legitimate user). Unlike the prevailing methods which are based on distorting the protected contents, or locking it through a digital signature, TaKE -- Tailored Key Encryption --...

[2000/059\(PDF\)](#)Last updated: 2000-12-27

2. Essential Shannon Security with Keys Smaller Than the Encrypted Message

Gideon Samid

Foundations

To a cryptographer the claim that "Shannon Security was achieved with keys smaller than the encrypted message" appears unworthy of attention, much as the claim of "perpetuum mobile" is to a physicist. Albeit, from an engineering point of view solar cells which power satellites exhibit an "essential perpetuum mobile" and are of great interest. Similarly for Shannon Security, as it is explored in this article. We discuss encryption schemes designed to confound a diligent cryptanalyst...

[2000/011\(PDF\)](#)Last updated: 2000-04-21

1. Tailored Key Encryption (TaKE) Tailoring a key for a given pair of plaintext/ciphertext

Gideon Samid

Foundations

Abstract. The prevailing cryptographies are attacked on the basis of the fact that only a single element in the key space will match a plausible plaintext with a given ciphertext. Any cryptography that would violate this unique-key assumption, will achieve added security through deniability (akin to One Time Pad). Such cryptography is being described. It is achieved by breaking away from the prevailing notion that the key is a binary string of a fixed length. The described key is random-size...