Finite Key OTP Functionality

Ciphers That Hold Off Attackers Smarter Than Their Designers

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

Abstract: 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 OTP is immunized against smarter and better equipped attackers. Claude Shannon has shown that this size imposition on the key is non-negotiable in the context he analyzed. Alas, changing the context, one could achieve OTP equivalence. Three simple changes are introduced: (i) make the size of the key an integral part of the secret, (ii) every finite message is encrypted with an arbitrary part of the key, (iii) allow for open-ended dilution of the contents-bearing bits of the ciphertext, with content-devoid bits, which don't confuse the intended recipient, but impose an open-ended cryptanalytic barrier before the attacker. A-priori a cryptanalyst is facing a set of messages each of them deemed plausible to be the one hidden in the ciphertext. If the ciphertext is *Finite Key OTP compliant* then membership in this set will not change after an exhaustive cryptanalytic processing of the ciphertext. This constitutes functional equivalence with OTP. OTP functionality with a shared finite key creates a path to digital freedom, digital privacy and digital democracy.

1.0 Introduction

Fifty years ago cryptography divorced itself from the age-old premise stating that the encryption key and the decryption key are one and the same. The impact of the freedom from this limitation grew to a cultural tsunami; life on cyberspace is enabled by asymmetric cryptography. It is curious, in perspective, that until today cryptography has not released itself from the limitation of the old Kerckhoffs' principle that builds cryptography on the secret identity of a known count of bits. Accordingly a cipher is serviceable, as long as the size of its key is sufficiently large to sustain a brute force attack, given the current computing power, and as long as the mathematical complexity that was used to render the plaintext into the ciphertext is sufficiently robust to sustain smart-force attack, given the current math power. Under these terms however small the key is, it should be good enough to encrypt any message, however large.

This size variance between the key and the message renders the ciphertext to be fully committed to the key that generated it. The likelihood for the ciphertext to be matched with a plausible message and a corresponding key -- other than the one used -- is fast diminishing as the size disproportion grows. This reality creates a mathematical battlefield.

1.1 The Mathematical Battlefield

If a given ciphertext points unequivocally to one and only one key from the key space then the identity of the ciphertext bits bears a mathematical relationship to that key. That means: a smart enough mathematician will construct an algorithm that would regard the ciphertext as an input, and generate the key as an output. Cipher breached.

Let M be an arbitrary scale of 'mathematical difficulty'. Let a given cipher C_1 be associated with mathematical difficulty of measure M_1. M_1 may then be regarded as the cryptanalytic barrier of C_1. We consider a human environment wherein t mutually apprehensive groups of people G_1, G_2, ... G_t share an information highway, but wish to remain private about their own communication, while wishing to read what the others are writing. Let group G_i be of higher mathematical talent than group G_{i+1}. for i = 1,2,...(t-1).

The optimal strategy for the smartest group, G_1, will be to introduce a cipher C_1 which is associated with mathematical difficulty M_1. M_1 may then be regarded as the cryptanalytic barrier of C_1.

The choice of C_1 will be such that the measure of mathematical talent of G_1, which is T_1 is higher than. the barrier M_1, while the respective talents of the other groups: T_2, T_3, .. T_t will be less: $T_i < M_1$. for i=2,3,...t.

In that case cipher C_1 will appear as unbreakable to everyone except to the G_1 people. If everyone is using C_1 for their most sensitive secrets, then all the groups believe that their communication remains private. However group G_1 is reading what the other are writing, even more conveniently than if no encryption was used. Because each group concentrates its most sensitive secrets in the C_1 ciphertext, which group 1 reads right away.

Over time group G_2 also breaks through the mathematical barrier of C_1, and now group G_1 lost its clear advantage. In response group G_1 will construct another cipher C_2 which is associated with a mathematical breach difficulty (extracting the key from the ciphertext), M_2. Where $M_2 > M_1$. Group G_1 is smart enough to break M_2: $T_1 > M_2$, but for group 2 and on we have. $T_i < M_2$. for i=2,3,..t. Group G_1 now introduces cipher C_2 to the community of mutually apprehensive groups and impresses the community that C_1 is no longer strong enough, but C_2 is. Thereby group G_1 restores its advantages.

Overtime these "loops" will repeat through ciphers C_3, C_4,... etc. securing for group G_1 an enduring advantage.

This is a 'mathematical description' of the history of cryptography: a repeated loop; the top mathematical talent constructs ciphers that their adversaries, with less talent are unable to crack. These ciphers are promoted as 'uncrackable' as indicated by the absence of a published breach; creating a most desired state for the leading cryptographic powerhouse: channeling the secrets of interest into a cipher that appears secure to its users while it is an open book to its promoter. Over time mathematical insight on one hand, and computing power on the other hand together render the prevailing cipher into 'insecure'. It is then that the mathematical advantage of the leading cryptographic powerhouses come into action again: more mathematical complexity is engaged and manifest itself with a new cipher, which again most users believe it to be unbreakable, while its designers have the mathematical talent and the computing power to break them. When the new ciphers yield to their former users, this conceptual loop is repeated.

Some sixty years ago computers became the reservoir for world data, and digital communication became the popular method for moving this data about. All this moving took place over a shared information highway. This evolution graduated cryptography from an obscure spy craft few knew anything

about, to a cultural mainstay where assorted algorithms were used to protect data through encryption. The US government was very interested to read what the world writes, and so, as is widely believed, they came up with this ingenious idea to impress the world with a single cipher, broadly regarded as secure, but secretly yielding to the government cracking tools, a combination of mathematical insight and comuting power . It appears to have worked, the whole world used DES -- until computers became fast enough to crack it with brute force and various mathematical shortcuts have surfaced. The US government then upgraded DES to 3DES -- a new application of the cryptographic loop described above. 3DES lasted several decades. In fact only in early 2024 did the US government officially retire 3DES from its data centers. 3DES was replaced by the next loop: AES, which is in force today. AES now stands in the shadow of the new class of computing machine -- the quantum variety -- and the US government is now busy initiating another round of the same loop under the category of Post-Quantum ciphers: another layer of mathematical complexity to keep the discrimination between the NSA top math talent combined with advanced computing, and the community without this combination of talent and machine. This strategy has an endemic flaw. It is never a solid assumption to believe your adversary is not smarter than expected.

While this math-advantage strategy has served the US well for many decades, this very strategy is ready for retirement. Here is why:

Since remaining the world single super power, the US has cast many weaker countries into the adversarial category. These many hostile, or not very friendly countries have no realistic chance to match the US army, air force or navy. The cost of an air carrier battle group is prohibitive for the majority of countries. By contrast the cyber front is where mathematical talent is coming to its power expression. Even a small and poor country can be fortunate enough to have a citizen with the intellectual capacity of Alan Turing. *A single mathematical genius is all that is needed to best the NSA*. A rational analysis of cryptographic reality will lead to the conclusion, then, that the hitherto strategy of math-advantage is loosing its efficacy.

The entire field of cryptography has now to be revisited from the ground up. In fact we go back 107 years to look again at the famous Vernam cipher, patented in 2017, which Claude Shannon, a quarter of a century later, proved to be unbreakable.

What we have done in BitMint was to apply the Innovation^{SP}, [6] and identify the underlying first principles of the Vernam cipher, as well as list the subtle underlying assumptions thereto.

1.2 Challenging the Commitment of the Ciphertext to a single Key

The underlying principle of the cryptographic 'loops' described above is the commitment of the ciphertext to the cryptographic key that generated it. To crack these loops one needs to revisit this premise: *what does it take for a ciphertext not to be committed to the key that generated it?*

Reducing this abstract premise into practical terms, we describe a "cryptographic conflict" where a transmitter releases into the open a ciphertext, C, aimed at a friendly recipient, such that the ciphertext will convey to the recipient a message m_0. The environment includes an adversary who wishes to gain advantage from being exposed to the ciphertext.

A cryptographic advantage is defined as follows: Any given cryptographic conflict situation may be defined with respect to a set Ω of plausible messages m_1, m_2, ... m_h, each of which is associated with a respective probability p_1, p_2, ... p_h to be the one which is actually carried by ciphertext C. These h probability values define a state entropy H for the case in point.

$$H = -\sum_{1}^{h} p_i \, log(p_i)$$

Accordingly we define a cryptographic advantage associated with knowledge of ciphertext C, as a situation where the entropy H is reduced. In other words if the h probability ratings will be less spread out then the ciphertext offers a cryptographic advantage to its attacker. The ideal situation from the attacker's point of view is that the entropy of the situation collapses to zero; one message m_i is identified as the message conveyed by C. $m_i = m_0$. No advantage case is when the entropy of the situation remains unchanged.

This is the logic used by Claude Shannon when he proved that Vernam cipher is mathematically secure. The Vernam cipher C_{OTP} points to all h messages as being the one sent to the recipient, and hence its contents does not offer the attacker any advantage.

The current crop of ciphers where the ciphertext commits to the key that generated it, it also, therefore commits to the message m_0 that was encrypted into C, and the cryptographic conflict becomes a mathematical battleground as described above.

If we are able to release ourselves from the 'commitment' limitation then we can switch the cryptographic conflict into the *entropy battlefield.* The sender wishes to keep the entropy of the situation as high as possible despite sending messages to the recipient, while the attacker wishes to push the entropy down, to zero if possible.

We stop and notice that while Vernam's cipher is working very well as a zero commitment ciphertext generator, it is in fact an over-kill. The Vernam ciphertext will accommodate any plaintext message of same bit count. A message m of bit count |m| will match its C_{OTP} with $2^{|m|}$ messages (and same number of keys), while in every practical situation the set Ω of h plausible messages is much smaller: $|\Omega| << 2^{|m|}$. This points us towards a cipher that shares the underlying principles of Vernam OTP cipher, but is only effective where it should be, with respect to the set of plausible messages.

Two strategies arise: (i) explicit packing, and (ii) probability packing. In the former one packs into the ciphertext all the plausible h messages (the set Ω is assumed to be known to all participants in the situation). An omnipotent attacker will realize that the ciphertext may be interpreted through the h keys that each lead to its corresponding message, so all h messages are covered, and therefore the entropy of the situation remains unchanged, which creates OTP equivalence. A non omnipotent attacker may reveal a subset of Ω and may altogether miss the right message.

In the probability packing strategy the ciphertext creates a situation where probability wise more than one plausible message is left with a non-zero probability to have been the one used. Unlike the former strategy, probability packing has continuity. It may offer a variable advantage to the attacker, diminishing the entropy to some degree but not to zero.

Either strategy the commitment of the ciphertext to its generating key is being successfully challenged, and hence the loop strategy described above will have to be retired. A new cryptographic era comes to cyberspace.

1.3 Allegory

A very fitting way to describe the end of mathematical advantage cryptography is through a short allegory that runs like this: One very smart (VS) person engages a not-so-smart (NSS) fellow in a guessing game. Each in turns would toss two dice, and the other would guess. After one hundred rounds a winner is

declared. The smart person, VS, realized that mathematics guides one to guess the number 7 each time, since it is more likely than other numbers. Thus the smart fellow guessed 7 many times, but not all the times, to keep Not-so-Smart in the dark. Since the Not-so-Smart fellow simply chose randomly along the range 2-12, it so happened that VS won each time they played a game of one hundred rounds.

Over time Mr. Not-so-smart has understood the probability calculus and he too made 7 his favorite choice. In order to keep their advantage the VS people upgraded the game to three dice with a guessing range from 3 to 18. This reaffirmed the VS math advantage for a while until the Not-so-Smart, NSS, figured out the new game. VS reacted by adding more complexity: *if the number shown and the number guessed together add up to a prime number than the guesser gets another guessing chance*. The very smart people figured the new terms to their advantage, but the NSS did not -- and kept losing.

One bright morning the Not-so-Smart became assertive and declared: we are going to reduce the game to its basic simplicity -- throwing one dice only, with a guessing range of 1-6. When the games resumed VS realized that their math advantage has become irrelevant. The game became a level playing field!

That is the effect of Level-Playing cryptography on the Mathematical Advantage cryptography that tries hard to remain relevant.

2.0 Operation

We describe operations to construct ciphers wherein the ciphertext does not commit to its generating plaintext, or generating key. We discuss (i) explicit packing, and (ii) probability packing. A mix of the two is also possible.

Such non committing ciphertexts do not point to the key, nor to the message that generated them and hence this key or this message cannot be extracted from them regardless of cryptanalytic assets.

2.1 Explicit Packaging

To carry out explicit packaging one needs to come up with a cryptographic way to achieve *contents discrimination.*

Contents discrimination is defined over a ciphertext. Let the c bits of a ciphertext C sent to recipient R be mixed with d bits of a 'decoy text' D. Where decoytext bits are bits that are irrelevant for recipient R. The decoytext is content-devoid as far as recipient R is concerned. The mixture, C*(C,D) allows recipient R to separate it. C* → C, D, ignore D and decrypt C. This ability to discriminate between content-bearing bits (C) and content-devoid bits (D) is based on the shared information between the sender of the ciphertext and its recipient R. Say then that an attacker A looking at C* will have no way to separate the mixed stream, C* to C and D without access to the shared key held in secret by the parties.

A cryptographic construction that ensures contents-discrimination as described above can be used for explicit packing.

2.1.1 Explicit Packing Procedure

We consider again a practical cryptographic conflict situation where a ciphertext C is associated with a set Ω comprising h plausible messages m_0, m_1, ... m_h, each associated with probability rating, respectively p_1, p_2, ... p_h.

Transmitter (sender) and recipient share a fully randomized key k_i used to encrypt message m_i to ciphertext c_i.

The transmitter then uses (h-1) randomized keys: k_1, k_2, ...k_{i-1}, k_{i+1}.. k_h to encrypt the other (h-1) plausible messages m_1, m_2, ...m_{i-1},m_{i+1}.. m_h to their respective h-1 ciphertexts: c_1, c_2, ...c_{i-1},c_{i+1}.. c_h.

Next the transmitter will mix all the decoy (t-1) ciphertexts in a content-discrimination mode with the true ciphertext c_i, so that C = c_i. and D = $c_1 + c_2 + ...c_{i-1} + c_{i+1}.. + c_h$, to yield:

$$C^* = C + D = c_1 + c_2 + ... c_h.$$

Recipient R will readily discriminate between the decoy and the contents bearing ciphertext, extract C = c_i from C*, then use its key k_i to decrypt c_i to p_i.

Attacker A will not be able to discriminate between C bits and D bits. For them every bit is potentially contents bearing. An omnipotent attacker will at best discover that every plausible message m_i for i=1,2,...h can be matched with a key k_i that will regard a portion of the ciphertext compendium C* as content bearing (c_i), while regarding all other C* bits as decoy. Accordingly, the entropy of the situation before having

knowledge of C* is the same as after having knowledge of C*, which upgrades this cryptographic situation into OTP functionality -- mathematical secrecy.

2.1.2 Explicit Packing Applications

The explicit packing procedure is most useful in cryptographic situations where the set of plausible plaintext message, Ω, is well defined and rather limited. For example, stock handling instructions may range from 'buy' to 'sell' through 'hold'. Moving on a grid may be: right, left, up, down. In such cases the composite ciphertext C* will easily include all the available messages, keeping the omnipotent attacker in OTP confusion.

In more common cases where the Ω set is not so well defined, one can apply the explicit packing procedure over a subset of Ω, and achieve a corresponding degree of OTP attacker confusion.

Explicit packing can also be used by communicators to protect them against coercion. Let $m_{implicating}$ be the message that implicates the communicators, and let $k_{implicating}$ be the corresponding key. The communicators can set up another key, $k_{innocence}$ and use it to encrypt an innocent message $m_{innocent}$. The composite ciphertext C* will include both $c_{implicating}$ and $c_{innocent}$. When confronted the parties point to $k_{innocent}$ and claim they have communicated $m_{innocent}$.

The explicit packing procedure can be used to build a composite ciphertext that would be interpreted to different plaintext messages by different readers.

2.2 Probability Packaging

Probability packing is a procedure where the contents bearing bits of the ciphertext are mixed with randomized content-devoid bits in a growing proportion as the encrypted accumulated message becomes larger.

Let a key K be used to encrypt an accumulated message M into a cipher C. Let m_i be a plausible message of the set Ω which was not part of M. Let M be mixed with contents-devoid randomized decoy bits D, to form C*(C,D). For a sufficiently large D the probability for identifying a key k_i that would that would encrypt m_i to c_i such that C* can be seen as composed of c_i and the remainder of C*, namely D_i , as decoy bits with respect to k_i can be made as large as desired. And in that case the key K can be denied and k_i may be proclaimed as the shared key so that the exchanged C* is interpreted to m_i and decoy bits. An omnipotent

attacker will have therefore to attach a non-negligent probability to plausible message m_i as the one that has been transmitted through C*.

This logic applies to every member of the plausible set, Ω, thereby affirming the OTP functionality.

This procedure applies because these new ciphers come with an unknown size of key, and any finite amount of message, M, may have been encrypted with only part of the shared key, therefore allowing for an unused key material to be claimed as above.

This procedure applies also without denying the encryption of M. In other words the key claimed by the users may be k_i as above or it may be $K + k_i$. Same for any part of M.

The measure of the probability for any given member message of the plausible set, Ω, to be deemed as a sent message, depends on the particular finite key OTP functionality (FKOF) cipher that is being used, but the overall logic applies to all qualifying ciphers.

The key space from which k_i is drawn, (K_i), is naturally large therefore for any given message m_i, there is a large variety of corresponding key options and a matching bit string c_i such that a large enough decoy string will include a qualifying c_i.

Mixed Packaging; Explicit packing and probability packing can be mixed.

2.3 Contents Discrimination

There are many ways to accomplish contents discrimination. One common method is described herein.

Let a plaintext alphabet A be comprised of n latters a_1, a_2, ... a_n. Let each letter a_i of A be represented by an information "stamp" s_i, where s_i is likely a bit string or a bit string equivalent. The set of stamps S, s_1, s_2, ... s_n is a shared secret between a transmitter and a recipient. The S values are being randomized.

Let T be certain logical terms that may be satisfied T=1 or not satisfied T=0, as applied to a pointer information package p_i to a pointed stamp s_i.

$T(p_i, s_i) = 1; p_i \rightarrow s_i$

$T(p_i, s_i) = 0; p_i \not\rightarrow s_i$

A transmitter will send letter a_i to the recipient by sending them a pointer p_i such that:

$T(p_i, s_i) = 1; p_i \rightarrow s_i$

$T(p_i, s_j) = 0; p_i \not\rightarrow s_j$ *for j=1,2,..(i-1),(i+1),..n*

If p_i does not satisfy the two conditions above then p_i is regarded as decoy -- contents devoid. Any pointer package p_i that either does not satisfy T with respect to s_i or satisfies T for both s_i and some other s_j, where $j \neq i$, qualifies as decoy.

We further impose that every stamp s_i may be pointed to by an at will large infinite number of pointers, and each pointer may point to at will large number of stamps. This allows for a decoy-compliant ciphertext to be generated.

Case in point: BitFlip [7]. Here the stamp is a bit string of arbitrary length, and the pointer is a bit string of same length. The T-term is a specified Hamming distance between the stamp and the pointer. For a Hamming distance close to half size of the string there are many pointer strings that point to a given stamp, and in turn, there are many stamps to which a given pointer may point. A pointer string that points to no stamp, or that points to more stamps than one is a decoy. A given letter can be represented by more than one stamp.

2.4 Implementation

Finite-Key OTP functional (FKOF) compliant ciphers use randomness extensively. The better the quality of the randomness they use -- the stronger they are. The weakest case is algorithmic randomness. It can be improved with certain tools and methodologies. The more secure is randomness generated through physical complexity and the most secure is quantum randomness.

Two categories of randomness are involved: shared and unilateral. The former is used for the key and the latter for operational choices and for ciphertext dilution.

Some FKOF-compliant ciphers pack a lot of information into the key by using a geometric key where the randomized geometry of the key structure adds entropy to the bit count. The key size is always part of the secret.

The use of unilateral randomness is managed by the transmitter, who is also the party that is most aware as to how sensitive a particular message is.

No doubt that the open size of the key and the large variety of the ciphertext flow are not welcome situations for their well-organized cryptographic system builder. Alas, this inconvenient is a reasonable price for one to pay for the benefit of security against an attacker smarter than one is.

The detailed technology, the discussions of various ciphers, etc. are extensively covered in reference: [1] and [2].

3.0 Digital Freedom, Digital Privacy, Digital Democracy

In a finite key OTP compliant regimen any two or more remote parties who share a private key can communicate with mathematical assurance that their data traffic cannot be hacked and unveil the contents of their exchange. The parties may have shared their private key a-priori, or have used any of the prevailing means to allow remote parties to share a secret key, but once the shared secret key is there, then FKO-compliant cryptography will ensure private communication. This means that individuals, pairs of people, or a large group of people or organizations in cyberspace will have the freedom to organize, debate, communicate with complete privacy. This will emulate the pre cyberspace reality where people convene in private and communicate in confidence.

There are further cryptographic tools that will allow parties to hide the fact that they communicated at all.

One envisions the FKO-compliant regimen to allow residents in cyberspace to privately organize against any authoritarian power which may be aiming to choke off free speech, and the freedom to organize. FKO compliance will ensure power to the governed, the voters. Without FKO-compliance democracy in the digital age would be in jeopardy. If math-advantage remains relevant in every day cryptography then the powers that be can spot any budding resistance, however civilized. If the government has access to things people say in private, it can extinguish any attempt to assemble a counter movement in its budding state. The democratic freedom to speak up, to organize, is only meaningful if the people have the means to prepare for it without interruption. And in cyberspace these means are technology, and in particular cryptography.

One must admit that FKO-compliance privacy will also help the criminal element and terrorists among us, however, this is a price worth paying because what is being bought for that price is digital freedom, digital privacy, digital democracy.

Reference

A thorough review of existing FKO-compliant ciphers is given in the chapter

[1]"Pattern Devoid Cryptography" in the book "Cryptography - Recent Advances and Research Perspectives" Dr. Sudhakar Radhakrishnan, Editor. https://www.intechopen.com/online-first/pattern-devoid-cryptography

Further description of the methodology is given in:

[2] "Tesla Cryptography:" Powering Up Security with Other Than Mathematical Complexity https://eprint.iacr.org/2023/803

Background Items:

[3]. Shannon Proof of Vernam's Cipher Unbreakability

https://www.youtube.com/watch?v=cVsLW1WddVI&t=135s

[4] "Communication Theory of Secrecy Systems". Claude Shannon (1949) http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf

[5]. USPTO “Secret Signaling System” US1310719A (The Vernam Cipher)

[6] "Artificial Intelligence Assisted Innovation" G. Samid (2020) https://www.intechopen.com/chapters/75159

Finite Key OTP Compliant Ciphers:

[7] BitFlip -- A Randomness Rich Cipher, Popov, Samid, (2017) https://eprint.iacr.org/2017/366

[8] A Unary Cipher with Advantages over the Vernam Cipher, 2020, Samid https://eprint.iacr.org/2020/389

[9] SpaceFlip : Unbound Geometry Cryptography, Samid, 2020, https://eprint.iacr.org/2019/285

Literary Companion:

The implications of a finite key OTP compliant cipher are projected to reverberate cultural changes in cyberspace, owing to the new disposition between the public and security technology. Musing on such possible changes led to penning a cyber thriller:

[10] "The Cipher Who Came in from the Cold" Samid, 2022, available as e-book everywhere. https://www.bitmintalk.com/thriller