The Perpetual Equivocation Method (White Paper)

Helder Figueira
Perpetual Encryption, London, England;

E-Mail: helder@perpetualencryption.com URL: www.perpetualencryption.com

Abstract. In this paper, we firstly introduce the concept of Perpetual Equivocation and then propose a new information-theoretic multi-purpose encryption scheme which uses the concept in a practical manner, namely the Perpetual Encryption Stream Cipher. By expanding on Shannon's treatment of equivocation as a valid secrecy index for information-theoretic security, specifically "ideal secrecy", we demonstrate that the addition of entropy to a cryptosystem at a faster rate than it is consumed in the encryption process, allows for the augmentation of the equivocation of key $H_E(K)$ and message $H_E(M)$, such that they never attain unity, thereby guaranteeing information theoretic security using a finite length key, irrespective of the length of the message M.

In short, we demonstrate a practical means of overcoming the problems which have prevented one-time pads from being used in practice.

Index Terms – perfect secrecy; ideal secrecy; secret key; perpetual encryption

© Perpetual Encryption (2016), London, UK.

All Rights Reserved

The Perpetual Equivocation White Paper (and its components, including this Title Page) is copyright material and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the author or the publisher, as allowed under the terms and conditions under which it was purchased or distributed, or as strictly permitted by applicable copyright law. The unauthorised distribution or use of this text in any manner, will be construed as a direct infringement of the author's and publisher's rights, and the author and publisher will seek whatever legal remedies may be available.

1 Introduction

The Perpetual Equivocation concept and its practical implementation, the Perpetual Encryption Cipher (PE Cipher), is presented in this paper.

This paper is firmly grounded in the principles of information theoretic secrecy and equivocation as defined by Claude Shannon in his seminal 1949 paper "Communication Theory of Secrecy Systems" [1]. For the sake of brevity and in keeping with Shannon's definitions and proofs, readers are requested to familiarise themselves intimately with Shannon's paper, specifically with the basic concepts of information theory such as redundancy, and the definitions of "perfect secrecy", "ideal secrecy" and equivocation.

From a security definition perspective, we will therefore be strictly limited to the principles of information theoretic security such that "perfect secrecy" is attained when the *a priori* message probabilities are equal to the *a posteriori* message probabilities (and thus the equivocation of key $H_E(K)$ is exactly equal to the equivocation of message $H_E(M)$, namely $H_E(K) == H_E(M)$, and "ideal secrecy" is attained when the equivocation of message or key is not equal to unity, such that $H_E(M) \neq 0$ or $H_E(K) \neq 0$. In other words, "perfect secrecy" is attained when an assailant cannot reduce the probable set of all possible messages before encryption irrespective of the amount of cryptanalysis on the intercepted ciphertext, and "ideal secrecy" is attained when the assailant cannot reduce that probable set of all possible messages before encryption to a single unique message.

Considering the advent of the QC/AI (quantum computing / artificial intelligence) security threat, we assume an assailant with unbounded time, computational and cryptanalytic capabilities. The Perpetual Equivocation method proposed in this paper therefore represents a watershed with regards to Shannon's statement that "perfect secrecy" requires an infinite key in order to encrypt an infinite number of messages. We propose that "perfect secrecy" can be exceeded using a finite length key, and message expansion with random strings of at most the length of the message, irrespective of the length of the message, and provided the key is at least 100 bits in length.

1.1 Importance of Results

The research in this paper has a number of important theoretical and practical implications.

1. Current academic treatments of "perfect secrecy" use the one-time pad as an example and hold that although it is the best security that can be attained theoretically, it is practically impossible. We show that "perfect secrecy" is a glass ceiling, and only represents the best that can be attained within the very limited scope of a pure cipher using a static key and message. The Perpetual Equivocation method allows for the practical implementation of an information-theoretic cryptosystem. Note that the one-time pad is almost impossible to use in a digital context.
2. We therefore open up an entirely new field of information theoretic security – equivocation (conditional entropy) augmentation cryptography – Perpetual Equivocation. Technically, we demonstrate that "ideal secrecy" is not inferior to "perfect secrecy", indeed it can be superior from a security perspective.
3. Message expansion using random strings allows for the reduction of message redundancy.
4. We demonstrate an exception to Shannon's rule that "perfect secrecy" requires a key as long as the message, and demonstrate that "perfect secrecy" is a balancing act, and can be

exceeded using a finite length key, irrespective of the length of the message. Technically, we use a finite key to encrypt an infinite key, which can then be used to encrypt any infinite number of messages.

5. We propose a simple example of a viable PE cipher which uses the principle of Perpetual Equivocation.

In section 2 of this paper, we extend Shannon's treatment of equivocation, or conditional entropy, beyond static key and message systems and demonstrate Perpetual Equivocation, or perpetual equivocation augmentation using entropy augmentation. We also challenge a number of information theoretic security notions and highlight some exceptions to various information theoretic principles. Section 3 describes the Perpetual Encryption cipher from a conceptual perspective. Section 4 concludes the paper.

2 Information Theory and Equivocation

With his 1949 "Communication Theory of Secrecy Systems" paper, Shannon mathematically defined what it means to be information theoretically secure. He therefore defined "perfect secrecy", "ideal secrecy" and explained the use of equivocation as a theoretical secrecy index. All cryptographic terms used, will follow the definitions as laid out by Shannon.

For the purposes of brevity, this section on information theory basics has been moved to Appendix A at the end of this paper. The appendix describes and defines various information theory elements which including information, entropy, redundancy, probability etc. In the event of any discrepancy, Shannon's definitions will take precedence.

2.1 Perfect Secrecy

Shannon's Definition of Perfect Secrecy is as follows:

> **Definition 1. (Perfect Secrecy)** *"Let us suppose that the possible messages are finite in number $M_1,\ldots, M_n$ and have* **a priori** *probabilities $P(M_1), \ldots, P(M_n)$, and that these are enciphered into the possible cryptograms $E_1,\ldots, E_m$ by $E = T_iM$. The cryptanalyst intercepts a particular E and can then calculate, in principle at least, the* **a posteriori** *probabilities for the various messages, $P_E(M)$. It is natural to define perfect secrecy by the condition that, for all E the* **a posteriori** *probabilities* ***are equal*** *to the* **a priori** *probabilities independently of the values of these." (Shannon's Definition)*

Shannon's Perfect Secrecy Equation

Shannon's interpretation of Bayes' Theorem in the cryptographic context of message *M* and cryptogram *E* leads to the "perfect secrecy" equality equation:

$$P(M|E) = \frac{P(E|M) * P(M)}{P(E)}$$

where:

P(M)	= the ***a priori*** probability of message *M*.
P(E)	= probability of obtaining cryptogram *E* from any cause.

$P(E\|M)$ or $P_M(E)$	= a conditional probability, namely the probability of observing cryptogram E if message M is chosen – namely the sum of the probabilities of all keys which produce cryptogram E from message M.
$P(M\|E)$ or $P_E(M)$	= the ***a posteriori*** probability of message *M* if cryptogram *E* is intercepted.

"Perfect secrecy" requires $P(M|E) = P(M)$ for all *E* and *M*. $P(M) = 0$ is excluded since equality is independent of the values of $P(M)$. Likewise, if $P(E|M) = P(E)$, then $P(M|E) = P(M)$. Any inequality in $P(M|E) = P(M)$, will render the perfect secrecy condition invalid. It is essentially a perfectly balanced condition.

Inequality not only occurs in the XXX usual case where $P(M|E) < P(M)$ when the *a priori* message probabilities have been reduced through cryptanalysis, but also includes the special exception case where $P(M|E) > P(M)$. In defining pure ciphers, Shannon demonstrated that with pure ciphers, P(M|E) is independent of the key chosen, with all keys being equally likely.

Exploring the Boundaries of Perfect Secrecy

The "perfect secrecy" equality as proposed by Shannon is wholly dependent on two requirements. Firstly, that it must be possible, in principle at least to calculate the *a priori* message probabilities $P(M)$, and secondly that it must be possible to determine the *a posteriori* message probabilities $P(M|E)$. However, the exception where $P(M|E) > P(M)$ occurs, relates specifically to the situation where messages are expanded using random strings.

In the context of a one-time pad or a Vigenere cipher using $E_i=M_i+K_i(mod\ n)$ modular addition, or an XOR, the encryption of a message *M* with an equal length key *K* results in a ciphertext *E* of similar length. The interception of *E* by an assailant allows for the trivial calculation of $P(M)$ since the message length is known. Likewise the calculation of $P(M|E)$ is also trivial given that the assailant can derive all *K* and *M* relationships given the ciphertext *E*.

> **Theorem 1. (Exceeding Perfect Secrecy with Random Strings)** *Perfect secrecy requires P(M|E) to be exactly equal to P(M). In the case where a known message M is expanded with a random string of any length, and encrypted with two pure ciphers such as a Vigenere and a transposition, the* a posteriori *message probabilities P(M|E) will be greater than P(M), breaching the "perfect secrecy" condition, yet be more secure than encrypting with a Vigenere alone (which is perfectly secret if the key is as long as the message)*
>
> **Proof:** Consider the case where that same message *M* of length *N* is expanded with a random string *R* also of length *N*, and the concatenated string is subsequently super-encrypted with two encryption operations, namely a Vigenere and a transposition cipher each using a key of length *N* such that $E=T_{k2}(V_{k1}(M+R))$, and decryption entailing $M=(V_{k1}^{-1}(T_{k2}^{-1}(E))) – R$. In such a case, with a Vigenere and a transposition, it is not possible from the ciphertext to distinguish which letters belong to the message *M* or the random string *R*. With 2 possible sources for viable messages, namely *M* and *R*, the effective *a priori* message probabilities for *M*, namely $P(M)$, are "polluted" by the additional message source *R*. In such a case, the *a posteriori* message probabilities of *M,* namely $P(M|E)$, are augmented by $P(R|E)$ such that $P(M) < P(M|E) + P(R|E)$. Thus we have the exceptional condition that whilst the

Vigenere ensures “perfect secrecy”, and the transposition with independent key adds to the security of the cipher, making it more secure than the Vigenere alone, $P(M) < P(M|E) + P(R|E)$, or alternatively, $P(M) \neq P(M,R|E)$, and thus it is not “perfectly secret”, yet stronger than if one simply used a Vigenere alone. We shall later see that “ideal secrecy” is applicable in all cases where $P(M) \neq P(M|E)$, and $P(M) \neq 1$.

The exception mentioned above can be further enhanced, by segmenting the message *M* into random variable length segments $M=\{M_1||M_2||M_3,\ldots,M_{n-1}||M_n\}$, and concatenating each segment with a random variable length random string, $\{M_1||R_1, M_2||R_2, M_3||R_3,\ldots, M_{n-1}||R_{n-1}, M_n||R_n\}$, and then applying sequential Vigenere and transposition encryptions over each variable length concatenated $\{M||R\}$ segment using equivalent length encryption operations. The required variables for message segment and random string lengths can be communicated in the random strings contained in previous segments. The resultant ciphertext can then be presented in a contiguous manner, hiding the exact extent or length of the encryption operations as shown below:

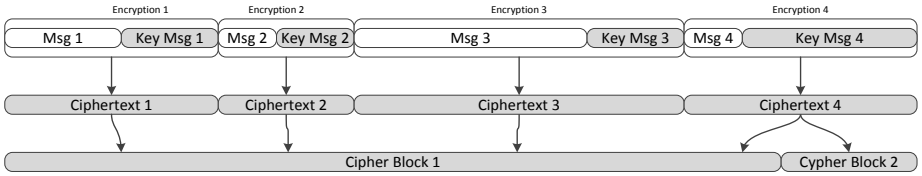

Figure 1: Random arrangement of message, random strings and encryption operations

Thus, in such a case, upon the assailant intercepting a ciphertext *E*, the *a priori* message probabilities of *M* must be expanded to include all possible $\{M||R\}$ segments, since it is not possible to derive the length of *M or R* from the ciphertext alone. In addition, since message segments may include only *R* with no *M*, with variable length encryptions, the assailant must therefore account for all possibilities of *M*, such that $0 \leq P(M) \leq P(M) * P(R)$. Under these circumstances, the calculation of $P(M)$ which is necessary to determine “perfect secrecy” becomes problematic since it must cover all possible $\{M||R\}$ segment possibilities (with regards to all possible variable length $\{M||R\}$ segments which may be contained in the ciphertext, and the probable distribution of the values of the individual M and R components of each $\{M||R\}$ segment). With every character of the ciphertext, the number of possible variations in P(M) increases exponentially according to the following formula:

$$= \sum_{k=0}^{n} 2^{n+1}$$

Thus, by the 128th ciphertext character, there are 6.8×10^{38} possible segment and content combinations, each having a distinct *a priori* set of probable messages $P(M)$. In other words, there are more possible sets of distinct *a priori* message probability $P(M)$, than there are distinct values in a 256 bit key. Thus, it is no longer possible, even in principle, to calculate the *a priori* message probabilities P(M), given *E*, because it is impossible to ascertain with certainty exactly which P(M) it is. In such a case, where all possible variations of $P(M)$ can be calculated but it is impossible to discern exactly which P(M) is in play, how exactly does one ascertain whether “perfect secrecy” has been attained?

2.4 Equivocation

Shannon defined "perfect secrecy" on the basis of the conditional probability of message *P(M)* and ciphertext *P(E)*. Note that there is no mention of the probability of the key *P(K),* just that it must be truly random, or have entropy as large as *log n*, where *n* includes all possible variations of the key.

Equivocation is essentially the application of Bayes Theorem to the message and the key entropy, with regards to a known ciphertext. More specifically, Shannon proposed equivocation (or conditional entropy) as a theoretical secrecy index, and highlighted two key equivocations, namely equivocation of message $H_E(M)$ and equivocation of key $H_E(K)$. Equivocation is a function of N, the number of ciphertext letters intercepted, and thus the quantity $H_E(N)$ determines in a statistical way how much intercepted material N is required to obtain a unique "solution" to the cryptogram

From a practical perspective, equivocation allows for the determination of the *a priori* and *a posteriori* message and key probabilities, such that they may be plotted and visualised on a graph.

Shannon's paper provides the proof that in the case of a static key cryptosystem "perfect secrecy" requires a key as long as the message or more specifically, that following interception of the ciphertext, the *a posteriori* message probabilities derived by the assailant are exactly equal to the *a priori* message probabilities. In other words, since the assailant is unable to reduce the set of all possible messages prior to interception, the *a priori* message probabilities the act of cryptanalysis is largely pointless.

Equivocation therefore allows for the calculation and determination of the rate at which an assailant may derive the valid set of message and key probabilities, given the amount of ciphertext that has been intercepted.

In addition, Shannon stated that the entropy of a cryptosystem is limited to the key entropy. In dealing with finite length keys, Shannon demonstrated that the interception of additional ciphertext letters beyond the length of the key results in a reduction in the *a posteriori* message probabilities such that at some point (the unicity point), only a single viable decryption remains.

The reduced *a posteriori* message and key probabilities may be calculated with regards to the intercepted ciphertext E, on the basis of the conditional entropy of message *M* or key *K* given the captured ciphertext.

Explaining Equivocation

With a set of possibilities with probabilities $p_1, p_2, \ldots p_n$, the amount of information or entropy information *H* for a probability space can be calculated using the formula $H = -\Sigma p_i \log p_i$ .Thus, the entropy for the message *M* or key *K* can be calculated using the following formulas: $H(M) = -\Sigma p(M) \log p(M)$, and $H(K) = -\Sigma p(K) \log p(K)$. The conditional entropy or equivocation of message $H_E(M)$ and key $H_E(K)$, as proposed by Shannon, is therefore the conditional entropy of *M* and *K* given *E* and can be calculated using the following formulas:

$$H_E(M) = \sum_{E,K}^{\infty}(P_E(\mathrm{E},\mathrm{K}) \log P_E(\mathrm{K}) \quad) \qquad , H_E(K) = \sum_{E,K}^{\infty}(P_E(\mathrm{E},\mathrm{K}) \log P_E(\mathrm{K}) \quad)$$

where *M* is the message, *K* is the key and *E* is the cryptogram. *P(E,K)* represents the probability of *K* and *E*, and $P_E(K)$ is the *a posteriori* probability of *K* given E. Likewise, *P(E,M)* and $P_E(M)$ represent similar probabilities with regards to *M*.

With regards to the properties of equivocation, Shannon demonstrated that the equivocation of key $H_E(K)$ is a non-increasing function of *N*, where *N* is the number of intercepted ciphertext letters.

However, we propose some additional properties of equivocation with regards to the fact that it can be increased, and that the equivocation of key does not decrease with random string messages.

> **Theorem 3. (Equivocation of key can be increased Indefinitely)** *The equivocation of key is increased when key entropy is applied before encryption, and when additional independent key entropy is added to the existing key entropy before or after encryption.*
>
> **Proof:** Prior to encryption, assume that there is an empty key space is known, $K_0 = \{0,0,0,0\}$, and that $H(K_0) = 1$ and $H_E(K_0)$ is equal to 0. The insertion of a key K_1 into the known key space using modular addition (thus encrypting it), results in $H(K_1) = H(K_0) + H(K_1)$, thus $H_E(K_1)$ is increased. Adding an additional independent key K_2 results in $H(K_2) = H(K_1) + H(K_2)$ and again, $H_E(K_2)$ is increased. In the case where the existing key space is used in encryption, $H_E(K)$ is reduced, but the entropy of the existing key will be augmented if the new key is encrypted with the old key using modular addition. There is no limit as to how many times the existing key space may be encrypted with new key entropy, or when it may be encrypted, each encryption with new key entropy will augment the entropy (and the equivocation) of the key space provided the new entropy is independent from the key space. The only limitation is that the entropy of the existing key space cannot be increased beyond the maximum entropy that it can accommodate, namely - $\Sigma p(K) \log p(K)$.

The encryption of a message having redundancy using a finite length key, will result in a decrease in the equivocation of key, and an increase and subsequent decrease in equivocation of message. Random string messages behave differently, since they ensure *HE(K) = H(K)*, and thereby, $H_E(M)$ is increased whilst $H_E(K)$ remains constant.

> **Theorem 4. (Equivocation of key is not reduced with random string messages)** *The encryption of a random string does not result in a decrease in HE(K), irrespective of the length of the random string.*
>
> **Proof:** From Shannon's paper, we note that $H_E(K) = H(K) – DN$, where *D* is the redundancy in the message and *N* is the number of intercepted ciphertext letters. Since *D* = 0 for a random string message, $H_E(K) = H(K) – 0N = H(K)$

In direct contrast to random strings having no redundancy, we have known plaintext messages having no information. The formula $H_E(K) = H(K) – DN$ offers an interesting solution to the problem of known plaintext attacks, in that there is a limit to the amount of key entropy $H_E(K)$which can be reduced. The use of super encryption, or compound encryption using multiple encryption operations with multiple keys, allows the key entropy *H(K)* and thus the equivocation of key $H_E(K)$ to be augmented with each additional key, but the $H_E(K)$ can at most only be reduced by the redundancy in the message.

Theorem 5. (Increasing the equivocation of key $H_E(K)$ is unlimited, decreasing is limited) *The use of compound encryption with independent keys, allows for unlimited increases in the equivocation in key $H_E(K)$, with every independent encryption key, but $H_E(K)$ can only be reduced by the amount of redundancy D in the message.*

Proof: Like the above theorem, let us note that $H_E(K) = H(K) - DN$, where D is the redundancy in the message and N is the number of intercepted ciphertext letters. Since HE(K) can be increased, in the case of multiple encryptions with multiple independent keys $\{K_1,K_2,\ldots,K_n\}$, if $H(K) = H(K_1) + H(K_2) + \ldots + H(K_n)$, then given that $H_E(K) = H(K) - DN$, we have

$$H_E(K) = (H(K_1) + H(K_2) + \ldots + H(K_n)) - DN$$

alternatively, in the case of two encryptions

$$H_E(K_1) = H(K_1) - DN$$

$H_E(K_2) = H(K_2) - 0N$, since the first encryption has no redundancy, thus

$$H_E(K) = H_E(K_1) + H_E(K_2).$$

Following the first Vigenere encryption with key K_1, $H_E(M)$ will increase and $H_E(K) = H_E(K_1)$ will decrease such that at length N, $H_E(M) = H_E(K)$. Applying a second Vigenere encryption using an independent key K_2, as long as the encryption space, will result in the effective equivocation of the key becoming $H_E(K) = H_E(K_1) + H_E(K_2)$.

Thus, it can be demonstrated with an experiment, that in the case of where a known plaintext is encrypted twice with two Vigenere or any combination of pure ciphers with independent keys as long as the message, the assailant gains no advantage in information with regards to the second key, even in the case of a known plaintext.

2.4 Ideal Secrecy

Shannon's "ideal secrecy", definition is as follows:

Definition 2. (Ideal Secrecy) "*With a finite key size, the equivocation of key and message generally approaches zero, but not necessarily so. In fact, it is possible for $H_E(K)$ to remain constant at its initial value H(K). Then, no matter how much material is intercepted, there is not a unique solution but many of comparable probability. We will define an "ideal" system as one in which $H_E(K)$ and $H_E(M)$ do not approach zero as $N \rightarrow \infty$. A "strongly ideal" system is one in which $H_E(K)$ remains constant at H(K)." (Shannon's Definition).*

Message redundancy is of great importance to cryptanalysts and the determination of "ideal secrecy" in particular. Every natural language has an inherent statistically valid structure with regards to letter, word and sentence arrangements, such that certain combinations of letters and words do not constitute valid representations of the natural language. For a given message length the proportion of valid to invalid possible messages can be represented as the proportion of average information to average redundancy for that language. For normal English, the average proportion of information to redundancy in each 8 bit character is about 1.3 bits information to 6.7 bits redundancy (16% info, 84% redundancy).

The above equation therefore specifies the amount of ciphertext required to successfully execute a brute-force attack on the key or the message. With ordinary English (having about 84% redundancy – 6.7 bits of every 8 bits), and using a 256 bit key (32 bytes or characters), the unicity distance is

32/0.84 = 38.09 bytes. Thus any message having less than 38 characters will have “ideal secrecy”, and be secure.

When a finite key (shorter than the message) is used with a cryptosystem, and *N* letters of the cryptogram are intercepted, the assailant will be in principle, able to determine the probabilities of the various viable messages which may be contained within the ciphertext. When *N* increases, the number of possible viable messages will decrease until there is a single uniquely valid message for the cryptogram. As mentioned previously, equivocation is the quantity $H_E(N)$ which determines in a statistical way how much intercepted material is required to obtain a unique “solution” to the cryptogram. With random ciphers having keys with *H(K)* entropy, the point which indicates the amount of ciphertext required to produce a unique result is called the “unicity point”, or “unicity distance” and for most symmetric cryptosystems is calculated as :

$Unicity\ Distance = \frac{H(K)}{D}$, where

- $H(K) = log_2 (K)$ - the entropy of the key is the base 2 logarithm of the number of possible keys. A cryptosystem with a 64 bit key therefore has 64 bits of entropy.
- *D* = the redundancy of the language of the message.

Therefore, the amount of redundancy in a message is of great importance when determining whether a cryptosystem has attained *ideal secrecy.* The greater the redundancy, the greater the reduction in the equivocation of key $H_E(K)$. However, Shannon’s treatment of *ideal secrecy* was limited to instances where the redundancy of a message was reduced through compression.

Shannon noted that if a language consists of a sequence of letters all chosen independently and with equal probabilities, then the redundancy is zero, and we have a strongly ideal system with $H_E(K) = H(K)$. Inadvertently, this includes ransom string messages.

> **Theorem 6. (Random Strings reduce overall message redundancy)** *The redundancy of messages may be decreased, when messages are combined with a random string and a transposition is applied over the combined string.*
>
> **Proof:** Assume that the message and the random string have the same language and therefore the same absolute language rate R, where $R = log_2 L$, and where *L* is the number of characters in the language. The amount of information (or entropy) in the message and the random string is combined when H(M) and H(R) are concatenated. The application of a transformation over the combined set results in $H(M,R) = H(M) + H(R)$, dissipating the redundancy of the message over the entire message space.

Irrespectively, *perfect secrecy* and *ideal secrecy* systems have one characteristic in common – they prevent an assailant from effectively elimination all *a posteriori* message probabilities. The presence of any known plaintext, such as standard document headers or standard transmission headers, reduces the effective *H(K)* key entropy and thus the unicity distance. However, in the same way that predictable known plaintext effectively reduces the unicity distance calculation, random strings are capable of increasing the unicity distance, or in special cases even resetting the “unicity distance” calculation completely.

2.5 Perpetual Equivocation

Thus, from Shannon's perspective, perfect secrecy requires an infinite amount of key in order to encrypt an infinite number and length of messages. With keys of finite length, the equivocation of messages and keys will in general approach zero at the unicity point, where there will be a unique solution. An "ideal secrecy "system is therefore one in which the $H_E(K)$ and $H_E(M)$ do not approach zero as N tends to infinity. In other words, any secrecy system where the ciphertext is shorter than the unicity distance is "ideally secret".

In addition, he defined "strongly ideal secrecy" when $H_E(K)$ remains constant at $H(K)$. Unfortunately, Shannon did not consider the prospect of entropy augmentation, namely where $H_E(K)$ may be increased or augmented, since he limited himself to static key systems and there is therefore a limit to the amount of entropy that a finite length key space may hold, never above its maximum, $H_E(K)$.

Using the theorems mentioned above, we will now demonstrate that it is possible to continuously augment the entropy in a cryptosystem, such that $H_E(K)$ and $H_E(M)$ never approach zero, using random strings and multiple encryption. Thus, with every augmentation in system entropy, the unicity distance calculation is restarted, and therefore the unicity distance is moved further towards infinity, always being longer than the ciphertext.

If the entropy of the cryptosystem can be augmented after every use of the key space in an encryption, and the key space can be increased in length to accommodate the additional entropy, then every encryption operation effectively entails a "perfectly secret" encryption. Under these conditions, we have the exception, that "perfect secrecy" can be exceeded using a finite length key.

The Underlying Concepts

There are three underlying principles to perpetual equivocation:

1. With a one-time pad, there are two required communication channels, one for key distribution and one for encryption. There is the possibility that both channels may be combined with every encryption, such that the entropy required for the next encryption may be transmitted with the encrypted message.
2. Whilst Shannon stated that "perfect secrecy" requires an infinite length key for an infinite number of messages, there is the possibility that a finite length key may be used to encrypt an infinite length key which is used to encrypt the messages.
3. The intuitive concept of inflight refuelling, explains how an aircraft may be theoretically allowed to maintain infinite flight, never landing, without requiring an infinitely large fuel tank. An infinite amount of fuel is required however.

With Perpetual Equivocation, we apply all three concepts to cryptography. If entropy can be perpetually transmitted and injected into a cryptosystem, then "perfect secrecy" can be attained with a finite length key, and "ideal secrecy" can be attained, irrespective of the amount of ciphertext.

The Mechanics of Perpetual Equivocation

We will demonstrate the benefit of perpetual equivocation using a comparative example.

Without Perpetual Equivocation. Let us assume we have a 16-byte message in English, with redundancy D of 0.84 (84%), and a key K of finite length of 10 bytes with 2^{80} possible values and $H(K)$

= 80. Using a Vigenere modular addition encryption, and using Shannon's unicity distance calculation for a random cipher , the unicity distance for the encryption is calculated as follows:

$$\frac{H(K)}{D} = +\frac{80}{0.84} = 95.23\ bits = 11.90\ bytes$$

Since the length of the message is 16 bytes, and the key is 10 bytes, we do not have "perfect secrecy". Since the ciphertext (16 bytes) will be longer than the unicity distance, "ideal secrecy" is also not attained. We do not have any information theoretical security.

With Perpetual Equivocation. In addition to the elements of the example above, we will require the following:

(1) a random string R as long as the message, of 16 bytes.
(2) An additional encryption operation (transposition) after the main Vigenere.

We will first split the 10 byte key K into 3 keys, namely $K=\{K_1||K_2||K_3\}$, with K_1 having 2 bytes, and K_2 and K_3 having 4 bytes each.

A graphic depiction of perpetual on equivocation is shown below.

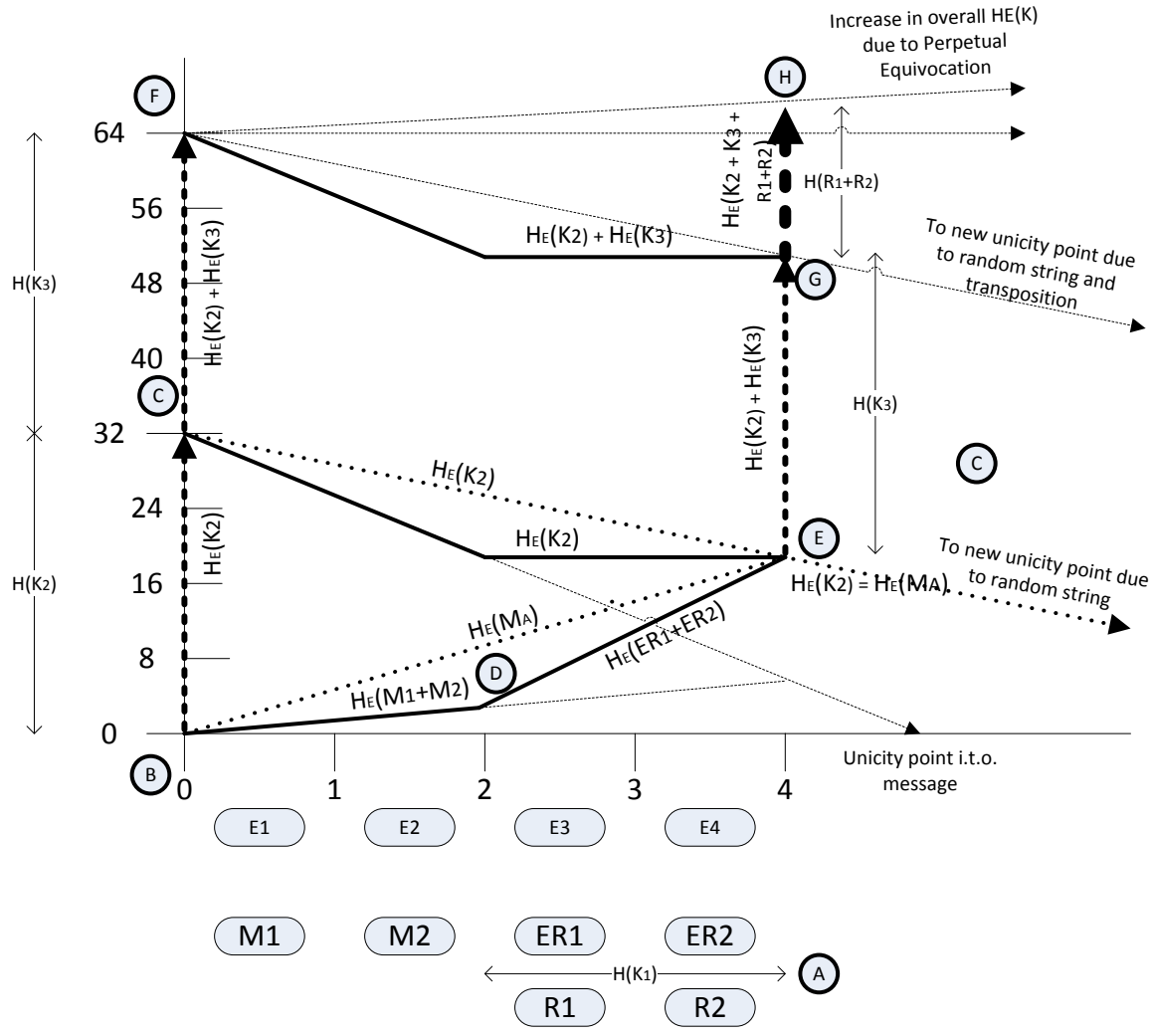

Figure 2. The Perpetual Equivocation graph

Using the graph above, the Perpetual Equivocation sequence is as follows:

1. At point A, we encrypt the first 2 random bytes R_1 and R_2 from the 16-byte random string R, using a Vigenere or XOR, with the K_1. This results in a "strongly ideal secrecy" encryption of R_1 and R_2 into ER_1 and ER_2, since they have no redundancy. We will then append ER_1 and ER_2 to the first 2 bytes of the message M_1 and M_2 such that the message segment M_A to be encrypted is $M_A = \{M_1||M_2||ER_1||ER_2\}$.
2. At point B, before encryption and before applying message and key K_2, $HE(K_2)$ and $H_E(M_A)$ are equal to zero.
3. At point C, applying K_2, increases $H_E(K_2)$ to 2^{32}. The message segment M_A is then firstly encrypted with K_2, resulting in the increase of the message equivocation following the slope $H_E(M_A)$, and the equivocation of key following the slope $H_E(K_2)$. $H_E(M_A)$ first follows the slope $H_E(M_1+M_2)$ for M_1 and M_2 , out to point D, then follows the slope $H_E(ER_1+ER_2)$since $ER_1$and ER_2 out to point E. At point E, $H_E(K_2) = H_E(M_A)$ and we have perfect secrecy following the first XOR encryption. Note that the amalgamation of $H_E(M_1+M_2)$ and $H_E(ER_1+ER_2)$ into $H_E(M_A)$, requires some mixing to occur over the entire M_A. This is the purpose of the transposition cipher which is used next.
4. Point F indicates the addition of K_3 for the transposition encryption over *period d*, d being equal to 4. Since the second encryption following an XOR has no information loss, the overall equivocation of key $HE(K_2)$ is increased by $H_E(K_3)$, raising the effective equivocation for the entire cipher to the value shown at point *G*.
5. Point *H* is where the "magic" happens. Since R_1 and R_2 have already suffered the indignity of an encryption prior to being added to M_A, their entropy can be added directly to the current key equivocation at G, namely $H_E(K_2) + H_E(K_3)$ can be augmented by $H(R_1+R_2)$. Entropy augmentation occurs with a mixing of the entropy, not a replacement. This may be done by encrypting the existing K_2 and K_3 with $R_1$and R_2.
6. Thus, we have the result, that the equivocation of K_2 and K_3 has been increased, replenishing their entropy to the state prior to the encryption operations, with entropy to spare.
7. In addition, the "perfectly secret" first encryption has the additional secrecy of a transposition, thus we have exceeded perfect secrecy.
8. The activity can be then conducted *ad nauseum*, thus the conclusion that "perfect secrecy" can be exceeded using a finite length key, irrespective of the length of the message. We also have the condition that "ideal secrecy" is guaranteed..

Further observations- the amount of entropy enhancement is increased with additional random string material, but the information theoretic secrecy attained above can be attained with at most 100 percent increase in message size. The benefit of the operation is increased with a decrease in message redundancy. Thus, better results can be obtained if the message is compressed prior to encryption.

It should be relatively obvious, that the use of static keys, whilst viable, does make it difficult with regards to the encryption of the existing keys with the new key entropy. In order to benefit from the additional entropy, a larger entropy pool is required, such as that used with a stateful PRNG. In such a case, the augmentation process merely requires the encryption of the current internal state of the PRNG with the new entropy.

3 The PE Cipher Concept

In this section, we discuss the PE Cipher from a conceptual perspective, in order to demonstrate that the Perpetual Equivocation principle is practically possible. The complete technical specification for the PE cipher will be covered in a subsequent paper.

The PE stream cipher is an extensible, fast, modular, software-based, dynamic super-stream cipher and has been purposefully designed with information-theoretic security considerations in mind. Whilst composed of simple cryptographic modules, the PE cipher is complex in its execution, effectively being dynamically polymorphic. By this we mean that every encryption operation is unique, since the state of the PE instance is randomly altered multiple times during each communication session. Uniquely, given the same static key *K* and message *M*, every encryption of that message will result in a unique and different ciphertext C.

The following is a basic conceptual diagram of the PE Cipher.

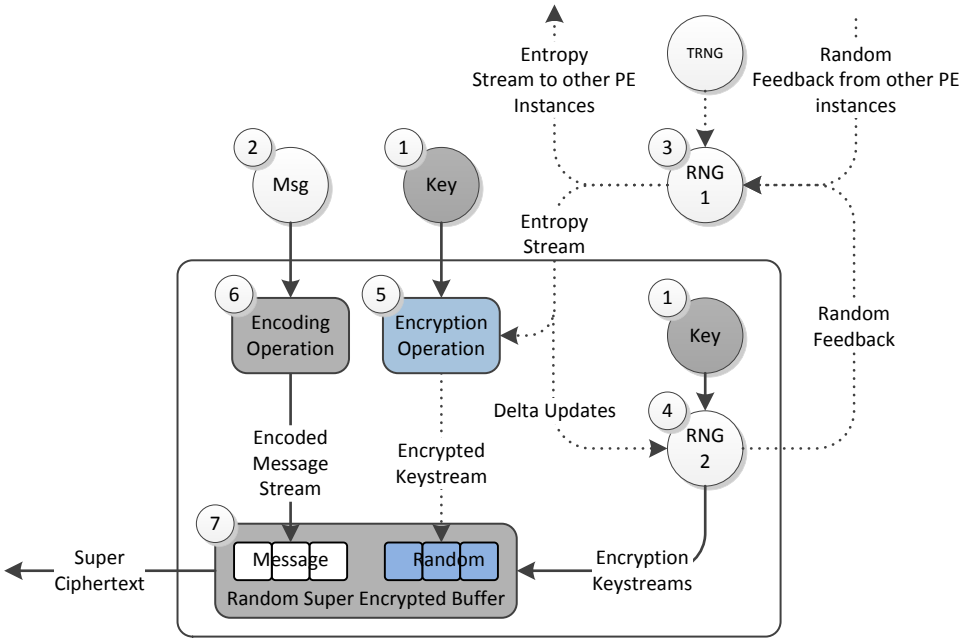

Figure 3. PE Cipher – Conceptual Design.

From the diagram above, we see that the PE cipher is composed of a number of simple components in a complex arrangement, namely:

- **A key K (1)** – used to initialise the state of the internal RNG2, and is also used to encrypt the entropy stream (the OTP pad) before transmission. Key can be of any size.
- **A message M (2)** – kept independent from the encrypted entropy keystream.
- **An unsynchronised external random number generator - RNG1 (3)** – (of specific design) a stateful random number generator serves as the source of the perpetual truly random entropy key stream (the OTP pad, and therefore the "actual" key to the system). The RNG is composed of an internal array of variable length (normally 256 bytes upwards) with random elements. Elements are usually 8-bit, but any bit-length is supported. It's future proof, and will support 128-bit elements and above when the technology becomes available. The RNG

is unique, in that its internal state and variable values can be dynamically and randomly altered between encryption operations. This allows for the random alteration of the deterministic number generation process – making true random number generation using a mathematical PRNG possible.

- **A synchronised PE RNG Instance - RNG2 (4)** – (of specific design) provides the truly random encryption keystreams for the encryption buffer. Of similar construction to RNG1. With RNG2, we allow for the production of multiple keystreams, for multiple encryption operations and to secure message authentication processes.
- **A minor Key Encryption Operation (5)** - the entropy stream is encrypted with the key K before transmission to the receiver, producing a brute-force resistant "ideal secrecy" encrypted entropy cipher-stream and a new K with every encryption. This operation may be further augmented with an initialisation vector, or an asymmetric authentication solution. In such a case the asymmetric encryption would operate in a "protected and secured" area.
- **A minor Message Encoding Operation (6)** – all messages are pre-processed before final encryption and transmission, allowing various cryptanalytic countermeasures to be deployed. May include message re-encoding, message reconstruction, redundancy alteration, and message randomisation procedures. The Encoding Process aims to increase the rate of "false positives" already provided by the main encryption process, in that every random decryption has an increased probability of producing a viable message.
- **A main Random Superencryption Process** (7) - where 3 separate and simple encryption operations are applied to an Encryption Buffer of random and variable composition (containing the Encoded Message Stream, and the Encrypted Entropy Stream). This prevents attacks against the keystreams and internal state of RNG2. It also ensures that there are no message/key/ciphertext pairs to speak of, providing message indistinguishability. The block size and composition of the encryption buffer is changed with every separate encryption using the random OTP entropy stream.
- **A Random Feedback Process** - To ensure that RNG1 produces a truly random keystream, a feedback operation is used. This ensures that RNG1 never encounters an entropy depletion problem.

Decryption entails using a remote synchronised RNG2, to remove the super-encryption process, revealing the Encoded Message Stream and Encrypted Keystream. Completion of the Decoding operation presents the message, on completion of the simple key decryption process RNG2 is updated in synchronicity for the next encryption operation.

The PE cipher was developed as a solution to the problems which prevented a one-time pad (OTP) from being practically possible. In essence, it allows for the "OTP pad" and the messages to be sent as a combined operation. Ordinarily, the OTP static key encryption mechanics are too restrictive to allow for a practical info-theoretic security solution. The use of an RNG allows for an interim dynamic "entropy" repository, making simultaneous pad/message delivery possible. The OTP pad is therefore used to alter the RNG output (the true one time pad). So "perfect secrecy" is attained indirectly. Indeed, controlling the amount of random entropy added to the message allows for the security of the system to be increased or decreased on demand.

4 Conclusion

In this paper, we demonstrated the Perpetual Encryption method as a means of overcoming a 70 year old cryptographic rule, that “perfect secrecy” cannot be attained with a finite length key. Our analysis indicates that it is not only possible to attain “perfect secrecy”, but to exceed it, provided we step out of the confines of static simple encryption systems with single keys, messages and operations, into the domain of dynamic complex encryption systems with multiple keys, messages and encryption operations. There is a world of cryptographic complexity to be explored.

5 References

[1] C. Shannon, “Communication Theory of secrecy systems.” Bell Systems Technical Journal, 28(4), 656-715 (1949).