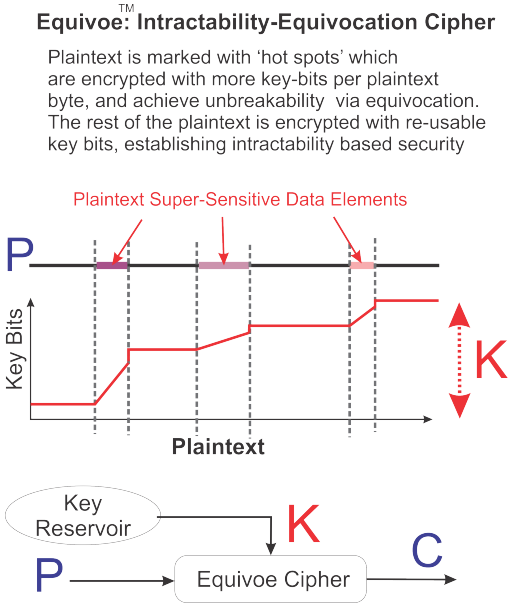
Equivoe™: A New Direction in Cryptography

The universal paradigm of today's ciphers is to create mathematical complexity via a good "mixing" of the plaintext and the key. This paradigm suffers from two important weaknesses: (i) mathematical complexity may yield to new mathematical insight that would melt it instantly; (ii) the price of the achieved complexity is a heavy computational burden, often to the power of two, three or higher relative to the size of the key. These two weaknesses render common cryptography into the "erosive intractability" category, and it bans it from situations where the prevailing computing power is insufficient for an effective exercise of these crypto algorithms.



Preceding this "erosive intractability" cryptography we find the famous "One Time Pad", or Vernam cipher, patented in 1917 by Gilbert S. Vernam, where the "mixing" of the plaintext with the key is utterly simple. Complexity is secured via the size of the key. Alas, this issue of key size is also the reason why the Vernam crypto philosophy has been abandoned.

AGS Encryptions Ltd. decided to revisit old Vernam, and extract from his philosophy a new kind of crypto security. We noticed that Vernam encryption effort is proportional to the size of the plaintext, (which happens to be also the size of the key). It is not quadratic or cubic relationship! We also noticed that Vernam's unassailable mathematical security is based on equivocation, *not on intractability*. The Vernam ciphertext can be matched to any plaintext of same length. The subtle point here is that Vernam offers *an equivocation overkill*. To frustrate a cryptanalyst it is sufficient to have even a few mutually contradictory plausible plaintexts. We also noticed that Vernam rigidity on key size is a serious burden on its user. Taking all these observations into account we have come up with a very simple plaintext-key interaction where processing effort is not a function of key size (only a function of the size of plaintext, but that cannot be helped), and we make that size part of the secrecy of the key. In this new crypto approach the fixed key is replaced with a *key reservoir*, which can be drained sparingly, and project the common "erosive intractability," or it can be "eaten up" fast, and provide mathematical security. A common plaintext can be marked as to "hot spots" that will be encrypted using a lot of key material, but attain guaranteed mathematical security, and then mark "medium hot spots" that would be encrypted with less key bits, (a mild measure of re-use), while the rest will be encrypted with reusable keys. The cryptanalyst will have no indication as to how much key material was used. A particular ciphertext at hand might have been encrypted using the full Vernam equivocation measure, and it would be a waste of time to try to crack it.

The ultra processing speed of both the encryption and the decryption positions these class of ciphers as a perfect candidate for the Internet of Things, and the vast array of sensors and monitors that broadcast information which cannot be encrypted with the computational hog ciphers of today.

Gideon Samid, Chief Technology Officer AGS Encryptions Ltd. Gideon@AGSgo.com