Quantum & AI Security using One-Time Pads and Entropy Distribution

Incrypteon is pleased to announce Archaios, the world's most advanced and secure digital security system. It is a 3rd Generation military-grade security system – polymorphic, probabilistic, and active - that is information-theoretically secure against Quantum + AI threats using multiple One-Time Pads (proven to be secure) & Entropy Distribution (Key transmission).

SUMMARY

The Archaios security system was designed to comply with Claude Shannon's cryptographic requirements. None of today's commercially available security solutions comply with his requirements.

Shannon also proved mathematically, by applying Bayes Theorem to Entropy, that One-Time Pads were "perfectly secure". Unfortunately, the requirements for One-Time Pads are impossible to apply in a digital context. Keys must be as long as the message, keys must be perfectly random, and keys must be transmitted and stored securely.

Current security solutions also suffer from the Conditional Entropy Depletion Problem. To use a real-world analogy, all current encryption systems where key entropy is less than message entropy, can only protect a certain amount of message characters. Like a car with a sealed fuel tank, they eventually run out of fuel – Conditional Entropy is the fuel that remains, Equivocation is the range of the vehicle. For example, assuming no hidden defects in the cipher, AES-256 can only mathematically secure messages shorter than 40 characters (its range). Longer messages are guaranteed to be broken.

Archaios is the solution to the One-Time Pad Digital Problem, and the Conditional Entropy Depletion Problem, in that it uses multiple One Time Pad encryptions embedded inside an outer One-Time Pad encryption. Keys are not transmitted, but instead, starting with a fixed length key, entropy (random numbers) is transmitted with every encryption step. OTP-encrypted entropy portions are shuffled with OTP-encrypted message portions and encrypted with the outer OTP encryption. After each encryption step, the entropy is used to alter the values in a secret set of values (an entropy pool) which is used to create the keys for the next encryption step, until the message is completely sent. A key "refuelling" process if you like.

The core underlying principle is whether it is possible to infinitely "refuel" any encryption system using the Entropy Transmission solution. Mathematically and scientifically, this has been verified and can be demonstrated through experiments.

With unlimited entropy on tap, Archaios then uses the values in the entropy pool to behave completely chaotically – every encryption starting with the same key, has a completely different ciphertext. Since we never use more than half the values in the entropy pool, only half the keys can ever be brute-forced at any point in the encipherment. We consider this characteristic to still be unacceptable and have developed a technique which blocks any attempts at reconstructing the entropy pool.

Due to its simplicity, Archaios can be used to solve several complicated cryptographic problems such as (a) Encryption Quality of Service (a short urgent message does not have to wait for a long message encryption to complete, (b) Multiple cryptographic operations can be performed in parallel, at the same time – multiple messages, multiple authentications, multiple VPNs.

No existing cryptanalytic attack on the ciphertext is possible, it cannot be replayed, interfered with (it resets itself), or spoofed and supports integrated authentication. Any encryption algorithm can be used, but the external encryption must be a One-Time Pad.

INTRODUCTION

The Archaios security system was born when a former military cryptanalyst set out to accomplish two simple objectives – to (a) create a simple security system which complied with Claude Shannon's mathematical cryptographic requirements for "perfect secrecy" systems, and (b) which would make a cryptanalyst's job impossible to perform.

Claude Shannon (considered to be the father of the information age and modern cryptography) published 2 cryptographic papers after World War 2. In 1945 he published "A Mathematical Theory of Cryptography" and in 1949, a similar paper called "Communication Theory of Secrecy Systems". These 2 papers laid the foundations for a mathematical understanding of modern cryptography – they defined what it means to be "secure". They contained a description of the very techniques that were used to break the German Enigma Code during World War 2, and laid out basic cryptographic directives, and explained the concepts of "Conditional Entropy" and its application in a security index called "Equivocation".

Shannon's basic cryptographic requirements or directives include:

- Assume that the assailant has infinite computing and time resources.
- Measure the security of a system using conditional entropy (the set of results which remain after a comprehensive search) and use conditional entropy to determine the "Equivocation" of an encipherment (encipherments beyond a certain length are insecure).
- For practical systems (insecure systems that depend on mathematical problems and workload for their security) he specifically stated that it is not enough to not know of a fast solution to the mathematical problems – one must be sure that no fast solution exists.

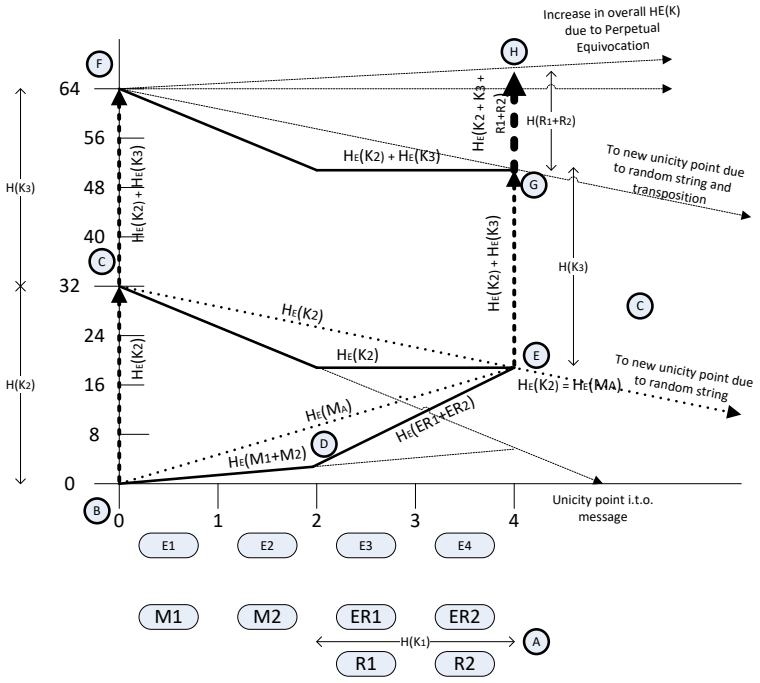
As mentioned in the Summary, only the One-Time Pad and Archaios can pass Shannon's strict cryptographic requirements. Unfortunately, none of the "NIST approved" security standards comply with Shannon's cryptographic

directives. They do not use an objective means of measuring security, and completely ignore Shannon's warning with regard to Practical Systems.

Since 1949 we have known that (a) the secrecy (or security) of any security system is measured using an objective quantity called "conditional entropy" (the logarithm of the number of valid decipherments of a given ciphertext after a brute-force attack), and (b) that One-Time Pad encipherments are mathematically proven to be "perfectly secret" in that their conditional entropy can never be reduced to less than the logarithm of all possible messages – even if subjected to a brute-force attack by an assailant with infinite computing and time resources. Technically, he stated that it was the additional valid decipherments (conditional entropy) which gave a secrecy system any secrecy, and that any secrecy system will be secure if its conditional entropy can never be reduced to zero (reduce to a single unique valid decryption).

Importantly, Shannon stated that any secrecy system capable of adding entropy to its encryption operations faster than can be removed by an attacker, will have the same security characteristics as an OTP and will also be secure.

In the same manner, any digital security system which aims to be secure against Quantum + AI assailants, must have the same secrecy characteristics as a OTP. Whilst an OTP cannot be used digitally due to practical implementation issues, Archaios has no such problem. The Archaios security system overcomes the OTP practical implementation issues by using multiple One-Time Pads (OTPs running inside OTPs) and a set of random values (an entropy pool) used to generate OTP keys. In an encryption step, OTP-encrypted message streams are combined and mixed with OTP-encrypted entropy update messages, inside a OTP-encrypted wrapper. The entropy updates are used after each encryption step to change the entropy pool values and generate new OTP keys for the next encryption step (much like a block-chain).



Above, is a conditional entropy graph demonstrating how conditional entropy can be calculated, visualized and managed, for a system using 2x 32-bit keys encrypting a 2-character message and 2-character random string. The increase in key entropy is evident from the Bold arrow. The point where the dotted lines cross the bottom axis is the

"unicity point" for that respective mix of cryptographic operations. Any encryption system security proof which does not contain a conditional entropy graph such as above, should never be trusted.

Incrypteon provides a solution, in that any cryptographic systems or ciphers, no matter their conditional entropy cryptographic strength, can be made "Shannon-Secure" (unbreakable) by simply running them inside Archaios – Using Archaios as a security wrapper.

THE CRYPTOGRAPHIC PROBLEMS

There are a few critical problems in the field of cryptography that we have addressed with Archaios:

- **The AI-Threat Problem –** The use of AI attack systems in cryptography is not new, it has been used in military cryptanalysis for over 35 years now. It is therefore a very real current threat ignored by the cryptographic community which is stuck using archaic pre-WWII security principles. Note that the One-Time Pad is "AI-Secure", since it is secure against an assailant with infinite computing resources. However, AI systems are superior to humans in cryptanalysis and pattern recognition and provide an additional high impact analytical threat, in that they can further decrease the number of valid decipherments after a brute-force attack based on probability of likelihood. Systems built on non-scientific cryptographic principles such as "Semantic Security" can never be AI-Secure since they are too predictable - (a) fixed operations, (b) fixed length keys, (c) fixed block sizes, (d) visible ciphertext, etc. One can even say that "Semantic Security" standards inadvertently guarantee insecurity due to their predictability, and subjective basis of determining the security of a system. Such systems are deemed secure merely because someone said so.
    - Incrypteon is AI-Secure in that it has OTP characteristics and has been specifically designed with AI threats in mind. Besides using scientific based security principles, it goes against the current standard model for encryption system design, in that it has been designed to be as chaotic and unpredictable as possible:
        - Encryption operations are not fixed, but random and are hidden.
        - Key lengths are not fixed but randomly determined, and keys are hidden
        - Base Ciphertext, Messages and Entropy are hidden by mixing them behind an encryption layer. Operations inside the Incrypteon system are secret.
        - Every encryption operation is unique, even if one uses the same message and starting key.

- The **Quantum + AI Threat Problem** – Before the Quantum Computing threat, cryptographic systems that were based on "Semantic Security" design principles, whilst being unscientific, were assumed to be good enough for commercial use. The advent of Quantum Computing now clearly highlights that "Semantic Security" systems are too weak against a Quantum Computing assailant. The advent of AI systems now increases the risk exponentially in using a non-scientific security standard such as "Semantic Security". We are now at the point where "Quantum + AI" attacks are a very real risk – we therefore have a compelling case for Shannon's assumption – that the assailant has infinite computing and time resources. Artificial Intelligence has been used in military cryptography for over 35 years, so A.I. attacks are now very certain to occur. There are currently no known solutions in the cryptographic community to the "Quantum + AI" Attack problem.
    - Archaios is the world's second "Quantum + AI secure" security system after the One-Time Pad. OTPs are "Quantum + AI secure" but cannot be used in digital communications.
    - Archaios is therefore the world's first digital "Quantum + AI secure" security system and exceeds the OTPs security characteristics.

- **Lack of Science-Based Cryptographic Standards** - NIST has just announced 4 new Quantum-resistant protocols. They are quantum-resistant and not quantum-secure because they rely on the assumption that a quantum algorithm for solving the specific mathematics problems used, is not known. It should be alarming that NIST (a scientific institute) is not selecting cryptographic systems on the basis of scientific criteria, but on an archaic "pre-World War 2" security standard that has no scientific basis – namely "Semantic Security" (or more accurately "Pseudo-Security"), with its unsubstantiated assumptions of complexity that Shannon warned against. Breaking the Enigma Machine Code proved that Semantic Security was a flawed security standard. Why NIST chose to ignore the cryptographic principles in Shannon's foundation paper (the most referenced paper in cryptography – over 250,000 references) and adopt a proven failed standard is an enigma. Conditional Entropy is the logarithm of the number of valid decipherments which remain after a comprehensive attack of all keys. If Entropy is the "fuel" of encryption, and the message is the distance to be covered, then Conditional Entropy is the fuel remaining in the tank at any point in the trip. Like a car, encryption systems can go on forever if their entropy is continually refueled.
    - Archaios solves this problem by demonstrating that science-based cryptographic design principles lead to better security systems, without resorting to invalid assumptions. Admittedly assumptions are allowed, but only if they favour the attacker – hence the assumption of insecurity (or Zero Trust) – that the assailant has infinite computing and time resources.
    - NIST should never be promoting non-science-based security products, it should be specifying the scientific standards which need to be complied with – such as "Upon a brute-force attack, it must not be possible to reduce the conditional entropy to zero for the duration of the message". Military cryptanalysts never trust "approved" algorithms, especially if the government approving them prohibits their use for securing classified documents.

- **The Conditional Entropy Cryptographic Barrier** – Shannon determined that a certain amount of key entropy can only secure an equal amount of message entropy. If the key is repeated in any form, the Conditional Entropy of any encipherment using any secrecy system will be reduced to zero under an attack on the keys or message, to the point where only one valid message will remain, and the encipherment is insecure. The point in the encipherment when this occurs depends on the size of the key and the redundancy in the language of the message only – not on the complexity of the encryption system, nor the opinions of academia. Mathematically, AES-256 cannot mathematically secure any message longer than 40 characters. Like a car that runs out of fuel if the trip is too long – the solution to securing the trip, is to refuel the car before you run out of fuel.
    - Archaios is the first and only security system that has broken the Conditional Entropy Depletion Barrier. This is possible because Archaios can continually add key entropy.

- The **One-Time Pad Digital Problem** – Whilst the One-Time Pad has been used for over a century, it cannot be properly deployed in a digital communication system. To be secure an OTP must, (a) have a truly random key which is as long as the message, and (b) the key must be securely transmitted, stored, and destroyed – requiring another one-time pad to do so. Any security system with the conditional entropy characteristics of the OTP will also be secure.
    - Archaios is the solution to the OTP Digital problem, in that it is based on using multiple OTPs inside multiple OTPs in a digital framework. The keys are not transmitted or stored but generated at the point of use. Additional entropy is transmitted and is used to increase the entropy in the entropy pools used to generate OTP keys which are unpredictable before the point of use.
    - Archaios can exceed the security characteristics of an OTP.

- **The Brute-Force Attack Problem** – Current systems are flawed cryptographically since they have no means of protecting themselves from brute-force attacks. They further make no attempt to protect themselves but rely on unscientific assumptions that it will take "millions of years" to break. This is an unsubstantiated assumption with no scientific basis, since the scientific viewpoint is that one must assume an assailant with infinite computing and time resources.
    - Archaios at least 4 techniques to prevent brute-force attacks.
        - Messages are hidden behind three layers of encryption
        - Messages are mixed with random strings
        - Encryption mechanics are hidden
        - An advanced technique (patent pending) is used to lock encryptions from the inside.

THE SOLUTION

The Archaios system is the world's most advanced science-based "Quantum + AI"-secure encryption system, capable of being secure against Quantum + AI assailants, and is built using Shannon's basic cryptographic principles:

- Assume that the assailant has infinite computing and time resources (as is the case with a Quantum/AI assailant.
- Use "conditional entropy" (an objective measurement) to determine the security of the system. Conditional entropy is the logarithm of the residual number of valid decipherments – must be greater than 2.
- Encipherments are insecure if the message is longer than the "unicity" point (the point where an attacker reduces conditional entropy to zero)
    - One-Time-Pad (OTP) is secure and "unbreakable" because its "unicity" point is always longer than the message.
- Systems such as all current digital asymmetric cryptographic systems today, which rely on the difficulty of mathematical problems – cannot be considered secure unless it can be proven that a fast solution does not exist. Shannon specifically stated that it is not enough to not know of any fast solution, it must be known that a fast solution does not exist. One must assume that the attacker is aware of a fast solution if one exists.

OTPs are used as the base foundation for Archaios because they are mathematically secure i.t.o. "conditional entropy" provided (a) the key is as long as the message, (b) the key is perfectly random and (c) the key has been shared and stored securely.

The Archaios system is a 3rd generation encryption system with the following design characteristics:

- It is a **Stream Cipher** - composed of an arrangement of multiple OTP encryptions using multiple OTP keys generated from a central entropy pool that is initialised with a shared key. OTPs are used for speed and simplicity.
- It is **Polymorphic** and **Probabilistic** – encryption operations are randomly determined - they differ randomly with each encryption.
- It is **Dynamic** and **Entropy Augmented** – A patented technique is used to continually refuel the entropy pools with new entropy, faster than can be reduced by a Quantum/AI attacker using brute force. The entropy augmentations are used to increase the key and dynamically alter the system with every minor encryption step.

- It is a **Multi-Tiered Multi-plexed Black Box** system – at least 3 degrees of independent encryption separate messages from visible ciphertext. Plaintext messages are mixed with random entropy, shuffled and encrypted.
- It is **Brute-Force Resistant** – A patent pending technique is used that prevents an attack where the attacker tries every possible key, or message.

Archaios is superior to the OTP in that it can increase its security merely by increasing the rate of entropy delivery. In addition, it has the same characteristics as a One Time Pad - (a) keys as long or longer than the message, (b) pure random OTP keys are provided using the entropy pool, and (c) keys are created and destroyed at the point of use, so no need for secure transmission or storage.

Below is a simple diagram of the Archaios Security System.

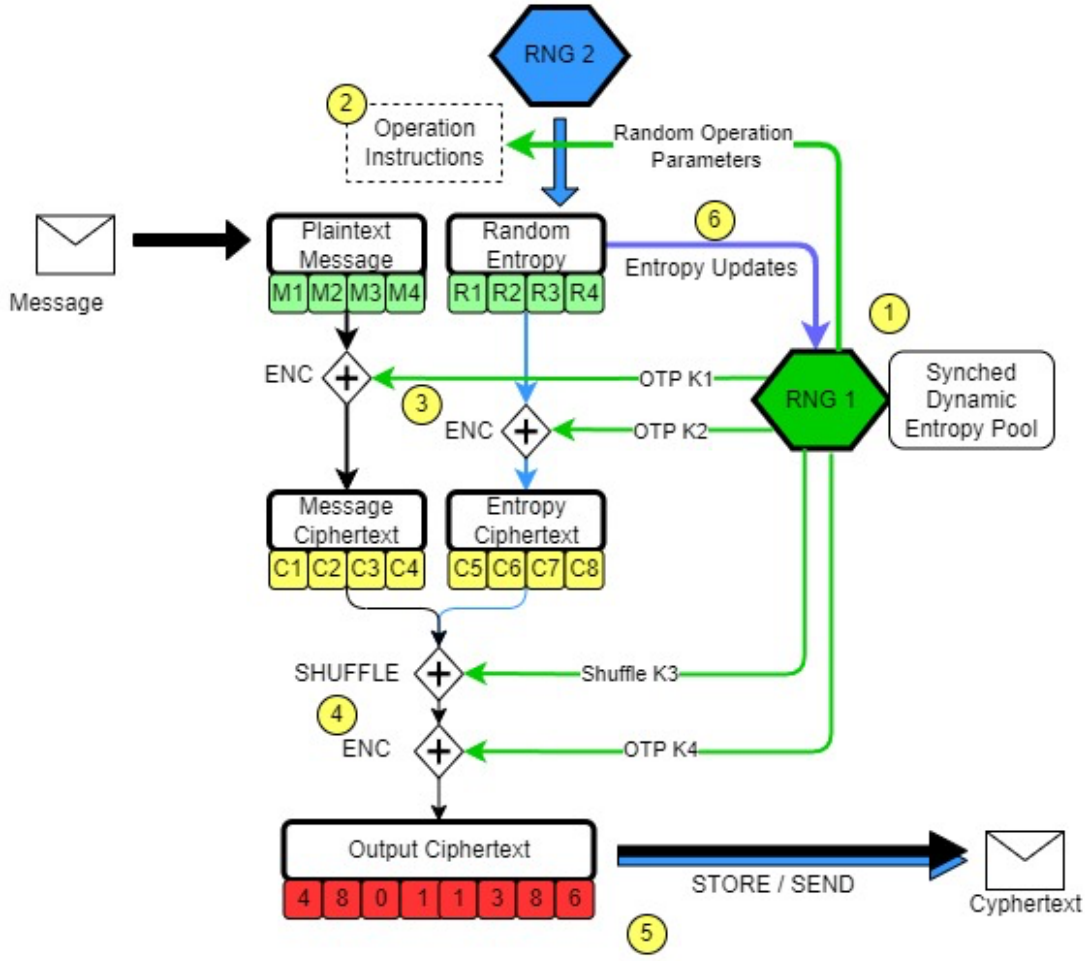


Figure 1. Archaios Security System – Basic Conceptual Design.

The Archaios Security System has been designed with “Conditional Entropy” security update characteristics in mind. The simple composition shown above for a single block encryption operation ensures that “Conditional Entropy” can never be reduced to zero (The fundamental problem with all encryption algorithms), because entropy is added to the message stream in point 3 above and point 6 details how it is applied to the entropy pool for the next encryption operation.

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

- (1) A dynamic entropy pool RNG1 is initialized with an Initial Shared Key by the Sender and Receiver.
- (2) Values in RNG2 determine the operations and order used for the next encryption operation. Each encryption step is randomly determined
- (3) A length of message M and a length of entropy R (provided by an external RNG2) are separately encrypted using any encryption algorithm, using the Keys K1 and K2 provided by RNG1. OTPs are preferred as they are the fastest. Any encryption algorithm is an OTP if the key is as long as the message segment.
- (4) The encrypted plaintext (C1-C4) and entropy (C5-C8) are then joined, shuffled and encrypted using keys K3 and K4. They are wrapped in an OTP container.
- (5) Output Ciphertexts are then either stored as a chain of ciphertexts or transmitted as a chain of ciphertexts. To decrypt, the receiver (if transmitted) or the sender (if stored) performs the same operations, but in reverse.
- (6) After every minor encryption operation, the random entropy is added to the residual conditional entropy in RNG1.

The example shown is the simplest possible composition. It can be extended to support multiple message streams, using multiple encryption variations and encryption protocols.

CRYPTOGRAPHIC CHARACTERISTICS

The Archaios system has the following important characteristics:

- It is the most secure encryption system ever invented.
- It is “Quantum + AI” Secure - secure against quantum machines and AI assailants.
- It is simple, small and fast, and its security is not derived from key size alone.
- Its security is based on science-based cryptographic principles specified by Shannon.
    - The secrecy (security) of Archaios is determined using “conditional entropy” and “equivocation”. “Conditional entropy” can be visualized and graphs of Archaios are available which visually depict the security of the system.
- Multiple OTPs are used, since Shannon proved OTPs to be mathematically secure against assailants with unlimited processing and time resources.
    - Any encryption algorithm that uses a key as long as the message is an OTP.
- Archaios does not rely on any assumptions of security, for its security
- It is the solution to the 50-Year One-Time Pad Digital Deployment problem.
    - Keys as long as message – infinite length random keys can be generated at very fast rates, with no entropy depletion.
    - Truly random keys – With every encryption step, entropy transfers are used to change synchronised entropy pools which are used to generate keys. Key generation has no bias, and OTP superencryption reduces the “truly random” requirement.
    - Keys are generated, transmitted and destroyed – variable length Keys are generated, used and destroyed with every encryption step. They are never stored.
- It cannot be broken using brute-force attacks. By “broken”, we mean that its conditional entropy of message or key cannot be reduced to zero by an assailant with infinite time and computing resources. It cannot be replayed or interfered with. Knowledge of messages does not compromise the keys used.

- It exceeds the capabilities of Semantic Security systems (a pre-WWII standard) – which cannot meet the requirements for “Quantum secure,” “AI secure” nor “Quantum + AI secure".
- It is truly crypto agile in that (a) it can support any combination of symmetrical encryption algorithms, (b) can be used to securely transmit any asymmetric keys, and (c) has asymmetric key integration.
- Archaios has built in redundancies – It can recover from multiple cryptographic failures. It can detect intrusion and has integrated authentication and key distribution.
- It has been designed to allow the attacker only the absolute minimum amount of information possible about the system. The attacker may know of all the different operation methods which can be used at a point in time but cannot identify exactly which one was used.

Lastly, and most importantly from a practical perspective - Archaios is superior but should not be perceived as a threat to existing FIPS-140 certified solutions which are required for compliance purposes. However, these FIPS-140 certified solutions can be made information-theoretically secure, just by wrapping them inside an Archaios wrapper, whose configuration is only known to the user. In this way users can benefit from the superior “Quantum + AI secure” security characteristics of Archaios and be FIPS-140 compliant.

Conclusion

The Archaios system has been publicly known for over 8 years now, with cryptographic community and the authorities have had over 5 years to discuss the analysis, deployment, and proliferation of Archaios to the public. Archaios will change the way that we design cryptographic systems forever. Archaios was designed to protect humanity from Artificial Intelligence or from those who wish to use Artificial Intelligence as a weapon against humanity. We are looking for support and to create relationships with government, military, commercial, academic, or private entities with an interest in advanced cryptography.

We respectfully ask that you please help us to protect you, and the rest of humanity. Further, the use of Archaios in any form which injures or deprives a human being of their liberty, or their human rights, is prohibited in the strongest terms, including military use.

References

- Shannon, C. E. (1948). "A mathematical theory of communication". *Bell System Technical Journal*. **27** (3): 379–423, 623–656 (drafted in 1945)
- Shannon, C. E. (1949). "Communication Theory of Secrecy Systems". *Bell System Technical Journal*. **28** (4): 656–715.