TECHNOLOGICAL BACKGROUND

FRAGMENTATION → DECIMAL & BINARY PROJECTIONS

Historically, **Ex0-SyS** has designed several digital data fragmentation technologies based on principles of description of the input binary data and not on transformative principles. The idea of this type of approach is to be able to secure digital data by describing its binary content and storing the description information in several separate output files. Thus, until all the fragmented data is brought together, it is impossible to reconstruct the original data, nor to obtain any coherent information from it. It's all or nothing!

Originally, we invented a principle of fragmentation by description and created **Alph@TaV Zéro**, an algorithm from which we produced and published the digital safe software **Alph@TaV Vault** (see dedicated website: www.alpha-tav-vault.com). In order to test this technology, we published an online competition aimed at hackers, crediting with ₿ 1.– (one bitcoin) anyone who succeeds in decoding a message and a secret e-mail address contained in a video fragmented by **Alph@TaV Vault**. The principle of the competition involved the weekly publication of four fragmented files, thus giving attackers more and more information to carry out their attacks (see dedicated website: www.decryption.ch). We resisted 1'757 independent and government attacks for almost a month, sometimes with massive computer performance available. It wasn't until the release of the last fragmented file that we were lucky enough to have a winner. The latter succeeded in a master stroke by exploiting an implementation flaw in the **Alph@TaV Vault** software, bypassing a lock, and thus partially reconstructing the video containing the secret information. On the other hand, the principle of security by fragmentation **Alph@TaV Zéro** could not be defeated during this test, because it is only with all the fragmented files in its possession that the winner, according to his own words, was able to exploit the software flaw linked to a lock, and not a technological flaw linked to the principle of fragmentation itself.

This fragmentation technology has also aroused the interest of various cybersecurity players, effectively introducing us into this very closed and sophisticated environment. Spotted by EPFL (Ecole Polytechnique Fédérale de Lausanne [Swiss Federal Institute of Technology in Lausanne]), **Ex0-SyS** participated in the 2019 Tech4Trust start-ups acceleration program set up by EPFL Innovation Park. During this course, we were able to refine our development strategy thanks to the recommendations of qualified experts, and to realise the untapped niche to date represented by technologies for securing digital data by fragmentation. We have also established solid relationships with the technological research hub of the French universities, Telecom ParisTech, of which a complete department is dedicated to research on data fragmentation security.

In parallel, we have imagined a new method of fragmentation by description, materialised by the **Alph@TaV Berechit** algorithm. The latter has the advantage of being available in two approaches, each with their advantage in terms of speed of execution or level of cryptographic resistance.

- The first approach, **Alph@TaV Berechit Standard**, achieves unparalleled cryptographic resistance scores to date for brute-force attacks on a group of output files (design of mathematical tools, modelling and results by an expert with two doctorates [PhD] in mathematics). Indeed, the smallest resistance index obtained being 98^n, where n represents the length of the binary chain to be analysed, this score far exceeds all known scenarios of resistance to brute force on a binary chain of the same length, the maximum limit being conventionally and logically set at 2^n for analysis on a binary system.

- The second approach, **Alph@TaV Berechit Evolved**, allows for greater speed of execution. It is an optimisation of the classic approach that offers only two fragmented files in output instead of three (see **Alph@TaV Berechit Standard** above), hence an increased speed.

In these two different technology implementation scenarios, the number of output files and their size play a role. This is because some of the output files have a high and predictable size reduction factor for the input data. Thanks to this particularity, we have, among other things, designed more advanced security systems, available in three technological products:

1. **Stellar Storage**: a secure, fragmented *cloud*-based data storage system.
2. **Crypto Access**: secure access authentication control whose True-random key is renewed with each use (possible fragmentation of keys for independent or simultaneous unlocking).
3. **NASOT**: secure data transmission system using the principles of fragmentation for an easy implementation of the conventional cryptographic system One-time pad on one of the keys obtained by fragmentation. It incorporates an advanced binary permutation system using a True-Random key to define the order of the permutations.

Technology product brochures are available in PDF format.

It is the **NASOT** secure data transmission system that has generated the greatest interest, especially from government agencies. By coupling our fragmentation technologies to the conventional cryptographic system of the One-time pad to facilitate its use, we have seen the reaction of more than one entity aware of the challenges of using this cryptography, historically known by mathematical demonstration to be the only truly unbreakable system (perfect secrecy), including facing current and post-post-quantum computing superpowers.

Quite naturally, our efforts focused on the **NASOT** system, which, in addition to data fragmentation and One-time pad cryptography, was made up of an advanced binary permutation system operated on one of three fragmented output files. These permutations use the True-Random encryption key required by the One-time pad to create a completely random permutation scheduling table and thus encode the data concerned. This then becomes absolutely indecipherable without the original decoding key. One of the initial difficulties was to obtain a True-Random binary data of sufficient size to perform all the possible permutations on the concerned binary chain. In response, we have designed a mathematical tool which creates, from the True-Random encryption key required for the One-time pad, a much longer binary data item with a sufficient number of bits. The stake (the absolute non-predictability of the result obtained without having the initial key) forced us to ensure the preservation of the True-Random character from an initial chain resulting from a material QRNG unit (Quantum Random Number Generation) until the result of the binary chain amplified by this tool. It is the same mathematician, doubly PhD graduate, who designed the tools, the models and obtained the results having demonstrated that the amplified binary chain was absolutely keeping the True-Random character of the starting binary chain, itself naturally True-Random thanks to a physical device of quantum generation.

From fragmentation to projections

During the search for the preservation of the True-Random character by the input binary chain amplification tool, we discovered, during the modelling of the mathematical environment and the design of the tools necessary to analyse and obtain the results, that we were dealing not only with an instrument, but also with a mathematical function in its own right, unknown until now. It has many mathematical properties, besides the preservation of the True-Random character, and among other things the peculiarity of being compatible, without error, with all the other mathematical functions it has been confronted with, including, remarkable fact, simple mathematical operators (+, –, x, ÷). Indeed, if it is relatively easy to create a mathematical function to solve a well-defined problem, it is on the other hand extremely rare and surprising, by the very strict definition of the context in which it must operate, that it turns out to be compatible with all the other functions and conventional operators. This nature makes it a fundamental mathematical discovery whose scientific and industrial opportunities are barely measurable. The analysis of this function has essentially focused on preserving the maximum entropy of an input binary chain, and its full effectiveness in this regard is demonstrated. In addition, during an out-of-context analysis, we were able to see that it could instantly optimise the size of a data by a factor 4 by using the tools dedicated to the analysis of data signals. This is unusual for a tool capable of maximum preservation of the quantum entropy of an initial QRNG chain, optimisation being the inverse of entropy.

As a result of this discovery, our efforts were once again reoriented towards possible interests and opportunities. Among the scientific and industrial openings linked to this function, one emerges, because it solves a historical problem. Indeed, if we know how to solve the problem of the amplification of the size of a True-Random input binary chain (with a calculable amplification factor and the guarantee of the preservation of the True-Random character of the amplified chain), then we have responded to the most restrictive problem of the One-time pad for strict compliance with its implementation, namely the mandatory and permanent physical exchange of True-Random keys. Our technology thus provides the long-awaited answer: from now on, no more than a single physical exchange of a small random key is necessary; all future keys will be exchanged through the network in an unconditionally secure manner.

We have thus chosen to focus on the entropy conservation property of this function. Due to its ease of use, our technology offers to implement the One-time pad in various categories of software and hardware infrastructure, which has been extremely uncomfortable until now.
There are two aspects to the technology of amplifying a starting binary chain. On one hand, a process performing decimal processing on an initial chain, which we call "decimal projection", represented by the name $\mathbf{\Pi_d}$; and on the other hand, a binary treatment on the resulting chain, represented by the name $\mathbf{\Pi_b}$. The interaction of these two operations amplifies the size of the starting True-Random chain and ensures the preservation of the True-Random character transmitted to the final binary chain.

What does the ease of use of the One-time pad imply?

Modern communications security cryptography is divided into two distinct categories:

1. The so-called asymmetric cryptography, which allows an exchange of information without having previously exchanged private decoding information with its interlocutor. This is extremely convenient, but security is totally dependent on the public encryption key known to all, as well as on the current or future opposing computer performance dedicated to an attack.
2. So-called symmetrical cryptography, which is not based on an encoding using a public key and allows an exchange of information only by having previously exchanged a private decoding information with its interlocutor. It greatly increases levels of cryptographic resistance but is much more restrictive to use and nevertheless remains sensitive to opposing power.

The One-time pad is clearly a symmetric cryptographic system. Moreover, it is the best of all cryptographic systems in its class, but on the other hand it is the least practical system to use in real conditions. Its constraints are the basis of the design of all modern symmetric cryptography algorithms, definitively ruling out the One-time pad from the competition for large-scale distribution. This ambivalence between the best symmetrical cryptography, the only mathematically definitively unbreakable system, and the impossibility of its use on a large scale, makes the One-time pad totally elitist and exclusively reserved for cryptographic exchanges of the highest importance, such as the world-famous Moscow-Washington hotline dedicated to secure government exchanges between the White House and the Kremlin.

In conclusion, our decimal and binary projection technology provides the answer to the historical problem of the One-time pad, allowing its practical use on a large scale, which can be addressed to all fields of applications currently using symmetric systems. The question then arises whether our technology is, in part, the death knell of all modern symmetrical cryptographs, as they were created by highly qualified mathematicians who had worked because of the practical impossibility of using the One-time pad, yet proven to be unconditionally safe for over a hundred years.
The technology of decimal and binary projections is not only a revolution in the field of data security, but also a fundamental scientific revolution.

FRAGMENTATION **VS** PROJECTIONS: **INACCURATE**!

FRAGMENTATION → PROJECTIONS: **FUTURE**!

Ex0-SyS

Swiss Tech Innovation

Ex0-SyS Sàrl
CP 99
CH-1296 Coppet
Vaud
Switzerland

IDE : CHE-446.943.138
DUNS : 480392700
Phone : +41 79 334 30 62
Fax : +41 22 960 53 44
Email : more@ex0-sys.com