# Alph@TaV(™) Vault® TECHNICALS

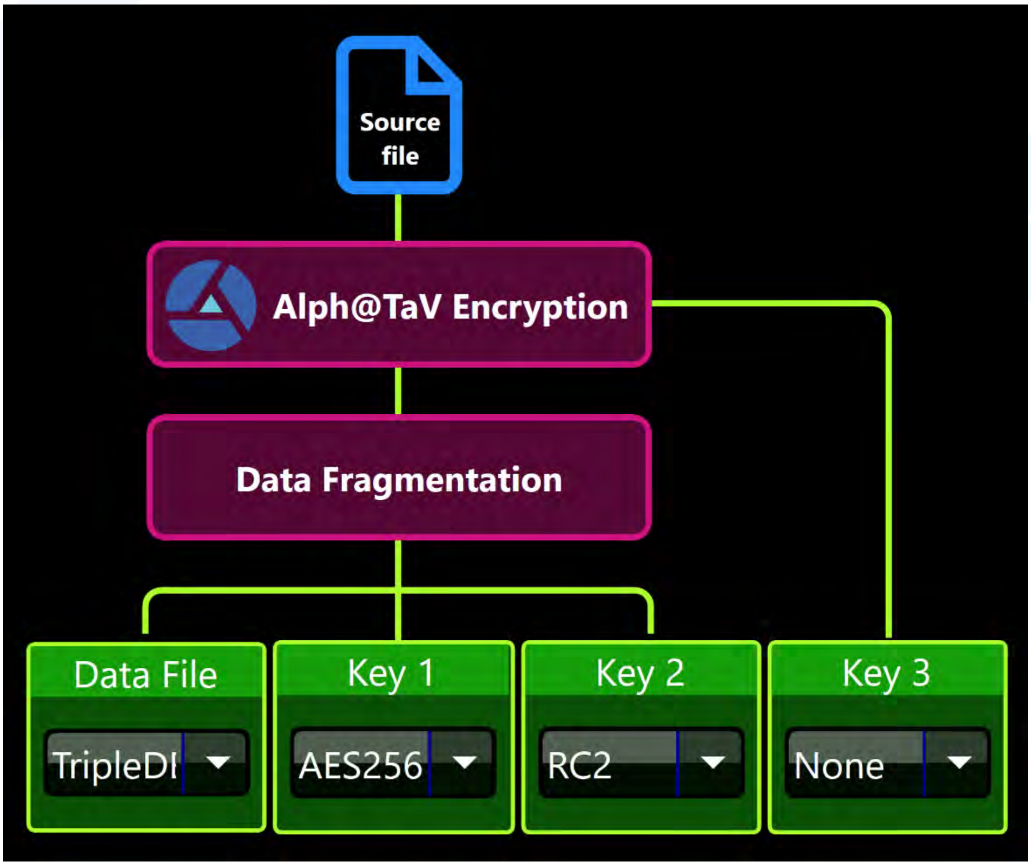
The **Alph@TaV(™)** solution acquires its resistance face to Quantum Computers through re-scheduling and securing methods applied to binary data inputs. **Alph@TaV**(™) technology produces 4 physical output files that all have a new re-scheduled binary scheme. This new schema has no analyzable consistency out of its strict context of use. Moreover, in the 4 output files **(* .ATD / * .ATK1 / * ATK2 / * ATK3)**, part of the binary code contained in the input data is missing. The **Alph@TaV**(™) technology allows algorithmically to remove part of the binary code in a structured way, but this at positions and random moments in time. The result produces the obligation to test infinite quantities of solutions at each position (bit) of the final binary code. This also implies nonlinear infinite processing on the possible size of the binary blocks to be simulated. In addition to many other security options, the **Alph@TaV**(™) **Vault**® software also offers users the ability to use hardware as a physical lock to protect data in a strict context. We also use our own Prime Numbers Analysis and Processing Technology (**Ex0-Prime**®) to generate and read one of the encryption keys. The length of this key can optionally reach 3'000 to 81'000 bits *(about 30 minutes at generation and reading)*. Finally, the 4 output files **(* .ATD / * .ATK1 / * ATK2 / * ATK3)** have no coherence of their own and as long as they are maintained or isolated from each other, out of their strict context of use, we think that the system actually acquires its "**Quantum Resistance**".

*WE THINK THAT OUR CRYPTOGRAPHIC TECHNOLOGY IS SAFE; BY SAFE, WE MEAN REALLY SAFE! BUT WHY SHOULD YOU TRUST US?*

This is why, we offer the user to decide that each of the 4 output files **(* .ATD / * .ATK1 / * ATK2 / * ATK3)**, can be "**Over-Encrypted**" during the security process.

Indeed, the **Alph@TaV(™) Vault®** software allows selecting any type of conventional cryptographic algorithm available during software updates (*v1.5.2 included*: **AES256** / **TripleDES** / **RC2**).

The user can manually select which Over-Encryption algorithm will be applied independently for each output files, or choose the automatic random selection mode.



*DO WE THINK OUR TECHNOLOGY IS RELIABLE? YES, WE THINK! HOWEVER, WE WISH TO CHALLENGE IT AND COUNT ON YOUR EXPERTISE TO IMPROVE IT! THANK YOU.*