SK : 512+-bit eAES key, key derivation using SHA2+HKDF

Team :
John Underhill, designer and implementer of the RHX pqsym C++ code
Stiepan Kovac, CH ISO SC27 WG2 expert, business contact

thirty original AES rounds

or classical pre-shared keys (e.g. SIM) Qkd,

Qkd, or classical pre-shared keys (e.g. SIM)

Cyber-Security   Development

itk

GPG fingerprint for stie@itk.swiss:
1AB4 D367 AA1E 40BA D853 C029 253A

SK : 512+-bit eAES key, key derivation using SHA2+HKDF

Some find protecting our communications' content « boring » and prefer to spread « new hope » while they feed their AI frankensteins with the information we provide them in the exercise of our (more and more) limited e-freedoms.

We are of a different opinion : <u>protecting content is the first and foremost priority</u>, be it to protect artists' work, business communications or our medical data. To make it a continuous, quantum-safe reality, we <u>need to upgrade legacy technology</u> at the core of protecting content : AES. We provide a solution that caters specifically to this issue and <u>can use today's CPUs</u>.