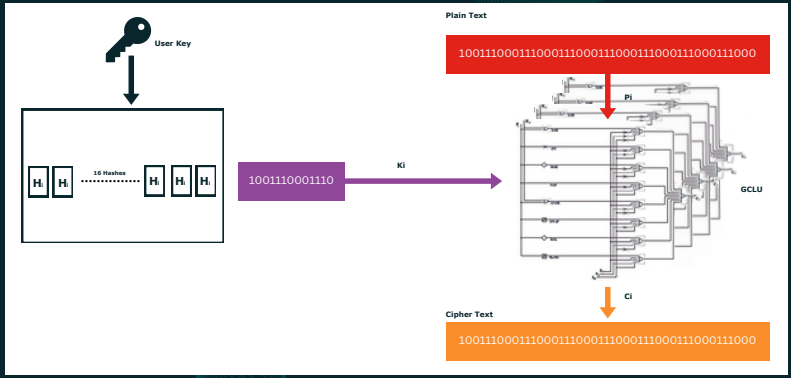
VERNEWELL

SHINING STAR

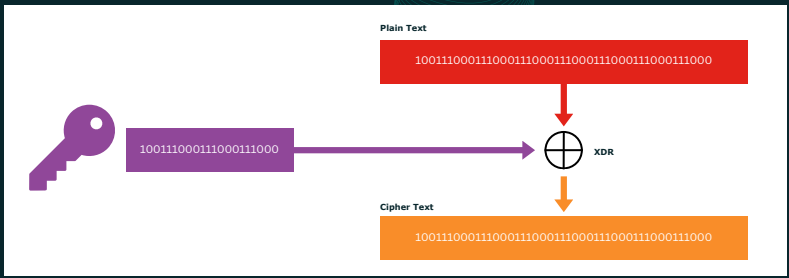
POST-QUANTUM CIPHER

Shining Star is quantum-resistant cryptographic algorithm draws inspiration from the foundational concept of the ONE-TIME PAD (OTP), integrates the Generalized Crypto Logic Unit (GCLU), and a cascade of two Hash functions mechanism.



ONE TIME PAD (OTP)

OTP inherently quantum-resistant when employed correctly, even in the face of formidable quantum computing capabilities. The practical encryption technique of OTP used key generator, and encryption/decryption unit where the key generator utilizes a pseudorandom number generator, while the encryption/decryption unit employs a bitwise XOR (exclusive OR) operation on each character of the message in conjunction with the corresponding character in the key.

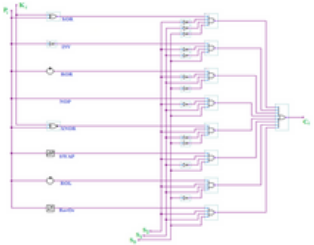


GENERALIZED CRYPTO LOGIC UNIT (GCLU)

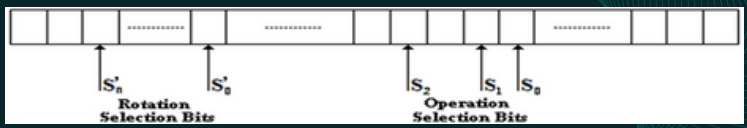
The Generalized Crypto Logic Unit (GCLU) is a unit defined by building eight low-level operations. These eight low-level operations are:

- (XOR) by XORing a key bit with a plaintext bit,
- (INV) by inverting a plaintext bit,
- (NOP) by producing the plaintext without any change,
- (ROR) by exchanging one plaintext bit with another one in a given plaintext word using a right rotation operation,
- (XNOR) by XNORing a key bit with a plaintext bit,
- (SWAP) by exchanging one plaintext bit with another one in a given plaintext word using a swap operation,
- (ROL) by exchanging one plaintext bit with another one in a given plaintext word using a left rotation operation,
- (RevOr) by exchanging one plaintext bit with another one in a given plaintext word using a reverse order operation.

Mnemonic	Operation	Select Operation Code
XOR	Ci = Ki⊕ Pi	"000"
INV	Ci =Ø Pi	"001"
ROR	Ci = Pi⇏ m	"010"
NOP	Ci =Pi	"011"
XNOR	Ci =Ki ⊙ Pi	"100"
SWAP	Ci =≠Pi	"101"
ROL	Ci =Pi⇍ m	"110"
RevOr	Ci =↓↑Pi	"111"

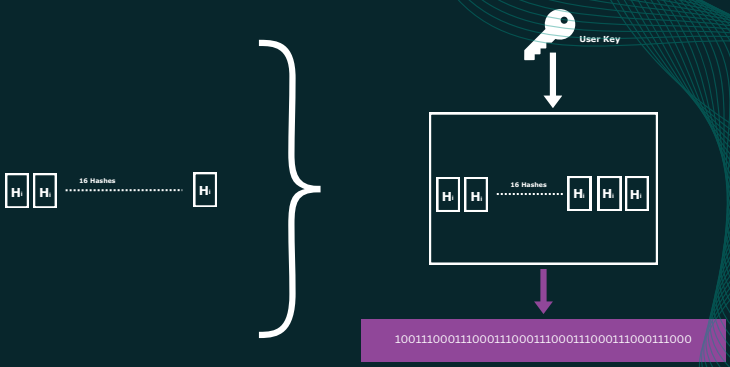


The GCLU is used as the encryption and the decryption unit where by changing the output cipher bit to become an input plaintext bit, the new output will be the same as the old plain text bit. But, this is a feature for XOR, INV, NOP, XNOR, SWAP, or RevOr functions. The exceptions are in the cases of the decryption of ROR will use ROL, and the decryption of ROL will use ROR. Likewise, the operation_selection_bits (S2S1S0) can be chosen from any three sub-key bits; the same idea applies for the rotation_selection_bits (S'n...S'0).



KEY GENERATOR

The key generator employs the user's key only once to create sub-keys. This process involves the utilization of two distinct hash functions, namely H0, and H1, using a cascade mechanism. This method randomly alternates between these hash functions, introducing a significant level of randomness and entropy into the sub-key generation process.



IMPLEMENTING SHINING STAR ALGORITHM

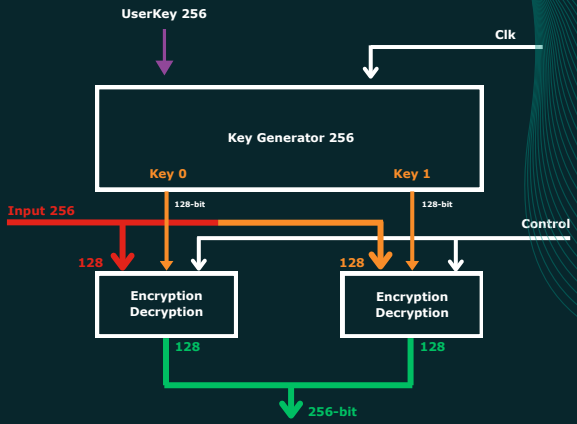
The implementing is done using FPGA (Field Gate Programmable Array) chip. Through two main parts; the Key Generator and the Encryption/Decryption module.

- **KEY GENERATOR**

  This part is responsible for generating the keys required for encryption and decryption. It takes an initial 256-bit user key and generates sub-keys using 16 pseudo-randomly generated hash functions. These sub-keys are then used for encryption and decryption.

- **ENCRYPTION/DECRYPTION**

  This part is responsible for the actual encryption and decryption of data. the Generalized Crypto Logic Unit (GCLU) used 8 subkeys generated inside GCLU from the 128-bit key, performing 17 times encryption/decryption where two 128-bit GCLU are used to encrypt/decrypt 256-bit packet.



WHAT ARE THE BENEFITS OF SHINING STAR CIPHER?

- The primary benefit is resilience against attacks by quantum computers.
- Long-term Security: As quantum computers are still in the early stages of development, it's crucial to implement cryptographic solutions that will provide long-term security.
- Diversity: The ability to integrate this algorithm into any current security infrastructure.
- Security in the Quantum Era: organizations can stay ahead of potential security risks associated with quantum computing, maintaining the confidentiality and integrity of their data even in the presence of powerful quantum computers.

APPLICATIONS

- Automotive
- Security Solutions
- Space Applications
- Information and Communication Technology (ICT)
- Healthcare and Lifestyle
- Renewables
- Industrial
- Smart Home and Building
- Robotics

Contact Us for More Info