NOVEL 5G AUTHENTICATION KEY AGREEMENT WITH QUANTUM AND POST QUANTUM CIPHERKEY DYNAMIC ON TELECOMMUNICATION NETWORKS

RAKOTONDRAMANANANA Radiarisainana Sitraka[1],
RANDRIAMITANTSOA Paul Auguste[2],

[1] *PhD student, TASI, ED-STIII, Antananarivo, Madagascar*
[2] *Thesis director, TASI, ED-STII, Antananarivo, Madagascar*

ABSTRACT

The 5G telecommunication network security is based on the standard specified by 3GPP (3rd Generation Partnership Project) and on the security of the master key shared between the UE (User Equipment) and the operator. To authenticate to the network, the 5G-AKA (5G-Authentication Key Agreement) protocol uses mutual authentication. Users resp. operators use cryptography to verify the authenticity of the operator resp. users. However, knowledge of the master key can create a hacker network that can capture the traffic of users. The QPQ-CD module (Quantum and Post Quantum Cipherkey Dynamic) consists of modifying the 3GPP standard by adding a recurrent change of this key to each successful authentication. The quantum part of QPQ-CD will be formed by a quantum confusion technique based on the Hilbert QHT (Quantum Hilbert Transform) method and the Arnold QAT (Quantum Arnold Transform) method on 3 matrices. The Post-Quantum part of QPQ-CD will focus on multiple hashing methods. The 12 families of hash algorithm used will reduce the matrices to 256 bits. An optimizer based on a one-bit change and an effective probability selector perfect the choice of the next key. The effective probability of the key will be based on probability of extremity, probability of proximity, probability of a bit changed, and probability of disorder or binary entropy and probability of penalties. According to the order of its probabilities, the following key after QPQ-CD thus has the behavior: very far from the ends of the key (00 ... 000 and 11 ... 111); very far from the previous key; several bits changed and very messy from the point of view bit zero and bit one and the penalty of bad extremity proximity. One of the 5 approaches of selectors and key optimizer will be perfected to refine the result. By simulating on MATLAB several authentication tests, the probability of the extremity and proximity will both be greater than or equal to 50% and the probability in case of binary entropy and disorder will be close to 100%. The effective probability of selection at this time will be greater than 50%

Keyword *5G-AKA, QPQ-CD, QHT, QAT, MATLAB*

1. Introduction

The telecom regulator, [1][2][3][4][5][6] has identified three main families of uses for 5G:

- mMTC: communications between a large number of objects in particular connected objects.
- eMBB: Very-high-speed Internet connections. This is particularly the case of streaming with 4K quality.
- uRLLC: Ultra reliable communications for critical needs, with very low latency. These new uses could be born with 5G, like autonomous cars

Cryptography has also been improved on new concepts such as the family of H2020 (Horizons 2020) robust against quantum attacks (Post Quantum Cryptography), robust against attacks of physical types, perfected on power consumption.

The overall architecture of the 5G telecommunication network consists of a Radio Access or Next Generation RAN (NG-RAN) and a core network or 5G Core (5 GC). The new module will be implemented at the UE and AUSF.

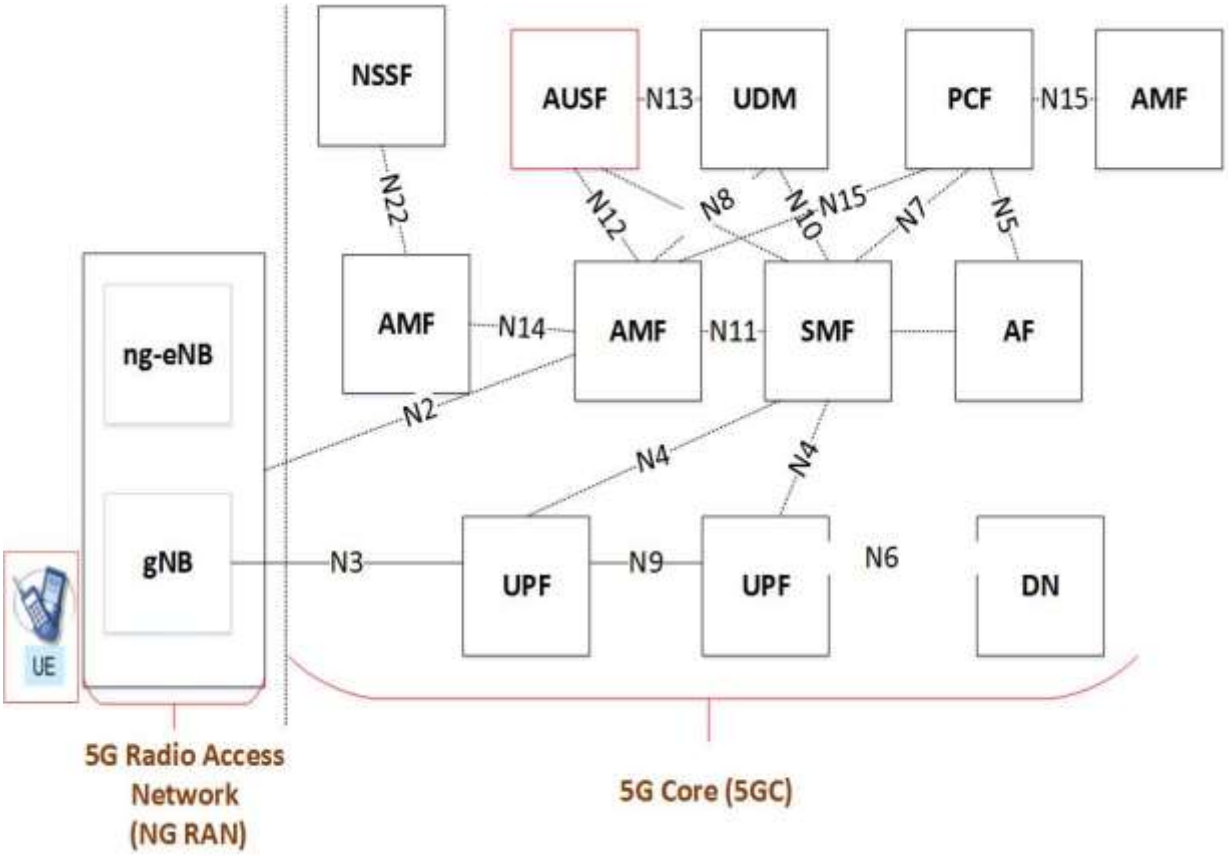

Fig -1 5G architecture and interfaces between entities

AUSF : Authentication Server Function (AuC)
UDM : Unified Data Management (HLR/HSS)
AMF : Access and Mobility Management Function (MME)
SMF : Session Management Function (MME)
NSSF : Network Slice Selection Function
PCF : Policy Control Function
UPF: User Plane Function (S/PGW)
DN : Data Network (PDN)
AF : Application Function
UE : User Equipment

In the network core, the following blocks are present:

- Authentication Server Function (AUSF): Process the authentication of the UE
- Core Access and Mobility Management Function (AMF): Deals with EU Mobility Management
- Policy Control Function (PCF): Deals with the management of any type of policy applicable to the EU (mobility management policy, QoS management, access technology selection management, etc.)
- Session Management Function (SMF): processes the EU session management
- Unified Data Management (UDM): Serves as an interface to all network functions that require access to EU subscription data.
- User plane Function (UPF): processes outgoing and incoming user plan flows from the EU
- Function Application (AF): Can use the PCF interface to request QoS implementation for a given IP flow
- Network Slice Selection Function (NSSF): Identifies the appropriate AMF function for supporting mobility management in the UE.
- Data Network (DN): Concerns Data Networks.

This architecture could be simplified by the Figure 2.

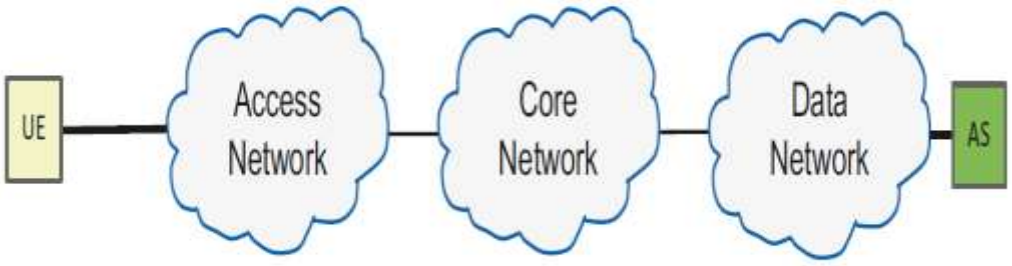

Fig -2 5G simplified architecture

The simplified architecture of the network shown in Figure 2 can be summarized as follows: access part, core part, and part of the data. As an interconnection, the different applications in AS will be exchanged with UE through the simplified architecture of the 5G network.

2. The 5G-AKA and Algorithm QPQ-CD

The authentication vectors [7][8][9][10][11][12] are in red in Figure 3. All acronyms will be defined after this Figure.
The U-SIM card of the operator has:

- the permanent identity of the SUPI cards
- the master key K protecting the user
- the SQN authentication sequence to protect against the reuse of the authentication vectors
- the public key pk_{HN} to protect the identity of the user in OTA (Over The Air) and inter-operators

The Authentication Key Agreement (AKA-5G) follows a well-defined 3GPP standard :

- To authenticate to the network, the UE sends signaling number 1 via its SUCI which is calculated by public encryption from pk_{HN}, SUPI, R.
- The authentication request to UDM by the signaling number 3 makes it possible to generate the Authentication Vectors formed by: RAND, AUTN, xRES.
- The AUSF in turn generates the server key and forms the Authentificaion vectors formed by: RAND, AUTN, xRES, K_{AUPF}.
- In the AMF module after signaling number 5, the authentication vectors are formed by: RAND, AUTN, hxRES, K_{AMF}.

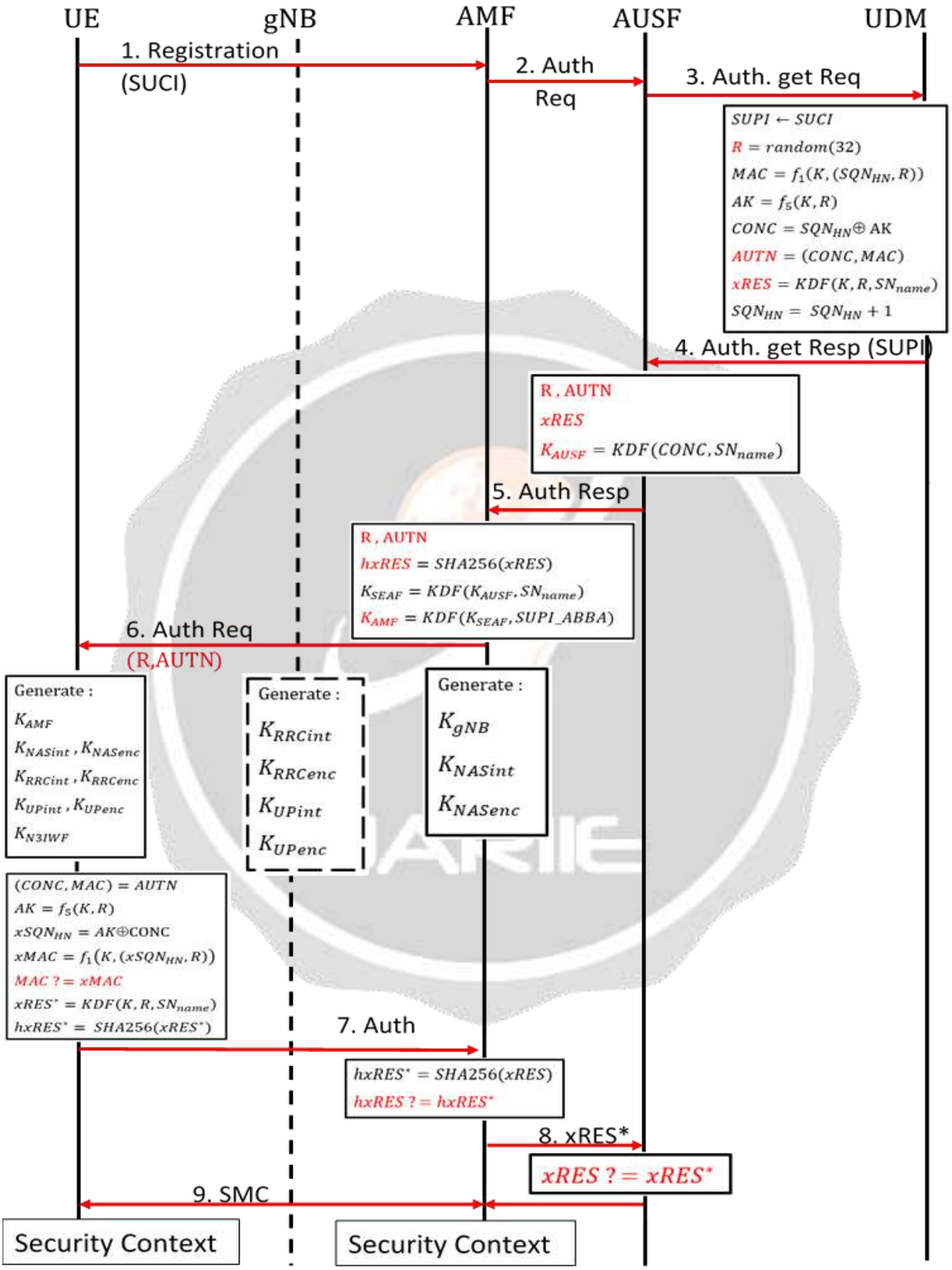

Fig -3 5G-AKA

UE : User Equipement

gNB : gigabit NodeB
AMF : Access and Mobility Management Function
AUSPF : Authentication Server Function
UDM : Unified Data Management Function
SUPI : Subscription Permanent Identifier
SUCI : Subscription Permanent Identifier
R : Random Number
MAC : *Message Authentication Code*
K : Master Key
SQN_{HN} : Sequence number of Home Network
AK : Anonimity Key
CONC : CONCEALEMENT
AUTN : Authentication Number
SN_{name} : Serving Network Name
$xRES$: eXepted Result
$hxRES$: Hashed eXepted Result
K_{AUSF} : Key of AUSF
K_{SEAF} : Key of SEcurity Anchor Function
K_{AMF} : Key of gNB
$SUPI, ABBA$: SUPI, Anti Bidding down Between Architectures
K_{gNB} : Key of gNB
K_{NASint} : Key of Non Access Stratum Integrity
K_{NASenc} : Key of Non Access Stratum Security
K_{RRCint} : Key of Radio Ressource Control Integrity
K_{RRCenc} : Key of Radio Ressource Control Security
K_{UPint} : Key Uplink Integrity
K_{UPenc} : Key Uplink Security
K_{N3IWF} : Non-3GPP Interworking Function
$xMAC$: eXepted MAC
$hxRES^*$ and $xRES^*$: Hashed eXepted Result from user and eXepted Result from user
SMC : Security Mode Command

- For the OTA part, the gNodeB then sends 2 parts of the authentication vector RAND, AUTN which AUTN allows the UE to check the authenticity of the operator and the RAND to give an answer to the operator if the EU is the same through hxRES.
- For the terminal equipment and the operator to ensure interconnection: the UE checks whether it really authenticates to the real network of the operator and not to a hacker network through the verification of MAC and sometimes SQN_{HN}. The EU then calculates the result to ensure its authenticity.
- The hxRES result will be sent to the AMF is verified and xRES will be verified by the AUSPF.
- Once authenticated, the mobile network sends the Session Message Context (SMC) signaling to confirm the interconnect establishment. The QPQ_CD algorithm on the part of the sender uses the SMC_ACTIVATION_UE message from the user and

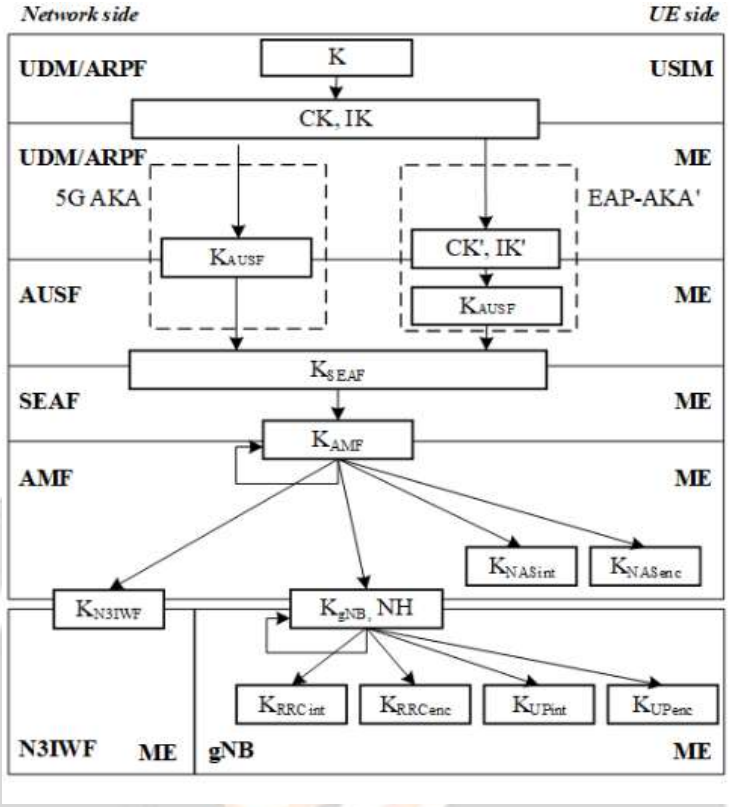

Fig -4 Hierarchy of keys

All the keys are mentioned in Figure 3. The Key generation will be provided by the KDF function (Key Derivation Function) whose input has a key K and some parameters of modifications and outputs the derived key. All keys on the Figure 4 derive from the master key K. EAP-AKA (Extensible Authentication Protocol) allows the authentication of a UE-4G in the 5G network.

2.1 Implementation of simplified QPQ-CD

QPQ_CD uses the master key Dynamicity K. This function has as input the previous key K and an activation signal A and a parameter r defining the complexity rule of QPQ-CD.
The steps of the algorithm are:

- The initialization phase: the goal is to initialize K, r, and i an activation counter and to generate from the Expansion towards the Matrix (E.M) a matrix of 16r × 16r of 8 bits
- The insertion phase: It consists of periodically inserting while scanning the line of the matrix 16r × 16r a key obtain through the Expansion towards the Linearity (E.L). The insertion is executed only at each activation signal. Since the QPQ-CD algorithm uses 3 16r × 16r matrices, a key-generating function denoted by G makes it possible to generate 3 parts of the key of initializations for each matrix.
- The phase of Quantum Cryptography: The phase of Quantum Cryptography uses the method of confusion either by the Hilbert method or by Arnold's method.
- The PQ phase cryptography: it uses several hash algorithm samples to summarize the matrix after confusion in order to have a 256 bits key.
- Phase selectors : it selects the next key K+ appropriate.

The output of the QPQP-CD algorithm is another key generated K+, for other applications especially in the authentication. QPQ-CD is also a family of KDF algorithm. The simplified schema of the QPQ-CD algorithm is represented in Figure 5.

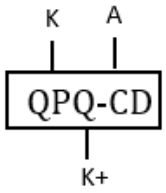

Fig -5 QPQ-CD

2.2 Expansion, Expansion towards linearity and Expansion towards the Matrix of QPQ-CD

The expansion uses two boxes following the Figure 6
- The SBOX substitution box
- Round algorithm of the RCON algorithm (Round CONstant)

The input of expansion has keys of 16 bytes, rcon of 4j bytes and s_box of 16x16 bytes and L_expansion. The output produce key of 16xL_expansion bytes named by w.

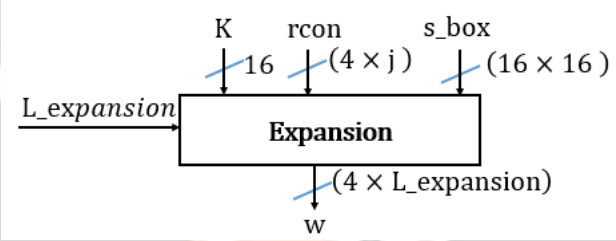

Fig -6 Diagram block of Expansion

The expansion algorithm registers two by two the 128-bit key to form an initial vector of $16 \times 8bit = 16byte$. Each component noted by $k_{11}, k_{12}, k_{13}, k_{14}, k_{21}, k_{22}, k_{23}, k_{24}, k_{31}, k_{32}, k_{33}, k_{34}, k_{41}, k_{42}, k_{43}, k_{44}$ of the matrix represented by Figure 7 will be organized to form an initial matrix of 4×4

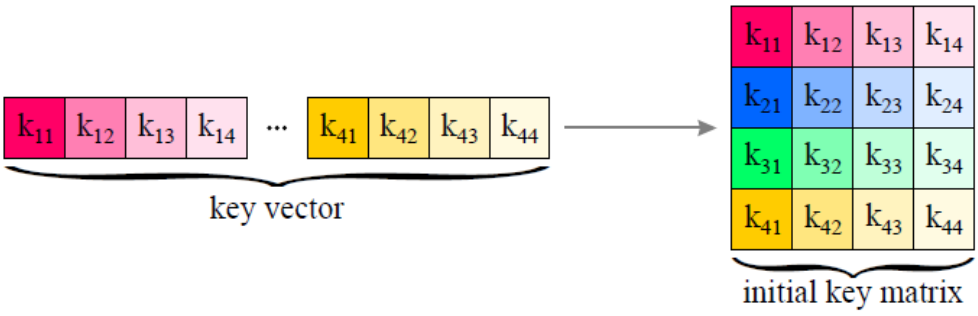

Fig -7 Initialization of expansion

The expansion is done by Figure 8.a which is repeated using the expansion sub-module of Figure 8b. The first line of the next block is obtained using the expansion sub-module of Figure 8b and doing the xor operation with the first line of the current block. The second line to the fourth line of the next block is obtained by doing an xor operation of the preceding line of the next block and the line of the current block. The operation is repeated j-times. The block providing the expansion sub-module has 16 bytes input rcon_j of input and (4 × L_expansion) byte output. This sub-module consists of substitutions via the box s_box and a round operation using xor at each time rcon_j.

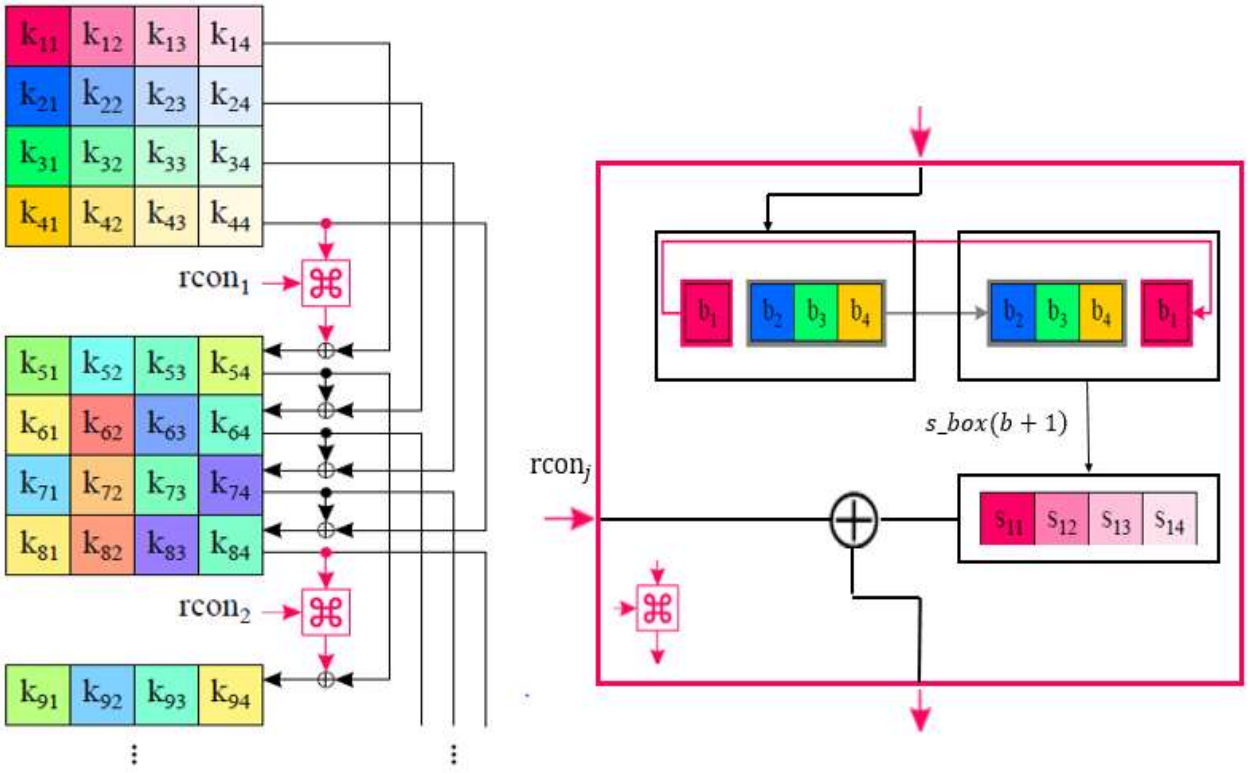

Fig -8a : *General Module of Expansion* **Fig -8b :** *Sub-Module of Expansion*

Fig -8 Module of Expansion

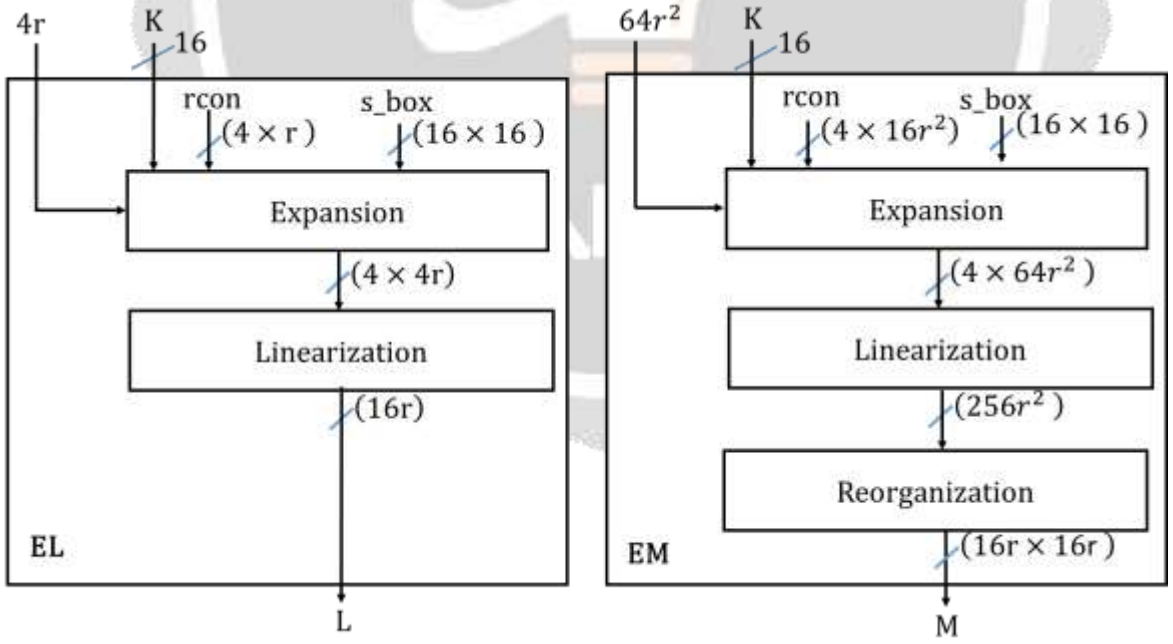

Fig -9a : *Expansion towards the Linearity QPQ-CD* **Fig -9b :** *Expansion towards the Matrix QPQ-CD*

Fig -9 Module of Expansion used with QPQ-CD

The Expansion towards the linearity resp. Expansion toward the Matrix has an input parameter K, a 16 bytes or 12 8bits key. The permutation and substitution matrices allowing the key to be expanded in a size of 4 × 4r resp. $4 \times 64r^2$ using the modules in Figure 9. The linearization module makes it possible to have a linear matrix of size 16r resp. $256r^2$. The reorganization module transforms the linearized matrix into a 16r × 16r matrix.

2.2 Generation (G) of Key block diagram

The key generator block allows you to have three 12 8bits (16bytes) keys K1, K2, K3, from a K key with 256 bits (32 bytes). The block first divides the key K into two keys K1 and K3. K3 is obtained by making xor between K1 and K2. Figure 10 shows the key generation block.

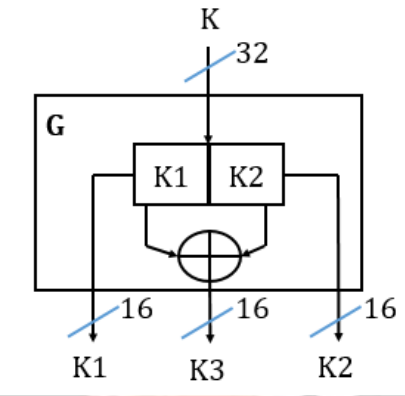

Fig -10 Generation of Key

2.3 Quantum Cryptography Algorithm (QC)

The Q-Cryptography [13] [14] algorithm implements a technique of scrambling on the digital image processed by quantum processors using QIS (Quantum Image Scrambling). The input of the algorithm is a classical image of size 16r × 16r. The matrix will be transformed into a quantum FRQI model then processed in QAT (Quantum Arnold Transform) and QHT (Quantum Hilbert Transform). Since the matrixes of the red, green, blue have their own component separately, the corresponding FRQI images are processed separately according to the inputs JR, JG, JB. To be able to process by conventional computers, the PQ-Cryptography module after Q-Cryptography, a measurement module FRQI makes it possible to determine the digital matrix result of qht_R, qat_R, qht_G, qat_G, qht_B, qat_B.

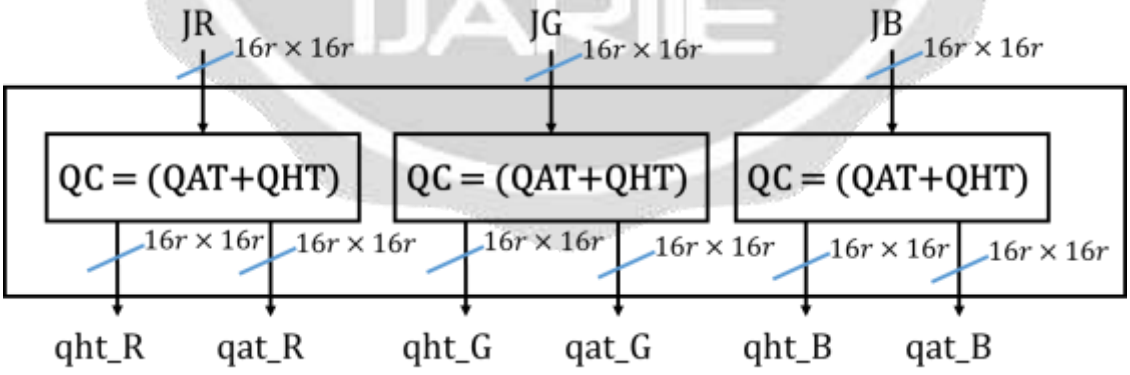

Fig -11 QC algorithm

In the general application qht_R, qat_R, qht_G, qat_G, qht_B, qat_B will be simplified by q formed by the components q1 ... .q6

2.4 Algorithm Quantum Crypto (PQC)

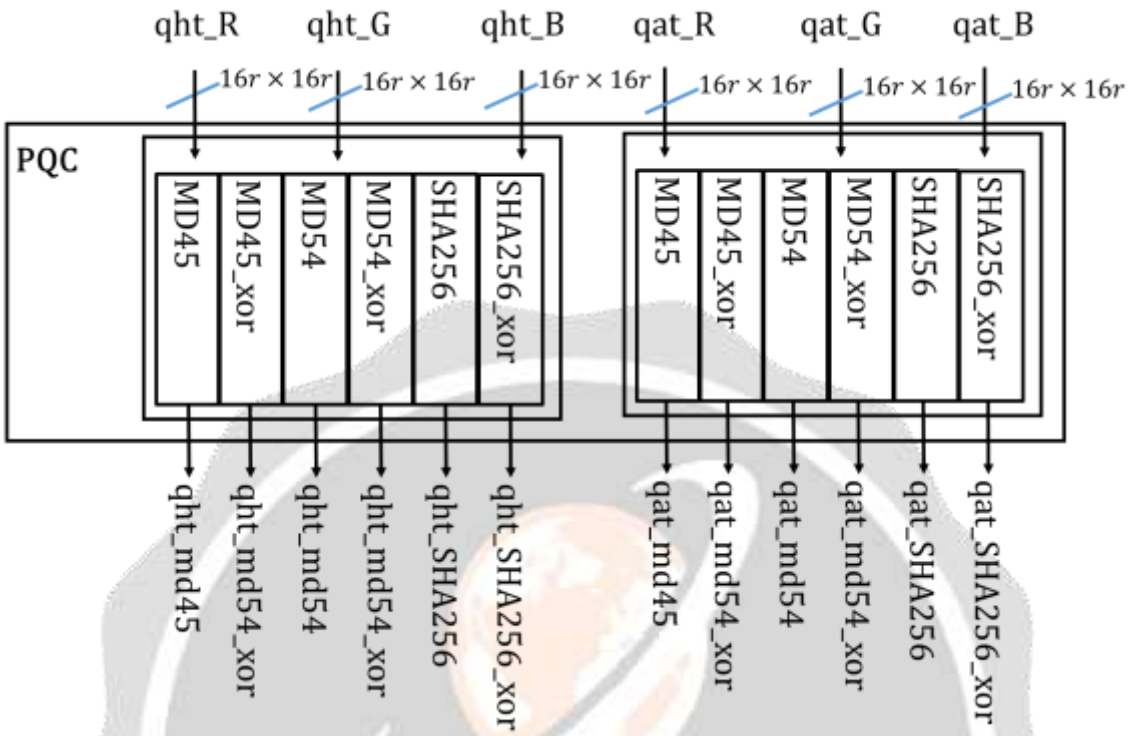

Fig -12 PQC algorithm

MD45: MD4 concatenated with MD5 on block matrices _R, _G, _B
MD54: M5 concatenated with MD4 on block matrices _R, _G, _B
SHA256: SHA 256 on block matrices _R, _G, _B
MD45: MD4 concatenated with MD5 on the separated matrices _R, _G, _B followed by xor between them
MD54: M5 concatenated with MD4 on the separated matrices _R, _G, _B followed by xor between them
SHA256: SHA 256 on the block matrices _R, _G, _B followed by xor between them
The PQC [15-16] used in this module use multiple hash function. The block matrix _R, _G, _B is a matrix of three dimensions of (16r × 16r × 3) byte by grouping the 3 parts qht_R, qht_G, qht_B resp. qat_R, qat_G, qat_B each size (16r × 16r). 12 outputs : qht_md45, qht_md45_xor, qht_md54, qht_md54_xor, qht_sha256, qht_sha256_xor, qat_md45, qat_md45_xor, qat_md54, qat_md54_xor, qat_sha256, qat_sha256_xor can also be simplified by a vector p formed by the elements p1 ... p12

2.5 QPQ-CD-UE Algorithm

The initialization phase is performed during the first purchase of the USIM card.

- The initialization algorithm makes it possible to initially initialize the parameters i and r then the key K having a value of 32 bytes or 256 bits.
- The key K will be subdivided into 3 keys of 16 bytes K1, K2, K3 and the Expansion towards the Matrix (E.M.) allows to have the matrixes JR, JG, JB of size 16r × 16r

Figure 13 represented the QPQ-CD-UE algorithm about initialization.

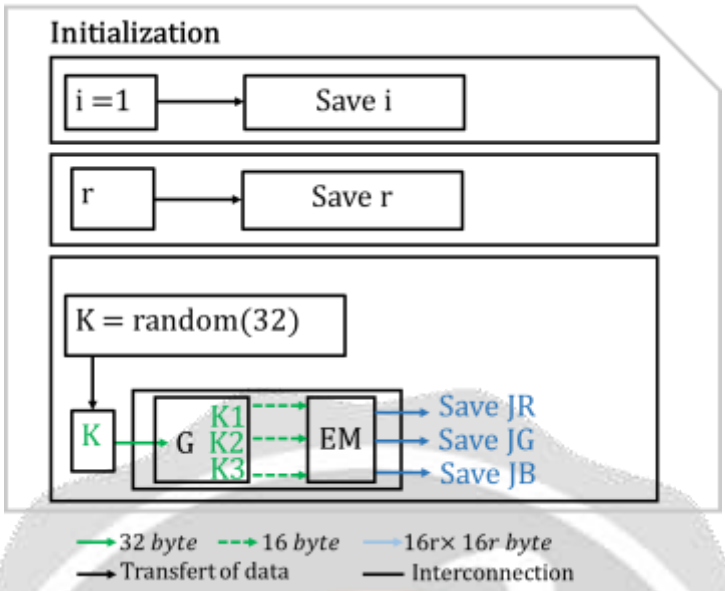

Fig -13 Initialization QPQ-CD UE

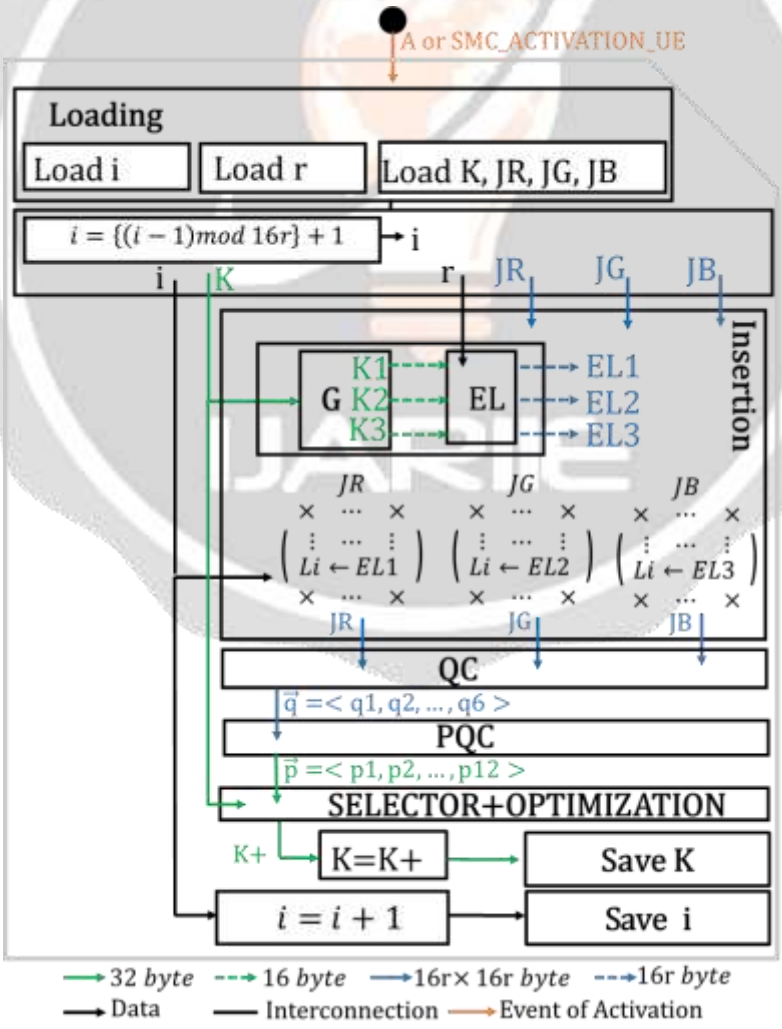

Fig -14 Activation QPQ-CD UE

In Figure 14, the activation phase is triggered on each successful authentication by the UE. The initialization parameters r, i, K and JR, JV, JB will be loaded. The value of i is first set to be in 1 ... 16r.
During each trigger, each key K will be subdivided into 3 keys K1, K2, K3 and will be transformed by an Expansion towards the Linearity (E.L) to have EL1, EL2, EL3.
These keys EL1, EL2, EL3 are successively inserted into the matrices JR, JV, JB on the i-th lines. The confusion technique by the QC module makes it possible to have the matrices q1 ... q6.
PQC algorithms of the multiple hash family summarize the matrices q1 ... q6 for 12 keys p1 ... p12 of 32 bytes or 256 bits. The selector and optimization make it possible to choose only one suitable key among the 12 keys. The key will be registered and the activation counter will be increased before being saved.

2.6 QPQ-CD AUSF

The initialization phase QPQ-CD AUSF is the same as that of QPQ-CD UE, the difference is that the AUSF manages several users. Backups should be associated with each SUPI.

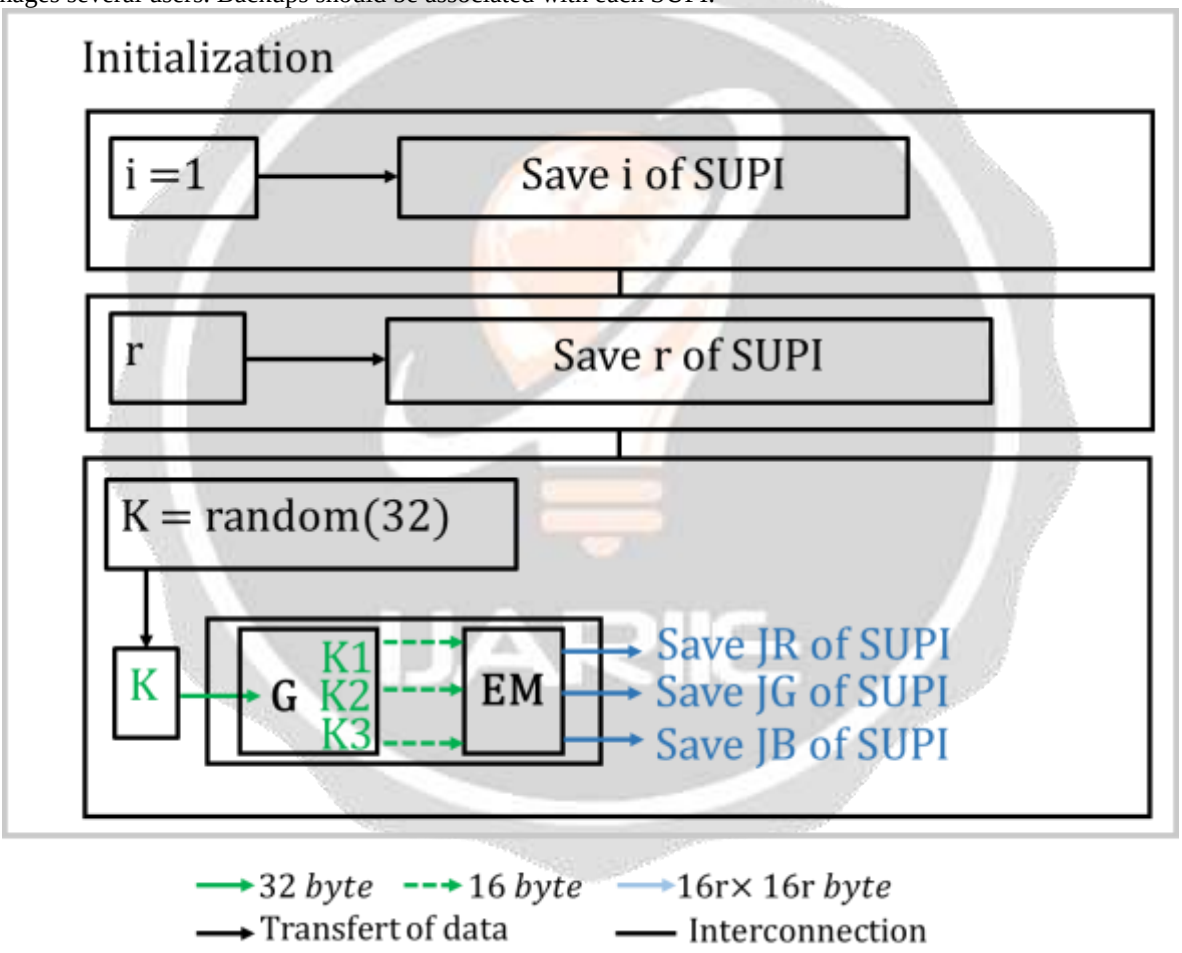

Fig -15 Initialization QPQ-CD AUSF

The activation phase QPQ-CD AUSF is the same as that of QPQ-CD UE, the difference is that the AUSF manages several users. Backups and uploads should be associated with each SUPI.

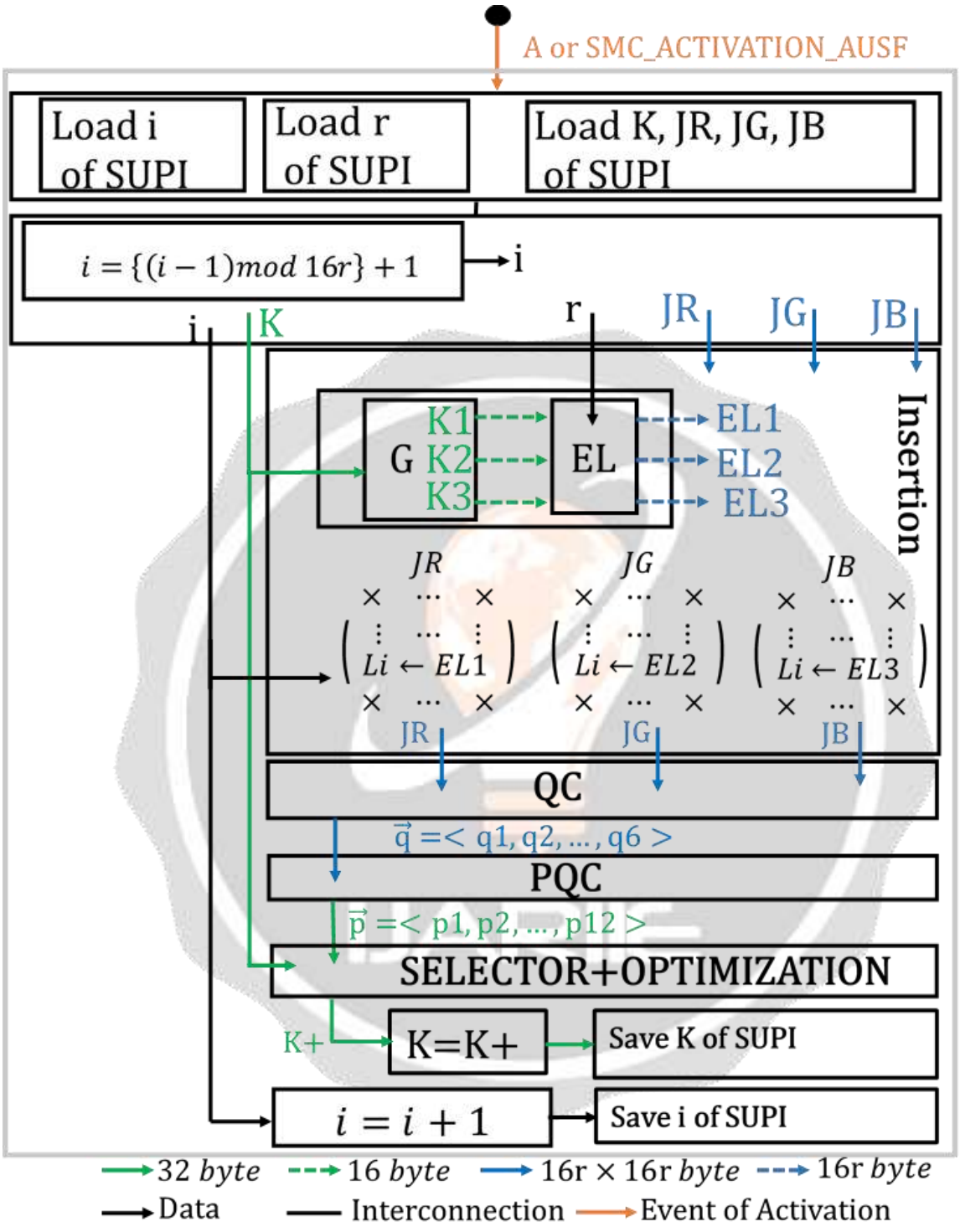

Fig -16 Activation QPQ-CD AUSF

2.6 Evaluation of QPQ-CD

For the performance study of the QPQ-CD algorithm, the activation counter will be traversed until the end of the insertion line. Thus, i vary from 1 ... 16r.

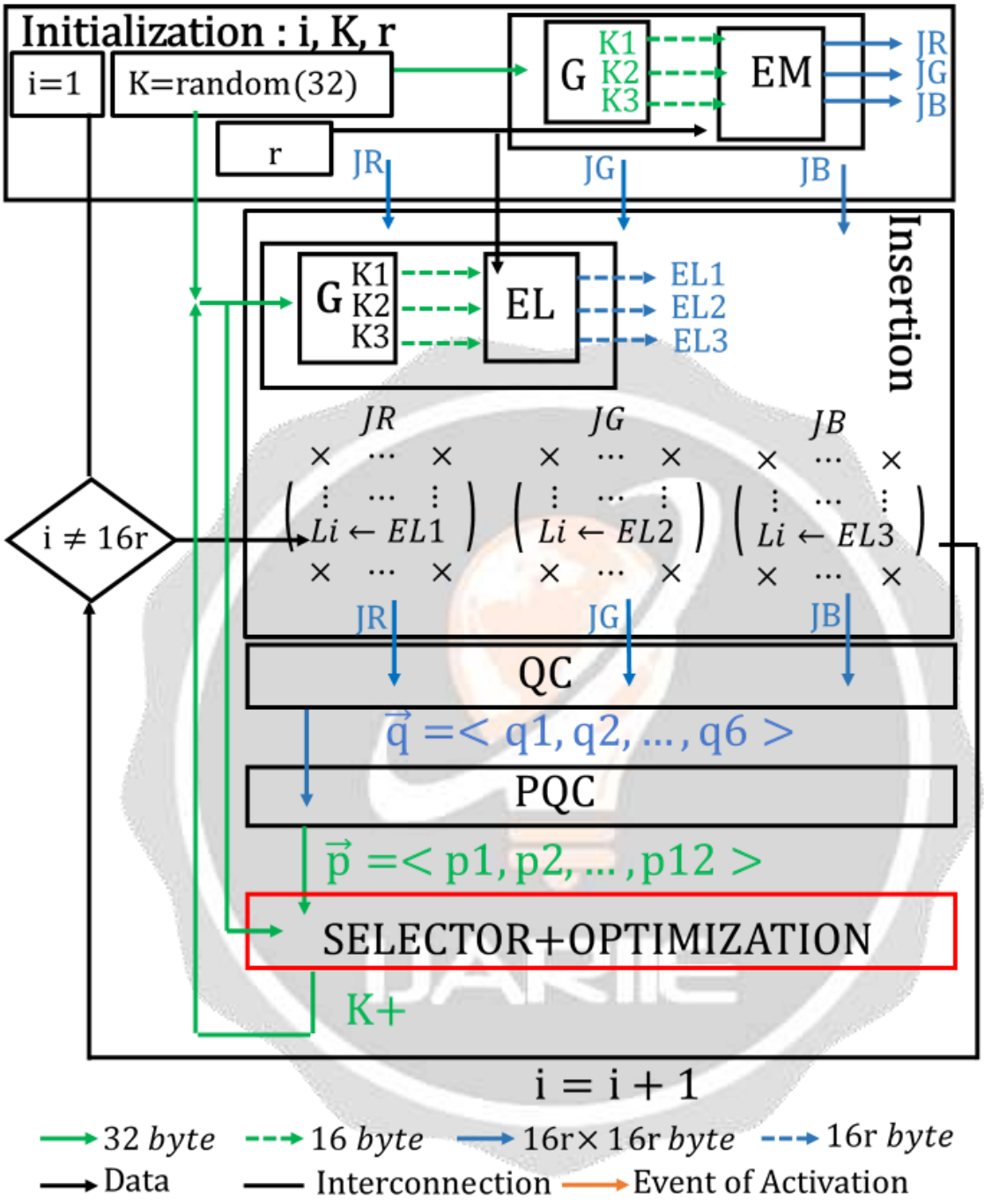

Fig -17 Evaluation QPQ-CD

The QPQ-CD algorithm will be characterized by the initialization phase that generates r, i, K then JR, JG and JB. The insertion of the keys generated by the Expansion towards the Linearity (E.L) and the key generator G will be repeated at each blur up to 16r. The QC algorithm followed by PQC will be finalized by the optimization selector to obtain the key next K +.

The selection algorithm uses several criteria to identify the best key using the probability of not detecting the key from the previous key by focusing on how opponents think and other relevant criteria. Since the insertion of the matrix is done at each line from 1 to 16r, the authentication sample will be limited to this value 16r.

3. Interpreting approach for QPQ-CD

The selector uses the effective probability to select the best option. The effective probability is derived from the probability of extremity, probability of proximity, probability of a bit changed, probability of disorder and probability of penalties. All the curves studied use interpolation by Hermite polynomials as known as PCHIP (Piecewise Cubic Hermite Interpolating Polynomial).

- Probability of the extremity:

The brute force attack is to browse all the possibilities in a random way is not profitably compared to the orderly way. According to the logic as well, an opponent wanting to test all possible keys using the brute force algorithm always starts with 00...000 up to 11...111 using increases or starting with 11...111 up to 00 ...000 using decreases.

$$\underbrace{\begin{cases} 00000 \dots \dots \dots 000 \\ \dots \dots \dots \dots \dots \dots \dots \dots \\ 11111 \dots \dots \dots .111 \end{cases}}_{\text{Increases}} \quad \underbrace{\begin{cases} 11111 \dots \dots \dots .111 \\ \dots \dots \dots \dots \dots \dots \dots \dots \\ 00000 \dots \dots \dots 000 \end{cases}}_{\text{Decreases}} \tag{1}$$

The closer the key is to 00 ... .000 or closer to 11 ... .111, the lower the probability of not detecting the key.

If the key is close to 0, the high-order one is difficult to detect. Because of this, the probability of not detecting the key if it is close to zero is defined by:

$$p = \frac{\sum_{i=0}^{n-1}[k(i) == 1].\, 2^i}{\sum_{i=0}^{n-1} 2^i} \tag{2}$$

If the key is close to 1, the high-order zero value bit is difficult to detect. Because of this, the probability of not detecting the key if it is close to one is defined by:

$$q = \frac{\sum_{i=0}^{n-1}[k(i) == 0].\, 2^i}{\sum_{i=0}^{n-1} 2^i} \tag{3}$$

Using both approaches, the probability that the key is close to 00 ... 000 and 11 ... 111 is formed by the appearance of one of two formulas (2) and (3):

$$prob_{extr} = \begin{cases} p = \dfrac{\sum_{i=0}^{n-1}[k[i] == 1].\, 2^i}{\sum_{i=0}^{n-1} 2^i} & if\ near(k, 0000 \dots 000) = 1 \\ q = \dfrac{\sum_{i=0}^{n-1}[k[i] == 0].\, 2^i}{\sum_{i=0}^{n-1} 2^i} & if\ near(k, 1111 \dots 111) = 1 \\ \begin{cases} near(k, 0000 \dots 000) = (k[n] == 0) \\ near(k, 1111 \dots 111) = (k[n] == 1) \end{cases} \end{cases} \tag{4}$$

Where n is the size of the key.
prob_extr is the probability that key k will be close to the extremity 00 ... 000 or 11... 111
The near function is defined as follows the formula (4)

- Probability of the proximity:

The probability of the proximity is summed up by the fact that the two keys: current key and next key are all closer to one another. By imagining two specific keys to compare:

$$(k_1, k_2) = (0010, 0100)$$

The distance between the two bits is the subtraction between the two keys:

$$xor(k_1, k_2) = 0110$$

To go from $k_1 \rightarrow k_2$ will be equivalent to going from $0000 \rightarrow xor(k_1, k_2)$
To go from $k_2 \rightarrow k_1$ will be equivalent to go from $1111 \rightarrow xor(k_1, k_2)$

$$prob\_prox = prob\_extr\left(xor(k_1, k_2)\right) \quad (5)$$

- bit probability changed:

  Assuming two keys (k_1, k_2), the probability of bit change is not good if it's near to 256 bits so, it's defined by :

$$prob_{change} = \begin{cases} \frac{\sum_{i=0}^{n-1} xor(k_1,k_2)[i]}{n} & if \ \frac{\sum_{i=0}^{n-1} xor(k_1,k_2)[i]}{n} \leq 0.5 \\ \left|1 - \frac{\sum_{i=0}^{n-1} xor(k_1,k_2)[i]}{n}\right| & others \end{cases} \quad (6)$$

- Binary Entropy: The entropy of the following key is defined by:

$$H = -p(0)log_2(p(0)) - p(1)log_2(p(1)) \quad (7)$$

3.1 Effective probability options 1

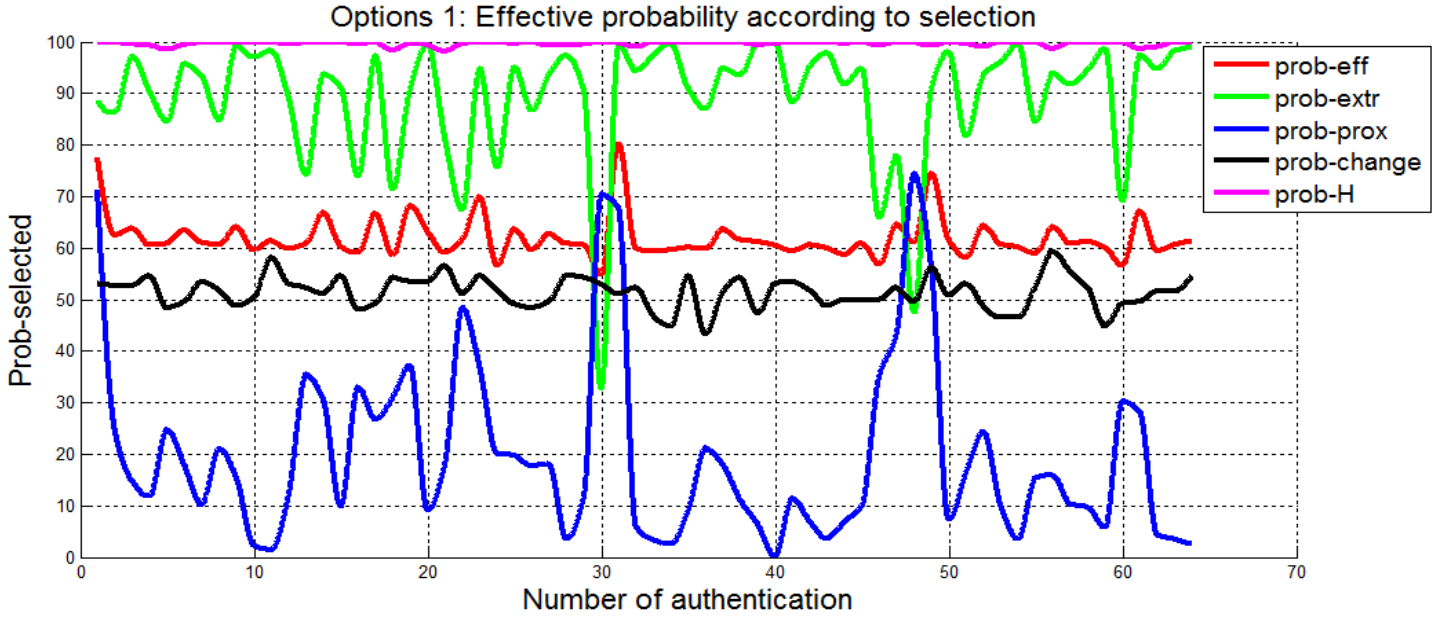

Fig -18 Effective probability using option 1

Interpretation:

The effective probability will be obtained using an evaluation according to the weighting according to the different criteria by using the average and the linear combination:

$$prob_{eff1} = Max\left\{\frac{4 * prob_{extr} + 3 * prob_{prox} + 2 * prob_{change} + prob_H}{4 + 3 + 2 + 1}\right\} \quad (8)$$

In option 1, the key chosen after QPQ-CD will be obtained by weighting in order of priority. The two most important criteria are the probability of finding a key far from the extremities and especially also the probability that the two keys (previous and next) will be separated from each other. The weights are in increasing order successive: probability for the bits are in disorder or prob-H, then the probability of finding several bits that change in the next key or prob-changed, probability of proximity and finally the probability of extremity. According to Figure 18, in this, the effective probability is close to 60% which seems a good approach but by doing a thorough analysis, only the probability of extremity approach 90% while the probability of proximity can reach even very low value less than 10%. Thus, the following key is very resistant to brute force attacks as it is very far from keys 00 ... .000 and 11..111 but the following key is not far enough from the previous key.The option 1, also allows to have a probability of disorder close to 100% but probability to find a bit changed by only about 50%. The curve stops for the value 64 which is due to the fact that r is equal to 4.

3.2 Effective probability options 2

The option 2 consists of prioritizing the proximity probability weighting with respect to the extremity.

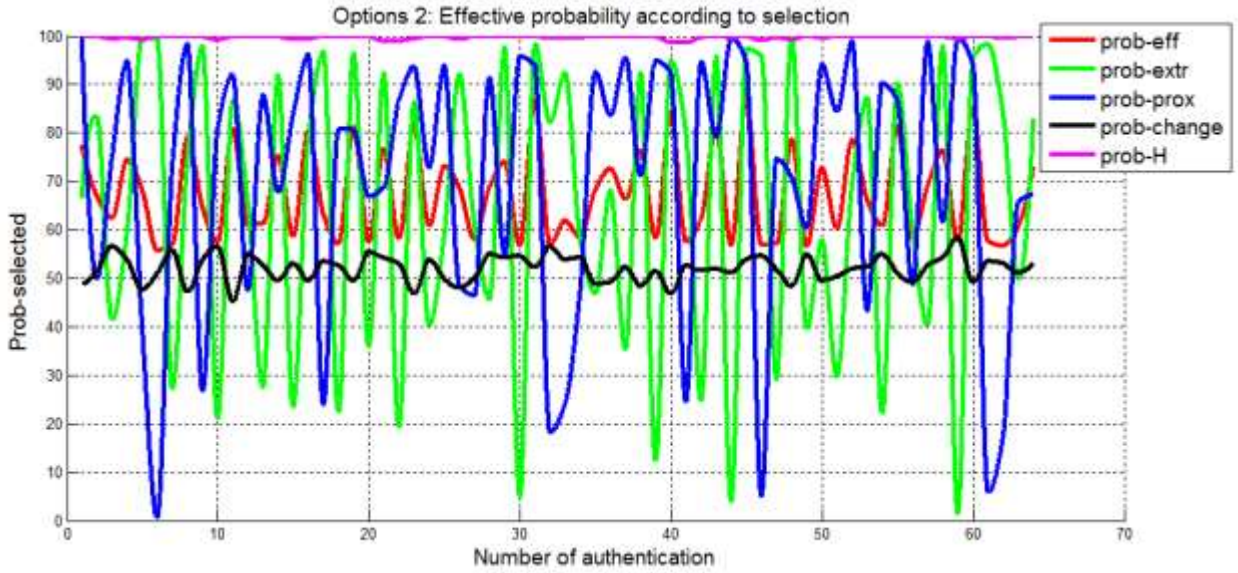

Fig -19 Effective probability using option 2

Interpretation:

Taking into account the priority of the probability of proximity. The effective probability is greater than 50%. However, by analyzing the probability of extremity or the probability of proximity, several cases present between 10% and 30% when this key is chosen.

If the extremity probability resp. proximity is very high, even if the probability of proximity resp. extremity is very small, the selector still chooses this key instead of other better option. In Figure 19, the option 2 also allows for a probability of disorder close to 100% but probability of finding a bit changed is only about 50%.

3.3 Effective probability option 3

Studying the case: two probabilities of extremity and probability of proximity parameters separately is not a good approach. When one reaches an optimal value, the other reaches a very low value while the effective probability shows a value greater than 50%.The option 3 consists of combining the two to have the parameter $prob_{extr\_prox}$ by:

$$\begin{cases} prob_{eff3} = Max\left\{\dfrac{3*\left(prob_{extr\_prox}\right)+2*prob_{change}+prob_{H}}{3+2+1}\right\} \\ prob_{extr\_prox} = \dfrac{prob_{prox}+prob_{extr}}{2} \end{cases} \quad (9)$$

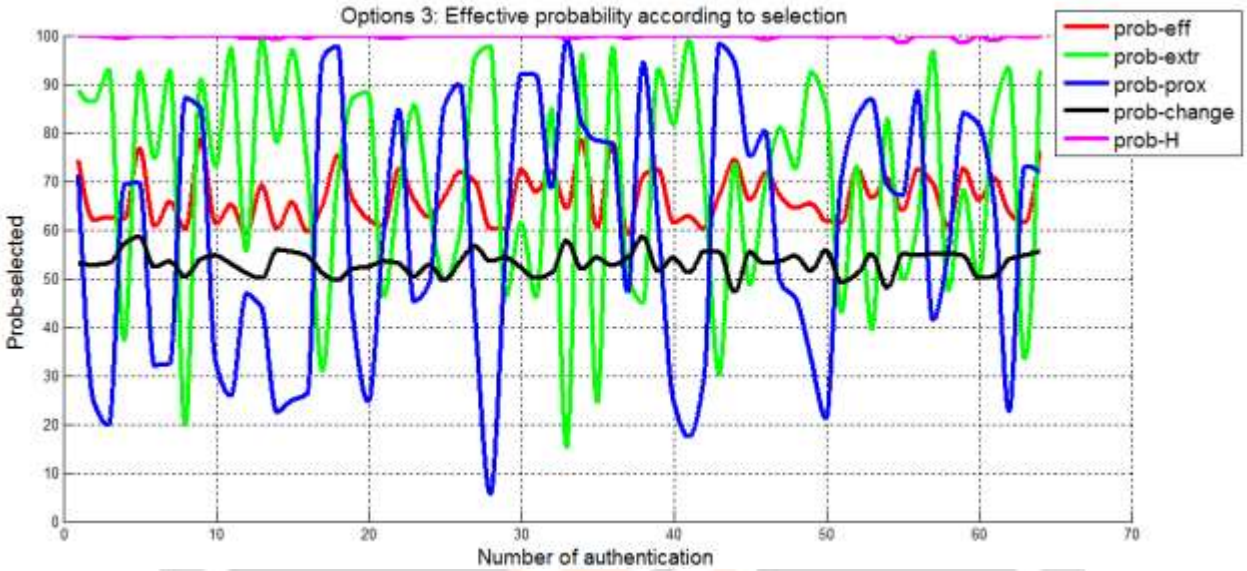

Fig -20 Effective probability using option 3

Interpretation:

The effective probability deviates greater than 60%, the circumstance shows that the probability of extremity resp. probability of proximity close to 90% results in some authentication having a probability of proximity or an extremity probability of less than 20%. Compared to the option 2, this minimum value is no longer very close to zero. In Figure 20, the option 3 also allows for a probability of disorder close to 100% but probability of finding a bit changed by only about 50%.

3.4 Effective probability option 4

The option 4 takes into account the improvement obtained in option 3, the goal is to have at the same time a probability of proximity and probability of high proximity. However, even combining the two parameters, this case is not yet solved. Therefore, if the average exceeds a reference value 70, the key obtained with is penalized defined by the formula 10.

$$\begin{cases} prob_{eff4} = Max\left\{\dfrac{3*\left(prob_{extr\_prox}\right)+2*prob_{change}+prob_{H}}{4+3+2+1}+Penalty\left(prob_{extr\_prox}\right)\right\} \\ prob_{extr\_prox} = \dfrac{prob_{prox}+prob_{extr}}{2} \\ Penalty\left(prob_{extr\_prox}\right) = \begin{cases} min(x-ref, y-ref)\ si\ \left((x-ref)<0\right) ou\ \left((y-ref)<0\right) \\ 0 \qquad\qquad others \end{cases} \end{cases} \quad (10)$$

Probability of extremity and proximity exceeding the ref value (70%) will be penalized during the selection.

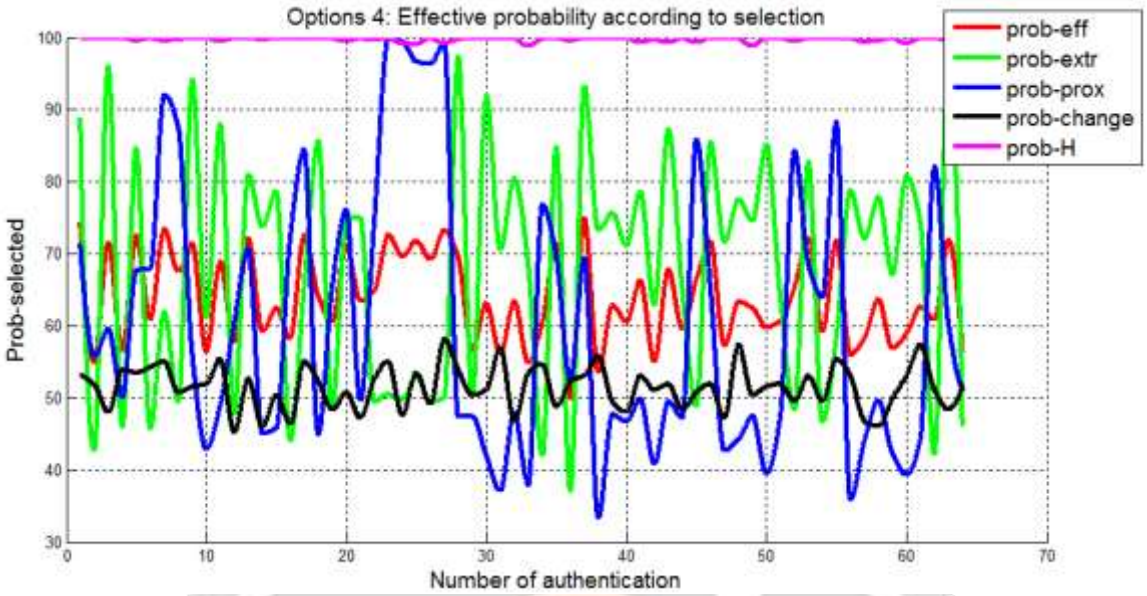

Fig -21 Effective probability using option 4

Interpretation:

The effective probability being greater than 50% with which the probability proximity and the probability of the extremity will be greater than 30% both with a probability in case of the binary entropy about 50% and probability of disorder about 100%.

To obtain a comparison of the probability of the extremity and proximity, Figure 21 was introduced to the key distance.

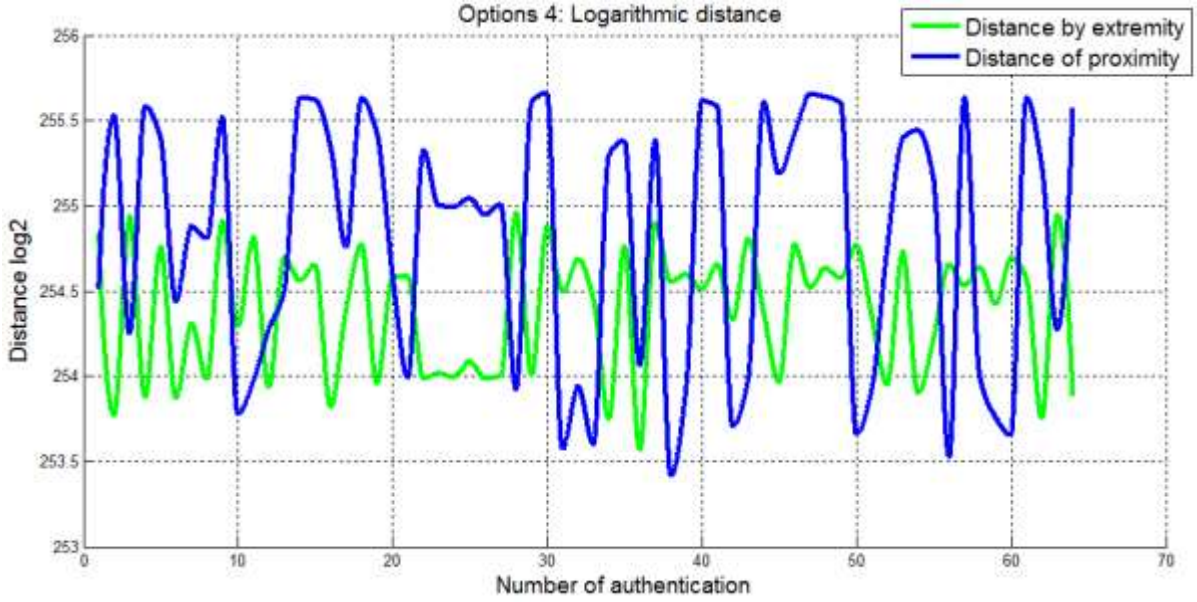

Fig -22 Distance logarithmic using option 4

Interpretation:

Testing all combinations of a 256-bit key is equivalent to visiting the entire universe. Plotting the distance between the two keys (previous and next) and the minimum distance from the extremity (00 ... 000 or 11 ... 111) will be represented by a logarithmic distance in base 2.

The logarithmic distance is defined by:

$$\begin{cases} d_{prox} = log_2(|(K_+)_{10} - (K)_{10}|) = log_2(|(K_+) \oplus (K)|) \\ d_{extr} = \min\left(log_2(|(K_+) \oplus (00 \dots 000)|); log_2(|(K_+) \oplus (11 \dots 111)|)\right) \end{cases} \quad (11)$$

K+ key next after QPQ-CD
K previous key before the QPQ-CD
d_{prox} proximity distance between the two incoming and outgoing keys of the QPQ-CD
d_{extr} distance from the key ends coming out of the QPQ-CD
The Figure 23 shows that the distance between the next key and the preceding key and the distance separating the key at borders 00 ... 00 and 11 ... 11 is distanced between $2^{253.5}$ and $2^{255.5}$.

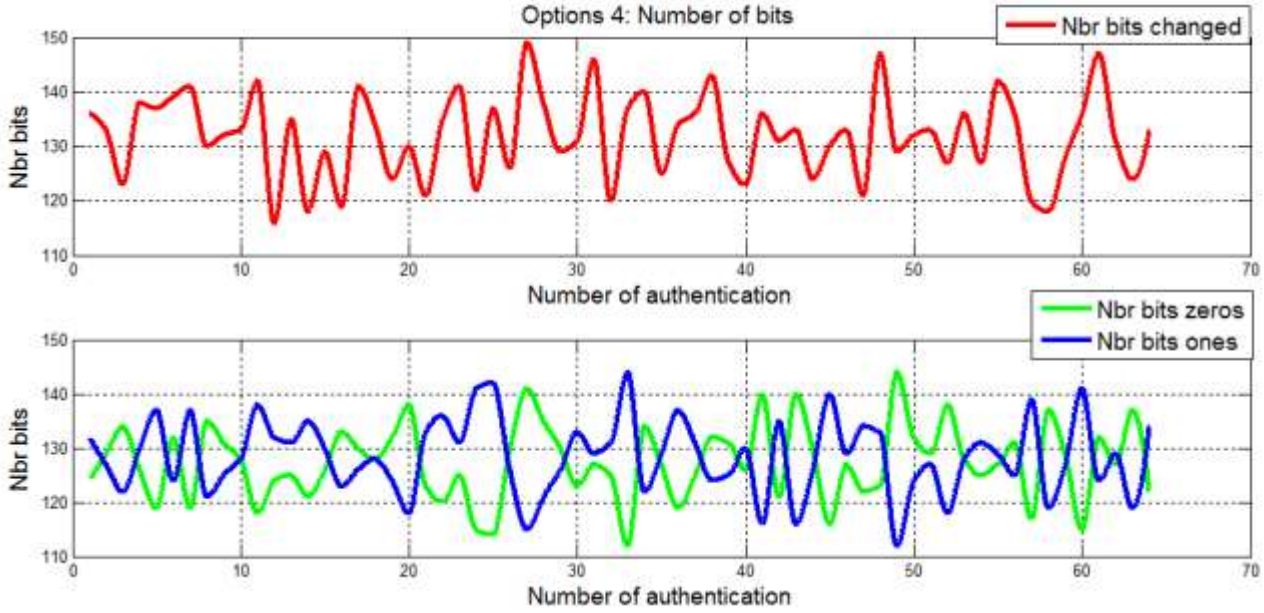

Fig -23 Number bit using option 4

Interpretation:
To better visualize the probability of clutter of the key and the probability of a bit changed Figure 23 was introduced. The number of bits changed thus varies from 115 to 150. Thus, the probability bit according to Figure 21 is 50% as the key size is 256 bit.
In addition, the number of zeros bits and the number of bits makes it possible to check the Prob-H disorder probability of Figure 21. More the probability of occurrence of zeros and ones in the key is close to 50% then, more the key is out of order. As a result, the number of bits of zeros and one is close and symmetrical to the 128-bit number that is 50% of 256 in Figure 23. The goal is to have both the probability of disorder close to 100% and the probability of a bit changed is really equal to 50% not near only, to lead to option 5.

3.5 Effective probability options 5
The option 5 is to add a selection optimizer before the selection itself. The optimizer is used to increase the number of choices in the key by 256 times by changing only one bit in the key. Then, it possible to use a selector from option 4. The 12 optimized keys coming out of the PQC block will then be selected by the same selector of option 4. The Figure 24 shows the selector with optimization.

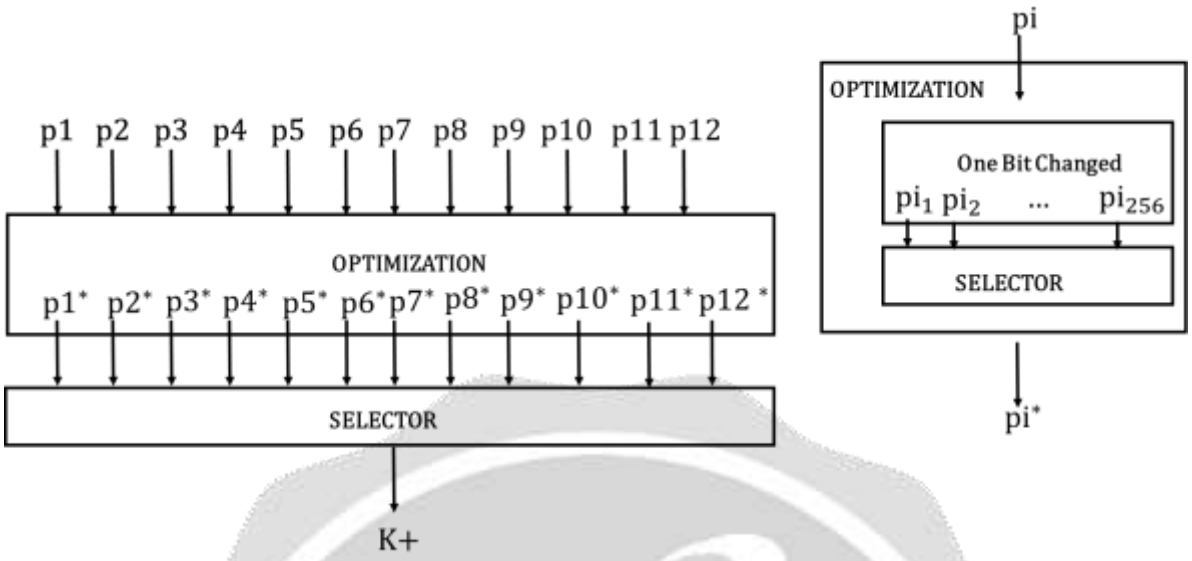

Fig -24 Optimization and Selector

Each key is received after the PQC block, 12 outputs qht_md45, qht_md45_xor,qht_md54, qht_md54_xor,qht_sha256,qht_sha256_xor,qat_md45,qat_md45_xor,qat_md54, qat_md54_xor, qat_sha256,qat_sha256_xor can also be simplified by a vector p formed by the elements $p_1 \dots p_{12}$. The optimizer will choose the best keys by changing one bit on each of its keys to give ${p_1}^* \dots {p_{12}}^*$. The selector will choose one of the optimized keys to have only one key K +

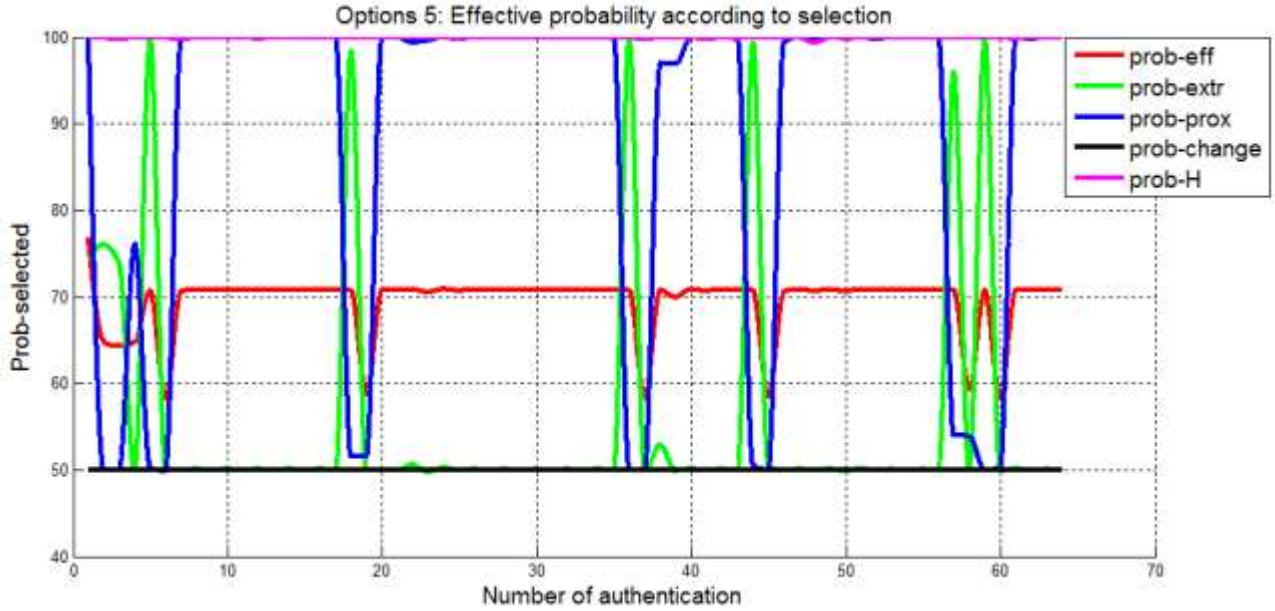

Fig -25 Effective probability using option 5

Interpretation:

Compared to the option 4, the optimizer was able to achieve up to about 50% and could achieve until 100% effective probability while having a probability of proximity greater than or equal 50%. Probability of the extremity is ranging from 50% to 100%. Most importantly, instead of having a bit probability changed close the 50%, for Figure 25, it is really equal of 50% which is the maximum value for this parameter. The probability of disorder is very close to 100%.

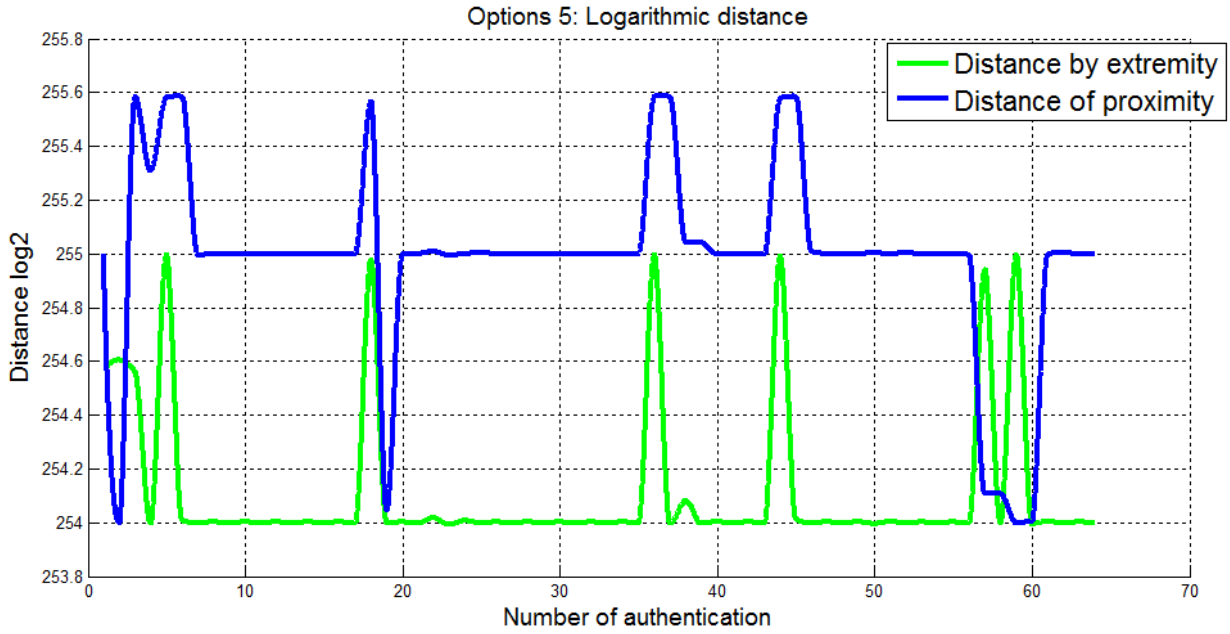

Fig -26 Distance logarithmic using option 5

Interpretation:

The proximity distance and the extremity distance will be greater than 2^{254} in Figure 26. The logarithmic distance is a very sensitive parameter. In the case of the option, the two minimum distances are $2^{253.5}$. Changing the logarithmic distance by 0.5, the optimizer was able to optimize about $2^{0.5}$ which is 1.414 times compared to $2^{253.5}$ of the option 4.

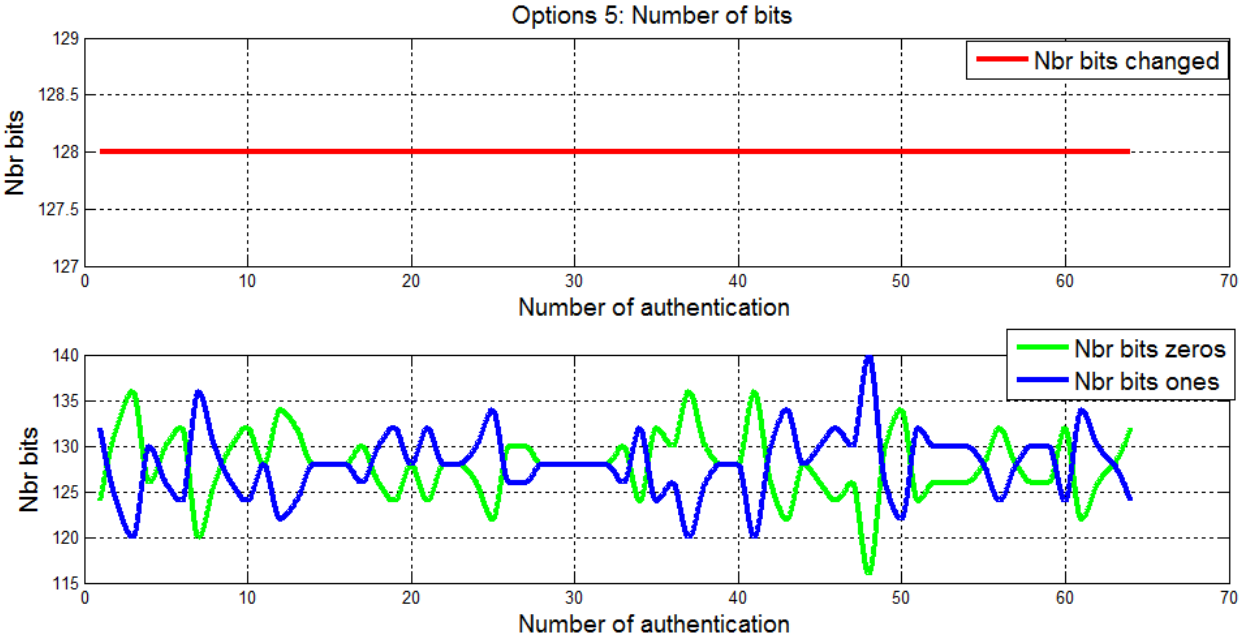

Fig -27 Effective probability using option 3

Interpretation:

According to Figure 25, the probability of disorder prob-H is about 100% both. The probability of bit change is equal to 128. It's the maximum value for this parameter because if the adversary knows that near 100% of key change , it's very easy to crack the key .Moreover, The Figure 27 shows that the number of bits changed is very close to varying between 254 and 255. The curve representing the number of bits zeros and bits ones are symmetrical to the number 128 bits so both are disordered. .

3.5 Effective probability option 5

Table -1 Summarize of all options

Options	**Ponderation**				Penalty	**Optimizer**
	Prob_prox	Prob_extr	Prob_change	entropie		
1	3	4	2	1	**Non**	**Non**
2	4	3	2	1	**Non**	**Non**
3	3		2	1	**Non**	**Non**
4	3		2	1	**Oui**	**Non**
5	3		2	1	**Oui**	**Oui**

The Table 5.01 shows that the first approach uses only priority weighting. The problem with this approach will be that the probability of extremity will be very optimal but the probability of proximity varies from better to worse. The second approach is very close to the first but the weighting will be reversed between the probability of extremity and the probability of proximity. The problem with this approach is that: the two probabilities of extremities and proximities are not optimal at the same time. In the third approach, these two probabilities will be studied at the same time. The problem with this approach is that some edge or proximity probability value will be much less than 10%. For this, the fourth approach uses the concept of penalties : if one of these two probabilities exceeds a certain value, the penalty allows not to have a very large value but assert stable about 70% of the two cases. The problem with this approach will be that the probability of a bit changed still stagnates in the 50%. The concept of optimizer changes a bit with each chosen key to increase the choice. Because of this, the probability disorder is very close to 100%. The probability of changed bit is really equal to 50%.

4. Conclusion

The overall architecture of the 5G network can be translated into a simplified architecture with access; the heart and the data. To authenticate to the 5G network, the AKA protocol uses mutual authentication while checking whether the operator is authentic and whether the user is authentic. The master key shared between the operator and the U-SIM card will be the basis of the protocol security. This key is static. The QPQ-CD algorithm that will be formed matrix expansion algorithms then the confusion algorithm using the representation of quantum images and will end with a post-quantum algorithm to have a 256-bit key. After each successful authentication, the master key dynamically changes while respecting certain criteria: far from the keys easy to guess such as the ends of the attack on brute force, far from the previous key, changed from bits number to maximum and very disorder. These criteria are named respectively probability of the extremity, proximity probability, changed bit probability, and probability in case of binary entropy. The last approach taken into account uses the weighting grading method combined with a penalty algorithm and optimized by increasing the choice by changing only one bit. The weighting is done in increasing order of the probability according to the binary entropy followed by changed bit and the average of the probability of the extremity and proximity. These two probabilities cannot be maximum at the same, so the selector penalizes the keys generated having its values higher than 70%. After optimization, the probability of proximity and

extremity will always be greater than 50% both, the probability according to the binary entropy will be of near 100% and the bit probability changed have the maximum value equal to 50%

4. Bibliographies

[1] Y. Wu, H. Huang, C. Wang, Y. Pan, *« 5G Enabled Internet of Thing »*, CRC Press, 2019

[2] V. C. M. Leung, H. Zhang, X. Hu, Q. Liu, Z. Liu, *« 5G for Future Wireless Networks »*, ICST Institute for Computer Sciences, 2019

[3] V. C. M. Leung, H. Zhang, X. Hu, Q. Liu, Z. Liu, *« 5G for Future Wireless Networks »*, ICST Institute for Computer Sciences, 2019

[4] W. Lei, Anthony C.K. Soong, L. Jianghua ,W. Yong , B. Classon, W. Xiao, D. Mazzarese, Z.Yang, T. Saboorian, *«5G System Design An End to End Perspective»*, Springer, 2020

[5] H. Fattah, *« 5G LTE Narrowband Internet of Things »*, CRC Press, 2019

[6] S. M. A. Kazmi, L. U. Khan, N. H. Tran, C. S. Hong, *« Network Slicing for 5G and Beyond Networks »*, Springer, 2019

[7] T. Q. Duong, X. Zhou, H. V. Poor, *« Ultra-dense Networks for 5G and beyond»*, the Institution of Engineering and Technology, John Wiley, 2019

[8] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, *« A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions»*, Journal of IEEE, Juil. 2019

[9] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, *« Novel 5G Authentication Protocol to Improve the Resistance against Active Attacks and Malicious Serving Networks»*, Journal of IEEE, Sept. 2019

[10] L. Song, Z. Xu, Z. Tian, J. Chen, R. Zhi, *« Research on 4G And 5G Authentication Signaling»*, International Journal Of Physics, 2019

[11] R. Khan, P. Kumar, D. N. K. Jayakody, M. Liyanage, *« A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements and Future Directions»*, Journal of IEEE, Juil. 2019

[12] R. Borgaonkar, L. Hirschi,, S. Park, and A. Shaik, *« New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols»*, Journal of Sciendo, 2019

[13] H. Liu, B. Zhao, L. Huang, *«Quantum Image Encryption Scheme Using Arnold Transform and S-box Scrambling»*, Journal of MDPI, Mar. 2019

[14] S. Heidari, M. Houshmand, N. T. Mashadi, *«A dual quantum image scrambling method»*, Quantum Information Processing, Jan. 2019

[15] M. Heigly, M. Schrammy, D. Fiala, *«A Lightweight Quantum-Safe Security Concept for Wireless Sensor Network Communication»*, Journal of IEEE 2019

[16] M S. Shoba, *«A Survey on Post Quantum Digital Signature Schemes for Blockchain»*, International Journal of Computer Science and Mobile Computing, June 2019