ΦΛΩΡΙΑΣ ΠΑΠΑΔΟΠΟΥΛΟΣ

Η ΠΑΡΟΥΣΙΑΣΗ ΘΑ ΞΕΚΙΝΗΣΕΙ ΣΥΝΤΟΜΑ

ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΤΗ ΜΕΤΑΚΒΑΝΤΙΚΗ ΕΠΟΧΗ

ΦΛΩΡΙΑΣ ΠΑΠΑΔΟΠΟΥΛΟΣ

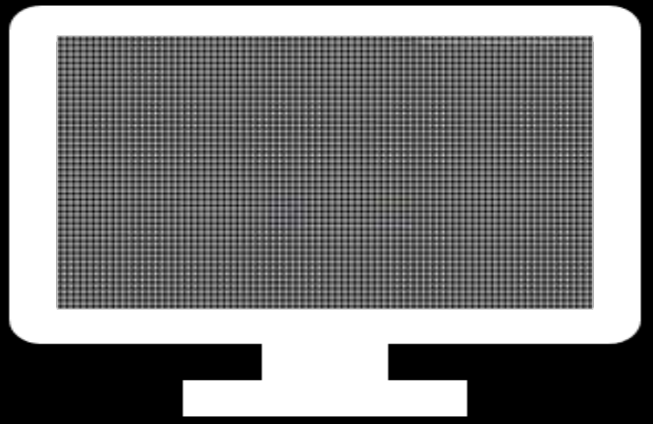
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΔΗΜΗΤΡΙΟΣ ΠΟΥΛΑΚΗΣ

Θεσσαλονίκη, 2 Μαρτίου 2022

Θεωρητικό Υπόβαθρο

Κρυπτογραφία

Κβαντικοί υπολογιστές & Κρυπτογραφία



Κύριο Μέρος

Κρυπτογραφία Συν. Κατακερματισμού

Κρυπτογραφία Κωδίκων

Επίλογος

Μια ματιά στο μέλλον

ΚΡΥΠΤΟΓΡΑΦΙΑ

Βασικό αντικείμενο Κρυπτογραφίας

Η ασφάλεια των πληροφοριών και γενικώς η εξασφάλιση της επικοινωνίας μέσω μη ασφαλών διαύλων.

- Ιδιότητες της επικοινωνίας

✓**Εμπιστευτικότητα**

Ποιος έχει πρόσβαση στην πληροφορία?

✓**Ακεραιότητα**

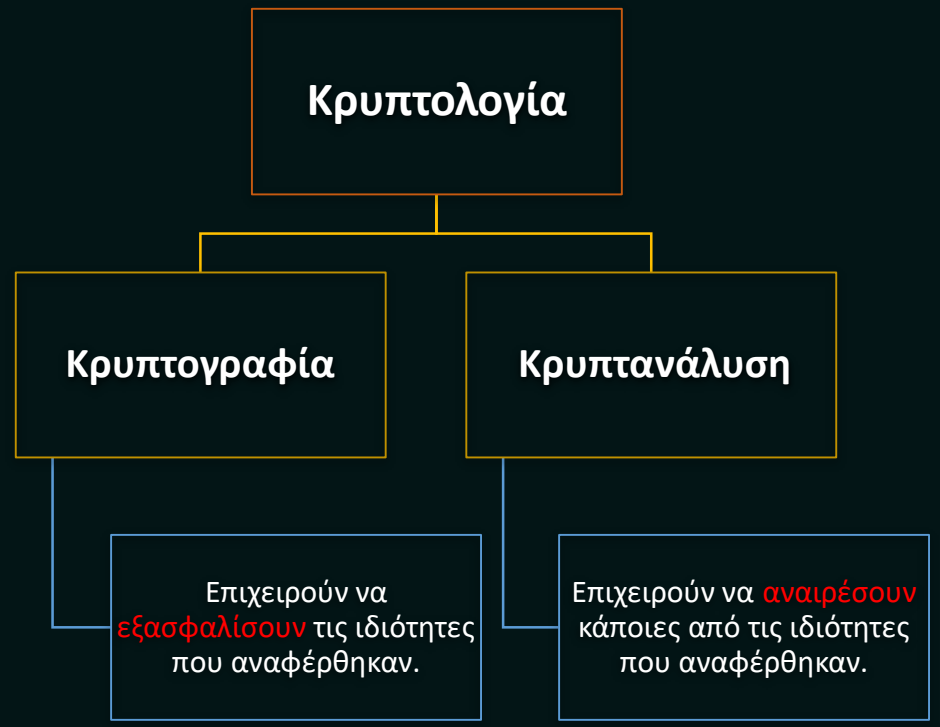
Ποιος μπορεί να αλλοιώσει την πληροφορία?

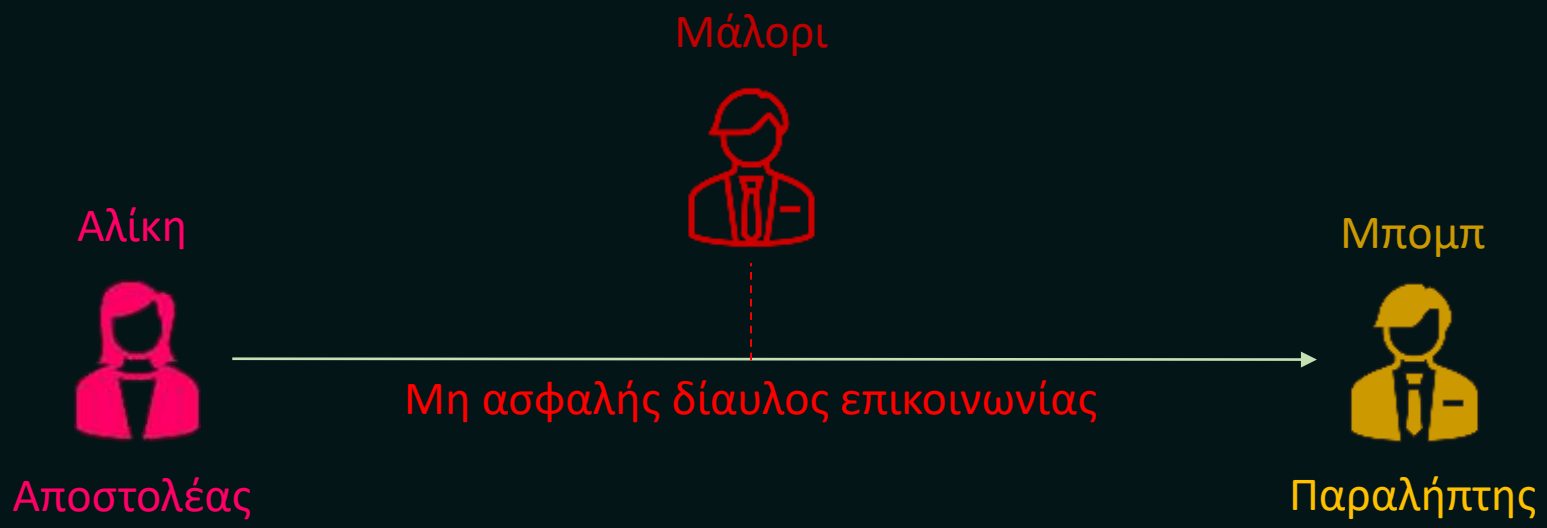
✓**Αυθεντικότητα**

Είμαστε σίγουροι για τις ταυτότητες αυτών που επικοινωνούν?

✓**Αδυναμία αποκήρυξης**

Μπορεί να γίνει άρνηση της αυθεντικότητας της μετάδοσης?





- Πως μπορεί η Αλίκη να στείλει ένα μήνυμα στον Μπομπ με ασφάλεια;

Κρυπτογράφηση

Διαδικασία μετασχηματισμού πληροφοριών σε μορφή κατανοητή μόνο από εξουσιοδοτημένο χρήστη.

Κρυπτογραφικός αλγόριθμος

Μέθοδος που μετασχηματίζει δεδομένα για τους σκοπούς της κρυπτογράφησης.

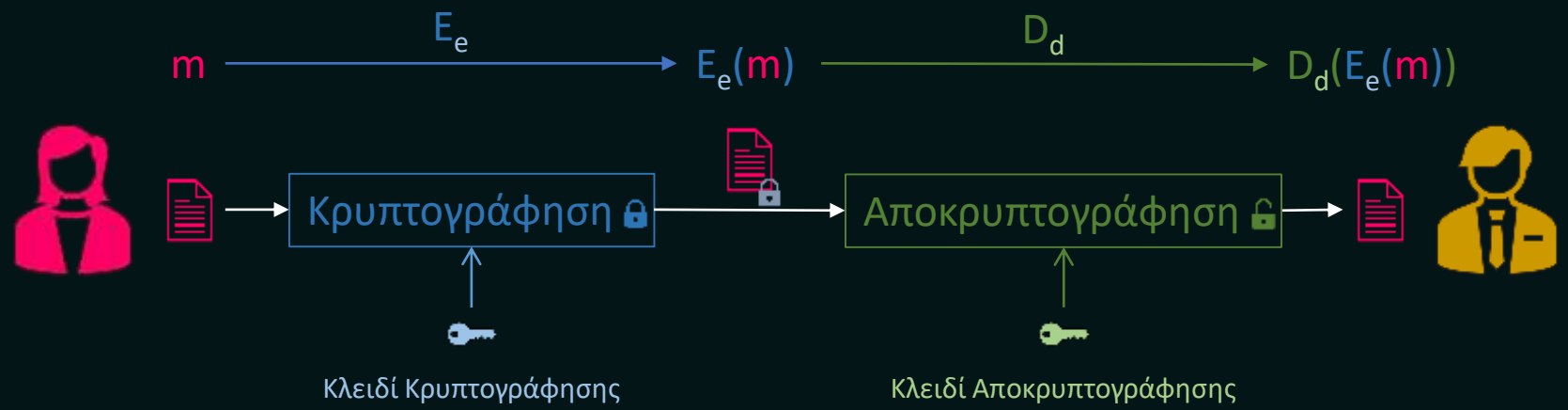
- Κατά κανόνα είναι μία πολύπλοκη μαθηματική συνάρτηση.

Κρυπτοσύστημα

Καλούμε κρυπτοσύστημα ή κρυπτογραφικό σχήμα μια πεντάδα (P, C,K, E,D) , όπου :

- P : ο χώρος των απλών κειμένων
- C : ο χώρος των κρυπτογραφημένων κειμένων
- K : ο χώρος των κλειδιών
- $E = \{E_k : P \rightarrow C \mid k \in K\}$: συναρτήσεις κρυπτογράφησης
- $D = \{D_k : C \rightarrow P \mid k \in K\}$: συναρτήσεις αποκρυπτογράφησης

❖ Ισχύει ότι : $\forall e \in K, \exists d \in K$ τέτοιο ώστε : $D_d(E_e(m)) = m, \forall m \in P$



Κρυπτογραφία - Ιστορική Αναδρομή

Κρυπτεία Σκυτάλη

Κρυπτοσύστημα Viginère

Σύγχρονη Κρυπτογραφία

500 π.Χ.

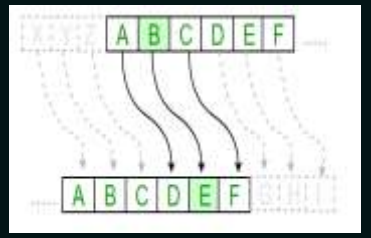
50 π.Χ.

1500 μ.Χ.

1900 μ.Χ.

Παρόν

Όχι τόσο μακρινό μέλλον



Κώδικας του Καίσαρα

Μηχανή Enigma

Κρυπτογραφία στη Μετακβαντική Εποχή

ΑΛΓΟΡΙΘΜΟΙ

Αλγόριθμος

Μια πεπερασμένη, συγκεκριμένη, αποτελεσματική διαδικασία, με μια είσοδο και κάποια έξοδο που χρησιμοποιείται για τον υπολογισμό μιας ποσότητας.

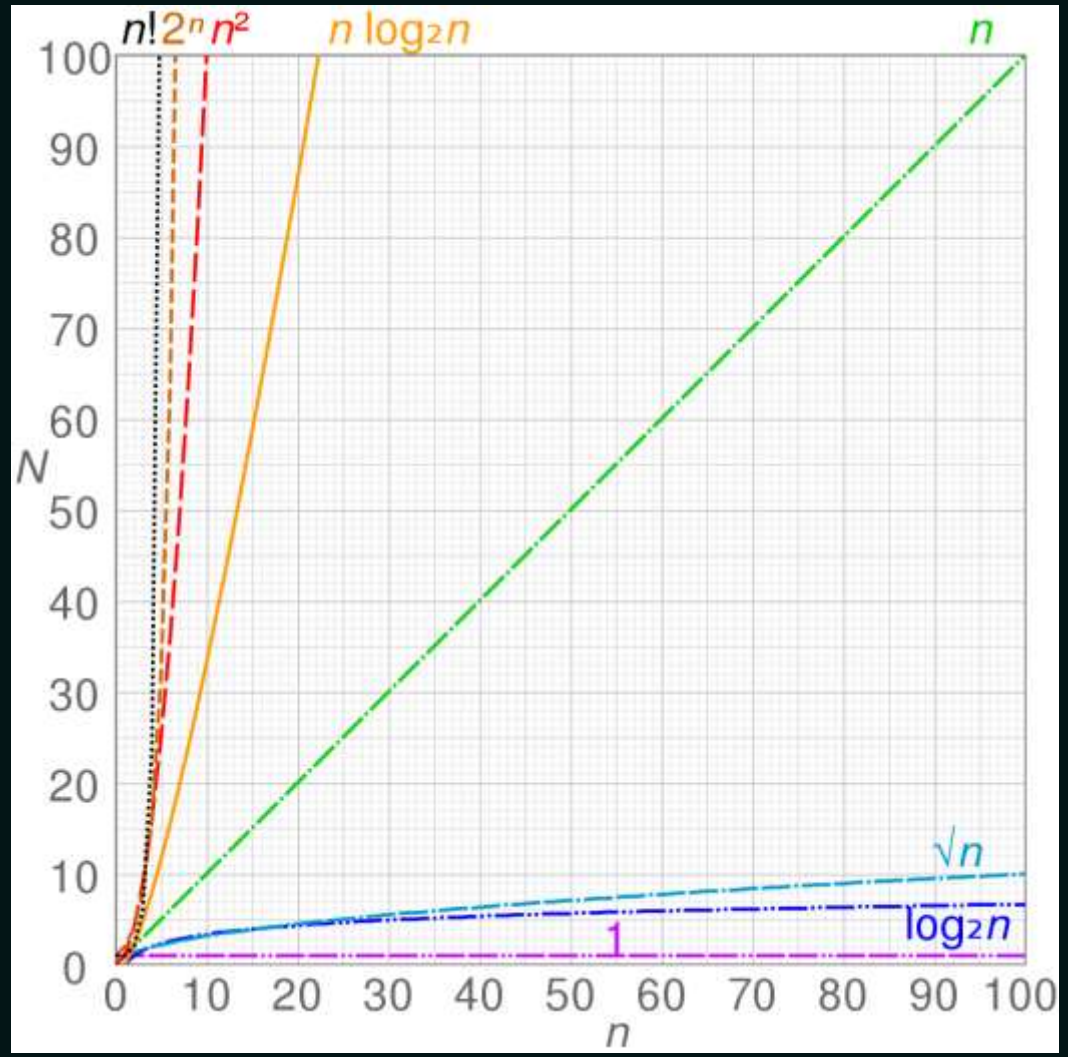
Χρονική πολυπλοκότητα - Χρόνος εκτέλεσης

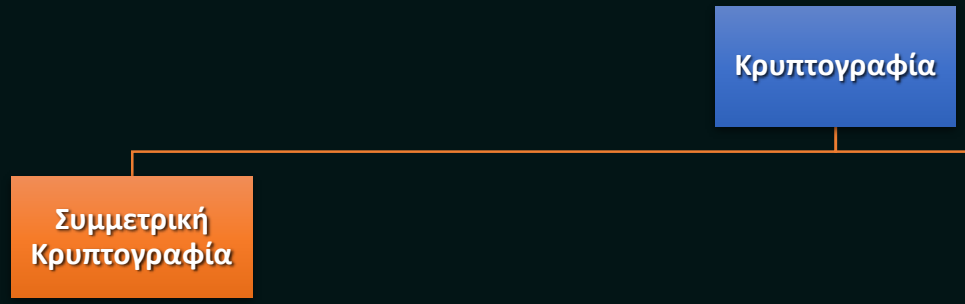
Ο αριθμός των στοιχειωδών λειτουργιών που εκτελούνται από έναν αλγόριθμο σαν συνάρτηση του μεγέθους της εισόδου.

Πολυωνυμικός χρόνος

Εκθετικός χρόνος

- Ένας αλγόριθμος είναι **αποδοτικός** αν έχει πολυωνυμικό χρόνο εκτέλεσης.





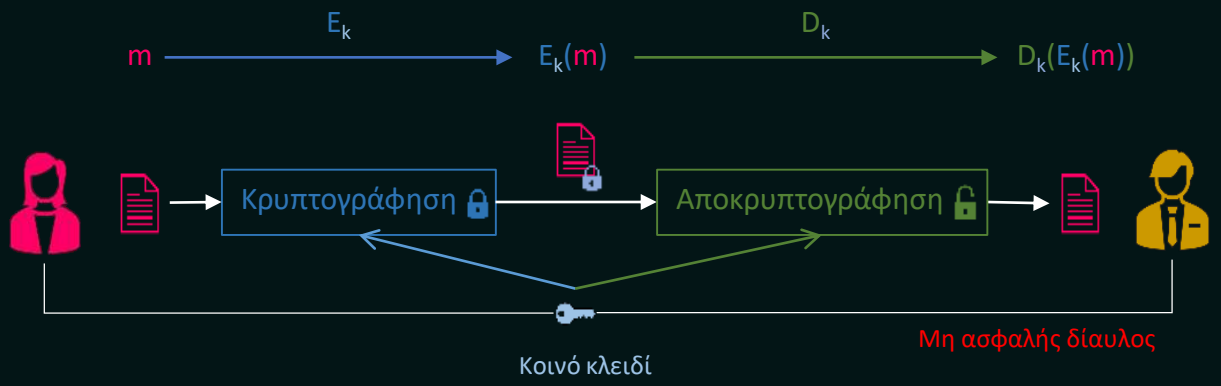
Συμμετρικό κρυπτοσύστημα

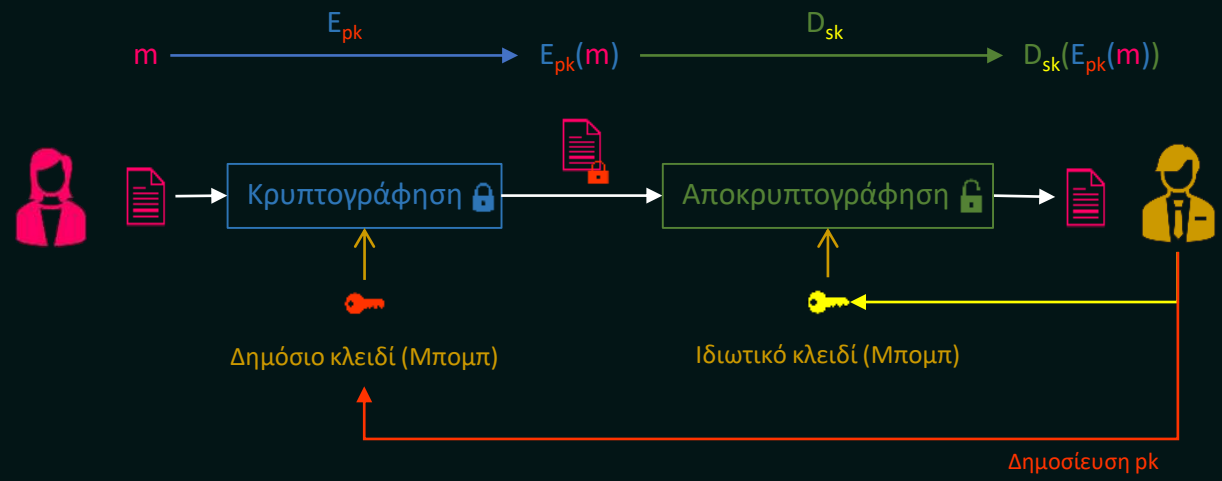
Είδος κρυπτοσυστήματος στο οποίο χρησιμοποιείται ένα κοινό κλειδί για τις διεργασίες τις κρυπτογράφησης και της αποκρυπτογράφησης.

Ασύμμετρο κρυπτοσύστημα - Κρυπτοσύστημα Δημοσίου Κλειδιού

Είδος κρυπτοσυστήματος στο οποίο χρησιμοποιούνται δύο διαφορετικά κλειδιά για τις διεργασίες τις κρυπτογράφησης και της αποκρυπτογράφησης.

- Συγκεκριμένα, κάθε χρήστης διαθέτει ένα **ιδιωτικό κλειδί** και ένα **δημόσιο κλειδί** τα οποία, αν και διαφορετικά, έχουν μαθηματική σχέση μεταξύ τους.





ΠΟΥ ΒΑΣΙΖΕΤΑΙ Η ΑΣΦΑΛΕΙΑ ΤΩΝ ΚΡΥΠΤΟΣΥΣΤΗΜΑΤΩΝ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ?

- Πρέπει να είναι υπολογιστικά αδύνατο να βρεθεί το ιδιωτικό κλειδί από το δημόσιο κλειδί.
  Δηλαδή, καθώς το ιδιωτικό και το μυστικό κλειδί συνδέονται με μια μαθηματική σχέση,
  πρέπει αυτή η σχέση να είναι δύσκολο να αντιστραφεί.

Κρυπτοσύστημα Δημοσίου Κλειδιού RSA

Γίνεται επιλογή $p \neq q$ πρώτων και υπολογίζουμε το $n=p \cdot q$.

Επιλέγεται ακόμη ένας ακέραιος e που εξαρτάται από το n και υπολογίζεται εύκολα μέσω του e ένας αριθμός d.

- Δημόσιο Κλειδί pk : Το ζεύγος (n,e)
- Ιδιωτικό Κλειδί sk : Το d

Είναι υπολογιστικά δύσκολο έχοντας γνώση του δημοσίου κλειδιού (n,e) να βρεθεί το d, για μεγάλες τιμές των p, q.

Πρόβλημα Παραγοντοποίησης Μεγάλων Ακεραίων
Έστω ότι έχουμε έναν ακέραιο $n=p \cdot q$, με q και p δύο αρκετά μεγάλους πρώτους. Γνωρίζοντας μόνο το n, να βρεθούν τα p και q.

→ Δεν έχει βρεθεί κλασσικός αλγόριθμος παραγοντοποίησης πολυωνυμικού χρόνου.

- Πρόταση: Ο υπολογισμός του d είναι ισοδύναμος με τον υπολογισμό των p και q.

Ψηφιακές Υπογραφές

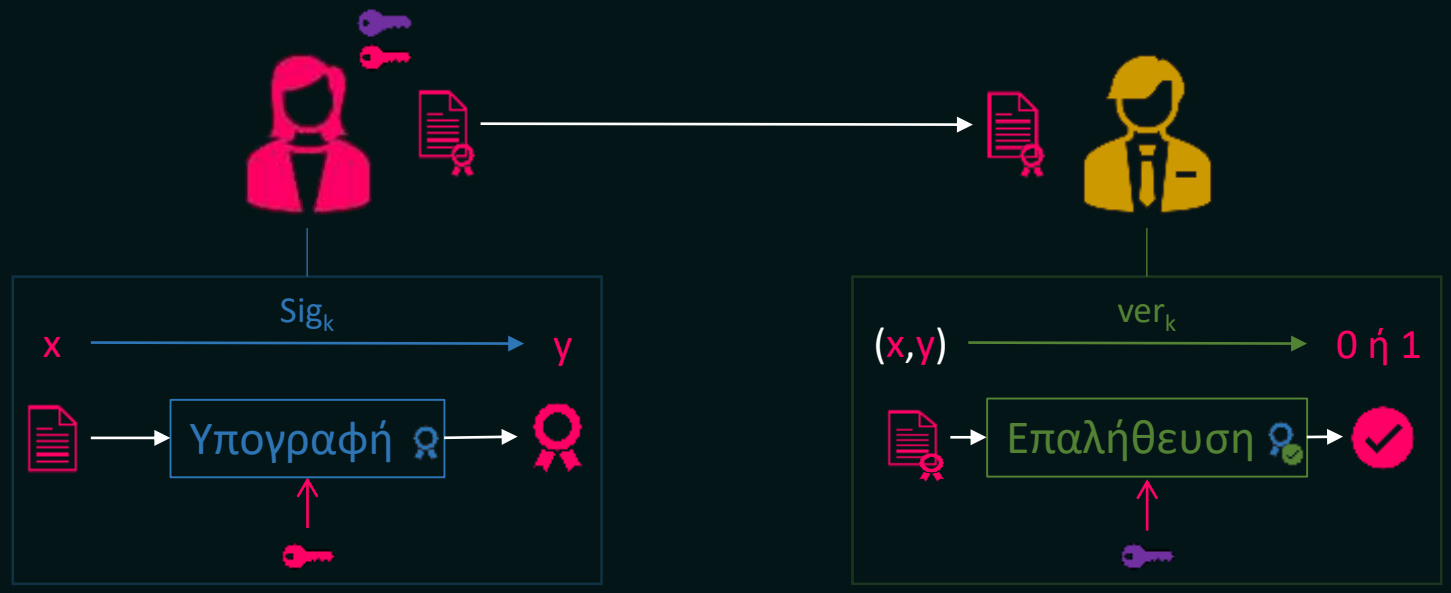
Καλούμε σχήμα ψηφιακής υπογραφής μια πεντάδα (P,Y,K,S,V), όπου :

- P : ο χώρος των μηνυμάτων
- Y : ο χώρος των υπογραφών
- K : ο χώρος των κλειδιών
- $S = \{sig_k : P \rightarrow Y \mid k \in K\}$: συναρτήσεις υπογραφής
- $V = \{ver_{k'} : P \times Y \rightarrow \{0, 1\} \mid k \in K\}$: συναρτήσεις επαλήθευσης

❖ Ισχύει ότι $\forall k,k' \in K$ και $(x, y) \in P \times Y$, έχουμε: $ver_{k'}(x, y) = \begin{cases} 1, \alpha\nu\ sig_k(x) = y \\ 0, \alpha\nu\ sig_k(x) \neq y \end{cases}$

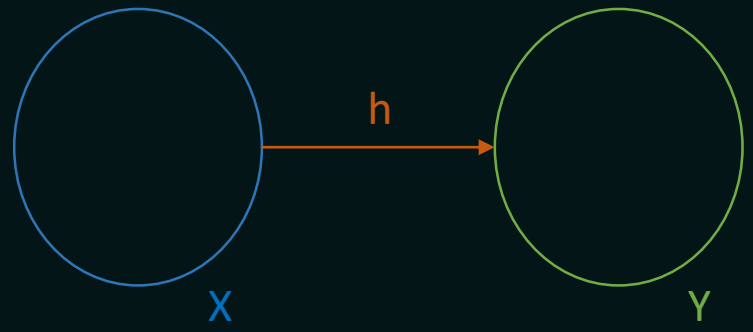
Θα πρέπει να είναι υπολογιστικά εύκολο να παραχθεί μια υπογραφή, όπως και να επαληθευτεί η γνησιότητα της.

Θα πρέπει να είναι υπολογιστικά αδύνατο για έναν αντίπαλο να πλαστογραφήσει την υπογραφή ενός μηνύματος.



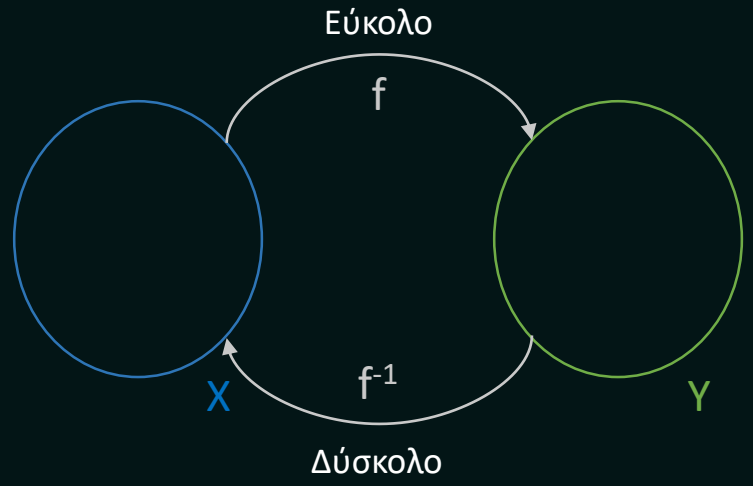
Συναρτήσεις Κατακερματισμού – Ασφαλείς υπογραφές

Καλούμε **συνάρτηση κατακερματισμού** κάθε συνάρτηση h : X → Y τέτοια ώστε το σύνολο Y να είναι πεπερασμένο και να ισχύει |X| > |Y|.

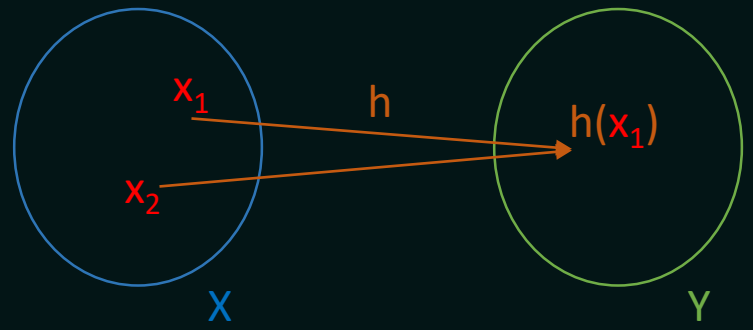


- **Συνάρτηση μιας κατεύθυνσης**

Κάθε συνάρτηση f : A → B για την οποία υπάρχει αλγόριθμος πολυωνυμικού χρόνου ο οποίος να υπολογίζει την τιμή f(x) για κάθε x ∈ A αλλά η εύρεση ενός x ∈ A από δοθέν f(x) είναι υπολογιστικά ανέφικτη.

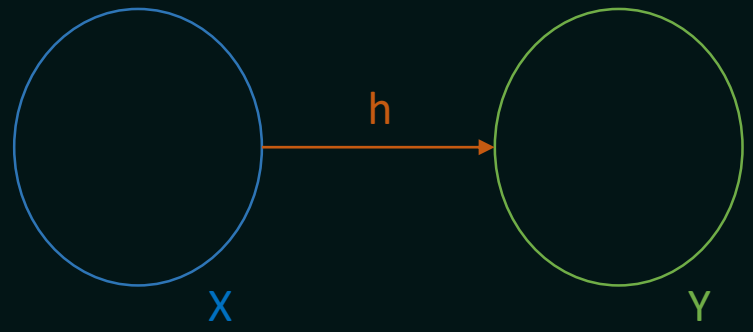


- Έστω h : X → Y μια συνάρτηση κατακερματισμού. Ένα ζεύγος (x1,x2) καλείται **σύμπτωση** της h αν ισχύει $x_1 \neq x_2$ με $h(x_1) = h(x_2)$.
  - Η συνάρτηση h θα καλείται **ελεύθερη σύμπτωσης** είναι υπολογιστικά ανέφικτο να βρεθεί μια σύμπτωση της.

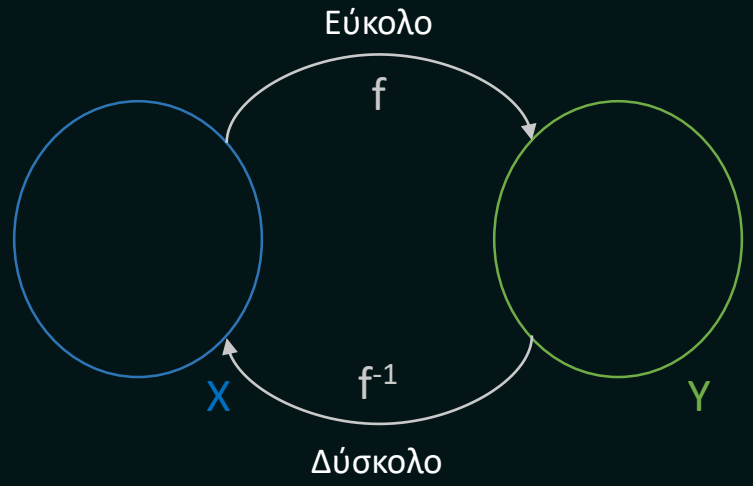


Συναρτήσεις Κατακερματισμού – Ασφαλείς υπογραφές

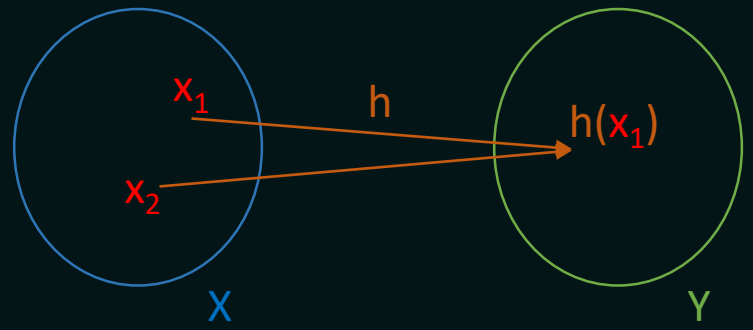
Καλούμε **συνάρτηση κατακερματισμού** κάθε συνάρτηση h : X → Y τέτοια ώστε το σύνολο Y να είναι πεπερασμένο και να ισχύει |X| > |Y|.



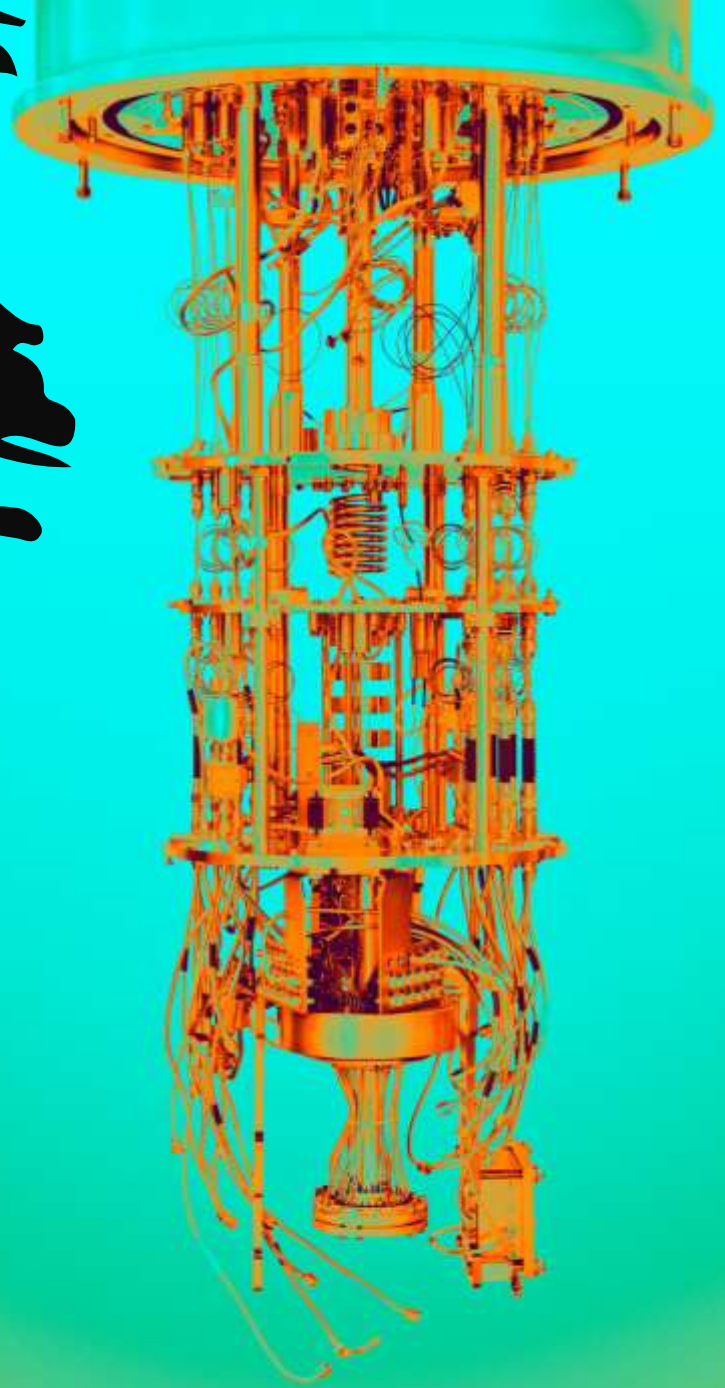
- Καλούμε **συνάρτηση μιας κατεύθυνσης** κάθε συνάρτηση f : A → B για την οποία υπάρχει αλγόριθμος πολυωνυμικού χρόνου ο οποίος να υπολογίζει την τιμή f(x) για κάθε x ∈ A αλλά η εύρεση ενός x ∈ A από δοθέν f(x) είναι υπολογιστικά ανέφικτη.



- Έστω h : X → Y μια συνάρτηση κατακερματισμού. Ένα ζεύγος (x1,x2) καλείται **σύμπτωση** της h αν ισχύει $x_1 \neq x_2$ με $h(x_1) = h(x_2)$.
  - Η συνάρτηση h θα καλείται **ελεύθερη σύμπτωσης** είναι υπολογιστικά ανέφικτο να βρεθεί μια σύμπτωση της.



ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΚΡΥΠΤΟΓΡΑΦΙΑ



Πηγή: Richard Feynman Messenger Lectures at Cornell The Character of Physical Law Part 6 Probability and Uncertainty (YouTube)

Richard Phillips Feynman
Αμερικανός θεωρητικός φυσικός διεθνούς φήμης.

"Nobody understands Quantum Mechanics"

- Τι είναι η Κβαντομηχανική ;

Κβαντομηχανική
Θεωρία της Φυσικής που μελετάει τη συμπεριφορά της ύλης και της ακτινοβολίας σε ατομική κλίμακα.

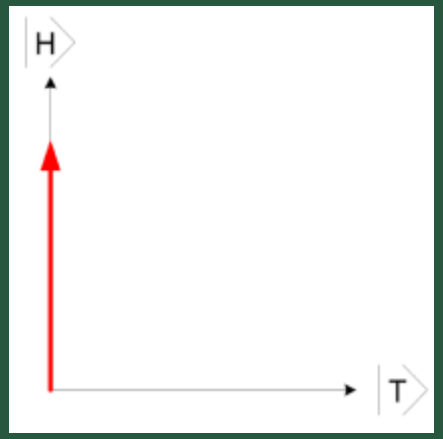
- Τι είναι η Κβαντικός υπολογιστής ;

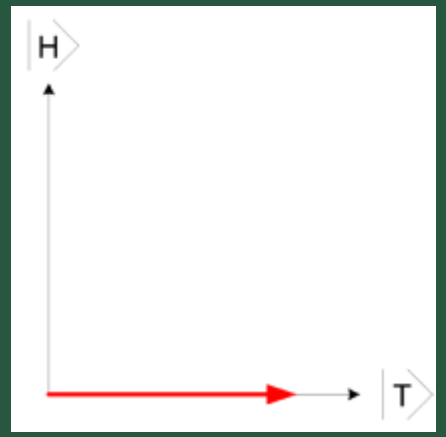
Κβαντικός υπολογιστής
Υπολογιστική συσκευή που εκμεταλλεύεται χαρακτηριστικές ιδιότητες της κβαντομηχανικής, όπως η κβαντική υπέρθεση και η κβαντική διεμπλοκή, για την επεξεργασία δεδομένων και την εκτέλεση υπολογισμών.

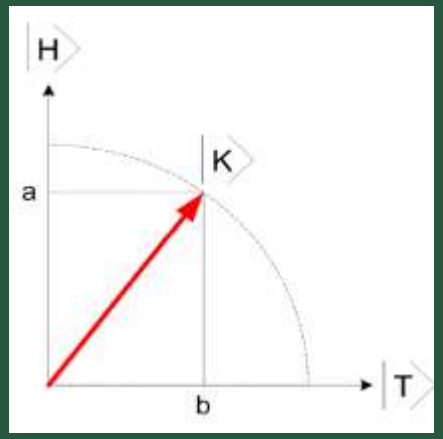
Κβαντική κατάσταση
Αφηρημένη έννοια που χρησιμοποιείται για την περιγραφή της κατάστασης στην οποία βρίσκεται ένα κβαντικό αντικείμενο.

ΚΒΑΝΤΙΚΗ ΥΠΕΡΘΕΣΗ









Κβαντική υπέρθεση

Θεμελιώδης αρχή της κβαντικής μηχανικής σύμφωνα με την οποία :

- Κάθε δύο (ή περισσότερες) κβαντικές καταστάσεις μπορούν να προστεθούν μαζί («επάλληλα») και το αποτέλεσμα θα είναι μια άλλη έγκυρη κβαντική κατάσταση.
- Αντίστροφα, κάθε κβαντική κατάσταση μπορεί να παρασταθεί ως ένα άθροισμα δύο ή περισσότερων άλλων διακριτών καταστάσεων.

Η πράξη της παρατήρησης ενός συστήματος το αλλάζει και ο παρατηρητής είναι κατά κάποιο τρόπο μέρος του πειράματος.

ΔΙΕΜΠΛΟΚΗ - ENTANGLEMENT

Κβαντική διεμπλοκή

Φαινόμενο κατά το οποίο δύο σωματίδια ή ομάδες σωματιδίων δημιουργούνται μαζί ή αλληλοεπιδρούν με τέτοιο τρόπο, ώστε η κβαντική κατάσταση καθενός σωματιδίου δεν μπορεί να περιγραφεί ανεξάρτητα απ' την κατάσταση των υπολοίπων, ασχέτως της απόστασης του ενός από το άλλο.

Πηγή: Quantum Computing Expert Explains One Concept in 5 Levels of Difficulty | WIRED (YouTube)

Talia Gershon
Director, Hybrid Cloud Infrastructure Research at IBM

ΠΩΣ ΛΕΙΤΟΥΡΓΕΙ ΕΝΑΣ ΚΒΑΝΤΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ ?

Το **qubit** είναι ένα κβαντικό σύστημα δύο καταστάσεων, δηλαδή είναι ένα σύστημα που όχι μόνο περιλαμβάνει τις δύο αυτές καταστάσεις, αλλά και όλες τις ενδιάμεσες μέχρι να μετρηθεί. Μόλις μετρηθεί, το qubit καταρρέει σε μία από τις δυνατές καταστάσεις με ορισμένη πιθανότητα.

$$|\psi\rangle = a|0\rangle + b|1\rangle \text{ , με } a, b \in \mathbb{C}^2 \text{ τ.ω. } |a|^2 + |b|^2 = 1$$

Ισχύς των κβαντικών υπολογιστών

Κβαντικός Υπολογιστής

Ένα σύνολο qubits θα αποτελεί έναν **κβαντικό καταχωρητή**.

Δύο qubits μπορούν να αναπαραστήσουν οποιαδήποτε υπέρθεση τεσσάρων δυνατών καταστάσεων που ορίζονται να είναι της μορφής $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.

Κλασσικός Υπολογιστής

Ένα σύνολο bits αποτελεί έναν **καταχωρητή**

Όταν έχουμε δύο bit και παραπάνω, τα γράφουμε στη μορφή 00, 01,κλπ.

$[1\ 0\ 0\ 0]$

$[0\ 1\ 0\ 0]$

$[0\ 0\ 1\ 0]$

$[0\ 0\ 0\ 1]$

Qubits	Bits
1	2
2	$2\times2=2^2$
3	$2\times2\times2=2^3$
⋮	⋮
100	2^{100} → 1,267,650,600,228,229,401,496,703,205,376 bits

31 ψηφία

Μετα-κρυπτογραφία

Κβαντικοί Αλγόριθμοι

Περί Κβαντικών Υπολογιστών

Περί Κβαντομηχανικής

Κβαντικός αλγόριθμος
Ένας αλγόριθμος ο οποίος εκτελείται σε ένα ρεαλιστικό μοντέλο κβαντικού υπολογισμού. Συνήθως ο όρος χρησιμοποιείται για αλγορίθμους που χρησιμοποιούν κάποια κβαντική ιδιότητα και μπορούν να εκτελεστούν μόνο σε κβαντικούς υπολογιστές.

Κβαντικοί Αλγόριθμοι & Κρυπτογραφία

- Αλγόριθμος του Grover
- Αλγόριθμος του Shor

Κβαντικός Αλγόριθμος του Grover

Αλγόριθμος του Grover (Love Grover, 1996)
Αλγόριθμος ο οποίος καταφέρνει να επιταχύνει (τετραγωνικά) την διαδικασία διερεύνησης μιας μη δομημένης βάσης δεδομένων.

Περιέχει πληροφορίες οι οποίες:

- είτε δε συμμορφώνονται με ένα προκαθορισμένο μοντέλο δεδομένων
- είτε δεν είναι οργανωμένες στη βάση δεδομένων με έναν προκαθορισμένο τρόπο.

Πόσες προσπάθειες χρειάζονται για την εύρεση ενός στοιχείου σε μια μη δομημένη βάση N δεδομένων ?

Κλασσικός Υπολογιστής	Κατά μέσο όρο N/2 (τυχαία επιλογή)
Κβαντικός Υπολογιστής	Περίπου √N (αλγόριθμος του Grover)

Κρυπτανάλυση & Αλγόριθμος του Grover

Ο κβαντικός αλγόριθμος του Grover μπορεί να επιταχύνει τις παρακάτω διαδικασίες:

- Η εύρεση μιας προεικόνας για μια τιμή s μιας συνάρτησης f, δηλαδή η εύρεση x τ.ω. f(x)=s.

- Η εύρεση συμπτώσεων σε μια συνάρτηση f, δηλαδή η εύρεση x, y τ.ω. f(x) = f(y).

Κβαντικός Αλγόριθμος του Shor

Ο **αλγόριθμος του Shor** καταφέρνει να λύσει σε πολυωνυμικό χρόνο το εξής πρόβλημα :
Δοθέντος $n \in \mathbb{N}$, *να βρεθεί η περίοδος της συνάρτησης* $f_{n,a}(x) = a \cdot x \bmod n$, $a \in \mathbb{N}$ με μκδ(a,n) = 1.

Προβλήματος Παραγοντοποίησης Μεγάλων Ακεραίων

- Κρυπτοσύστημα Δημοσίου Κλειδιού RSA
- Σχήμα Ψηφιακής Υπογραφής RSA
- Κρυπτοσύστημα Δημοσίου Κλειδιού Rabin
- Σχήμα Ψηφιακής Υπογραφής Rabin

Πρόβλημα Διακριτού Λογαρίθμου

- Πρωτόκολλο Ανταλλαγής Κλειδιού Diffie-Hellman
- Κρυπτοσύστημα Δημοσίου Κλειδιού ElGamal
- Αλγόριθμος Ψηφιακής Υπογραφής (DSA)
- Αλγόριθμος Ψηφιακής Υπογραφής Ελλειπτικών Καμπυλών (ECDSA)

Ταχύτητα αλγορίθμου του Shor

In 2001, Shor's algorithm was demonstrated by a group at IBM, who factored 15 into 3 × 5, using an NMR implementation of a quantum computer with 7 qubits

with a classical computer

# bits	1024	2048	4096
factoring in 2006	10^5 years	$5x10^{15}$ years	$3x10^{29}$ years
factoring in 2024	38 years	10^{12} years	$7x10^{25}$ years
factoring in 2042	3 days	$3x10^8$ years	$2x10^{22}$ years

with potential quantum computer

# bits	1024	2048	4096
# qubits	5124	10244	20484
# gates	$3x10^9$	$2X10^{11}$	$X10^{12}$
factoring time	4.5 min	36 min	4.8 hours

Πηγή: R.J. Hughes and D.F.V. James. \Prospects for Quantum Computation with Trapped Ions". In: *Fortschritte der Physik* 46.6-8, 759-769 (Nov. 1998)

ΟΙ ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΘΑ ΣΠΑΣΟΥΝ ΤΟ ΙΝΤΕΡΝΕΤ

nature

Explore content · About the journal · Publish with us · Subscribe

nature › news feature › article

NEWS FEATURE | 08 February 2022

The race to save the Internet from quantum hackers

The quantum computer revolution could break encryption – [redacted]

MIT Technology Review

Featured · Topics · Newsletters · Events · Podcasts · Sign in · Subscribe

COMPUTING

How a quantum computer could break 2048-bit RSA encryption in 8 hours

A new study shows that quantum technology will catch up with today's encryption standards much sooner than expected. That should worry anybody who needs to store data securely for 25 years or so.

By Emerging Technology from the arXiv — May 30, 2019

c|net TECH

Featured · Mobile · Computing · Gaming · Home Entertainment · Services & Software

Quantum computers could crack today's encrypted messages. That's a problem

There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."
– Dr. Michele Mosca (2015)

CRYPTOCURRENCY

Quantum hackers can bring down Bitcoin: expert

Chinese university professor tells Asia Times' webinar how over $3 trillion in cryptocurrency assets are at unseen risk

ber 2020

Quantum-computing pioneer warns of complacency over Internet security

Nature talks to Peter Shor 25 years after he showed how to make quantum computations feasible – and how they could endanger our data.

ΟΙ ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΔΕΝ ΘΑ ΣΠΑΣΟΥΝ ΤΟ ΙΝΤΕΡΝΕΤ

Κβαντική Κρυπτογραφία
Επιστήμη που χρησιμοποιεί τις ιδιότητες της κβαντομηχανικής σε κρυπτογραφικές εφαρμογές.

- **Κβαντική διαχείριση κλειδιών**
- Κβαντικές ψηφιακές υπογραφές
- Quantum commitment
- Oblivious transfer
- Quantum fingerprinting

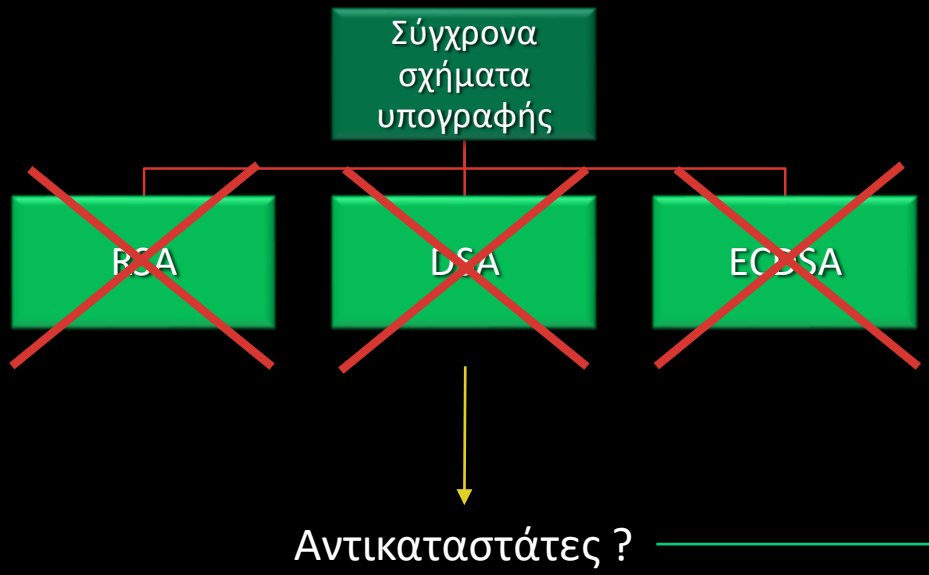
Μετακβαντική Κρυπτογραφία
Οικογένεια κρυπτογραφικών αλγορίθμων οι οποίοι (εικάζεται ότι) εξασφαλίζουν ένα υψηλό επίπεδο ασφάλειας, ακόμη και ενάντια σε έναν επιτιθέμενο που διαθέτει έναν κβαντικό υπολογιστή.

- **Κρυπτογραφία Συναρτήσεων Κατακερματισμού**
- **Κρυπτογραφία Κωδίκων**
- Κρυπτογραφία Δικτυωτών
- Κρυπτογραφία Πολυμετάβλητων Τετραγωνικών Εξισώσεων

Μετα-κρυπτογραφία
Κβαντικοί Αλγόριθμοι
Περί Κβαντικών Υπολογιστών
Περί Κβαντομηχανικής

ΚΡΥΠΤΟΓΡΑΦΙΑ ΣΥΝΑΡΤΗΣΕΩΝ ΚΑΤΑΚΕΡΜΑΤΙΣΜΟΥ

Σχήματα Ψηφιακών Υπογραφών



Σχήματα Υπογραφής Συναρτήσεων Κατακερματισμού (Hash-based)

Σχήματα Υπογραφής Μιας Φοράς (OTS)

Συνάρτηση μιας κατεύθυνσης

Οι συναρτήσεις μιας κατεύθυνσης είναι ικανές και αναγκαίες για την ύπαρξη ασφαλών ψηφιακών υπογραφών. (J. Rompel, 1990)

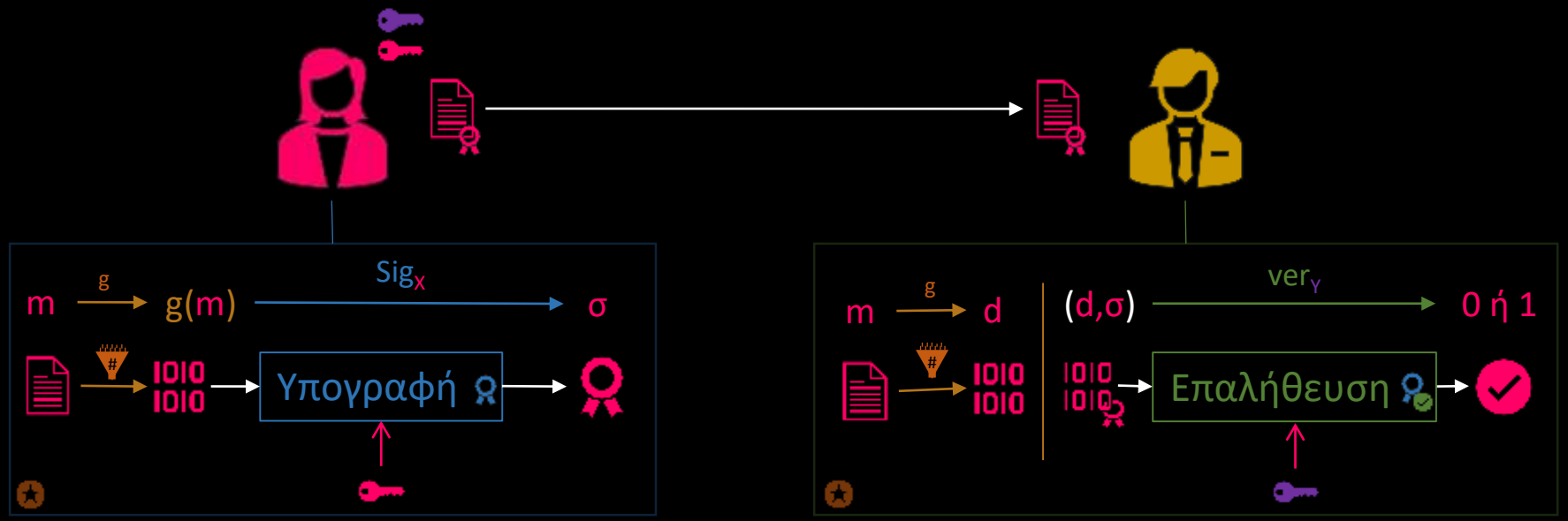
Συνάρτηση Κατακερματισμού

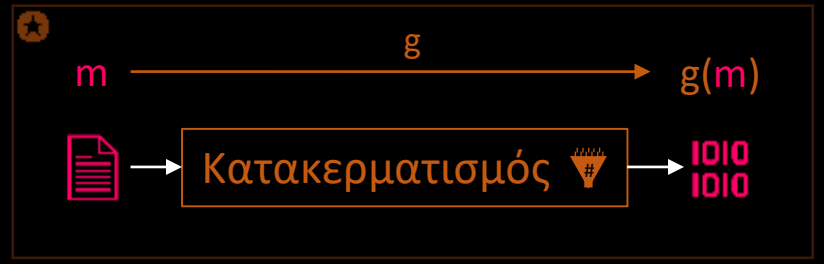
Πρέπει να είναι ελεύθερη σύμπτωσης.

- Η ασφάλεια ενός OTS βασίζεται μόνο στην ιδιότητα «ελεύθερης σύμπτωσης».
- Κάθε ζεύγος κλειδιών που παράγεται μπορεί να χρησιμοποιηθεί μόνο μια φορά.

Σχήμα Υπογραφής Merkle – Δέντρο Merkle (MSS)

Σχήμα Υπογραφής Μιας Φοράς Lamport-Diffie (L-D OTS)



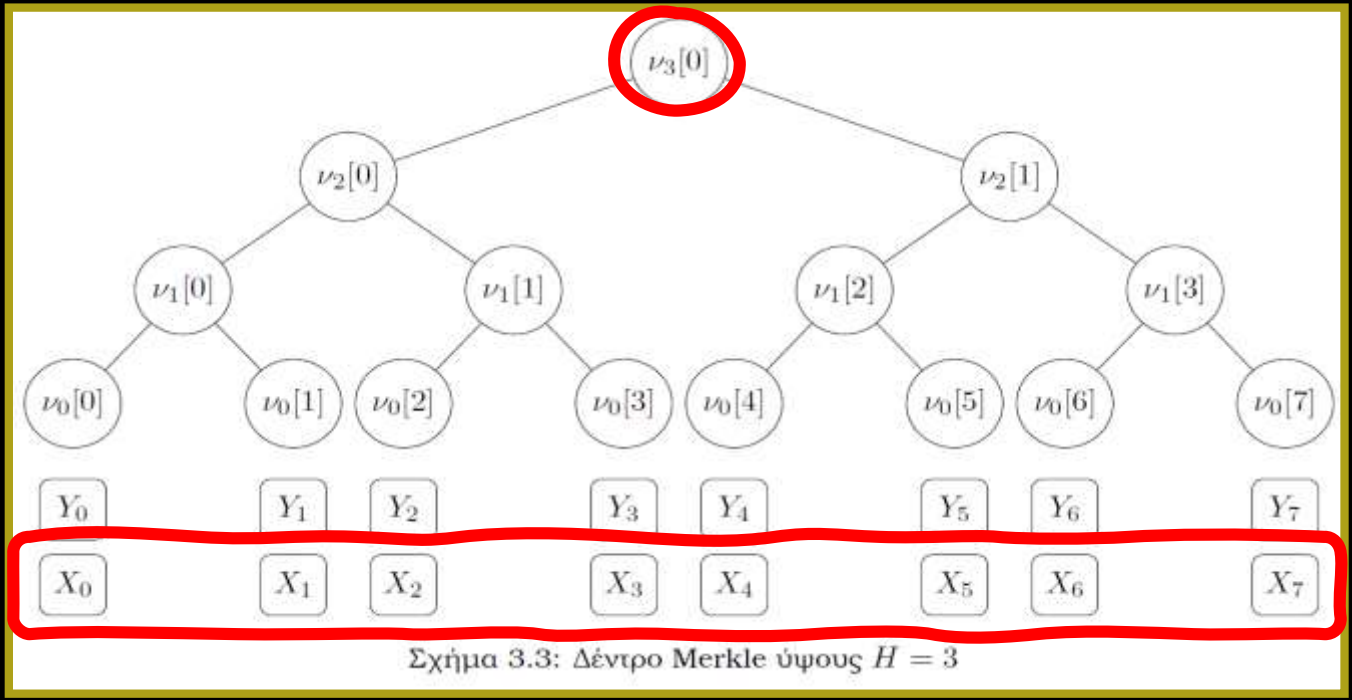


Σχήμα Υπογραφής Merkle (MSS)

➢ Παραγωγή Ζεύγους Κλειδιών (X,Y)

1. Επιλογή $n \in \mathbb{Z}^+$, συνάρτησης κατακερματισμού $g : \{0, 1\}^* \rightarrow \{0, 1\}^n$ και επιλογή OTS.
2. Επιλογή $H \in \mathbb{N}, \geq 2$.
3. Παραγωγή 2^H ζεύγη κλειδιών μιας φοράς (X_i,Y_i).
4. Δημιουργία του δέντρου Merkle.*
5. Υπολογισμός ρίζας δέντρου Merkle.

- **(Ιδιωτικό) Κλειδί Υπογραφής**: Η ακολουθία των X_i.
- **(Δημόσιο) Κλειδί Επαλήθευσης**: Η ρίζα του δέντρου Merkle ($v_H[0]$).



Σχήμα 3.3: Δέντρο Merkle ύψους $H = 3$

- *Τα **φύλλα** του δέντρου Merkle είναι οι τιμές κατακερματισμού $g(Y_j)$, $j \in [0, 2H)$.
- *Οι **εσωτερικοί κόμβοι** του δέντρου Merkle υπολογίζονται σύμφωνα με τον παρακάτω κανόνα κατασκευής :

  ''Κάθε γονέας κόμβος θα είναι η τιμή κατακερματισμού της παράθεσης του αριστερού και δεξιού παιδιού κόμβου του''

Αν 0101 και 1111 είναι δύο αριθμοί, παράθεση τους θα είναι το ''0101||1111 = 01011111''

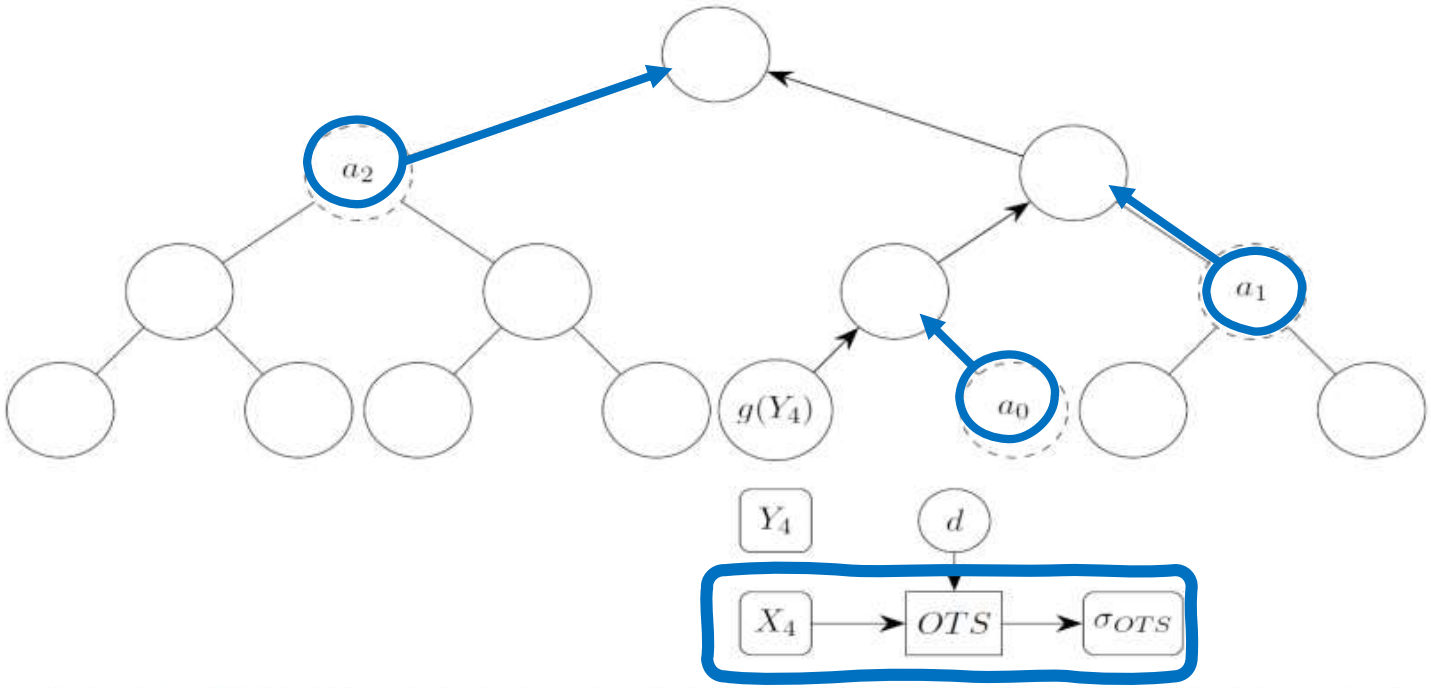
Σχήμα Υπογραφής Merkle (MSS)

➢ Παραγωγή Υπογραφής

Έστω ότι θέλουμε να παράγουμε την s-οστή υπογραφή για μήνυμα m ($s \in \{0, \ldots, 2^H-1\}$).

1. Υπολογισμός $d=g(m)$.
2. Παραγωγή σ_{OTS} για το d, χρησιμοποιώντας το X_s.
3. *Δημιουργία **μονοπατιού αυθεντικοποίησης** $A_s=(a_0, \ldots, A_{h-1})$ για το Y_s.

$$\sigma_s = (s, \sigma_{OTS}, Y_s, (a_0, \ldots, a_{H-1}))$$



Σχήμα 3.4: Δημιουργία υπογραφής Merkle για $s = 4$. Οι κόμβοι που έχουν διακεκομμένο περίγραμμα ανήκουν στο μονοπάτι αυθεντικοποίησης για το φύλλο $g(Y_4)$. Τα βέλη δείχνουν το μονοπάτι από το φύλλο $g(Y_4)$ μέχρι την ρίζα.

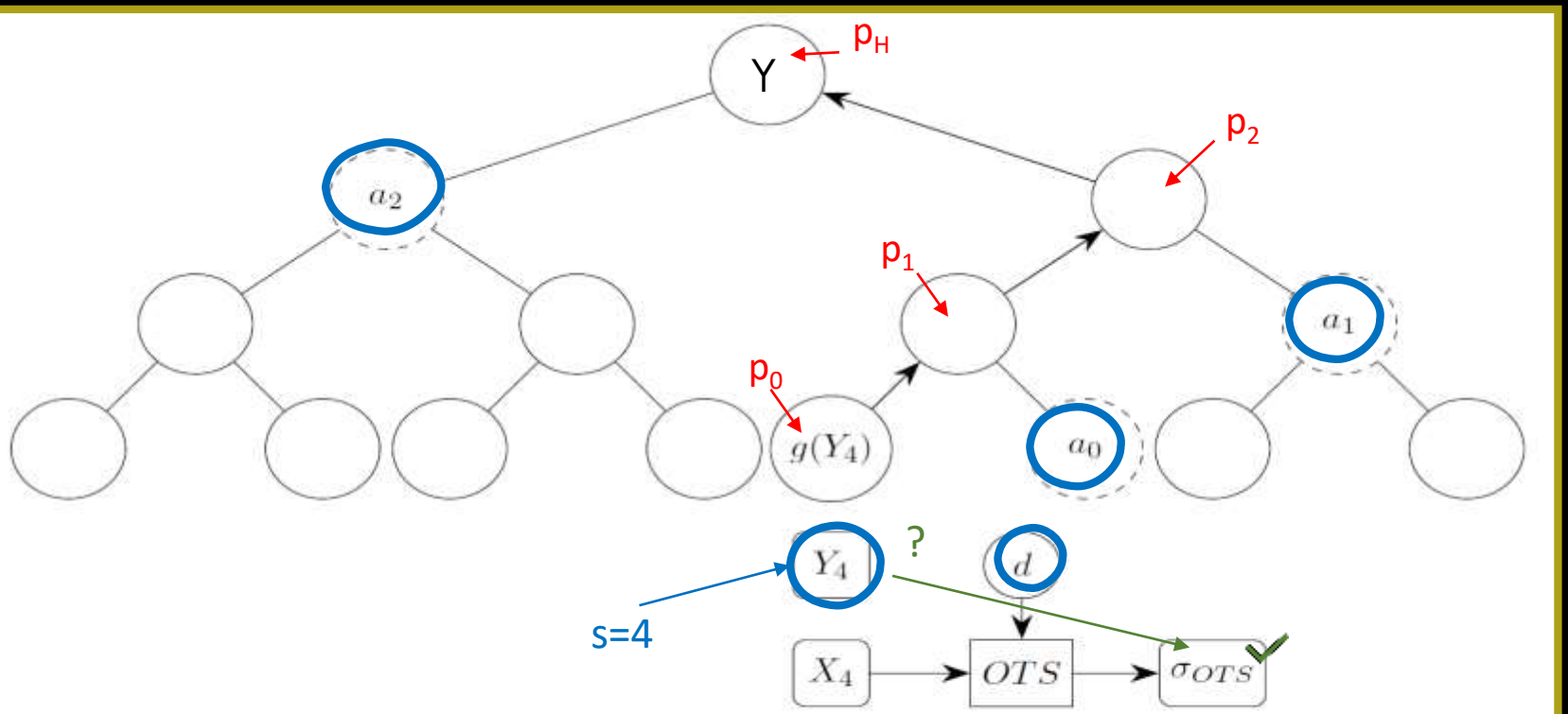
*Κανόνας κατασκευής :
Ο h-οστός κόμβος $a_h \in A_s$ είναι ο αδερφός κόμβος του κόμβου που βρίσκεται στο μονοπάτι από το $g(Y_s)$ μέχρι τη ρίζα σε ύψος h.

Σχήμα Υπογραφής Merkle (MSS)

$\sigma_s = (s, \sigma_{OTS}, Y_s, (a_0, \ldots, a_{H-1}))$

➢ Επαλήθευση Υπογραφής

Η επαλήθευση της s-οστής υπογραφής σ_s γίνεται σε 2 βήματα, πρώτα επαληθεύεται η υπογραφή μιας φοράς σ_{OTS} μέσω και έπειτα επαληθεύεται η αυθεντικότητα του Y_s.



Σχήμα 3.4: Δημιουργία υπογραφής Merkle για $s = 4$. Οι κόμβοι που έχουν διακεκομμένο περίγραμμα ανήκουν στο μονοπάτι αυθεντικοποίησης για το φύλλο $g(Y_4)$. Τα βέλη δείχνουν το μονοπάτι από το φύλλο $g(Y_4)$ μέχρι την ρίζα.

Σχήμα Υπογραφής Merkle (MSS)

Μειονεκτήματα

- Τεράστιες απαιτήσεις χώρου.
- Χρόνος κ χώρος όσον αφορά τα μονοπάτια.

CMSS (Chained MSS) → **GMSS** (Generalized MSS) → **XMSS** (eXtended MSS)

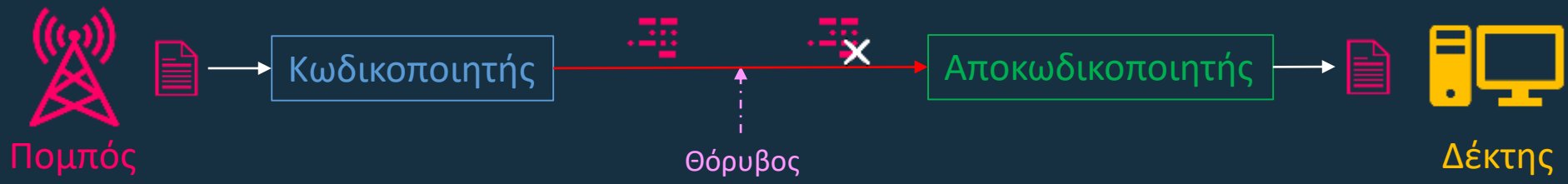
Ασφάλεια	Κβαντικός Αλγόριθμος Grover	Επιταχύνει κάποιες γενικευμένες επιθέσεις, αλλά όχι αρκετά.
	Κβαντικός Αλγόριθμος Shor	Δεν έχει βρεθεί κάποιος τρόπος χρήσης του.

ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΩΔΙΚΩΝ

Θεωρία Κωδίκων

Βασικό αντικείμενο Θεωρίας Κωδίκων

Κωδικοποίηση της πληροφορίας με τέτοιον τρόπο, ώστε αν μικρό πλήθος αλλοιώσεων έχει εισχωρήσει σ' ένα μήνυμα, η αποκωδικοποίηση του να τις διορθώνει.



➢ Παράδειγμα (ASCII) :

✓ Υπολογιστές χρησιμοποιούν μ

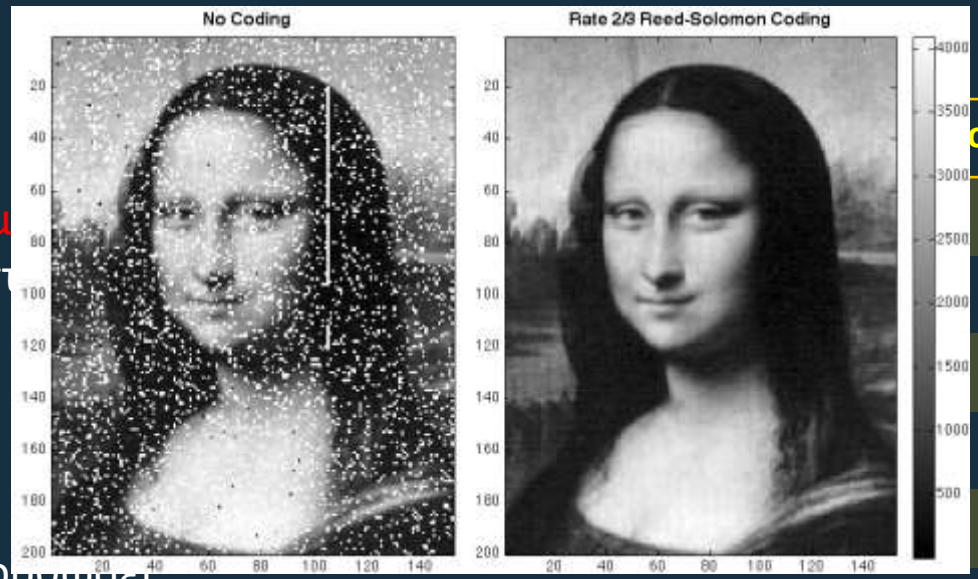
✓ Αδύνατη η αποφυγή λαθών στ

↓

ASCII

✓ Ανιχνεύει λάθη.

✓ Δεν μπορεί να τα διορθώσει.



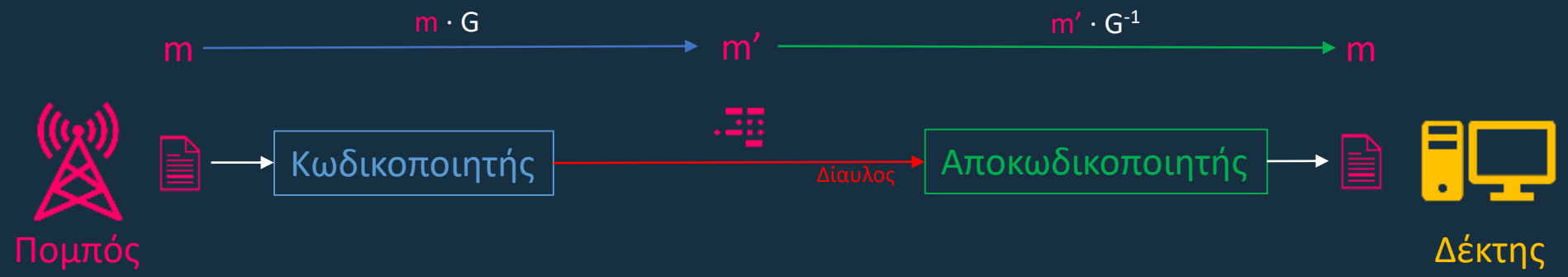
F

1+1=0

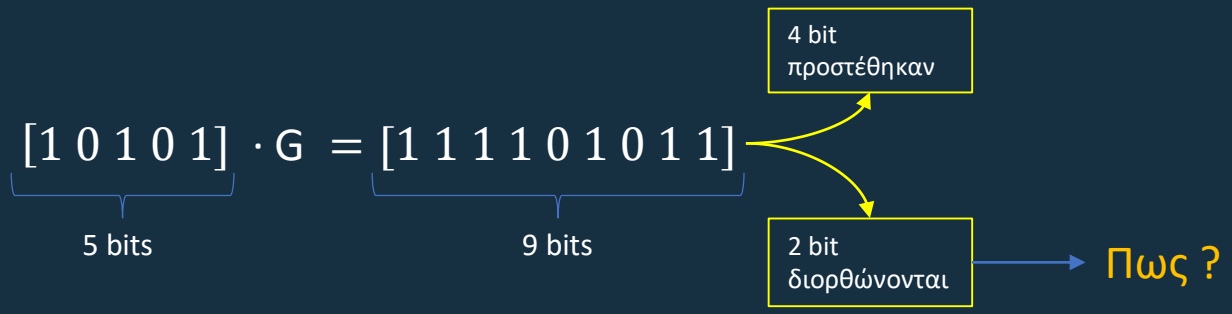
1+1+1=1

ου) Λέξεις ASCII
10000010
10000100
10000111
10001000
10001011
10001101

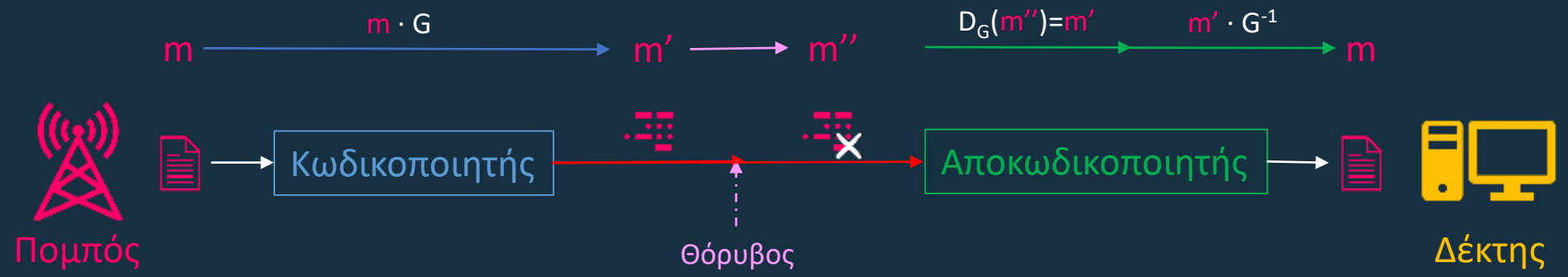
Γραμμικοί Κώδικες



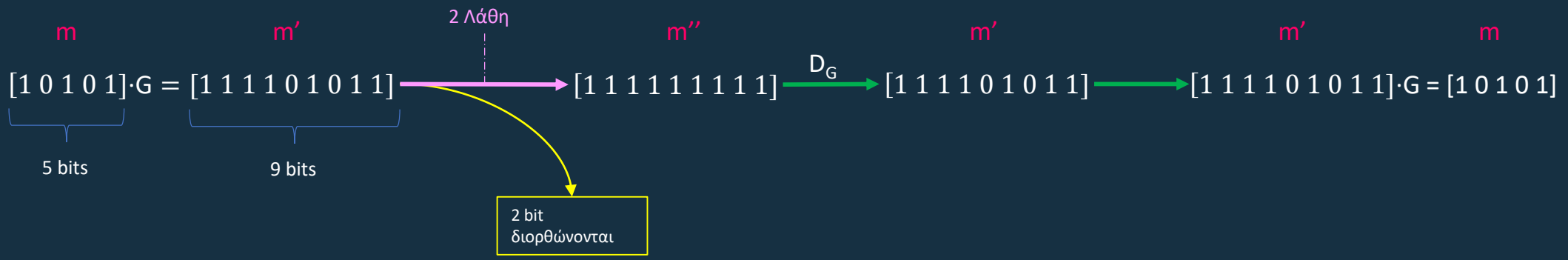
- Παράδειγμα:



Γραμμικοί Κώδικες



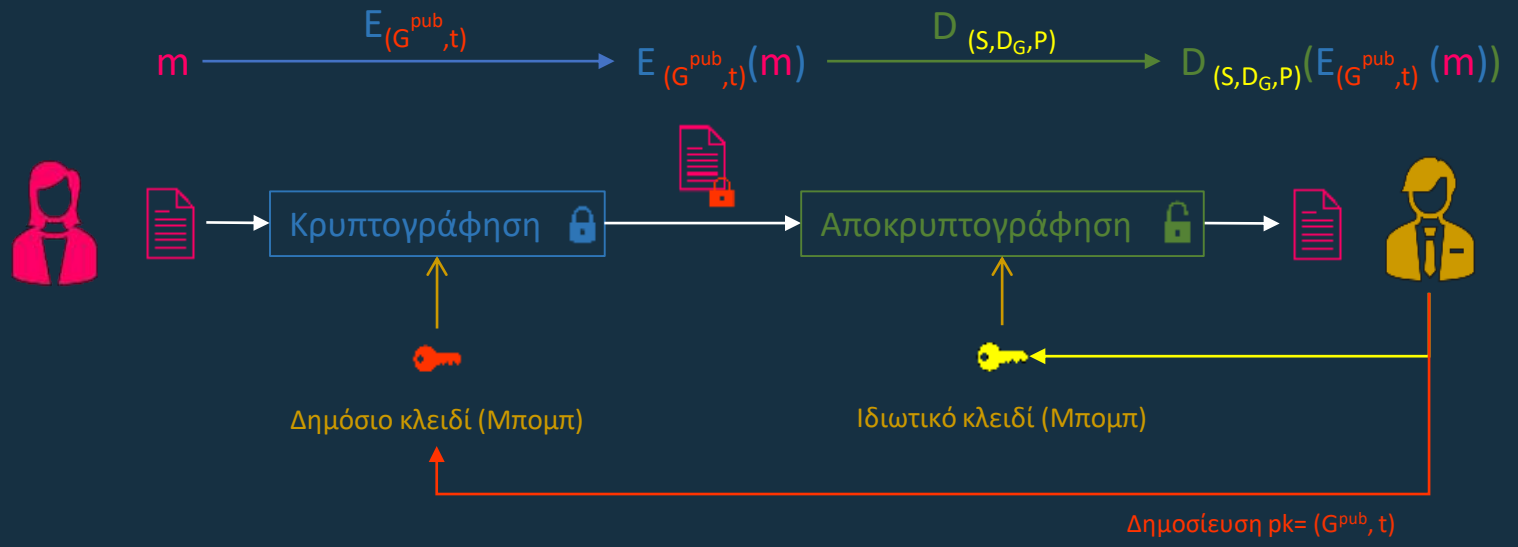
- Παράδειγμα:



Κρυπτοσύστημα McEliece

- Παραγωγή κλειδιών:
  1. Επιλογή τριών πινάκων G,S,P
  2. Υπολογισμός $G^{pub}=S\cdot G\cdot P$
- Δημόσιο κλειδί: (G^{pub}, t) , όπου t ο αριθμός των λαθών
- Ιδιωτικό κλειδί: (S,D_G,P)
- Κρυπτογράφηση: Πολλαπλασιασμός $m\cdot G^{pub}$ και έπειτα εισαγωγή t λαθών.
- Αποκρυπτογράφηση: Διόρθωση λαθών με D_G και έπειτα πολλαπλασιασμός αντίστροφο πίνακα.

Δυαδικοί Κώδικες Goppa
Μπορούν να διορθωθούν λάθη σε πολυωνυμικό χρόνο. (Αλγόριθμος Patterson)



Κρυπτογραφικά Σχήματα Κωδίκων

➢ Κρυπτοσύστημα McEliece

Ασφάλεια	Κβαντικός Αλγόριθμος Grover	Προσφέρει παρόμοιες ταχύτητες με ήδη γνωστούς αλγορίθμους.
	Κβαντικός Αλγόριθμος Shor	Δεν έχει βρεθεί κάποιος τρόπος χρήσης του.

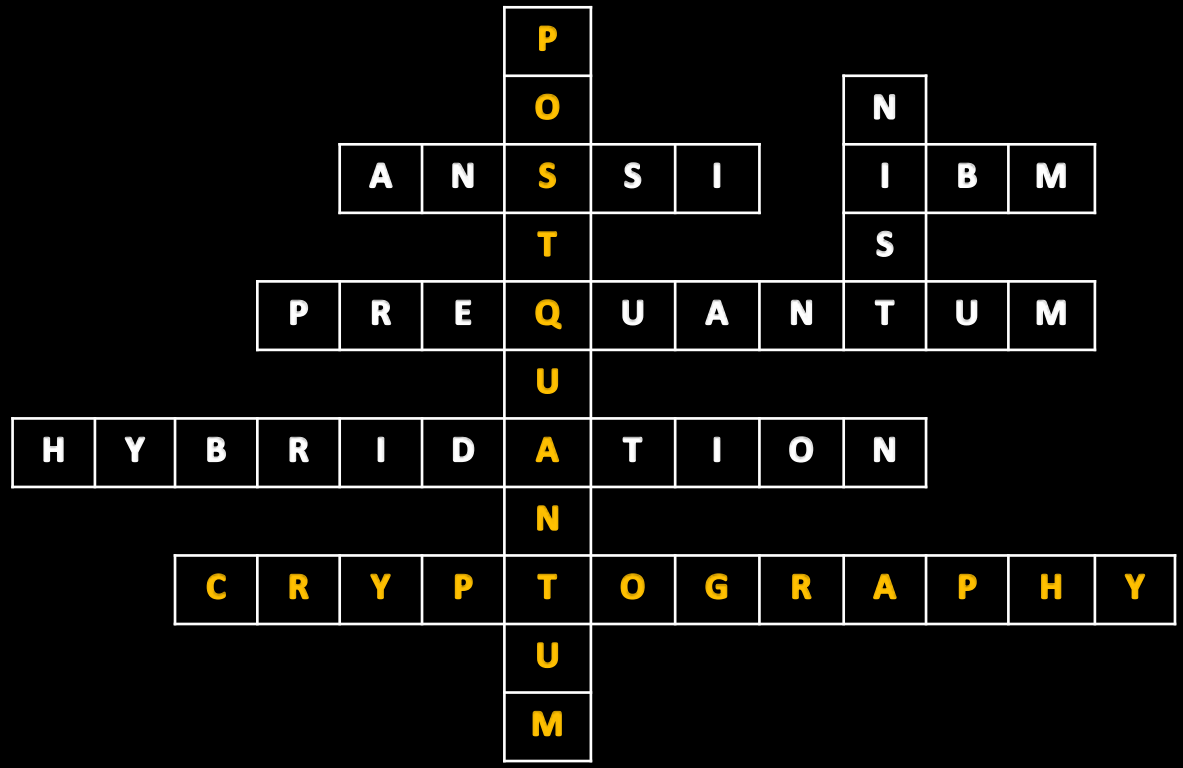
Μειονεκτήματα

- Μεγάλες απαιτήσεις μνήμης

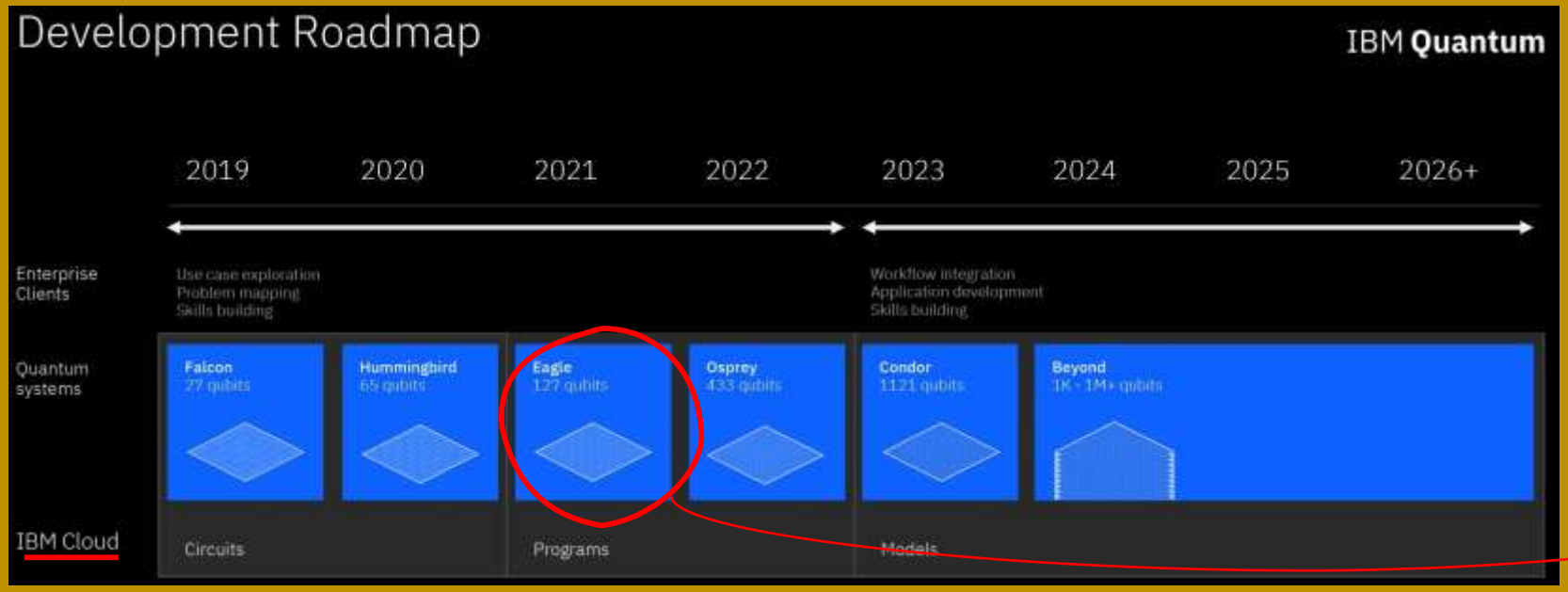
➢ Άλλα Σχήματα:

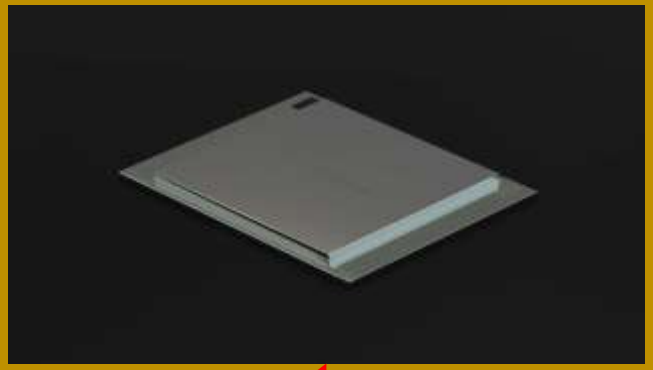
- ✓ Σχήμα ταυτοποίησης του Stern
- ✓ Συναρτήσεις κατακερματισμού
- ✓ Γεννήτριες τυχαίων αριθμών
- ✓ Σχήματα υπογραφής (γίνονται προσπάθειες)

ΜΙΑ ΜΑΤΙΑ ΣΤΟ ΜΕΛΛΟΝ



Κβαντικοί Υπολογιστές





Δεν είναι τόσο απλό
- Κβαντική Αποσυνοχή
- Διόρθωση Λαθών

→ Πολλοί επιστήμονες πιστεύουν ότι θα πάρει δεκαετίες μέχρι την κατασκευή ενός αρκετά μεγάλου κβαντικού υπολογιστή.

↓

Γιατί να μας νοιάζει από τώρα ?

↓

STORE NOW, DECRYPT LATER

There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031."
– Dr. Michele Mosca (2015)

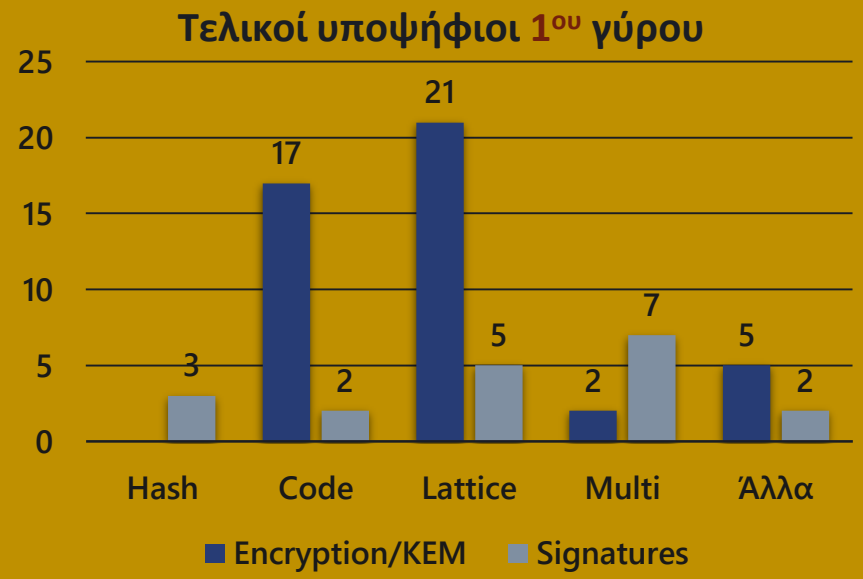
ΗΝΩΜΕΝΕΣ ΠΟΛΙΤΕΙΕΣ ΤΗΣ ΑΜΕΡΙΚΗΣ

❑ National Institute of Standards and Technology (NIST)

ΔΙΑΓΩΝΙΣΜΟΣ NIST (2016)

«Μετακβαντικούς» Αλγορίθμους που να μπορούν με ασφάλεια να εκτελούν:

- Κρυπτογράφηση (Encryption)
- Ασφαλή Διαμοιρασμό Κλειδιού (KEM*)
- Ψηφιακές Υπογραφές (Signatures)



*KEY ENCAPSULATION MECHANISM

(**2020**) 3ος γύρος – 7 φιναλίστ

(**2024**) «Τυποποίηση» ;

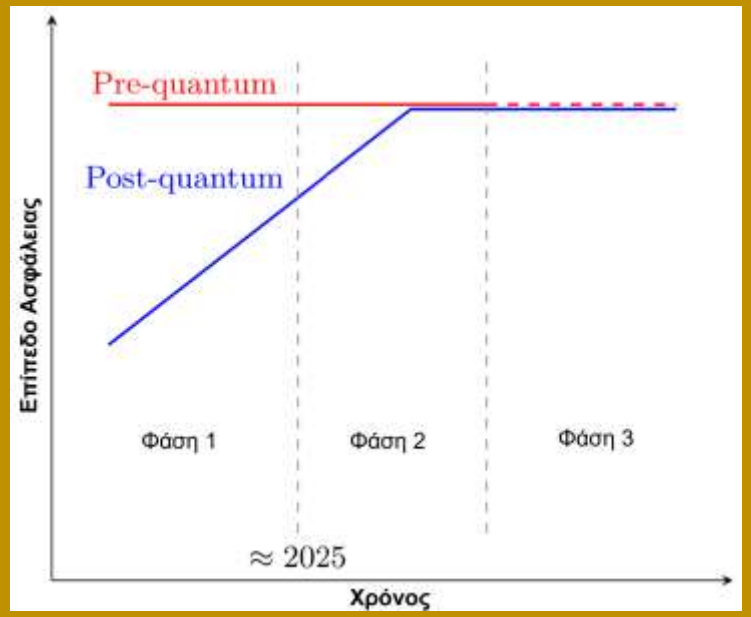
ΓΑΛΛΙΑ (ΕΥΡΩΠΗ)

- **Agence Nationale de la Securité des Systèmes d' Information (ANSSI)***
  - Δημιουργία ''Regroupement de l'Industrie française pour la Sécurité Post – Quantique (RISQ)''

Μετακβαντική Μετάβαση (Άρθρο 2022)

Χρήση υβριδικών μηχανισμών :

- Για δημιουργία κοινού κλειδιού.
- Για ψηφιακές υπογραφές.



*BSI (Bundesamt für Sicherheit in der Informationstechnik)