ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Εθνικόν και Καποδιστριακόν
Πανεπιστήμιον Αθηνών

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

**ΤΜΗΜΑΤΑ ΦΥΣΙΚΗΣ &
ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

**ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ
«ΗΛΕΚΤΡΟΝΙΚΗ – ΡΑΔΙΟΗΛΕΚΤΡΟΛΟΓΙΑ»**

«ΠΡΟΗΓΜΕΝΑ ΘΕΜΑΤΑ ΤΗΛΕΠΙΚΟΙΝΙΑΚΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ»

ΤΕΧΝΙΚΗ ΑΝΑΦΟΡΑ

«ΑΣΦΑΛΕΙΑ ΚΑΙ ΙΔΙΩΤΙΚΟΤΗΤΑ ΔΙΚΤΥΩΝ – ΤΑ ΟΡΙΑ ΤΩΝ ΣΥΓΧΡΟΝΩΝ ΤΕΧΝΙΚΩΝ ΚΡΥΠΤΟΓΡΑΦΙΑΣ»

Όνομα: Πολύβιος
Επώνυμο: Τσιχριτζής
Αριθμός Μητρώου: 7110132200103

Διδάσκοντες: **Ρεΐσης Διονύσιος,** Καθηγητής
Σταθόπουλος Βασίλειος, Δρ.

ΑΘΗΝΑ

07 Ιουλίου 2023

Περιεχόμενα

1. Εισαγωγή

Η λέξη κρυπτογραφία συντίθεται από τα δύο συνθετικά, «κρυπτός», που σημαίνει μυστικός, φτιαγμένος με τέτοιο τρόπο που να μην μπορεί να βρεθεί, και «γράφω», που σημαίνει σχεδιάζω σύμβολα ή αριθμούς σε κάποια επιφάνεια.

Στόχοι της κρυπτογραφίας είναι:

- εμπιστευτικότητα: πρόσβαση δηλαδή από εξουσιοδοτημένα μέλη μόνο
- ακεραιότητα: επεξεργασία της πληροφορίας μόνο από εξουσιοδοτημένα μέλη και ανίχνευση σε περίπτωση αλλοίωσης
- μη απάρνηση: αποστολέας και παραλήπτης δεν μπορούν να αμφισβητήσουν την αυθεντικότητα της μετάδοσης
- πιστοποίηση: εξακρίβωση ταυτότητας αποστολέα και παραλήπτη και προέλευση/προορισμό πληροφορίας

Οι άνθρωποι ανέκαθεν ενθουσιάζονταν με το να κρατούν πληροφορίες κρυφές από τρίτους. Η ιστορία είναι γεμάτη με παραδείγματα από ανθρώπους που προσπαθούσαν να κρατήσουν πληροφορίες μυστικές από εχθρούς. Βασιλιάδες και στρατηγοί επικοινωνούσαν με τους στρατιώτες χρησιμοποιώντας μεθόδους κρυπτογραφίας ώστε να αποτρέψουν τους εχθρούς απ' το να μάθουν ευαίσθητες στρατιωτικές πληροφορίες.

Η εξέλιξη της κοινωνίας προβάλλει τη ανάγκη για πιο εκλεπτυσμένες μεθόδους για την προστασία δεδομένων. Πλέον ζούμε στην εποχή της πληροφορίας κι αυτό είναι πιο εμφανές από ποτέ. Με την συνεχώς αυξανόμενη δικτύωση του κόσμου, οι απαιτήσεις των πληροφοριακών και ηλεκτρονικών υπηρεσιών ακολουθούν την ίδια αυξητική τάση. Ήδη οι ανταλλαγές ευαίσθητων πληροφοριών, όπως για παράδειγμα τα στοιχεία τραπεζικών καρτών μέσω διαδικτύου είναι πολύ κοινή πρακτική. Η προστασία τέτοιου τύπου δεδομένων και των συστημάτων, μέσω των οποίων μεταφέρονται, είναι ζωτικής σημασίας.

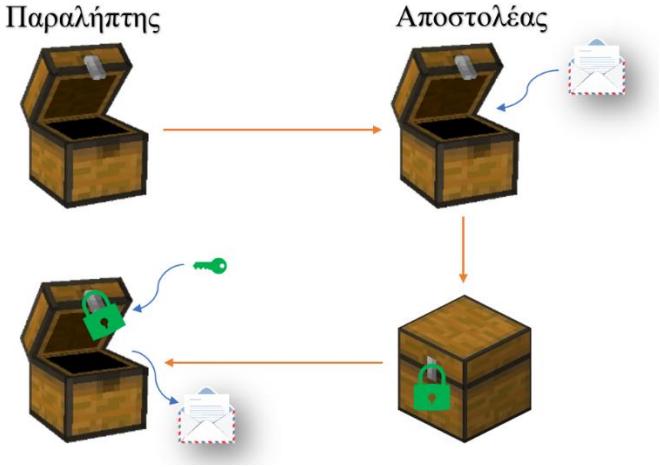
Οι τεχνικές που χρησιμοποιούνται για την προστασία των δεδομένων ανήκουν στο πεδίο της κρυπτογραφίας. Για την ακρίβεια, ο τομέας έχει τρεις ονομασίες, κρυπτογραφία (cryptography), κρυπτολογία (cryptology) και κρυπτανάλυση (cryptanalysis).

Σε γενικές γραμμές, η κρυπτογραφία είναι το αντικείμενο μελέτης μαθηματικών τεχνικών για την επιβολή πολιτικών στη διάδοση πληροφορίας. Αυτές οι πολιτικές καθορίζουν ευρέως ποιος επιτρέπεται να στείλει, να λάβει, να διαβάσει και να επεξεργαστεί ψηφιακή πληροφορία. Μερικές κοινές πρακτικές περιλαμβάνουν ασφάλεια ενάντια σε «ωτακουστές», έλεγχο πρόσβασης ανάγνωσης και εγγραφής στα δεδομένα, και έλεγχο αυθεντικότητας μηνυμάτων. Όλες αυτές οι τεχνικές έχουν κάτι κοινό, ότι εξαρτώνται από συγκεκριμένα δυσεπίλυτα μαθηματικά προβλήματα. Για την επιβεβαίωση ότι ένα κρυπτοσύστημα είναι ασφαλές, πρέπει να αποδειχθεί ότι η κατάρρευσή του είναι τουλάχιστον τόσο δύσκολή όσο η επίλυση ενός μαθηματικού προβλήματος, θεωρητικά δυσεπίλυτου από οποιονδήποτε δε κατέχει κάποιο κομμάτι μυστικής πληροφορίας, γνωστή ως κλειδί. Πέρα από τα σφάλματα εφαρμογής, η όλη δυσκολία έγκειται στην εγγύηση ασφάλειας του κρυπτοσυστήματος και αν αυτή η δυσκολία αναιρεθεί από κάποια τεχνική κρυπτανάλυσης, τότε το σύστημα θεωρείται «σπασμένο».

2. ***Σύγχρονες Τεχνικές Κρυπτογραφίας***

Οι μέθοδοι κρυπτογράφησης/αποκρυπτογράφησης εμπίπτουν σε δύο κατηγορίες, συμμετρικού κλειδιού και δημόσιου κλειδιού. Στους αλγόριθμους συμμετρικού κλειδιού, τα κλειδιά κρυπτογράφησης/αποκρυπτογράφησης είναι γνωστά και στον αποστολέα και στον παραλήπτη. Για παράδειγμα, το κλειδί κρυπτογράφησης είναι ήδη διαμοιρασμένο και το αντίστοιχο κλειδί αποκρυπτογράφησης υπολογίζεται εύκολα από το πρώτο. Σε πολλές περιπτώσεις, τα δύο κλειδιά είναι ακριβώς τα ίδια. Όλα τα κλασικά κρυπτοσυστήματα (πριν το 1970), είναι συμμετρικά, όπως και τα πιο πρόσφατα DES (Data Encryption Standard) και AES (Advanced Encryption Standard).

Οι αλγόριθμοι δημόσιου κλειδιού εισήχθησαν τη δεκαετία του 1970 και έφεραν την επανάσταση στη κρυπτογραφία. Αν υποθέσουμε ότι ένας αποστολέας θέλει να επικοινωνήσει με ασφάλεια με έναν παραλήπτη, αλλά η απόσταση μεταξύ τους είναι τέτοια που να χρειάζεται να σπαταλήσουν χρόνο και πόρους ώστε να βρεθούν από κοντά και να το ανταλλάξουν ή να βρουν έναν έμπιστο μεταφορέα να στείλει το κλειδί στον άλλο. Η λύση σε αυτό το πρόβλημα είναι η κρυπτογραφία δημόσιου κλειδιού. Το κλειδί κρυπτογράφησης είναι δημοσίως γνωστό, αλλά το κλειδί αποκρυπτογράφησης είναι υπολογιστικά ακατόρθωτο να βρεθεί χωρίς πληροφορίες γνωστές αποκλειστικά στον παραλήπτη. Η πιο δημοφιλής υλοποίηση είναι ο RSA, που βασίζεται στην παραγοντοποίηση τεράστιων ακέραιων αριθμών.



Το μη επιστημονικό ανάλογο επικοινωνίας δημόσιου κλειδιού, είναι αυτό με το σεντούκι. Ο παραλήπτης στέλνει στον αποστολέα ένα ξεκλείδωτο σεντούκι. Ο αποστολέας βάζει το μήνυμά του στο ξεκλείδωτο σεντούκι και το κλειδώνει με το λουκέτο, του οποίου το κλειδί έχει ο παραλήπτης. Το κλειδωμένο σεντούκι επιστρέφεται στον παραλήπτη. Φυσικά προκύπτουν άλλα ζητήματα ασφαλείας. Αν για παράδειγμα ένας κακόβουλος παρεμβάλει την πρώτη αποστολή και αντικαταστήσει το λουκέτο του παραλήπτη με το δικό του, μπορεί να διαβάσει το περιεχόμενο του σεντουκιού.

Η κρυπτογραφία δημόσιου κλειδιού αναπαριστά πιθανότατα το τελευταίο βήμα σε μία ιδιαίτερα ενδιαφέρουσα ιστορική πρόοδο. Στα νωρίτερα χρόνια της κρυπτογραφίας, η ασφάλεια βασιζόταν στη διατήρηση της μεθόδου κρυπτογράφησης μυστική. Αργότερα, η μέθοδος θεωρούνταν γνωστή και η ασφάλεια στηριζόταν στη ιδιωτικότητα του συμμετρικού κλειδιού. Στη κρυπτογραφία δημόσιου κλειδιού, η μέθοδος και το κλειδί κρυπτογράφησης είναι δημοσίως γνωστά και όλοι γνωρίζουν τη διαδικασία εύρεσης του κλειδιού αποκρυπτογράφησης. Η ασφάλεια επαναπαύεται (ελπίζει) στην αδυναμία των υπολογιστικών συστημάτων να «σπάσουν» τη κρυπτογραφία.

Οι μέθοδοι δημόσιου κλειδιού είναι πανίσχυρες και δείχνουν να καθιστούν τις αντίστοιχες συμμετρικού κλειδιού απαρχαιωμένες. Εννοείται πως αυτή η ευελιξία δεν έρχεται χωρίς

υπολογιστικό κόστος. Η υπολογιστική ισχύς που απαιτείται στους αλγόριθμους δημόσιου κλειδιού είναι τυπικά αρκετές τάξεις μεγέθους μεγαλύτερη από αυτή που απαιτείται για παράδειγμα στους DES ή AES. Ο εμπειρικός κανόνας είναι ότι οι μέθοδοι δημόσιου κλειδιού χρησιμοποιούνται σε εφαρμογές όπου μόνο μικρές ποσότητες δεδομένων χρειάζονται επεξεργασία, όπως ψηφιακές υπογραφές και αποστολή κλειδιών που χρησιμοποιούνται σε αλγόριθμους συμμετρικού κλειδιού.

a) DES (Data Encryption Standard)

Το 1973 το NBS (National Bureau of Standards: Εθνικό Γραφείο Προδιαγραφών), πλέον NIST (National Institute of Standards and Technology: Εθνικό Ινστιτούτο Προδιαγραφών και Τεχνολογίας), ανακοίνωσε προκήρυξη αναζητώντας ένα κρυπτογραφικό αλγόριθμο που θα γινόταν το νέο εθνικό πρότυπο. Το 1974 η IBM υπέβαλε έναν αλγόριθμο που λεγόταν LUCIFER. Το NBS τον προώθησε στη NSA (National Security Agency: Πρακτορείο Εθνικής Ασφάλειας), και έπειτα από ελέγχους και τροποποιήσεις επέστρεψε με τον αλγόριθμο DES, τον οποίο το 1975 η NBS κυκλοφόρησε και έθεσε ως το επίσημο εθνικό πρότυπο κρυπτογράφησης.

Ο DES χρησιμοποιήθηκε εκτενώς στο ηλεκτρονικό εμπόριο, όπως για παράδειγμα στις τραπεζικές συναλλαγές. Αν δύο τράπεζες ήθελαν να ανταλλάξουν δεδομένα, χρησιμοποιούσαν πρώτα έναν αλγόριθμο σαν τον RSA για να μεταδώσουν ένα κλειδί για DES και στη συνέχεια χρησιμοποιούσαν DES για τη μετάδοση δεδομένων. Η διαδικασία ήταν ταχύτατη και αρκετά ασφαλής.

Ο αλγόριθμος DES είναι κρυπτογραφικός αλγόριθμος δέσμης. Αφού οι δέσμες κρυπτογραφούνται ξεχωριστά, θεωρούμε για το παράδειγμα ότι το πλήρες μήνυμα αποτελείται μόνο από μια δέσμη. Το μήνυμα έχει 12 bits και είναι γραμμένο με μορφή L_0R_0, όπου L_0 αποτελείται από τα πρώτα 6 bits και R_0 από τα υπόλοιπα 6 bits. Το κλειδί K έχει 9 bits. Ο n-οστός κύκλος μετατροπών μετατρέπει ένα σήμα εισόδου $L_{n-1}R_{n-1}$ σε εξόδου L_nR_n, χρησιμοποιώντας ένα κλειδί 8 bit K_n που προέρχεται από το K.

Το κύριο μέρος της διαδικασίας κρυπτογράφησης είναι μια εξίσωση $f(R_{n-1}, K_n)$ που λαμβάνει είσοδο R_{n-1} των 6 bits και μια ακόμα είσοδο των 8 bits K_n και παράγει αποτέλεσμα 6 bit.

Το αποτέλεσμα για το n-οστό κύκλο ορίζεται ως εξής:

$$L_n = R_{n-1} \,\&\, R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$$

όπου $\oplus$ δηλώνει τη λογική πράξη XOR, δηλαδή την πρόσθεση bit προς bit $(\mathrm{mod}\ 2)$.

b) Αλγόριθμος AES-Rijndael

Το 1977, το NIST έκανε έκκληση για υποψήφιους να αντικαταστήσουν το DES. Μεταξύ των απαιτήσεων ήταν ότι ο αλγόριθμος θα έπρεπε να επιτρέπει κλειδιά με μεγέθη 128, 192 και 256 bits, θα έπρεπε να λειτουργεί με δέσμες που έχουν είσοδο 128 bits και έπρεπε να μπορούν να λειτουργούν πάνω σε μία ποικιλία υλικού, όπως για παράδειγμα επεξεργαστές των 8 bits σε έξυπνες κάρτες και επεξεργαστές 32 bits που βρίσκονται σε προσωπικούς υπολογιστές του εμπορίου. Η ταχύτητα και η κρυπτογραφική ισχύς ήταν εξίσου σημαντικές.

Το 1998, η κρυπτογραφική κοινότητα κλήθηκε να κρίνει 15 υποψήφιους αλγορίθμους, εκ των οποίων οι πέντε τέθηκαν σε συζήτηση για την εφαρμογή τους: ο MARS (της IBM), ο RC6 (των εργαστηρίων RSA), ο Rijndael (των Joan Daemen και Vincent Rijmen), ο Serpent (των Ross Anderson, Eli Biham, και Lars Knudsen) και ο Twofish (των Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson). Εν τέλει ο Rijndael επιλέγει ως AES, και παρά το γεγονός ότι οι άλλοι τέσσερις αλγόριθμοι απορρίφθηκαν σε εκείνο το στάδιο, είναι πολύ ισχυροί και πιθανότατα θα βρουν εφαρμογή σε μελλοντικά κρυπτοσυστήματα. Πρόκειται για ένα κρυπτογραφικό αλγόριθμο δέσμης (block cipher), δηλαδή κατά την διενέργειά του τεμαχίζεται το μήνυμα σε τμήματα και το καθένα από αυτά κρυπτογραφείται ξεχωριστά.

Τα 128 bits στην είσοδο ομαδοποιούνται σε 16 Bytes των 8 bits το καθένα

$$a_{0,0}a_{1,0}a_{2,0}a_{3,0}\cdots$$

που οργανώνονται σε πίνακα

$$\begin{matrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{matrix}$$

99	124	119	123	242	107	111	197	48	1	103	43	254	215	171	118
202	130	201	125	250	89	71	240	173	212	162	175	156	164	114	192
183	253	147	38	54	63	247	204	52	165	229	241	113	216	49	21
4	199	35	195	24	150	5	154	7	18	128	226	235	39	178	117
9	131	44	26	27	110	90	160	82	59	214	179	41	227	47	132
83	209	0	237	32	252	177	91	106	203	190	57	74	76	88	207
208	239	170	251	67	77	51	133	69	249	2	127	80	60	159	168
81	163	64	143	146	157	56	245	188	182	218	33	16	255	243	210
205	12	19	236	95	151	68	23	196	167	126	61	100	93	25	115
96	129	79	220	34	42	144	136	70	238	184	20	222	94	11	219
224	50	58	10	73	6	36	92	194	211	172	98	145	149	228	121
231	200	55	109	141	213	78	169	108	86	244	234	101	122	174	8
186	120	37	46	28	166	180	198	232	221	116	31	75	189	139	138
112	62	181	102	72	3	246	14	97	53	87	185	134	193	29	158
225	248	152	17	105	217	142	148	155	30	135	233	206	85	40	223
140	161	137	13	191	230	66	104	65	153	45	15	176	84	187	22

AES-Rijndael S-box

Χρησιμοποιούμε το μοντέλο των GF(2^8) με γεννετήριο πολυώνυμο $X^8 + X^4 + X^3 + X + 1$. Τα στοιχεία του είναι Bytes και μπορούν να προστεθούν με XOR. Γράφουμε ένα Byte ως 8 bits, έστω 10001011. Αναζητούμε στο S-box την όγδοη (1000) σειρά και την ενδέκατη (1011) στήλη. Ο αριθμός που παίρνουμε είναι $61_{10} = 111101_2$.

Το αποτέλεσμα του βήματος SubBytes δίνει πάλι έναν πίνακα 4×4

$$\begin{matrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{matrix}$$

Οι τέσσερις σειρές του πίνακα ολισθαίνουν κυκλικά αριστερά (ShiftRows) με βήματα 0, 1, 2 και 3 για να δώσουν

$$\begin{matrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{matrix} = \begin{matrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{matrix}$$

Θεωρούμε ένα Byte ως ένα στοιχείο του πεδίου Galois GF(2^8). Πολλαπλασιάζουμε τα στοιχεία του πεδίου Galois με αυτά του πίνακα 4×4 που προέκυψαν από το ShiftRows

$$\begin{matrix} 00000010 & 00000011 & 00000001 & 00000001 \\ 00000001 & 00000010 & 00000011 & 00000001 \\ 00000001 & 00000001 & 00000010 & 00000011 \\ 00000011 & 00000001 & 00000001 & 00000010 \end{matrix} \times \begin{matrix} c_{0,0} & c_{0,1} & c_{0,2} & c_{0,3} \\ c_{1,0} & c_{1,1} & c_{1,2} & c_{1,3} \\ c_{2,0} & c_{2,1} & c_{2,2} & c_{2,3} \\ c_{3,0} & c_{3,1} & c_{3,2} & c_{3,3} \end{matrix}$$
$$= \begin{matrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{matrix}$$

Το κλειδί (RoundKey Addition), αποτελείται από 128 bits, τα οποία οργανώνονται σε πίνακα 4×4 Bytes. Γίνεται η λογική πράξη XOR μεταξύ αυτού του πίνακα και του MixColumns

$$\begin{matrix} d_{0,0} & d_{0,1} & d_{0,2} & d_{0,3} \\ d_{1,0} & d_{1,1} & d_{1,2} & d_{1,3} \\ d_{2,0} & d_{2,1} & d_{2,2} & d_{2,3} \\ d_{3,0} & d_{3,1} & d_{3,2} & d_{3,3} \end{matrix} \oplus \begin{matrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{matrix} = \begin{matrix} e_{0,0} & e_{0,1} & e_{0,2} & e_{0,3} \\ e_{1,0} & e_{1,1} & e_{1,2} & e_{1,3} \\ e_{2,0} & e_{2,1} & e_{2,2} & e_{2,3} \\ e_{3,0} & e_{3,1} & e_{3,2} & e_{3,3} \end{matrix}$$

Το αρχικό κλειδί αποτελείται από 128 bits, οργανωμένα σε πίνακα 4×4 Bytes. Ο πίνακας επεκτείνεται ενώνοντας 40 επιπλέον στήλες. Οι 4 πρώτες ονομάζονται W(0), W(1), W(2) και W(3). Οι νέες στήλες παράγονται αναδρομικά. Υποθέτουμε ότι οι στήλες μέχρι W(n-1) είναι ορισμένες. Αν το n δεν είναι πολλαπλάσιο του 4

$$W(n) = W(n-4) \oplus W(n-1)$$

ενώ αν είναι πολλαπλάσιο

$$W(n) = W(n-4) \oplus T(W(n-1))$$

όπου $T(W(n-1))$ η ακόλουθη μετατροπή. Έστω a, b, c, d τα στοιχεία της στήλης $W(n-1)$. Τα ολισθαίνουμε κυκλικά ώστε να πάρουμε b, c, d, a. Αντικαθιστούμε κάθε Byte με τα αντίστοιχα στοιχεία από το S-box από το βήμα SubBytes, για να λάβουμε 4 Bytes e, f, g, h. Τέλος, υπολογίζουμε τη σταθερά κύκλου

$$r(n) = 00000010^{(n-4)/4}$$

στο GF(2^8).

Το $T(W(n-1))$ είναι το διάνυσμα στήλης $(e \oplus r(n), f, g, h)$. Έτσι, οι στήλες W(4), …, W(43) παράγονται από τις αρχικές 4 στήλες. Το κλειδί για το n-οστό γύρο αποτελείται από τις στήλες

$$W(4n), W(4n+1), W(4n+2), W(4n+3)$$

c) <u>Αλγόριθμος RSA (Rivest, Shamir και Adleman)</u>

Έστω ένας αποστολέας θέλει να στείλει ένα μήνυμα σε έναν παραλήπτη, αλλά δεν είχαν ποτέ ξανά επαφή και δε θέλουν να προσλάβουν έναν έμπιστο μεταφορέα ώστε να μοιραστούν το κλειδί.

Φυσικά, ελλοχεύει ο κίνδυνος ένας κακόβουλος «ωτακουστής» να αποκτήσει πρόσβαση στο μήνυμα. Είναι εφικτό βέβαια, το μήνυμα να σταλεί με τέτοιο τρόπο, ώστε ο κακόβουλος να μην μπορεί να αποκτήσει πρόσβαση στο περιεχόμενό του.

Σύμφωνα με τις προηγούμενες μεθόδους αυτό θα ήταν αδύνατο. Κατά την αποστολή, ο ωτακουστής» θα παρεμβαλλόταν, θα έκλεβε το κλειδί και συνεπώς θα μπορούσε να αποκρυπτογραφήσει όλα τα ακόλουθα μηνύματα. Πρόκειται για κρυπτοσύστημα δημόσιου κλειδιού, το οποίο είχε προταθεί δημόσια από τους Diffie και Hellman, στη κλασική τους δημοσίευση του 1976, Diffie-Hellman. Η πρότασή τους δεν είχε πρακτική υλοποίηση, παρά το γεγονός ότι παρουσίασαν μία εναλλακτική διαδικασία ανταλλαγής κλειδιού που λειτουργεί σε δημόσια κανάλια. Στα επόμενα χρόνια, προτάθηκαν αρκετές άλλες μέθοδοι, εκ των οποίων η πιο πετυχημένη βασιζόταν στη δυσκολία παραγοντοποίησης ακεραίων αριθμών σε παράγοντες πρώτων αριθμών, και ήταν αυτή που προτάθηκε από τους Rivest, Shamir και Adleman το 1977 και είναι γνωστός ως αλγόριθμος RSA.

Υπήρχε η υπόθεση ότι κυβερνητικά πρακτορεία είχαν ανακαλύψει τον αλγόριθμο RSA αρκετά χρόνια πριν, αλλά οι κανόνες τούς απέτρεπαν από το να το μοιραστούν με το κοινό. Τελικά, το 1977, έγγραφα από το CESG[1] (Εθνική Τεχνική Αρχή Διασφάλισης Πληροφορίας της κυβέρνησης του Ηνωμένου Βασιλείου), ένα βρετανικό κρυπτογραφικό πρακτορείο, έδειξε ότι ο James Ellis το 1970 ανακάλυψε τη κρυπτογραφία δημόσιου κλειδιού και το 1973 ο Clifford Cocks είχε συντάξει ένα έγγραφο, περιγράφοντας μια έκδοση του αλγόριθμου RSA, στον οποίο το εκθετικό κρυπτογραφίας e, ήταν ίδιο με το συντελεστή n.

i) Λειτουργία Αλγόριθμου RSA

Ο παραλήπτης επιλέγει δύο διακριτούς μεγάλους πρώτους αριθμούς και τους πολλαπλασιάζει μεταξύ τους για να σχηματίσει:

$$n = pq$$

Επιλέγει επίσης ένα εκθετικό κρυπτογραφίας e, τέτοιο ώστε

$$gcd\big(e,(p-1)(q-1)\big) = 1$$

Ο παραλήπτης στέλνει το ζευγάρι (n,e) στον αποστολέα, αλλά κρατάει τις τιμές των p και q μυστικές. Συγκεκριμένα, ο αποστολέας, που θα μπορούσε κάλλιστα να είναι κακόβουλος, δε χρειάζεται να γνωρίζει τους p και q για να στείλει το μήνυμά του στον παραλήπτη με ασφάλεια. Ο παραλήπτης γράφει το μήνυμά του ως ένα αριθμό m. Αν ο m είναι μεγαλύτερος από τον n, το μήνυμα κατατμείται σε κομμάτια, το καθένα μικρότερο από n. Για χάρη ευκολίας, συνεχίζουμε υποθέτοντας ότι $m < n$. Ο παραλήπτης υπολογίζει

$$c \equiv m^e \ (mod\ n)$$

και στέλνει στον αποστολέα το c. Εφόσον ο παραλήπτης γνωρίζει το p και q, μπορεί να υπολογίσει $(p-1)(q-1)$ και συνεπώς μπορεί να βρει το εκθετικό αποκρυπτογράφησης d με το εξής

[1] https://www.gov.uk/government/organisations/cesg

$$de \equiv 1\big(mod(p-1)(q-1)\big).$$

Ο παραλήπτης μπορεί να διαβάσει το μήνυμα, δεδομένου ότι $m \equiv c^d (mod\ n)$.

ii) <u>Παράδειγμα</u>

Η Αθηνά θέλει να στείλει στον Παύλο τη λέξη «cat».

Ο Παύλος επιλέγει

$$p = 885.320.963, \qquad q = 238.855.417$$

$$n = p \cdot q = 211.463.707.796.206.571$$

Θέτουμε το κρυπτογραφικό εκθετικό

$$e = 9.007$$

Οι τιμές αποστέλλονται στην Αθηνά.

Αριθμούμε τα γράμματα της λέξης ξεκινώντας από α=01, έως ω=24.

$$\text{cat} \rightarrow m = 30120$$

Η Αθηνά υπολογίζει

$$c \equiv m^e = 30.120^{9.007} = 113.535.859.035.722.866 \ \ (mod\ n)$$

και το στέλνει στον Παύλο.

Εφόσον ο Παύλος γνωρίζει τα p και q, γνωρίζει $(p-1)(q-1)$. Χρησιμοποιεί τον εκτενή Ευκλείδειο αλγόριθμο να υπολογίσει το d ώστε

$$de \equiv 1\big(mod(p-1)(q-1)\big) = \big(mod(885.320.963-1)(238.855.417-1)\big)$$

που δίνει

$$d = 116.402.471.153.538.991$$

Ο Παύλος υπολογίζει

$$c^d \equiv 113.535.859.035.722.866^{116.402.471.153.538.991} \equiv 30120(mod\ n)$$

και βλέπει το αρχικό μήνυμα.

iii) Σύνοψη

1	Ο Παύλος διαλέγει τους p και q, κρατώντας τους μυστικούς, και υπολογίζει $n = p \cdot q$.
2	Ο Παύλος διαλέγει e, με $gcd\big(e, (p-1)(q-1)\big) = 1$.
3	Ο Παύλος υπολογίζει το d, με $de \equiv 1\big(mod(p-1)(q-1)\big)$.
4	Ο Παύλος γνωστοποιεί δημόσια τα n και e, κρατώντας τα p, q, d $κρυφά$.
5	Η Αθηνά κρυπτογραφεί το m ως $c \equiv m^e \ (mod\ n)$ και στέλνει το c στον Παύλο.
6	Ο Παύλος αποκρυπτογραφεί το αρχικό μήνυμα υπολογίζοντας $m \equiv c^d \ (mod\ n)$.

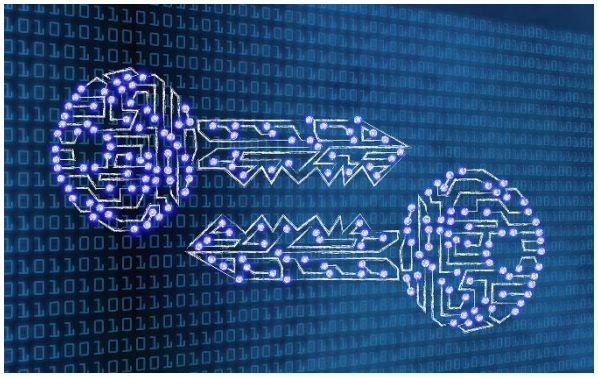
d) Αλγόριθμοι ECC (Elliptic Curve Cryptography)

Οι ελλειπτικές καμπύλες μελετώνται για πολλά χρόνια και η βιβλιογραφία για αυτές είναι τεράστια. Το 1985, οι Neal Koblitz και V. S. Miller ανεξάρτητα πρότειναν τη χρήση τους σε κρυπτοσυστήματα δημόσιου κλειδιού. Δεν εφηύραν κάποιο νέο κρυπτογραφικό αλγόριθμο με ελλειπτικές τροχιές πάνω σε άπειρες διαστάσεις, αλλά υλοποίησαν ήδη υπάρχοντες αλγόριθμους δημόσιου κλειδιού, όπως το Diffie-Hellman, χρησιμοποιώντας ελλειπτικές τροχιές.

Οι ελλειπτικές καμπύλες παρουσιάζουν ενδιαφέρον επειδή παρέχουν έναν τρόπο δόμησης «στοιχείων» και «κανόνες συνδυασμού» που παράγουν ομάδες. Αυτές οι ομάδες παρουσιάζουν αρκετές οικείες ιδιότητες για να χτίσουμε αλγόριθμους κρυπτογραφίας, αλλά δεν έχουν ορισμένες ιδιότητες που να διευκολύνουν τη κρυπτανάλυση. Για παράδειγμα, δε υπάρχει καλή αίσθηση «ομαλού» με τις ελλειπτικές καμπύλες. Με άλλα λόγια, δεν υπάρχει ένα σύνολο μικρών στοιχείων όσον αφορά ποιο τυχαίο στοιχείο έχει πιθανότητα να μπορεί να εκφραστεί από έναν απλό αλγόριθμο. Ως εκ τούτου, οι αλγόριθμοι διακριτών λογαρίθμων δε λειτουργούν.

Οι ελλειπτικές καμπύλες πάνω στο πεπερασμένο πεδίο Galois (GF/2^n) είναι ιδιαίτερα ενδιαφέρουσες. Οι αριθμητικοί επεξεργαστές για το υποκείμενο πεδίο είναι εύκολο να κατασκευαστούν και σχετικά απλοί στην υλοποίηση για n μεταξύ 130 και 200. Προσφέρουν τη δυνατότητα ταχύτερων κρυπτοσυστημάτων δημόσιου κλειδιού με μικρά μεγέθη κλειδιών. Πολλοί αλγόριθμοι δημόσιου κλειδιού, όπως οι Diffie-Hellman και ElGamal, μπορούν να υλοποιηθούν με ελλειπτικές καμπύλες πάνω σε πεπερασμένα πεδία.

i) Ανταλλαγή Κλειδιού με Ελλειπτική Καμπύλη Diffie-Hellman



https://www.thesslstore.com/blog/post-quantum-cryptography-data-security-in-a-post-quantum-world/

Η Αθηνά κι ο Παύλος θέλουν να ανταλλάξουν ένα κλειδί. Προκειμένου να γίνει αυτό, συμφωνούν ένα δημόσιο σημείο αναφοράς G σε μια ελλειπτική καμπύλη

$$\text{E: } y^2 \equiv x^3 + bx + c \ (mod\ p)$$

Έστω $p = 7211$, $b = 1$ και $G = (3, 5)$. Αυτό μας ωθεί να επιλέξουμε $c = 7206$ ώστε να έχουμε το σημείο πάνω στη καμπύλη. Η Αθηνά επιλέγει $N_A = 12$ και ο Παύλος $N_B = 23$, και οι δύο τυχαία. Διατηρούν τα N_A και N_B ιδιωτικά, αλλά δημοσιοποιούν τα $N_A G$ και $N_B G$.

$$N_A G = (1794, 6375)\ \&\ N_B G = (3861, 1242)$$

Η Αθηνά πολλαπλασιάζει το $N_B G$ με το N_A για να λάβει το κλειδί:

$$N_A(N_B G) = 12(3861, 1242) = (1472, 2098)$$

Ομοίως ο Παύλος

$$N_B(N_A G) = 23(1794, 6375) = (1472, 2098)$$

Τα κλειδιά που προκύπτουν και για τους δύο είναι ίδια.

ii) Ψηφιακές Υπογραφές ElGamal

Η Αθηνά θέλει να στείλει ένα μήνυμα m, το οποίο μπορεί κάλλιστα να είναι ένα τεμάχιο που προκύπτει από το κατακερματισμό ενός μεγαλύτερου μηνύματος. Υποθέτουμε ότι το m είναι ακέραιος. Σχεδιάζει μία ελλειπτική καμπύλη $E\ (mod\ p)$, όπου p ένας μεγάλος πρώτος αριθμός και ένα σημείο A πάνω στη καμπύλη E. Υποθέτουμε επίσης ότι ο αριθμός των σημείων N πάνω στην E έχει υπολογιστεί και αν $0 \leq m < N$, όλα καλώς. Αλλιώς, πρέπει να επιλέξει μεγαλύτερο p. Η Αθηνά επιλέγει επιπλέον ένα ακέραιο a, που κρατά ιδιωτικό, και υπολογίζει $B = aA$. Ο πρώτος αριθμός p, η καμπύλη E, ο ακέραιος n και τα σημεία A και B γνωστοποιούνται δημοσίως. Για να υπογράψει το μήνυμα η Αθηνά, κάνει τα εξής:

- Επιλέγει έναν τυχαίο ακέραιο k, με $1 \leq k < N$ και $gcd(k, N) = 1$, και υπολογίζει $R = kA = (x, y)$
- Υπολογίζει $s \equiv k^{-1}(m - ax)\ (mod\ N)$
- Στέλνει το υπογεγραμμένο μήνυμα στον Παύλο

Δεδομένου ότι R είναι σημείο πάνω στην E, και m και s είναι ακέραιοι, ο Παύλος επαληθεύει τη γνησιότητα υπογραφής ως εξής:

- Αποκτά πρόσβαση στη δημόσια πληροφορία της Αθηνάς p, E, A, B
- Υπολογίζει $V_1 = xB + sR$ και $V_2 = mA$

- Ανακηρύσσει την υπογραφή γνήσια αν $V_1 = V_2$

Η διαδικασία επαλήθευσης λειτουργεί επειδή

$$V_1 = xB + sR = xaA + k^{-1}(m - ax)(kA) = xaA + (m - ax)A = mA = V_2$$

Πρέπει να σημειωθεί ότι σε αυτή την εξίσωση επαλήθευσης χρησιμοποιήσαμε το k^{-1} ως ακέραιο $mod\ N$, ικανοποιώντας $k^{-1}k \equiv 1\ (mod\ N)$. Αυτό σημαίνει ότι $k^{-1}k$ δεν ισούται με 1, αλλά μάλλον με έναν ακέραιο, συγκλίνων σε $1\ (mod\ N)$. Άρα, $k^{-1}k \equiv 1 + tN$, για κάποιον ακέραιο t. Αποδεικνύεται ότι $NA = \infty$. Συνεπώς,

$$k^{-1}kA \equiv (1 + tN)A = A + t(NA) = A + t\infty = A$$

Αυτό υποδηλώνει ότι τα k^{-1} και k αλληλοαναιρούνται στην εξίσωση επαλήθευσης.

Το κλασικό σύστημα ElGamal και η συγκεκριμένη έκδοση ελλειπτικής καμπύλης είναι ανάλογα μεταξύ τους. Οι ακέραιοι $mod\ p$ αντικαθίστανται από την ελλειπτική καμπύλη E και ο αριθμός $p - 1$ γίνεται N. Ας σημειώσουμε ότι οι υπολογισμοί στο κλασικό μοντέλο δουλεύει με μη μηδενικούς ακεραίους $mod\ p$ και υπάρχουν $p - 1$ συγκλίνουσες κλάσεις. Η έκδοση ελλειπτικής καμπύλης δουλεύει με σημεία της ελλειπτικής καμπύλης που είναι πολλαπλάσια του A και το πλήθος των σημείων αυτών είναι διαιρέτης του N.

Η χρήση της συνιστώσας x του R στην ελλειπτική έκδοση είναι κάπως αυθαίρετη. Οποιαδήποτε μέθοδος ανάθεσης ακεραίων σε σημεία της καμπύλης θα λειτουργούσε. Η χρήση της συνιστώσας x είναι εύκολη επιλογή. Ομοίως, στο κλασικό σύστημα ElGamal, η χρήση του ακέραιου r στην εξίσωση $mod\ p - 1$ για το s ίσως φανεί σχετικά αφύσικο, αφού το r ορίστηκε αρχικά ως $mod\ p$. Από την άλλη, οποιαδήποτε μέθοδος ανάθεσης ακεραίων στους ακεραίους $mod\ p$ θα λειτουργούσε.

3. ***Υλοποίηση σε Υλικό (Hardware Implementation)***

α) Ασφάλεια Συστημάτων UTMS

Η ασφάλεια είναι ένα τεράστιο θέμα στα παγκόσμια δίκτυα ασύρματων τηλεπικοινωνιακών συστημάτων (UMTS: Universal Mobile Telecommunication Systems). Τα δίκτυα πρόσβασης πρέπει να είναι φυσικά ασφαλή, αλλά πρέπει επιπροσθέτως να λάβουμε υπόψιν κι άλλες παραμέτρους ασφαλείας. Για να επιτύχουμε αποδοτική και ασφαλή περιαγωγή μεταξύ διαφόρων δικτύων, τα UMTS υποστηρίζουν πολύ πιο περίπλοκους μηχανισμούς ασφαλείας από τα προηγούμενα συστήματα, όπως ήταν τα GSM (Global System for Mobile communications) και DECT (Digital Enhanced Cordless Telecommunications). Η εμπιστευτικότητα των κλήσεων φωνής, δηλαδή η μεταδιδόμενη πληροφορία των χρηστών, επιτυγχάνεται στο δίκτυο ραδιο-πρόσβασης (RAN: Radio Access Network). Αυτό σημαίνει ότι ο χρήστης ελέγχει με ποιούς επικοινωνεί, αλλά σε κάθε περίπτωση, η επιβεβαίωση ότι πράγματι εφαρμόζεται η προστασία της εμπιστευτικότητας είναι απαραίτητη για να είναι ήσυχος ο χρήστης, και για αυτό υπάρχουν και κατάλληλοι μηχανισμοί που το επιβεβαιώνουν.

Η αρχιτεκτονική UTMS βασίζεται σε τρεις διαδικασίες. Αρχικά, ο χρήστης επιβεβαιώνει το δίκτυο και αντίστροφα. Έπειτα απαιτείται προστασία ακεραιότητας της σηματοδοτούμενης πληροφορίας,

και τέλος, προστατεύεται η εμπιστευτικότητα χρήστη και πληροφορίας. Η αυθεντικοποίηση εκτελείται από τη διαδικασία αυθεντικοποίησης και συμφωνίας κλειδιού (AKA: Authentication and Key Agreement). Πέρα από την αυθεντικοποίηση, η διαδικασία AKA παράγει και το κλειδί κρυπτογραφίας (CK: Cipher Key) και το κλειδί ακεραιότητας (IK: Integrity Key). Στα UMTS χρησιμοποιείται μόνο η μέθοδος κρυπτογράφησης του κρυπτογραφικού αλγορίθμου δέσμης Rijndael, ως μια επαναλαμβανόμενη συνάρτηση κατακερματισμού. Τα μήκη των τεμαχίων και του κλειδιού έχουν οριστεί στα 128 bits.

Από την άποψη προδιαγραφών, το κύριο πεδίο λειτουργίας του 3GPP (3rd Generation Partnership Project) είναι να ορίσει και να διατηρήσει τις προδιαγραφές του UMTS. Στα UMTS, ο τερματικός εξοπλισμός του τελικού χρήστη ονομάζεται εξοπλισμός χρήστη (UE: User Equipment). Από την πλευρά του δικτύου, ο UE είναι υπεύθυνος για τις λειτουργίες επικοινωνιών που είναι απαραίτητες στην άλλη πλευρά της διεπιφάνειας, εξαιρουμένων τυχόν εφαρμογών που αφορούν τον τελικό χρήστη. Γενικά, ο μηχανισμός αυθεντικοποίησης στηρίζεται σε ένα κυρίως κλειδί (MK: Master Key), K, το οποίο διαμοιράζεται μεταξύ της κάρτας USIM (Universal Subscriber Identity Module) και της βάσης δεδομένων του οικιακού δικτύου. Πρόκειται για ένα μόνιμο μυστικό, μήκους 128 bits. Το κλειδί K δε γίνεται ποτέ ορατό σε καμία από τις δύο πλευρές. Καθ' όλη τη διάρκεια της αυθεντικοποίησης, τα κλειδιά κρυπτογράφησης και ακεραιότητας προκύπτουν από υπολογισμούς. Αυτά είναι προσωρινά κλειδιά με ίδιο μήκος, 128 bits. Νέα κλειδιά δημιουργούνται από το μόνιμο κλειδί κάθε φορά που έχουμε συμβάν αυθεντικοποίησης.

Η AKA είναι ενσωματωμένη στη USIM, ενώ η διαδικασία MAC (Message Authentication Code), που διαχειρίζεται την ακεραιότητα της πληροφορίας, και εμπιστευτικότητας είναι ενσωματωμένες στις φορητές συσκευές.

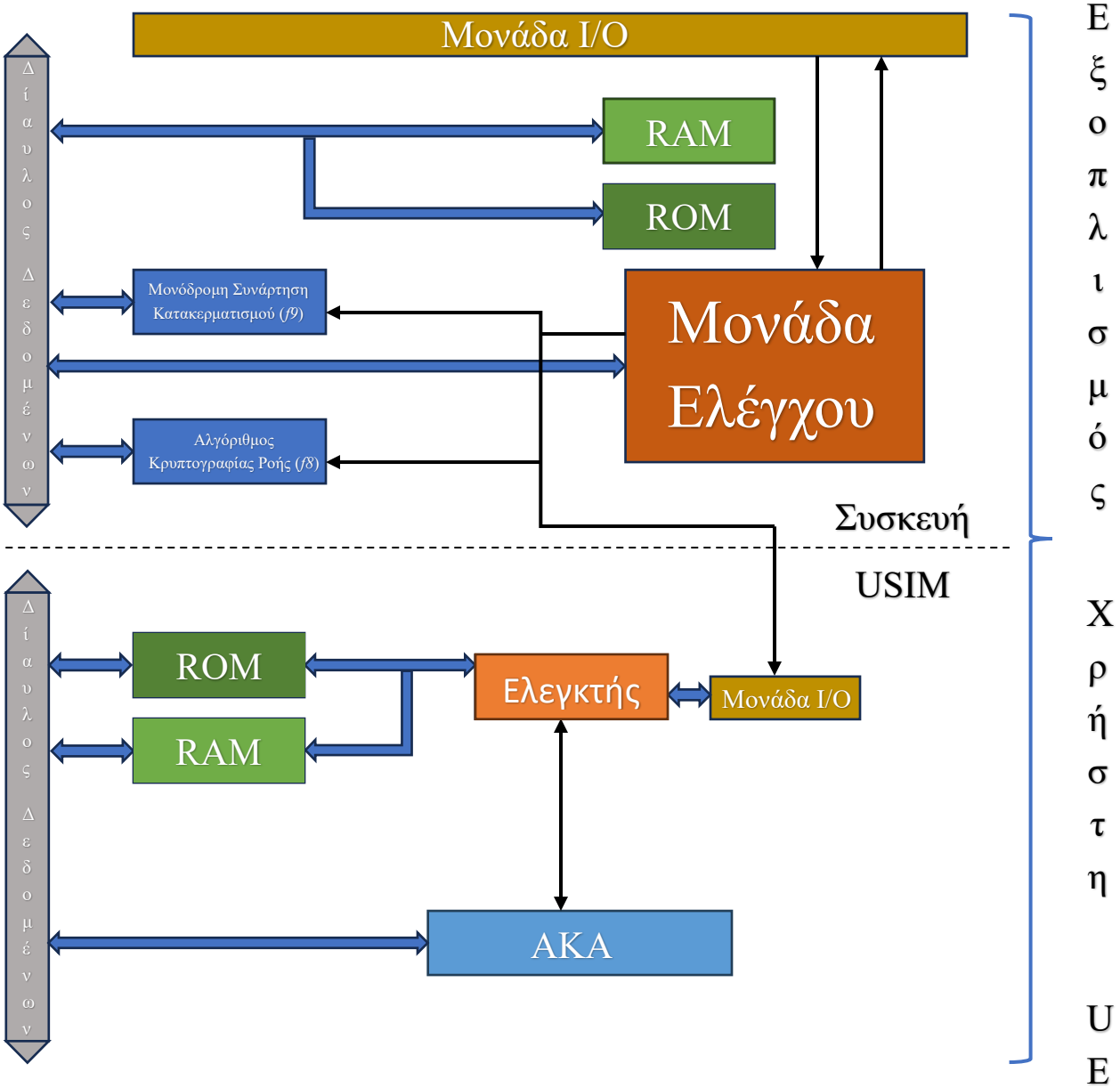
Η διαδικασία αυθεντικοποίησης μπορεί να ξεκινήσει όταν ο χρήστης ταυτοποιείται στο δίκτυο παροχής υπηρεσιών (SN: Service Network). Η ταυτοποίηση συμβαίνει όταν η ταυτότητα του χρήστη μεταδίδεται στο καταχωρητή τοποθεσίας επισκέπτη (VLR: Visitor Location Register) ή στο SGSN[2]. Έπειτα, είτε ο VLR είτε ο SGSN στέλνει αίτημα αυθεντικοποίησης δεδομένων στο κέντρο αυθεντικοποίησης (AuC: Authentication Center), που βρίσκεται στο οικείο δίκτυο. Στη συνέχεια, το AuC στέλνει στο χρήστη τις κατάλληλες παραμέτρους αυθεντικοποίησης, το τεκμήριο αυθεντικοποίησης (AUTN: Authentication Token) και μια τυχαία πρόκληση (RAND: Random challenge). Αυτές οι παράμετροι, μαζί με το μυστικό κλειδί K, είναι οι μόνες πληροφορίες που χρειάζεται το εξάρτημα AKA για να εκτελέσει τη διαδικασία. Το AUTN είναι μία τιμή 176 bits, που περιέχει 3 υποτιμές, το προϊόν της πράξης XOR (⊕) του αριθμού ακολουθίας (SQN: Sequence Number) και του κλειδιού ανωνυμίας (AK: Anonymity Key), το πεδίο διαχείρισης αυθεντικοποίησης (AMF: Authentication Management Field) και το κωδικό αυθεντικοποίησης μηνύματος (MAC-A: Message Authentication Code).

Η υλοποίηση που ακολουθεί έχει δύο τμήματα, αυτό που εκτελεί την AKA και βρίσκεται μέσα στη USIM, και το άλλο που εκτελεί τον αλγόριθμο κρυπτογραφίας και τη μονόδρομη συνάρτηση κατακερματισμού και είναι ενσωματωμένο στη συσκευή. Υποστηρίζεται από από μια μονάδα ελέγχου, που συντονίζει όλες τις λειτουργίες και διεργασίες που εκτελούνται στο σύστημα. Στο

[2] υποστηρικτικός κόμβος που λειτουργεί ως GPSN (General Packet Radio Service)

τμήμα της συσκευής, χρησιμοποιείται ένας δίαυλος δεδομένων 64 bits, για την εσωτερική μεταφορά δεδομένων. Τα κατάλληλα κλειδιά του αλγορίθμου αποθηκεύονται στη RAM, ενώ οι παράμετροι για τον αλγόριθμο που διαχειρίζεται τις διαδικασίες υπολογισμού του τεμαχίου κλειδιού ροής (*f8*) και του αλγορίθμου που είναι υπεύθυνος για την ακεραιότητα (*f9*), αποθηκεύονται στη ROM. Μέσω της διεπιφάνειας I/O μεταφέρεται πληροφορία από και προς το εξωτερικό περιβάλλον.

Στο τμήμα της USIM, χρησιμοποιείται ένας δίαυλος δεδομένων 8 bits, για την εσωτερική μεταφορά δεδομένων. Οι απαραίτητες παράμετροι αποθηκεύονται στη RAM. Οι διεπιφάνειες I/O χρησιμοποιούνται για την επικοινωνία της USIM με το υπόλοιπο σύστημα.



Αρχιτεκτονική Υλοποίησης Συστήματος Ασφαλείας UTMS σε Υλικό

b) <u>Κρυπτογραφικός Αλγόριθμος Δέσμης Rijndael</u>

Οι μετατροπές της αρχιτεκτονικής του αλγορίθμου εκτελούνται στο ενδιάμεσο αποτέλεσμα, που ονομάζουμε κατάσταση. Αυτή μπορεί να αναπαρασταθεί ως ένας πίνακας, με τα στοιχεία του να είναι bytes. Το πλήθος των γραμμών είναι τέσσερις (4) ενώ το πλήθος των στηλών (N_b) είναι ίσο με το μήκος της δέσμης, διαιρεμένο με 32. Το κλειδί μπορεί επίσης να θεωρηθεί ως ένας πίνακας, με τέσσερις (4) γραμμές και πλήθος στηλών (N_k) ίσο με το μήκος του κλειδιού, διαιρεμένο με 32. Το πλήθος των κύκλων (N_r), εξαρτάται από τα N_b και N_k. Αν η δέσμη και το κλειδί έχουν μήκη ίσα με 128 bits, $N_b = 8$ και $N_k = 8$ και $N_r = 10$.

Η προτεινόμενη αρχιτεκτονική Rijndael απαρτίζεται από τη μονάδα επέκτασης κλειδιού, το κύκλο μεταμόρφωσης βασικής δέσμης, τον αρχικό γύρο και τους αρμόζοντες καταχωρητές. Για την ολοκληρωμένη μεταμόρφωση απλού κειμένου 128 bit, χρειάζονται 41 κύκλοι.

Ο κύκλος μεταμόρφωσης βασικής δέσμης συντίθεται από τέσσερα δομικά στοιχεία, τα S-boxes, την ολίσθηση δεδομένων, την ανάδευση στηλών, και την πρόσθεση κλειδιού. Τα S-boxes εφαρμόζονται στα τμήματα της ROM, ώστε να επιτευχθούν επιδόσεις υψηλής ταχύτητας.

Γενικά, οι συσκευές FPGAs, διαθέτουν εσωτερική ROM (RAM). Στη συγκεκριμένη εφαρμογή, 4 τμήματα ROM θα χρησιμοποιηθούν με διαστάσεις [256 × 8] bits. Η καθυστέρηση των S-boxes προκύπτει 12,8 ns.

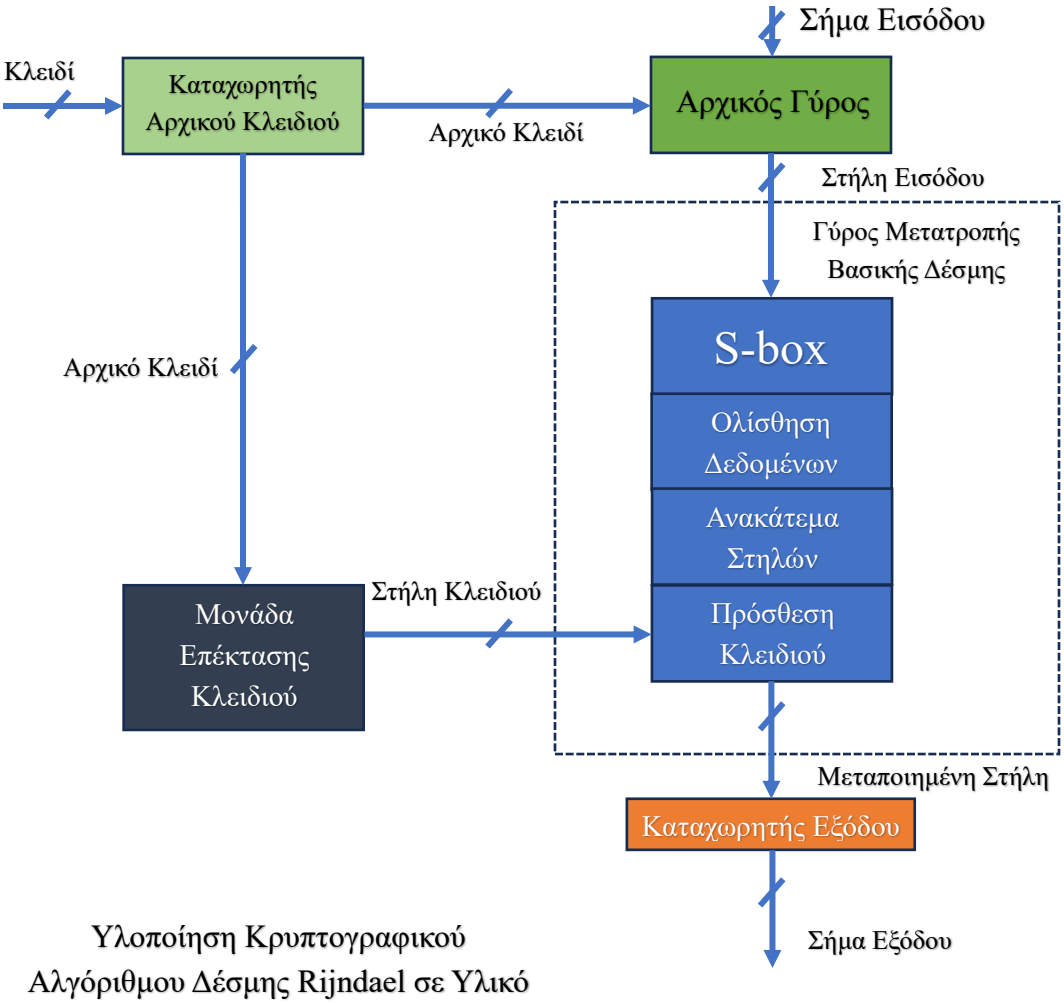
Τα S-boxes απαιτούν δύο διαφορετικές μαθηματικών λειτουργιών, τον πολλαπλασιασμό των ανάστροφων κάθε bit της κατάστασης στο πεπερασμένο πεδίο GF (2^8) και την εγγύς αντιστοίχιση της μετατροπής πάνω στο πεδίο GF (2^8). Η πιο γνωστή αρχιτεκτονική ολοκλήρωσης σε πολύ μεγάλη κλίμακα (VLSI) για την πολλαπλασιαστική αντιστροφή στα GF (2^m) χρησιμοποιεί πίνακες βασικής αναστροφής κελιών δέσμης. Αυτή η σχεδίαση έχει προαπαιτήσεις χώρου και χρόνου. Η εκτέλεση της πολλαπλασιαστικής αντιστροφής στα GF (2^m) χρειάζεται έναν αριθμό κύκλων ανά αντιστροφή, που εκτείνεται από *m* έως *3m+2.* Πρόκειται βέβαια για υψηλές τιμές , οι οποίες δεν γίνονται αποδεκτές σε εφαρμογές υψηλών ταχυτήτων ενός κρυπτογραφικού αλγορίθμου. Η συνάρτηση πολλαπλασιαστικής αντιστροφής παράγει ένα byte, που τροφοδοτείται στην είσοδο της συνάρτησης εγγείως αντιστοίχισης μετατροπής:

$$Output = Input[i]\ XOR\ Input[(i+4)\ mod 8]\ XOR\ Input[(i+5)\ mod 8]\ XOR$$

$$Input[(i+6)\ mod 8]\ XOR\ Input[(i+7)\ mod 8]\ XOR\ C(i)$$

όπου $Input[i]$ το i-οστό bit του byte εισόδου και $C(i)$ το i-οστό bit της σταθεράς

$C = (01100011)$, όπως ορίζεται από τις προδιαγραφές του αλγορίθμου. Τα κλειδιά των κύκλων υπολογίζονται επιτόπου από τη μονάδα επέκτασης κλειδιού. Ως αποτέλεσμα, η διαδικασία παραγωγής κλειδιών δε συνεισφέρουν σε επιπλέον καθυστερήσεις του κρίσιμου μονοπατιού Rijndael.



Υλοποίηση Κρυπτογραφικού Αλγόριθμου Δέσμης Rijndael σε Υλικό

c) ***Ασφάλεια Επιπέδου Ασύρματης Μεταφοράς (WTLS)***

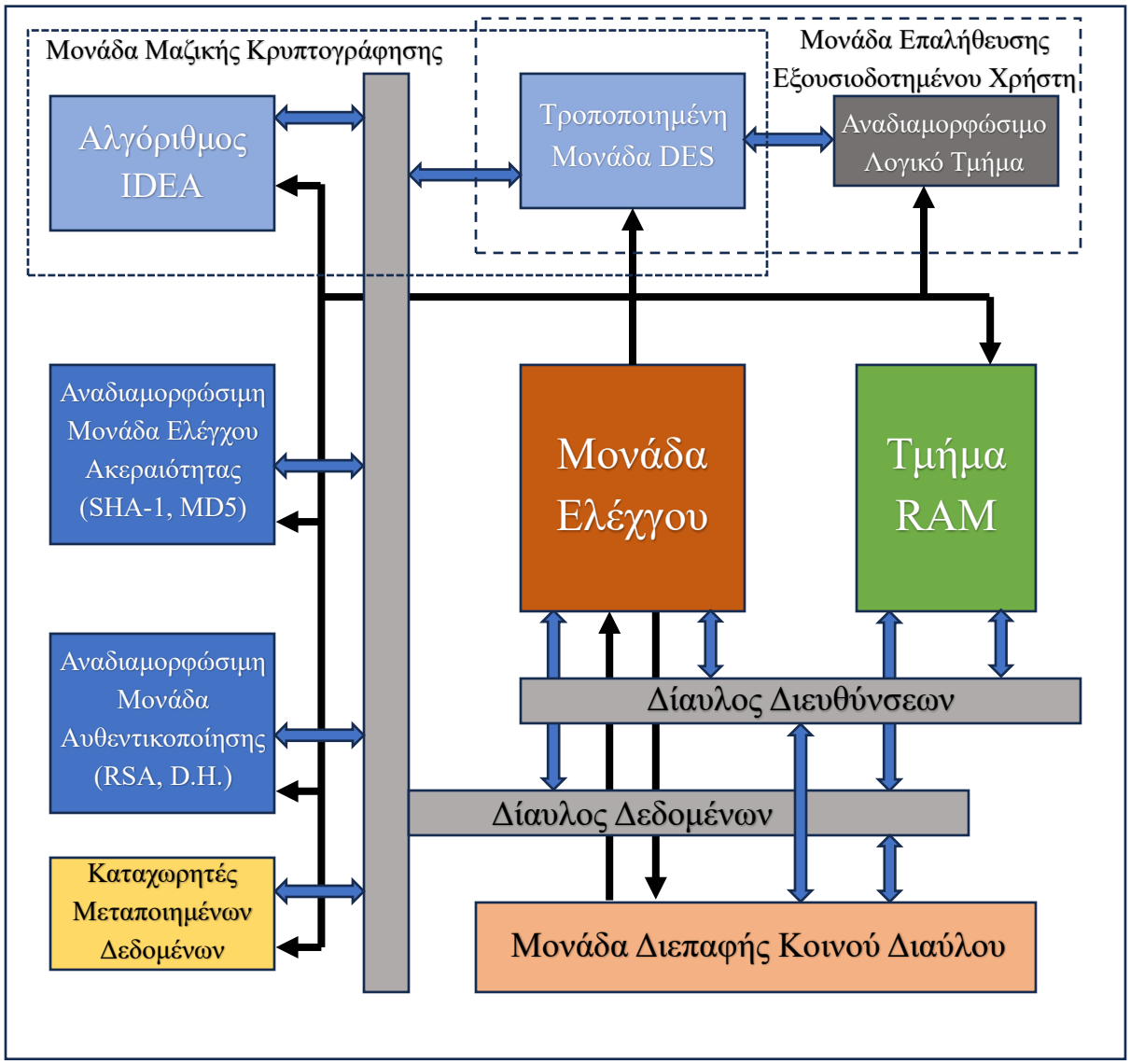
Η WTLS (Wireless Transport Layer Security) είναι το επίπεδο ασφάλειας του Πρωτοκόλλου Ασύρματης Εφαρμογής (WAP: Wireless Application Protocol) και είναι απαραίτητο να υπάρχει κάποιου είδους ασφάλεια για την ασφαλή παροχή υπηρεσιών, και ιδίως αυτών με ευαίσθητα περιεχόμενα, όπως ηλεκτρονική διαχείριση τραπεζών και ηλεκτρονικό εμπόριο.

Ακολουθεί η προτεινόμενη αρχιτεκτονική κρυπτο-επεξεργαστή για την υλοποίηση της WTLS σε υλικό.

Ο προτεινόμενος κρυπτο-επεξεργαστής υποστηρίζει έξι διαφορετικούς αλγόριθμους κρυπτογραφίας. Οι αλγόριθμοι IDEA και DES επιλέγονται για τη μονάδα μαζικής κρυπτογράφησης (bulk encryption unit). Η αναδιαμορφώσιμη μονάδα ελέγχου ακεραιότητας λειτουργεί αποδοτικά με δύο διαφορετικούς τρόπους λειτουργίας για συναρτήσεις κατακερματισμού SHA-1 και MD5. Οι λειτουργίες για τους RSA και Diffie-Hellman εκτελούνται από την αναδιαμορφώσιμη μονάδα αυθεντικοποίησης. Ένα αναδιαμορφώσιμο λογικό τμήμα, σε συνδυασμό με την τροποποιημένη μονάδα DES, υλοποιεί τη μονάδα επαλήθευσης

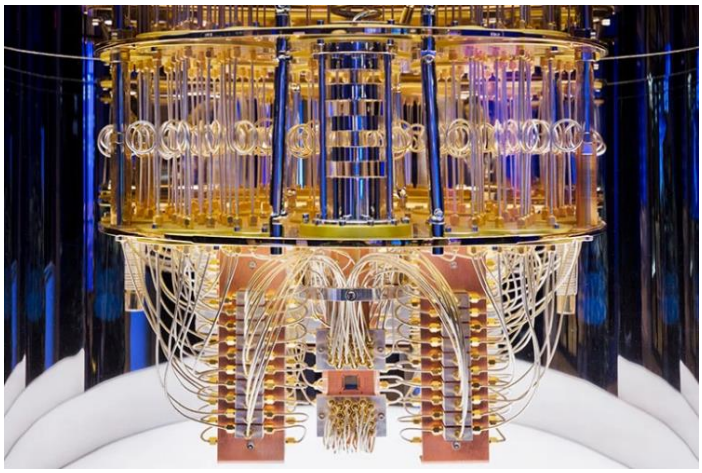
εξουσιοδοτημένου χρήστη. Ένας κοινός δίαυλος δεδομένων των 64 bits και ένας δίαυλος διευθύνσεων των 64 bits χρησιμοποιούνται για τους σκοπούς εσωτερικής μεταφοράς δεδομένων. Έχουν επίσης ενσωματωθεί δύο διαφορετικές μονάδες αποθηκευτικού χώρου. Τα κατάλληλα κρυπτογραφικά κλειδιά αποθηκεύονται και φορτώνονται στα τμήματα της RAM, ενώ τα μεταποιημένα δεδομένα διατηρούνται για όσο χρειάζεται στους αντίστοιχους καταχωρητές. Υλοποιείται επίσης μία μονάδα διεπαφής κοινού διαύλου, που υποστηρίζει σήματα εισόδου των 32 bits και διαύλους διευθύνσεων 32 bits για την αποδοτική επικοινωνία του κρυπτο-επεξεργαστή με το εξωτερικό περιβάλλον, το οποίο μπορεί κάλλιστα να είναι ένας επεξεργαστής γενικής χρήσης ή κάποια συγκεκριμένη CPU.

Το WAP προορίζεται για εφαρμογή κυρίως σε κινητές συσκευές. Εξαιτίας των περιορισμών ολοκλήρωσης σε υλικό, μόνο ένα μέρος των κρυπτογραφικών αλγορίθμων, και όχι όλοι οι αλγόριθμοι που καθορίζονται από τη WTLS, μπορούν να υλοποιηθούν σε κάποιο ευέλικτο ενσωματωμένο σύστημα. Η επιλογή των αλγορίθμων κρυπτογράφησης γίνεται με γνώμονα το υψηλότερο επίπεδο ασφαλείας και τη βέλτιστη επίδοση του υλικού.



4. *Έλευση Κβαντικών Υπολογιστών*

Τις τελευταίες δεκαετίες, ο τομέας της κρυπτογραφίας έχει αναπτυχθεί από ένα δυσνόητο σύνολο στοιχειωδών τεχνικών ανακατέματος σε μία ώριμη, επίσημη επιστήμη. Συνάμα με τις καλύτερες τεχνικές κρυπτογράφησης, αναπτύσσονται και τεχνικές κρυπτανάλυσης. Μία από αυτές τις τεχνικές κρυπτανάλυσης σχετίζονται με τους κβαντικούς υπολογιστές, απειλώντας τα θεμέλια των εγγυήσεων ασφάλειας που η κρυπτογραφία μοχθεί να προσφέρει.



Κβαντικός Υπολογιστής IBM με 127qubits
https://www.nature.com/articles/d41586-021-03476-5

Η υιοθέτηση τέτοιων τεχνικών μετα-κβαντικής κρυπτογραφίας καθιστά μια πρόκληση και στόχος είναι η προστασία οργανισμών (επιχειρήσεως, υπουργείων, μη κερδοσκοπικώς οργανισμών και άλλα).

Εκτιμάται ότι οι κβαντικοί υπολογιστές θα καταρρίψουν τη κρυπτογραφία δημόσιου κλειδιού (public key), χάρη στον αλγόριθμο του Shor. Ως εκ τούτου, τα σύγχρονα συστήματα κρυπτογραφίας είναι αναγκαίο να αντικατασταθούν από αλγόριθμους, που είναι ικανοί να αντισταθούν στη δύναμη των κβαντικών υπολογιστών, γνωστούς και ως μετα-κβαντικούς αλγόριθμους κρυπτογραφίας (PQC: Post Quantum Cryptography). Η έρευνα στο πεδίο της μετα-κβαντικής κρυπτογραφίας ακμάζει τα τελευταία 20 χρόνια, οδηγώντας στη δημιουργία μεγάλης ποικιλίας αλγορίθμων, ικανών να αντισταθούν στη κβαντική απειλή. Οι αλγόριθμοι μετα-κβαντικής κρυπτογραφίας επιλέγονται και προτυποποιούνται από διάφορα σώματα προτυποποίησης. Εντούτοις, ακόμα και με τη καθοδήγηση από αυτούς τους σημαντικούς κόπους, ο κίνδυνος ακόμα ελλοχεύει. Δισεκατομμύρια συσκευές, ανεξαρτήτως παλαιότητας, χρειάζεται να κάνουν τη μετάβαση στο σύνολο των αλγορίθμων PQC. Ακολούθως, η συζήτηση πρόκειται για μία πολυετή διαδικασία μετάβασης, κατά την οποία πρέπει να ληφθούν υπ' όψιν τομείς όπως η ασφάλεια, η επίδοση των αλγορίθμων αυτών, η ευκολία στην ασφαλή εφαρμογή, η συμμόρφωση με τους κανονισμούς και άλλα πολλά.

α) Η κβαντική απειλή στην παραδοσιακή κρυπτογραφία

Οι κύριες μαθηματικές τεχνικές που θεμελιώνουν τα σύγχρονα κρυπτοσυστήματα είναι στενά συνδεδεμένα και βασίζονται στο πρόβλημα παραγοντοποίησης ακεραίων και στο πρόβλημα διακριτού λογαρίθμου. Το 1994 ο μαθηματικός Peter Shor επινόησε έναν κβαντικό αλγόριθμο που υπόσχεται εκθετική επιτάχυνση παραγοντοποίησης ακεραίων και εύρεση διακριτών λογαρίθμων πάνω σε μη κβαντικούς αλγορίθμους, που στη θεωρία επιτρέπει σε ένα κβαντικό υπολογιστεί να «σπάσει» την πλειοψηφία των πλέον χρησιμοποιούμενων κρυπτοσυστημάτων δημόσιου κλειδιού. Δεδομένου αυτού, πολλά από τα τωρινά κρυπτοσυστήματα θα καταρριφθούν όταν φτιαχτούν

επαρκώς μεγάλοι και ανεκτικοί σε σφάλματα (LFT)[3] κβαντικοί υπολογιστές. (Dr. Michele Mosca January 2022)

MIT Technology Review
https://www.technologyreview.com

Κβαντικοί υπολογιστές υπάρχουν και σήμερα, αλλά είναι πολύ στοιχειώδεις και ατελείς μηχανές και είναι απαραίτητη ακόμα αρκετή τεχνολογική πρόοδος, για να επιτευχθεί ευρεία εφαρμογή. Τα εμπόδια για κβαντικούς υπολογισμούς έγκεινται κυρίως στη δημιουργία υλικού (hardware) υψηλής ακρίβειας. Ακόμα και με qubits που εκτελούν βασικές λειτουργίες με αναλογίες σφαλμάτων 0,1%, στο σύνολο τους μέσα στο σύστημα, τα σφάλματα διαδίδονται και αυξάνουν εκθετικά, περιορίζοντας το μέγεθος της χρήσιμης κβαντικής πληροφορίας. Κάθε επιπλέον qubit διπλασιάζει την ισχύ του κβαντικού υπολογιστή και έτσι, όταν η Google AI Quantum ανακοίνωσε κβαντική κυριαρχία στα τέλη του 2019, το πείραμά τους εκτελέστηκε σε επεξεργαστή μόνο 53 qubits. Ο αριθμός των θορυβωδών qubits που κρίνονται απαραίτητα για το «σπάσιμο» του RSA-2048, εκτιμάται ότι είναι περίπου 20 εκατομμύρια.

Συνεπώς, νέες μέθοδοι κρυπτογράφησης είναι απαραίτητες για τη διατήρηση ασφάλειας επικοινωνιών και αποθήκευσης πληροφορίας, εν όψει των κβαντικών απειλών. Παρά το γεγονός ότι υπάρχουν ήδη κβαντικές μέθοδοι κρυπτογραφίας που είναι ικανές να παραμείνουν ασφαλείς απέναντι στους κβαντικούς υπολογιστές, ένα σημαντικό πλεονέκτημα της PQC έναντι των κβαντικών εναλλακτικών είναι ότι τα συστήματα PQC μπορούν να συνδεθούν σε οποιαδήποτε συμβατική συσκευή επικοινωνίας υποδομών ή σύγχρονη συσκευή.

b) <u>Αλγόριθμος του Shor</u>

Διαλέγουμε m, τέτοιο ώστε $n^2 \leq 2^m < 2n^2$. Ξεκινάμε με m qubits, όλα στη κατάσταση 0: $|000000000\rangle$. Αλλάζοντας άξονες, μπορούμε να μετατρέψουμε το πρώτο bit σε γραμμικό συνδυασμό $|0\rangle$ και $|1\rangle$, το οποίο μας δίνει:

$$\frac{1}{\sqrt{2}}(|000000000\rangle + |100000000\rangle)$$

Στη συνέχεια κάνουμε κατά τον ίδιο τρόπο την αντίστοιχη μετατροπή για το δεύτερο bit, το τρίτο και ου το καθεξής μέχρι το n-οστό, βρίσκοντας τη κβαντική κατάσταση:

$$\frac{1}{\sqrt{2^m}}(|000000000\rangle + |000000001\rangle + |000000010\rangle + \cdots + |111111111\rangle)$$

Συνεπώς, όλες οι πιθανές καταστάσεις των m qubits είναι υπερτεθειμένες σε αυτό το άθροισμα. Για απλότητα στο συμβολισμό, αντικαθιστούμε κάθε σειρά από 0 και 1 με το δεκαδικό τους αντίστοιχο, οπότε έχουμε:

[3] LFT: Large & Fault-Tolerant

$$\frac{1}{\sqrt{2^m}}(|0\rangle + |1\rangle + |2\rangle + \cdots + |2^m - 1\rangle)$$

Διαλέγουμε έναν τυχαίο αριθμό a που να ισχύει $1 < a < n$. Μπορούμε να υποθέσουμε ότι $gcd(a, n) = 1$, αλλιώς έχουμε συντελεστή του n. Ο κβαντικός υπολογιστής υπολογίζει τη συνάρτηση $f(x) = a^x \ (mod\ n)$ για αυτή τη κβαντική κατάσταση, για να εξάγει:

$$\frac{1}{\sqrt{2^m}}\left(|0, a^0\rangle + |1, a^1\rangle + \left|2, a^2\right\rangle + \cdots + \left|2^m - 1, a^{2^m-1}\right\rangle\right)$$

όπου a^x χρησιμοποιείται για να συμβολίζει το $a^x \ (mod\ n)$, για χάρη ευκολίας συμβολισμού. Από αυτό προκύπτει η λίστα όλων των τιμών του a^x. Εντούτοις, μέχρι στιγμής δε βλέπουμε καλύτερα αποτελέσματα από αυτά που δίνει ένας συμβατικός ηλεκτρονικός υπολογιστής.

Αν πρόκειται να μετρήσουμε τη κατάσταση του συστήματος, αποκτάμε μία βασική κατάσταση $|x_0, a^{x_0}\rangle$ για κάποιο τυχαία επιλεγμένο x_0. Δεν μπορούμε καν να καθορίσουμε ποιο x_0 θέλουμε να χρησιμοποιήσουμε. Επιπροσθέτως, το σύστημα ωθείται σε αυτή τη κατάσταση, εξολοθρεύοντας όλες τις υπόλοιπες τιμές του a^x που υπολογίστηκαν προηγουμένως. Άρα, δεν επιθυμούμε να μετρήσουμε όλο το σύστημα. Αντίθετα, Κρατάμε μόνο την τιμή του δεύτερου μισού. Κάθε βασικό τεμάχιο έχει μορφή $|x_0, a^x\rangle$, όπου το x αναπαριστά m bits και το a^x αναπαρίσταται από $\frac{m}{2}$ bits (εφόσον $a^x \ (mod\ n) < n < 2^{\frac{m}{2}}$) Αν μετρήσουμε τα τελευταία $\frac{m}{2}$ bits, λαμβάνουμε κάποιον αριθμό $u \ (mod\ n)$ και ολόκληρο το σύστημα ωθείται σε ένα συνδυασμό αυτών των καταστάσεων, της μορφής $|x, u\rangle$ όπου $a^x \equiv u \ (mod\ n)$:

$$\frac{1}{C} \sum_{\substack{0<x<2^m \\ a^x \equiv u\ (mod\ n)}} |x, u\rangle$$

όπου C οποιοσδήποτε παράγοντας είναι απαραίτητος ώστε το διάνυσμα να έχει μήκος 1 (για την ακρίβεια, το C είναι η τετραγωνική ρίζα του αριθμού των όρων στο άθροισμα.

c) <u>Η καταστροφική επίδραση του αλγόριθμου του Shor</u>

Στο δημοφιλές σύστημα δημόσιου κλειδιού RSA, το δημόσιο κλειδί είναι προϊόν $N = pq$ των δύο κρυφών πρώτων αριθμών p και q. Η ασφάλεια ενός τέτοιου συστήματος εξαρτάται σημαντικά από τη δυσκολία εύρεσης των παραγόντων p και q. Παρά το γεγονός αυτό, το 1994, ο Shor εισήγαγε ένα ταχύ κβαντικό αλγόριθμο που βρίσκει την παραγοντοποίηση πρώτων αριθμών οποιουδήποτε θετικού ακεραίου N.

Ο αλγόριθμος του Shor εκτιμά μία περιοδική συνάρτηση σε μία υπέρθεση όλων των τιμών στην είσοδο εντός ευρέος φάσματος, εφαρμόζει μετασχηματισμό Fourier για να αποκτήσει μία εκτιμώμενη υπέρθεση περιόδων της συνάρτησης και μετρά την υπέρθεση για να βρει μία τυχαία περίοδο. Η περιοδική συνάρτηση είναι $e \mapsto a^e \ mod\ N$, όπου a ένας τυχαίος ακέραιος αριθμός, σχετικά πρώτος στο N, το βελάκι υποδηλώνει «ανάθεση σε» και "$mod\ N$" δηλώνει το υπόλοιπο της διαίρεσης με N. Αν ο N δεν είναι δύναμη ενός πρώτου αριθμού (εύκολα αναγνωρίσιμη

περίπτωση), τότε η τυχαία περίοδος αποκαλύπτει έναν παράγοντα του N με αρκετά υψηλή πιθανότητα να αποτελέσει πρόβλημα ασφαλείας.

Ο Shor εισήγαγε στη συζήτηση έναν παρόμοιο αλγόριθμο για την εύρεση περιόδων της συνάρτησης $e, f \mapsto g^e h^f \bmod p$, που αποκαλύπτει το k, τέτοιο ώστε $h = g^k \bmod p$. Αντικαθιστώντας τον πολλαπλασιασμό του $\bmod p$ με πρόσθεση σημείων ελλειπτικής καμπύλης $\bmod p$, σπάει ο αλγόριθμος ECC, δημοφιλής εναλλακτική του RSA.

Όταν αυτοί οι αλγόριθμοι εφαρμόζονται σε ευρέως χρησιμοποιούμενα μεγέθη δημόσιων κλειδιών RSA και ECC, απαιτούν δισεκατομμύρια λειτουργίες σε χιλιάδες λογικά qubits. Επιθέσεις FT μάλλον θα χρειάζονται τρισεκατομμύρια λειτουργίες σε εκατομμύρια qubits με φυσική υπόσταση. Ίσως οι κβαντική υπολογιστική συναντήσει θεμελιώδη εμπόδια, που θα την εμποδίσει στο να κλιμακώσει επιτυχώς σε τέτοια μεγέθη. Πάντως δεν εντοπιστεί φανεί τέτοια εμπόδια και η συνετή διαχείριση διακινδύνευσης απαιτεί πρόληψη σε περίπτωση που τέτοιου είδους επιθέσεις αποβούν επιτυχείς.

d) <u>Αποθήκευσε-Τώρα-Αποκωδικοποίησε-Αργότερα</u>

Οι επιθέσεις SNDL (store-now-decrypt-later) προβάλλουν απειλή για πληροφορία που είναι τώρα κρυπτογραφημένη, χρησιμοποιώντας κβαντικά ευάλωτη κρυπτογραφία. Τέτοιου τύπου κρυπτογραφημένα δεδομένα, τα οποία μεταδίδονται μέσω της δημόσιας υποδομής του διαδικτύου, μπορούν να συλλεχθούν, να αποθηκευτούν επ' άπειρον και αν αποκρυπτογραφηθούν μελλοντικά όταν ο κακόβουλος θα έχει πρόσβαση σε ένα LFT κβαντικό υπολογιστή. Σε κάποιες περιπτώσεις, δεν πρόκειται για κάτι το οποίο μας ανησυχεί ιδιαίτερα. Εντούτοις, υπάρχουν κάποια σημαντικά εμπορικά μυστικά, ιατρικά ιστορικά, έγγραφα που αφορούν τη κρατική ασφάλεια και άλλα πολλά δεδομένα που έχουν πολυετείς κύκλους ζωής για την αποθήκευσή τους και πρέπει να παραμείνουν εμπιστευτικά για εκτενείς χρονικές περιόδους.

Αντιλαμβανόμαστε τη κρισιμότητα της κατάστασης, διαβάζοντας το υπόμνημα του Λευκού Οίκου των Η.Π.Α. προς τους διευθυντές των προϊσταμένων εκτελεστικών τμημάτων και πρακτορείων σχετικά με τη «Μετάβαση στη Μετα-Κβαντική Κρυπτογραφία», το οποίο παρέχει καθοδήγηση για τα πρακτορεία να συμμορφωθούν με το Υπόμνημα 10 (NSM-10)[4], για την «Προώθηση της Πρωτιάς των Η.Π.Α. στους Κβαντικούς Υπολογιστές παράλληλα με τη Μετρίαση Διακινδύνευσης στα Ευάλωτα Κρυπτογραφικά Συστήματα»[5]. (Young 2022)

Ενισχύεται η ζωτικότητα της υπόθεσής μας με τον Sundar Pichai, διευθύνων σύμβουλο της Google και της Alphabet, ο οποίος σε συνέντευξη που έδωσε στο World Economic Forum το 2020 ανέφερε «Σε ένα χρονικό παράθυρο 5-10 ετών, οι κβαντικοί υπολογιστές θα σπάσουν τη κρυπτογραφία όπως τη γνωρίζουμε σήμερα.» και «Μπορούμε να δουλέψουμε γύρω από αυτό. Μπορούμε να κάνουμε κβαντική κρυπτογραφία.», ισχυριζόμενος ότι ο συνδυασμός κβαντικών υπολογιστών και τεχνητής νοημοσύνης θα μας βοηθήσει να επιλύσουμε πολλά από τα προβλήματα που έχουμε σήμερα, αλλά φυσικά θα υπάρξουν εμπόδια. Η αναφορά γίνεται φυσικά και για τους κακόβουλους «ωτακουστές», που εν δυνάμει θα χρησιμοποιήσουν τους κβαντικούς υπολογιστές για τη

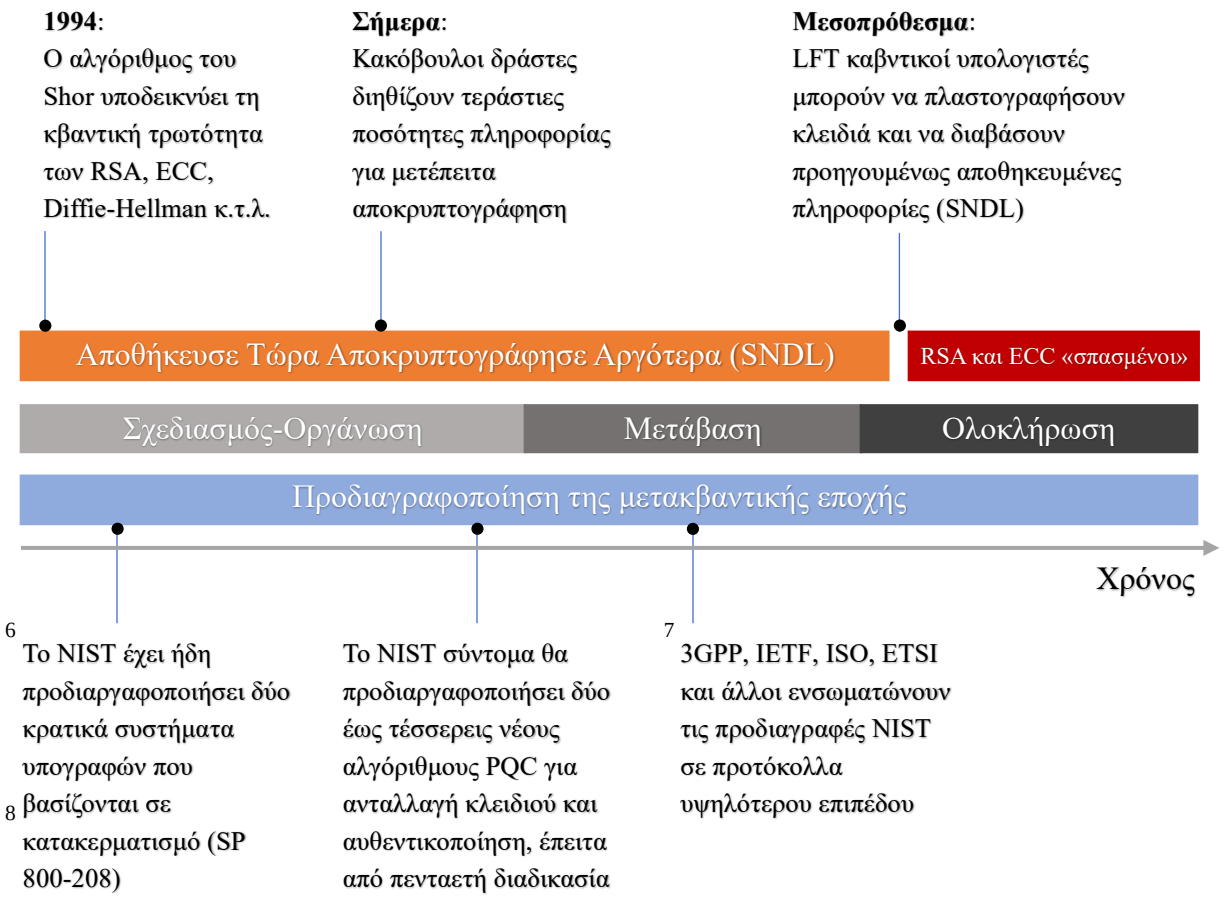
[4] National Security Memorandum 10 (NSM-10)
[5] Migrating to Post-Quantum Cryptography (whitehouse.gov)

κατάρριψη των σύγχρονων τεχνικών κρυπτογραφίας, ώστε να αποκτήσουν πρόσβαση σε ευαίσθητες πληροφορίες. (Video 2020)

5. Χρονισμός Μετάβασης σε PQC

Όταν μιλάμε για κβαντικές επιθέσεις, είναι φυσικό να διερωτηθούμε πότε πρέπει να ξεκινήσει η μετάβαση προς τη PQC. Δεδομένου ότι οι LFT κβαντικοί υπολογιστές δεν είναι ακόμα διαθέσιμοι, όλα τα δεδομένα υποδεικνύουν ότι η μετάβαση πρέπει να ξεκινήσει άμεσα.

α) Το χρονοδιάγραμμα μετάβασης σε PQC



Τα τρία χρονοδιαγράμματα χωρίζονται ως εξής: η άνω γραμμή αναπαριστά τις απειλές για τη κρυπτογραφία, η μεσαία τα βήματα από τα οποία θα πρέπει να περάσουν οι οργανισμοί κατά τη

[6] NIST: National Institute of Standards and Technology
[7] The Mobile Broadband Standard (https://www.3gpp.org/), Internet Engineering Task Force (https://www.ietf.org/), International Organization for Standardization (https://www.iso.org/home.html), European Telecommunications Standards Institute (https://www.etsi.org/)
[8] https://csrc.nist.gov/publications/detail/sp/800-208/final

διάρκεια της μετάβασης και η κάτω τα στάδια προδιαγραφοποίησης, που ηγείται από πολυεθνικά σώματα προδιαγραφοποίησης.

Το άνω χρονοδιάγραμμα καταγράφει τις δύο πιο σημαντικές απειλές και πότε θα φτάσουν κρίσιμη σημασία. Η πρώτη, γνωστή και ως απειλή Store-Now-Decrypt-Later, είναι ενεργή σήμερα. Κακόβουλοι καταγράφουν πολύτιμες πληροφορίες τώρα, τις αποθηκεύουν και τις αποκρυπτογραφούν αργότερα, όταν γίνουν διαθέσιμοι οι LFT κβαντικοί υπολογιστές. Φυσικά, η επίθεση SNDL προϋποθέτει ότι η αποθηκευμένη πληροφορία θα παραμείνει πολύτιμή στο μέλλον. Η δεύτερη κβαντική απειλή αναφέρεται στη δυνατότητα κατάρριψης των RSA και ECC, των δύο πιο διαδεδομένων αλγορίθμων δημόσιου κλειδιού για κρυπτογράφηση πληροφορίας σήμερα, που ο αλγόριθμος του Shor μπορεί να «σπάσει». Αυτό θα επέτρεπε στους κακόβουλους να πλαστογραφήσουν τις ψηφιακές υπογραφές RSA και ECC και προβάλλουν κίνδυνο σε συστήματα που στηρίζονται σε αυτά, όπως ασφαλής πλοήγηση διαδικτύου, αρχιτεκτονικές Zero Trust (μηδενικής εμπιστοσύνης)[9] και κρυπτονομίσματα.

Το μεσαίο χρονοδιάγραμμα αναπαριστά τις δύο δράσεις που απαιτούνται από οργανισμούς κατά τη μετάβαση στη PQC. Το πρώτο μέρος αφορά το στρατηγικό σχεδιασμό και τον τεχνολογικό πειραματισμό για αυτή τη μετάβαση, ενώ το δεύτερο αφορά την αποδοτική υιοθέτηση της PQC σε παραγόμενα συστήματα. Είναι σημαντικό ότι η στρατηγική φάση σχεδίασης πρέπει να έχει ολοκληρωθεί πολύ πριν οι LFT κβαντικοί υπολογιστές σταθούν ικανοί να επιτεθούν τους αλγόριθμους RSA και ECC.

Τέλος, το κάτω χρονοδιάγραμμα αφορά τις διαδικασίες προδιαγραφοποίησης που ενορχηστρώνονται από κυβερνητικά και βιομηχανικά σώματα, με ιδιαίτερη έμφαση στη PQC διαδικασία καθορισμού θεμελιώδους ασφαλείας NIST.

b) <u>Μακροπρόθεσμα Σχέδια</u>

Ένας ακόμα λόγος που καθιστά τη μετάβαση σε PQC άμεσης σημασίας, είναι τα σχέδια για τεχνολογικά αντικείμενα και υποδομές, με μεγάλο κύκλο ζωής (πολλών δεκαετιών). Τα οχήματα είναι καλό παράδειγμα, αφού οι κατασκευαστές αυτοκινήτων, πλοίων, αεροσκαφών και τραίνων υπό κατασκευή τώρα, αναμένεται να χρησιμοποιηθούν έως και 20 ή ακόμα και 30 χρόνια. Σε κάποιες περιπτώσεις, περιέχουν μετρητές, όπου το ένα κρυπτοσύστημα θα μπορεί να αντικατασταθεί με κάποιο άλλο, δίχως να ισχύει για όλα. Σε αυτόν τον τομέα ακριβώς φαίνεται η ευελιξία και η χρησιμότητα υλικού για συγκεκριμένες εφαρμογές (ASICs), το οποίο χρησιμοποιείται για την υλοποίηση κρυπτογραφίας και παραμένει αμετάβλητο στον χρόνο.

Τα σχέδια σημαντικών εθνικών υποδομών είναι ένα ακόμα παράδειγμα, που απαιτείται υψηλή διαθεσιμότητα, με κάποιες υποδομές να απαιτούν 99,999% διαθεσιμότητα ή περιθώριο 6 λεπτά το χρόνο που να μη λειτουργεί το σύστημα), και η αναβάθμιση του κρυπτογραφικού λογισμικού/υλικού αναπαρίσταται από ανεπίτρεπτο κόστος.

[9] https://www.nist.gov/publications/zero-trust-architecture

6. Συμπεράσματα

Το απόρρητο και η ασφάλεια των ψηφιακών επικοινωνιών είναι αδιαπραγμάτευτο αγαθό/δικαίωμα. Η πάλη για τη διασφάλισή τους υποστηρίζεται από ένα σύνολο επιστημών, είτε αυτό είναι τα Μαθηματικά για τη μοντελοποίηση των αλγορίθμων κρυπτογραφίας, είτε η Επιστήμη Υπολογιστών για την υλοποίηση αυτών σε πραγματικά συστήματα, είτε η Νομική για τη θέσπιση των Νομικών Πλαισίων.

Η κρυπτογραφία είναι το εργαλείο, με το οποίο προσπαθούμε να διατηρούμε ασφαλή τα δεδομένα που διαδίδονται στο δημόσιο ιστό του διαδικτύου. Έχουμε στη διάθεσή μας πολλούς αλγορίθμους που είναι ικανοί να μας προστατεύσουν προς το παρόν, αλλά επειδή δεν παύουν να υπάρχουν κακόβουλοι, πρέπει να βλέπουμε στο μέλλον και να προετοιμαζόμαστε για τα χειρότερα σενάρια.

Είδαμε πως δύο από τους πιο δημοφιλείς αλγορίθμους κρυπτογραφίας, οι RSA και ECC, θα μπορούσαν να καταρρεύσουν με την έλευση των κβαντικών υπολογιστών, όταν δηλαδή φτάσουν σε σημείο να είναι αρκετά ισχυροί, προσβάσιμοι και σταθεροί. Αν ένας συμβατικός υπολογιστής λειτουργούσε ακατάπαυστα, θα χρειαζόταν 300 τρισεκατομμύρια χρόνια να σπάσει τον RSA-2048, ενώ ένας τέλειος κβαντικός υπολογιστής με 4099 σταθερά qubits, θα τον έσπαγε σε 10 δευτερόλεπτα. (QuintessenceLabs χ.χ.) Το 2021, περισσότεροι από του μισούς ειδικούς που ερωτήθηκαν κατά τη διάρκεια έρευνας, πιστεύουν ότι υπάρχει πιθανότητα μεγαλύτερη από 50% εντός των επόμενων 15 ετών, οι κβαντικοί υπολογιστές LFT να σπάσουν τη κρυπτογραφία παραγοντοποίησης ακεραίων και διακριτού λογαρίθμου. Πιθανές λύσεις, όπως η PQC, είναι υπό έρευνα εδώ και πολλά χρόνια και οι προσπάθειες συνεχίζονται για ένα ασφαλές ψηφιακό περιβάλλον για τα ερχόμενα έτη. (Craig Gidney χ.χ.)

Βιβλιογραφία

Craig Gidney, Martin Ekerå. χ.χ. «How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.» https://arxiv.org/abs/1905.09749.

Daniel J. Bernstein, Tanja Lange. 2017. «Post-quantum cryptography.» *Nature.*

David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, Royal Hansen. 2022. «Transitioning organizations to post-quantum cryptography.» *Nature.*

Dr. Michele Mosca, Dr. Marco Piani. January 2022. «2021 Quantum Threat .» *Global Risk Institute.*

John Preuβ Mattsson, Pinar Comak, Ferhat Karakoç. χ.χ. *The evolution of cryptography in mobile networks and how to secure them in the future.*

Kak, Avi. 2023. *Public-Key Cryptography and the RSA Algorithm.* Avinash Kak, Purdue University.

Liyanage Madhusanka, Ahmad Ijaz, Abro Ahmed Bux, Gurtov Andr. 2018. *A Comprehensive Guide to 5G Security.* John Wiley & Sons, Ltd.

χ.χ. *National Institute of Standards and Technology.* https://www.nist.gov/.

Nicolas Sklavos, Xinmiao Zhang. 2007. *Wireless Security and Cryptography Specifications and Implementations.* CRC Press.

NIST. 2022. «5G Cybersecurity.» https://www.nccoe.nist.gov/5g-cybersecurity.

Patrik Ekdahl, Alexander Maximov. χ.χ. *Encryption in virtualized 5G environments.*

Qian, Yi. 2020. «5G Wireless Communication Networks Challenges in Security and Privacy.» *IEEE Wireless Communications* (IEEE Wireless Communications) 27 (4).

QuintessenceLabs. χ.χ. «Breaking RSA Encryption - an Update on the State-of-the-Art.» https://www.quintessencelabs.com/blog/breaking-rsa-encryption-update-state-art#:~:text=It%20would%20take%20a%20classical,%E2%80%9Csafe%E2%80%9D%20from%20these%20attacks.

R. Chen, C. Li, S. Yan, R. Malaney and J. Yuan. 2019. «Physical Layer Security for Ultra-Reliable and Low-Latency Communications.» *IEEE Wireless Communications* 26 (5).

Schneier, Bruce. 2017. *Applied Cryptography Protocols, Algorithms and Source Code in C.* Wiley.

Stallings, William. 2005. *Cryptography and Network Security Principles and Practices.* Prentice Hall.

Video, World Economic Forum. 2020. «An Insight, An Idea with Sundar Pichai - Quantum Computing.»

Wade Trappe, Lawrence C. Washington. 2020. *Introduction to Cryptography with Coding Theory.* Pearson.

Young, Shalanda D. 2022. «Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems .» 18 November. https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf.