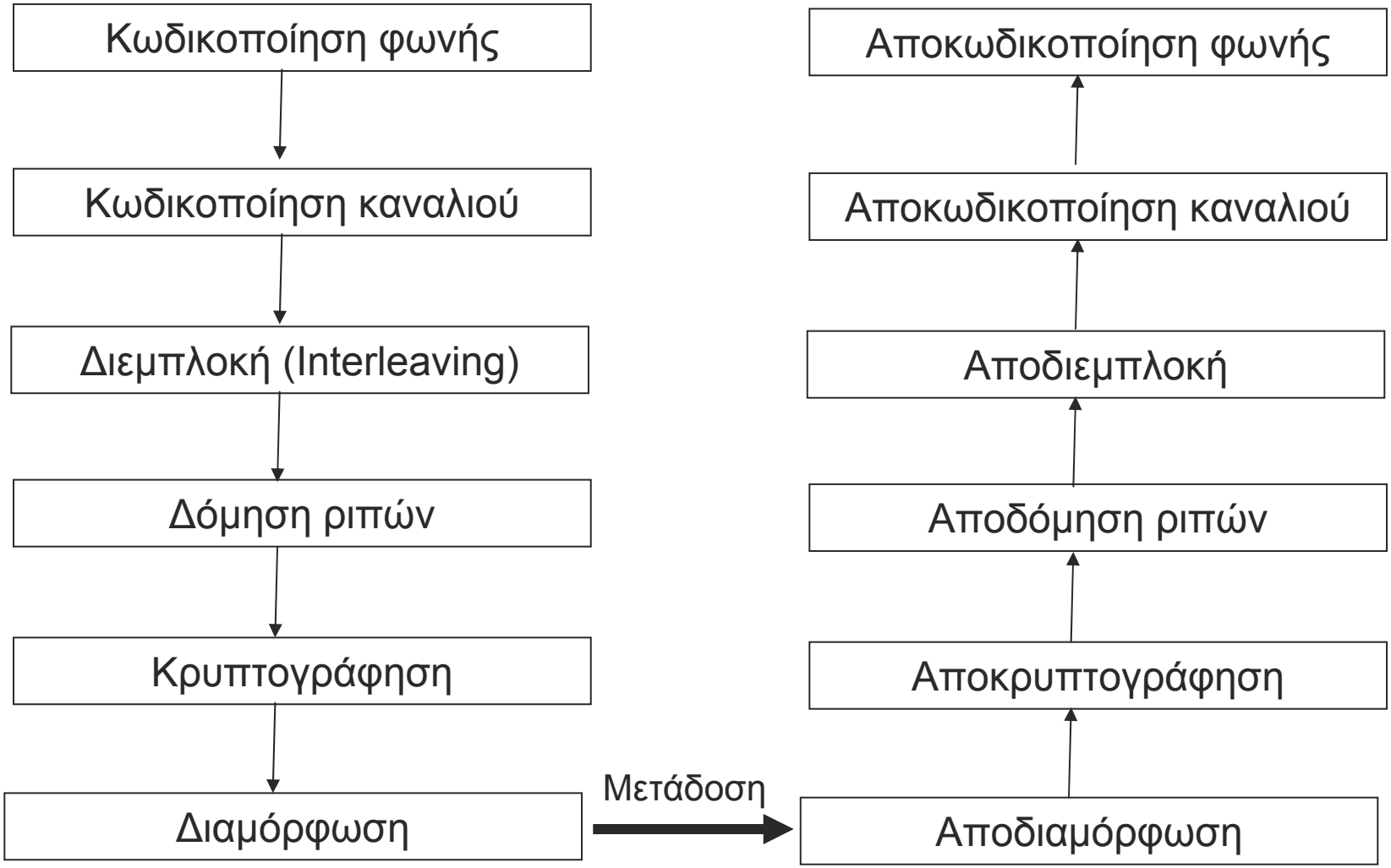
Κινητές επικοινωνίες

Κεφάλαιο 5

Ψηφιοποίηση φωνής, μετάδοση δεδομένων και ασφάλεια στο GSM

Από την πηγή πληροφορίας στα ραδιοκύματα

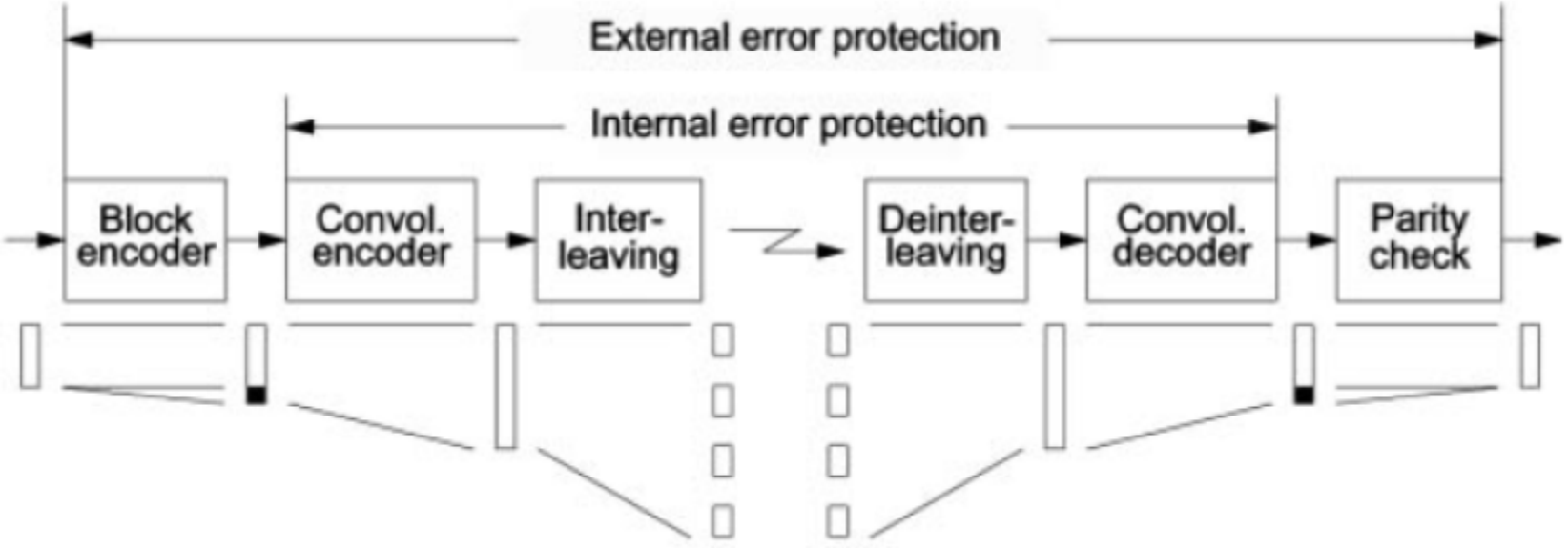


Κωδικοποίηση φωνής

- Η φωνή δειγματολειπτείται με ρυθμό 8000 δείγματα ανά sec. Κάθε δείγμα ψηφιοποιείται σε 13 bits (ο κωδικοποιητής κωδικοποιεί με 16 bit ανά δείγμα, αλλά το GSM αγνοεί 3 bit). Άρα, ο ρυθμός είναι 104Kbit/sec.
- Στην είσοδο του κωδικοποιητή, 160 ομάδες των 13 bit φτάνουν μέσα σε ένα διάστημα 20msec. Ο κωδικοποιητής συμπιέζει τα δεδομένα αυτά, μετατρέποντάς τα σε μπλοκ των 260 bit (άρα, ρυθμός 13kbit/sec). Έχουμε λοιπόν μία συμπίεση της τάξης 1:8.
- Η συμπίεση γίνεται με τον αλγόριθμο που λέγεται Regular Pulse Excitation - Long term Prediction – Linear Predictive Coder (RPE-LTP). Βασίζεται στο ότι χρησιμοποιούνται προηγούμενα δείγματα για την πρόβλεψη των επομένων, λόγω του ότι σε πολύ μικρό χρονικό διάστημα η πληροφορία αλλάζει ελάχιστα. Στην ουσία, δεν ψηφιοποιείται το δείγμα αυτό καθ' αυτό, αλλά η διαφορά του από το προηγούμενο δείγμα (κάτι που απαιτεί πολύ λιγότερα bit)

Κωδικοποίηση καναλιού

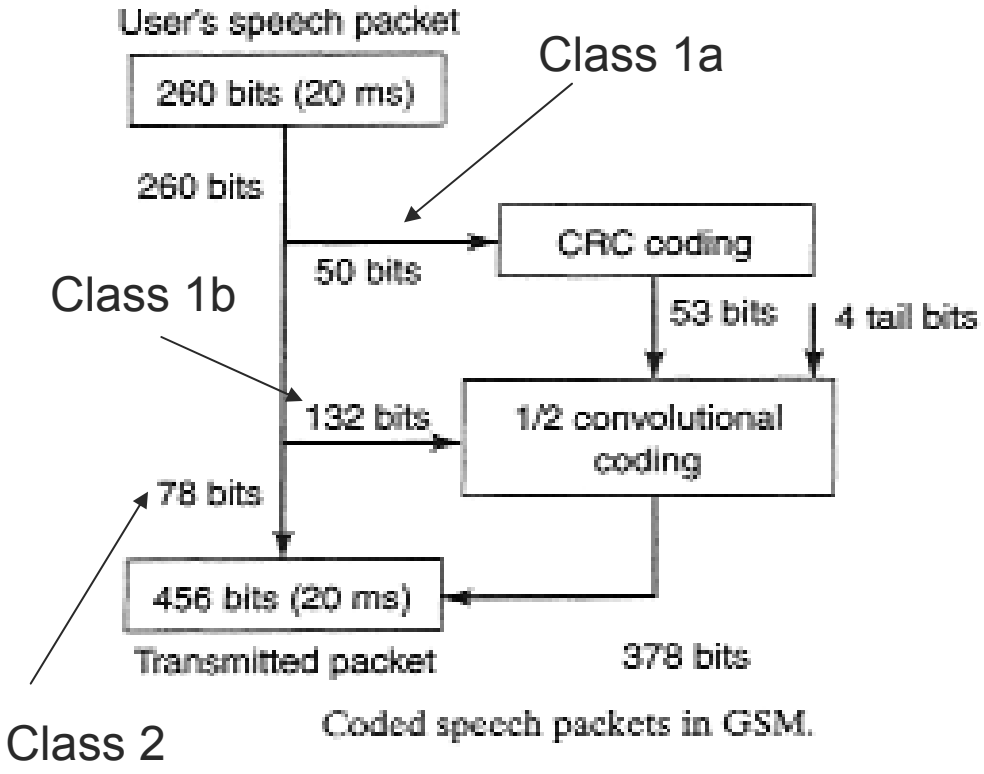
- Αντίθετα με την κωδικοποίηση φωνής, εδώ προστίθενται bit (αντί να συμπιέζονται) για τη διόρθωση σφαλμάτων κατά τη μετάδοση (συνήθως, το ασύρματο κανάλι έχει BER από 10^{-3} έως 10^{-1}, ενώ εμείς επιθυμούμε να είναι της τάξης 10^{-5}).



Περιγραφή κωδικωποιήσεων

- Χρησιμοποιείται και συγκεραστικός κώδικας (convolutional code) και κώδικας τμήματος (block code)
- Τα μπλοκ ομιλίας μεγέθους 260 bit από τον κωδικοποιητή φωνής (που αντιστοιχούν σε χρόνο 20msec), χωρίζονται σε τρεις κλάσεις:
  - class 1a : 50 bits
    - Κωδικοποιούνται με κώδικα τμήματος, ο οποίος επισυνάπτει 3 bit ισοτιμίας
  - class 1b : 132 bits
    - Κωδικοποιούνται μαζί με τα 1a bits (+ τα 3 bit ισοτιμίας) μέσα από έναν συγκεραστικό κωδικοποιητή ρυθμού ½.
  - class 2 : 78 bits
    - Δεν κωδικοποιούνται – απλά επισυνάπτονται στο τελικό αποτέλεσμα

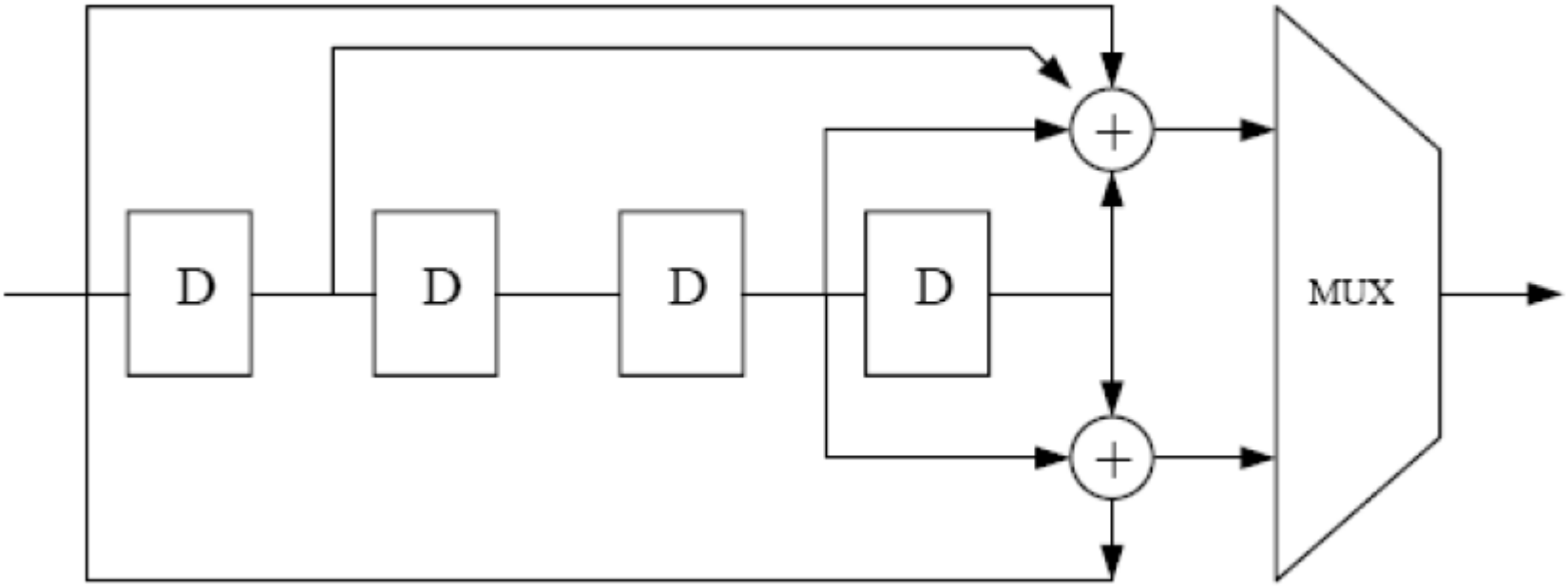
Σχηματική αναπαράσταση κωδικοποιήσεων



Coded speech packets in GSM.

- Κάθε bit που μπαίνει στον συγκεραστικό κώδικα, παράγει 2 bit στην έξοδο (ρυθμός ½)
- Τα 456 bits τελικά αντιστοιχούν σε 22.8kbps
- Τα 456 bit χωρίζονται σε 8 block των 57 ριπών. Αυτά στη συνέχεια αποτελούν την πληροφορία σε 4 ριπές. Για να δομήσουν όμως τις ριπές, πρώτα διαπλέκονται (δηλαδή, με απλά λόγια, «ανακατώνονται»). Για την περιγραφή αυτής της διαδικασίας, ανατρέξτε στο Κεφάλαιο 3, σελίδα 23 των σημειώσεων)

Σχήμα συγκεραστικού κωδικοποιητή



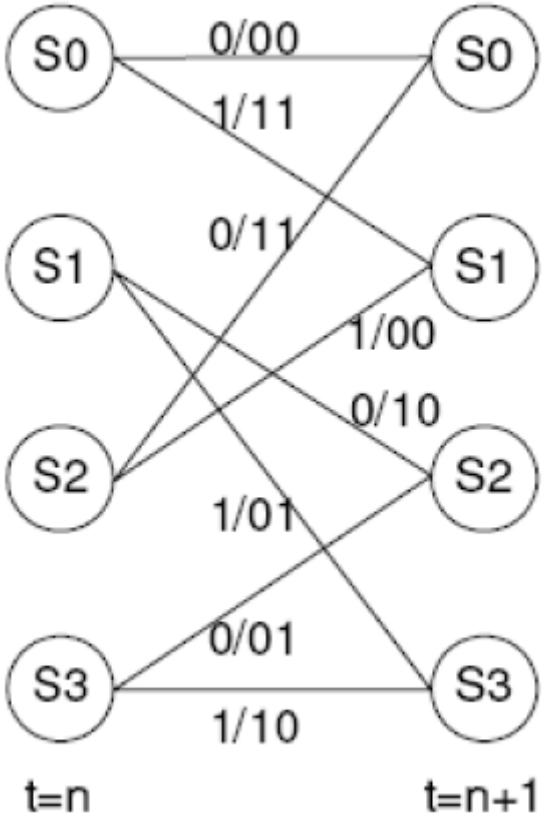
- Κάθε χρονική στιγμή, οι δύο έξοδοι εξαρτώνται από την τρέχουσα κατάσταση του καταχωρητή και το bit εισόδου. Η αναλυτική περιγραφή της λειτουργίας δίνεται στην επόμενη διαφάνεια

Πίνακας καταστάσεων/εξόδου του συγκεραστικού κωδικοποιητή

FSM State		Next State		Output Symbol	
		in = 0	in = 1	in = 0	in = 1
S0	0000	0000	1000	00	11
S1	0001	0000	1000	11	00
S2	0010	0001	1001	11	00
S3	0011	0001	1001	00	11
S4	0100	0010	1010	00	11
S5	0101	0010	1010	11	00
S6	0110	0011	1011	11	00
S7	0111	0011	1011	00	11
S8	1000	0100	1100	10	01
S9	1001	0100	1100	01	10
S10	1010	0101	1101	01	10
S11	1011	0101	1101	10	01
S12	1100	0110	1110	10	01
S13	1101	0110	1110	01	10
S14	1110	0111	1111	01	10
S15	1111	0111	1111	10	01

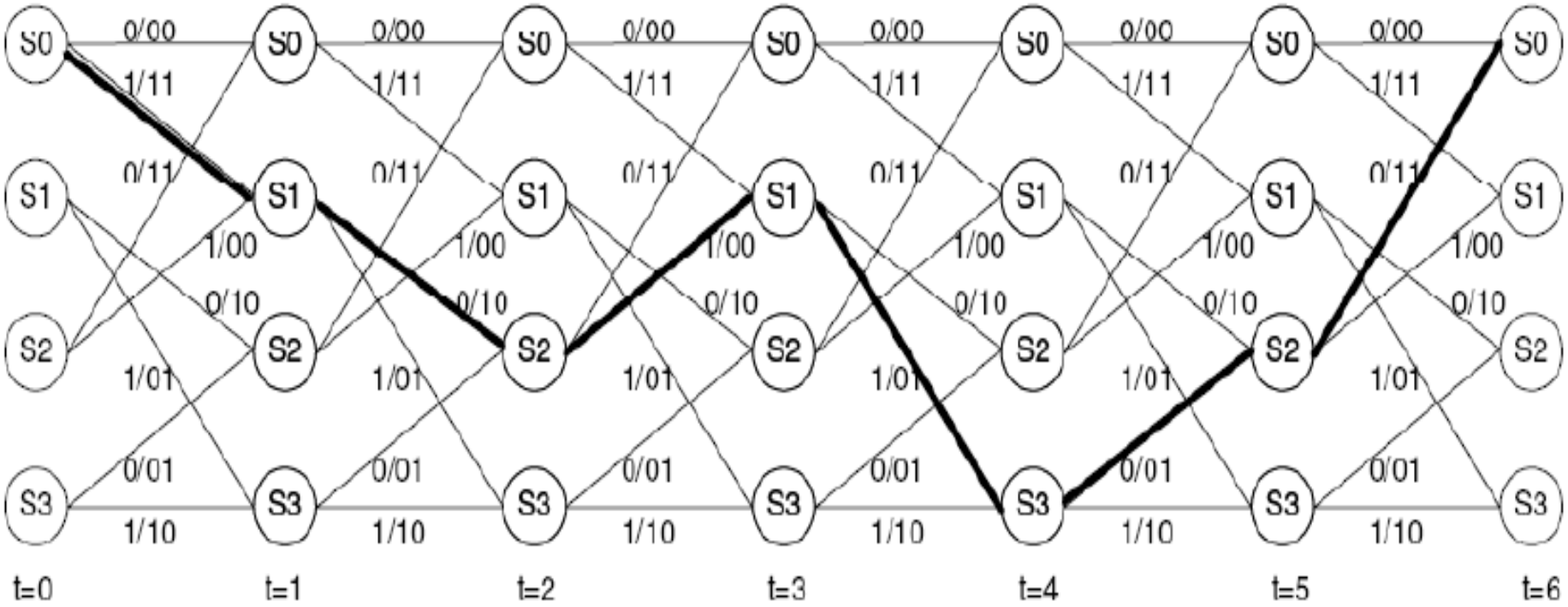
Διάγραμμα trellis

- Αντί για τον προηγούμενο πίνακα, μπορούμε να χρησιμοποιήσουμε το διάγραμμα Trellis για να περιγράψουμε τον συγκεραστικό κώδικα.
- Π.χ. για έναν απλοποιημένο συγκεραστικό κώδικα, με 4 καταστάσεις (άρα, δύο θέσεις μνήμης), μπορεί να έχουμε το εικονιζόμενο διάγραμμα trellis:
  - Από κάθε κύκλο (κατάσταση) φεύγουν δύο γραμμές. Η πρώτη αντιστοιχεί στο τι γίνεται αν έρθει είσοδος 0, η δεύτερη στο τι γίνεται αν έρθει είσοδος 1
  - Ο συμβολισμός a/bc πάνω από τις γραμμές (π.χ. 1/01) υποδηλώνει ότι ήρθε η είσοδος a και έξοδο είχαμε 01.
  - Οι γραμμές υποδηλώνουν μετάβαση καταστάσεων.
  - Παράδειγμα: Το ότι υπάρχει γραμμή που συνδέει την S3 με την S2 με ένδειξη 0/01, σημαίνει ότι αν είμαστε στην κατάσταση S3 και έρθει είσοδος ‘0’, τότε η έξοδος θα είναι 01 και η νέα κατάσταση θα είναι η S2



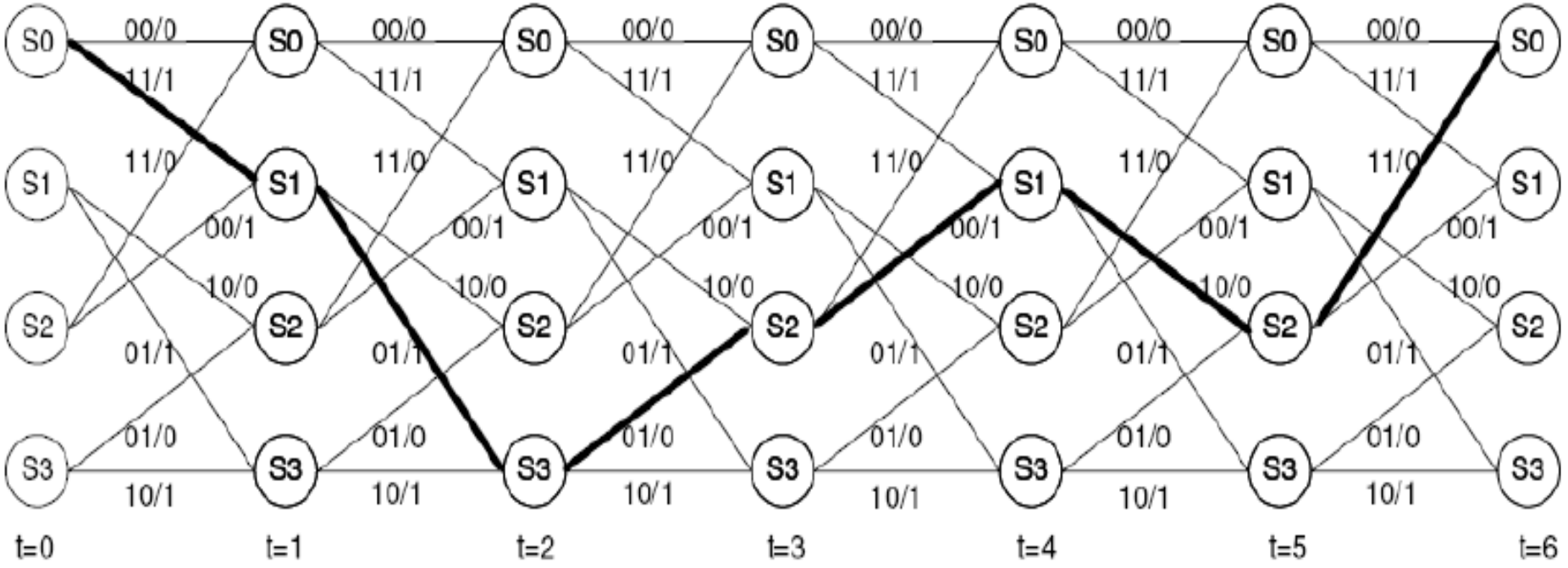
Παράδειγμα

- Για είσοδο 101100, η αλληλουχία καταστάσεων και η έξοδος φαίνεται στο Σχήμα



Αποκωδικοποίηση

- Η αντίστροφη διαδικασία: για λαμβανόμενη έξοδο 11 01 01 00 10 11, έχουμε



Όταν γίνονται σφάλματα?

- **Αλγόριθμος Viterbi**: κατά την αποκωδικοποίηση, θεωρείται σωστό το «μονοπάτι» εκείνο με τη μεγαλύτερη πιθανότητα – εκείνο που η έξοδός του διαφέρει λιγότερο σε σχέση με τα δεδομένα που λάβαμε.

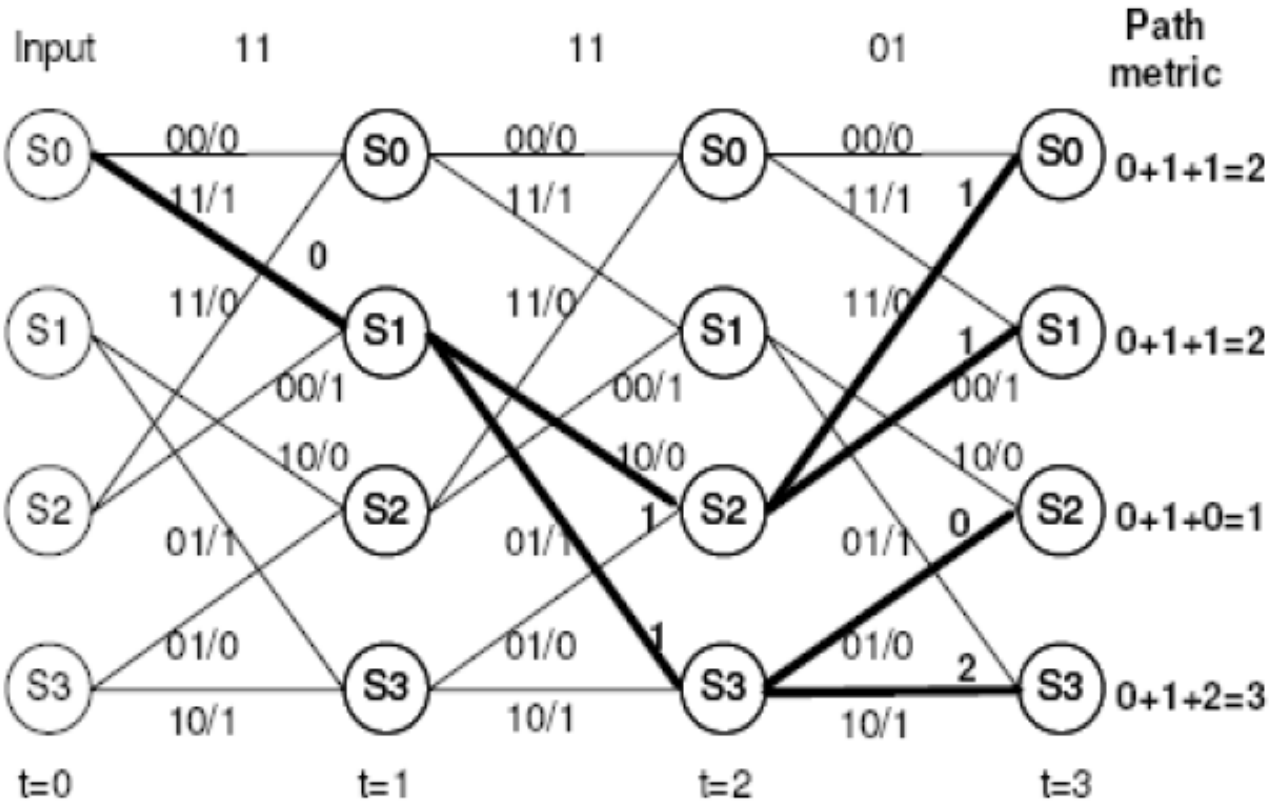
Παράδειγμα: Έστω ότι λάβαμε στον δέκτη 11 11 01. Αυτό δεν αντιστοιχεί σε καμία είσοδο (βλέπε σχήμα).

Για το 11, θεωρούμε ότι είχαμε σαν είσοδο 1 (και δεν έγινε σφάλμα)

Για το επόμενο 11, έγινε σίγουρα σφάλμα. Καταγράφουμε και για τις δύο πιθανές εισόδους πόσο απέχει η έξοδος που θα έβγαζαν από το 11 που λάβαμε. Πλέον, η επόμενη κατάσταση μπορεί να είναι είτε η S2 είτε η S3

Για το 01 κάνουμε το ίδιο και για τις δύο S2,S3.

Τελικά, πιο πιθανή είσοδος: 110 (με έξοδο 110101)

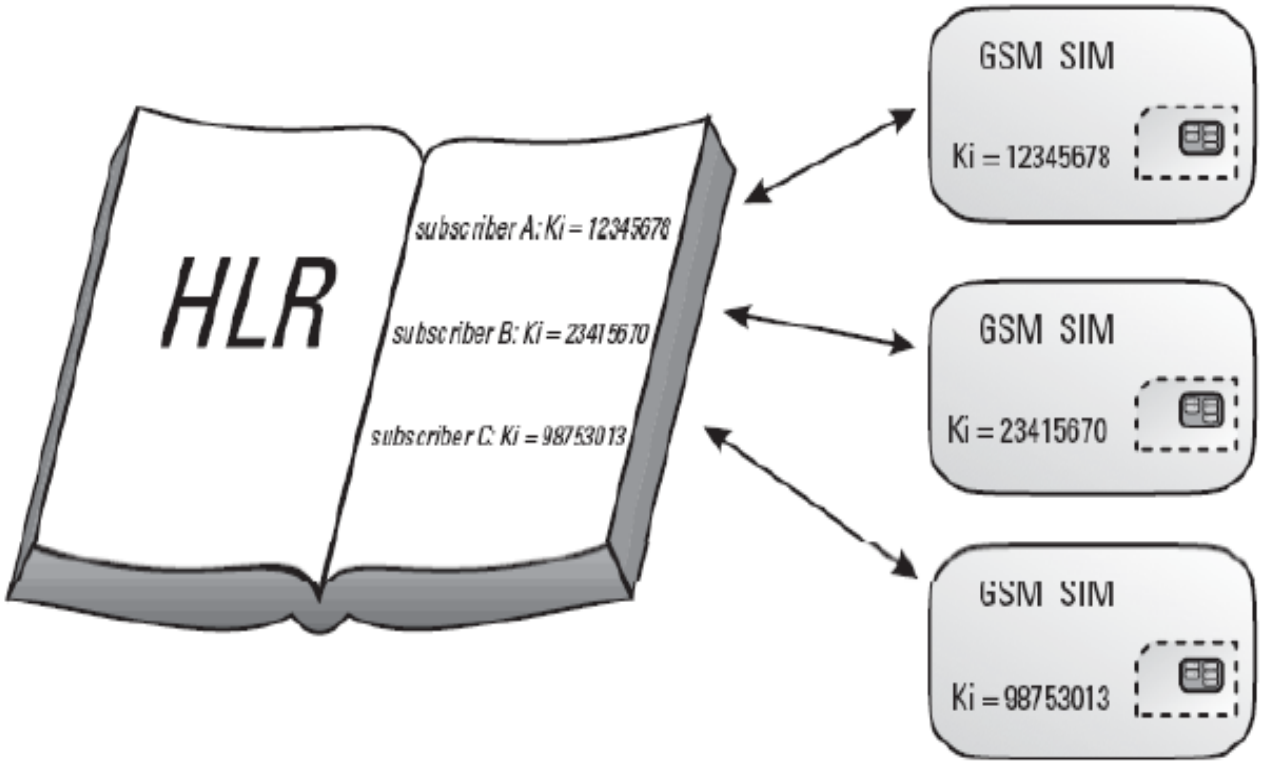


Ασφάλεια στο GSM

Επίπεδα κρυπτογράφησης

- Ασφάλεια σε 3 επίπεδα
  - Αυθεντικοποίηση του χρήστη
  - Κρυπτογράφηση μετάδοσης (δεδομένα/σηματοδοσία)
  - Απόκρυψη του IMSI, που χαρακτηρίζει έναν συνδρομητή, από τα μηνύματα που μεταδίδονται εντός δικτύου (π.χ. κατά την αυθεντικοποίηση).

Κλειδί K_i



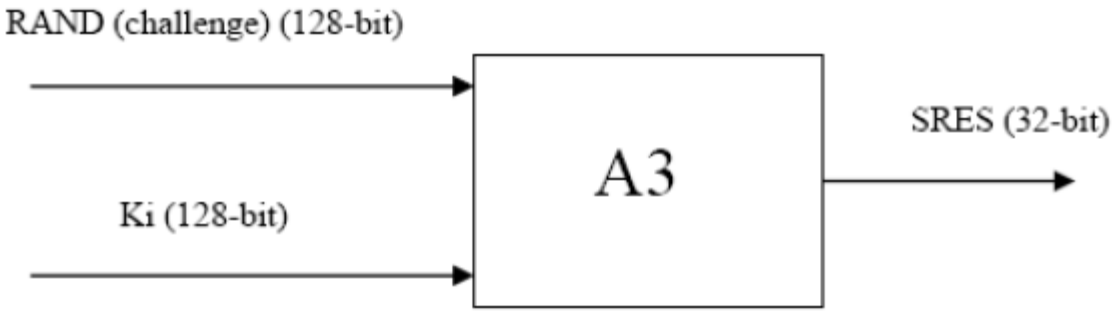
- Μυστική ποσότητα K_i, που την ξέρουν μόνο ο HLR και η SIM

Βασική ιδέα

- Το μυστικό κλειδί Ki είναι 128 bit, και χρησιμοποιείται για να παραχθεί μία απάντηση μήκους 32 bit, που λέγεται SRES, σε μία τυχαία ερώτηση (Challenge) που ονομάζεται RAND και παράγεται από τον MSC.
- Χρησιμοποιείται επίσης για να παραχθεί ένα 64-bit κλειδί, που ονομάζεται Kc, το οποίο χρησιμοποιείται για την κρυπτογράφηση των δεδομένων που μεταδίδονται στον αέρα.
- Όταν ο MS πρωτοεισάγεται στο δίκτυο, ο HLR δίνει στον MSC 5 τριπλέτες, που περιέχουν ένα RAND, μία απάντηση SRES σε αυτό το RAND η οποία προέκυψε από το Ki, καθώς και το κλειδί Kc το οποίο επίσης προέκυψε από το Ki. Κάθε τριπλέτα χρησιμοποιείται για την αυθεντικοποίηση του εν λόγω MS.
- Όταν χρησιμοποιηθούν όλες οι τριπλέτες, ο HLR παρέχει άλλες 5 τριπλέτες στον MSC.
- Το Ki το γνωρίζει μόνο η SIM – η συσκευή η ίδια δεν το μαθαίνει ποτέ

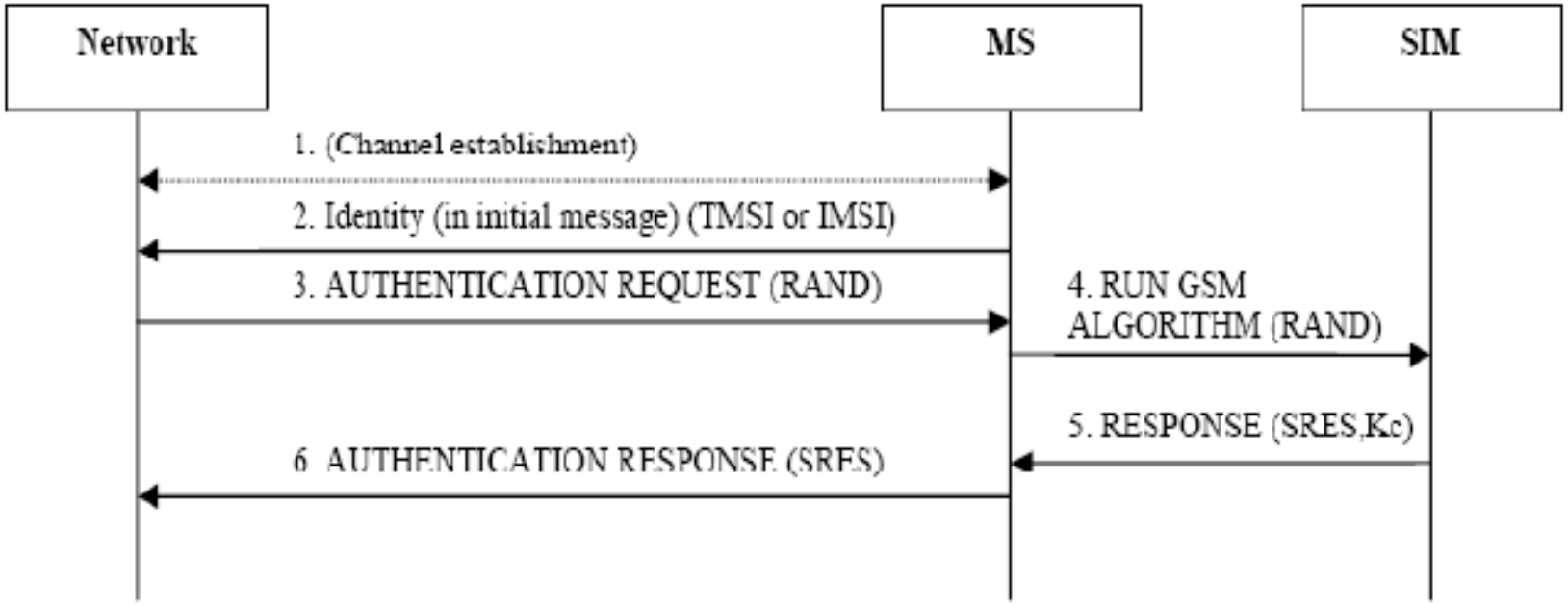
Αυθεντικοποίηση

- Όταν ο MSC φτάσει στην περιοχή ευθύνης ενός MSC, ο MSC του στέλνει την ερώτηση RAND (challenge) – το πρώτο μέλος από τη σχετική τριπλέτα.
- Ο MS υπολογίζει μία απάντηση SRES, κάνοντας χρήση του Ki αλλά και της ερώτησης RAND. Για τον υπολογισμό του SRES, κάνει χρήση του αλγόριθμου A3.



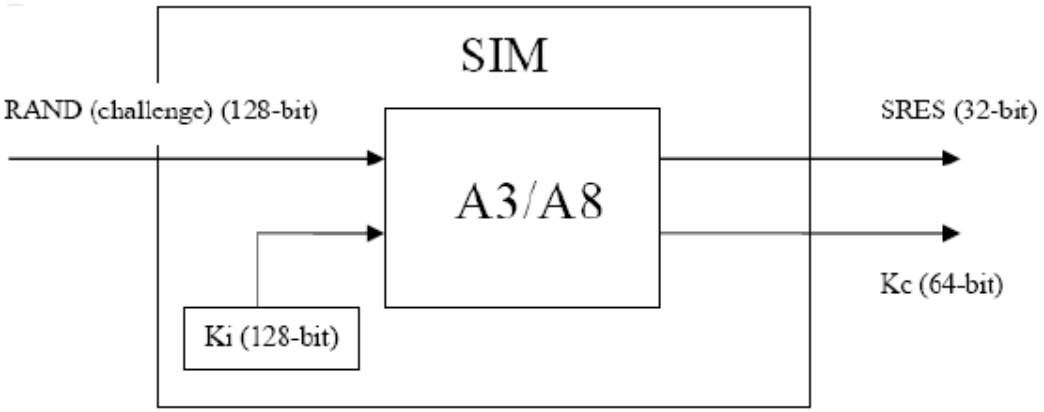
- Ο MSC εξετάζει την απάντηση και ελέγχει αν είναι σωστή, οπότε και αυθεντικοποιεί τον χρήστη.

Σχηματική αναπαράσταση



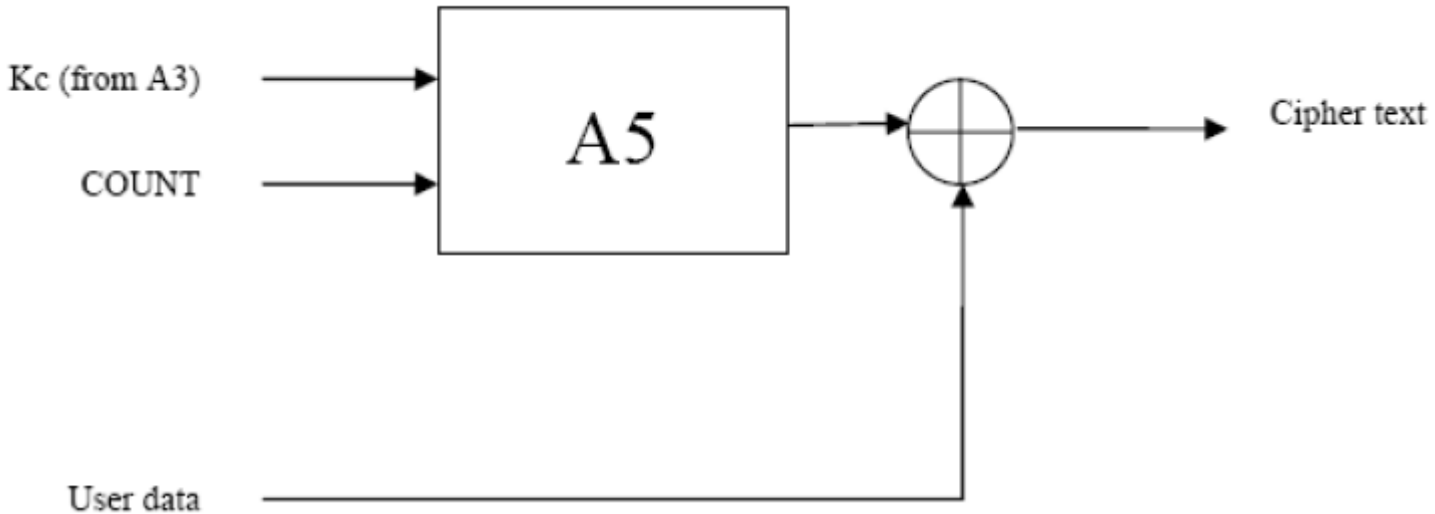
Δημιουργία κλειδιού Kc

- Οποτεδήποτε ζητείται στη SIM να υπολογίσει το SRES (με την εντολή RUN GSM ALGORITHM), υπολογίζει ταυτόχρονα και ένα νέο Kc (κλειδί κρυπτογράφησης – περιγράφεται στη συνέχεια) με τον αλγόριθμο A8.
- Κατά συνέπεια, η διαδικασία αυθεντικοποίησης δεν γίνεται μόνο για να πιστοποιηθεί η ταυτότητα ενός χρήστη, αλλά και οποτεδήποτε το δίκτυο θέλει να αλλάξει το κλειδί κρυπτογράφησης.

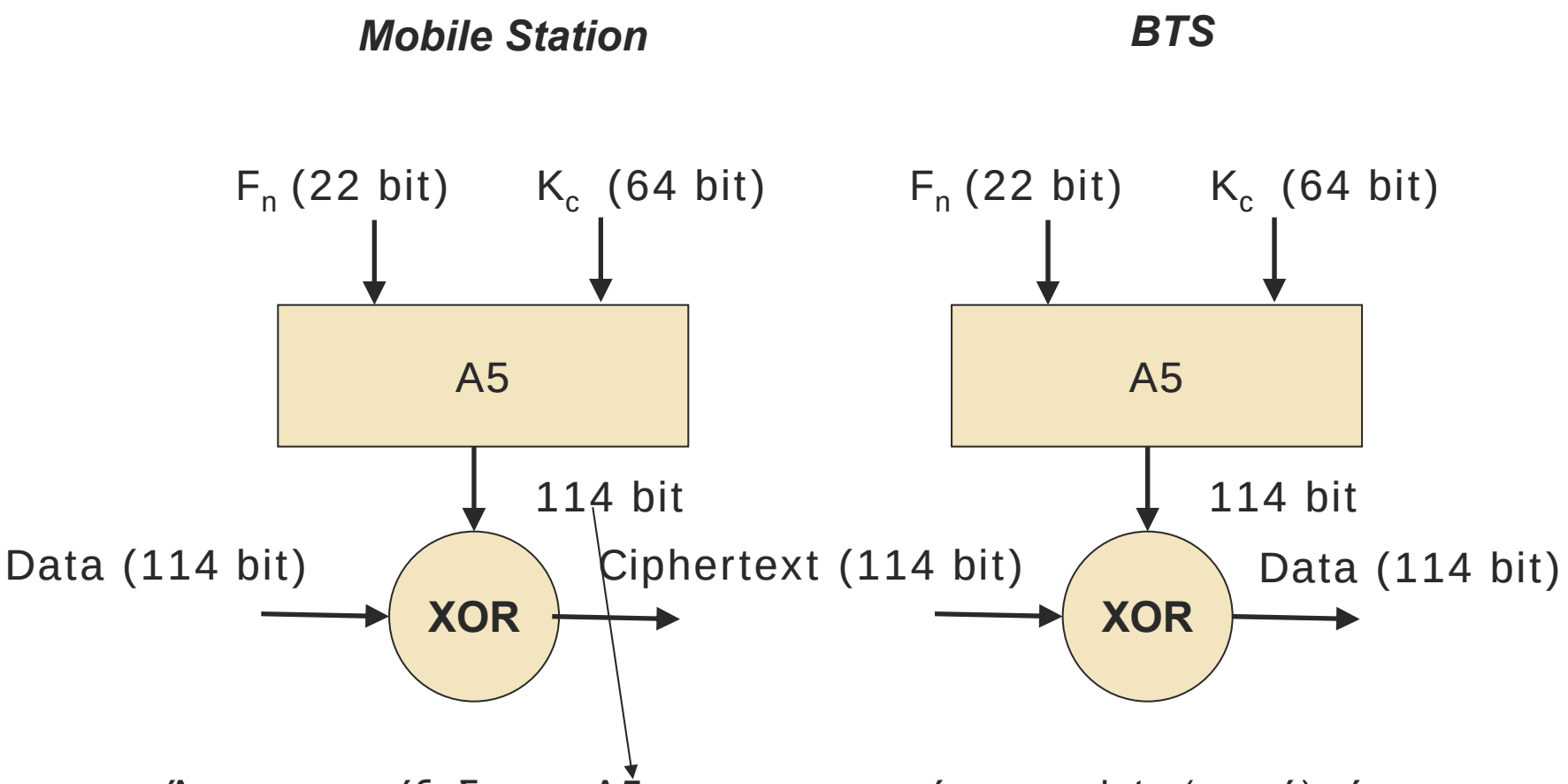


Κρυπτογράφηση

- Όλα τα δεδομένα μεταδίδονται κρυπτογραφημένα
- Τα bit του μηνύματος γίνονται XOR με τα bits της κλειδοροής, τα οποία παράγονται με χρήση του αλγορίθμου A5 εφαρμόζοντάς του στην είσοδο το Kc. Άρα, μόνο το δίκτυο και ο χρήστης, που είναι οι μόνοι που γνωρίζουν το Kc, μπορούν να παράγουν τη συγκεκριμένη κλειδοροή. Για την αποκρυπτογράφηση, γίνεται πάλι η ίδια πράξη XOR μεταξύ των κρυπτογραφημένων bits και της κλειδοροής, ανακτώντας έτσι τα bit του μηνύματος. Με άλλα λόγια, ο A5 είναι ένας αλγόριθμος ροής (stream cipher).
- Στην είσοδο του A5 υπεισέρχεται και μία άλλη ποσότητα, η COUNT, η οποία προκύπτει από το **TDMA Frame Number (Fn).**

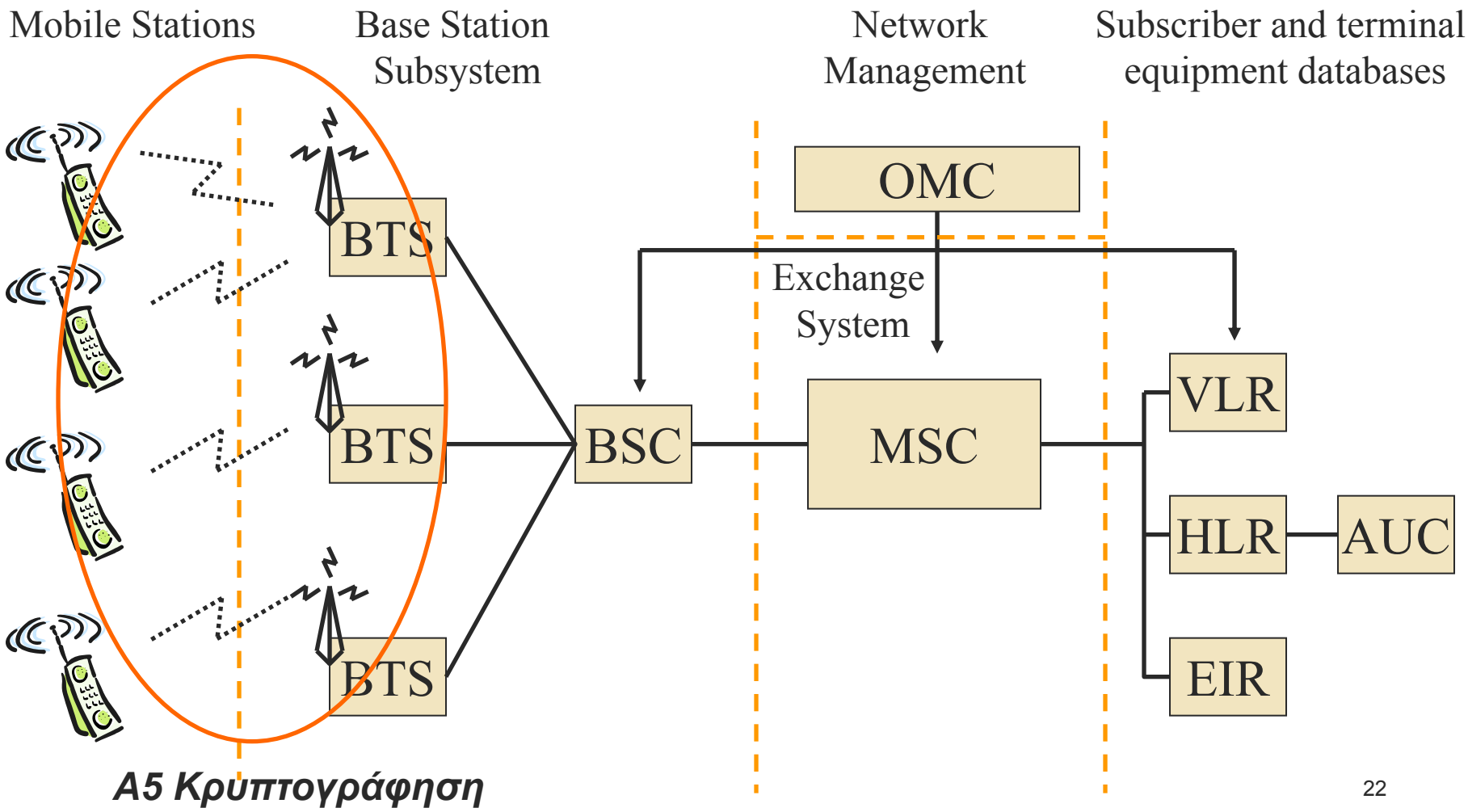


Κρυπτογράφηση - Αποκρυπτογράφηση

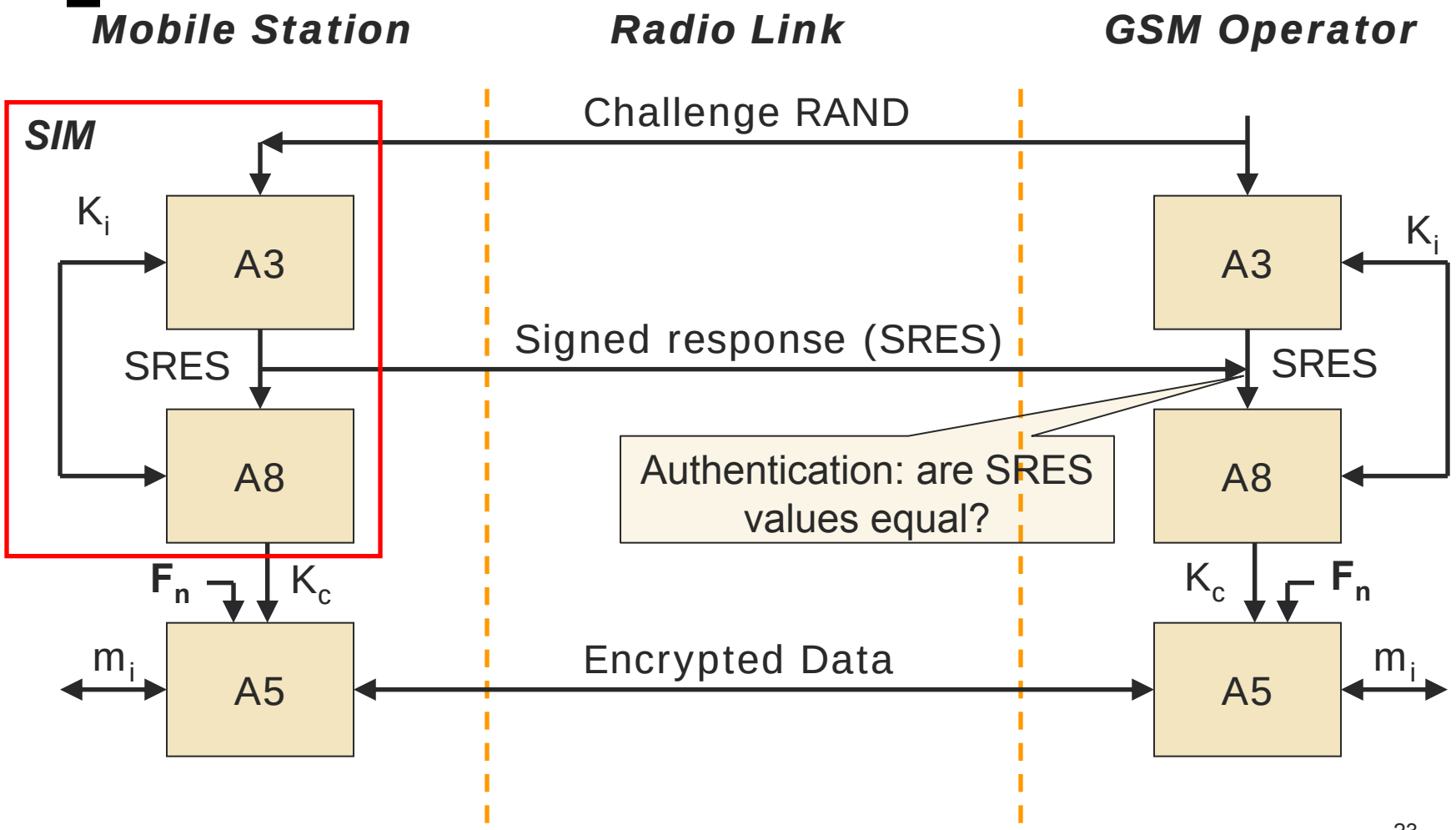


Άρα, με την έξοδο του A5, κρυπτογραφούνται τα data (φωνή) μίας ριπής (που είναι 57+57=114).

Πού γίνεται η κρυπτογράφηση A5?

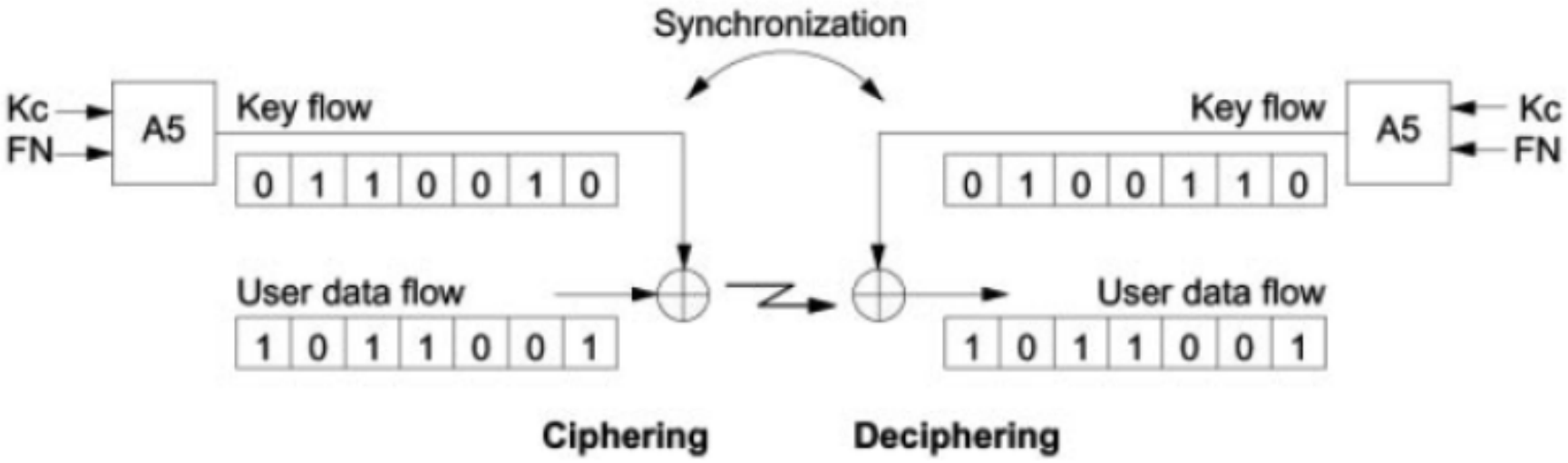


Συνολικό διάγραμμα αλγορίθμων



Οι αλγόριθμοι A3/A8 δεν έχουν τυποποιηθεί!! (σε αντίθεση με τον A5)

Μετάδοση των κρυπτογραφημένων δεδομένων



Ποιοι είναι οι αλγόριθμοι κρυπτογράφησης?

- Υπάρχουν τρεις αλγόριθμοι: A5/1, A5/2, A5/3
- Οι περισσότεροι υλοποιούν τον A5/2, ενώ έχει αρχίσει να διαδίδεται και ο A5/3 από το 2005
- Αν και οι A3, A8 ήταν μυστικοί, εν τούτοις διέρρευσαν. Ο αλγόριθμος ο κύριος που χρησιμοποιήθηκε είναι γνωστός με το όνομα COMP128, όμως υπήρξαν και εκδόσεις 2 και 3 σε αυτόν.
- Τεχνικές λεπτομέρειες των αλγορίθμων δεν θα μας απασχολήσουν εδώ

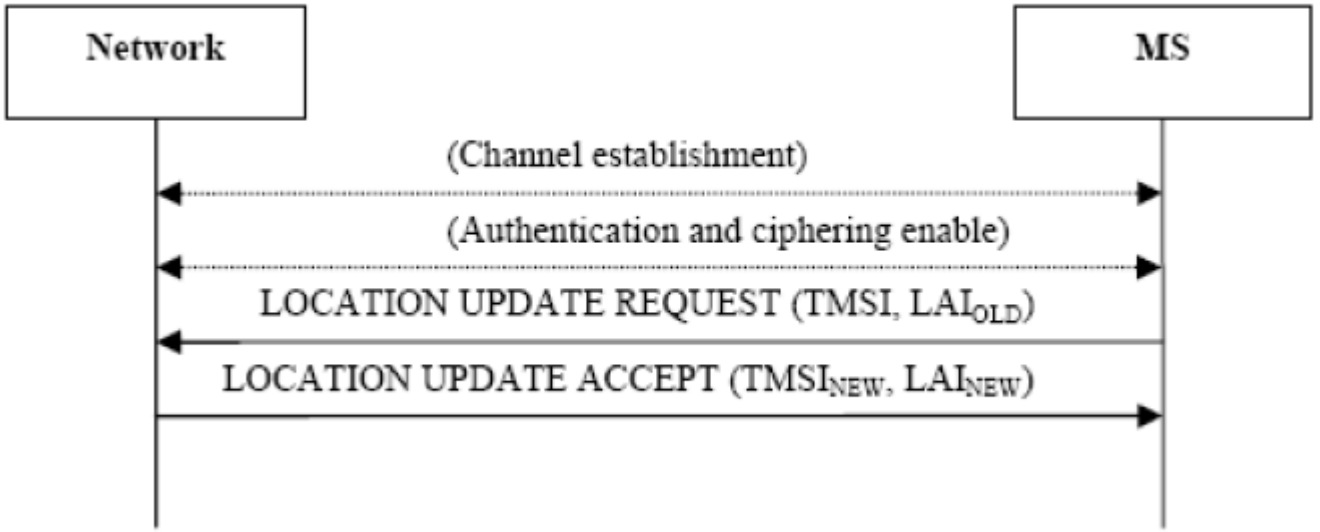
Πρόσθετο επίπεδο ασφαλείας: Άλματα συχνοτήτων

- Στο GSM πραγματοποιούνται άλματα συχνοτήτων (frequency hopping) όπου ο πομπός αλλάζει φυσικό κανάλι σε κάθε frame frame (4.615ms), δηλαδή περίπου 217 φορές το δευτερόλεπτο.
- Η ακολουθία των συχνοτήτων που αλλάζουν καθορίζεται γενικά από έναν σύνθετο αλγόριθμο.
- Αυτό προσδίδει επιπλέον επίπεδο ασφαλείας: αν ο επιτιθέμενος δεν ξέρει το πώς αλλάζουν οι συχνότητες, τότε για να ανακτήσει το κρυπτογραφημένο μήνυμα (και να επιχειρήσει, εάν είναι εφικτό, κρυπτανάλυση), θα πρέπει να ελέγξει όλο το φάσμα (κάτι μη πρακτικό) (βέβαια, αν γνωρίζει το εύρος φάσματος που χρησιμοποιεί ο πάροχος στη συγκεκριμένη περιοχή, περιορίζεται κάπως το μέγεθος του φάσματος που πρέπει να ελέγξει)

Προστασία της ταυτότητας του συνδρομητή

- Το GSM δεν περιλαμβάνει στα μηνύματα που στέλνονται το IMSI του συνδρομητή, έτσι ώστε να μην μπορεί ένας επιτιθέμενος να δει αν κάποιος συγκεκριμένος χρήστης ήταν στο δίκτυο, ούτε τι υπηρεσία χρησιμοποίησε.
- Σε κάθε συσκευή, την ώρα της κλήσης, της αποδίδεται ο TMSI, μήκους 32 bit. Ισχύει για μία Location Area – αλλάζει δηλαδή εάν αλλάξει η Location Area του χρήστη (ή εάν παρέλθει προκαθορισμένο χρονικό διάστημα).
- Το TMSI μεταδίδεται κρυπτογραφημένο

Σχηματική Αναπαράσταση



- Ωστόσο, αν το TMSI δεν αλλάζει συχνά, με μία στατιστική ανάλυση μπορεί και να ανακαλυφθεί. Αν σε ένα γνωστό τηλεφωνικό νούμερο στείλει κανείς πολλά SMS (ή επιχειρήσει πολλές κλήσεις) και παρατηρεί το κανάλι PCH (paging channel) όλες αυτές τις φορές, τότε είναι πιθανό να ανακαλύψει το TMSI (εάν το TMSI δεν αλλάζει σε κάθε νέα κλήση).

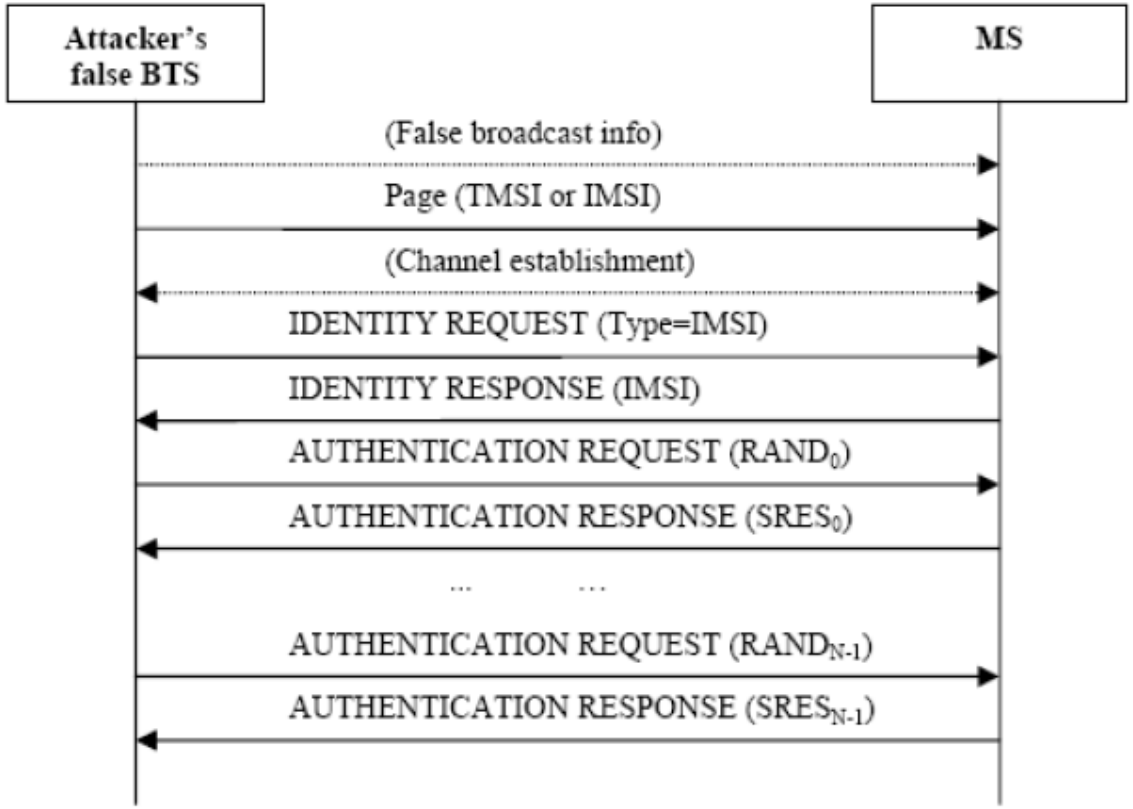
Περιορισμοί στην ασφάλεια του GSM

- Η σχεδίαση είναι τέτοια ώστε να παρέχει ασφάλεια μόνο σε επίπεδο πρόσβασης στο δίκτυο: τα δεδομένα και η σηματοδοσία εντός του σταθερού δικτύου της αρχιτεκτονικής δεν προστατεύονται
- Είναι εύκολο να προσποιηθεί κανείς ότι είναι «κόμβος του δικτύου» - η συσκευή δεν ζητάει ποτέ αυθεντικοποίηση του δικτύου!!

Επίθεση στους A3/A8

- Όχι καλή σχεδίαση του αλγορίθμου COMP128 (ο οποίος τελικά διέρρευσε). Με κατάλληλα επιλεγμένες τιμές του RAND, μπορούμε να ανακαλύψουμε το Ki απλά παρατηρώντας την έξοδο του αλγορίθμου, χωρίς να κάνουμε εξαντλητική αναζήτηση.
- Με περίπου 160.000 RAND, μπόρεσαν να ανακαλύψουν το Ki
  - Με βελτίωση της τεχνικής αργότερα, αρκούν μόνο 50000 RAND
- Το Ki υπολογίζεται μέσα σε λιγότερο από μία ώρα (Dejan Kaljevic, 2004)
- Για αυτό προχωρήσαμε σε αλγορίθμους COMP128-2 και COMP128-3 (για τα 3G δίκτυα, χρησιμοποιείται ο COMP128-4, που χρησιμοποιεί το Πρότυπο Κρυπτογράφησης AES).
- Τα παραπάνω αποτελούν απόδειξη ότι η ασφάλεια δεν πρέπει να βασίζεται στη μυστικότητα του αλγορίθμου!!

Σχηματική Αναπαράσταση Υποκλοπής του Ki



- Ο χρήστης μπορεί να υποψιαστεί κάτι μόνο από το γεγονός ότι η μπαταρία του θα τελειώσει πιο γρήγορα!
- Δεν χρειάζεται να ξέρει το IMSI ο επιτιθέμενος – του αρκεί να ξέρει ένα TMSI (Βλέπε προηγούμενα)

Αδυναμίες του A5/1

- Οι COMP128 και COMP128-2 έχουν σαν αποτέλεσμα τα τελευταία 10 bit του Kc να είναι μηδενικά. Αυτό περιορίζει τον έλεγχο εξαντλητικής αναζήτησης σε όλα τα πιθανά κλειδιά Kc του αλγορίθμου.

Table 5.5-2: Number of machines required to search a key space in a given time

Key length in bits	1 day	1 week	1 year
40	13	2	-
56	836788	119132	2.291
64	2.14x10^8	3.04x10^6	584542
128	3.9x10^27	5.6x10^26	10.8x10^24

- Όπως φαίνεται και στον Πίνακα, τα 56 bit κλειδιού δεν είναι πάρα πολλά - μία εξαντλητική αναζήτηση μπορεί να γίνει (να σημειωθεί ότι ο παραπάνω πίνακας είναι του 2005)

Αδυναμίες του A5/1 (συνέχεια)

Η δομή του επέτρεψε επιτυχείς επιθέσεις

- time-memory trade-off attacks από τους Biryukov, Shamir and Wagner (2000)– ο αλγόριθμος «σπάει» σε λιγότερο από 2 sec σε ένα απλό PC, αρκεί όμως να έχουν γίνει κάποιοι υπολογισμοί οι οποίοι διατηρούνται σε κάποιο αρχείο. Το σύνολο των υπολογισμών αυτών απαιτεί αποθηκευτικό χώρο περίπου 300 GB.

Table 5.5-3: Three possible tradeoff points in the attacks on A5/1

Attack type	Preprocessing steps	Available data	Number of 73GB disks	Attack time
Biased Birthday attack (1)	2^{42}	2 minutes	4	1 second
Biased Birthday attack (2)	2^{48}	2 minutes	2	1 second
Random Subgraph attack	2^{48}	2 seconds	4	minutes

- statistical attack από τους Ekdahl and Johansson (2002) and Maximov, Johansson and Babbage (2004). «Σπάνε» τον αλγόριθμο σε λιγότερο από ένα λεπτό, απαιτώντας τη γνώση μόνο λίγων δευτερολέπτων από τη μεταδιδόμενη ομιλία

Είναι ο A5/2 καλύτερος?

- Ουσιαστικά όχι
  - Κρυπτανάλυση από τους Barkan, Biham and Keller (2003), για την οποία δεν χρειάστηκε καν γνώση τμήματος της ομιλίας!
  - Με τη σημερινή τεχνολογία, ο A5/2 δεν παρέχει ουσιαστικά καμία ασφάλεια – δεν πρέπει να χρησιμοποιείται

Διαμόρφωση στο GSM

ΔΙΑΜΟΡΦΩΣΗ

- **ΔΙΑΜΟΡΦΩΣΗ** (Modulation)= Η μεταβολή, σύμφωνα με το σήμα πληροφορίας, των παραμέτρων ενός **φέροντος κύματος** (carrier wave) που είναι κατάλληλο για τη μετάδοση μέσα από δεδομένο κανάλι

- **ΑΠΟΔΙΑΜΟΡΦΩΣΗ** (Demodulation) είναι η αντίστροφη διαδικασία

- Το είδος της διαμόρφωσης καθορίζει:
  - Την αντοχή στο θόρυβο και την παραμόρφωση του καναλιού
  - Την πιστότητα αναπαραγωγής του αρχικού σήματος πληροφορίας
  - Το εύρος του απαιτούμενου για την μετάδοση φάσματος
  - Την πολυπλοκότητα των συστημάτων εκπομπής και λήψης

- Στις κινητές επικοινωνίες, χρησιμοποιησουμε το σήμα πληροφορίας για να **διαμορφώσουμε** ένα φέρον υψηλής συχνότητας f_c (Radio Frequency), έτσι ώστε οι απαιτούμενες διαστάσεις τις κεραίας (λ/4) να είναι λογικές

Τι επιτυγχάνουμε με την Διαμόρφωση

- Την μετάδοση **πολλών σημάτων** στον ίδιο χώρο με χρήση διαφορετικών φερόντων
- Την ελάττωση των απαιτήσεων στα χαρακτηριστικά των συστημάτων εκπομπής
- Την εκμετάλλευση περιοχών του φάσματος που έχουν καλύτερες συνθήκες μετάδοσης

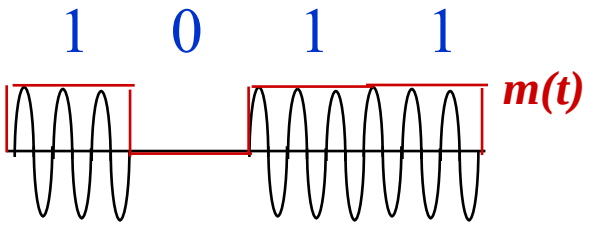
Διαμόρφωση με ημιτονοειδές φέρον

- Ψηφιακή διαμόρφωση συνεχούς κύματος
  - Το φέρον είναι ένα ημιτονοειδές σήμα **exit)=Acos(2πf t +φ)**
  - Το σημα **πληροφορίας** είναι μια ακολουθία παλμών
  - Παλμική διαμόρφωση πλάτους (ASK)
  - Παλμική διαμόρφωση συχνότητας (FSK)
  - Παλμική διαμόρφωση φάσης (PSK)
- Υπάρχει και η ψηφιακή διαμόρφωση όπου το φέρον είναι ακολουθία παλμών. Στις κινητές επικοινωνίες, χρησιμοποιείται η ημιτονοειδής διαμόρφωση.

Σχηματική περιγραφή

Amplitude Shift Keying (ASK)

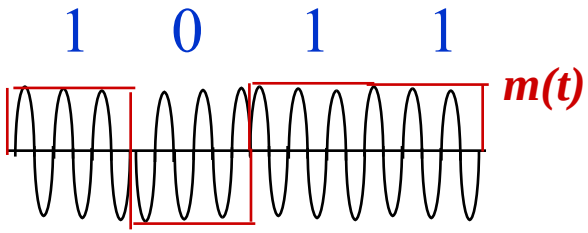
$$s(t) = m(t)A_c \cos(2\pi f_c t) = \begin{cases} A_c \cos(2\pi f_c t) & m(nT_b) = 1 \\ 0 & m(nT_b) = 0 \end{cases}$$



AM Modulation

Phase Shift Keying (PSK)

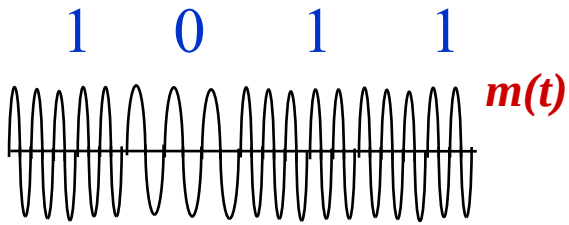
$$s(t) = A_c m(t) \cos(2\pi f_c t) = \begin{cases} A_c \cos(2\pi f_c t) & m(nT_b) = 1 \\ A_c \cos(2\pi f_c t + \pi) & m(nT_b) = 0 \end{cases}$$



PM Modulation

Frequency Shift Keying (FSK)

$$s(t) = \begin{cases} A_c \cos(2\pi f_1 t) & m(nT_b) = 1 \\ A_c \cos(2\pi f_2 t) & m(nT_b) = 0 \end{cases}$$

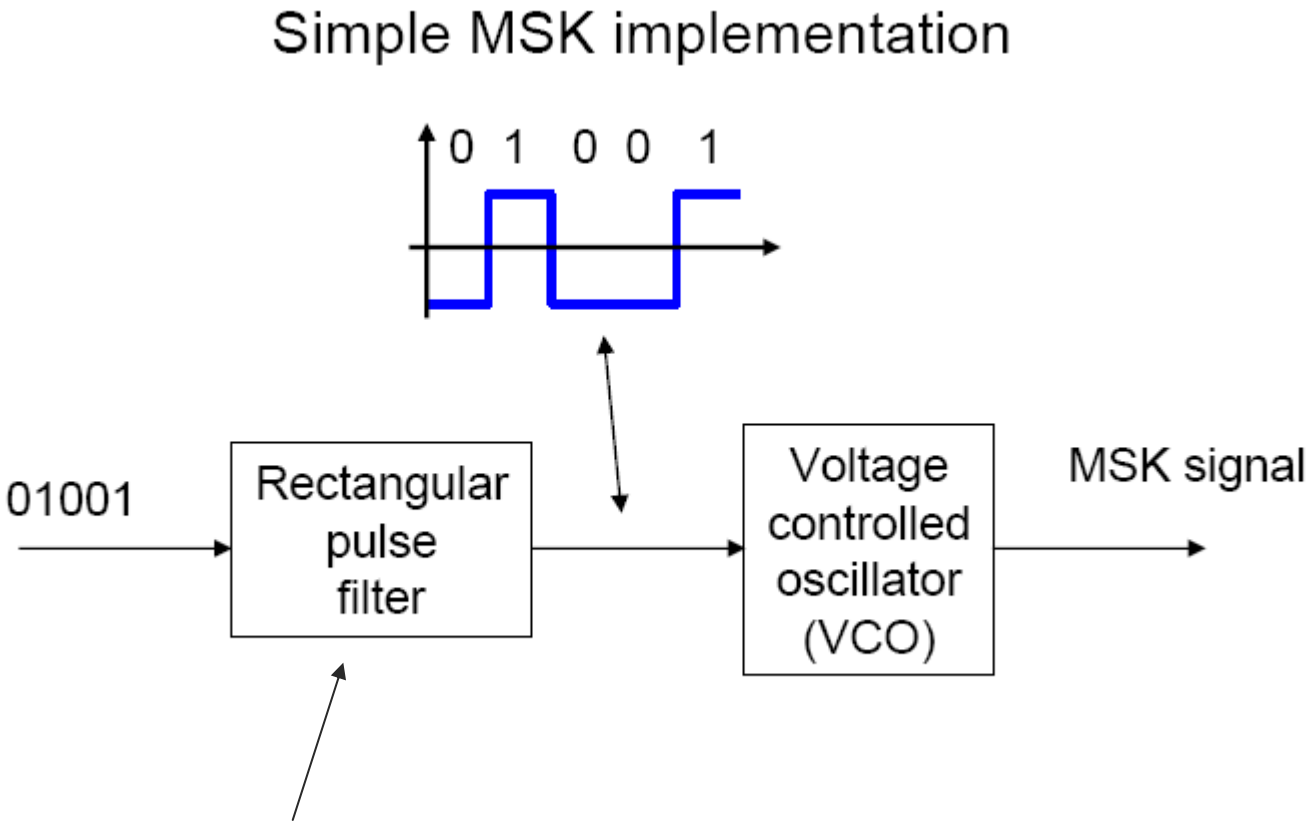


FM Modulation

Διαμόρφωση στο GSM?

- Gaussian Minimum Shift Keying (GMSK)
- Είναι παραλλαγή της τεχνικής MSK
- MSK (Minimum Shift Keying): διαμόρφωση συχνότητας, αλλά η φάση παραμένει συνεχής όταν αλλάζει η συχνότητα (δηλαδή το bit που πρέπει να διαμορφωθεί).
- Η διαφορά των συχνοτήτων είναι πάντα το μισό του ρυθμού των δεδομένων

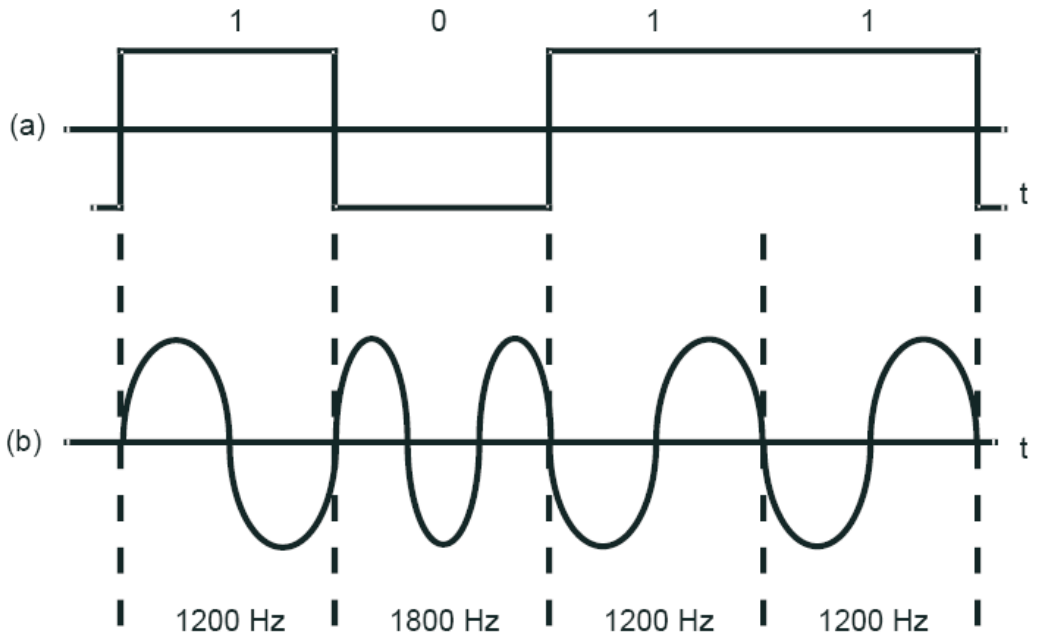
Γενικό διάγραμμα



Τα δυαδικά ψηφία περνάνε πρώτα από ένα NRZ φίλτρο (Non-Return-to-Zero)

Παράδειγμα της MSK

- 1200 bits/sec baseband MSK data signal
- Διαφορά συχνοτήτων = 600Hz



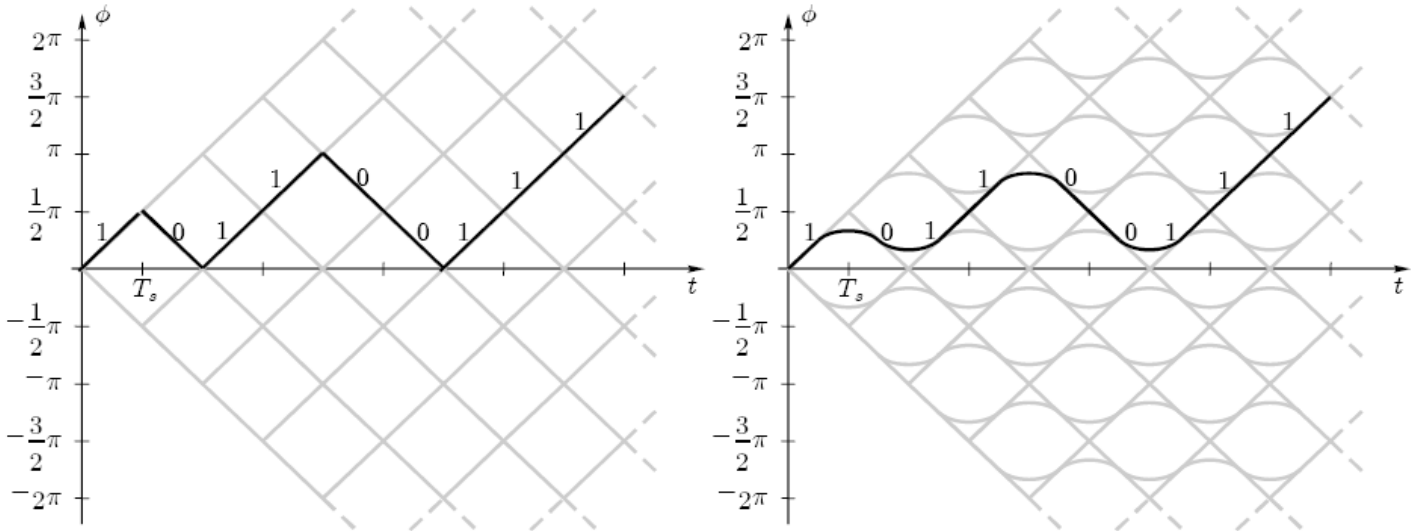
Gaussian Minimum Shift Keying (GMSK)

- Το GMSK είναι μια παραλλαγή του MSK. Οι πλάγιοι λοβοί του φάσματος μειώνονται ακόμα περισσότερο με μορφοποίηση του παλμού, χρησιμοποιώντας έναν gaussian παλμό.
- Αυτή η μορφοποίηση του παλμού είναι απαραίτητη για τις ασύρματες επικοινωνίες (για να μπορούν τα RF κυκλώματα να χειρίζονται τους παλμούς καλύτερα)
- Χρησιμοποιείται ένα φίλτρο προ-διαμόρφωσης με μορφή Gauss και εύρος φάσματος B. Το μικρό B ελαττώνει τους πλάγιους λοβούς αλλά δημιουργεί κάποια ISI (αλληλοπαρεμβολή συμβόλων).
- Στο GSM έχει γίνει η βέλτιστη επιλογή συχνότητας και ρυθμού μετάδοσης δεδομένων, έτσι ώστε να έχουμε καλή μορφοποίηση του παλμού με τη λιγότερη δυνατή ISI

Gaussian filtered MSK

Further improvement of the phase: Remove 'corners'

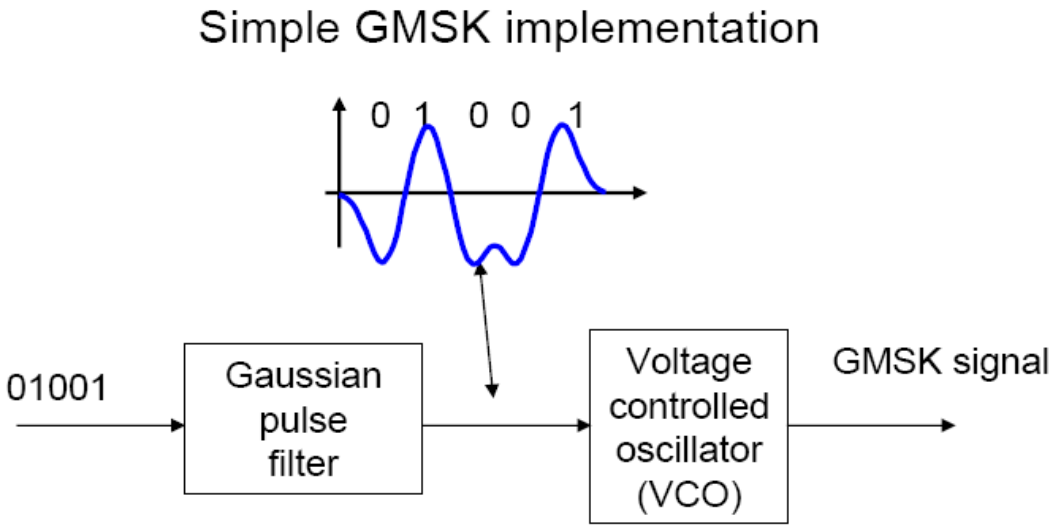
(Simplified figure)



MSK
(Rectangular pulse filter)

Gaussian filtered MSK - GMSK
(Gaussian pulse filter)

Gaussian filtered MSK



When implemented this “simple” way, it is usually called Gaussian filtered frequency shift keying (GFSK).

GSFK is used in e.g. Bluetooth.

Αναφορές

- Haykin, S. 2001: “Communication Systems”. 4th ed. New York, NY. John Wiley & Sons.

Πηγές

- Για τη διαμόρφωση των διαφανειών αυτού του κεφαλαίου, χρησιμοποιήθηκε υλικό (εικόνες, διαγράμματα κτλ.) από:
- «MONITORING AND MEASUREMENT OF GSM MOBILE TELEPHONY SIGNALS», Χ. Μελισσάρης (Πανεπιστήμιο Κρήτης), διαθέσιμη στο

  http://elocus.lib.uoc.gr//dlib/6/b/a/attached-metadata-dlib-2005melissaris/2005melissaris.pdf