Ασφάλεια Υπολογιστικών Συστημάτων

7ο Εξάμηνο

Επιθέσεις σε υλικό

Διδάσκων : Δρ. Παρασκευάς Κίτσος,
Καθηγητής

Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

https://ecsalab.ece.uop.gr/

e-mail: kitsos@uop.gr

ΚΕΦΑΛΑΙΟ 25: Ασφάλεια το Υλικό

Ασφάλεια Πληροφοριών & Συστημάτων στον Κυβερνοχώρο

Περιεχόμενα διάλεξης

- Εισαγωγή
  - Η ανάγκη για ασφαλές υλικό (HardWare-HW)
  - Ορολογία
- Αρχιτεκτονικές
  - Cryptographic coprocessors/accelerators
  - Cryptographic chip cards/smart cards
- Κατηγορίες Ασφάλειας
- Ασφάλεια smart cards (έξυπνων καρτών)

Ασφαλές υλικό

- Εγγυάται γρήγορες και ασφαλείς επικοινωνίες καθώς και ασφαλή αποθήκευση κρίσιμων πληροφοριών
- Ευαίσθητες πληροφορίες (π.χ. οικονομικές συναλλαγές, κλειδιά κρυπτογραφίας) που είναι αποθηκευμένα σε σκληρούς δίσκους ή μνήμες είναι ευπαθή
  - Ο αντίπαλος (με επαρκή δικαιώματα) μπορεί να τα προσπελάσει
  - Το αντίγραφο δεδομένων (back up) ενός σκληρού δίσκου μπορεί να αποθηκευτεί σε μη προστατευμένη συσκευή

- Προβλήματα με την ασφαλή διαγραφή/καταστροφή των δεδομένων που βρίσκονταν σε μη προστατευμένες συσκευές

Χρήσεις του!!!

- Οι κρίσιμες εφαρμογές εμπεριέχουν τραπεζικές συναλλαγές
  - Άρα απαιτείται ασφαλής αποθήκευση
  - Ευρεία χρήση καρτών σε ATM
  - Οι τράπεζες δεν εμπιστεύονται ούτε τους υπαλλήλους τους ούτε και τους πελάτες τους
  - Αυτό οδήγησε της ανάπτυξης αυτού που ονομάζεται Συστήματα Ασφαλούς Υλικού και δίκτυα τραπεζικών δεδομένων (τραπεζικές μηχανές, τερματικά πώλησης)

- Αρχές πιστοποίησης
  - Εξαιτίας της ανάγκης για αυξημένη ταχύτητα κρύπτο-λειτουργιών
  - Αύξηση τα τελευταία χρόνια της χρήσης αλγορίθμων δημοσίου κλειδιού

Ορολογία

- Διάταξη Υλικού Ασφάλειας (Hardware security modules -HSM)
  - Συνεπεξεργαστής (Coprocessor)
  - Επιταχυντές (Accelerators)
  - Έξυπνες κάρτες (Cryptographic smartcards)

- Επιθέσεις στις διατάξεις υλικού ασφάλειας
  - Φυσικές επιθέσεις (Physical attacks)
  - Επιθέσεις παράπλευρου καναλιού (Side channel attacks)
  - Επιθέσεις στο API

- Τα κρίσιμα κλειδιά (δημόσιο, ιδιωτικό) αποθηκεύονται πάντα σε HSM
  - Άλλα κλειδιά (συνόδου) αποθηκεύεται εκτός HSM αλλά κρυπτογραφείται από τη HSM

Παραδείγματα διατάξεων υλικού ασφάλειας

- Διατάξεις με ένα ολοκληρωμένο
- Διατάξεις με πολλά ολοκληρωμένα
  - IBM 4758

  - IBM PCI-X

  - SafeNet PSO

  - SafeNet PSG

  - Gemalto SmartCards

  - SafeNet iKey

  - Dallas iButton

  - Infineon TPM chip

  - VeriChip RFID TAGs

  - NXP/Phillips MIFARE

Αρχιτεκτονικές συνεπεξεργαστών και επιταχυντών

- Διαφέρουν από τη κλασσική von Neumann αρχιτεκτονική
- +Μηχανισμοί για φυσική ασφάλεια
  - Προστατευτικό κάλυμα, αισθητήρες

- +Γεννήτριες τυχαίων αριθμών
  - Γεννήτριες για διάφορα στοιχεία κρυπτογραφίας (κλειδιά, padding)
  - Αλγορίθμους ενάντια σε επιθέσεις παράπλευρου καναλιού
- +Εξειδικευμένοι συνεπεξεργαστές
  - Επιταχύνουν τις πράξεις στους αλγορίθμους ιδιωτικού και δημοσίου κλειδιού
- +RAM μόνιμης αποθήκευσης (Non-Volatile RAM- NVRAM) => δεν χάνεται το περιεχόμενό τους
  - Είναι συνδεδεμένες με μόνιμη πηγή ρεύματος
  - Αποθηκεύουν κρίσιμες πληροφορίες (master keys)
  - Έχουν I/Os
- Εύκολη επικύρωση

Χαρακτηριστικά έξυπνων καρτών…

- Παρόμοια δομή με τους συνεπεξεργαστές/επιταχυντές

- Τα πάντα είναι υλοποιημένα σε ένα ολοκληρωμένο κύκλωμα

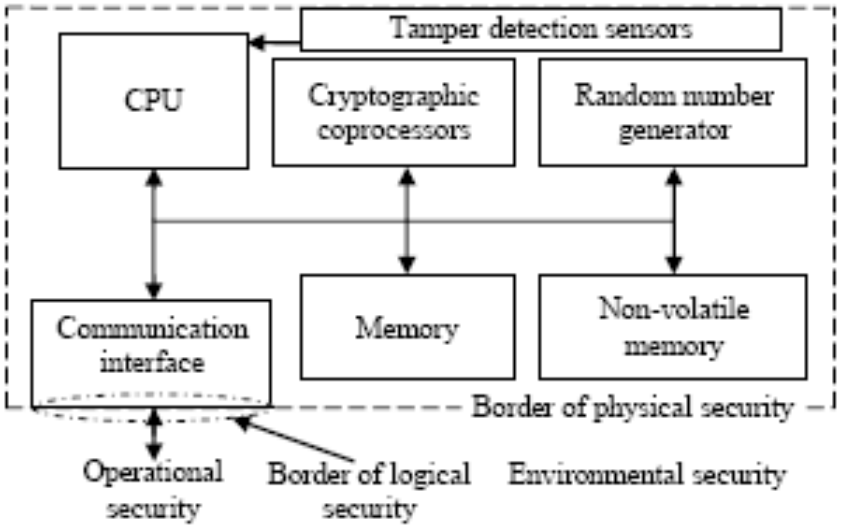
- Έχουν πολύ μικρή επιφάνεια κάλυψης υλικού (silicon area) →μικρό μέγεθος μνήμης RAM
- Λειτουργούν σε περιβάλλοντα με περιορισμένα επίπεδα τροφοδοσίας
  - Πρέπει να καταναλώνουν πολύ μικρή ενέργεια
- Υποστηρίζουν αλγορίθμους όπως ο DES, RSA, ECC και άλλους

…Χαρακτηριστικά έξυπνων καρτών

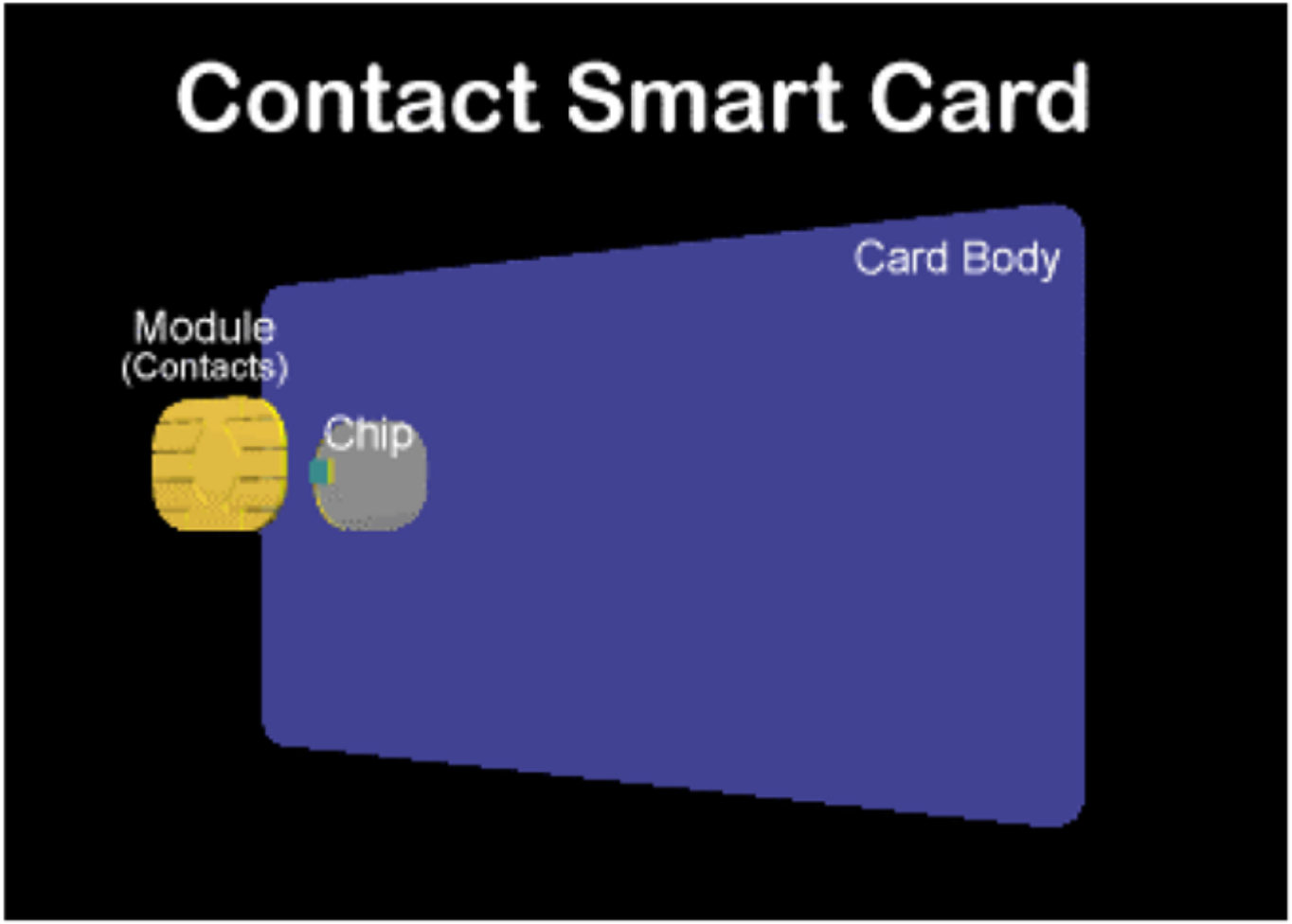
- Το λειτουργικό τους είναι αποθηκευμένο σε μνήμες ROM ενώ οι εφαρμογές τους σε μνήμες EEPROM
- Επικοινωνία σύμφωνα με το πρωτόκολλο κάθε εφαρμογής
  - Contact –περιέχει πέλμα επικοινωνίας
  - Contactless –περιέχει εσωτερική κεραία
  - Συνδυασμός των δύο προηγούμενων
  - Υβριδικός- περισσότερα ολοκληρωμένα σε μια έξυπνη κάρτα

Κατηγορίες ασφάλειας

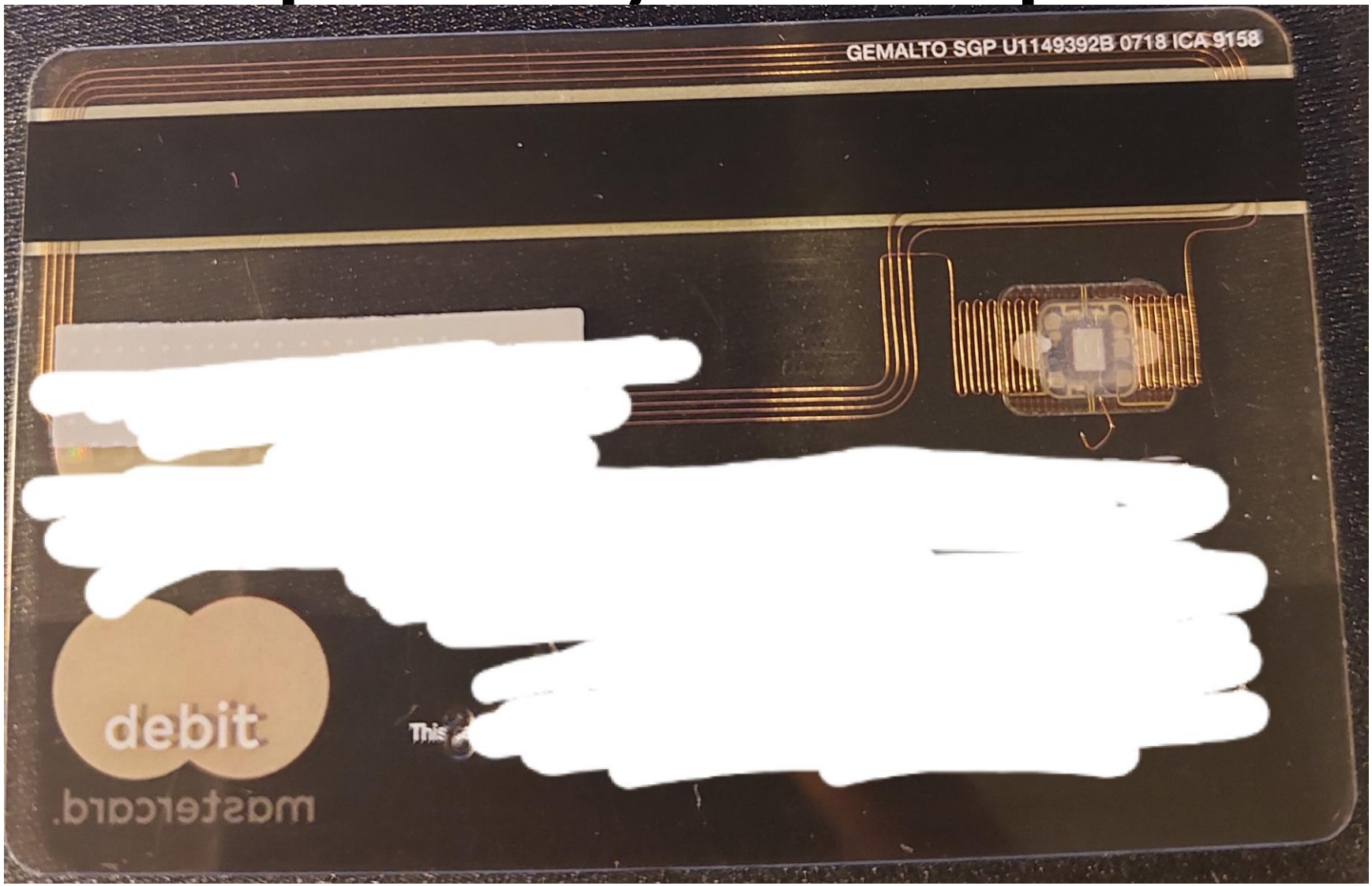
- Φυσική ασφάλεια
  - Χρησιμοποιούνται μεθοδολογίες για την περιφρούρηση των συστημάτων
- Λογική ασφάλεια
  - Μηχανισμοί των λειτουργικών προγραμμάτων με σκοπό την εμπόδιση μη πιστοποιημένης πρόσβασης
  - Έλεγχος πρόσβασης, αλγόριθμοι, πρωτόκολλα
- Περιβαλλοντική ασφάλεια
  - Η προστασία του πληροφοριακού συστήματος σαν οντότητα
- Λειτουργική ασφάλεια
  - Κρυπτογραφία



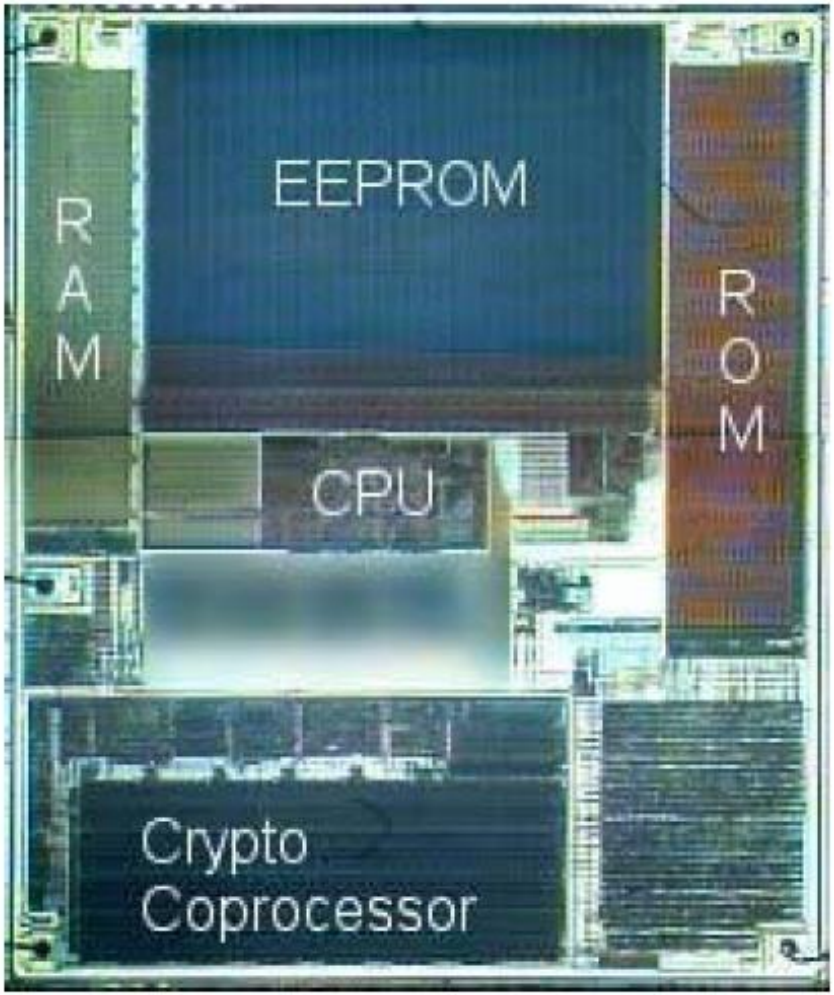
Ασφάλεια έξυπνων καρτών…



…Ασφάλεια έξυπνων καρτών



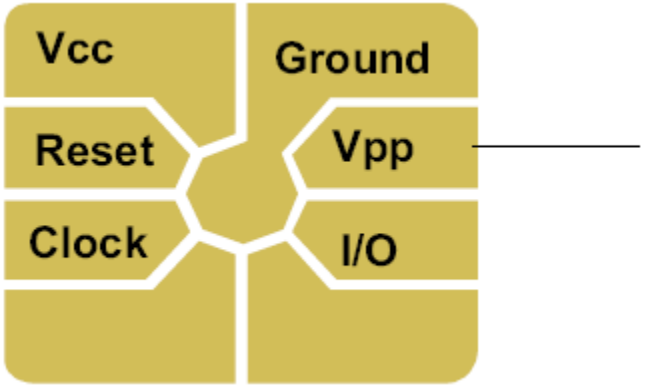
Δομή ολοκληρωμένου κυκλώματος



Τύποι επιθέσεων

- Φυσικοί (physical)
- Παράπλευρου καναλιού (side channel)
- Λογισμικού (software)
- Περιβαλλοντικοί (Environment)

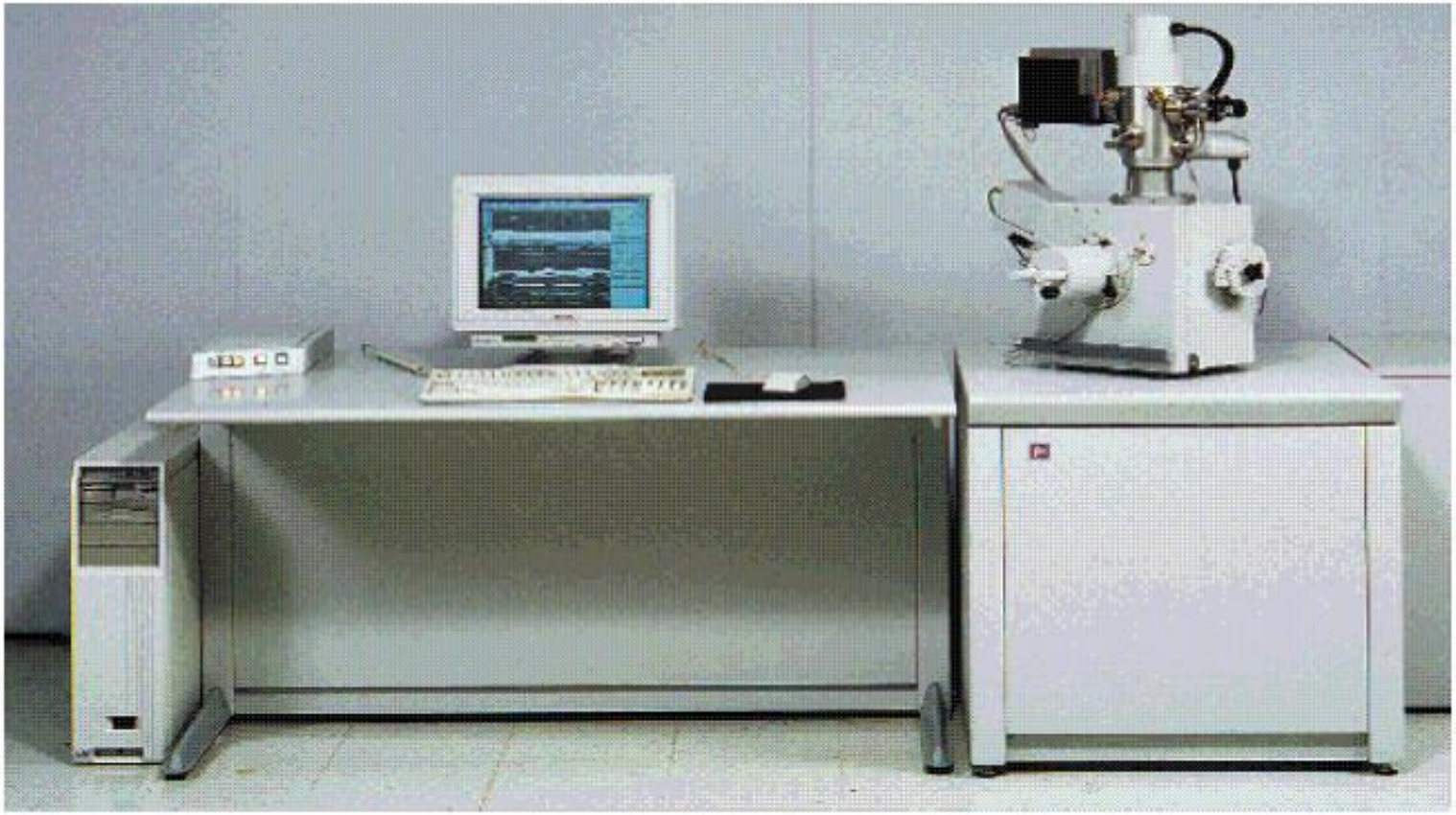
Διακοπή τροφοδοσίας



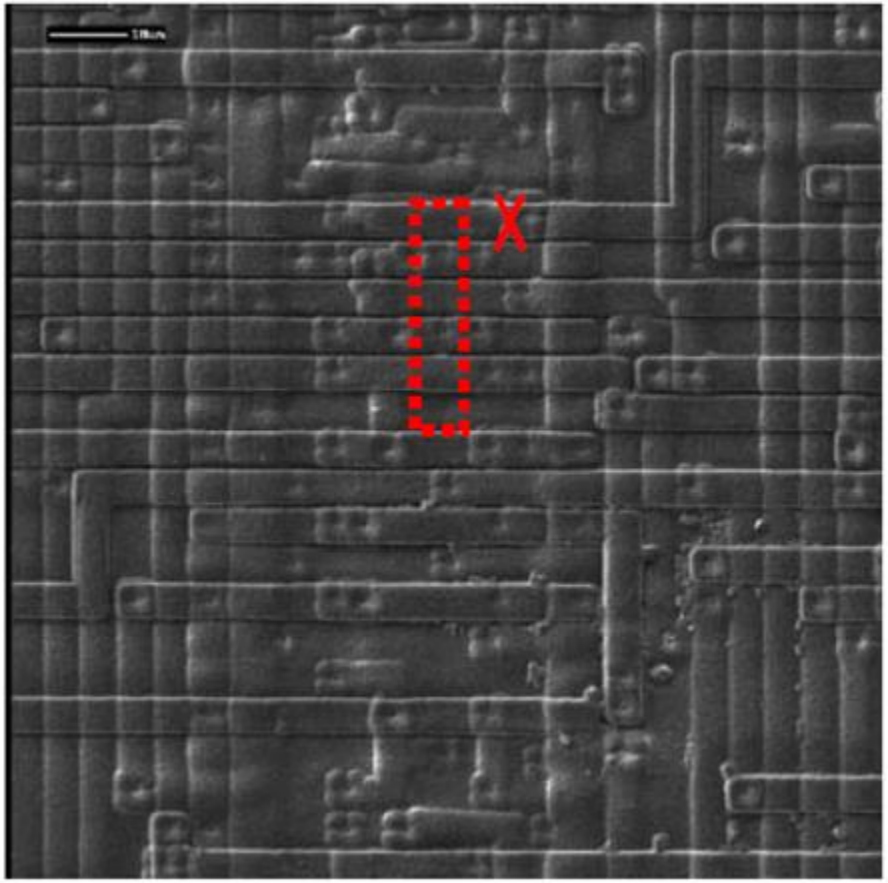
- Επίθεση στον ακροδέκτη V_{PP}
- Η κάρτα δεν διαβάζει/γράφει/επικοινωνεί

Σταθμοί ελέγχου (Probe Station)

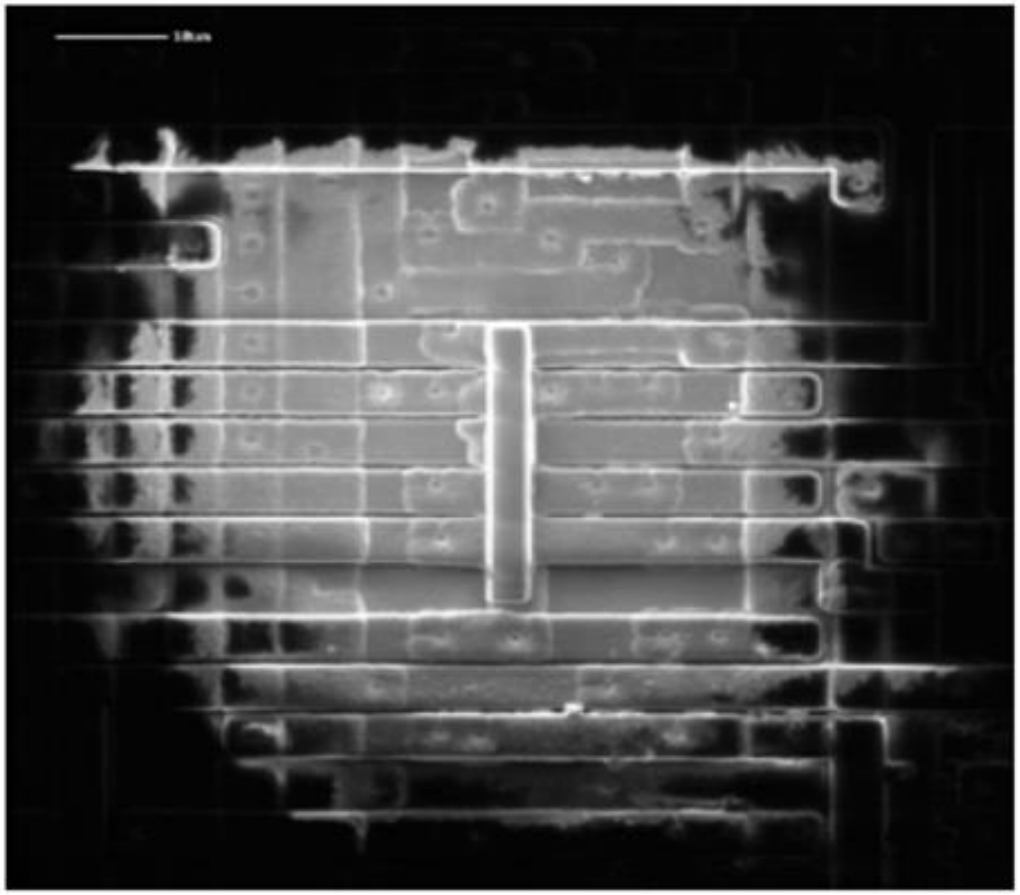
- Πολύ μεγάλο κόστος



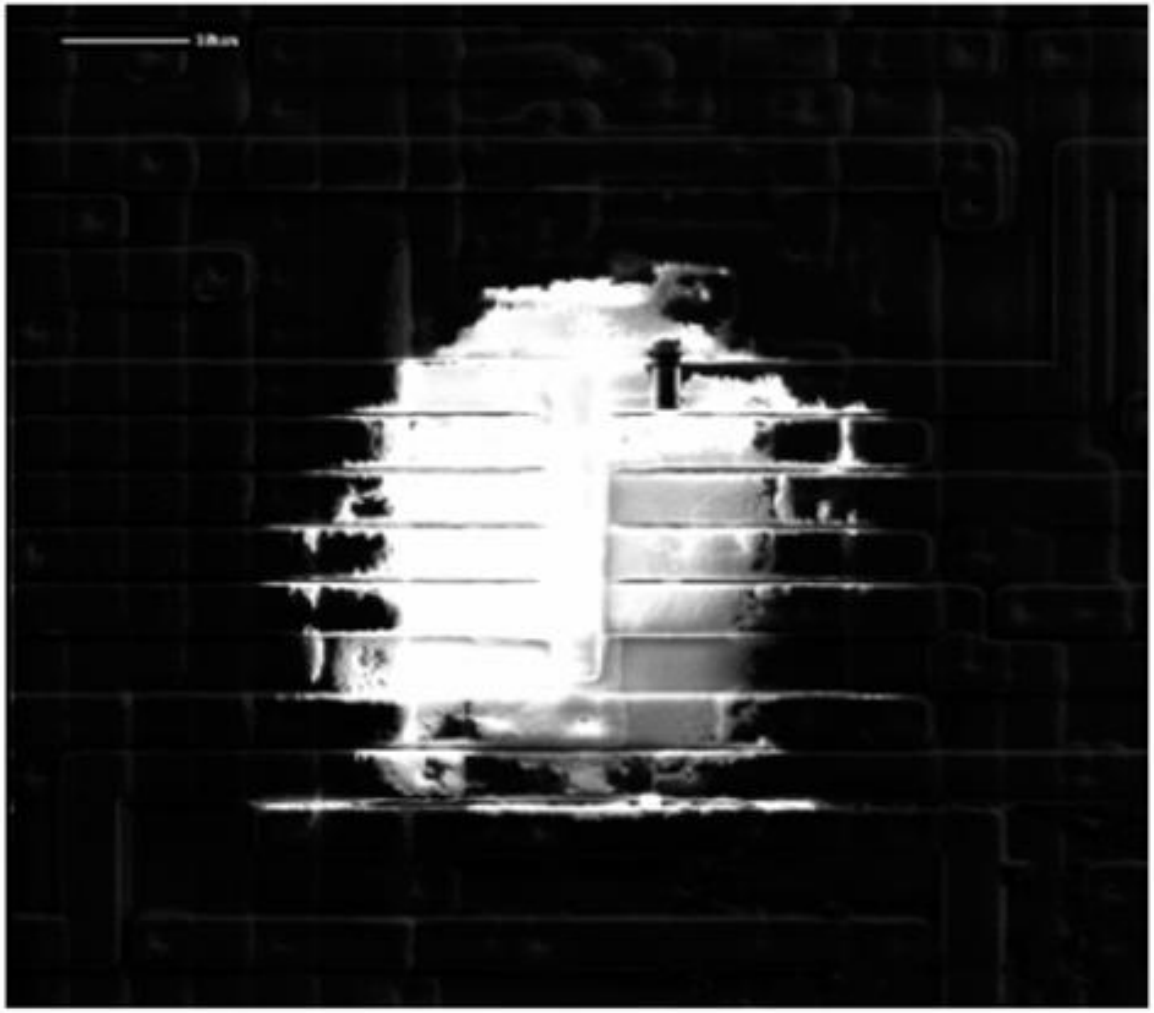
Αλλοίωση της καλωδίωσης του ολοκληρωμένου…



…Προσθήκη γέφυρας…

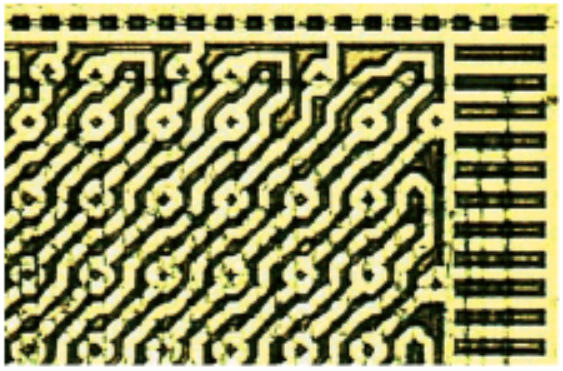


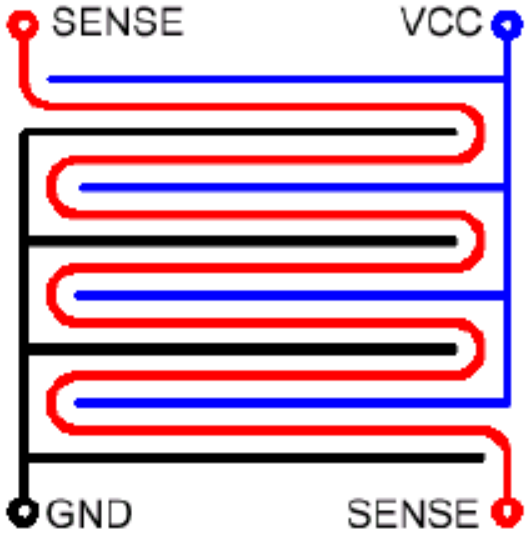
...Αποκοπή καλωδίου



Μέτρα προστασίας

- Πολλαπλά επίπεδα μετάλλων
- Bus scrambling
- Χρήση αισθητήρων στο ολοκληρωμένο που να μετράνε
  - θερμοκρασία, συχνότητα κλπ
- Ακεραιότητα
  - Χρήση αλγορίθμων κατά τη κατασκευή του ολοκληρωμένου





Επισκόπηση φυσικών επιθέσεων

ECSALab

- Μεγάλο κόστος
- Καταστρέφει το ολοκληρωμένο
- Εξαρτάται από τη συσκευή
- Χρονοβόρα διαδικασία

Επιθέσεις παράπλευρου καναλιού

- Ανιχνεύει πληροφορίες από τη διακίνηση δεδομένων στην έξυπνη κάρτα, όπως
- Χρόνος εκτέλεσης διεργασιών (Timing Attacks)
- Κατανάλωση ενέργειας (Simple Power-Analysis SPA, Differential Power Analysis DPA)
- Ηλεκτρομαγνητική ακτινοβολία (Electromagnetic SPA ή DPA)

Timing attacks…

- Έστω ότι τοποθετείται 10 $ στη μια κατσαρόλα και 28 $ στην άλλη

- Ερώτηση: Υπολόγισε
  - Green * 10 + blue *7
  - Πείτε μου αν το αποτέλεσμα είναι άρτιος ή περιττός αριθμός
- Είναι η απάντησή σας ικανή ώστε να αποκαλυφθεί το σωστό περιεχόμενο κάθε κατσαρόλας?

… Timing attacks

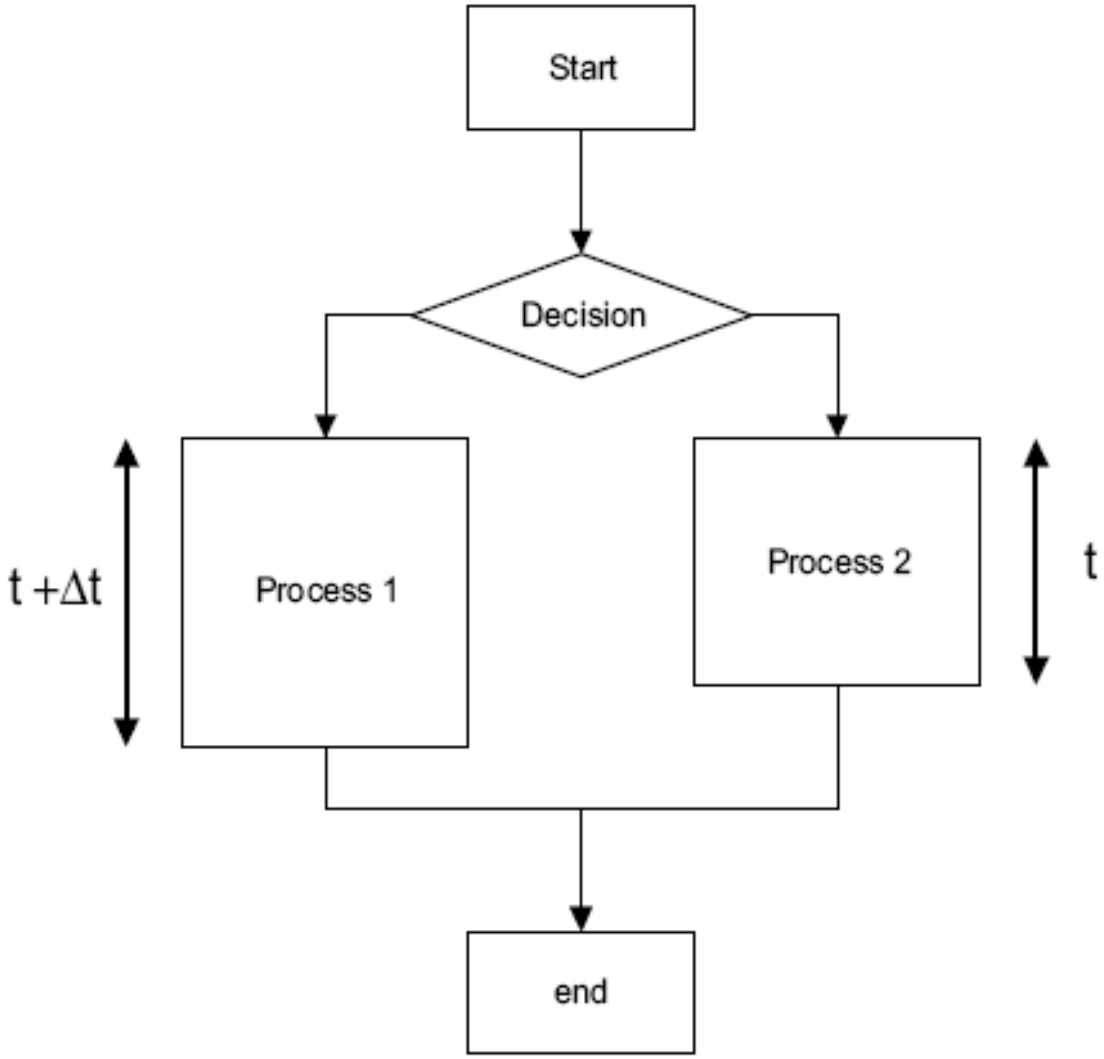
- Μάλλον όχι. Και αυτό γιατί…

  10 * 10 + 28∗ 7 = 296 (άρτιος)

  28 * 10 + 10 * 7 = 350 (περιττός)

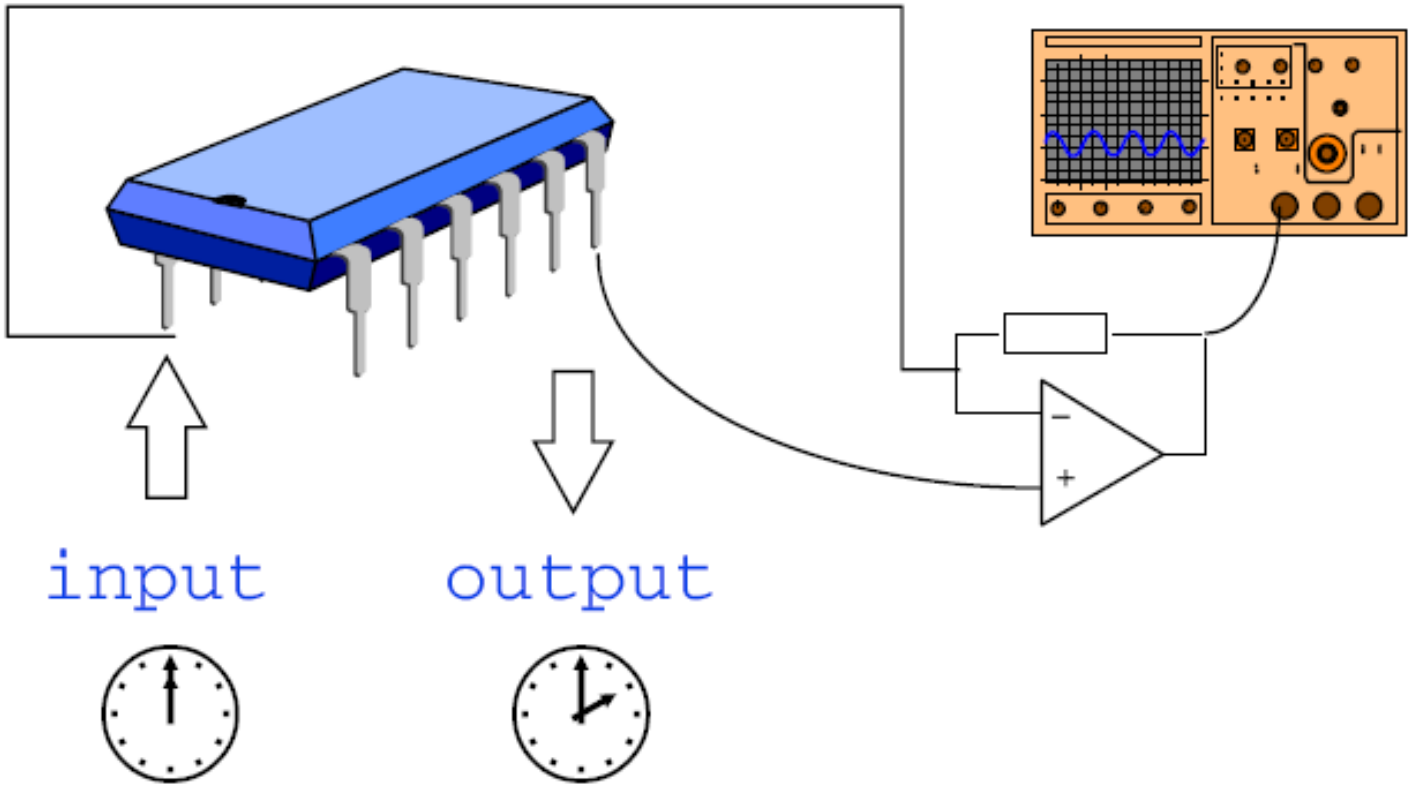
- Ωστόσο, με τον έλεγχο του χρόνου εκτέλεσης της κάθε πράξης θα ήταν δυνατή η εύρεση του σωστού περιεχομένου της κάθε κατσαρόλας

Timing attacks σε έξυπνες κάρτες



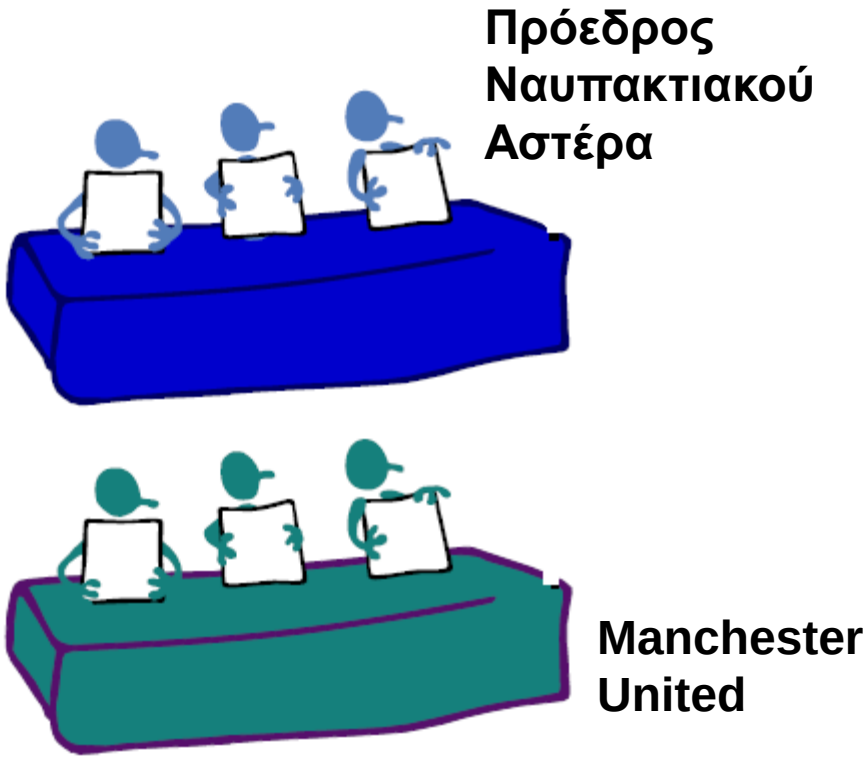
Power attacks…

- Μετράει τον χρόνο επεξεργασίας των δεδομένων και μετράει επίσης την κατανάλωση ενέργειας με σκοπό να ανακτήσει τα δεδομένα που εισάγονται



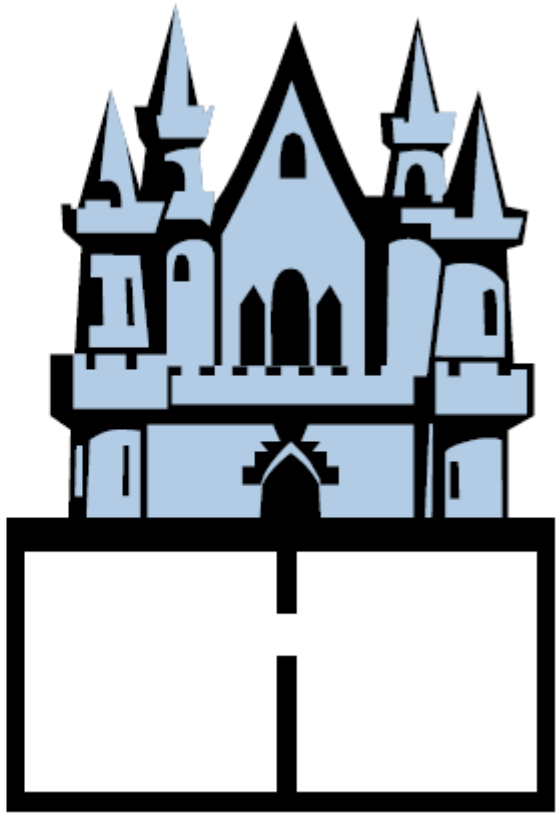
… Power attacks…

- Ο πρόεδρος της ποδοσφαιρικής ομάδας της Ναυπάκτου διαπραγματεύεται με τη Manchester United για την αγορά γνωστού κορυφαίου παίκτη της. Μια τοπική εφημερίδα στέλνει ένα δημοσιογράφο να διερευνήσει τη τελική απόφαση



… Power attacks …

- Όμως οι διαπραγματεύσεις λαμβάνουν χώρα σε ένα ξενοδοχείο του οποίου οι κουρτίνες είναι σκούρες και είναι κλειστές



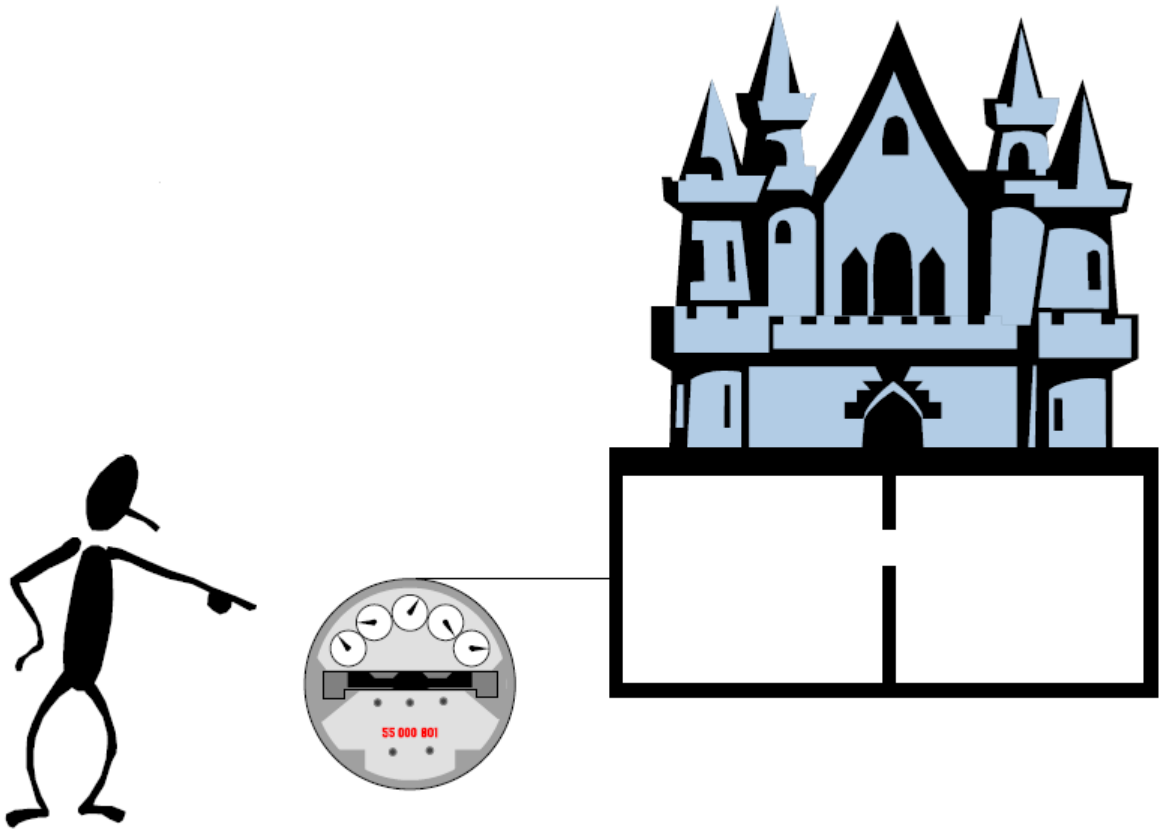
… Power attacks…

- Η ιδέα είναι η εξής

  Παρακολούθηση

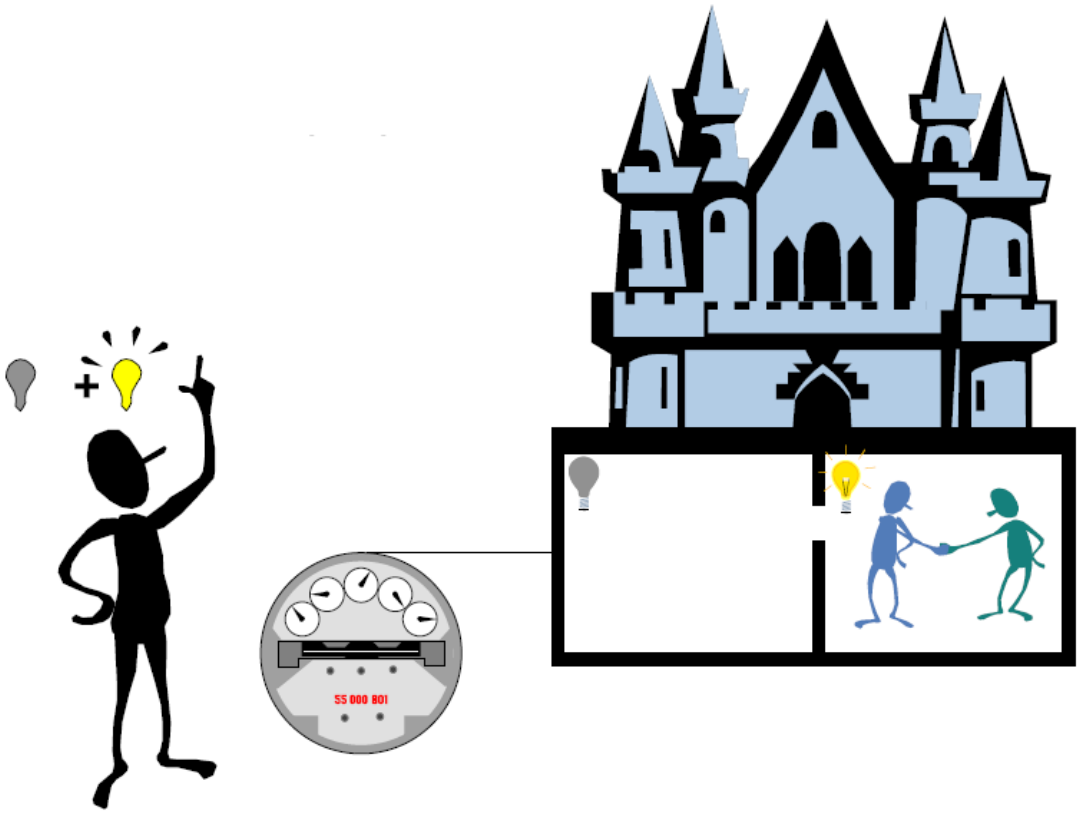
  του ρολογιού

  της ΔΕΗ



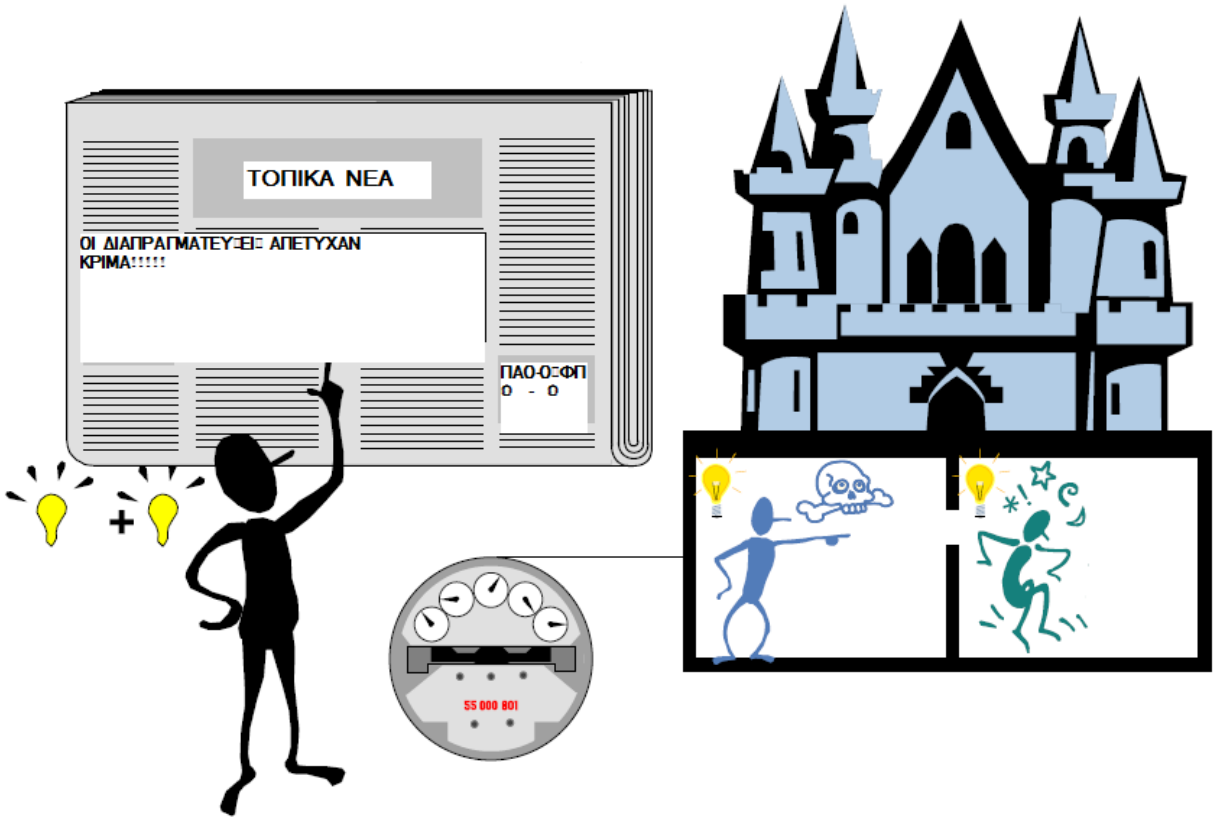
… Power attacks…

- Γυρνάει αργά?
  Επιτεύχθηκε η συμφωνία



…Power attacks

- Γυρνάει γρήγορα?
  Οι διαπραγματεύσεις
  συνεχίζονται!!!



Επίθεση Simple Power - Analysis στον RSA…

- SPA ενάντια στην RSA εκθετοποίηση του ιδιωτικού κλειδιού

$$s = m^d \bmod n$$

n αρκετά μεγάλο έστω 1024-bit

m μήνυμα

s αρχικό μήνυμα

d ο εκθέτης (ιδιωτικό κλειδί)

- Ο εισβολέας επιδιώκει την εύρεση του d

… Επίθεση Simple Power - Analysis στον RSA…

Η υλοποίηση του είναι γνωστή

- Αλγόριθμος “square and multiply”
- Τα bits του εκθέτη προσπελαύνονται από το MSB στο LSB (αριστερά προς δεξιά)

Let k = bitsize of d

Let s = m

For i = k-2 down to 0

Lets= s*s mod n *(SQUARE)*

If(bit i of d)is 1 then

Let s= s*m mod n *(MULTIPLY)*

End if

End for

Example : $s = m^9 = m^{(1001)b}$

init (MSB 1) $s = m$

round 2 (bit 0) $s = m^2$

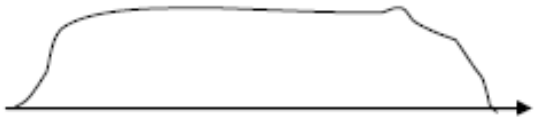
round 1 (bit 0) $s = (m^2)^2 = m^4$

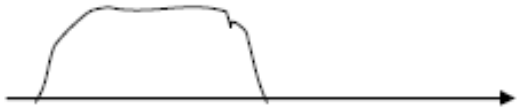
round 0 (bit 1) $s = (m^4)^2 * m = m^9$

… Επίθεση Simple Power - Analysis στον RSA…

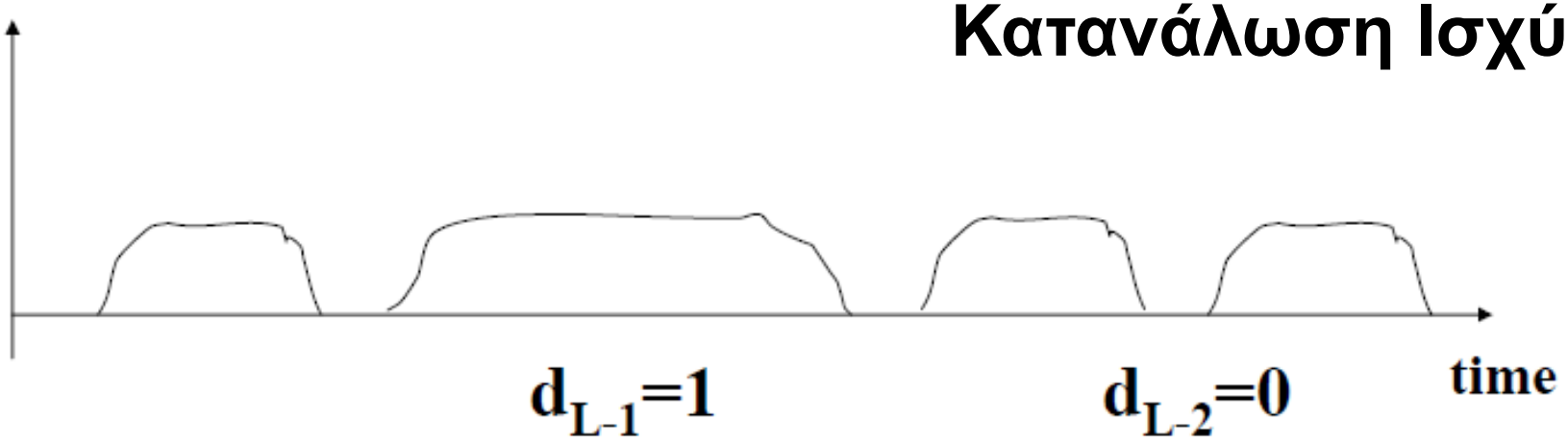
multiplication

squaring

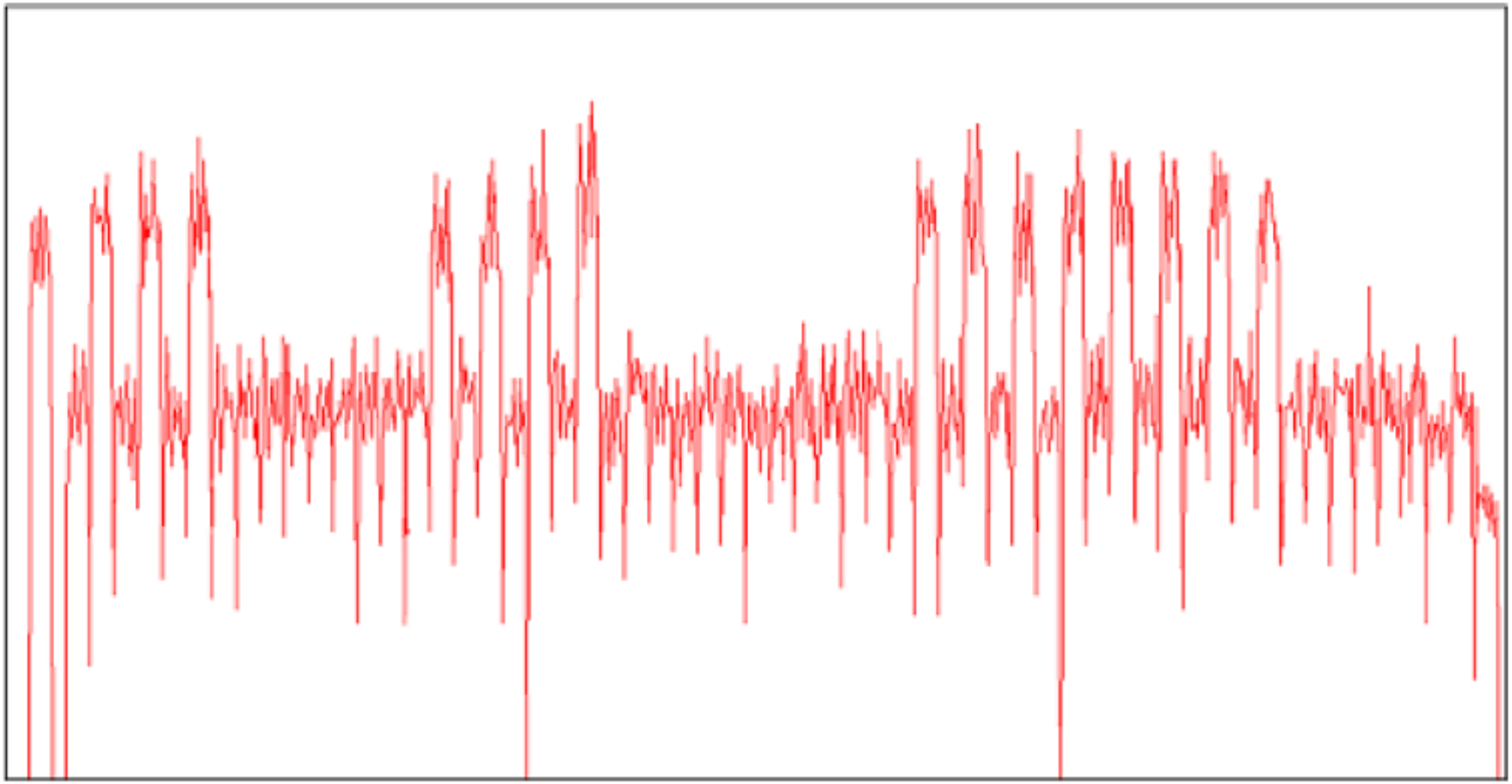




Κατανάλωση Ισχύος

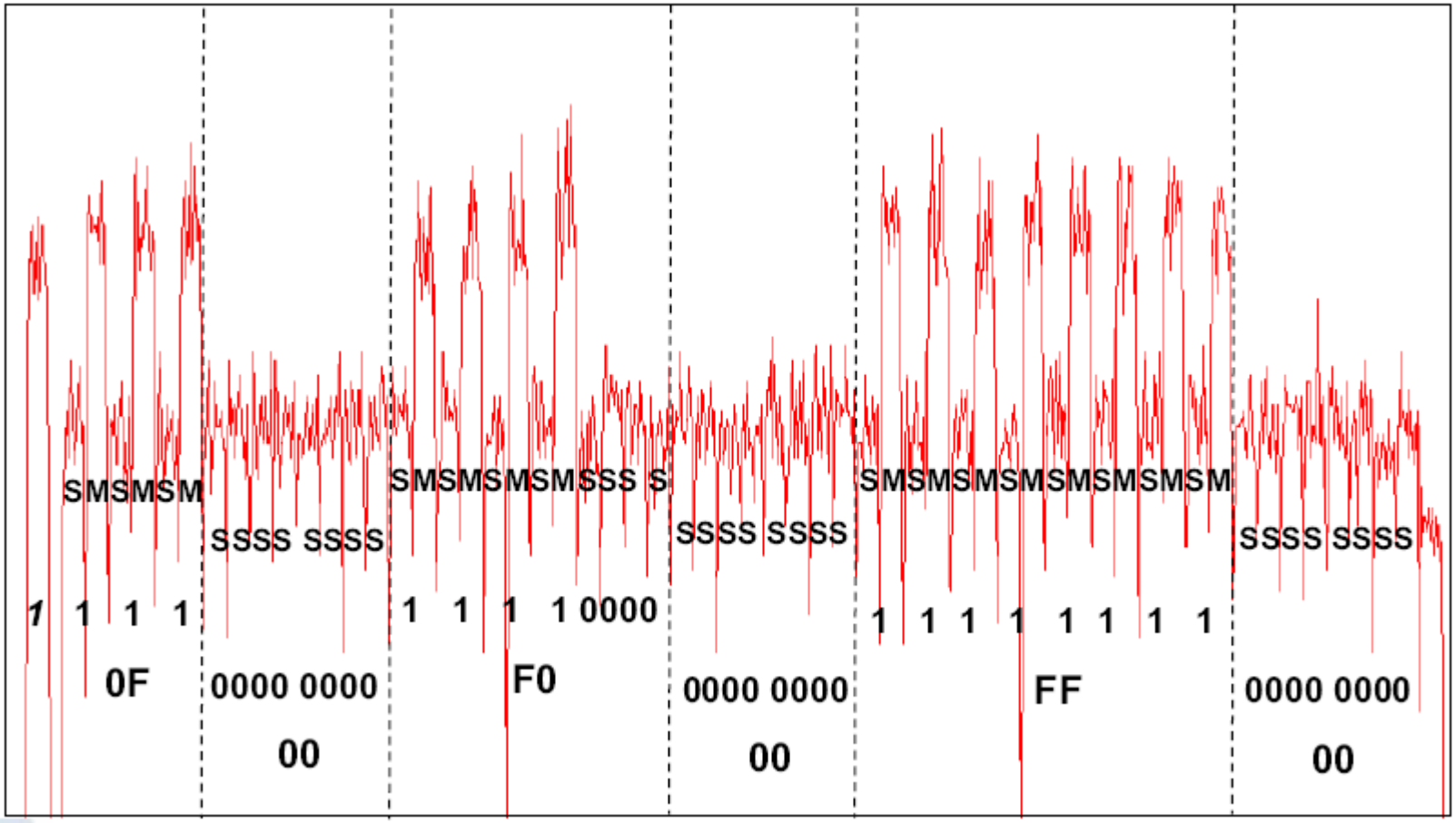


… Επίθεση Simple Power - Analysis στον RSA…



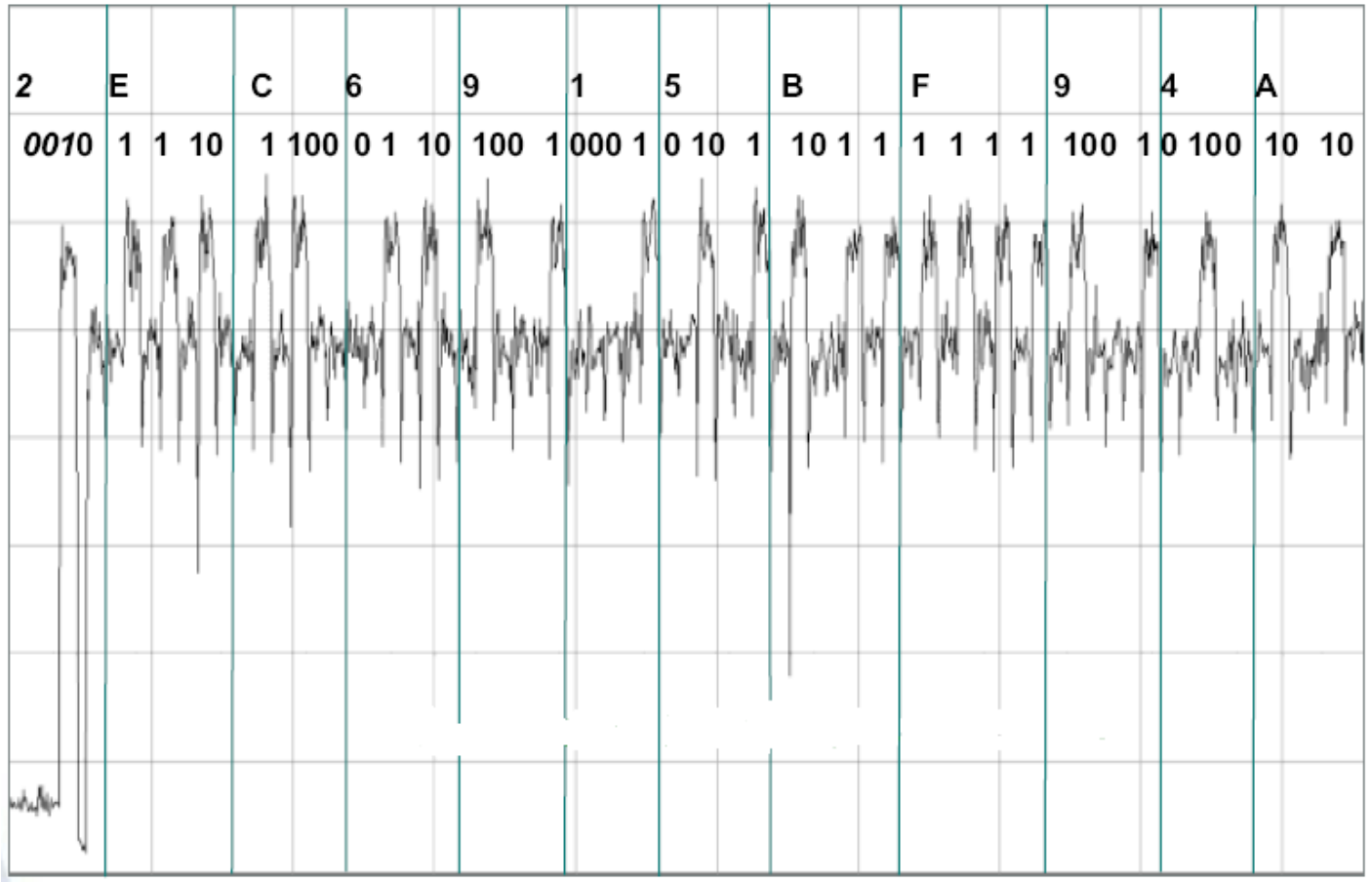
… Επίθεση Simple Power - Analysis στον RSA…

- Δοκιμή με το κλειδί **0F 00 F0 00 FF 00**



… Επίθεση Simple Power - Analysis στον RSA

- Κλειδί: **2E C6 91 5B F9 4A**



ECSALab

Απορίες/ σχόλια???