Power Analysis of RFID Tags

Yossi Oren and Adi Shamir
Computer Science Dept
The Weizmann Institute
Israel

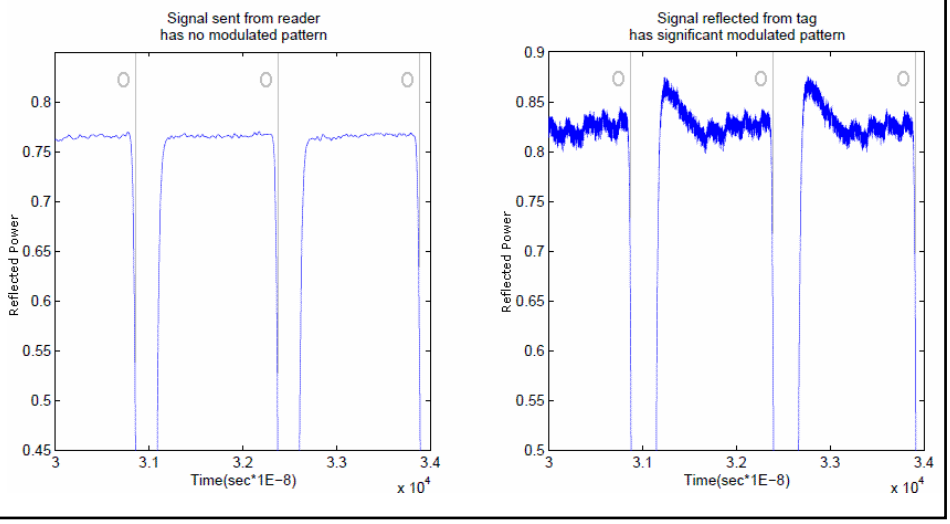
RFID Technology:

- Many types
- Many applications
- Cheap and simple
- No internal power supply
- Can we still apply power analysis?

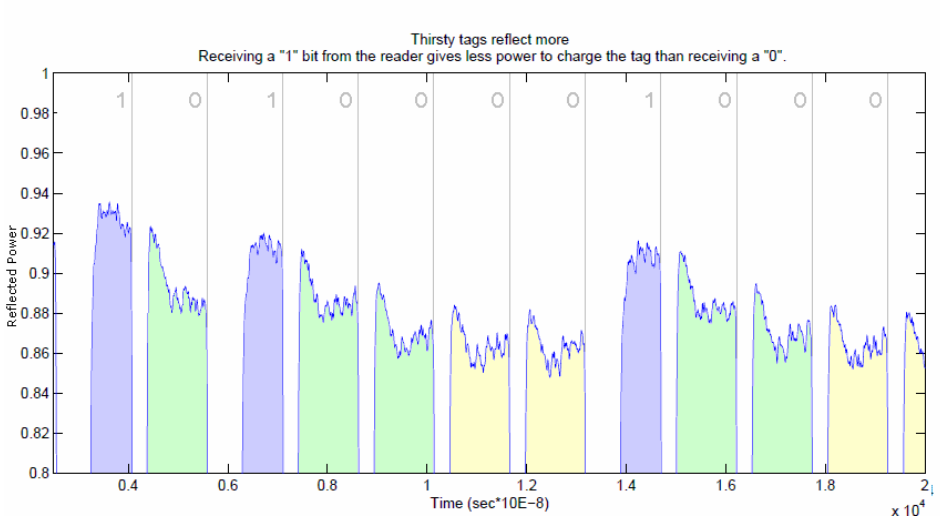
The laboratory set up:

- A standard tag (gen 1 or gen 2) and tag reader
- An antenna and amplifier for 900 MHz (note: already available in any GSM cellular phone)
- A digital scope to view and record the signals
- Total rental cost of all the equipment: <$1,000

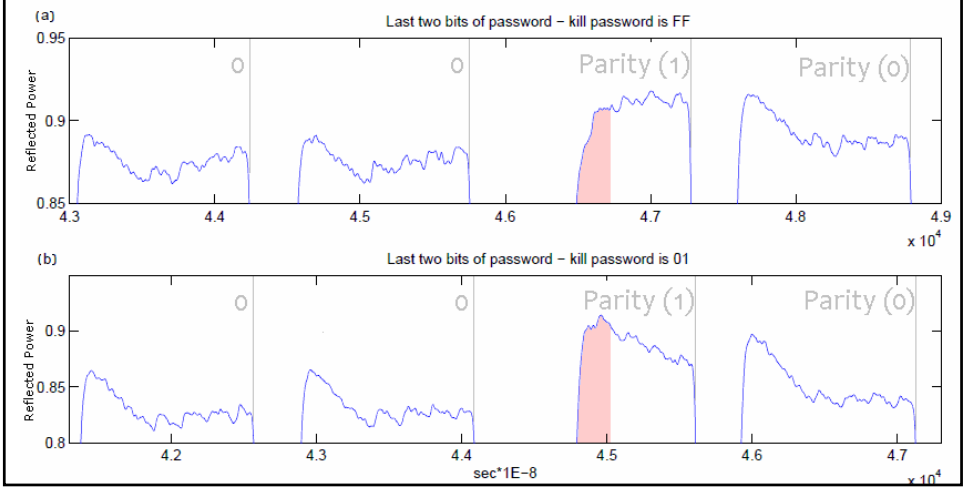
Electromagnetic signals: reader vs tag (recorded several meters away)



The tag's power consumption when it receives bits from the reader:



Power consumption when the tag receives a sequence of password bits:



Conclusions:

- Today's tags have kill and access passwords, but no high security crypto operations
- Just like smart cards, tags will evolve
- RFID tags seem to be particularly vulnerable to power analysis due to their simple design
- Countermeasures will have an impact on cost, power consumption, and operating range

More information available at:

www.wisdom.weizmann.ac.il/~yossio/rfid