Identification Systems
Lecture 4

Piotr Syga

2021-03-23

Examples of constrained devices

- Smartcards / Javacards
- RFID tags
- Pervasive systems / sensors

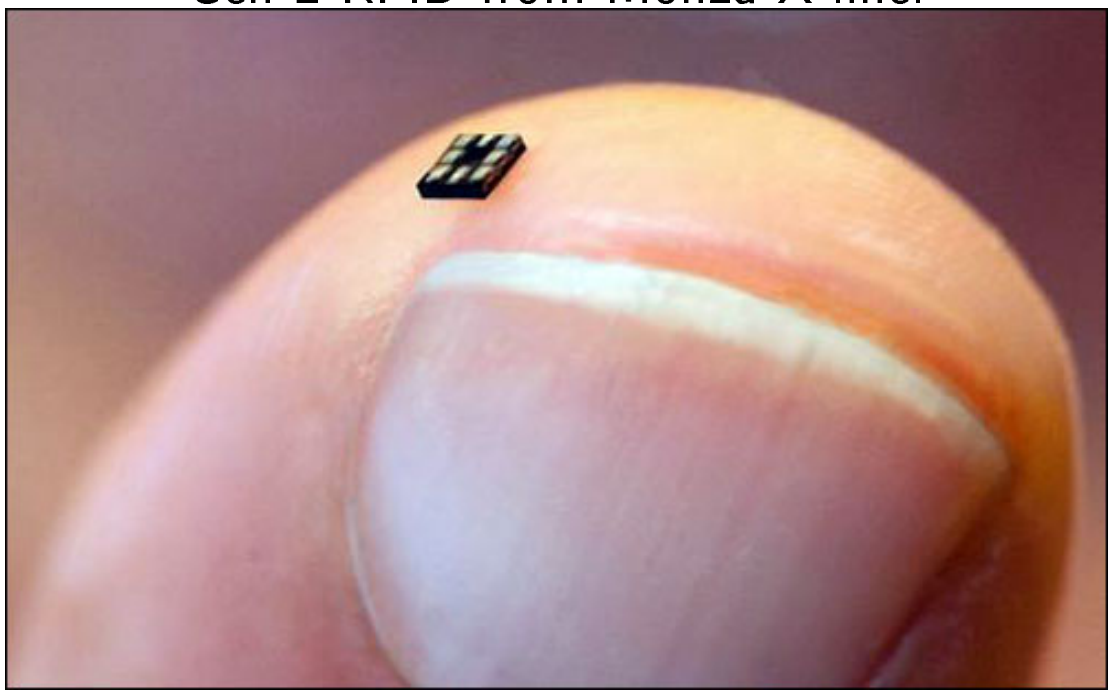
RFID systems

- varying computation power
- active tags vs passive tags
- applications from QR successor, pet door opener to documents



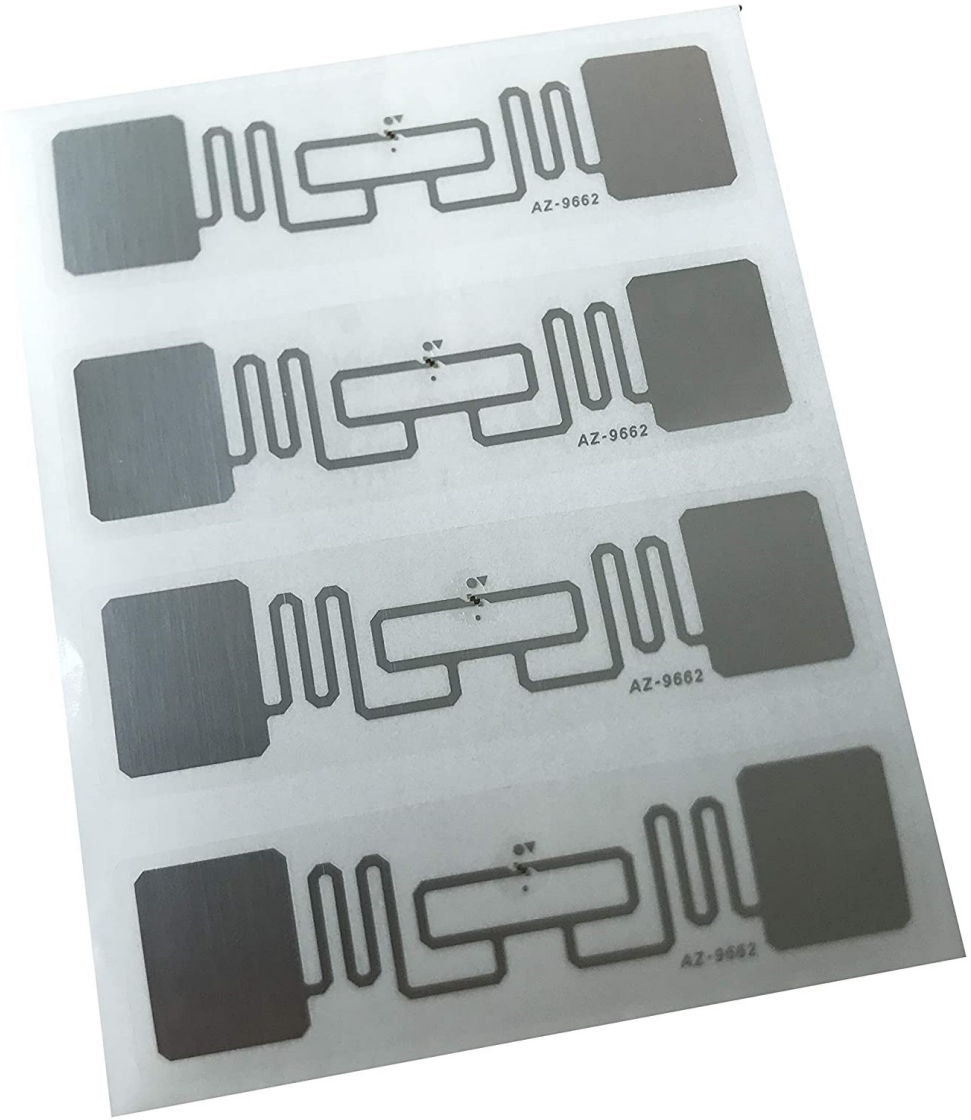
RFID systems

Gen-2 RFID from Monza-X line.

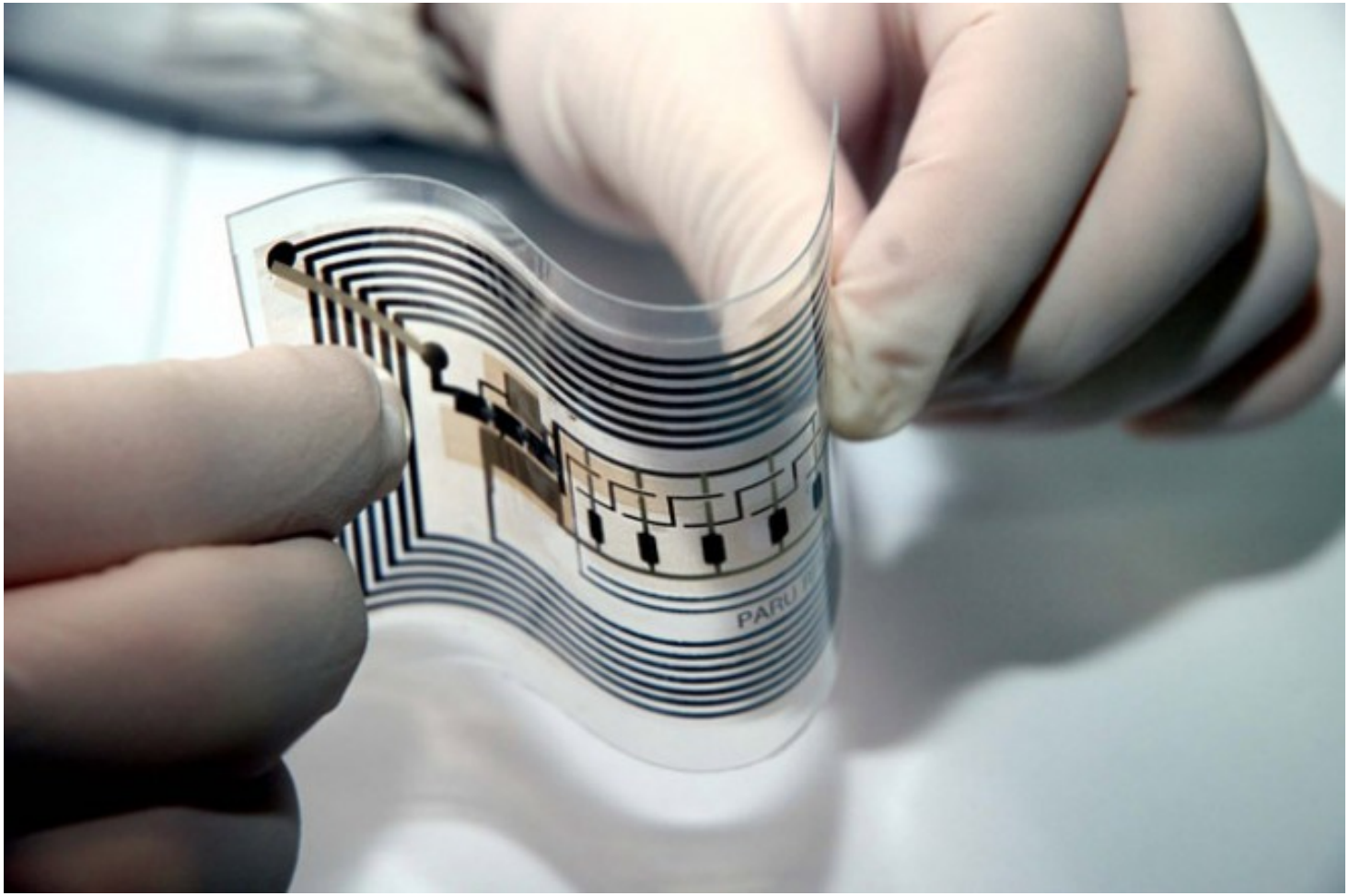


MX-8K provides 128b EPC and 8Kb User memory with physical size of 2x2x0.35 mm.

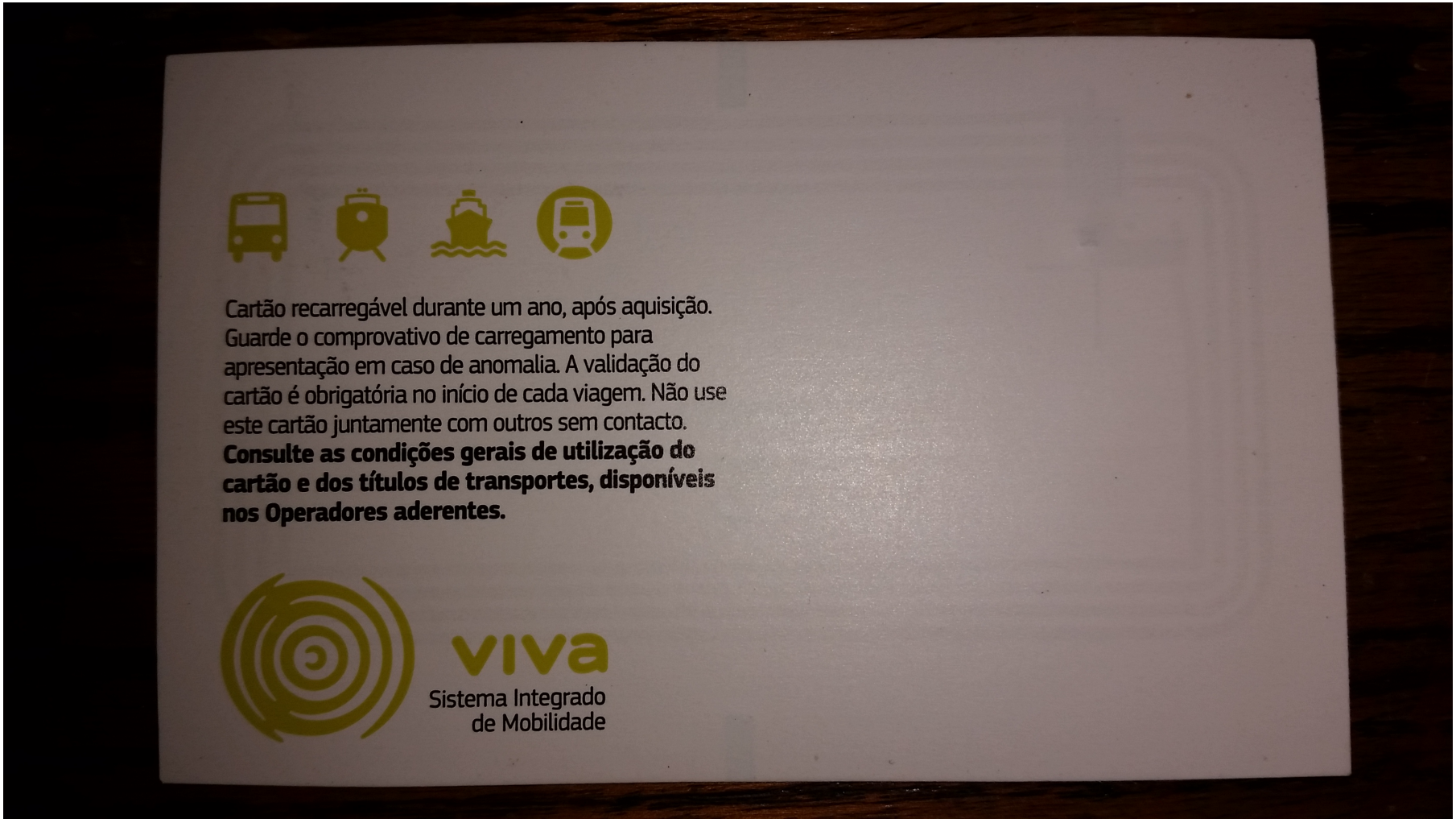
RFID systems



RFID systems



RFID systems

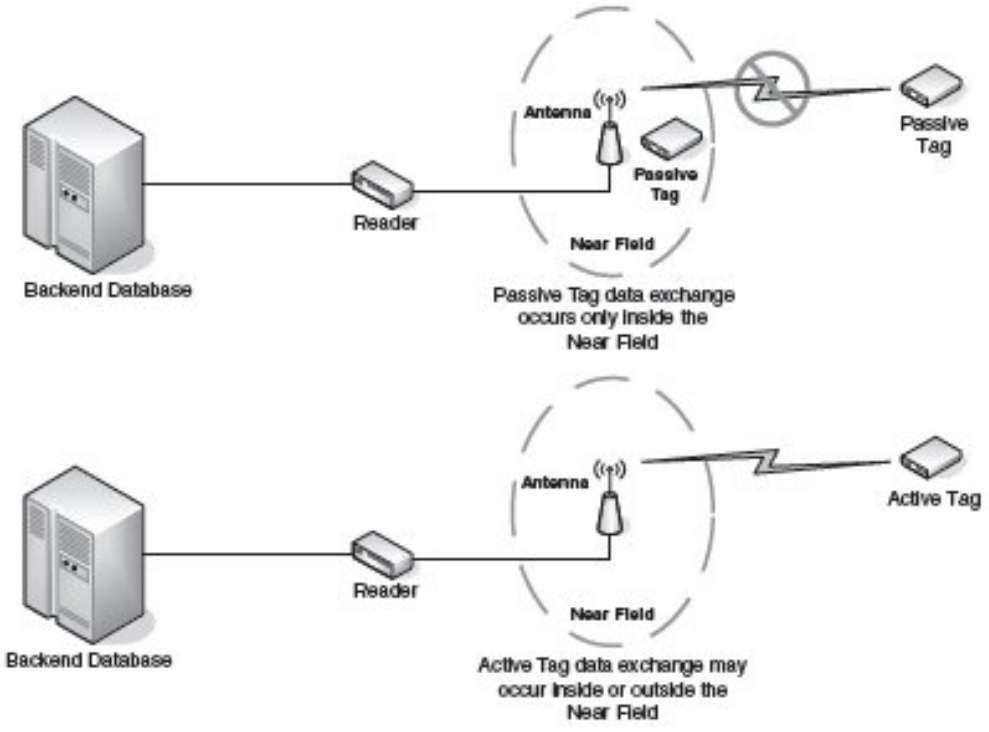


Tag Classes

EPC and ISO18000 describe:

- Class 0 : Read Only, passive tags
- Class 1 : Read Only, passive tags with unique ID (more memory and greater range)
- Class 2 : Read and Write (65K), passive tags
- Class 3 : Read and Write (65K), semi-passive tags with battery for increased range
- Class 4 : Read and Write, active tags able to communicate between each other
- Class 5 : Read and Write, active tags able to communicate with C4, C5 and stronger devices (protected memory)

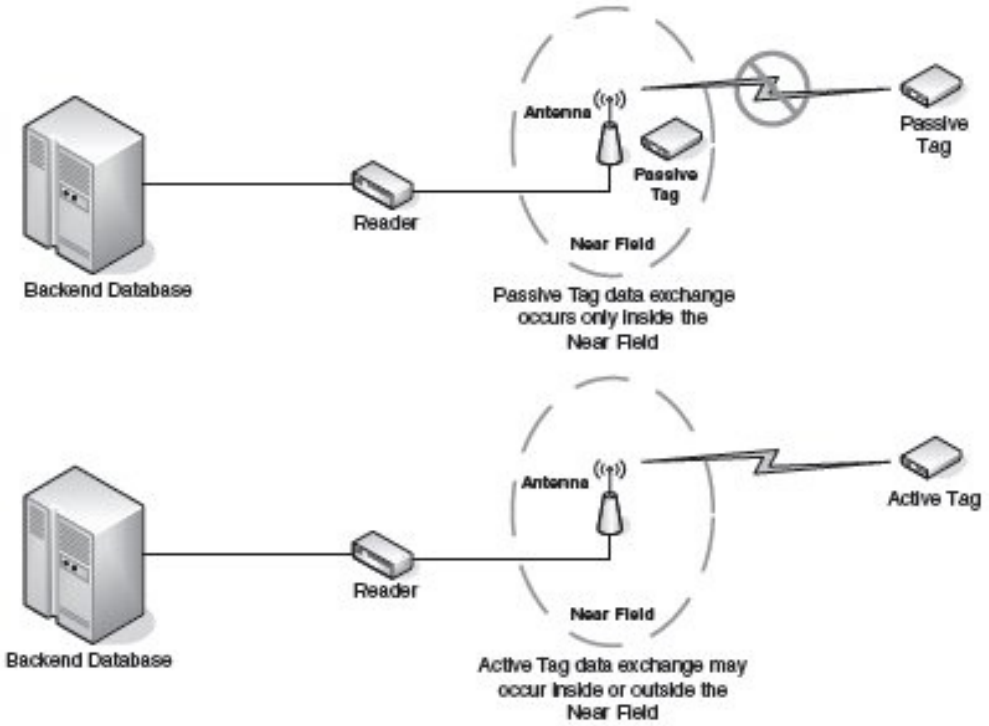
Communication



Communication models:

- MAC
- Beeping-model

Communication



Communication models:

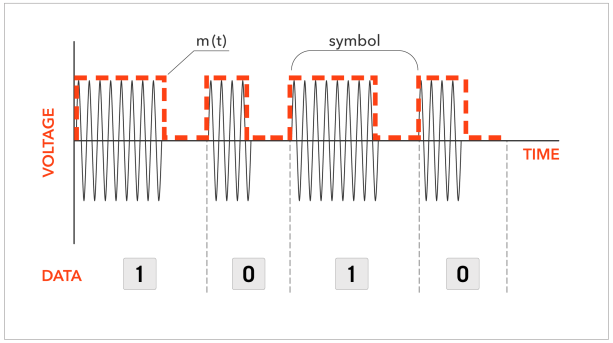
- MAC
- Beeping-model

Problem: Collisions – multiple tags in reader's range.

Coding

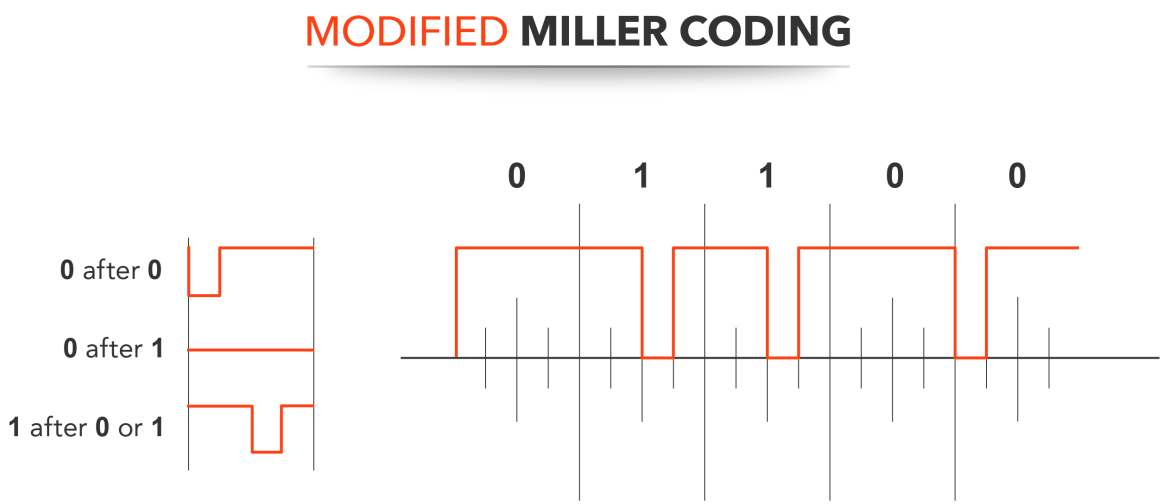
Images from www.atlasrfidstore.com





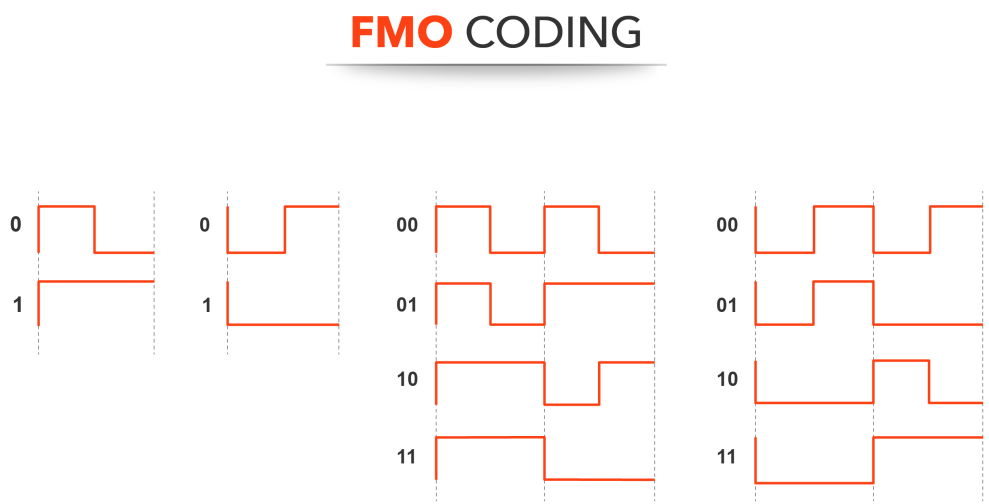
Coding

Images from www.atlasrfidstore.com

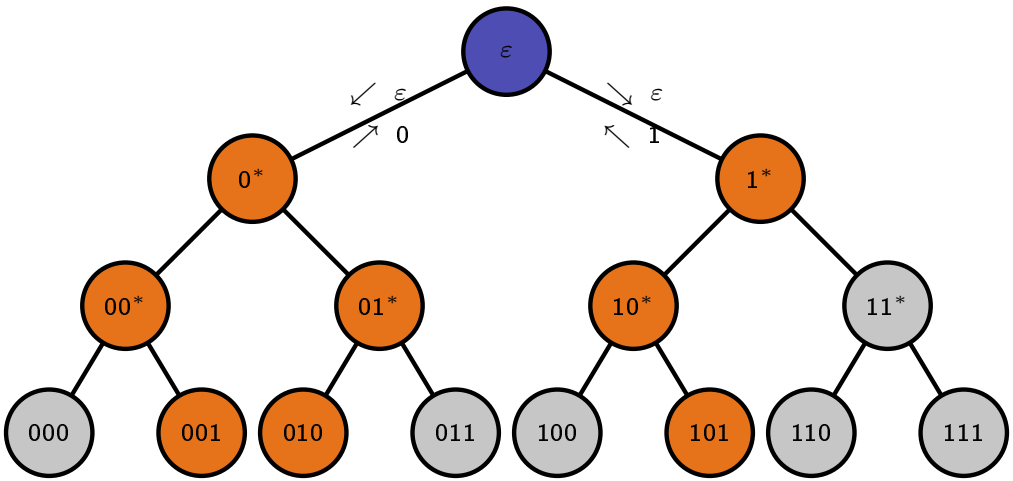


Coding

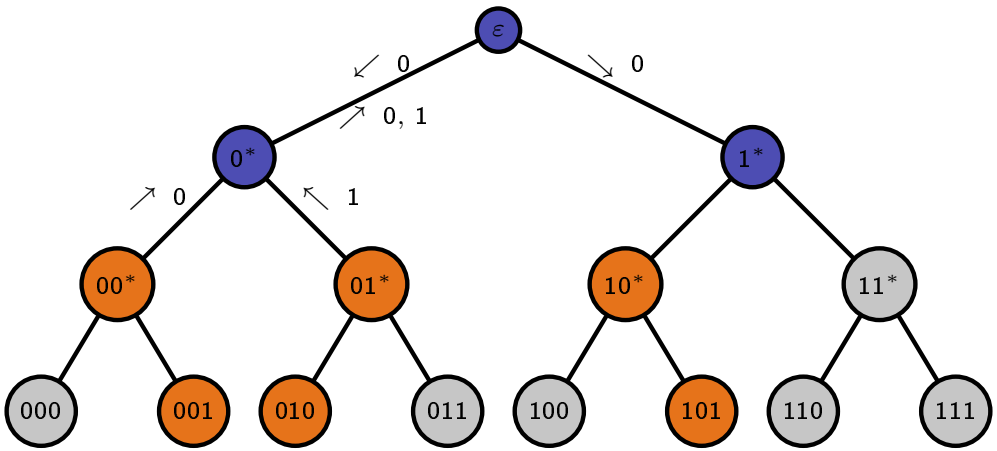
Images from www.atlasrfidstore.com



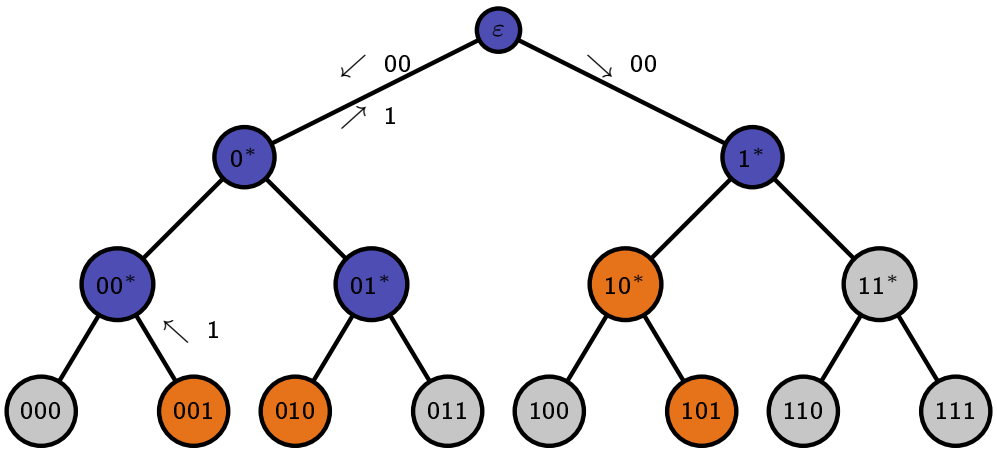
Query Tree



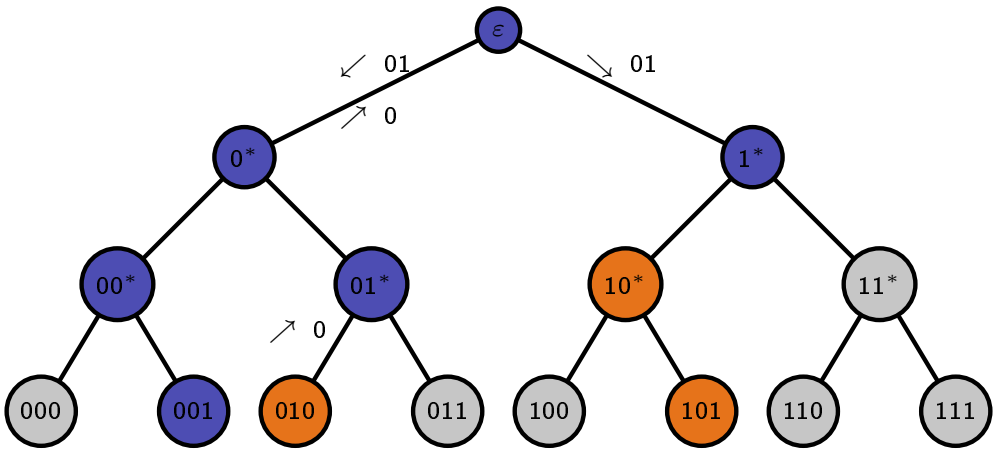
Query Tree



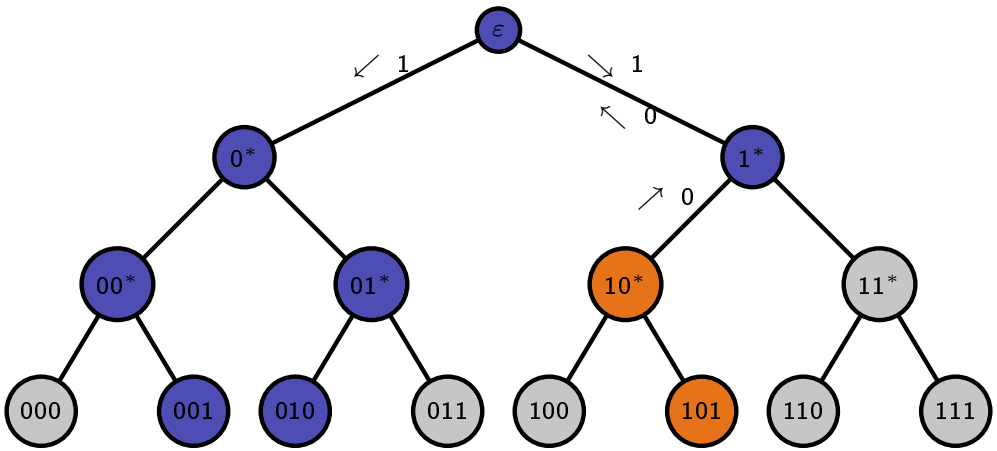
Query Tree



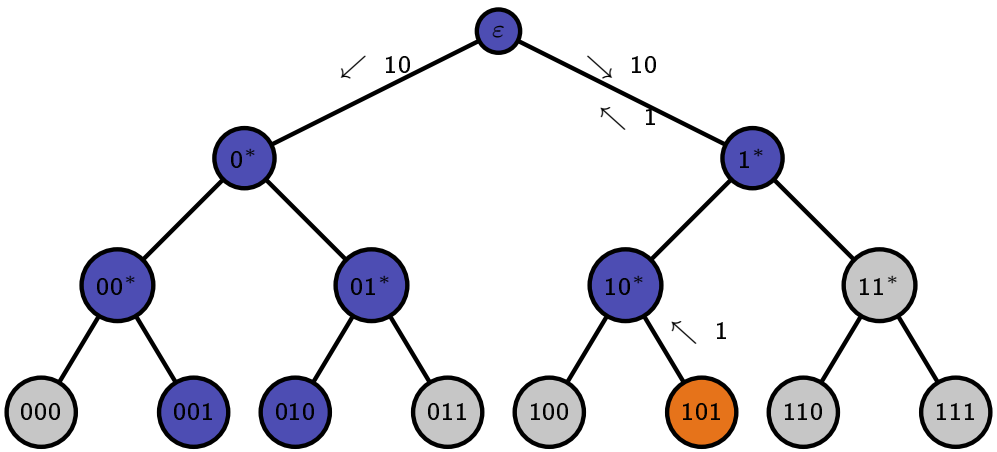
Query Tree



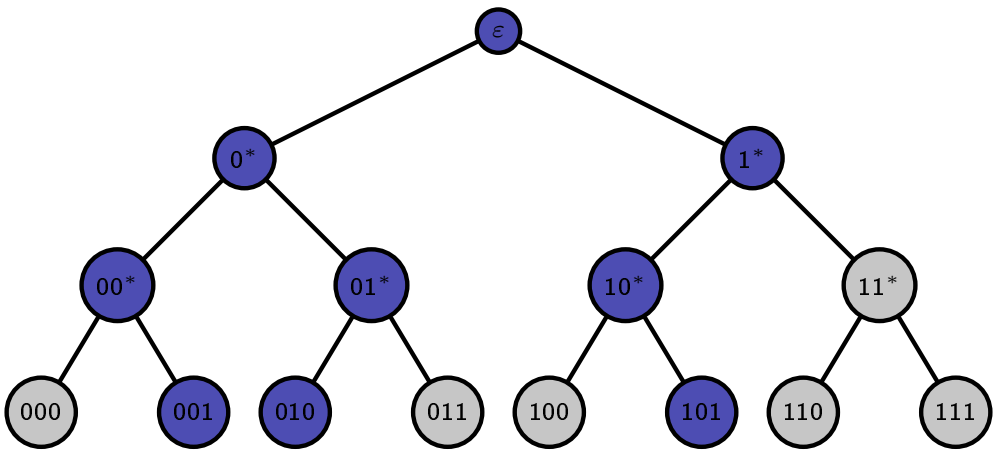
Query Tree



Query Tree



Query Tree



ALOHA – idea

- (Pure) ALOHA vs Slotted Aloha
- Send information whenever it is ready (for simplification enumerate it and add sender's ID)
- If no ACK-msg with the identifier is received – wait a random time and resend the message

Advantages:

- Simple method of transmission between reader and multiple tags
- Tags do not require synchronization
- Messages may be of arbitrary lengths
- Messages are sent immediately

E.g., protocol based on ALOHA by Chen and Kao.

Threats

- Denial of Service
- Tag cloning
- Privacy threats (eavesdropping, tracking, product identification, . . .)

Eavesdropping protection

Wang et al., *Securing Deployed RFIDs by Randomizing the Modulation and the Channel*

Communication : HF (13.56MHz, up to 10cm range), UHF (915MHz, up to 7m range).

Tags : Passive, wave modulation for data transmission.

Receiver : Perceives signal $y(t) = h_{rr}c(t) + h_{tr}x(t)c(t)$.

LocRF : Introduces random modulation to confuse the eavesdropper.

Eavesdropping protection

Wang et al., *Securing Deployed RFIDs by Randomizing the Modulation and the Channel*

Idea : Substituting the carrier $c(t)$ by a random noise $r(t)$ so that $y_{\text{reader}}(t)$ is readable and $y_{\text{eavesdropper}}(t)$ is hard to decode.

Frequency : Reader-generated $r(t)$ has to uphold to tag's response time (we assume 2MHz bandwidth), hence $2 \cdot 10^6$ complex samples per second is generated at random and quantized to 32b (due to DtA converter).

Eavesdropper's POV : After normalization, the eavesdropper perceives $y'(t) = r(t)[1 + \frac{h_{ce}}{h_{re}} x(t)]$.

Reader's POV : $y(t) = r(t)[h_{\text{self}} + h_{cr} x(t)]$. Since $r(t)$ is known and h_{self} may be removed due to circulator in full-duplex systems, the signal to be decoded stays as $\hat{y}(t) = h_{cr} x(t) r(t)$.

Eavesdropping protection

Wang et al., *Securing Deployed RFIDs by Randomizing the Modulation and the Channel*

Security:
For each bit b sent by the tag, adversary perceives k samples $(Y_1, \ldots, Y_k)$ $Y_i = R_i(1 + p_i^b)$, where R_i is randomly selected from complex Gausian distribution, and $(p_1^b, \ldots, p_k^b)$. Naturally, $p \approx \frac{h_{ce}}{h_{re}} x_0$ or $p \approx \frac{h_{ce}}{h_{re}} x_1$.
The maximum likelihood decoder compares probabilities $\Pr[b = 0|(Y_1, \ldots, Y_k)]$ and $\Pr[b = 1|(Y_1, \ldots, Y_k)]$. Since x_1 and x_0 are independent and equally probable, we can consider $\Pr[(Y_1, \ldots, Y_k)|b = 0]$ and $\Pr[(Y_1, \ldots, Y_k)|b = 1]$. Since each of k samples is independent, $\Pr[Y|b = 0] = \frac{1}{(2\pi)^{k/2}\Pi\sigma_i^0} \exp\{-\Sigma_i^k(\frac{|Y_i|}{\sigma_i^0})^2\}$, similarly $\Pr[Y|b = 1]$.

Eavesdropping protection

Wang et al., *Securing Deployed RFIDs by Randomizing the Modulation and the Channel*

Security cont.:
Assuming the number of p^0s and p^1s to be approximately even, we can state that $\Pi\sigma_i^0 = \Pi\sigma_i^1$, hence the compared probabilities may be simplified to comparing $\Sigma_i^k(\frac{|Y_i|}{\sigma_i^0})^2$ and $\Sigma_i^k(\frac{|Y_i|}{\sigma_i^1})^2$. Utilizing specific transmission model (HF or UHF) we may simplify it even further, to verification of two 'signal windows' and check whether (for HF) $|Y_2|^2 + |Y_4|^2 + |Y_6|^2 + |Y_8|^2 > |Y_9|^2 + |Y_{11}|^2 + |Y_{13}|^2 + |Y_{15}|^2$.

Eavesdropping protection

Wang et al., *Securing Deployed RFIDs by Randomizing the Modulation and the Channel*

BER (for HF):
Let us define $U = |Y_2|^2 + |Y_4|^2 + |Y_6|^2 + |Y_8|^2$ and $V = |Y_9|^2 + |Y_{11}|^2 + |Y_{13}|^2 + |Y_{15}|^2$, additionally $Z = U - V$. For the optimal decoder, $\mathrm{BER} = \frac{1}{2}\Pr[Z < 0|b = 0] + \frac{1}{2}\Pr[Z > 0|b = 1]$. Since Ys are independent and normal distributed, $U \sim \Gamma(4, 2\sigma_U^2)$ and $V \sim \Gamma(4, 2\sigma_V^2)$, we may show that $\Pr[Z < 0|b = 0] = \Pr[Z > 0|b = 1]$ and $\Pr[Z < 0|b = 0] = \int_{-\infty}^{0} \Pr[Z = z|b = 0]dz =$
$\frac{20\mu^3}{(1+\mu)^7} + \frac{10\mu^2}{(1+\mu)^6} + \frac{4\mu}{(1+\mu)^5} + \frac{1}{(1+\mu)^4} = \mathrm{BER}$

Tracking prevention

M. Klonowski, M. Kutyłowski, PS: *Chameleon RFID and Tracking Prevention*

- Constrained RFID tags without secrets
- Adversary may capture and temper with the tags
- Honest tags security is not compromised by capturing others
- Adversary is not ubiquitous
- Even compromised tags, when not observed *for a while* become untrackable again
- **Idea:** evolution of the ID.