AUTO-ID LABS

Tag Chip Technologies

Prof. Hao Min
Auto-ID Labs at Fudan University, China

Jan. 23, 2006

Outlines

- **User requirements**
- **Performance enhancements**
- **Some new technologies being developed**

User Requirements

- **Long read range**
- **100% read coverage**
- **Similar read performance in the worldwide frequency range 860-960MHz**
- **Security and authentication**

Improve the Read Range
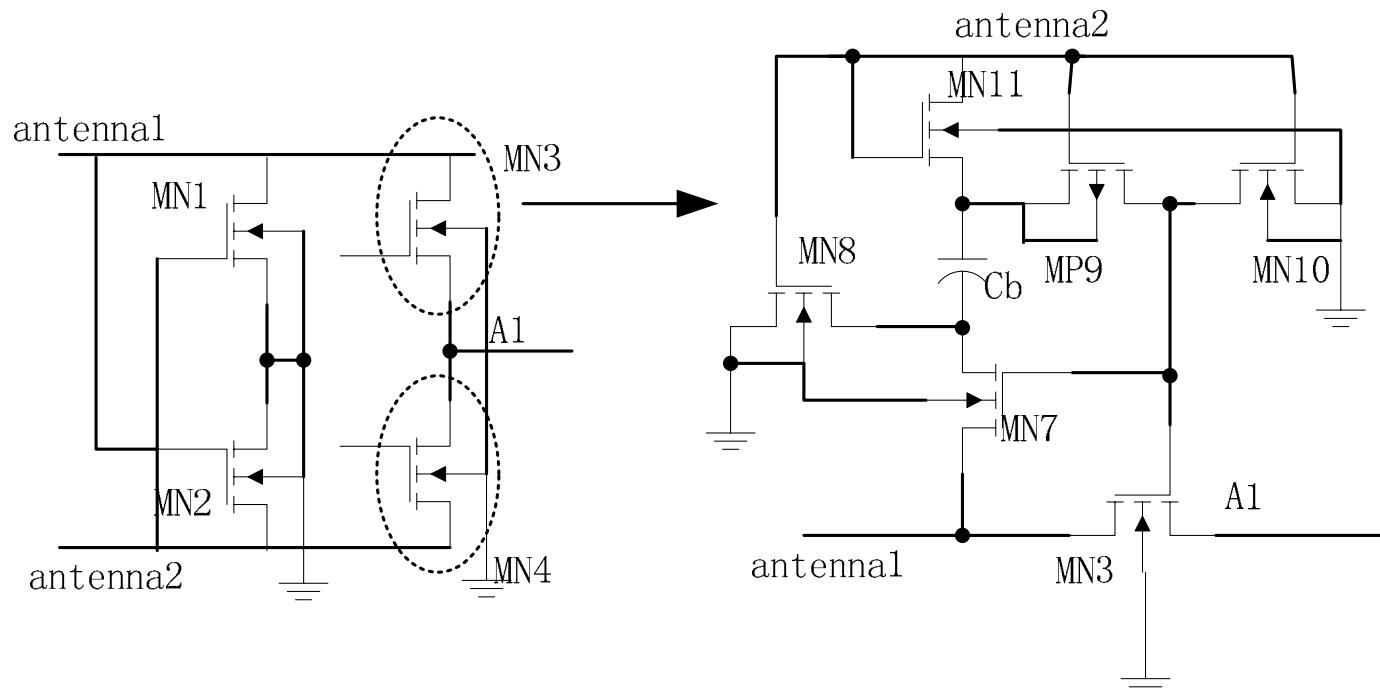
- **Lower the power consumption of tag chips**
  - Improve the conversion efficiency of rectifier
    - Bootstrapped circuits
    - Low Vt using Schottky diode
  - Sub-threshold digital circuits
    - Vdd =0.5V
    - Dynamic adjust of communication speed based on received power
  - Adiabatic circuits
    - Energy recycling
 - Conventional low power circuit design technologies

Bootstrapped Rectifier

- **Improve the rectify efficiency by 30-100%**
- **Suitable for HF tag**
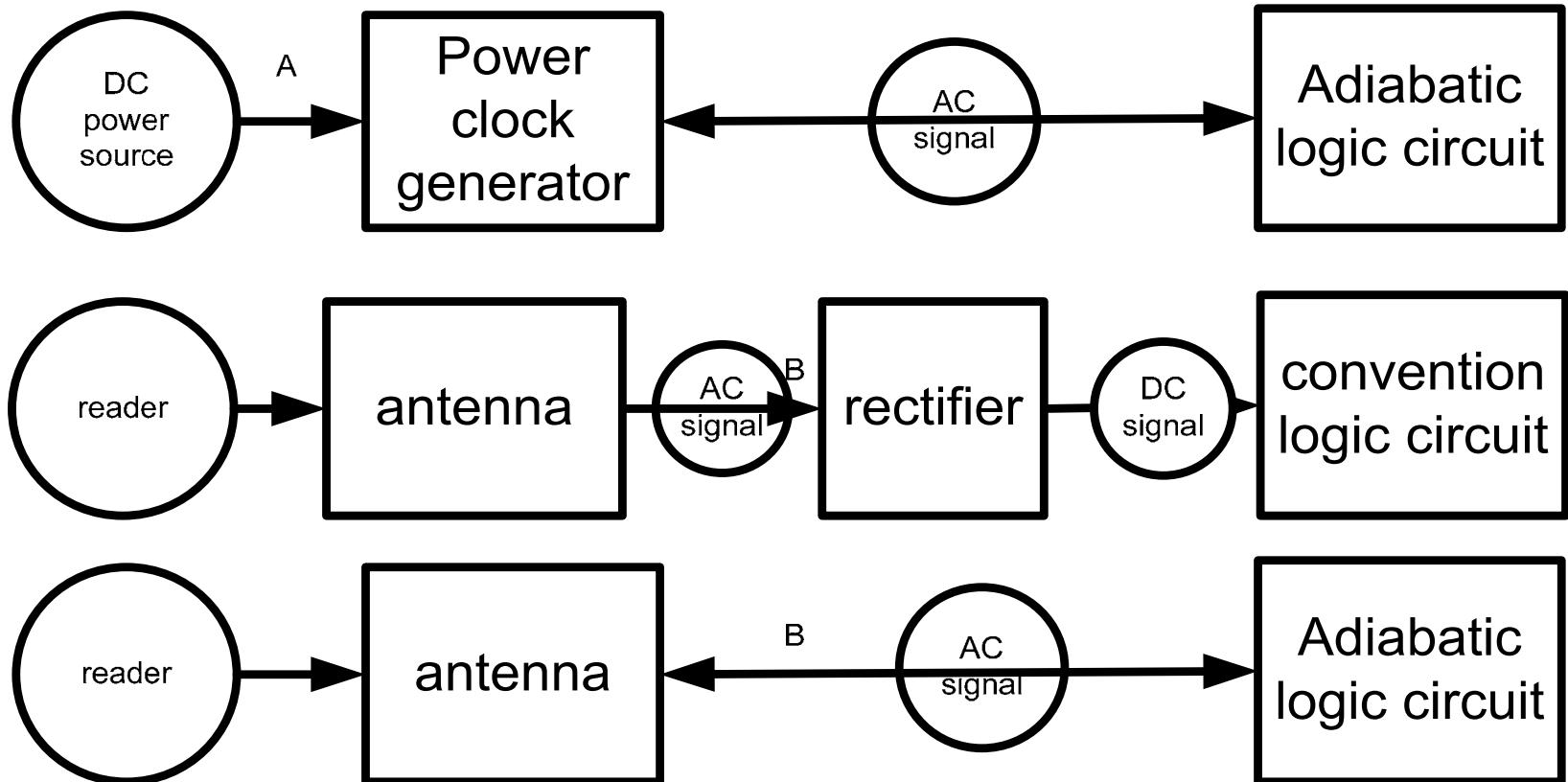
Adiabatic Circuits for RFID
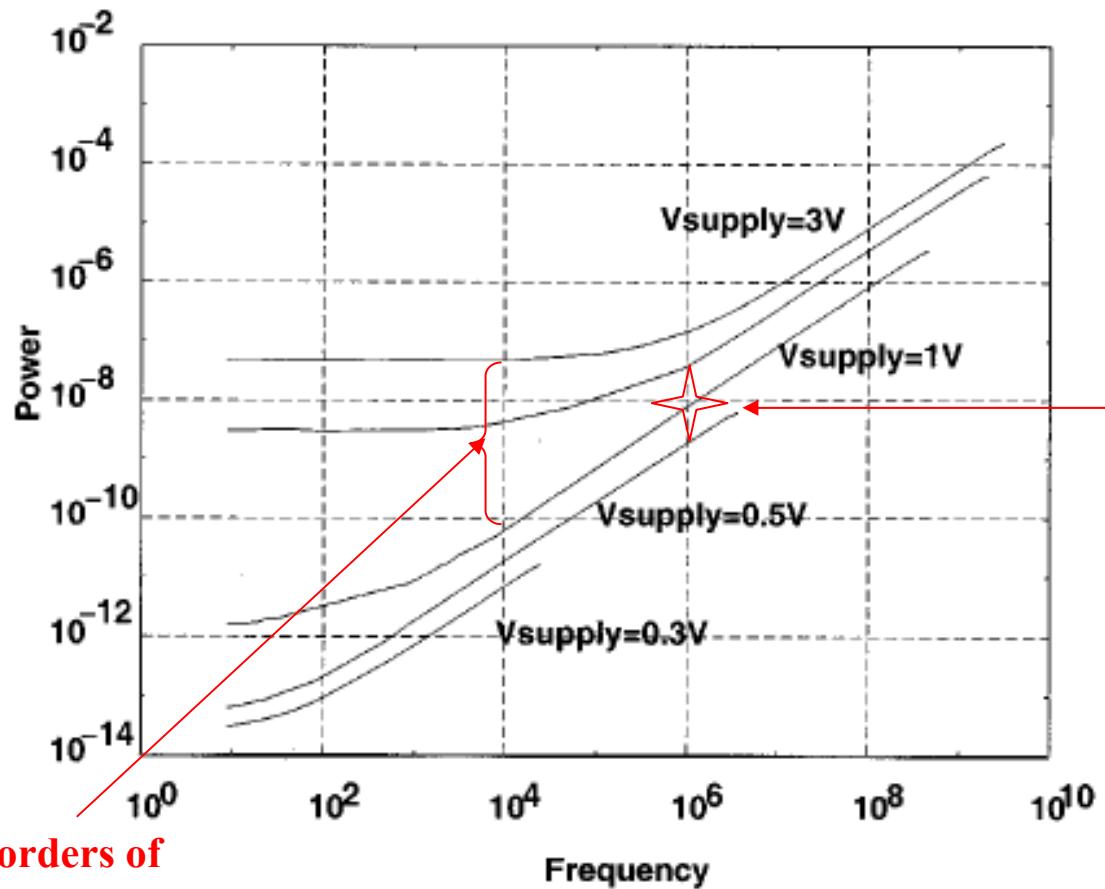
- **50% power drop is expected**

AUTO–ID LABS
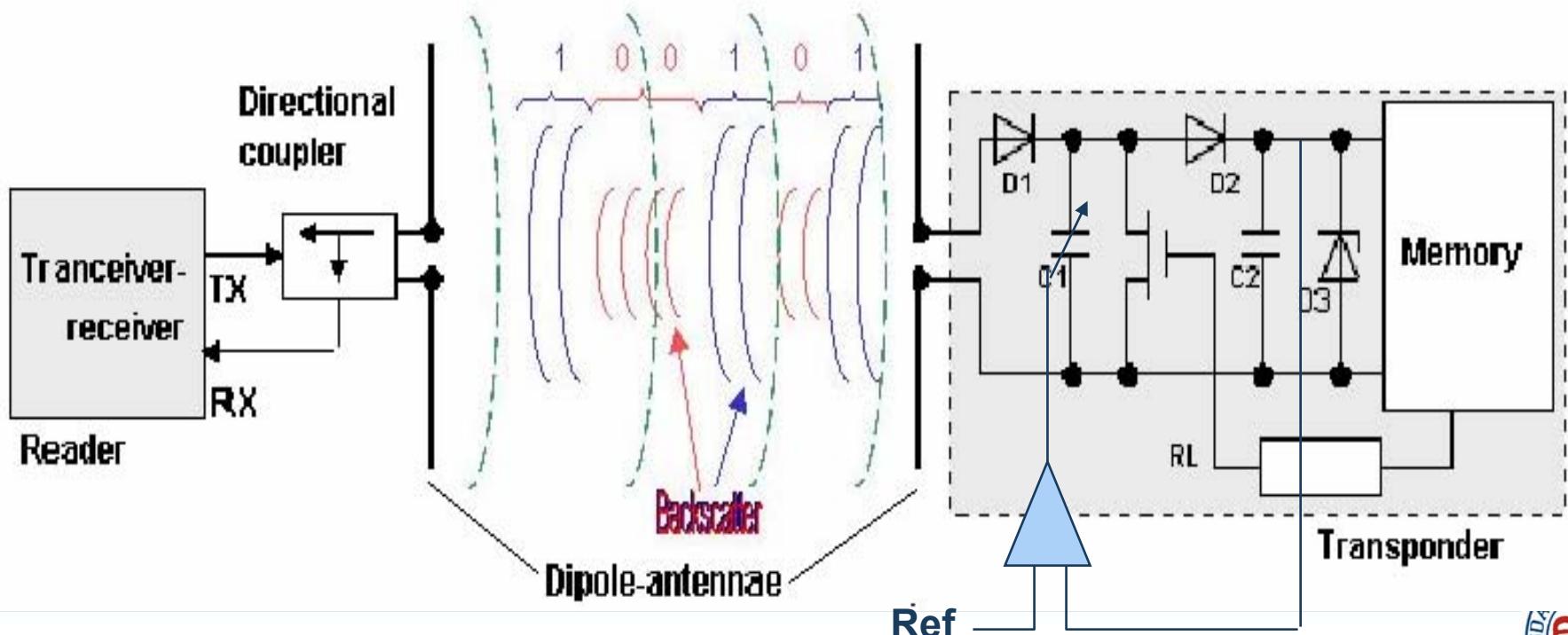
■**Frequency=1Mhz**

■**VDD=1V**

■**Power=10nA**

4 orders of magnitude

- **Dynamic antenna matching circuits**
  - Improve the mask effect of closer tags
  - Protect tags from being burned
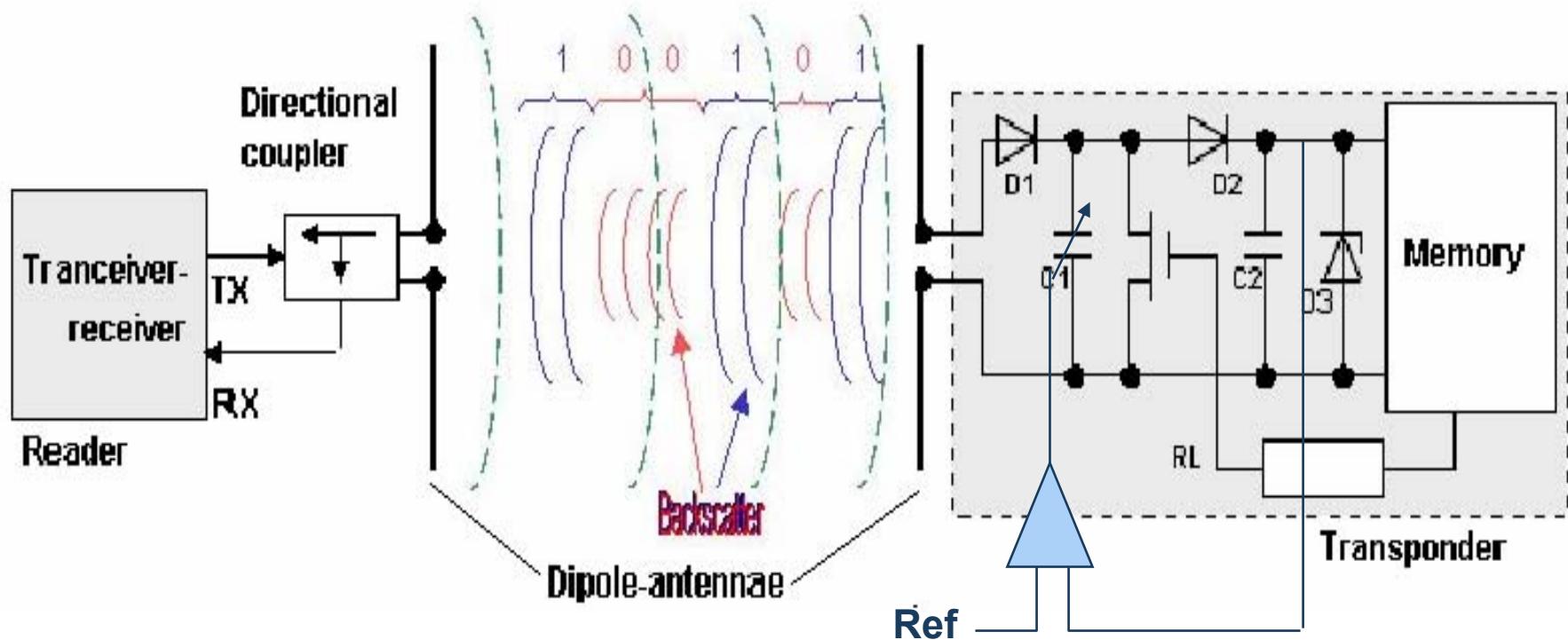
- **Adaptive tuning circuits**
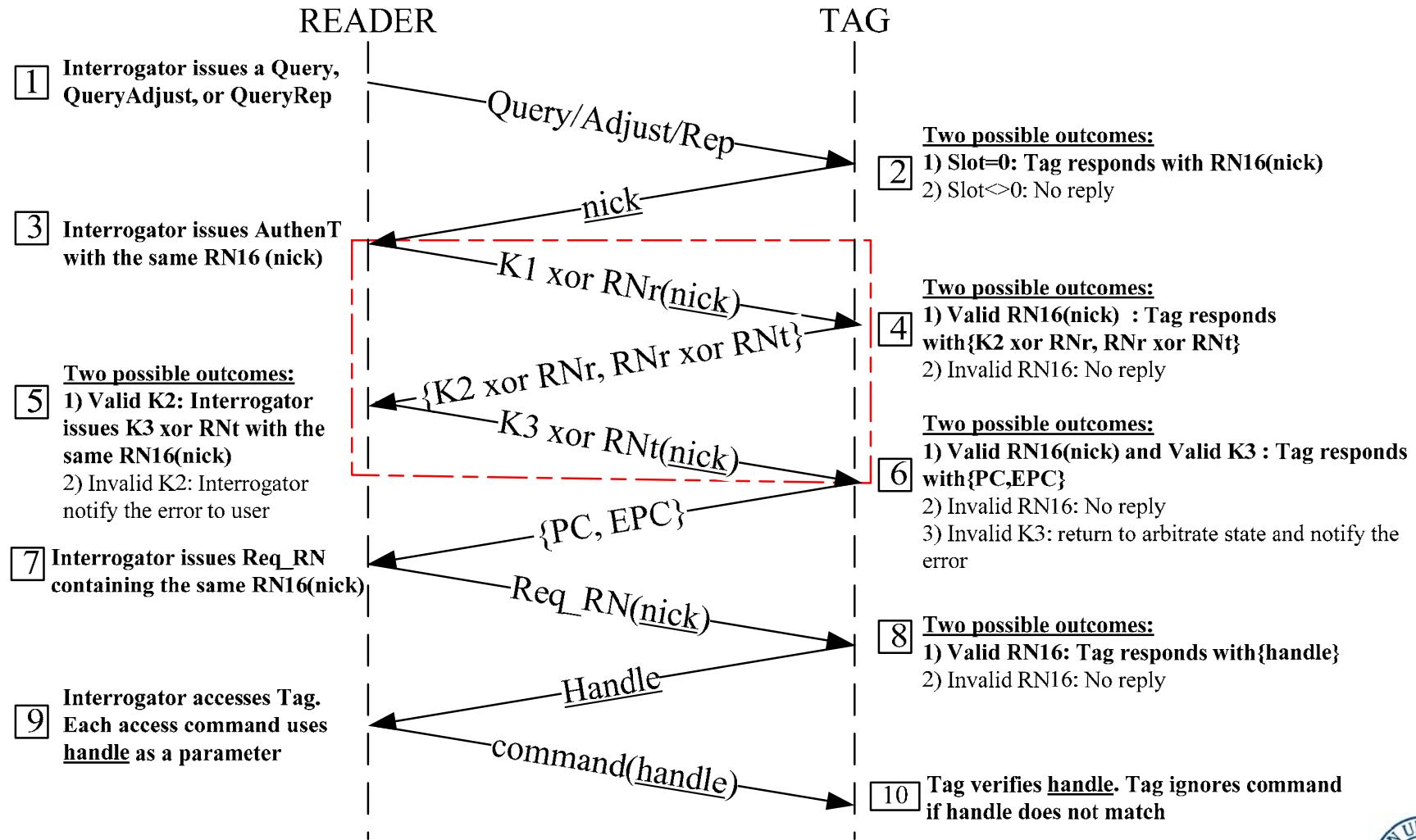
# Security and Authentication

- **Two way authentication**
- **Encrypted communication between tags and readers**
- **Light crypto engine**
  - Low cost
  - Low power
  - Adequate security between tags and readers
- **Shared random number generator (share with anti-collision)**

Authentication Flow Based on C1G2

READER   **TAG**

1. Interrogator issues a Query, QueryAdjust, or QueryRep

Query/Adjust/Rep

2. Two possible outcomes:
   1) Slot=0: Tag responds with RN16(nick)
   2) Slot<>0: No reply

nick

3. Interrogator issues AuthenT with the same RN16 (nick)

K1 xor RNr(nick)

4. Two possible outcomes:
   1) Valid RN16(nick) : Tag responds with{K2 xor RNr, RNr xor RNt}
   2) Invalid RN16: No reply

{K2 xor RNr, RNr xor RNt}

5. Two possible outcomes:
   1) Valid K2: Interrogator issues K3 xor RNt with the same RN16(nick)
   2) Invalid K2: Interrogator notify the error to user

K3 xor RNt(nick)

6. Two possible outcomes:
   1) Valid RN16(nick) and Valid K3 : Tag responds with{PC,EPC}
   2) Invalid RN16: No reply
   3) Invalid K3: return to arbitrate state and notify the error

{PC, EPC}

7. Interrogator issues Req_RN containing the same RN16(nick)

Req_RN(nick)

8. Two possible outcomes:
   1) Valid RN16: Tag responds with{handle}
   2) Invalid RN16: No reply

Handle

9. Interrogator accesses Tag. Each access command uses <u>handle</u> as a parameter

command(handle)

10. Tag verifies <u>handle</u>. Tag ignores command if handle does not match

AUTO-ID LABS

http://www.autoidcenter.cn