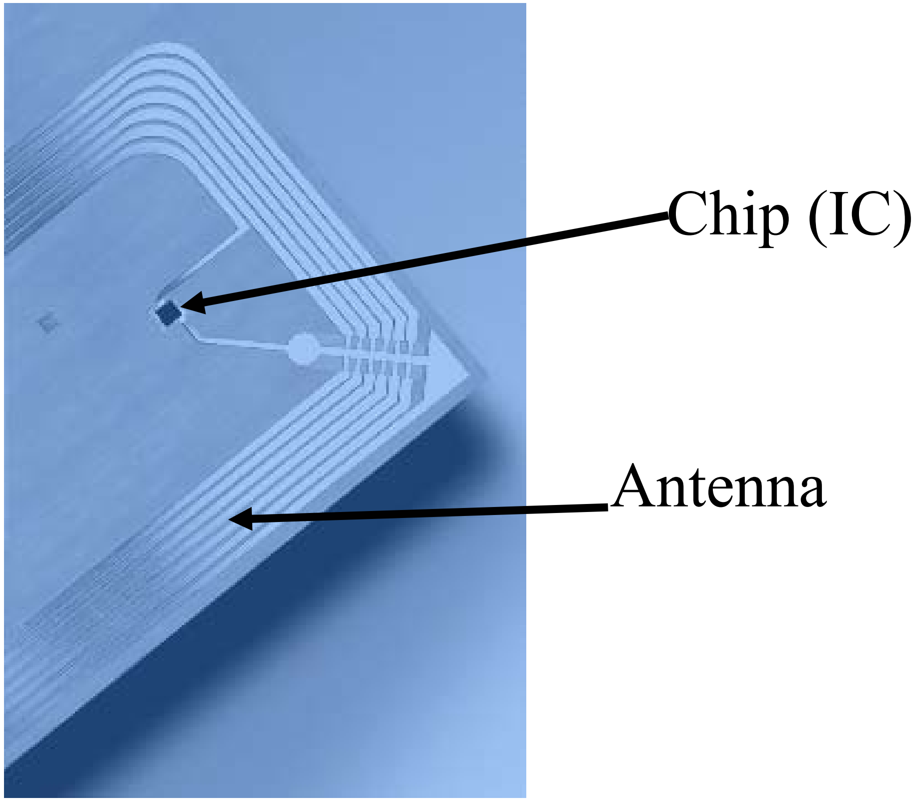
# Squealing Euros:
## Privacy Protection in RFID-Enabled Banknotes

Ari Juels
RSA Laboratories

Ravikanth Pappu
Thing Magic LLC

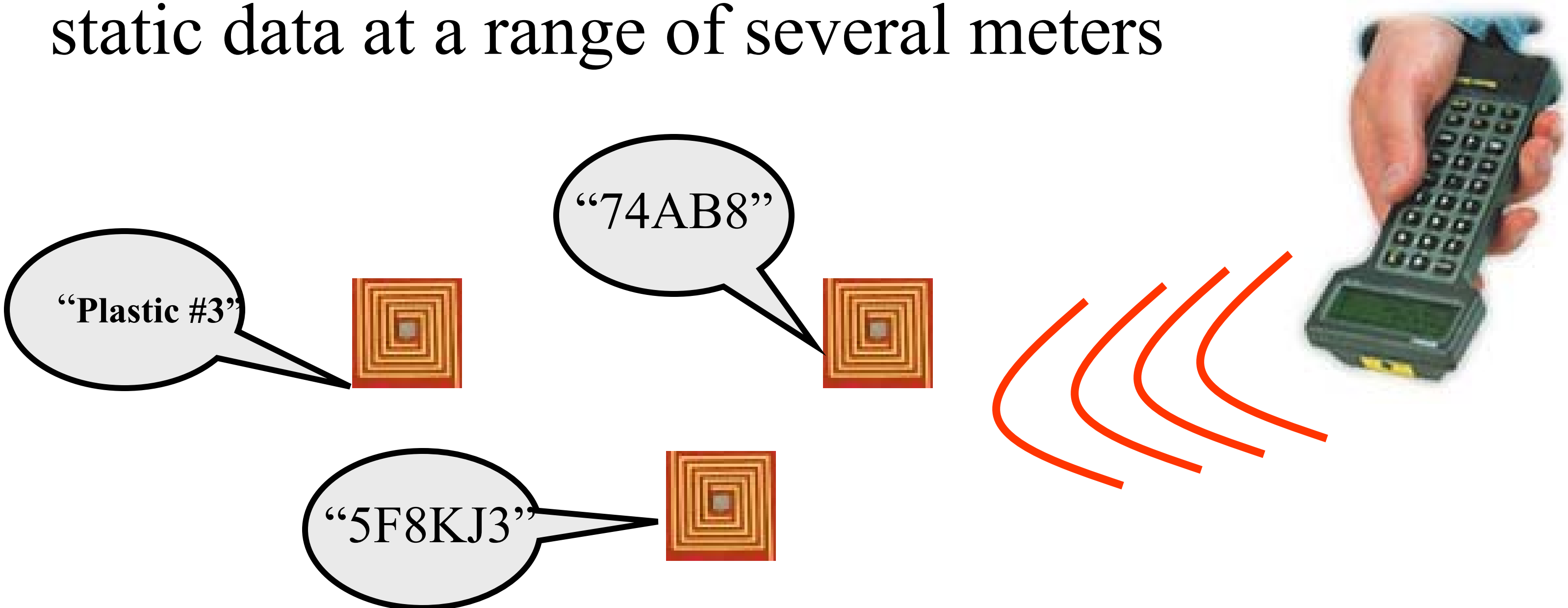
# What is a **R**adio-**F**requency **Id**entification (RFID) tag?

- In terms of appearance…



# What is an RFID tag?

- You probably own a few RFID tags…
  - Contactless physical-access cards
  - Automated toll payment
  - Inventory tags
- An RFID tag simply calls out its (unique) name or static data at a range of several meters



# There is an impending explosion in RFID-tag use

- Gillette has just ordered 500,000,000 RFID tags
  - Roughly two for every inhabitant of U.S.
  - “Smart shelf” application
- Auto-ID Center at MIT
  - Walmart, Gillette, etc.
  - RFID tags as next-generation barcodes
    - 2005: $0.05 per tag
    - 2008: $0.01 per tag

# Euro banknotes

- European Central Bank plans to implant RFID tags in banknotes by 2005

- Uses:
  - Anti-counterfeiting
  - Tracking of illicit monetary flows

# Other possible uses

- More efficient mugging

“Just in case you want to know, she’s carrying 550 Euro…”

- Fairly easy tracking of people and transactions by *anyone!*
    - Law-enforcement snooping capabilities made freely available

# The two messages of this talk

1. **Deployed naïvely, embedding of RFID tags in Euro notes presents a serious danger to privacy**

2. **The danger need not be quite so severe: There are reasonably practical ways to protect privacy.**

# The capabilities of RFID tags

- Little memory
  - Static 64-bit identifier in current ultra-cheap generation (five cents / unit)
  - Hundreds of bits soon
- Little computational power
  - A few thousand gates
  - *No* cryptographic functions available
  - Static keys for read/write permission

# What is meant by “naïve”?

- No technical details released by ECB – thus “security through obscurity”
  - Yet reverse-engineering a cheap RFID tag unlikely to be hard…
- Simple static identifiers are the most naïve
- How about encrypting ID?
  - Creates new static identifier, i.e., “meta-ID”
- How about a law-enforcement access key?
  - Tag-specific keys require initial release of identity
  - Universal keys subject to interception / reverse-engineering

# Protecting privacy in RFID tags

- To thwart tracking, appearance of ID should *change*
- No crypto on RFID tag
  - (With public-key crypto, good approaches possible)
- **First key idea:** Periodically re-encrypt ID in *external* computing agent

# El Gamal cryptosystem

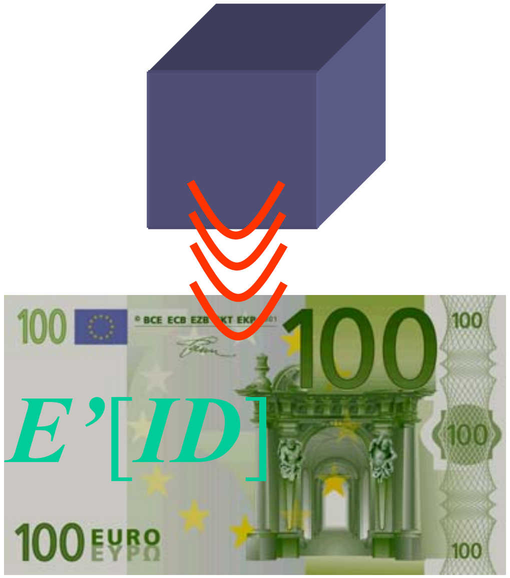
- Work in group $\boldsymbol{G}$ of order $\boldsymbol{q}$
  - For semantic security, Decision Diffie-Hellman hard
  - Published generator $\boldsymbol{g}$
- Key generation:
  - Private key is $\boldsymbol{x} \in_{\mathrm{U}} \boldsymbol{Z_q}$
  - Public key is $\boldsymbol{y} = \boldsymbol{g^x}$
- To encrypt message $\boldsymbol{m} \in \boldsymbol{G}$:
  - Select encryption factor $\boldsymbol{r} \in_{\mathrm{U}} \boldsymbol{Z_q}$
  - Ciphertext is $\boldsymbol{C} = (\boldsymbol{my^r}, \boldsymbol{g^r}) = (\boldsymbol{a},\boldsymbol{b})$
  - Plaintext computable as $\boldsymbol{m} = (\boldsymbol{a} / \boldsymbol{b^x})$
- **We write $\boldsymbol{C} = \mathbf{E}_{\boldsymbol{y}}[\boldsymbol{m},\boldsymbol{r}]$**

# First key idea:
# Periodic re-encryption

- We encrypt banknote serial numbers (IDs) using El Gamal
  - Public key $\boldsymbol{y}$ is published law-enforcement key
  - Authorities can decrypt any ID using $\boldsymbol{x}$
- Thus, banknote with serial number $\boldsymbol{ID}$ carries ciphertext $\boldsymbol{C} = \mathbf{E}_{\boldsymbol{y}}[\boldsymbol{ID},\boldsymbol{r}]$

# First key idea:
# Periodic re-encryption

- El Gamal has a special feature:
  It is possible to *blind* or *re-encrypt* a ciphertext without knowledge of plaintext or private key
  - $C' = \mathbf{E}_y[m,s]$



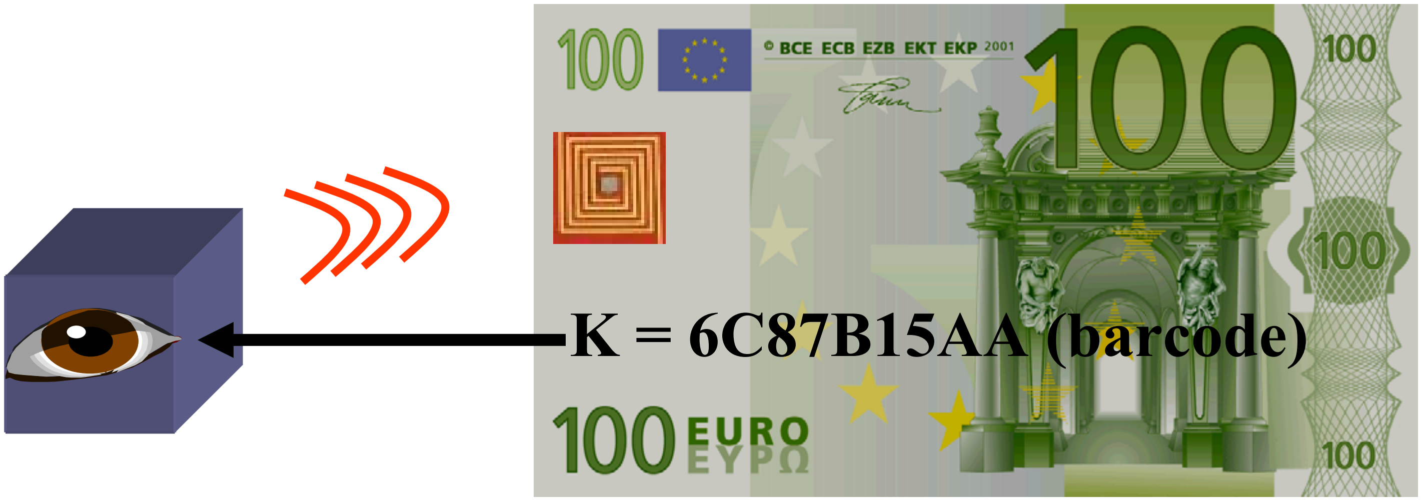
*E'*[*ID*]

# First key idea:
# Periodic re-encryption

- Presents an integrity problem: Rogue agents
  - Access to banknotes must be controlled

E[“ha ha!”]
100
BCE ECB EZB EKT EKP 2001
100 EURO ΕΥΡΩ

# Second key idea:
# Restrict access via optical channel



K = 6C87B15AA (barcode)

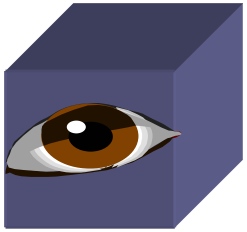
Re-encryption by optical devices in shops,
e.g., check-verification machines

# Third idea:
# Permit ciphertext-verification by agent

✓ $C = \mathrm{E}_y[ID, r]$

**Read access to *r* under key *K***

$K$ = **6C87B15AA**



# Putting it together

- Consumer carries banknote ***ID*** with ciphertext ***C*** into shop
- Shop does the following:
  - Optically reads printed key ***K***
  - Uses ***K*** to gain read access to ***r***
  - Reads ***C*** from RFID tag
  - Checks correctness of ***C*** using knowledge of ***r***
  - Re-encrypts ***ID***
  - Re-writes ***C'*** to RFID tag

# Also in the paper

- Use of digital signature scheme to mitigate risk of ***ID*** forgery
  - Special technical requirements on this scheme
- Security definitions
  - What does it mean to breach privacy in this system?
- Cost analysis
  - Bottom line: at most 780 bits of storage if we use ECC

# How well have we done?

- Privacy is clearly better than for naïve approaches
- Cloning attacks are possible
  - Equally easy against naïve systems
  - Possible countermeasure: Tie re-encryption factor cryptographically to shop identity
- Major drawback: Re-encryption perhaps not frequent enough

# Further research

- Durable and flexible foil linings for European wallets
- Other approaches…

# To Learn More

- Auto ID center at MIT
- Steve Weis – master’s thesis and papers
  - symmetric-key crypto; passive attacks
- Papers discussed here:
  - “Squealing Euro” paper
    - Google ← “Ari Juels”
  - “Blocker” paper
    - Google ← “Ron Rivest”
  - Universal re-encryption paper, pseudonym paper
    - Upon request