RFID Privacy Using User-controllable Uniqueness

Sozo INOUE, Hiroto YASUURA

System LSI Research Center,
Grad. Sch. Information Science & Electrical Engineering,
Kyushu Univ., Japan

Suppose: Ad.: Super RFID chips protect complete privacy!

.....Really?

How can we believe?

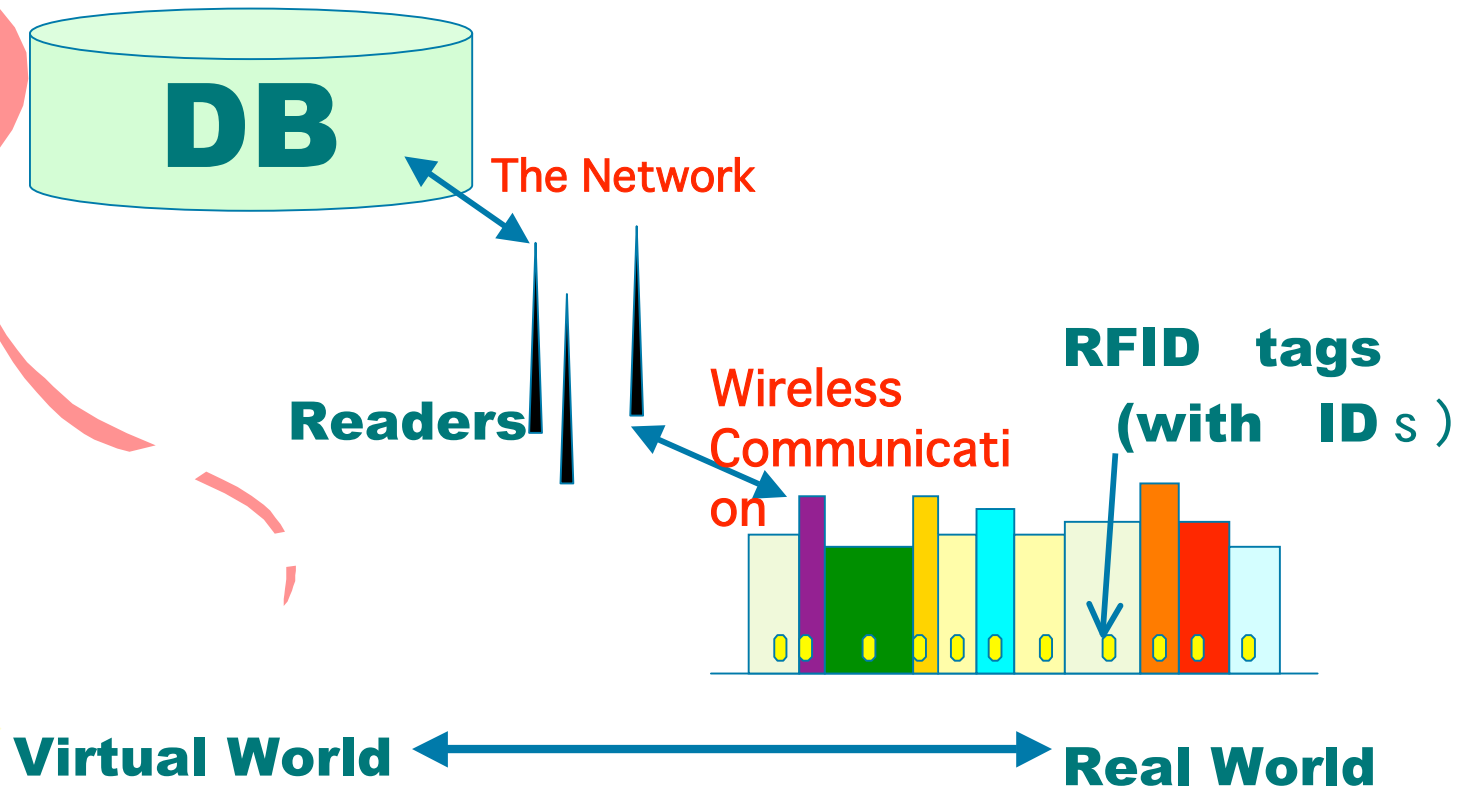
→the **Visibility** of Privacy Protection!

How? Visibility?

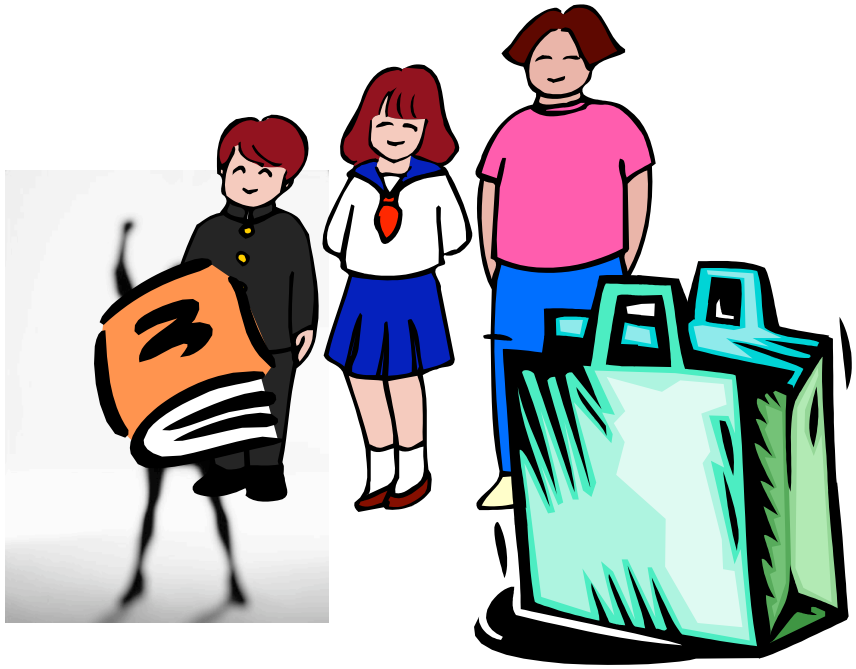
- Fully-automatic approach is not appropriate.
- How to 1:
  - Users can have something to do in a way they can trust.
- How to 2:
  - Physical “key” device to control the privacy.
    - e.g. Blocker tags

The Digitally Named World

- **Unique nouns** to any products by RFID tags: **Semiconductor technology**
- Correspondence between name (virtual) and entity (real) : **RF and Network technology**
- Automatic updates of the states, locations : **Database technology**
- **Traceable World** : Efficiency (easy retrieval) and Security (no counterfeit)



Privacy on Objects?

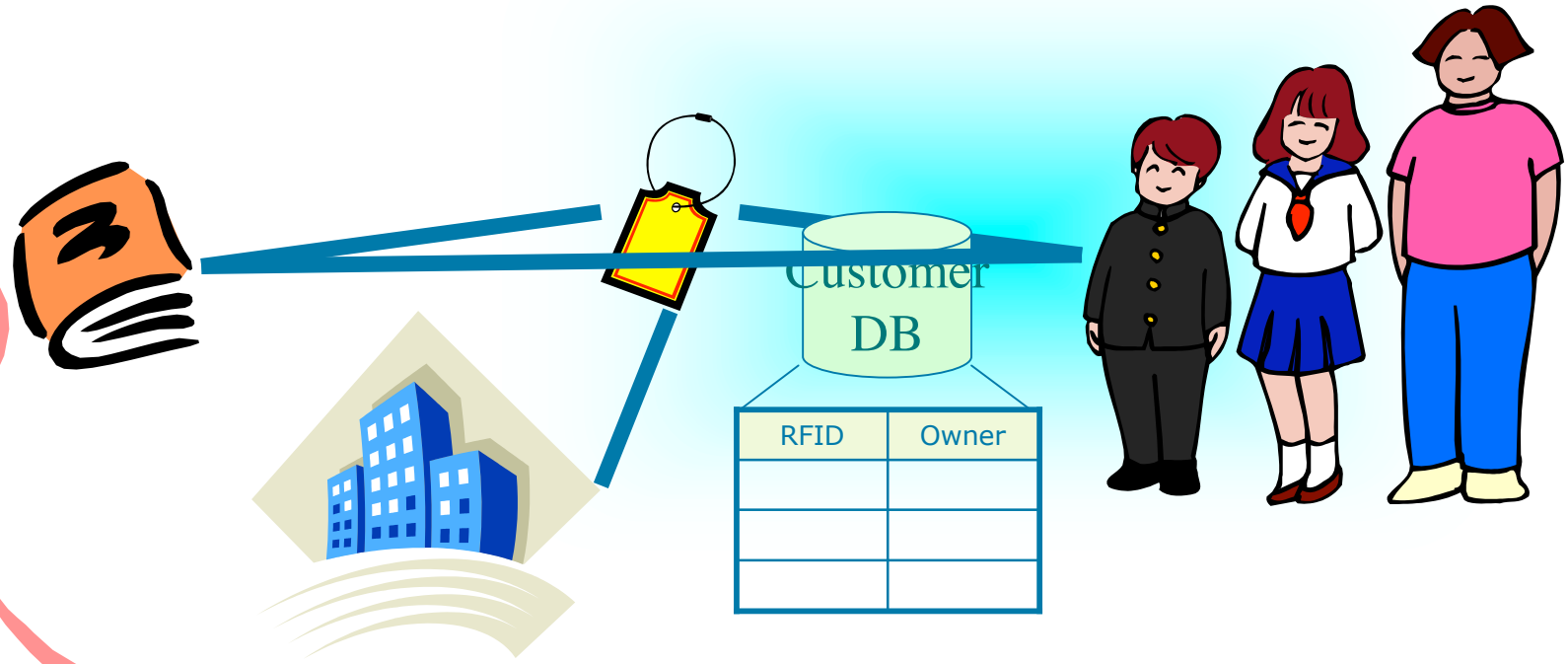


Usually, no privacy on objects themselves.

However, privacy occurs when an object and a user are **related**.

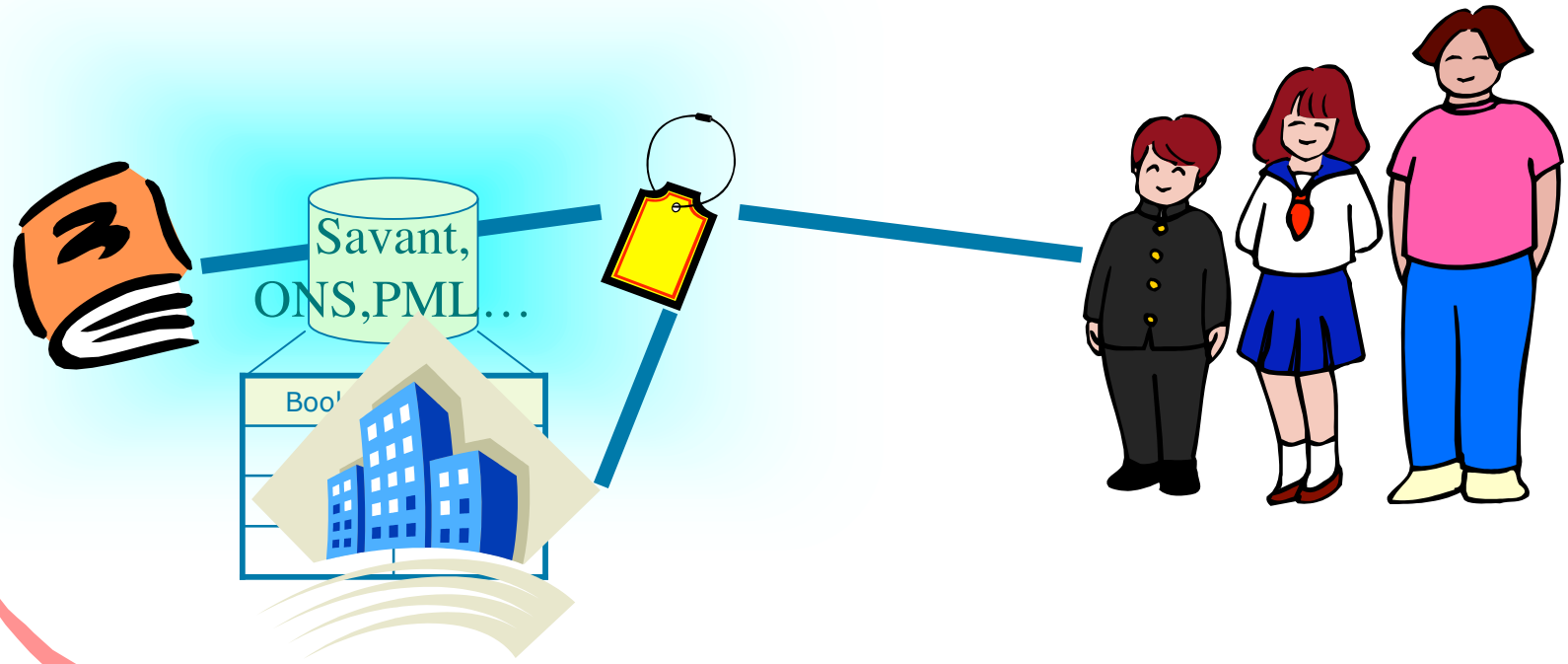
This can be occur without RFIDs.

Relationship between RFIDs & Users



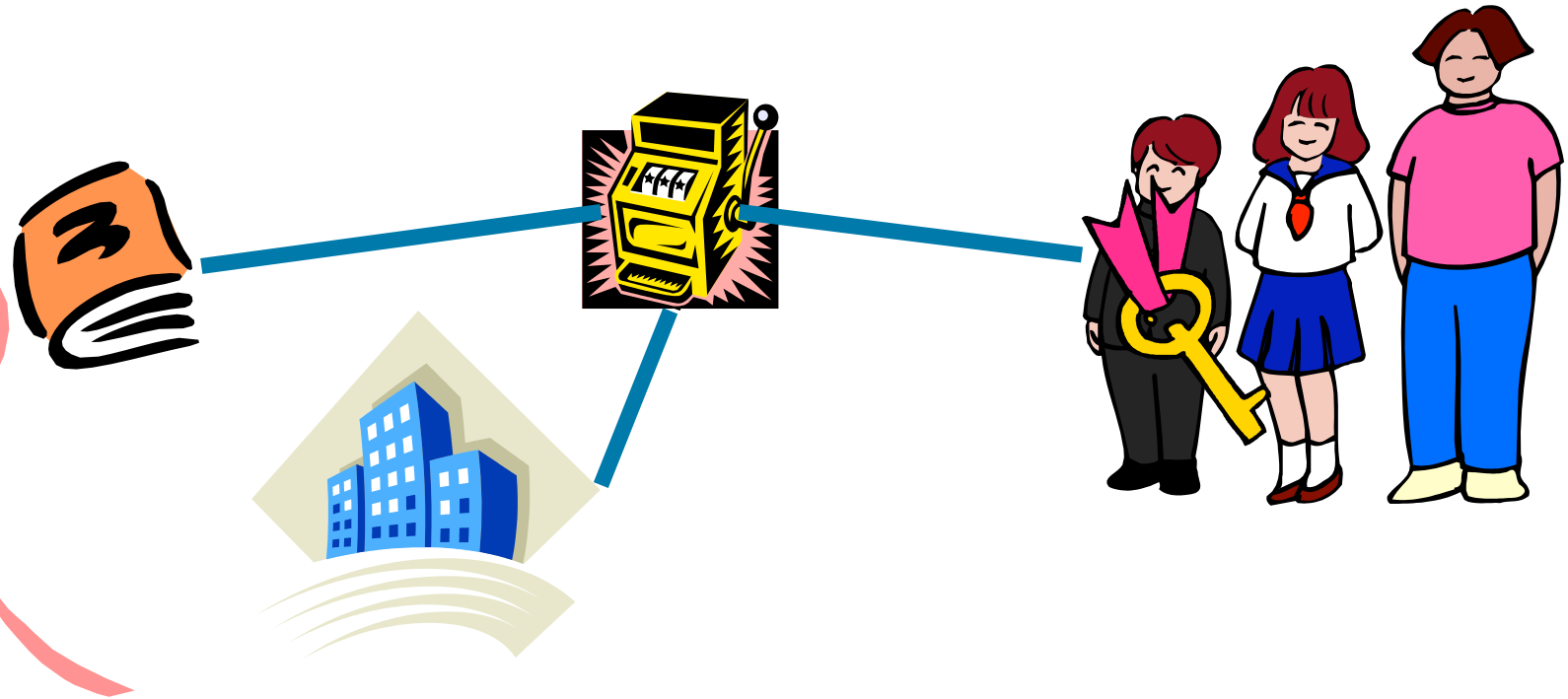
1. The **virtual world**: e.g.
   - Amazon.com relates a book ID and its consumer in the Customer database
2. The **real world**: e.g.
   - Objects located in a private room.
   - A book ID is detected by a ticket gate where the user is.

Relationship between Objects & RFIDs



1. If we have **open relationship** like EPC code, pessimistic
2. Even without the open relationship,
   Repeated reads expand the privacy of the real word. →Linkable
   - A ticket gate can know where the object was located.

Cryptography is powerful, but,…

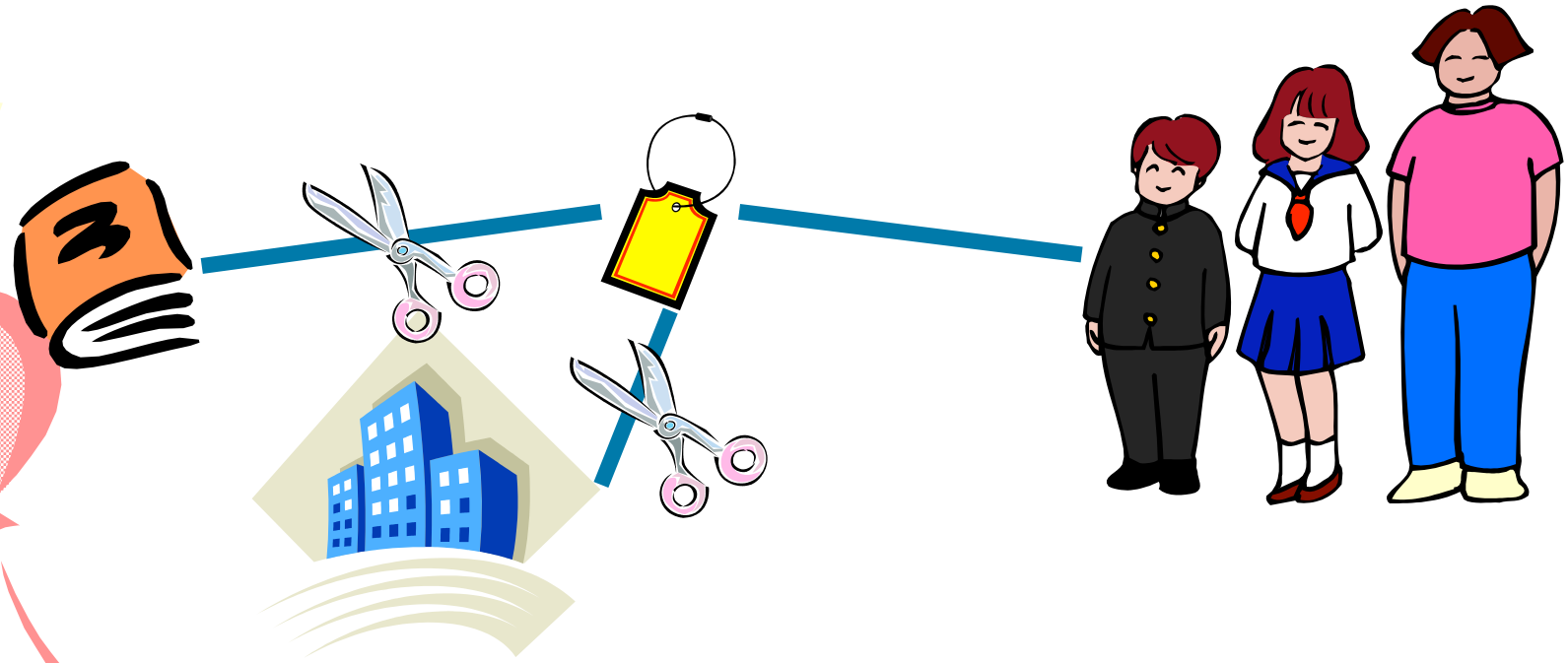


Too costly, and too automatic

Is there a solution without cryptography?

A Hint: Exam. Result (in Japan)

Lessons



Do not encrypt IDs, but,

Localize the ID: making IDs be defined by users

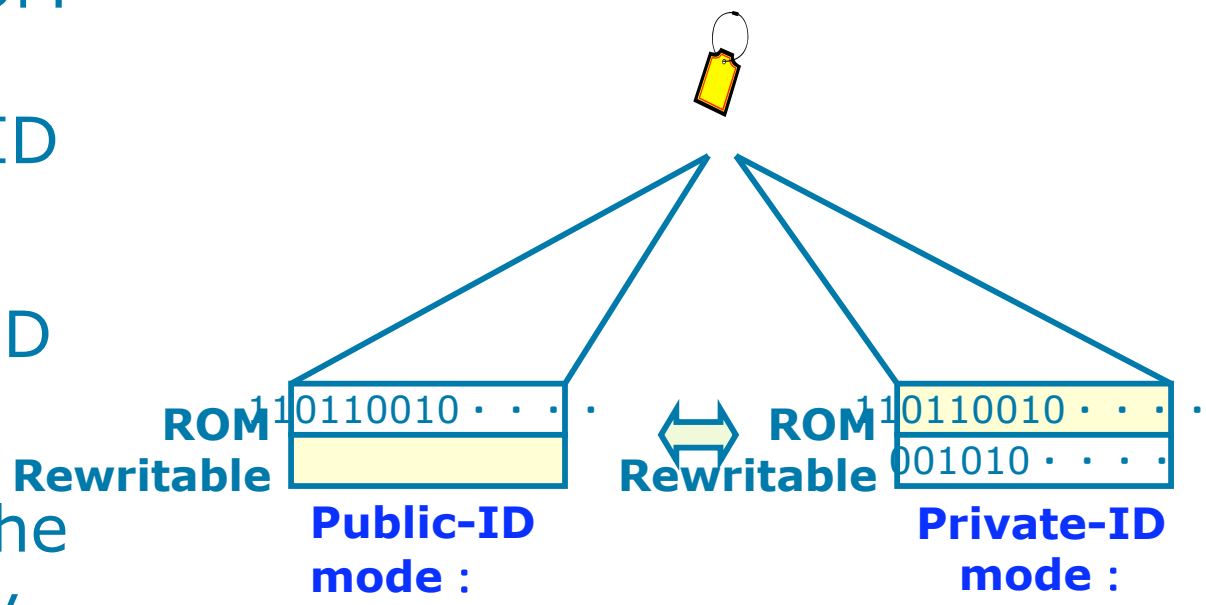
Our approach

- 1st: Localize the ID on rewritable memory
- 2nd: Localize the ID using physically separated RFID tags

1st Approach

Combination of ROM and rewritable memory on an RFID tag

- globally unique ID on the ROM
- localized ID on the rewritable memory (EEPROM, FRAM)
- Users cannot access the ROM when a private ID is set.



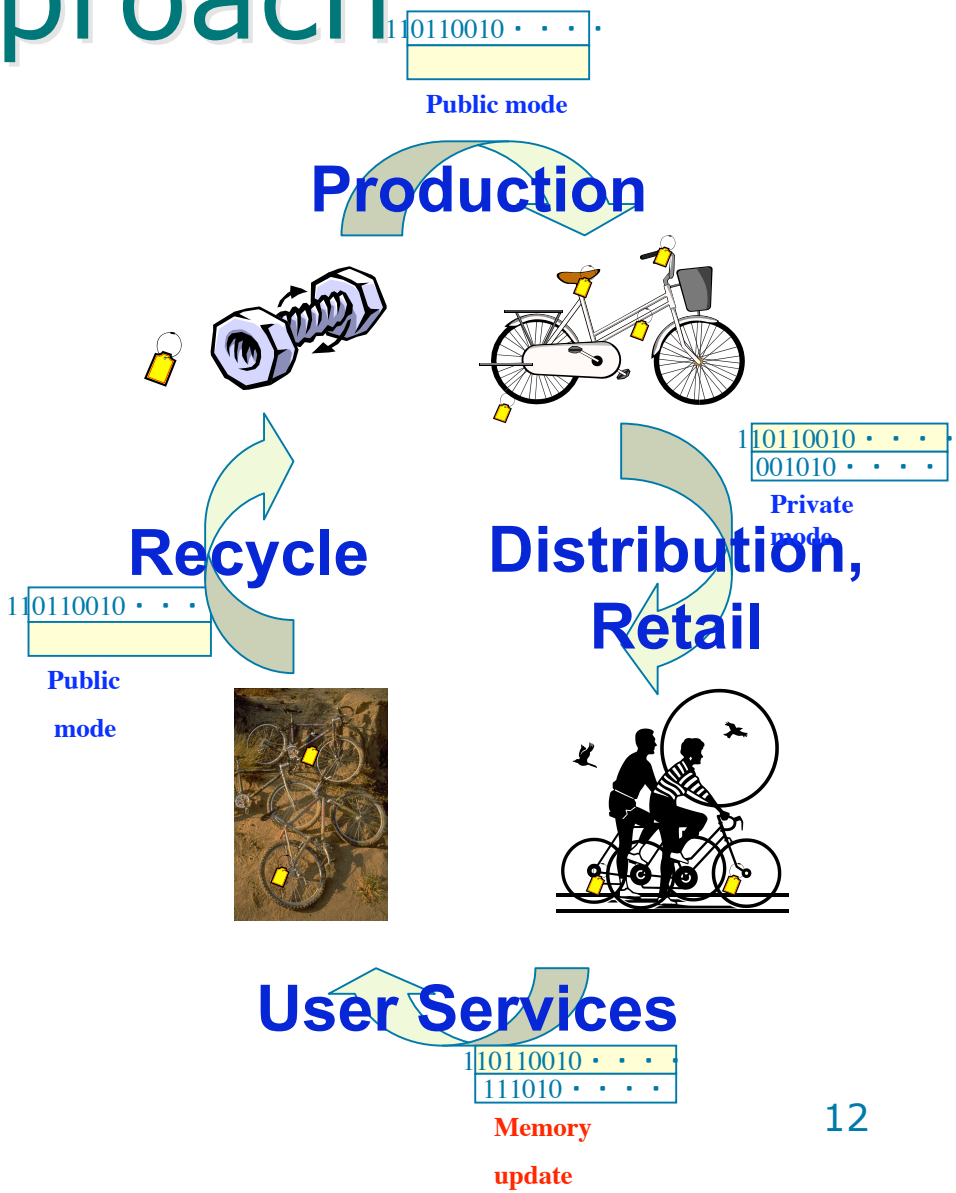
1st Approach

- Public-ID mode :
  - Any users can identify the product.
- Private-ID mode :
  - The owner **decides** the private ID value.

Only **the owner** can identify, and can relate the private ID and the public ID.

Avoids Linkability by visibly changing the private ID.

Low cost than implementing crypto.



2nd Approach

Option 1:

To a Consumer

Killed

~~101101001..~~ | ...101

011010...

User-defined Class ID

(Rewritable)

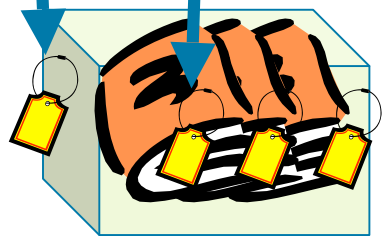
Globally Unique ID

101101001.. | ...101

Class ID

Pure ID

Option 2:



To a Consumer

...101

011010...

User-defined Class ID

(Rewritable)

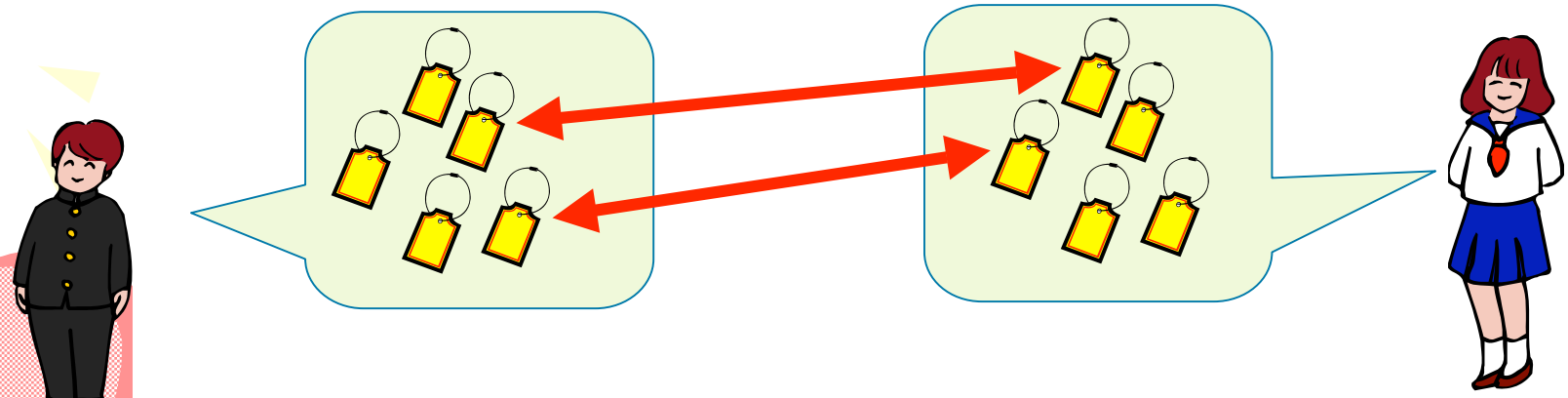
Class ID: the field related the object type.

Pure ID: the field to identify the object in the type.

2nd Approach

- The **owner can** identify,
- **Other users cannot**, from user-defined Class ID and Pure ID.
- The users **who can see the object** may identify: on-site identification
  - A repairer can know the product type (sometimes from the barcode) and identify from the Pure ID.
- Privacy is protected **by default** (without the owners' labor)
  - Object cannot be identified only by Pure ID.
- Privacy is **visible** by physically-separated RFID tags.
- **No more** special RFID tags.

IDs Conflict



Future solution:

- Location + ID= unique.
- If not (seldom, if ever), you have to check on site.
  - Distinguish by looking, and change the ID manually.

Compared to Crypto. Approach

	1st Approach	2nd Approach	Crypto. Approach
Anonymity on site	☺	☹	☺
Anonymity from remote	☺	☺	☺
Visibility of Privacy	☺	☺	☹
ID Manipulation	Secure Rewrite ☺ ☹	Secure Rewrite ☺ ☹	☺
Linkability	Secure Rewrite ☺ ☹	☹	☺
ID Conflicts	☹	☹	☺ ☹
Cost	☺	☺	☹

Concluding Summary

1. The Visibility of Privacy Protection
2. ID Localization Approach
   1. Combination of ROM and Rewritable memory
   2. Physical-ID Separation
   - Not necessarily cryptographic.
   - Visible to the owner and Low Cost.
3. Future Work:
   - System level solution for ID conflicts:
     - Technology for **Semi-AUTO-ID**:
       - e.g. Location + ID = Unique
   - 2nd approach: how to **associate** a Class RFID and a Pure RFID when there are multiple ones in a range?