Cryptographic Approach to "Privacy-Friendly" Tags

Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita

NTT Laboratories

Nippon Telegraph and Telephone Corporation

2003.11.15

RFID Privacy Workshop . MIT

Outline

1. Introduction (RFID System and RFID Privacy Problem)
2. Our Contribution
    1. Stronger security model
        Indistinguishability, forward security
    2. A new scheme providing stronger security
        low-cost and forward secure based on hash chain
3. Conclusion

RFID System

- Radio Frequency IDentification (RFID)
  - Each tag has a unique ID.
  - Anyone can read the ID through radio connection.

VERY USEFUL
FOR GOODS FLOW CONTROL

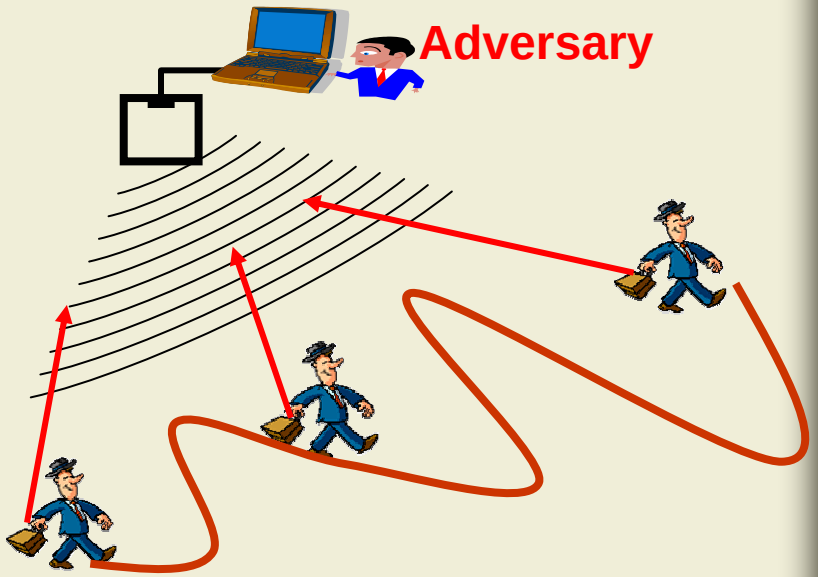
- Our Concern
  - What if the tag is linked to your identity?
  - What if someone is tracing the tag?

PRIVACY VIOLATION
(BIG BROTHER PROBLEM)

RFID Privacy Problems

- Leakage of personal belongings data
  - Leak data regarding belongings without awareness of user.

- ID tracing
  - Monitor tag owner's activity.



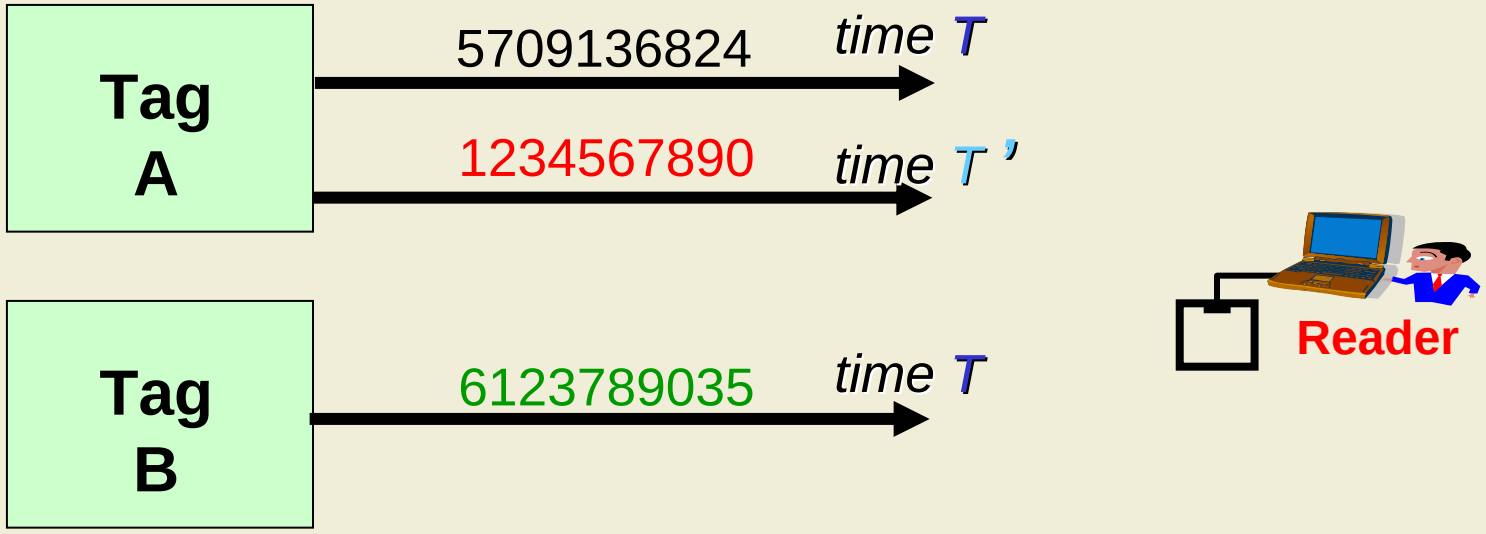
Outline

1. Introduction (RFID System and RFID Privacy Problem)
2. Our Contribution
    1. Stronger security model
        Indistinguishability, forward security
    2. A new scheme providing stronger security
        low-cost and forward secure based on hash chain
3. Conclusion

Formal Security Requirement

Indistinguishability

- The output from tag A cannot be distinguished from that from tag B.
- The ouput from tag A at time T cannot be distinguished from that of at time T'.

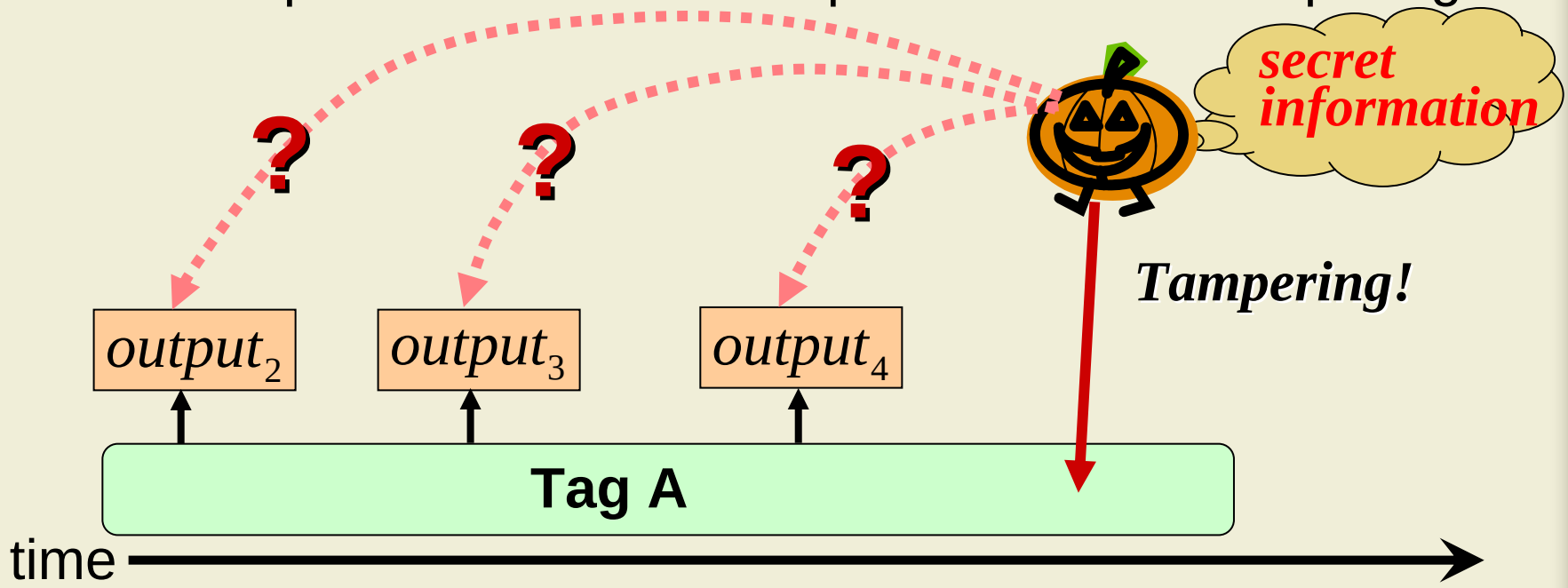


Stronger Property

Forward Security

- Once the secret in the tag is stolen, all past activities can be traced by searching past logs.

→Forward security ensures that the latest memory in the tag does not give a hint to guess past outputs. So the past activities can be protected from tampering.



Known Approaches (1/2)

- ID Encryption (against personal belongings data leakage)
  - Hide ID by encryption
    - so that only designated Reader can read it.

- Re-encryption (against ID tracing)
  - Re-encrypt the encrypted IDs to vary the ciphertext from time to time.
    - [KHKFO03] “Anonymous ID Scheme”
    - [JP03] “Re-encryption scheme”

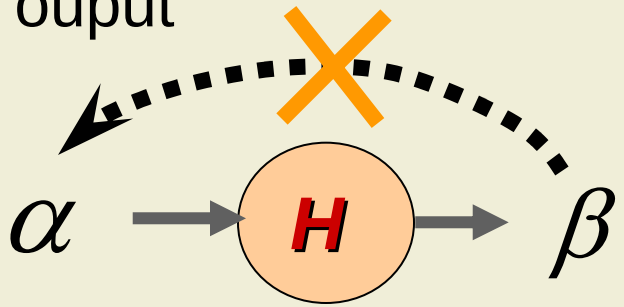
Costly encryption is done by on-line Reader.
But off-line schemes (that allow the tags to protect privacy by themselves) are more useful.

Known Approaches (2/2)

- ID Randomization approach
  - Using Hash function that is much less costly than encryption.
  - Allows tag to protect ID without any help of Reader.
  - [WSRE03] using Randomized Hashing
    - Simple
    - No forward security
  - [This work] using Randomized Hash Chain
    - Simple
    - Forward secure!

Hash Functions

- Functionality
  - One-way (Preimage-free): hard to guess the input from the ouput



- Existing Schemes
  - SHA-1, MD5, ...
- Hardware Implementation
  - 12KGates for SHA-1 while 165KGates for Elliptic Curve Enciphering
  - Security module should be < 2.5KGates to get a tag < 5 cents.
  - Currently, it is hard to meet with 2.5KG boundary but hash functions are much more promising than public-key encryption.

Known Approaches (2/2)

- ID Randomization approach
  - Using Hash function that is much less costly than encryption.
  - Allows tag to protect ID without any help of Reader.
  - [WSRE03] using Randomized Hashing
    - Simple
    - No forward security
  - [This work] using Randomized Hash Chain
    - Simple
    - Forward secure!

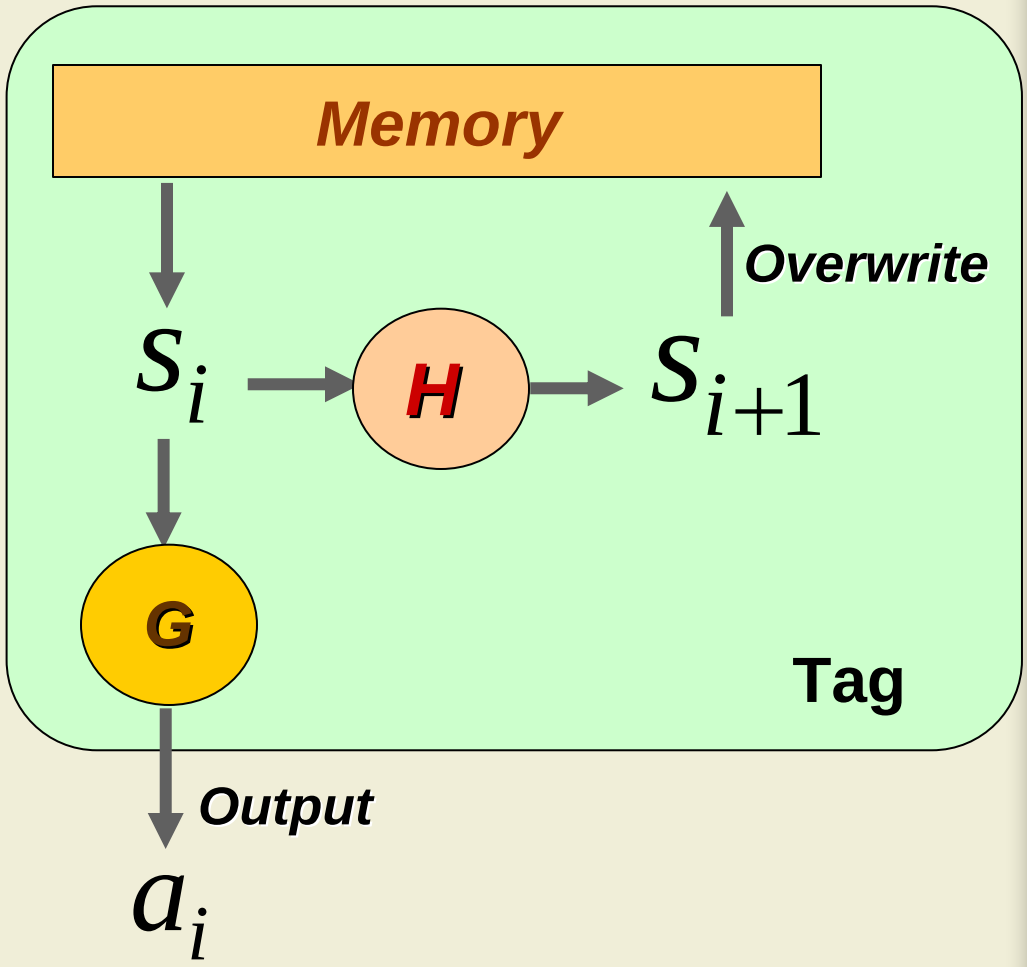
Outline

1. Introduction (RFID System and RFID Privacy Problem)
2. Our Contribution
    1. Stronger security model
        Indistinguishability, forward security
    2. A new scheme providing stronger security
        low-cost and forward secure based on hash chain
3. Conclusion

Proposed Scheme – Tag Operation

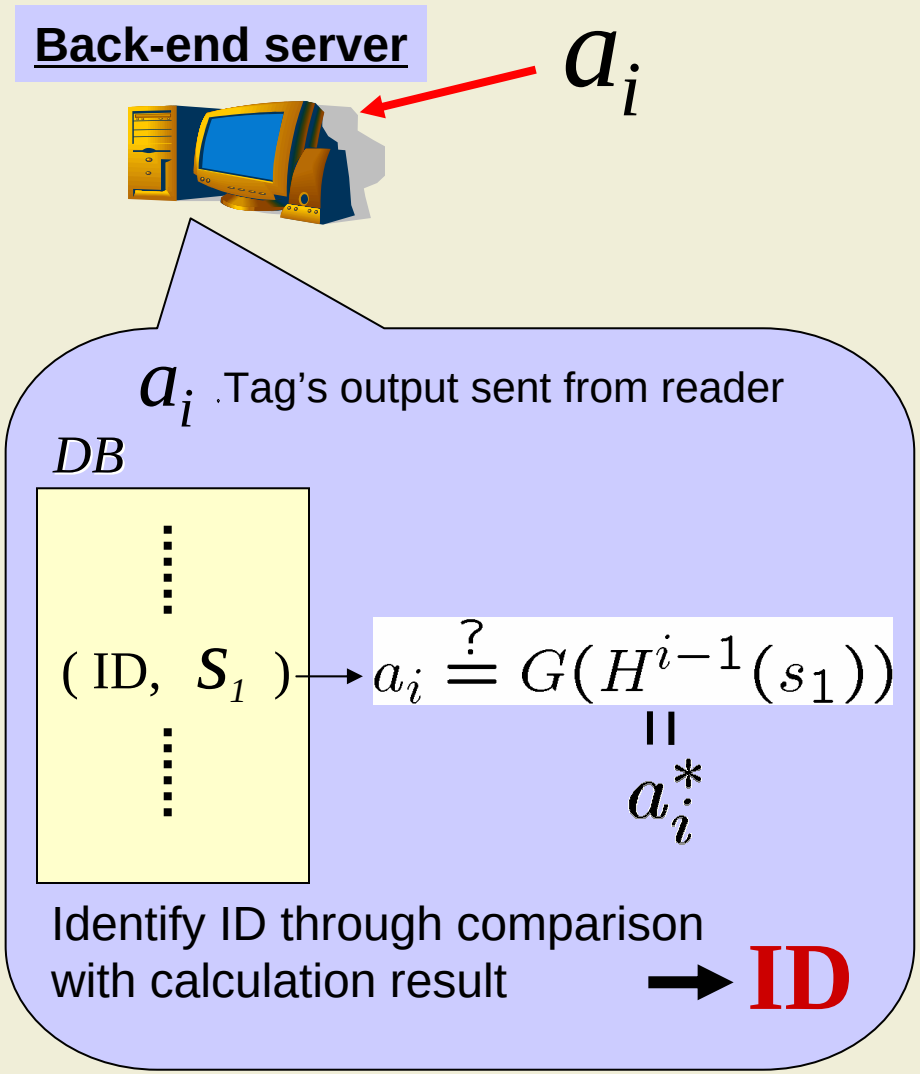
Tag

1. Receives a request from reader.
2. Calculates a_i by applying hash function G to s_i .
3. Calculates s_{i+1} by applying hash function H to s_i , and overwrite in memory



H, **G** } *One-way hash functions with different output distributions*

Proposed Scheme - Back-end Server Operation



Back-end server

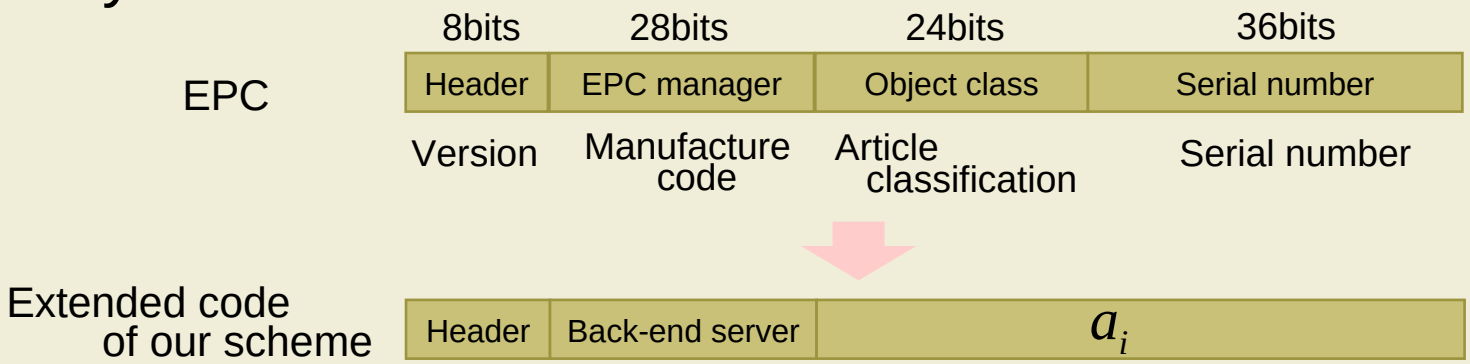
1. Receives a_i from reader.
2. For all ID,
   - $s_i = H^{i-1}(s_1)$.
   - $a_i^* = H(s_i)$.
   - $a_i \stackrel{?}{=} a_i^*$.
3. If the equation holds, identifies ID from database.

Implementation Issues

- Saving server's computation
  - Cash latest value s_i to reduce calculation cost, back-end server reduces calculation cost.
  - Apply efficient computing method for hash chain [Coppersmith and Jakobsson02][Sella03].
  - Our scheme allows parallel computation on the server-side.
- RFID lifetime
  - Using FRAM (100 million times) instead of simple memory, for example EPROM and RAM(hundred thousand times).

Application to Auto-ID System

- Layout



- Operation
  1. Reader sends an extended-EPC to the ONS server.
  2. ONS server resolves address of back-end server and responds to reader.
  3. Reader sends extended-EPC to back-end server.
  4. Back-end server resolves extended-EPC to original-EPC and returns it to reader.
  5. Next, the basic protocol in our scheme is performed.

Conclusion

- Defined security requirements
  - Indistinguishability
  - Forward security
- Proposed scheme
  - Low-cost
  - Security requirements are satisfied
    - Secret information is renewed using hash chain.
    - Output of tag is changed every requests and random.
- Future works
  - Reduce the computational cost of back-end server
  - Low-cost hash function