Privacy Protection for RFID with Hidden Subset Identifiers

Jacek Cichoń Marek Klonowski Mirosław Kutyłowski

Institute of Mathematics and Computer Science
Wrocław University of Technology
Poland

Pervasive 2008

Our third co-author
Mirek Kutyłowski

RFID-tags

- Simple device – piece of memory that can be remotely read
- Small size
- Batteryless
- Very low (if any) computational power

RFID-tags
Security requirements

- Tag must be easily recognized by its owner
- Untrecability – no one, except the legitimate party can trace the tag (privacy protection)
- Very simple computational operations are performed
- Security: moderate security for extremely low price

RFID-tags
Security requirements

- Tag must be easily recognized by its owner
- Untrecability – no one, except the legitimate party can trace the tag (privacy protection)
- Very simple computational operations are performed
- Security: moderate security for extremely low price

Basic idea
Our proposal

- Very low requirements - several dozens of logical gates is enough
- Very high flexibility
- Provable security in presence of reasonably limited adversary
- Scheme is generic and can be extended in many ways.

Basic idea
Answers from our tag

Answers from our tag

```
 1:   11001111010001111010
 2:   01101111011011011011
 3:   10010111100001100001
 4:   11111011100000100001
 5:   01111011101010010010
 6:   11000100000000000011
 7:   00000101101010001111
 8:   10110110111010010111
 9:   10000110110011001111
10:   00101010100111000000
```

This answers seems to be completely random. But they are not. There are hidden regularities which allows the owner to recognize particular tag !!!

Basic idea

Idea: responses seems to be completely random, but there are some dependencies know only to the owner (issuer) of the tag. We can trace the tag if and only if we know these dependencies.

Basic idea

Linear mappings

Construction of our tag

The answers are divided into two parts. The first part (independent part) is of length n. The second part (dependent part) is of length m. We have also

$$T : \{0,1\}^n \xrightarrow{linear} \{0,1\}^m ,$$

where $\{0,1\}^n$ and $\{0,1\}^m$ are treated as linear spaces over the field GF(2).

Basic idea

Generating answer

Generation of answer

1. generate a random sequence of bits $\overline{x} \in_R \{0,1\}^n$
2. send the answer

$$(x_1, \ldots, x_n, y_1, \ldots, y_m) = (\overline{x}, \mathrm{T}(\overline{x})) \in \{0,1\}^{n+m} .$$

The owner knows (n, m, T). Hence, it may check whether

$$(y_1, \ldots, y_m) = \mathrm{T}((x_1, \ldots, x_n)) .$$

Basic idea
Logical parts of our tag

Answers from our tag

	independent	dep.
1:	11001110100011	11010
2:	01101110110110	11011
3:	10010111000011	00001
4:	11110111000001	00001
5:	01111011010100	10010
6:	11000100000000	00011
7:	00000101101010	01111
8:	10110101110100	10111
9:	10000110110011	01111
10:	00101010100111	00000

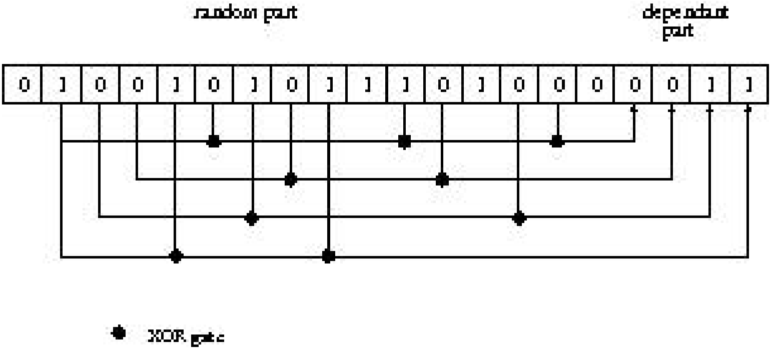
Basic idea

Production of tags

(n,m)-production schema

- flip $n \cdot m$ times a fair coin to produce a sequence $A_1, \ldots, A_m$ of random subsets of $\{1, \ldots, n\}$;
- define
$$T_i(x_1, \ldots, x_n) = \bigoplus_{j \in A_i} x_j$$
- put $\mathrm{T}(x) = (T_1(x), \ldots, T_m(x))$.

Basic idea
Example of (16,4)-tag



Basic mathematical facts
Rank of a random 01-matix

Theorem

Let $(\xi_i^j)_{i,j\in[n]}$ be a sequence of stochastically independent 0-1 *random variables such that* $\Pr[\xi_i^j = 1] = \frac{1}{2}$ *for each i and j. Let $x^{(j)} = (\xi_1^j, \ldots, \xi_n^j)$ for $j \in \{1, \ldots, n\}$. For $0 \leq k \leq n$, let $p_{n,k}$ be the probability of the event that vectors $x^{(1)}, \ldots, x^{(n-k)}$ are linearly independent over the field $\mathbb{Z}_2$. Then*

$$p_{n,k} = \prod_{a=k+1}^{n} \left(1 - \frac{1}{2^a}\right) \ .$$

Basic mathematical facts

Rank of a random 01-matrix

Corollary

Let $(\xi_i^j)_{i,j\in[n]}$ *be a sequence of stochastically independent* 0-1 *random variables such that* $\Pr[\xi_i^j = 1] = \frac{1}{2}$ *for each* i *and* j*. Let* $x^{(j)} = (\xi_1^j, \ldots, \xi_n^j)$ *for* $j \in [n]$*. For* $0 \le k \le n$*, let* $p_{n,k}$ *be the probability of the event that vectors* $x^{(1)}, \ldots, x^{(n-k)}$ *are linearly independent over the field* $\mathbb{Z}_2$*. Then*

$$1 - \frac{1}{2^k} < p_{n,k} < 1 - \frac{1}{2^{(k+1)}} \quad .$$

Basic mathematical facts
Rank of a random 01matrixx

Corollary

Let

$$A = \begin{pmatrix} \xi_{1,1} & \cdots & \xi_{1,n} \\ \cdots & \cdots & \cdots \\ \xi_{n,1} & \cdots & \xi_{n,n} \end{pmatrix}$$

be a matrix of random independent 01*-elements. Then*

$$\Pr[det(A) \neq 0] = \prod_{a=0}^{n-1} (1 - 1/2^a) \approx 0.2887 \quad .$$

Security analysis

Recognizing a single Tag

Assumptions

Assume that a reader has to check, if a tag T in its proximity is a tag T_0.

Theorem

Consider (n, m)-production schema. The tag $T \neq T_0$ can be recognized as T_0 (a false positive recognition) with probability not higher than

$$2^{-m}.$$

Security analysis

Finding a Tag in a Batch of Tags

Theorem

Assume there is a batch of L tags without TAG_0. Assume also that a tag different from TAG_0 yields an answer coherent with TAG_0 with probability q independently of all other tags. Then after t queries the system concludes (erroneously) that TAG_0 is in the batch with probability $1-(1-q^t)^L$.

In our case, using reasonable parameters, $q \approx 2^{-30}$, so

$$1-(1-q^t)^L \approx 1-\exp(-\frac{L}{2^{30\cdot t}}) \approx \frac{L}{2^{30\cdot t}} \quad .$$

Security analysis
Unlinkability model - linking game

1. L tags in the stystem
2. The adversary scans all these tags t times.
3. The challenger chooses i-th tag and presents $t+1$-thscann of i-th tag
4. The adversary wins it he can correctly point the number i

Security analysis

Unlinkability – one of results

Theorem

Consider the Linking Game with t trials for a family of L tags from (n, k)-tags. Suppose that $n \in [128, 1024]$, $t < n - 40$. Then for all $L < 2^{n-t-32}$ the probability that the ***any*** *adversary has* ***any*** *advantage (meaning that at least one tag can be excluded) is less than 2^{-30}.*

Proof of this theorem boils down to analysis of rank of $0-1$ random matrix. We showed that the new observation of the i-th tag is “coherent” with previous observations of other tags. Details in the paper.

Security analysis

Unlinkability – one of results

Theorem

Consider the Linking Game with t trials for a family of L tags from (n, k)-tags. Suppose that $n \in [128, 1024]$, $t < n - 40$. Then for all $L < 2^{n-t-32}$ the probability that the ***any*** *adversary has* ***any*** *advantage (meaning that at least one tag can be excluded) is less than 2^{-30}.*

Proof of this theorem boils down to analysis of rank of $0 - 1$ random matrix. We showed that the new observation of the i-th tag is "coherent" with previous observations of other tags.Details in the paper.

Basic scheme - recapitulation

- Scheme is scalable,
- Very high flexibility - tag can be personalized by the owner after the process of its production
- We need on average only $m \cdot n \cdot \frac{1}{2}$ XOR logical gates gates.
- Provable, very high level of security if the adversary has access to less than $n - 40$ scans (cloning, illegal tracing)

Possible improvements

- Other parameters - smaller hidden subsets without scarifying security
- Basic scheme is not immune against reply attack - it can be easily fixed
- Combining with other simple operations – difficult analysis

THANK YOU !