



M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Hidden Subsets Identifiers

Mirosław Kutylowski

Wrocław University of Technology
Institute of Mathematics and Computer Science

Dagstuhl, 18.09.2008



M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden

subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

digital authentication

- a device proves to a reader its identity by executing an interactive protocol
- proof of possessing a certain secret

limitations

- 1 communication between the reader and the device can be eavesdropped
- 2 communication volume should be low
- 3 computational power of a device severely limited



M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

electronic bar codes

- 1 the same as bar codes
- 2 but reading does not require special positioning



HB authentication protocol

Nicholas Hopper and Manuel Blum

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

learning parity with noise

a step

Public parameters: n, ε, η

Shared secret key: $\mathbf{x} \in \{0, 1\}^n$

Reader

choose $\mathbf{a} \in_R \{0, 1\}^n \xrightarrow{\mathbf{a}}$

Tag

$\nu := \begin{cases} 1 & \text{with pbb } \varepsilon \\ 0 & \text{with pbb } 1 - \varepsilon \end{cases}$

check $z \stackrel{?}{=} \mathbf{a} \cdot \mathbf{x} \xleftarrow{z}$

$z := (\mathbf{a} \cdot \mathbf{x}) \oplus \nu$



Protocol

- 1 repeat the basic step r times
- 2 count the number of successes
- 3 accept if the number of successes exceeds $r \cdot (1 - \eta)$

Number of Kbits sent during the authentication

n	$\eta = 1/20$	$\eta = 1/8$	$\eta = 1/4$
128	4	7	18
512	16	28	73



Active adversary

- use $a = (1, 0, 0, \dots, 0)$ several times for learning x_1 :
each time you get back

$$(\mathbf{a} \cdot \mathbf{x}) \oplus \nu = x_1 \oplus \nu,$$

where ν is biased towards 0.

- the same for x_2, x_3, \dots



HB+ authentication protocol

Ari Juels and Stephen Weis

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden

subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

a step

Public parameters: n, ε, η
 Secret key: $\mathbf{x}, \mathbf{y} \in \{0, 1\}^n$

Reader
 choose $\mathbf{a} \in_R \{0, 1\}^n$ $\xrightarrow{\mathbf{a}}$

$\xleftarrow{\mathbf{b}}$

$z \stackrel{?}{=} (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y})$ \xleftarrow{z}

Tag

$\mathbf{b} \in_R \{0, 1\}^n$
 $\nu := \begin{cases} 1 & \text{with pbb } \varepsilon \\ 0 & \text{with ppb } 1 - \varepsilon \end{cases}$

$z := (\mathbf{a} \cdot \mathbf{x}) \oplus (\mathbf{b} \cdot \mathbf{y}) \oplus \nu$



M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Chances for an attack

- 1 LPN is NP-hard (but it does not mean much)
- 2 attacks of superpolynomial complexity, but n cannot be big (time complexity, channel capacity)



Attack

Gołębiewski, Majcher, Zagórski, Zawada, ADHOC NOW'2008

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

scenario

- 1 collect about $2n$ transmissions
- 2 analyze

Efficiency

- 1 input size moderate
- 2 runtime asymptotically exponential, but for small n ...
- 3 the previous methods needed both exponential time and input



Attack idea

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Given

- (a_i, z_i) for $i = 1, \dots, 2n$
- where $a_i \cdot x = z_i$ holds for MOST parameters i

- 1 choose at random n pairs (a_i, z_i) that are linearly independent, say

$$A = (a_{j_1}, z_{j_1}), (a_{j_2}, z_{j_2}), \dots, (a_{j_n}, z_{j_n})$$

- 2 guess which answers are wrong assuming that their number is $\leq k$, and correct them
- 3 k might be small for practical values of n and ϵ
exploit deviations in minus concerning the expected value $n \cdot \epsilon$



Attack idea

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

- 1 choose at random n pairs (a_i, z_i) that are linearly independent, say

$$A = (a_{j_1}, z_{j_1}), (a_{j_2}, z_{j_2}), \dots, (a_{j_n}, z_{j_n})$$

- 2 guess $\leq k$ wrong answers, and correct them
- 3 **k might be small ...**
- 4 test correction: express the other a_i as a linear combination of vectors a_{j_l} :

$$a_i = \sum_{l=1}^n d_l a_{j_l}$$

and check if

$$z_i = \sum_{l=1}^n d_l z_{j_l}$$

for most cases



M. Kutyłowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden
subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Lesson learned

- error level and/or n must be large enough so that the number of correction trials becomes infeasible
- this increases the communication volume - a bad message is that for one test bit we need to transmit $2n$ bits in a 3 steps protocol!



Hidden subsets identifier

Example of (16,4)-tag

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

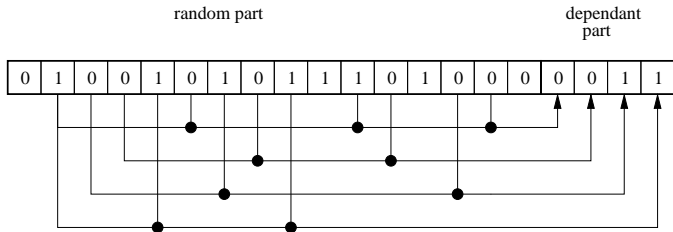
anonymity

reconstruction

attacks

Challenges

Basic design:



● XOR gate



Basic idea

Linear mappings

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

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

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

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



Basic idea

Generating answer

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Generation of answer

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

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

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

$$(y_1, \dots, y_m) = T((x_1, \dots, x_n)).$$



Basic idea

Production of tags

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

(n,m)-schema

- flip $n \cdot m$ times a fair coin to produce a sequence A_1, \dots, A_m of random subsets of $\{1, \dots, n\}$;

- define

$$T_i(x_1, \dots, x_n) = \bigoplus_{j \in A_i} x_j$$

- put $T(x) = (T_1(x), \dots, T_m(x))$.

Problem

some T_i may be linearly dependent on the other ones – dangerous waste



Redundancy

Rank of a random 01 matrix

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Lemma

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

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

Avoiding redundancies

quite probable unless the size of dependent part too big



False positives

recognizing a single tag

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Assumptions

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

Theorem

Consider (n, m) -schema. A tag $T \neq T_0$ can be recognized as T_0 (a false positive recognition) with probability

$$\leq 2^{-m}.$$

(not obvious due to dependencies between the values T_i)

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

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



Unlinkability game

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden
subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

assumptions

- 1 L tags in the system
- 2 the adversary scans all these tags t times.
- 3 the challenger chooses i -th tag and presents scan $t + 1$ of tag i ,
- 4 the adversary wins if he answers with i



Unlinkability

one of results

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden

subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

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 **an** 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 a 0 – 1 random matrix.



Basic scheme - recapitulation

M. Kutyłowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Properties

- 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 good level of security if the adversary has access to less than $n - 40$ scans



Against tag reconstruction

M. Kutyłowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Techniques

noise dependent bits of a tag are XOR-ed with a mask of random error bits,

permutation the reader and tag share and use a secret permutation σ :

- 1 the reader says j
- 2 the tag permutes its answer bits with σ^j



M. Kutyłowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Main issues

generating random bits extremely simple architecture

required,
(randomized oscillator+ shift registers +
sequential load)

challenge derive bounds on reconstruction complexity
given imperfect randomness
(you do not know what *imperfectness* mean)



Challenges

M. Kutylowski

Weak devices

HB and HB+

HB

HB+

Attacks

Hidden subsets

algorithm

redundancies

misinterpretations

anonymity

reconstruction

attacks

Challenges

Main

- co-design of algorithms, attacks and lower bounds
 - a fixed size world (n is more or less known), but still a huge space
- asymptotic results of little interest