Breaking and Fixing HB+DB

Ioana Boureanu[1] **David Gerault**[2] Pascal Lafourcade[2]
Cristina Onete [3]

[1]University of Surrey, [2]University Clermont Auvergne, [3]INSA/IRISA Rennes

Wisec'17

UNION EUROPÉENNE
Fonds Européen de Développement Régional

Introduction

The HB family of authentication protocols

- Lightweight (RFID)
- Based on the LPN problem
- HB(2001), HB$^+$(2005) $\cdots$ 20+ protocols
- Most vulnerable to active (MiM) attacks

HB+DB (Pagnin *et al*, Wisec'15)

- New approach for MiM security
- Basic idea: using distance bounding

We found attacks

- Fix: $\mathbb{BLOG}$

The $\mathrm{LPN}_{\eta,x}$ problem

LPN Problem

Given samples of the form $a, (a \bullet x) \oplus \epsilon$, recovering x is difficult

LPN Oracle

η, x

$a \xleftarrow{\$} \{0,1\}^{|x|}$

$\epsilon \leftarrow Ber_\eta$

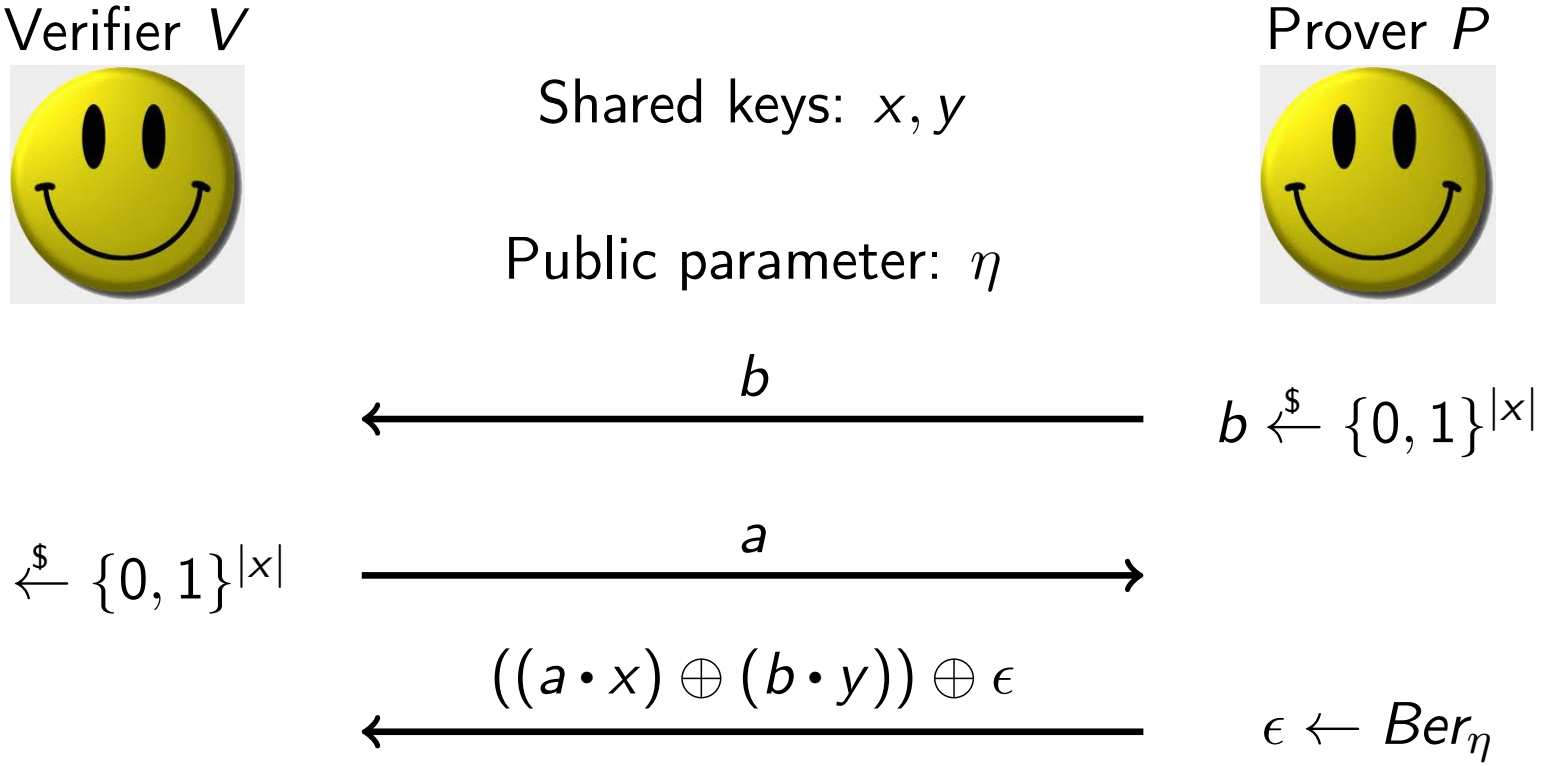
$?$ ←

→ $a, (a \bullet x) \oplus \epsilon$

Where $a \bullet x = \bigoplus_{i=1}^{|x|} a_i \cdot x_i$

Example: $01 \bullet 10 = 0 \cdot 1 \oplus 1 \cdot 0 = 0 \oplus 0 = 0$

The HB+ protocol



Repeat n times

If number of errors $\approx \eta \cdot n$, accept authentication

Security

An attacker impersonnating V has to solve $\mathrm{LPN}_{\eta,y}$ to recover y.

The HB+ protocol: MiM attack[GRS15]

Key idea

Flipping the i^{th} bit in the challenge flips the response bit iff $y_i = 1$.

The attack

Flip a_i. If the authentication fails, then $x_i = 1$, otherwise $x_i = 0$.

b

$b \xleftarrow{\$} \{0,1\}^{|x|}$

$a \xleftarrow{\$} \{0,1\}^{|x|}$ $\xrightarrow{a}$ $a' = \text{flip}_i(a)$ $\xrightarrow{a'}$

$((a' \cdot x) \oplus (b \cdot y)) \oplus \epsilon$

$\epsilon \leftarrow Ber_\eta$

Recovering y

y can be recovered in a similar way.

The HB+DB protocol

Basic Idea

Flipping bits takes time, closeby prover should respond faster.

Shared keys: x, y, z
Public parameter: η

Verifier V Prover P

$a_i \xleftarrow{\$} \{0,1\}^{|x|}$

start clock	$\xrightarrow{a_i}$	
	$\xleftarrow{((a_i \cdot x) \oplus (b_i \cdot y)) \oplus \epsilon_i$	
stop clock		

MiM detection

If a response takes too long to arrive, refuse authentication.

The HB+DB protocol

Basic Idea

Flipping bits takes time, closeby prover should respond faster.

Shared keys: x, y, z
Public parameter: η

Verifier V | Prover P

$s \xleftarrow{\$} \{0,1\}^{|x|}$

s ←

For $i \in \{1, n\}$

$a_i \xleftarrow{\$} \{0,1\}^{|x|}$

$b_i \leftarrow f_z(s, i)$

$\epsilon_i \leftarrow Ber_\eta$

start clock → a_i

stop clock ← $((a_i \cdot x) \oplus (b_i \cdot y)) \oplus \epsilon_i$

MiM detection

If a response takes too long to arrive, refuse authentication.

Why this is not sufficient

The problem

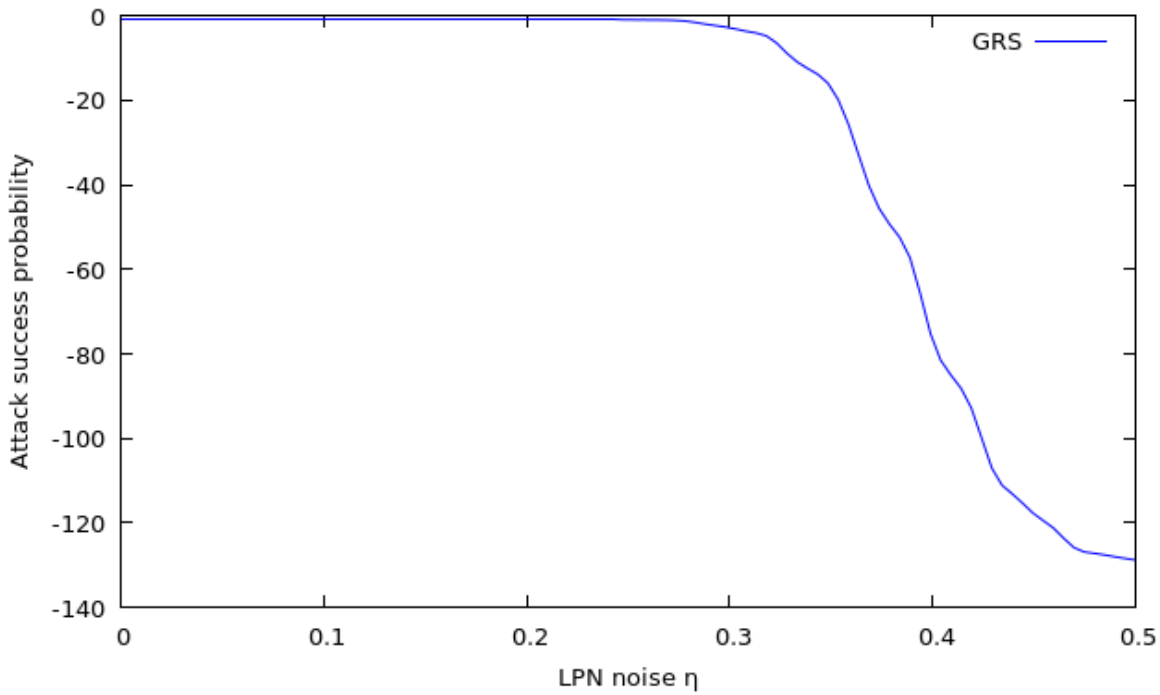
The adversary can overwrite one bit of the challenge without reading it!

The attack becomes slightly different: instead of $flip_i$, $write_i(1)$.

Limits of this attack

Intuition

If the challenge was 0, then it is flipped.



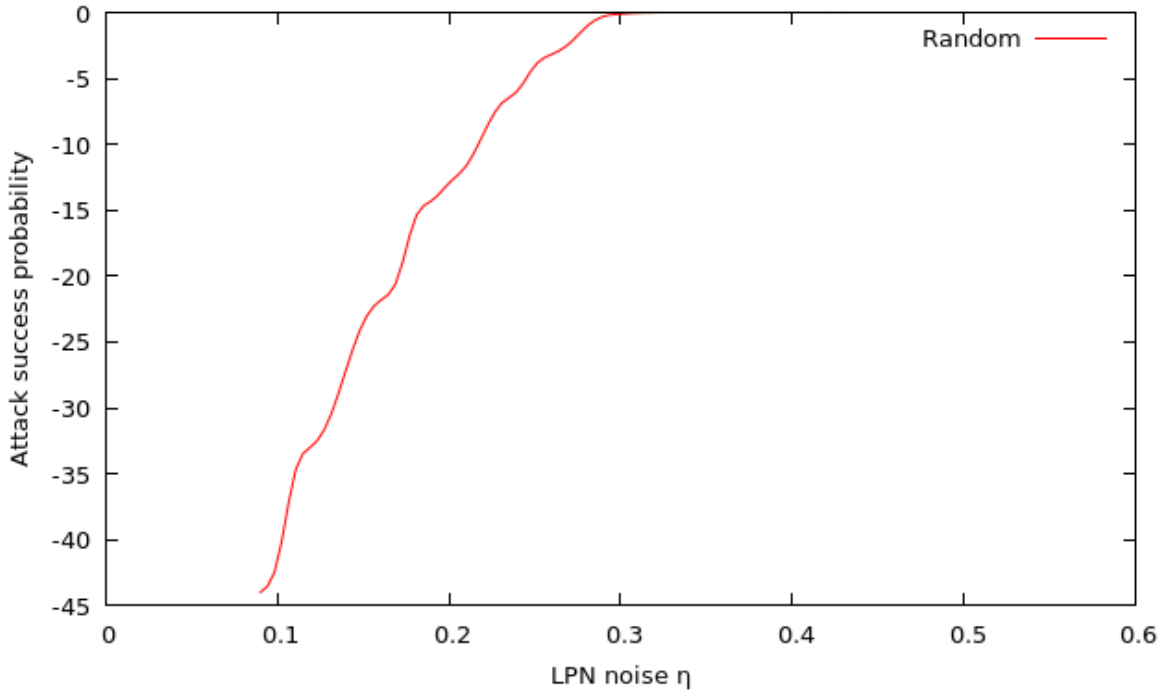
Behaviour

The success probability decreases as η increases.

Random guessing

Intuition

High $\eta \implies$ lots of errors tolerated.



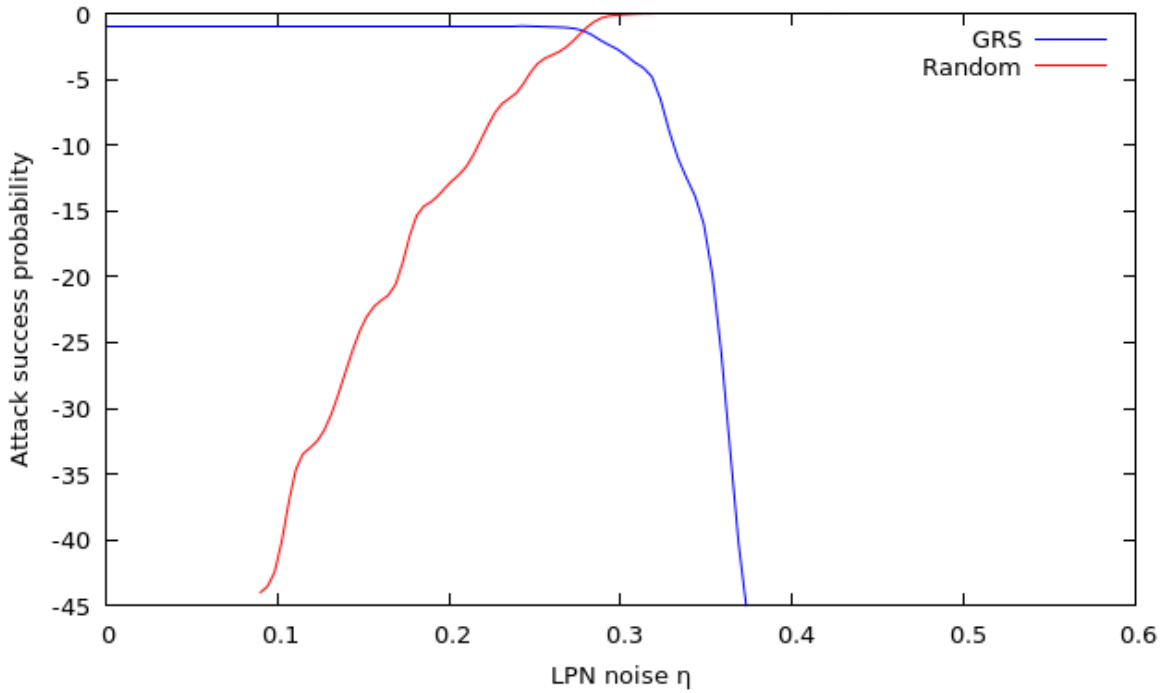
Behaviour

The higher η, the higher the probability to win by sending random responses.

Combining both attacks

Actual security

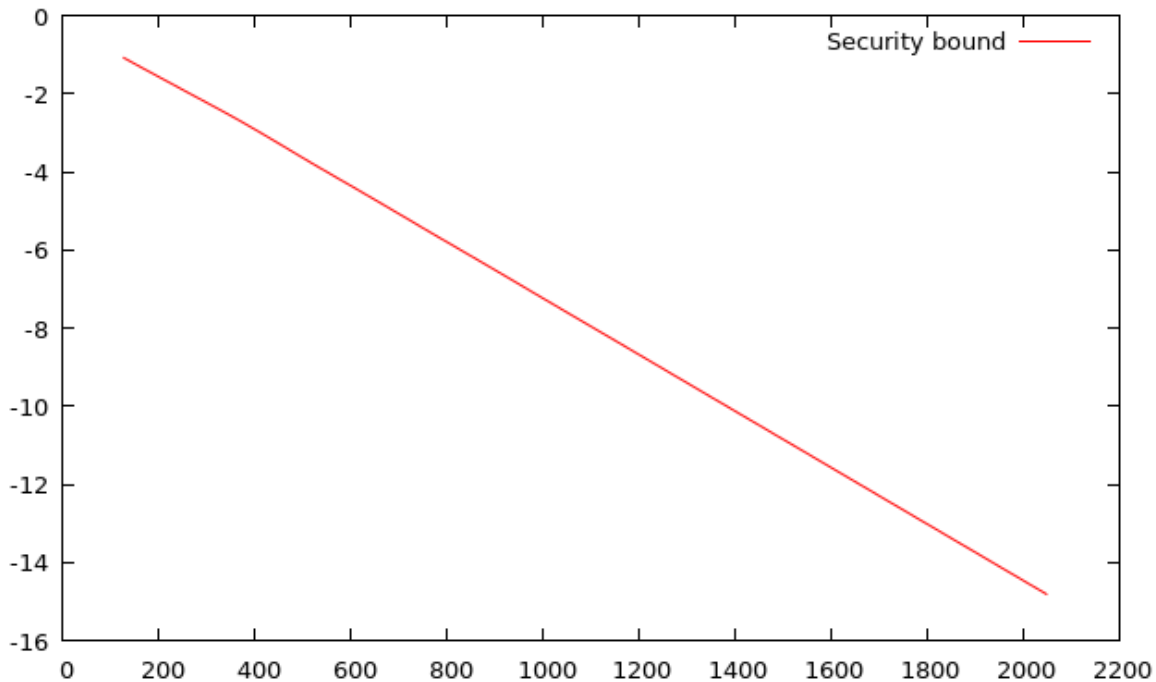
The intersection of the curves bounds the security for a given key size/n



Best achievable security level

Setting

For $|x| \in [128, 2048]$, $n = |x|$, $\min_{\eta=0}^{\frac{1}{2}}(max(p, q))$



Problems of the original protocol

- Challenge tempering
- Unnecessary LPN noise $\Longrightarrow$ High false acceptance rate
- Many PRF calls

Proposition

We propose $\mathbb{BLOG}$ to fix some these problems

BLOG

Verifier V

Shared keys: $x, \cancel{y, z}$
Public parameter: $\cancel{\eta}$

Prover P

$s \xleftarrow{\$} \{0,1\}^{|x|}$

s ←

$(xtemp||b) \leftarrow f_{\cancel{z}x}(s, \cancel{i})$

For $i \in \{1, n\}$

$a_i \xleftarrow{\$} \{0,1\}^{|x|}$

$\cancel{b_i \leftarrow f_z(s,i)}$
$\cancel{\leftarrow Ber_\eta}$

start clock a_i →

stop clock ← $a_i \bullet \cancel{x} xtemp \oplus b_i \bullet \cancel{y} \oplus \cancel{\epsilon_i}$

Properties

- Provable security against
  - Active attacks
  - Distance bounding adversaries (MF, DF, TF)
- More lightweight(ish)

Protocol	Secure	Memory	Dot products	PRF
HB+DB	No	$3 \cdot \|x\| + (n+1) \cdot \|x\| + n$	$2 \cdot n$	n
$\mathbb{BLOG}$	Yes	$\|x\| + 3 \cdot \|x\|$	n	1

Conclusion

- DB alone does not fix MiM attacks
- Designing a good LPN-based DB protocol is challenging

Thank you for your attention

Questions?

Number of errors

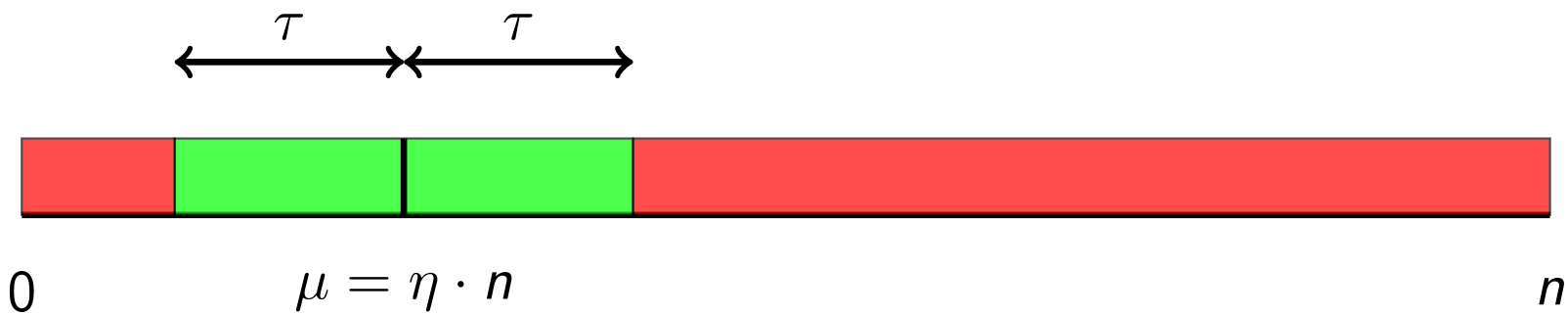
Verification

V counts the number of noisy (wrong) responses.

How many?

It should be roughly $n \cdot \mu$, but a security margin is necessary.

example: $\eta = 0.25$



Low tolerance τ leads to rejecting legitimate users, high τ increases the False Acceptance Rate.

Analysis

- $\mathcal{P}[Rand] = p =$ probability that tossing n fair coins results in $[n \cdot \mu - \tau, n \cdot \mu + \tau]$ successes.
- $\mathcal{P}[GRS] = q = (\frac{1-p}{2} + \frac{1-FRR}{2})^{|x|}$

Behaviour with $FalseRejectionRate = 0.01$

- When $\eta = 0$, $p \approx 0$ and $q \approx (\frac{1}{2} + 0.495)^{|x|} \approx 0.995^{|x|} \approx 2^{-0.007 \cdot |x|}$
- When $\eta = \frac{1}{2}, p = 1$