LPN Authentication

Krzysztof Pietrzak

IST AUSTRIA

Institute of Science and Technology

Bertinoro, Lattice Crypto and Algorithms, May 24th, 2018

https://spotniq.school/

Welcome to Spotniq

This IACR school will provide a comprehensive coverage of *proof techniques* used in symmetric cryptography. It will be targeted at Ph.D. students and post-docs who are primarily working in this area. The school will be taking place between 29 July 2018 and 2 August 2018 in Bertinoro, Italy.

Speakers

Mihir Bellare, UC San Diego
Phil Rogaway, UC Davies
John Steinberger, Tsinghua
Aishwarya Thiruvengadam, UC Santa Barbara
Krzysztof Pietrzak, IST Austria
Stefano Tessaro, UC Santa Barbara
Pooya Farshim, ENS

Efficient Authentication from Hard Learning Problems

Eike Kiltz

Krzysztof Pietrzak

David Cash

Abhishek Jain

Daniele Venturi

Eurocrypt 2011 May 16th, 2011

Outline

- The quest for lightweight authentication.
- The LPN problem.
- Authentication from LPN: HB and friends.
- The subset LPN problem.
- A new authentication protocol.
- Message authentication.

Authentication Protocols

Secret Key $\mathbf{s}$

prover $\mathcal{P}(\mathbf{s})$

verifier $\mathcal{V}(\mathbf{s})$

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$

verifier $\mathcal{V}(\mathbf{s})$

$\longrightarrow$ accept/reject

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$

verifier $\mathcal{V}(\mathbf{s})$

$\longrightarrow$ accept

Correctness : $\mathcal{V}(\mathbf{s})$ *accepts if interacting with* $\mathcal{P}(\mathbf{s})$

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$

$\longleftrightarrow$

$\rightarrow$ reject

Security : $\mathcal{V}(\mathbf{s})$ *rejects if interacting with* $\mathcal{A}$

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$

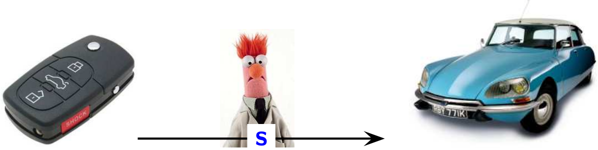
verifier $\mathcal{V}(\mathbf{s})$

$\xrightarrow{\quad \mathbf{s} \quad}$

Security : $\mathcal{V}(\mathbf{s})$ *rejects if interacting with* $\mathcal{A}$

Authentication Protocols

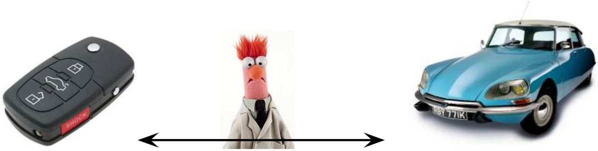
prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$



Security : $\mathcal{V}(\mathbf{s})$ *rejects if interacting with* $\mathcal{A}$

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$



Passive Security

1st phase: $\mathcal{A}$ can observe transcripts.

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\quad$ $\mathcal{A}$ $\quad$ verifier $\mathcal{V}(\mathbf{s})$



reject

Passive Security

1st phase: $\mathcal{A}$ can observe transcripts.

2nd phase: $\mathcal{V}(\mathbf{s})$ rejects if interacting with $\mathcal{A}$.

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$

Active Security

1st phase: $\mathcal{A}$ gets transcripts $+$ can interact with $\mathcal{P}(\mathbf{s})$.

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$

reject

Active Security

1st phase: $\mathcal{A}$ gets transcripts $+$ can interact with $\mathcal{P}(\mathbf{s})$.

2nd phase: $\mathcal{V}(\mathbf{s})$ rejects if interacting with $\mathcal{A}$.

Authentication Protocols

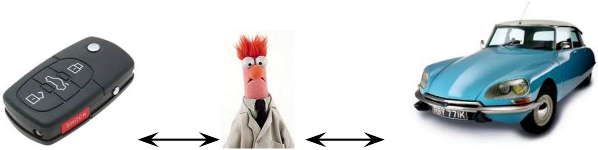
prover $\mathcal{P}(\mathbf{s})$ $\quad$ $\mathcal{A}$ $\quad$ verifier $\mathcal{V}(\mathbf{s})$

Man-In-The-Middle Security

1st phase: $\mathcal{A}$ can arbitrarily interact with $\mathcal{P}(\mathbf{s}), \mathcal{V}(\mathbf{s})$.

Authentication Protocols

prover $\mathcal{P}(\mathbf{s})$ $\mathcal{A}$ verifier $\mathcal{V}(\mathbf{s})$



Man-In-The-Middle Security

1st phase: $\mathcal{A}$ can arbitrarily interact with $\mathcal{P}(\mathbf{s}), \mathcal{V}(\mathbf{s})$.

2nd phase: $\mathcal{V}(\mathbf{s})$ rejects if interacting with $\mathcal{A}$.

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$

verifier $\mathcal{V}(\mathbf{s})$

1

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$

$\longleftarrow$ challenge $\longleftarrow$

verifier $\mathcal{V}(\mathbf{s})$

1

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$

—— $\mathrm{AES}(\mathbf{s}, \text{challenge})$ ⟶

verifier $\mathcal{V}(\mathbf{s})$

1

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$ verifier $\mathcal{V}(\mathbf{s})$

$\longrightarrow$ AES($\mathbf{s}$, challenge) $\longrightarrow$

What if block ciphers are not an option?

1

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$ — verifier $\mathcal{V}(\mathbf{s})$

$\longrightarrow$ AES($\mathbf{s}$, challenge) $\longrightarrow$

What if block ciphers are not an option?

1

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$ verifier $\mathcal{V}(\mathbf{s})$

- RFID[1] tags: 1k-10k gates, 200-2k for security.
- AES $\geq$ 5k gates.

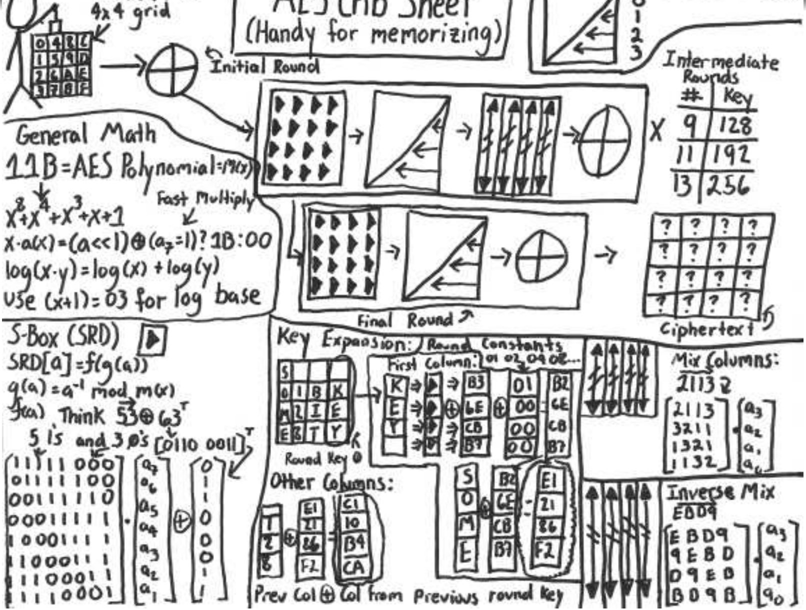
[1] Radio-Frequency IDentification

Authentication Using a Block Cipher (e.g. AES)

prover $\mathcal{P}(\mathbf{s})$ verifier $\mathcal{V}(\mathbf{s})$

- RFID[1] tags: 1k-10k gates, 200-2k for security.
- AES $\geq$ 5k gates.


[1] Radio-Frequency IDentification

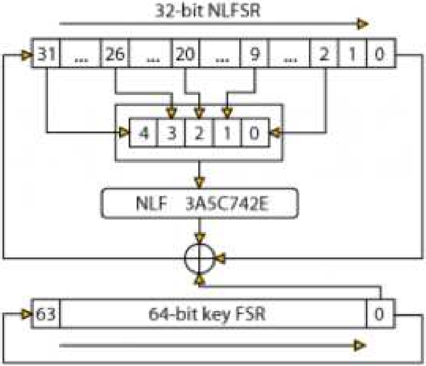


AES: $\mathcal{X} = \{0,1\}^{128}$, $\mathcal{K} = \{0,1\}^{\kappa}$ with $\kappa \in \{128, 196, 256\}$.

$\geq 5k$ gates

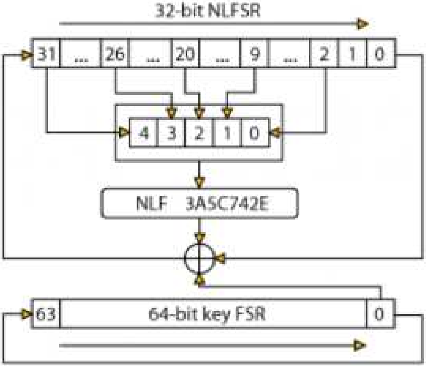
If AES is not an Option...

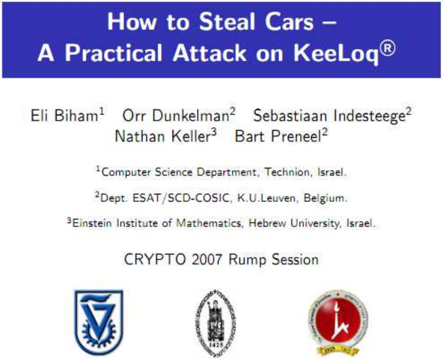
Leight-weight block ciphers: Keeloq, Present,. . .



If AES is not an Option...

Leight-weight block ciphers: Keeloq, Present,. . .





How to Steal Cars –
A Practical Attack on KeeLoq®

Eli Biham[1] Orr Dunkelman[2] Sebastiaan Indesteege[2]
Nathan Keller[3] Bart Preneel[2]

[1]Computer Science Department, Technion, Israel.

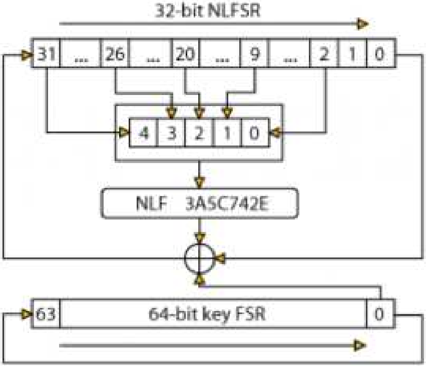
[2]Dept. ESAT/SCD-COSIC, K.U.Leuven, Belgium.

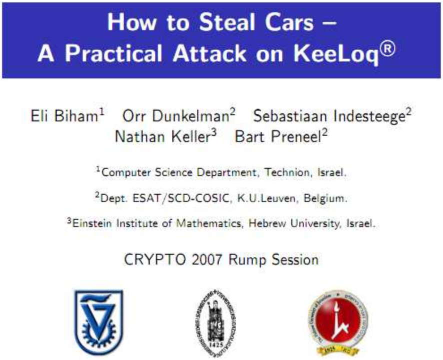
[3]Einstein Institute of Mathematics, Hebrew University, Israel.

CRYPTO 2007 Rump Session

If AES is not an Option...

Leight-weight block ciphers: Keeloq, Present,. . .





Provably Secure (LPN Based) Authentication Schemes. [HB'01],[JW'05],[ACPS'09],[KSS'10],. . .

Learning Parity with Noise (LPN)

The Learning Parity with Noise Assumption

$\mathbf{s} \in \mathbb{Z}_2^n \ , \ 0 < \tau < 0.5$

The Learning Parity with Noise Assumption

$\mathbf{s} \in \mathbb{Z}_2^n$, $0 < \tau < 0.5$

$\mathbf{r}_1 \leftarrow \mathbb{Z}_2^n$ $e_1 \leftarrow \mathsf{Ber}_\tau$

The Learning Parity with Noise Assumption

$\mathbf{s} \in \mathbb{Z}_2^n$, $0 < \tau < 0.5$

$\mathbf{r}_1, \langle \mathbf{r}_1, \mathbf{s} \rangle + e_1$

$\mathbf{r}_1 \leftarrow \mathbb{Z}_2^n \quad e_1 \leftarrow \mathsf{Ber}_\tau$

The Learning Parity with Noise Assumption

$\mathbf{s} \in \mathbb{Z}_2^n$, $0 < \tau < 0.5$

$\mathbf{r}_1, \langle \mathbf{r}_1, \mathbf{s} \rangle + e_1$

$\mathbf{r}_2, \langle \mathbf{r}_2, \mathbf{s} \rangle + e_2$

$\vdots$

$\mathbf{r}_2 \leftarrow \mathbb{Z}_2^n$ $e_2 \leftarrow \mathrm{Ber}_\tau$

The Learning Parity with Noise Assumption

$\mathbf{s} \in \mathbb{Z}_2^n$, $0 < \tau < 0.5$

$$\longrightarrow \mathbf{r}_1, \langle \mathbf{r}_1, \mathbf{s} \rangle + e_1 \longrightarrow$$
$$\longrightarrow \mathbf{r}_2, \langle \mathbf{r}_2, \mathbf{s} \rangle + e_2 \longrightarrow$$
$$\vdots$$

$\mathbf{r}_2 \leftarrow \mathbb{Z}_2^n$ $e_2 \leftarrow \mathrm{Ber}_\tau$

(q, n, τ) LPN assumption (Search Version)

Hard to find $\mathbf{s}$.

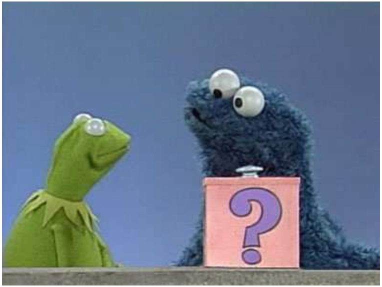
(q, n, τ) LPN assumption (Decisional Version)

Hard to distinguish outputs from uniformly random.

Hardness of LPN

- (Search) LPN equivalent to decoding random linear codes.

- Search & decision polynomially equivalent.
- Best (quantum) algorithms run in time $\Theta(2^{n/\log n})$.



Authentication from LPN

The HB protocol [Hopper and Blum AC'01]

$$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$$

$$
\begin{array}{ccc}
\mathcal{P}(\mathbf{s}) & & \mathcal{V}(\mathbf{s}) \\
 & \xleftarrow{\quad \mathbf{a} \quad} & \mathbf{a} \leftarrow \mathbb{Z}_2^\ell \\
e \leftarrow \mathrm{Ber}_\tau & & \\
z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e & \xrightarrow{\quad z \quad} & \text{accept if } \underbrace{\langle \mathbf{a}, \mathbf{s} \rangle \oplus z}_{e} = 0
\end{array}
$$

The HB protocol [Hopper and Blum AC'01]

$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{a} \quad}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathsf{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{\quad z \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s} \rangle \oplus z}_{e} = 0$

- Secure against passive attacks from LPN. ▸ to proof

The HB protocol [Hopper and Blum AC'01]

$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{a} \quad}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{\quad z \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s} \rangle \oplus z}_{e} = 0$

- Secure against passive attacks from LPN. to proof
- Correctness error 0.1. Soundness error $0.5 + \text{negl}$.

The HB protocol [Hopper and Blum AC'01]

$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{a} \quad}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathsf{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{\quad z \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s} \rangle \oplus z}_{e} = 0$

- Secure against passive attacks from LPN. to proof
- Correctness error 0.1. Soundness error $0.5 + \text{negl}$.
- Can be amplified repeating n times $\Rightarrow$ Errors become $2^{-\Theta(n)}$.

The HB protocol [Hopper and Blum AC'01]

$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{a} \quad}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{\quad z \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s} \rangle \oplus z}_{e} = 0$

- Secure against passive attacks from LPN. ▸ to proof
- Correctness error 0.1. Soundness error $0.5 +$ negl.
- Can be amplified repeating n times $\Rightarrow$ Errors become $2^{-\Theta(n)}$.
- Not secure against active attacks:
  1. ask for $\langle \mathbf{a}, \mathbf{s} \rangle \oplus e_i$ (for several i) $\Rightarrow$ majority is $\langle \mathbf{a}, \mathbf{s} \rangle$ w.h.p..
  2. recover $\mathbf{s}$ from $\langle \mathbf{a}_j, \mathbf{s} \rangle$ ($j = 1, \ldots, \ell$) using Gaussian elimination.

The HB$^+$ protocol [Juels and Weis Crypto'05]

$\tau = 0.1 \qquad \mathbf{s}', \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s}', \mathbf{s})$		$\mathcal{V}(\mathbf{s}', \mathbf{s})$
	$\xleftarrow{\ \mathbf{a}\ }$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathsf{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{\ z\ }$	accept if $\langle \mathbf{a}, \mathbf{s} \rangle \oplus z = 0$

The HB$^+$ protocol [Juels and Weis Crypto'05]

$\tau = 0.1 \qquad \mathbf{s}', \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s}', \mathbf{s})$		$\mathcal{V}(\mathbf{s}', \mathbf{s})$
$\mathbf{b} \leftarrow \mathbb{Z}_2^\ell$	$\xrightarrow{\mathbf{b}}$	
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{b}, \mathbf{s}' \rangle \oplus \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{z}$	accept if $\langle \mathbf{b}, \mathbf{s}' \rangle \oplus \langle \mathbf{a}, \mathbf{s} \rangle \oplus z = 0$

- Secure against active attacks. ▸ to proof

The HB$^+$ protocol [Juels and Weis Crypto'05]

$\tau = 0.1 \qquad \mathbf{s}', \mathbf{s} \leftarrow \mathbb{Z}_2^\ell$

$\mathcal{P}(\mathbf{s}', \mathbf{s})$		$\mathcal{V}(\mathbf{s}', \mathbf{s})$
$\mathbf{b} \leftarrow \mathbb{Z}_2^\ell$	$\xrightarrow{\mathbf{b}}$	
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell$
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{b}, \mathbf{s}' \rangle \oplus \langle \mathbf{a}, \mathbf{s} \rangle \oplus e$	$\xrightarrow{z}$	accept if
		$\langle \mathbf{b}, \mathbf{s}' \rangle \oplus \langle \mathbf{a}, \mathbf{s} \rangle \oplus z = 0$

- Secure against active attacks. ▸ to proof
- Can be amplified by repetition [KS'06].

HB

- ☺ Round Optimal (2 Rounds).
- ☺ Tight reduction: LPN ε-hard $\Rightarrow$ HB ε-secure.
- ☹ Passive security.

HB+

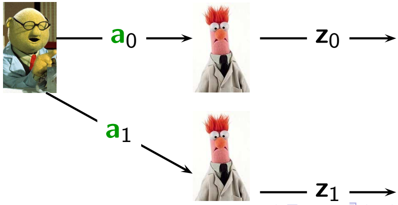
- ☺ Active Security.
- ☹ 3 Rounds (Prover must be stateful).
- ☹ Loose reduction: LPN ε-hard $\Rightarrow$ HB $\sqrt{\varepsilon}$-secure.
- ☹ Reduction not Quantum (No Cloning Theorem.)

HB

- ☺ Round Optimal (2 Rounds).
- ☺ Tight reduction: LPN ε-hard $\Rightarrow$ HB ε-secure.
- ☹ Passive security.

HB+

- ☺ Active Security.
- ☹ 3 Rounds (Prover must be stateful).
- ☹ Loose reduction: LPN ε-hard $\Rightarrow$ HB $\sqrt{\varepsilon}$-secure.
- ☹ Reduction not Quantum (No Cloning Theorem.)

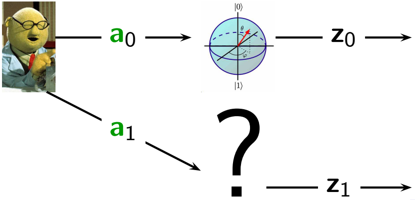


HB

- ☺ Round Optimal (2 Rounds).
- ☺ Tight reduction: LPN ε-hard $\Rightarrow$ HB ε-secure.
- ☹ Passive security.

HB+

- ☺ Active Security.
- ☹ 3 Rounds (Prover must be stateful).
- ☹ Loose reduction: LPN ε-hard $\Rightarrow$ HB $\sqrt{\varepsilon}$-secure.
- ☹ Reduction not Quantum (No Cloning Theorem.)



http://www.ecrypt.eu.org/lightweight/index.php/HB

1. Nicholas J. Hopper, Manuel BlumSecure Human Identification Protocols. ASIACRYPT 2001
2. Ari Juels, Stephen A. Weis.Authenticating Pervasive Devices with Human Protocols. CRYPTO 2005
3. Jonathan Katz, Ji Sun Shin.Parallel and Concurrent Security of the HB and HB+ Protocols. EUROCRYPT 2006
4. Éric Levieil, Pierre-Alain Fouque.An Improved LPN Algorithm. SCN 2006
5. Henri Gilbert, Matt Robshaw, Herve Sibert.An Active Attack Against HB+ - A Provably Secure Lightweight Authentication Protocol. Cryptology ePrint Archive.
6. Jonathan Katz, Adam Smith.Analyzing the HB and HB+ Protocols in the Large Error Case. Cryptology ePrint Archive.
7. Julien Bringer, Hervé Chabanne, Emmanuelle Dottax.HB++.a Lightweight Authentication Protocol Secure against Some Attacks. SecPerU 2006
8. Jonathan Katz.Efficient Cryptographic Protocols Based on the Hardness of Learning Parity with Noise. IMA Int. Conf. 2007
9. Jorge Munilla, Alberto Peinado.HB-MP.A further step in the HB-family of lightweight authentication protocols. Computer Networks 51(9).2262-2267 (2007)
10. Dang Nguyen Duc, Kwangjo Kim.Securing HB+ against GRS Man-in-the-Middle Attack. Proc. Of SCIS 2007, Abstracts pp.123, Jan. 23-26, 2007, Sasebo, Japan.
11. Henri Gilbert, Matthew J. B. Robshaw, Yannick Seurin.HB#.Increasing the Security and Efficiency of HB+. EUROCRYPT 2008
12. Henri Gilbert, Matthew J. B. Robshaw, Yannick Seurin.Good Variants of HB+ Are Hard to Find. Financial Cryptography 2008
13. Henri Gilbert, Matthew J. B. Robshaw, Yannick Seurin.How to Encrypt with the LPN Problem. ICALP (2) 2008
14. Julien Bringer, Herv Chabanne.Trusted-HB.A Low-Cost Version of HB+ Secure Against Man-in-the-Middle Attacks. IEEE Transactions on Information Theory 54(9).4339-4342 (2008).
15. Khaled Ouafi, Raphael Overbeck, Serge Vaudenay.On the Security of HB# against a Man-in-the-Middle Attack. ASIACRYPT 2008
16. Zbigniew Golebiewski, Krzysztof Majcher, Filip Zagorski, Marcin Zawada.Practical Attacks on HB and HB+ Protocols. Cryptology ePrint Archive.
17. Xuefei Leng, Keith Mayes, Konstantinos Markantonakis.HB-MP+ Protocol.An Improvement on the HB-MP Protocol. IEEE International Conference on RFID, 2008 April 2008.
18. Dmitry Frumkin, Adi Shamir.Un-Trusted-HB.Security Vulnerabilities of Trusted-HB. Cryptology ePrint Archive.

New Authentication Protocol

- ☺ Active Security.
- ☺ Round Optimal (2 Rounds).
- ☺ Tight (Quantum) Reduction.

Subset LPN

Subspace LWE, K.Pietrzak, Manuscript 2011.

LPN

$\mathbf{s} \in \mathbb{Z}_2^m$

LPN

$\mathbf{s} \in \mathbb{Z}_2^m$

$\mathbf{r} \leftarrow \mathbb{Z}_2^m \quad e \leftarrow \mathrm{Ber}_\tau$

LPN

$\mathbf{s} \in \mathbb{Z}_2^m$

$\xrightarrow{\mathbf{r},\ \langle \mathbf{r}, \mathbf{s} \rangle + e}$

$\mathbf{r} \leftarrow \mathbb{Z}_2^m \quad e \leftarrow \mathrm{Ber}_\tau$

Subset LPN

$\mathbf{s} \in \mathbb{Z}_2^m \quad n \leq m$

$\xleftarrow{\quad \mathbf{v} \in \mathbb{Z}_2^m,\ \|\mathbf{v}\|_1 = n \quad}$

Subset LPN

$\mathbf{s} \in \mathbb{Z}_2^m \quad n \leq m$

$\longleftarrow \mathbf{v} \in \mathbb{Z}_2^m, \|\mathbf{v}\|_1 = n \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle + e \longrightarrow$

$\mathbf{r} \leftarrow \mathbb{Z}_2^n \quad e \leftarrow \mathrm{Ber}_\tau$

$m = 6, n = 3$

$$
\begin{array}{rcccccc}
\mathbf{s} = & 1 & 0 & 0 & 0 & 1 & 1 \\
\mathbf{v} = & 0 & 0 & 1 & 1 & 1 & 0 \\
\mathbf{s}_{\downarrow \mathbf{v}} = & & & 0 & 0 & 1 &
\end{array}
$$

Subset LPN

$\mathbf{s} \in \mathbb{Z}_2^m \quad n \leq m$

$\longleftarrow \mathbf{v} \in \mathbb{Z}_2^m, \|\mathbf{v}\|_1 = n \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle + e \longrightarrow$

(m, n, τ) Subset LPN Assumption

Hard to distinguish outputs from uniform.

Subset LPN

$\mathbf{s} \in \mathbb{Z}_2^m \qquad n \leq m$

$\xleftarrow{\quad \mathbf{v} \in \mathbb{Z}_2^m,\ \|\mathbf{v}\|_1 = n \quad}$

$\xrightarrow{\quad \mathbf{r},\ \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle + e \quad}$

(m, n, τ) Subset LPN Assumption

Hard to distinguish outputs from uniform.

(m, n, τ) Subset LPN $\Rightarrow$ (n, τ) LPN.

Subset LPN

$\mathbf{s} \in \mathbb{Z}_2^m \quad n \leq m$

$\longleftarrow \mathbf{v} \in \mathbb{Z}_2^m, \|\mathbf{v}\|_1 = n \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle + e \longrightarrow$

(m, n, τ) Subset LPN Assumption

Hard to distinguish outputs from uniform.

(m, n, τ) Subset LPN $\Rightarrow$ (n, τ) LPN.

Theorem

(n, τ) LPN $\Rightarrow$ $(m, n - d, \tau)$ Subset LPN $(2^{-d} = \mathrm{negl})$

Authentication from Subset LPN

HB *and Friends*

$\mathcal{P}(\mathbf{s})$ $\qquad\qquad\qquad\qquad$ $\mathcal{V}(\mathbf{s})$

$$\xleftarrow{\quad \mathbf{a} \quad}$$

$$\xrightarrow{\quad \langle \mathbf{a}, \mathbf{s} \rangle \oplus e \quad}$$

New Approach

$\mathcal{P}(\mathbf{s})$ $\qquad\qquad\qquad\qquad$ $\mathcal{V}(\mathbf{s})$

$$\xleftarrow{\quad \mathbf{v} \quad}$$

$$\xrightarrow{\quad \mathbf{a}, \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e \quad}$$

HB *and Friends*

$\mathcal{P}(\mathbf{s})$ $\qquad\qquad$ $\mathcal{V}(\mathbf{s})$

$$\xleftarrow{\quad\mathbf{a}\quad} \qquad \mathbf{a} \leftarrow \mathbb{Z}_2^\ell$$

$$\xrightarrow{\quad\langle \mathbf{a}, \mathbf{s}\rangle \oplus e\quad}$$

New Approach

$\mathcal{P}(\mathbf{s})$ $\qquad\qquad$ $\mathcal{V}(\mathbf{s})$

$$\mathbf{a} \leftarrow \mathbb{Z}_2^\ell \qquad \xleftarrow{\quad\mathbf{v}\quad}$$

$$\xrightarrow{\quad\mathbf{a}, \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}}\rangle \oplus e\quad}$$

$\tau = 0.1 \qquad \mathbf{s} \leftarrow \mathbb{Z}_2^{2\ell}$

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{v} \quad}$	$\mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}\ ,\ \lVert\mathbf{v}\rVert_1 = \ell$
$\mathbf{a} \leftarrow \mathbb{Z}_2^{\ell}$		
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e$	$\xrightarrow{\quad \mathbf{a}, z \quad}$	accept if
		$\lVert \underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus z}_{e} \rVert_1 \leq 0.2n$

$\tau = 0.1$ $\quad$ $\mathbf{s} \leftarrow \mathbb{Z}_2^{2\ell}$ $\quad$ n : # of repetitions.

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{v} \quad}$	$\mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}$, $\|\mathbf{v}\|_1 = \ell$
$\mathbf{A} \leftarrow \mathbb{Z}_2^{\ell \times n}$		
$\mathbf{e} \leftarrow \mathrm{Ber}_\tau^n$		
$\mathbf{z} := \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}$	$\xrightarrow{\quad \mathbf{A}, \mathbf{z} \quad}$	accept if
		$\| \underbrace{\mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{z}}_{\mathbf{e}} \|_1 \leq 0.2n$
		and $\mathrm{rank}(\mathbf{A}) = n$

Active Security of New Protocol

▸ to protocol

If $\exists$  *who breaks active security, then Subset LPN is not hard.*

Active Security of New Protocol

▸ to protocol

If $\exists$  *who breaks* *<u>active</u>* *security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{P}(\mathbf{s})$

Active Security of New Protocol ▸ to protocol

If $\exists$  *who breaks* *<u>active</u>* *security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{P}(\mathbf{s})$

$\xleftarrow{\quad \mathbf{v} \quad}$

Active Security of New Protocol ▸ to protocol

If ∃  *who breaks* ***active*** *security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{P}(\mathbf{s})$

 $\xleftarrow{\quad \mathbf{v} \quad}$  $\xleftarrow{\quad \mathbf{v} \quad}$ 

Active Security of New Protocol ▸ to protocol

If $\exists$  *who breaks* ***active*** *security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{P}(\mathbf{s})$

$\xleftarrow{\mathbf{v}}$

$\xrightarrow{\mathbf{A},\ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}}$

$\xleftarrow{\mathbf{v}}$

Active Security of New Protocol to protocol

If $\exists$  *who breaks <u>active</u> security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{P}(\mathbf{s})$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

Active Security of New Protocol ▸ to protocol

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$ Simulates $\mathcal{V}(\mathbf{s})$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{V}(\mathbf{s})$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xrightarrow{\quad \mathbf{v}^* \quad}$

Active Security of New Protocol

▸ to protocol

If $\exists$  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{V}(\mathbf{s})$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xleftarrow{\quad \mathbf{v} \quad}$

$\xrightarrow{\quad \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \quad}$

$\xrightarrow{\quad \mathbf{v}^* \quad}$

$\xleftarrow{\quad \mathbf{A}^*, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}^*} \oplus \mathbf{e}^* \quad}$

Active Security of New Protocol ▸ to protocol

If ∃  *who breaks* *active* *security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$ Simulates $\mathcal{V}(\mathbf{s})$

$\longleftarrow \mathbf{v} \longleftarrow$

$\longrightarrow \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \longrightarrow$

$\longleftarrow \mathbf{v} \longleftarrow$

$\longrightarrow \mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \longrightarrow$

$\longrightarrow \mathbf{v}^* \longrightarrow$

$\longleftarrow \mathbf{A}^*, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}^*} \oplus \mathbf{e}^* \longleftarrow$

- If $\mathbf{e} \leftarrow \mathrm{Ber}_\tau^n \Rightarrow$ simulation of $\mathcal{P}(\mathbf{s})$ perfect $\Rightarrow \|\mathbf{e}^*\|_1 \leq 0.2n$.
- If $\mathbf{e}$ uniform $\Rightarrow \mathbf{s}$ hidden $\Rightarrow \mathbf{e}^*$ *uniform* $\Rightarrow \|\mathbf{e}^*\|_1 \approx 0.5n$.

Active Security of New Protocol

▸ to protocol

If $\exists$  *who breaks* *active* *security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$ Simulates $\mathcal{V}(\mathbf{s})$

$\leftarrow \mathbf{v}$

$\mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \rightarrow$

$\leftarrow \mathbf{v}$

$\mathbf{A}, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \rightarrow$

$\mathbf{v}^* \rightarrow$

$\leftarrow \mathbf{A}^*, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}^*} \oplus \mathbf{e}^*$

- If $\mathbf{e} \leftarrow \mathrm{Ber}_{\tau}^{n} \Rightarrow$ simulation of $\mathcal{P}(\mathbf{s})$ perfect $\Rightarrow \|\mathbf{e}^*\|_1 \leq 0.2n$.
- If $\mathbf{e}$ uniform $\Rightarrow \mathbf{s}$ hidden $\Rightarrow \mathbf{e}^*$ *uniform* $\Rightarrow \|\mathbf{e}^*\|_1 \approx 0.5n$.
- But... can't compute $\|\mathbf{e}^*\|_1$ from $\mathbf{A}^*, \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}^*} \oplus \mathbf{e}^*$.

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks active security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} \in \mathbb{Z}_2^{\ell}$

Simulates $\mathcal{V}(\mathbf{s})$

$\longleftarrow \mathbf{v} \longleftarrow$

$\longrightarrow \mathbf{A}, \mathbf{A}^T\mathbf{s}_{\downarrow\mathbf{v}} \oplus \mathbf{e} \longrightarrow$

$\longleftarrow \mathbf{v} \longleftarrow$

$\longrightarrow \mathbf{A}, \mathbf{A}^T\mathbf{s}_{\downarrow\mathbf{v}} \oplus \mathbf{e} \longrightarrow$

$\longrightarrow \mathbf{v}^* \longrightarrow$

$\longleftarrow \mathbf{A}^*, \mathbf{A}^T\mathbf{s}_{\downarrow\mathbf{v}^*} \oplus \mathbf{e}^* \longleftarrow$

- If $\mathbf{e} \leftarrow \mathrm{Ber}_{\tau}^{n} \Rightarrow$ simulation of $\mathcal{P}(\mathbf{s})$ perfect $\Rightarrow \|\mathbf{e}^*\|_1 \leq 0.2n$.
- If $\mathbf{e}$ uniform $\Rightarrow \mathbf{s}$ hidden $\Rightarrow \mathbf{e}^*$ *uniform* $\Rightarrow \|\mathbf{e}^*\|_1 \approx 0.5n$.
- But... can't compute $\|\mathbf{e}^*\|_1$ from $\mathbf{A}^*, \mathbf{A}^T\mathbf{s}_{\downarrow\mathbf{v}^*} \oplus \mathbf{e}^*$.
- Simulate protocol for key $\hat{\mathbf{s}} \in \mathbb{Z}_2^{2\ell}$ such that

$$\hat{\mathbf{s}}_{\downarrow\mathbf{v}^*} \text{ known} \qquad \hat{\mathbf{s}}_{\downarrow\overline{\mathbf{v}^*}} = \mathbf{s}$$

Length of LPN secret $\ell \approx 500$ # Repetitions $n \approx 160$

Efficiency

- Keysize $4\ell = 2000$ bits
- Communication $2\ell n \approx 20kb$
- Computation (small multiple of) ℓn.

Length of LPN secret $\ell \approx 500$ $\quad$ $\#$ Repetitions $n \approx 160$

Efficiency

- Keysize $4\ell = 2000c$ bits
- Communication $2\ell n \approx 20kb/c$
- Computation (small multiple of) ℓn.
- Communication vs. Keysize tradeoff $c \in \{1, \ldots, n\}$.

Length of LPN secret $\ell \approx 500$ # Repetitions $n \approx 160$

Efficiency

- Keysize $4\ell = 2000c$ bits
- Communication $2\ell n \approx 20kb/c$
- Computation (small multiple of) ℓn.
- Communication vs. Keysize tradeoff $c \in \{1, \dots, n\}$.

Protocol with Communication & Key-size ℓ and computation $\ell \log \ell$ from "Field-LPN" (with S.Heyse, E.Kiltz, V.Lyubashevsky, C.Paar) First prototype implemented.

Lapin: An Efficient Authentication Protocol Based on Ring-LPN

Stefan Heyse[1], Eike Kiltz[1], Vadim Lyubashevsky[2], Christof Paar[1], and Krzysztof Pietrzak[3*]

[1] Ruhr-Universität Bochum
[2] INRIA / ENS, Paris
[3] IST Austria

Public parameters: $\mathsf{R}, \pi{:}\{0,1\}^\lambda \to \mathsf{R}, \tau, \tau', \lambda$.
Secret key: $K = (s, s') \in \mathsf{R}^2$.

	Tag		**Reader**
①		$\xleftarrow{c}$	$c \xleftarrow{\$} \{0,1\}^\lambda$
②	$r \xleftarrow{\$} \mathsf{R}^*$; $e \xleftarrow{\$} \mathsf{Ber}_\tau^{\mathsf{R}} \in \mathsf{R}$		
③	$z := r \cdot (s \cdot \pi(c) \oplus s') \oplus e$	$\xrightarrow{(r,z)}$	
④			if $r \notin \mathsf{R}^*$ reject
⑤			$e' := z - r \cdot (s \cdot \pi(c) \oplus s')$
⑥			if $HW(e') > n \cdot \tau'$ reject else accept

Fig. 1. Two-round Lapin authentication protocol.

Hardware Implementation and Side-Channel Analysis of Lapin

Lubos Gaspar[1], Gaëtan Leurent[1,2], and François-Xavier Standaert[1]

[1] ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Belgium.
[2] Inria, EPI SECRET, Rocquencourt, France.
e-mails: {lubos.gaspar,fstandae}@uclouvain.be,gaetan.leurent@inria.fr

# of shares d	AES *softw.* [16, 8]	Lapin *softw.* [9]	Lapin *8b hardw.*
1	5100	112500	20977
2	286844	225016	41969
3	572069	337532	62961
4	1003154	450048	83953
5	1489539	562564	104945
6	2095756	675080	125937
7	2779561	787596	146929

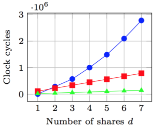


Fig. 3. Number of clock cycles vs. number of shares (d) for software AES [16, 8], software Lapin [9] and hardware Lapin. With increase of used shares, the computation time increases quadratically for the AES and only linearly for both Lapin implementations.

The Provable Security Mantra

Practical Efficiency OR Proveable Security

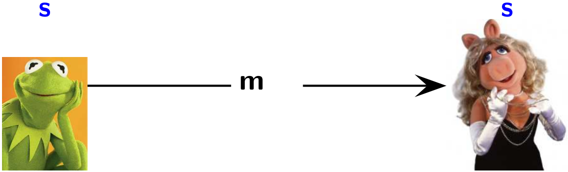
The Provable Security Mantra

Practical Efficiency OR Proveable Security

Efficient (cycles & gate count) AND Provably Secure

Message Authentication

Message Authentication Codes



Message Authentication Codes

s **s**

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \text{MAC}(\mathbf{s}, \mathbf{m})$

$\text{accept} \leftarrow \text{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

Message Authentication Codes

$\mathbf{s}$ $\mathbf{s}$

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$ $\mathsf{accept} \leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

Message Authentication Codes

$\mathbf{s}$ $\qquad\qquad\qquad\qquad$ $\mathbf{s}$

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$ $\qquad\qquad$ $\mathsf{accept} \leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\xrightarrow{\mathbf{m}} \mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

Message Authentication Codes

$\mathbf{s}$ $\mathbf{s}$

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$

$\mathsf{accept} \leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\longleftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m}) \longrightarrow \mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

Message Authentication Codes

$\mathbf{s}$ $\mathbf{s}$

$\mathbf{m}, \sigma$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$ accept $\leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\mathbf{m}, \sigma$

$\mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

Message Authentication Codes

$\mathbf{s}$ $\qquad\qquad$ $\mathbf{s}$

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$ $\qquad\qquad$ $\mathsf{accept} \leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

$\mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

Message Authentication Codes

$\mathbf{s}$ $\qquad\qquad\qquad\qquad$ $\mathbf{s}$

$\xrightarrow{\mathbf{m}, \sigma}$

$\sigma \leftarrow \mathsf{MAC}(\mathbf{s}, \mathbf{m})$ $\qquad\qquad$ $\mathsf{accept} \leftarrow \mathsf{VRFY}(\mathbf{s}, \mathbf{m}, \sigma)$

UF-CMA Security (UnForgeability under Chosen Message Attacks)

$\mathbf{m}^*, \sigma^* \longleftarrow$

$\mathsf{MAC}(\mathbf{s}, .)$

$\mathsf{VRFY}(\mathbf{s}, ., .)$

$$\Pr[\mathsf{VRFY}(\mathbf{m}^*, \sigma^*) = \mathsf{accept}] = \mathsf{negl}$$

MAC from Identification

$$\begin{array}{ccc} \mathcal{P}(\mathbf{s}) & & \mathcal{V}(\mathbf{s}) \\ & \xleftarrow{\quad \mathbf{v} \quad} & \mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}\ ,\ \|\mathbf{v}\|_1 = \ell \\ \mathbf{a} \leftarrow \mathbb{Z}_2^{\ell} & & \\ e \leftarrow \mathsf{Ber}_\tau & & \\ \mathbf{z} := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e & \xrightarrow{\quad \mathbf{z} \quad} & \text{accept if } \underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus \mathbf{z}}_{e} = 0 \end{array}$$

MAC from Identification

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{v} \quad}$	$\mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}$, $\|\mathbf{v}\|_1 = \ell$
$\mathbf{a} \leftarrow \mathbb{Z}_2^{\ell}$		
$e \leftarrow \mathsf{Ber}_\tau$		
$\mathbf{z} := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e$	$\xrightarrow{\quad \mathbf{z} \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle}_{e} \oplus \mathbf{z} = 0$

- $\mathsf{MAC}(\mathbf{s}, \mathbf{v}) : [\mathbf{A} \ , \ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}]$

MAC from Identification

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{v} \quad}$	$\mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}\ ,\ \|\mathbf{v}\|_1 = \ell$
$\mathbf{a} \leftarrow \mathbb{Z}_2^{\ell}$		
$e \leftarrow \mathsf{Ber}_\tau$		
$\mathbf{z} := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e$	$\xrightarrow{\quad \mathbf{z} \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle}_{e} \oplus \mathbf{z} = 0$

- MAC$(\mathbf{s}, \mathbf{v})$: $[\mathbf{A}\ ,\ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}]$
- Weakly secure MAC: no VRFY queries & random challange.

MAC from Identification

$\mathcal{P}(\mathbf{s})$		$\mathcal{V}(\mathbf{s})$
	$\xleftarrow{\quad \mathbf{v} \quad}$	$\mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}$, $\lVert \mathbf{v} \rVert_1 = \ell$
$\mathbf{a} \leftarrow \mathbb{Z}_2^{\ell}$		
$e \leftarrow \mathsf{Ber}_\tau$		
$\mathbf{z} := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e$	$\xrightarrow{\quad \mathbf{z} \quad}$	accept if $\underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle}_{e} \oplus \mathbf{z} = 0$

- $\mathsf{MAC}(\mathbf{s}, \mathbf{v}) : [\mathbf{A} \ , \ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}]$
- Weakly secure MAC: no VRFY queries & random challange.
- $\mathsf{MAC}(\mathbf{s}, \mathbf{m}) : [\mathbf{A} \ , \ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}] \qquad \mathbf{v} = \mathsf{encode}(\mathbf{m})$
- Weakly secure MAC: no VRFY queries & selective.

MAC from Identification

$$\begin{array}{ccc} \mathcal{P}(\mathbf{s}) & & \mathcal{V}(\mathbf{s}) \\ & \xleftarrow{\quad \mathbf{v} \quad} & \mathbf{v} \leftarrow \mathbb{Z}_2^{2\ell}\ ,\ \|\mathbf{v}\|_1 = \ell \\ \mathbf{a} \leftarrow \mathbb{Z}_2^{\ell} & & \\ e \leftarrow \mathsf{Ber}_\tau & & \\ \mathbf{z} := \langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle \oplus e & \xrightarrow{\quad \mathbf{z} \quad} & \text{accept if } \underbrace{\langle \mathbf{a}, \mathbf{s}_{\downarrow \mathbf{v}} \rangle}_{e} \oplus \mathbf{z} = 0 \end{array}$$

- $\mathsf{MAC}(\mathbf{s}, \mathbf{v}) : [\mathbf{A}\ ,\ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}]$
- Weakly secure MAC: no VRFY queries & random challange.
- $\mathsf{MAC}(\mathbf{s}, \mathbf{m}) : [\mathbf{A}\ ,\ \mathbf{A}^T \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e}]$ $\quad \mathbf{v} = \mathrm{encode}(\mathbf{m})$
- Weakly secure MAC: no VRFY queries & selective.
- Generic boosting to UF-CMA secure $\overline{\mathsf{MAC}}$:

$\overline{\mathsf{MAC}}(\{\mathbf{s}, \pi, h\}, \mathbf{m}) = \pi(z)$ *where*

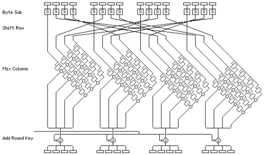
$$b \stackrel{U}{\leftarrow} \{0,1\}^{\mu} \qquad z \leftarrow \mathsf{MAC}(\mathbf{s}, h(\mathbf{m}, b))$$

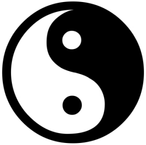
h, π *pairwise independent hash-function/permutation.*

Questions?

The Provable Security Mantra

Practical Efficiency OR *Provable Security*





RSA Encryption:

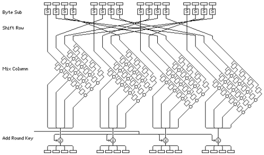
$$N = pq$$

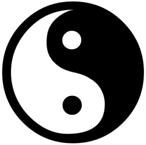
$$ENC(pk, m) = m^{pk} \bmod N$$

$$DEC(sk, c) = c^{sk} \bmod N$$

The Provable Security Mantra

Practical Efficiency OR Provable Security





RSA Encryption:

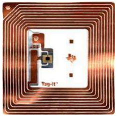
$$N = pq$$
$$ENC(pk, m) = m^{pk} \bmod N$$
$$DEC(sk, c) = c^{sk} \bmod N$$

Extremely Efficient AND Provably Secure

i.e. as hard to break as decoding random linear codes.

Final Disclaimer

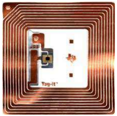
Efficient, Provably secure, RKA-secure Crypo for lightweight devices.



[2] compared to computation

Final Disclaimer

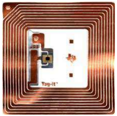
Efficient, Provably secure, RKA-secure Crypo for lightweight devices. Why not use everywhere!



[2] compared to computation

Final Disclaimer

Efficient, Provably secure, RKA-secure Crypo for lightweight devices. Why not use everywhere!

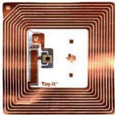


- Schemes need a lot of randomness.

[2]compared to computation

Final Disclaimer

Efficient, Provably secure, RKA-secure Crypo for lightweight devices. Why not use everywhere!



- Schemes need a lot of randomness.
- Randomness relatively[2]
  - cheap on RFIDs
  - expensive on chips

[2] compared to computation

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*

Passive Security of HB

Theorem

If ∃  who breaks passive security of HB, then LPN is not hard.

Passive Security of HB

Theorem

If $\exists$  who breaks passive security of HB, then LPN is not hard.

 $\xleftarrow{\quad \mathbf{A}_1, \mathbf{z}_1 \quad}$  $\xleftarrow{\quad \mathbf{A}_1, \mathbf{z}_1 \quad}$ 

Passive Security of HB

Theorem

If ∃  *who breaks passive security of HB, then LPN is not hard.*

 $\xleftarrow{\quad \mathbf{A}_2,\, \mathbf{z}_2 \quad}$  $\xleftarrow{\quad \mathbf{A}_2,\, \mathbf{z}_2 \quad}$ 

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*

 $\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$  $\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$ 

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*

$\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$

$\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$

$\longleftarrow \mathbf{A}_{q}, \mathbf{z}_{q} \longrightarrow$

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*

$\xleftarrow{\mathbf{A}_{q-1},\, \mathbf{z}_{q-1}}$

$\xleftarrow{\mathbf{A}_{q}}$

$\xleftarrow{\mathbf{A}_{q-1},\, \mathbf{z}_{q-1}}$

$\xleftarrow{\mathbf{A}_{q},\, \mathbf{z}_{q}}$

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*

$\xleftarrow{\quad \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \quad}$

$\xleftarrow{\quad \mathbf{A}_{q} \quad}$

$\xrightarrow{\quad \hat{\mathbf{z}} \quad}$

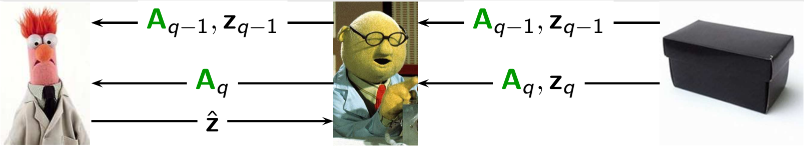
$\xleftarrow{\quad \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \quad}$

$\xleftarrow{\quad \mathbf{A}_{q}, \mathbf{z}_{q} \quad}$

Passive Security of HB

Theorem

If ∃  *who breaks passive security of HB, then LPN is not hard.*



output $\|\mathbf{z}_q \oplus \hat{\mathbf{z}}\| \overset{?}{\leq} 0.4 \cdot n$

Passive Security of HB

Theorem

If $\exists$  who breaks passive security of HB, then LPN is not hard.

$\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$

$\longleftarrow \mathbf{A}_{q} \longrightarrow$

$\longrightarrow \hat{\mathbf{z}} \longrightarrow$

$\longleftarrow \mathbf{A}_{q-1}, \mathbf{z}_{q-1} \longrightarrow$

$\longleftarrow \mathbf{A}_{q}, \mathbf{z}_{q} \longrightarrow$

output $\|\mathbf{z}_q \oplus \hat{\mathbf{z}}\| \overset{?}{\leq} 0.4 \cdot n$

If $\mathbf{z}_i = \mathbf{A}_i^T \mathbf{s} + \mathbf{e}_i$ *with* $\mathbf{e}_i \leftarrow \mathrm{Ber}_\tau^n$

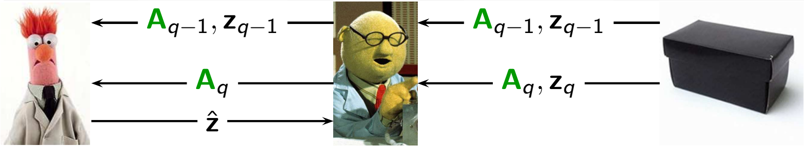
- *View of*  *like in HB.* ▸ to protocol
-  *breaks security:* $\hat{\mathbf{z}} = \mathbf{A}_q^T \mathbf{s} \oplus \hat{\mathbf{e}}$ *where* $\|\hat{\mathbf{e}}\| \leq 0.2 \cdot n$.
- *Then* $\|\mathbf{z}_q \oplus \hat{\mathbf{z}}\| = \|\mathbf{A}_q^T \mathbf{s} \oplus \hat{\mathbf{e}} \oplus \mathbf{A}_q^T \mathbf{s} \oplus \mathbf{e}_q\| = \|\hat{\mathbf{e}} \oplus \mathbf{e}_q\| \approx 0.3 \cdot n$

$\Rightarrow$ *output is 1*

Passive Security of HB

Theorem

If $\exists$  *who breaks passive security of HB, then LPN is not hard.*



$$\text{output } \|\mathbf{z}_q \oplus \hat{\mathbf{z}}\| \overset{?}{\leq} 0.4 \cdot n$$

$$\textit{If } \mathbf{z}_i = \mathbf{A}_i^T \mathbf{s} + \mathbf{e}_i \textit{ with } \mathbf{e}_i \leftarrow \mathrm{Ber}_{0.5}^n$$

- $\Rightarrow \mathbf{z}_q \oplus \hat{\mathbf{z}}$ *is random.*
- $\|\mathbf{z}_q \oplus \hat{\mathbf{z}}\| \approx 0.5 \cdot n$

$\Rightarrow$ *output is* 0

Active Security of HB+

Theorem

If $\exists$  who breaks <u>active</u> security of HB+, then LPN is not hard.

Active Security of HB+

Theorem

If $\exists$  who breaks active security of HB+, then LPN is not hard.

1st Phase of Active Attack

$\mathbf{S}_1$

$\mathbf{S}_2$

Active Security of HB+

Theorem

If $\exists$  who breaks <u>active</u> security of HB+, then LPN is not hard.

1st Phase of Active Attack

$\mathbf{s}_1$

$\xrightarrow{\quad \mathbf{B},\ \mathbf{B}^T\mathbf{s}_1 \oplus \mathbf{e} \quad}$

$\mathbf{s}_2$

Theorem

If ∃  *who breaks active security of HB+, then LPN is not hard.*

1st Phase of Active Attack

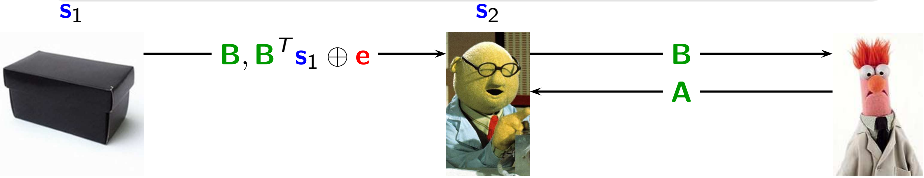
$\mathbf{s}_1$  $\xrightarrow{\mathbf{B},\ \mathbf{B}^T\mathbf{s}_1 \oplus \mathbf{e}}$ $\mathbf{s}_2$  $\xrightarrow{\mathbf{B}}$ 

Active Security of HB+

Theorem

If ∃  *who breaks <u>active</u> security of HB+, then LPN is not hard.*

1st Phase of Active Attack

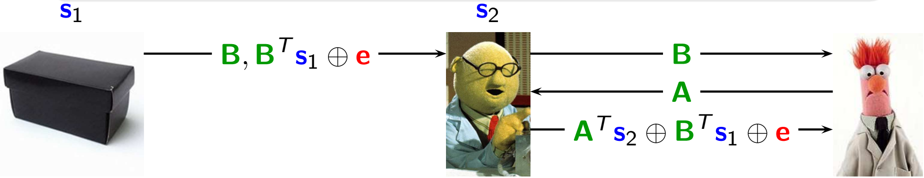


Active Security of HB+

Theorem

If ∃  *who breaks <u>active</u> security of HB+, then LPN is not hard.*

1st Phase of Active Attack



- If $\mathbf{e} \leftarrow \mathrm{Ber}_\tau^n$ then perfectly simulates HB+.
- If $\mathbf{e} \leftarrow \mathrm{Ber}_{0.5}^n$ then perfectly hides $\mathbf{s}_2$.

Active Security of HB+

Theorem

If $\exists$  *who breaks <u>active</u> security of HB+, then LPN is not hard.*

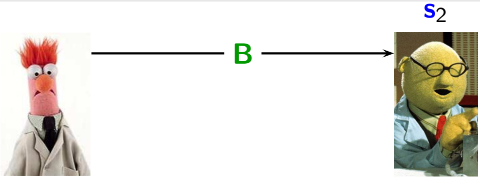
2nd Phase of Active Attack

$\mathbf{s}_2$

Theorem

If $\exists$  who breaks <u>active</u> security of HB+, then LPN is not hard.

2nd Phase of Active Attack

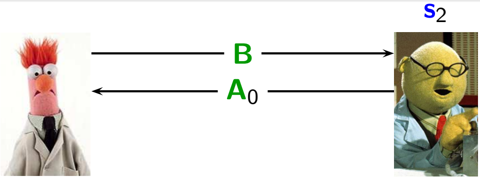


Active Security of HB+

Theorem

If ∃  *who breaks active security of HB+, then LPN is not hard.*

2nd Phase of Active Attack



Active Security of HB+

Theorem

If ∃  *who breaks* <u>*active*</u> *security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\quad \mathbf{B} \quad}$

$\xleftarrow{\quad \mathbf{A}_0 \quad}$

$\xrightarrow{\quad \mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_0 \quad}$

$\mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_0$

Active Security of HB+

Theorem

If $\exists$  *who breaks active security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\mathbf{B}}$

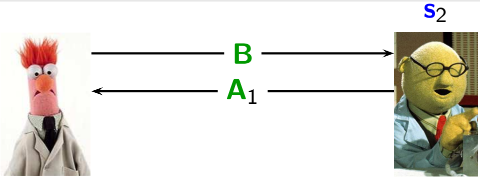
$\mathbf{A}_0^T\mathbf{s}_2 \oplus \mathbf{B}^T\mathbf{s}_1 \oplus \mathbf{e}_0$

Active Security of HB+

Theorem

If $\exists$  *who breaks* <u>*active*</u> *security of HB+, then LPN is not hard.*

2nd Phase of Active Attack



$\mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_0$

Active Security of HB+

Theorem

If $\exists$  *who breaks* <u>*active*</u> *security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\quad \mathbf{B} \quad}$

$\xleftarrow{\quad \mathbf{A}_1 \quad}$

$\xrightarrow{\quad \mathbf{A}_1^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_1 \quad}$

$$\mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_0 \oplus \mathbf{A}_1^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_1$$

Active Security of HB+

Theorem

If $\exists$  *who breaks active security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\quad \mathbf{B} \quad}$

$\xleftarrow{\quad \mathbf{A}_1 \quad}$

$\xrightarrow{\quad \mathbf{A}_1^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_1 \quad}$

$$\mathbf{A}_0^T \mathbf{s}_2 \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_0 \oplus \mathbf{A}_1^T \mathbf{s}_2 \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_1$$

Theorem

If ∃  *who breaks <u>active</u> security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\mathbf{B}}$

$\xleftarrow{\mathbf{A}_1}$

$\xrightarrow{\mathbf{A}_1^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_1}$

$$\mathbf{A}_0^T \mathbf{s}_2 \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_0 \oplus \mathbf{A}_1^T \mathbf{s}_2 \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_1 \oplus \mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{A}_1^T \mathbf{s}_2$$

Active Security of HB+

Theorem

If $\exists$  *who breaks <u>active</u> security of HB+, then LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s}_2$

$\xrightarrow{\quad \mathbf{B} \quad}$

$\xleftarrow{\quad \mathbf{A}_1 \quad}$

$\xrightarrow{\quad \mathbf{A}_1^T \mathbf{s}_2 \oplus \mathbf{B}^T \mathbf{s}_1 \oplus \mathbf{e}_1 \quad}$

$$\cancel{\mathbf{A}_0^T \mathbf{s}_2} \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_0 \oplus \cancel{\mathbf{A}_1^T \mathbf{s}_2} \oplus \cancel{\mathbf{B}^T \mathbf{s}_1} \oplus \mathbf{e}_1 \oplus \cancel{\mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{A}_1^T \mathbf{s}_2} = \mathbf{e}_0 \oplus \mathbf{e}_1$$

- 1st Phase good: $\|\mathbf{e}_0\|_1, \|\mathbf{e}_1\|_1 \leq \tau' \cdot n \Rightarrow \|\mathbf{e}_0 \oplus \mathbf{e}_1\|_1 \leq 2\tau' \cdot n$.
- 1st Phase bad: $\mathbf{A}_0^T \mathbf{s}_2 \oplus \mathbf{A}_1^T \mathbf{s}_2$ uniform $\Rightarrow \|\mathbf{e}_0 \oplus \mathbf{e}_1\|_1 \approx 0.5 \cdot n$

Active Security of New Protocol

to protocol

If $\exists$  *who breaks <u>active</u> security, then Subset LPN is not hard.*

Active Security of New Protocol

▸ to protocol

If ∃  who breaks active security, then Subset LPN is not hard.

1st Phase of Active Attack

$\mathbf{s} = 0101$

$\mathbf{s} = 1001$

- Simulate protocol with key $\mathbf{s} = 01100101$.

Active Security of New Protocol ▸ to protocol

If ∃  *who breaks* <u>*active*</u> *security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} = 0101$

$\mathbf{s} = 1001$

$\longleftarrow \mathbf{v} = 11110000$ ——

- Simulate protocol with key $\mathbf{s} = 01100101$.

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} = \mathbf{01}01$ $\qquad\qquad$ $\mathbf{s} = \mathbf{10}01$

 $\longleftarrow$ $\mathbf{v}' = 1100$ —  $\longleftarrow$ $\mathbf{v} = 11110000$ — 

- Simulate protocol with key $\mathbf{s} = \mathbf{01}\mathbf{10}0101$.

Active Security of New Protocol

to protocol

If ∃  *who breaks active security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} = \mathbf{01}01$

$\longleftarrow \mathbf{v}' = 1100 \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, 01 \rangle \oplus e \longrightarrow$

$\mathbf{s} = \mathbf{10}01$

$\longleftarrow \mathbf{v} = 11110000 \longleftarrow$

- Simulate protocol with key $\mathbf{s} = \mathbf{0110}0101$.

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

1st Phase of Active Attack

$\mathbf{s} = \mathbf{01}01$ $\qquad\qquad$ $\mathbf{s} = \mathbf{10}01$

$\longleftarrow \mathbf{v}' = 1100 \longrightarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, 01 \rangle \oplus e \longrightarrow$

$\longleftarrow \mathbf{v} = 11110000 \longrightarrow$

$\longrightarrow \mathbf{rr}', \langle \mathbf{rr}', 0110 \rangle \oplus e \longrightarrow$

- Simulate protocol with key $\mathbf{s} = \mathbf{0110}0101$.
- $e \leftarrow \mathrm{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- $e \leftarrow \mathrm{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks* *<u>active</u>* *security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} = 1001$

- Simulate protocol with key $\mathbf{s} = 01100101$.
- $e \leftarrow \text{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- $e \leftarrow \text{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.

Active Security of New Protocol

▸ to protocol

If $\exists$  *who breaks active security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} = 1001$

 $\longleftarrow$ $\mathbf{v}^* = 00111100$ —— 

- Simulate protocol with key $\mathbf{s} = 01100101$. $\mathbf{s}_{\downarrow \mathbf{v}^*} = \mathbf{s}$.
- $e \leftarrow \mathrm{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- $e \leftarrow \mathrm{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} = 1001$

$\longleftarrow \mathbf{v}^* = 00111100 \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}^*} \rangle + e \longrightarrow$

- Simulate protocol with key $\mathbf{s} = 01100101$. $\mathbf{s}_{\downarrow \mathbf{v}^*} = \mathbf{s}$.
- $e \leftarrow \mathrm{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- $e \leftarrow \mathrm{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.

Active Security of New Protocol

▸ to protocol

If ∃  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} = 1001$

$\longleftarrow \mathbf{v}^* = 00111100 \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}^*} \rangle + e \longrightarrow$

- Simulate protocol with key $\mathbf{s} = 01100101$. $\mathbf{s}_{\downarrow \mathbf{v}^*} = \mathbf{s}$.
- $e \leftarrow \mathrm{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- Error e must be low weight.
- $e \leftarrow \mathrm{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.

Active Security of New Protocol ▸ to protocol

If $\exists$  *who breaks <u>active</u> security, then Subset LPN is not hard.*

2nd Phase of Active Attack

$\mathbf{s} = 1001$

$\longleftarrow \mathbf{v}^* = 00111100 \longleftarrow$

$\longrightarrow \mathbf{r}, \langle \mathbf{r}, \mathbf{s}_{\downarrow \mathbf{v}^*} \rangle + e \longrightarrow$

- Simulate protocol with key $\mathbf{s} = 01100101$. $\mathbf{s}_{\downarrow \mathbf{v}^*} = \mathbf{s}$.
- $e \leftarrow \mathrm{Ber}_\tau \Rightarrow$ perfectly simulates protocol.
- Error e must be low weight.
- $e \leftarrow \mathrm{Ber}_{0.5} \Rightarrow$ perfectly hides $\mathbf{s}$.
- $\langle \mathbf{r}, \mathbf{s} \rangle$ uniform $\Rightarrow$ error e is uniform.