Subspace LWE & Non-HB Style Authentication from LPN

Krzysztof Pietrzak

CWI Centrum Wiskunde & Informatica

Crypto 2010 Rump Session, Aug. 17ht

Learning Parities with Noise

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

Learning Parities with Noise

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

← next sample —

Learning Parities with Noise

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

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

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

Learning Parities with Noise

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

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

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

Definition (Learning Parities with Noise)

(n, τ)-LPN Problem: distinguish oracle from random.

- Equivalent to decoding of random linear codes.
- Generalization: "Learning with Errors" (LWE) [Regev'05].

The HB authentication protocol [Hopper and Blum AC'01]

$\mathbf{s} \in \mathbb{Z}_2^k \qquad 0 < \tau < 0.5$

$\underline{\mathcal{P}(\mathbf{s}, \tau)}$		$\underline{\mathcal{V}(\mathbf{s})}$
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^k$
$e \leftarrow \mathsf{Ber}_\tau$		
$z := \langle \mathbf{s}, \mathbf{a} \rangle \oplus e$	$\xrightarrow{z}$	
		verify: $z \stackrel{?}{=} \langle \mathbf{s}, \mathbf{a} \rangle$

The HB authentication protocol [Hopper and Blum AC'01]

$\mathbf{s} \in \mathbb{Z}_2^k \qquad 0 < \tau < 0.5$

$\underline{\mathcal{P}(\mathbf{s}, \tau)}$		$\underline{\mathcal{V}(\mathbf{s})}$
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^k$
$e \leftarrow \mathsf{Ber}_\tau$		
$z := \langle \mathbf{s}, \mathbf{a} \rangle \oplus e$	$\xrightarrow{z}$	
		verify: $z \stackrel{?}{=} \langle \mathbf{s}, \mathbf{a} \rangle$

- Secure against passive attacks.
- Correctness error τ. Soundness error $0.5 + \mathsf{negl}$.
- Can be amplified by parallel repetition.
- Not secure against active attacks.

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

$$\mathbf{s}_1, \mathbf{s}_2 \in \mathbb{Z}_2^k \qquad 0 < \tau < 0.5$$

$\underline{\mathcal{P}(\mathbf{s}_1, \mathbf{s}_2, \tau)}$		$\underline{\mathcal{V}(\mathbf{s}_1, \mathbf{s}_2)}$
$\mathbf{b} \leftarrow \mathbb{Z}_2^k$	$\xrightarrow{\mathbf{b}}$	
	$\xleftarrow{\mathbf{a}}$	$\mathbf{a} \leftarrow \mathbb{Z}_2^k$
$e \leftarrow \mathrm{Ber}_\tau$		
$z := \langle \mathbf{s}_1, \mathbf{b} \rangle \oplus \langle \mathbf{s}_2, \mathbf{a} \rangle \oplus e$	$\xrightarrow{z}$	verify:
		$z \stackrel{?}{=} \langle \mathbf{s}_1, \mathbf{b} \rangle \oplus \langle \mathbf{s}_2, \mathbf{a} \rangle$

- Secure against active attacks.
- Can be amplified by parallel repetition [KatzShin'06].
- Security Reduction loose:

  LPN ϵ-hard $\Rightarrow$ protocol $\sqrt{\epsilon}$-secure.
- 3-Rounds :(

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

1. Nicholas J. Hopper, Manuel Blum: Secure 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.

A New Protocol

$$\mathbf{s} \in \mathbb{Z}_2^k \quad 0 < \tau < 0.5$$

$\underline{\mathcal{P}(\mathbf{s},\tau)}$		$\underline{\mathcal{V}(\mathbf{s},\tau)}$
	$\xleftarrow{\mathbf{v}}$	$\mathbf{v} \leftarrow \{\mathbf{x} \in \mathbb{Z}_2^k : \lvert\mathbf{x}\rvert_1 = \frac{k}{2}\}$
$e \xleftarrow{\tau} \mathbb{Z}_2$ $\mathbf{b} \leftarrow \mathbb{Z}_2^k$		
$z := \langle \mathbf{b}, \mathbf{s} \wedge \mathbf{v} \rangle \oplus e$	$\xrightarrow{z,\mathbf{b}}$	verify:
		$\mathbf{b} \wedge \mathbf{v} \overset{?}{\neq} 0^k \qquad \langle \mathbf{b}, \mathbf{s} \wedge \mathbf{v} \rangle \overset{?}{=} z$

- Secure against active attacks.
- Can be amplified by parallel repetition.[1]
- Security Reduction tight:

  LPN ϵ-hard $\Rightarrow$ protocol $\epsilon - 2^{-\Theta(\#rep)}$-secure.
- round-optimal

[1] same $\mathbf{v}$, linearly independent $\mathbf{b}$'s.

Subspace LWE/LPN

an adaptive version LWE/LPN

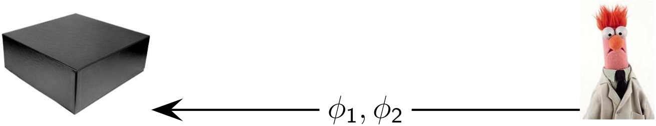
NGC 6543 by Hubble

Subspace Learning Parities with Noise

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

Subspace Learning Parities with Noise

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



$\phi_1, \phi_2 : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^m$ *affine & overlap in n-dim subspace.*

$$\phi_r(\mathbf{r}) \stackrel{\text{def}}{=} \mathbf{X}_r \cdot \mathbf{r} + \mathbf{x}_r \quad \phi_s(\mathbf{s}) \stackrel{\text{def}}{=} \mathbf{X}_s \cdot \mathbf{s} + \mathbf{x}_s \quad \text{rank}(\mathbf{X}_r^T \cdot \mathbf{X}_s) \geq n$$

Subspace Learning Parities with Noise

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

$\mathbf{r}, \langle \phi_1(\mathbf{r}), \phi_2(\mathbf{s}) \rangle + e$ →

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

$\phi_1, \phi_2 : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^m$ *affine & overlap in n-dim subspace.*

$$\phi_r(\mathbf{r}) \stackrel{\text{def}}{=} \mathbf{X}_r \cdot \mathbf{r} + \mathbf{x}_r \quad \phi_s(\mathbf{s}) \stackrel{\text{def}}{=} \mathbf{X}_s \cdot \mathbf{s} + \mathbf{x}_s \quad \mathrm{rank}(\mathbf{X}_r^T \cdot \mathbf{X}_s) \geq n$$

Subspace Learning Parities with Noise

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

$\longrightarrow \mathbf{r}, \langle \phi_1(\mathbf{r}), \phi_2(\mathbf{s}) \rangle + e \longrightarrow$

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

$\phi_1, \phi_2 : \mathbb{Z}_q^m \rightarrow \mathbb{Z}_q^m$ *affine & overlap in n-dim subspace.*

$$\phi_r(\mathbf{r}) \stackrel{\text{def}}{=} \mathbf{X}_r \cdot \mathbf{r} + \mathbf{x}_r \quad \phi_s(\mathbf{s}) \stackrel{\text{def}}{=} \mathbf{X}_s \cdot \mathbf{s} + \mathbf{x}_s \quad \text{rank}(\mathbf{X}_r^T \cdot \mathbf{X}_s) \geq n$$

Definition (Subspace Learning Parities with Noise)

(m, n, τ)-SLPN Problem: distinguish oracle from random.

Hardness of Subspace LPN

Claim (SLPN hard $\Rightarrow$ LPN hard (trivial))

- *if* (m, n, τ)*-SLPN is* ϵ *hard*
- *then* (n, τ)*-LPN is* ϵ *hard.*

Theorem (LPN hard $\Rightarrow$ SLPN hard)

- *if* (n, τ)*-LPN is* ϵ *hard*
- *then* $(m, n + d, \tau)$*-SLPN is* $\epsilon - 2^{-d} \cdot \#queries$ *hard*