1 HB

HB is an authentication protocols first introduced by Blum et al. [HB01], [BFKL94] that relies on the hardness of the learning parity with noise problem (LPN) for security and is provably secure against passive attacks. Figure 1 shows one iteration of the authentication of HB.

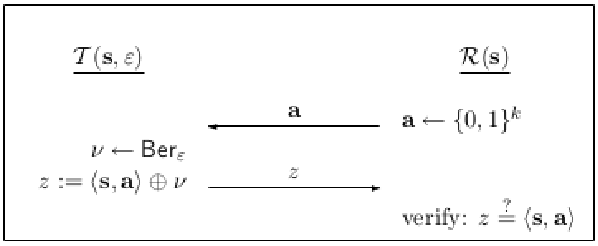

Figure 1: One iteration of the HB protocol

A tag $\mathcal{T}$ and a reader $\mathcal{R}$ share a random secret key $\boldsymbol{s} \in \{0,1\}^k$. One iteration (all of which happen in parallel) of the authentication step consists of the following: $\mathcal{R}$ sends a random challenge $\boldsymbol{a} \in \{0,1\}^k$ to $\mathcal{T}$ who in turn calculates $\boldsymbol{z} := \langle \boldsymbol{s}, \boldsymbol{a} \rangle \oplus v$ with $v \leftarrow \mathrm{Ber}_\varepsilon$. This result is sent back to $\mathcal{R}$ who then calculates if the iteration is *successful*, i.e. $\boldsymbol{z} = \langle \boldsymbol{s}, \boldsymbol{a} \rangle$. Notice that even iterations of an honest tag using the correct key s can be unsuccessful with probability ε. The reader therefore accepts the authentication of the tag if the number of unsuccessful iterations is at most $\approx \varepsilon \cdot n$.

2 HB+

A modification of the HB protocol in order for it to be secure against an active adversary is the HB+ protocol by Juels and Weis [JW05] shown in Figure 2.

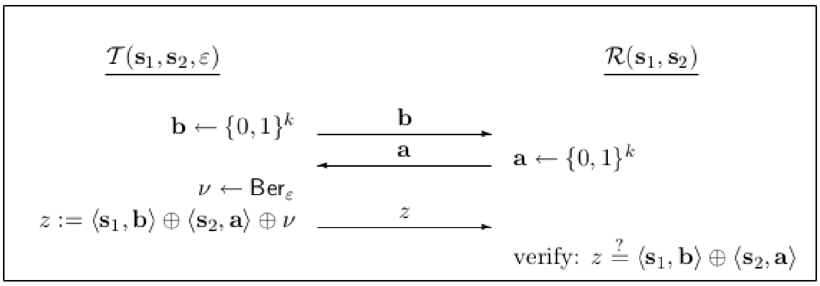

Figure 2: One iteration of the HB+ protocol

$\mathcal{R}$ and $\mathcal{T}$ now share two secret keys $\boldsymbol{s_1}, \boldsymbol{s_2} \in \{0,1\}^k$. One iteration of the authentication step now looks as follows: $\mathcal{T}$ first sends a random "blinding factor" $\boldsymbol{b} \in \{0,1\}^k$ to $\mathcal{R}$. The reader then, as for HB, sends a random challenge $\boldsymbol{a} \in \{0,1\}^k$ to $\mathcal{T}$ who in turn calculates $z := \langle \boldsymbol{s_1}, \boldsymbol{b} \rangle \oplus \langle \boldsymbol{s_2}, \boldsymbol{a} \rangle \oplus v$ with $v \leftarrow \mathrm{Ber}_\varepsilon$. This result is sent back to $\mathcal{R}$ who then calculates if the iteration is *successful*, i.e. $z = \langle \boldsymbol{s_1}, \boldsymbol{b} \rangle \oplus \langle \boldsymbol{s_2}, \boldsymbol{a} \rangle$. Again, even if $\mathcal{T}$ sends an honest z using the correct keys $\boldsymbol{s_1}$, s_2 the iteration can be *unsuccessful.* Therefore, up to $\approx e \cdot n$ *unsuccessful* iterations are allowed fot the tag to still be accepted.

3 AUTH, MAC1, MAC2

The AUTH protocol shown in Figure 3 was introduced by Kiltz et al. [KPV+17] and represents a two-round authentication protocol secure against active attacks and man-in-the-middle attacks, even in a quantum setting. The security of this protocol relies on the *subspace LPN problem* which is reducible to LPN.

Prover $\mathcal{P}_{\tau,n}(\mathbf{s} \in \mathbb{Z}_2^{2\ell})$		Verifier $\mathcal{V}_{\tau',n}(\mathbf{s} \in \mathbb{Z}_2^{2\ell})$
	$\xleftarrow{\mathbf{v}}$	$\mathbf{v} \xleftarrow{\$} \{\mathbf{x} \in \mathbb{Z}_2^{2\ell} : \mathbf{wt}(\mathbf{x}) = \ell\}$
if $\mathbf{wt}(\mathbf{v}) \neq \ell$ abort		
$\mathbf{R} \xleftarrow{\$} \mathbb{Z}_2^{\ell \times n}$; $\mathbf{e} \xleftarrow{\$} \mathsf{Ber}_\tau^n$		
$\mathbf{z} := \mathbf{R}^\mathsf{T} \cdot \mathbf{s}_{\downarrow \mathbf{v}} \oplus \mathbf{e} \in \mathbb{Z}_2^n$	$\xrightarrow{(\mathbf{R},\mathbf{z})}$	if rank$(\mathbf{R}) \neq n$ reject
		if $\mathbf{wt}(\mathbf{z} \oplus \mathbf{R}^\mathsf{T} \cdot \mathbf{s}_{\downarrow \mathbf{v}}) > n \cdot \tau'$ reject, else accept

Figure 3: Two-round authentication protocol AUTH

Whereas the random challenges $\boldsymbol{R} \in \mathbb{Z}_2^{l \times n}$ (each row of the matrix $\boldsymbol{R}^T$ corresponding to one challenge a in HB) were computed by the Verifier $\mathcal{V}$ in HB, they are now computed by the Prover $\mathcal{P}$. $\mathcal{V}$ instead sends a random vector $\boldsymbol{v} \in \mathbb{Z}_2^{2l}$ with Hamming weight $\mathrm{wt}(\boldsymbol{v}) = l$ to select l of the $2l$ key bits of s to produce a key subset $\boldsymbol{s}_{\downarrow v}$ which is derived from $\boldsymbol{s}$ by deleting all bits $\boldsymbol{s}[i]$ where $\boldsymbol{v}[i] = 0$. Then, $\boldsymbol{z} \in \mathbb{Z}_2^n$ is computed as $\boldsymbol{R}^T \cdot \boldsymbol{s}_{\downarrow v} \oplus \boldsymbol{e}$ and sent to $\mathcal{V}$ along with $\boldsymbol{R}$. $\mathcal{V}$ rejects the authentication if either $\mathrm{rank}(\boldsymbol{R}) \neq n$ or if the number of unsuccessful iterations denoted as $\mathrm{wt}(\boldsymbol{z} \oplus \boldsymbol{R}^T \cdot \boldsymbol{s}_{\downarrow v})$ is greater than the threshold $n \cdot \tau'$ with $\tau' = 0.25 + \tau/2$.

References

[BFKL94] Avrim Blum, Merrick Furst, Michael Kearns, and Richard J. Lipton. Cryptographic primitives based on hard learning problems. In Douglas R. Stinson, editor, *Advances in Cryptology — CRYPTO' 93*, pages 278–291, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[HB01] Nicholas J. Hopper and Manuel Blum. Secure human identification protocols. In Colin Boyd, editor, *Advances in Cryptology — ASIACRYPT 2001*, pages 52–66, Berlin, Heidelberg, 2001. Springer Berlin Heidelberg.

[JW05] Ari Juels and Stephen A Weis. Authenticating pervasive devices with human protocols. In *Annual international cryptology conference*, pages 293–308. Springer, 2005.

[KPV+17] Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi, David Cash, and Abhishek Jain. Efficient authentication from hard learning problems. *Journal of Cryptology*, 30(4):1238–1275, Oct 2017.