<https://eprint.iacr.org/2008/241.pdf>

HB and HB+ are a shared-key authentication protocol designed for low-cost devices such as RFID tags. It was proposed by Juels and Weis at Crypto 2005. The security of the protocol relies on the “learning parity with noise” (LPN) problem, which was proved to be NP-hard.

**1 Introduction**

The HB Scheme HB and HB+ schemes are based on the “learning parity with noise” (LPN) problem, which was proved to be NP-hard. HB/HB+ are designed to be reliable authentication protocols for low-cost devices with small computational power.

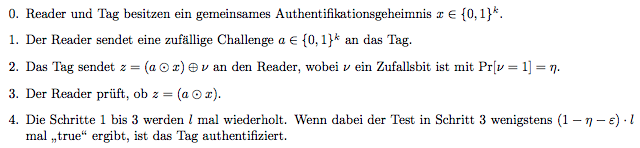
<https://crypto.iti.kit.edu/fileadmin/User/SicherheitSS12/Uebungsblatt_6_Lsg.pdf>

0. Reader und Tag besitzen ein gemeinsames Authentifikationsgeheimnis x ∈ {0, 1} k.

1. Der Reader sendet eine zufällige Challenge a ∈ {0, 1} k an das Tag.

2. Das Tag sendet z = (a x) ⊕ ν an den Reader, wobei ν ein Zufallsbit ist mit Pr[ν = 1] = η.

3. Der Reader pruft, ob ¨ z = (a x).

4. Die Schritte 1 bis 3 werden l mal wiederholt. Wenn dabei der Test in Schritt 3 wenigstens (1 − η − ε) mal „true“ ergibt, ist das Tag authentifiziert.

<https://link.springer.com/content/pdf/10.1007%2Fs00145-010-9061-2.pdf>

The HB protocol is proven secure against a passive (eavesdropping) adversary, while the HB+ protocol is proven secure against active attacks.

**HB**

Code Size

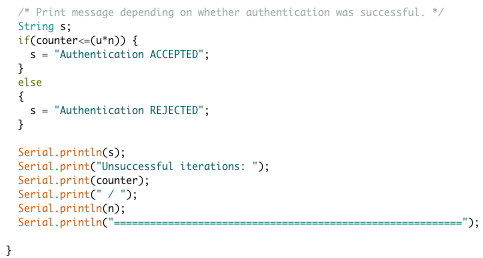
Der Sketch verwendet 4930 Bytes (15%) des Programmspeicherplatzes. Das Maximum sind 32256 Bytes.

Memory Size

Globale Variablen verwenden 482 Bytes (23%) des dynamischen Speichers, 1566 Bytes für lokale Variablen verbleiben. Das Maximum sind 2048 Bytes.

Complexity (rounds)

Power consumption



**HB+**

Code Size

Der Sketch verwendet 5400 Bytes (16%) des Programmspeicherplatzes. Das Maximum sind 32256 Bytes.

Memory Size

Globale Variablen verwenden 542 Bytes (26%) des dynamischen Speichers, 1506 Bytes für lokale Variablen verbleiben. Das Maximum sind 2048 Bytes.

Complexity

Power consumption

**AuthMac**

Code Size

Der Sketch verwendet 5864 Bytes (18%) des Programmspeicherplatzes. Das Maximum sind 32256 Bytes.

Memory Size

Globale Variablen verwenden 520 Bytes (25%) des dynamischen Speichers, 1528 Bytes für lokale Variablen verbleiben. Das Maximum sind 2048 Bytes.

Complexity

Power consumption

Clock Speed ​​und Clock Cycles. Je höher die Taktrate eines Tags ist, desto mehr Taktzyklen können durch den Verschlüsselungsauthentifizierungsprozess sicher verbraucht werden. Wie bereits im vorherigen Absatz erwähnt, schreiben Faktoren wie das Leistungsbudget eines passiv betriebenen RFID-Tags eine Obergrenze für seine Taktfrequenz vor. Viele Arbeiten betrachten 100 kHz als die vorherrschende Taktrate, die bei extrem eingeschränkten RFID-Tags durchführbar ist, z. B. [9, 32, 35]. Dieser Wert stimmt mit den Informationen überein, die wir von den Herstellern von RFID-Hardware erhalten haben, die Vertraulichkeit gefordert haben. Unter der Annahme einer oberen Grenze von 150 ms zum Ausführen einer vollständigen Authentifizierungsinstanz impliziert daher eine Taktgeschwindigkeit von 100 kHz sofort eine obere Grenze von 15.000 Taktzyklen auf der Seite des Tags, um sich erfolgreich zu authentifizieren. Beachten Sie jedoch, dass keines der Protokolle in Anhang B als undurchführbar erachtet wird. Ultra-Constrained-Geräte ausschließlich aufgrund ihrer Komplexität. Es ist jedoch anzumerken, dass viele von ihnen unsere obere Grenze von 15.000 Taktzyklen sogar um Größenordnungen (z. B. MAC1 und MAC2) überschreiten und daher auch für höhere Taktraten wie 1 MHz eindeutig nicht durchführbar wären.

Conversion base: 1 cps = 0.001 kHz

Conversion base: 1 kHz = 1000 cps