Numeriek toetsenbord afluisteren

Leerdoel: Inzicht in “Side channel attack”.
Zijkanaal informatie (side channel) is informatie die (onbedoeld) ontstaat door de werking van een apparaat.

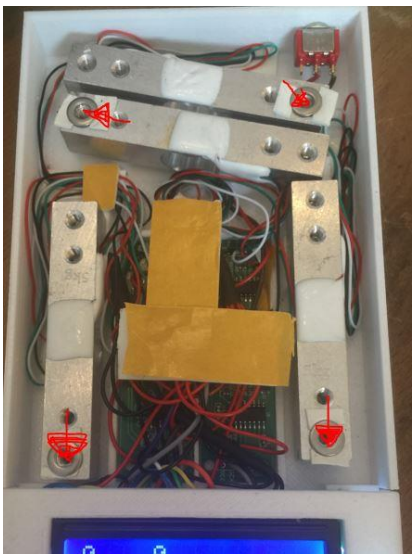
Benodigdheden:

- Arduino ontwikkelomgeving (pc met software)
- Afluister unit (zie figuur 1)
- Kopie van de sketch afluisterbasis
- Ervaring met Arduino

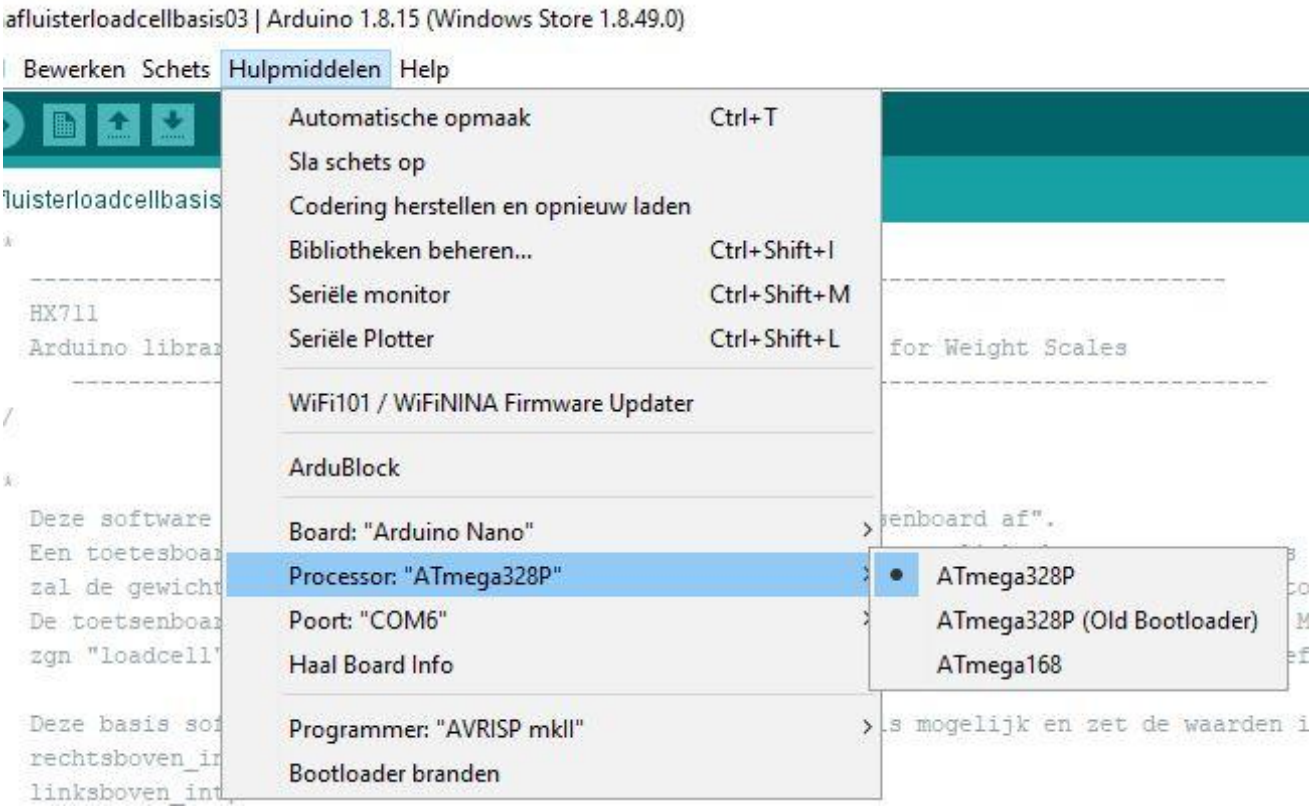
Het toetsenbord staat op vier pootjes. Als op een toets wordt gedrukt, zal op ieder pootje een druk worden uitgeoefend. Als we bv op de toets “000 “ drukken zal op de onderste pootjes meer druk worden uitgeoefend dan op de bovenste pootjes. Dit wordt “side channel information” genoemd. Door nu de verhouding van de vier drukken te berekenen, kunnen bepalen welke toets is ingedrukt.

Hieronder links zie de afluisterunit zonder toetsenbord en rechts zonder deksel. Met vier loadcells (de aluminium staafjes) worden de drukken gemeten die bij de rode pijlen wordt uitgeoefend.

Afluister unit figuur 1



In de afluister unit zit een computer board met de naam Arduino Nano. Je moet de Arduino ontwikkelomgeving instellen zoals op de figuur hieronder aangegeven.



In de sketch afluisterbasis is al veel voorbereid.
In de variabelen:

- rechtsboven_int;
- linksboven_int;
- rechtsonder_int;
- linksonder_int.

wordt continue bijgehouden welke druk door de vier toetsenbord pootjes wordt uitgeoefend. Op de LCD worden de vier drukken en de som weergegeven.

Aan jou nu de taak op de volgende werkzaamheden uit te voeren:

1. Uitzoeken wanneer er op een toets wordt gedrukt;
2. Hoe verhouden de drukken zich ;
3. Bepaal de toets.