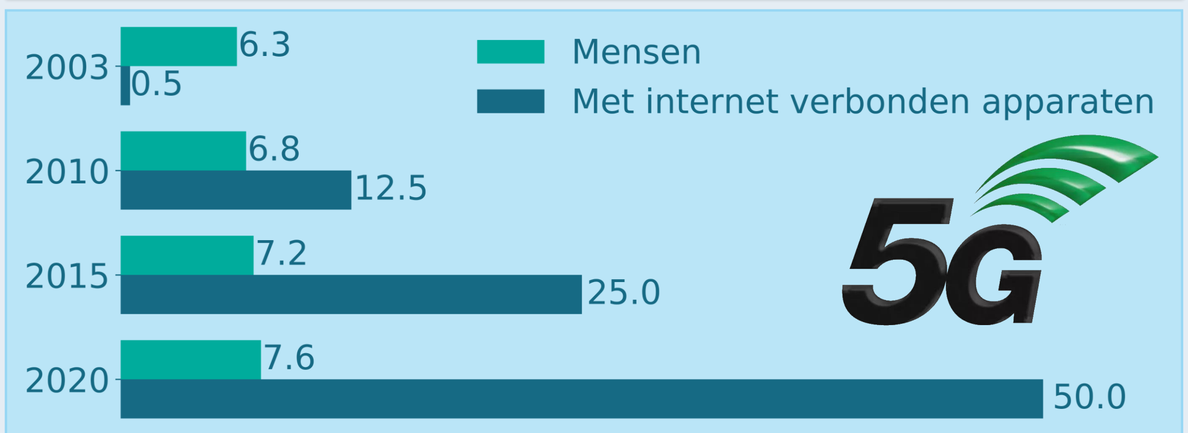
Departement Computerwetenschappen
Jurriaan Declerc, Rene Fekkes
Begeleiders: Prof. D. Hughes, H. Janjua, M. Ammar

Proof-Carrying Communication for the Internet of Things

1. Motivatie

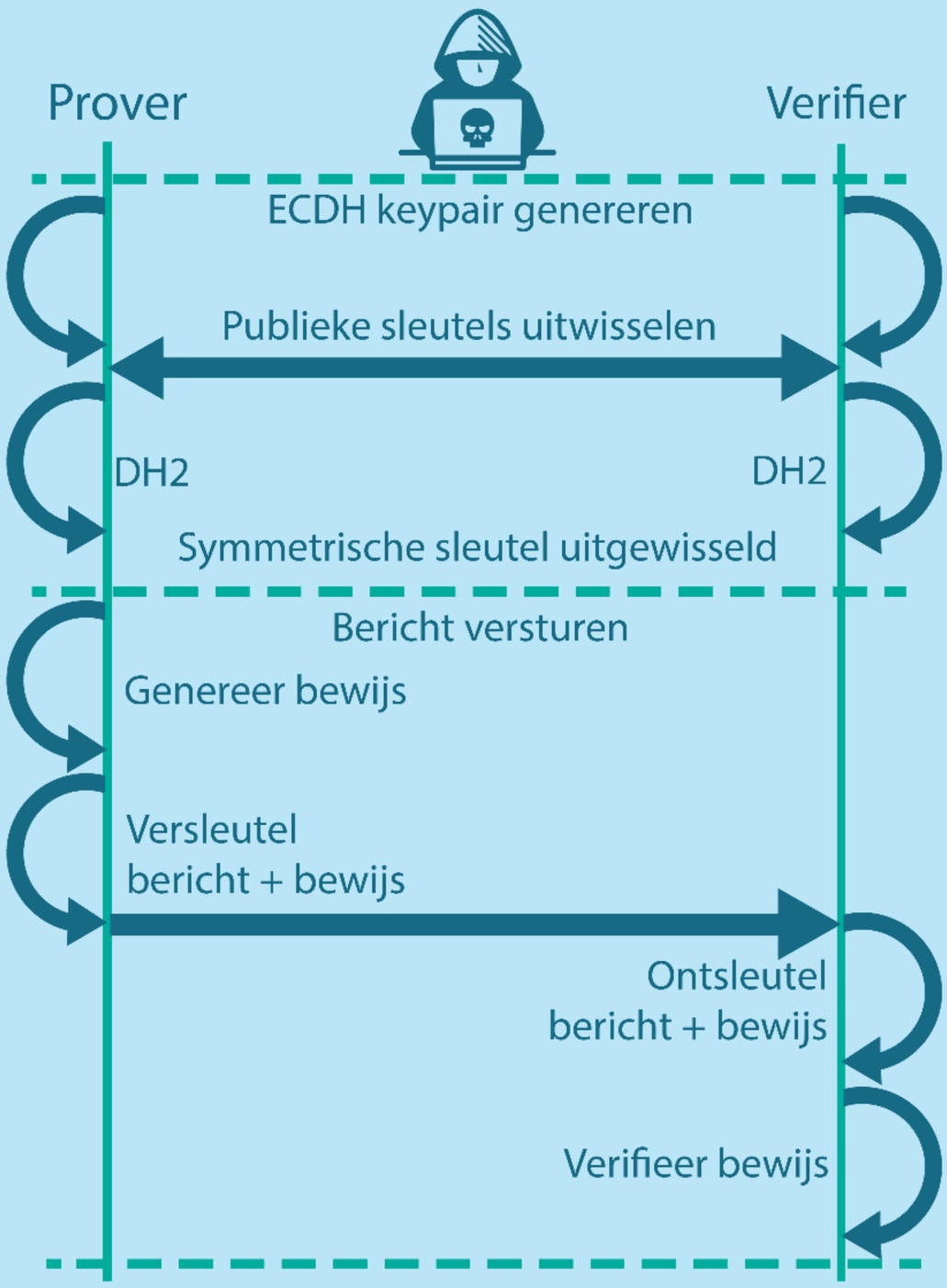


Aantal in miljard[1]

2. Probleem

- In de context van IoT is het cruciaal om de geldigheid van ontvangen berichten na te kunnen gaan.
- Bestaande oplossingen verifiëren de integriteit van IoT apparaten periodiek om voordien verzonden berichten te valideren.

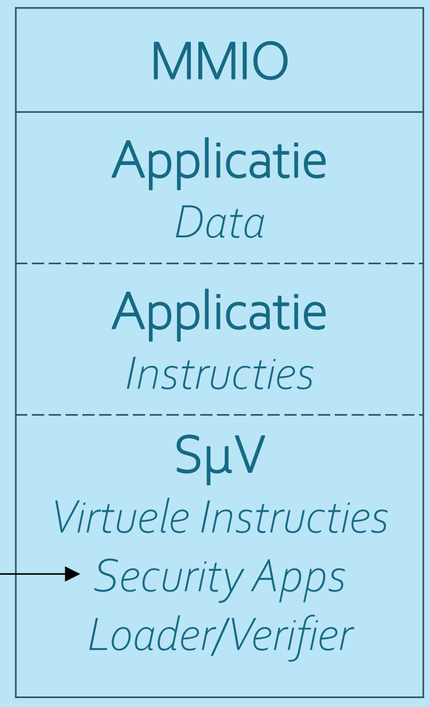
3. Aanpak



4. Trusted Computing

- Bescherming van data & uitvoeringsomgeving
- Speciale hardware, software of hybride
- De Security MicroVisor[2] zorgt voor een TC omgeving zonder speciale hardware

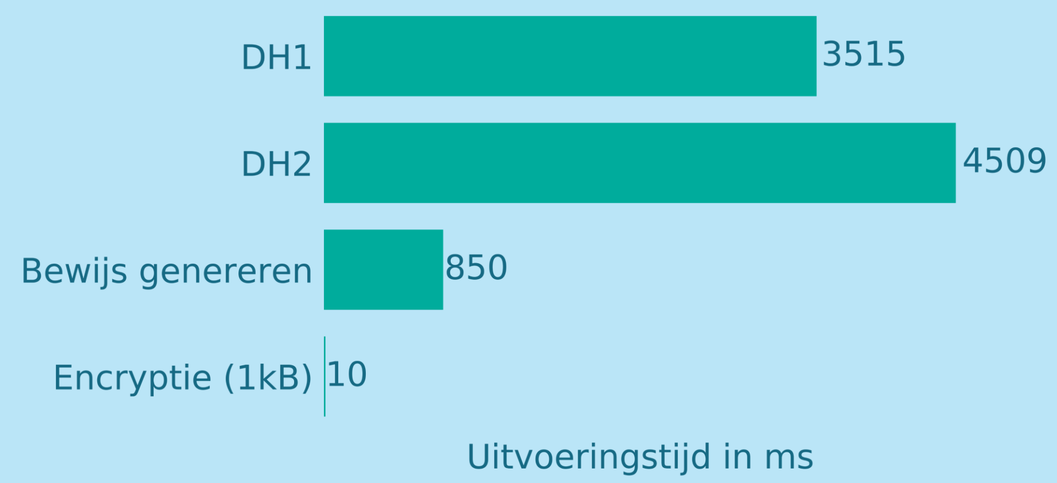
Proof-carrying messages →



5. Highlights

- **Bewijs integriteit van verzender** met een hash van het instructiegeheugen
- **Implementatie op Arduino Uno WiFi Rev2**
- **Symmetrische sleuteluitwisseling** met Elliptic Curve Diffie-Hellman

6. Resultaten en Conclusies



- ❑ Aanzienlijke kost om sessie op te starten
- ❑ Een bewijs in ieder bericht verwerken is enkel praktisch voor netwerken met lage doorvoer

7. Verder Werk

- Integratie met de Security MicroVisor
- Onderzoek het gebruik van policies voor het genereren van een bewijs.

[1] D. Evans, The Internet of Things: How the Next Evolution of the Internet Is Changing Everything
[2] Wilfried Daniels, Danny Hughes, Mahmoud Ammar, Bruno Crispo, Nel-son Matthys, en Wouter Joosen. 2017. SμV - the Security Microvisor: A Virtualisation-based Security Middleware for the Internet of Things