KU LEUVEN

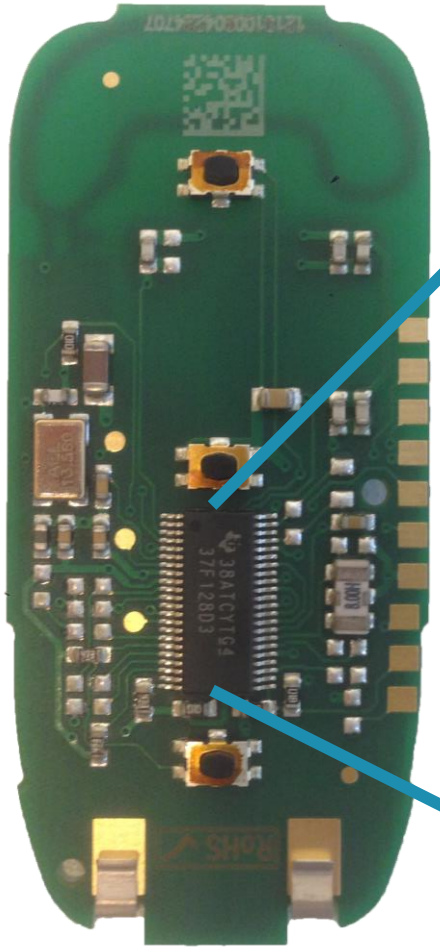
Fast, Furious and Insecure

Lennert Wouters, Eduard Marin, Tomer Ashur, Benedikt Gierlichs and Bart Preneel

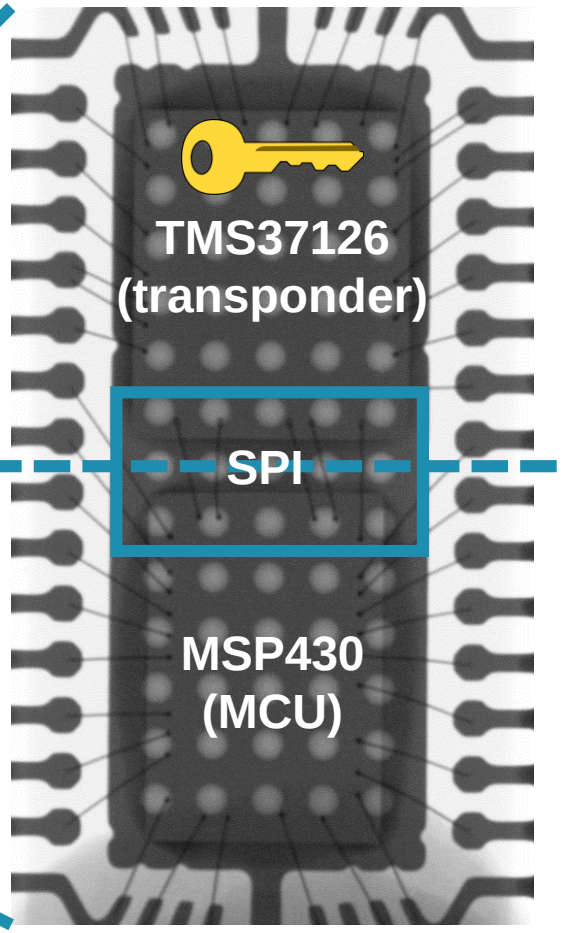
COSIC

an imec research group at KU Leuven

The Tesla Model S key fob



TI TMS37F128



X-ray picture

No firmware readout protection

Findings

- 40-bit key DST40 cipher [1]
  - 40-bit challenge and 24-bit response

[1] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin and Michael Szydlo
In Proceedings of the USENIX Security Symposium (2005), vol. 31, pp. 1–16.

Findings

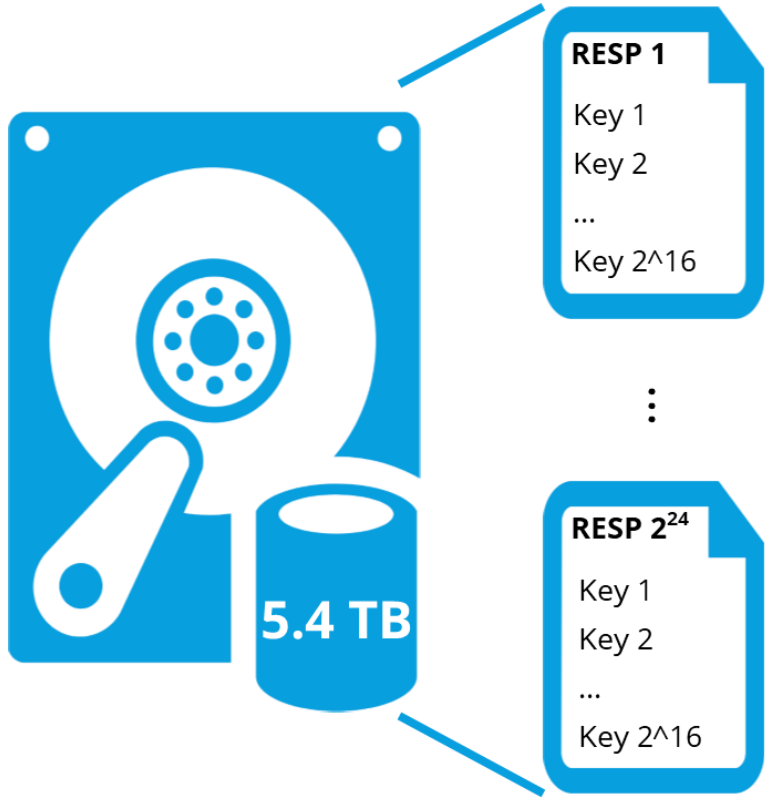
- 40-bit key DST40 cipher [1]
  - 40-bit challenge and 24-bit response
- No mutual authentication

[1] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin and Michael Szydlo
In Proceedings of the USENIX Security Symposium (2005), vol. 31, pp. 1–16.

Findings

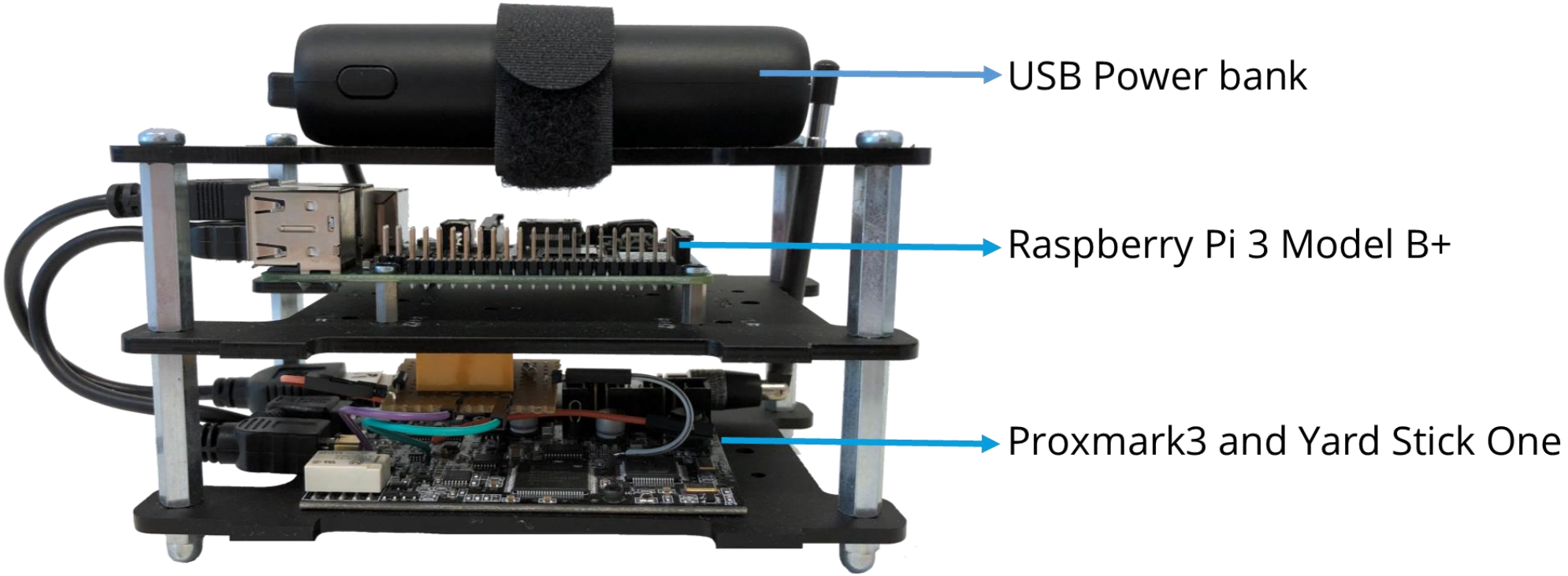
- 40-bit key DST40 cipher [1]
  - 40-bit challenge and 24-bit response
- No mutual authentication

- Time-Memory Trade-Off Table
  - Key recovery in ~2s on a Raspberry Pi



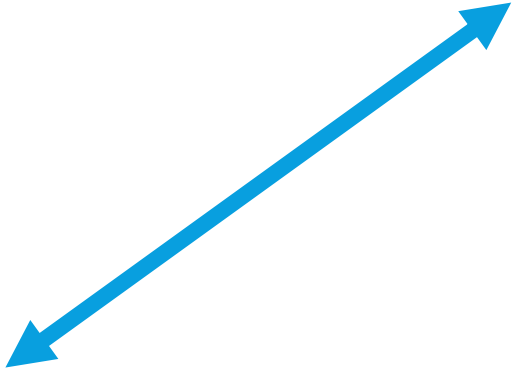
[1] Steve Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin and Michael Szydlo
In Proceedings of the USENIX Security Symposium (2005), vol. 31, pp. 1–16.

Proof of Concept attack

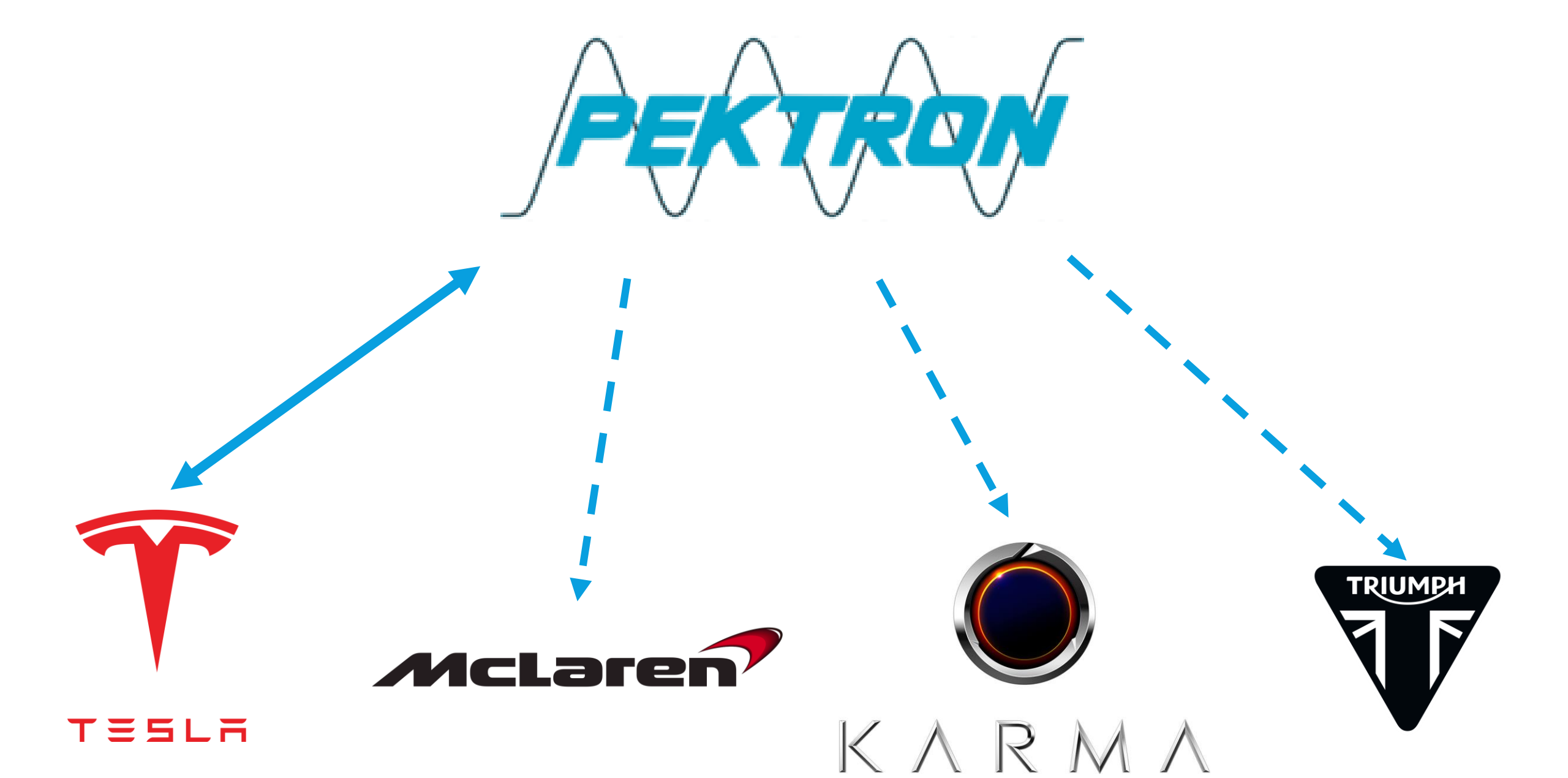



TESLA

PEKTRON



TESLA


PEKTRON
TESLA
McLaren
KARMA
TRIUMPH

Responsible disclosure

- First notified Tesla on 31/08/2017

Responsible disclosure

- First notified Tesla on 31/08/2017
- Tesla vehicles produced from June onwards use a new key fob

Responsible disclosure

- First notified Tesla on 31/08/2017
- Tesla vehicles produced from June onwards use a new key fob
- OTA update includes a Pin to Drive feature and the ability to disable PKE

Responsible disclosure

- First notified Tesla on 31/08/2017
- Tesla vehicles produced from June onwards use a new key fob
- OTA update includes a Pin to Drive feature and the ability to disable PKE

More information

- esat.kuleuven.be/cosic/cosic-cryptography-blog/
- Poster sessions
- @CosicBe or @LennertWo
- WIRED article
- Live demo?!