Karlsruhe Institute of Technology

The Landscape of Security from Physical Assumptions

IEEE Information Theory Workshop (ITW) 2021 | Invited Session

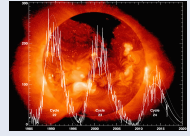
Alexander Koch | 20. October 2021

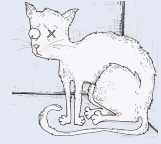
Overview: Physical Assumptions in Cryptography

Idealized Hardware

Physical Objects

Physical Processes





Main advantages:

- Transparency and ease of understanding for the user
- Strong, otherwise unachievable, security guarantees

German Voting Machine Judgement

German Constitutional Court:
“When electronic voting machines are deployed, it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge.” (Judgment of the Second Senate of 03 March 2009)

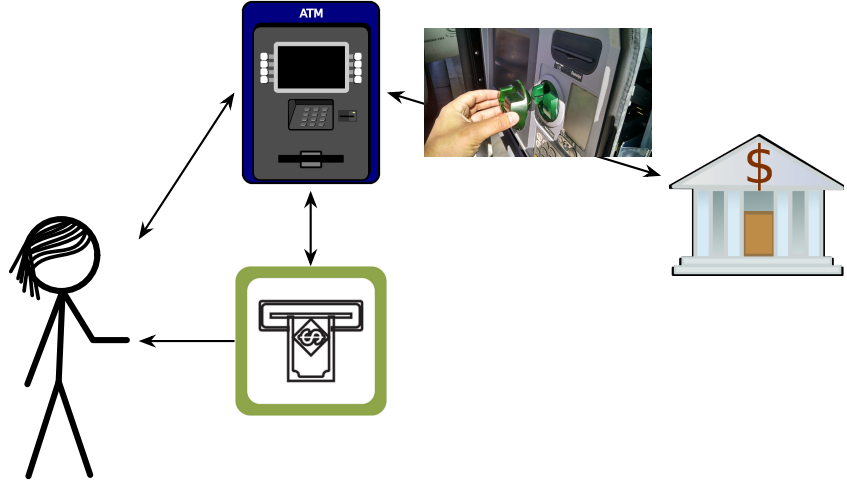
This sets a very high bar to transparency for voting machines in Germany!

Secure Multiparty Computation from Idealized Hardware

1. Physically Unclonable Functions (PUFs)
2. Signature Cards
3. Tamper-Proof Hardware Tokens
4. Trusted Hardware with Constrained Functionality
5. Secure Processors

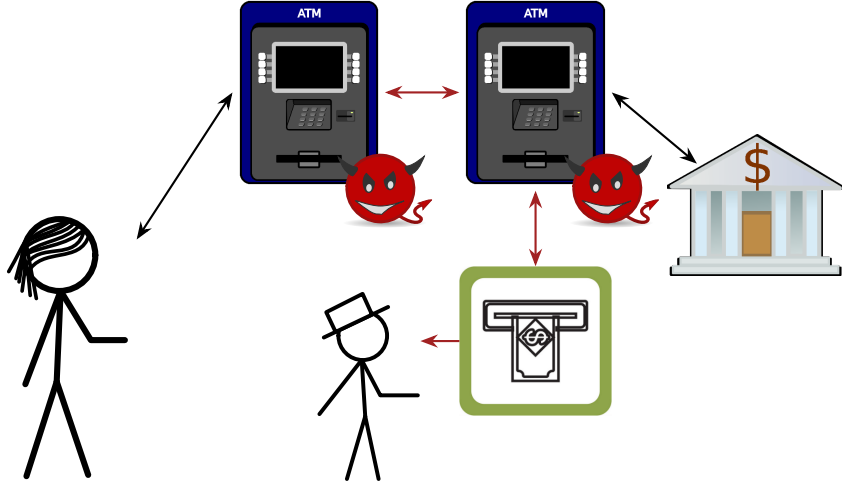
PUF schema (1st row) from (Pappu et al. 2002), TAN generator copyrighted; others CC0

Secure Money Withdrawal



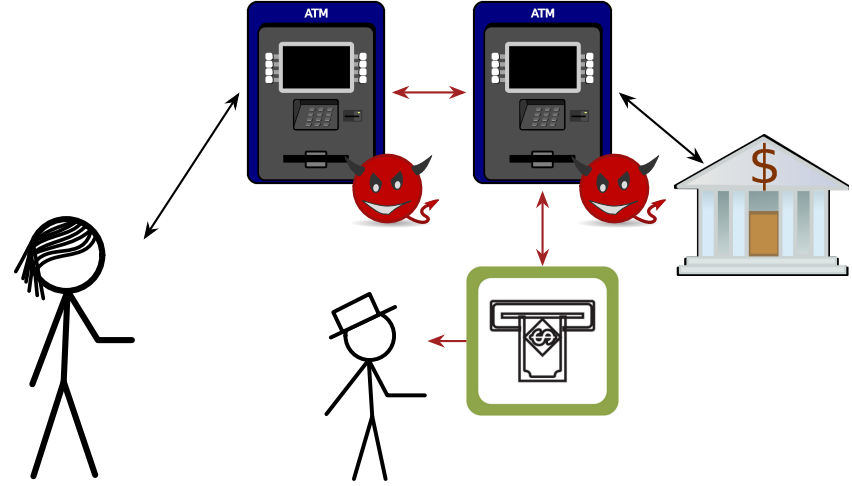
Achenbach et al. (2019)

Secure Money Withdrawal



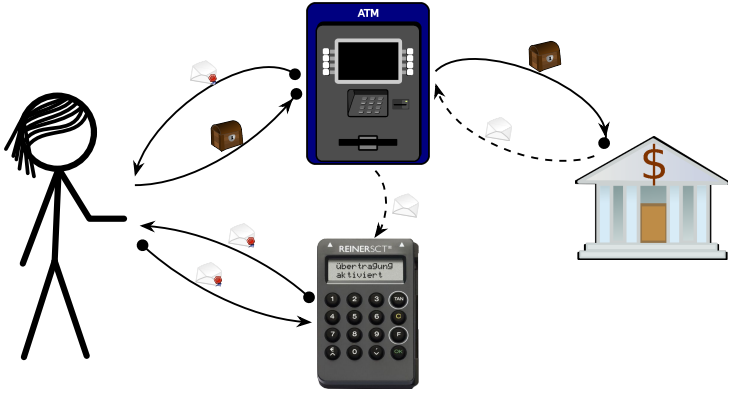
Achenbach et al. (2019)

Secure Money Withdrawal: A potential attack



Achenbach et al. (2019)

Human Authentication via a Corrupted Platform



Authentication Model: Basin, Radomirovic, and Schläpfer (2015), Variant: Achenbach et al. (2019)

Using Simple Idealized Hardware for Fortified Security

Typical Adaptive Corruptions

Usually, an attacker that corrupts adaptively, learns all inputs and outputs of that party

However, there is a difference in attacks (physical vs. remote):

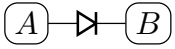
Stronger and More Refined Corruption Model

Aim: Upon remote attacks (only when online), an attacker (usually) cannot learn inputs/outputs

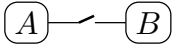
Broadnax et al. (2021)

Using Simple Idealized Hardware for Fortified Security II

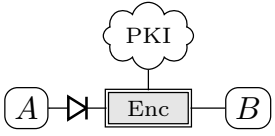
Data Diode

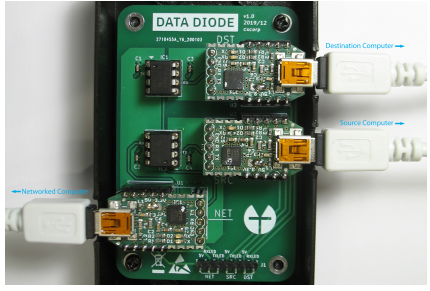


Air-Gap Switch



Encryption unit

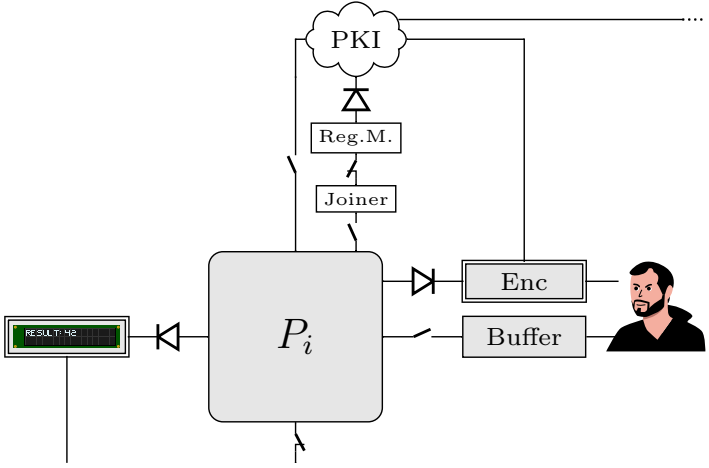




Broadnax et al. (2021)

Data diode image by Markus Ottela, cf. https://github.com/maqp/tfc

Fortified MPC Architecture



Secure Multiparty Computation from Physical Objects

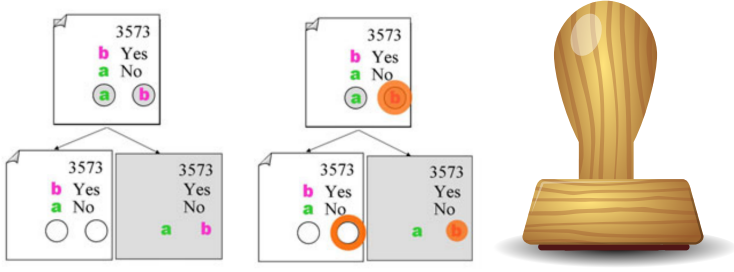
1. Physical Envelopes and Ballots (Tamper-Evident Seals)
   cf. Moran and Naor (2010)
2. Playing Cards
3. Other Objects (cups, PEZ dispenser, dial locks, etc.)



“Miscellaneous Playing Cards” (excerpt) by Philippa Willitts CC BY-NC 2.0; Scratch-off cards copyrighted

Cryptographic Voting (PunchScan)

Reconciling Receipt-Freeness with Verifiablity using Physical Assumptions



Sheets from PunchScan (Popoveniuc and Hosp 2010)

Conclusion

Physical assumptions ...

- feature already a wealth of nice, simple protocols
- allow for stronger, information-theoretic security assumptions
- often feature a higher level of transparency
- may close the gap between human user and untrusted machine
- serve as a bridge to reality (guarantee that inputs correspond to something real)
- may be fun to work with (as in the case of cards)

For a more extensive (survey-like) overview of all domains, please take a look at the accompanying paper

References I


Dirk Achenbach et al. “Your Money or Your Life—Modeling and Analyzing the Security of Electronic Payment in the UC Framework”. In: Sept. 30, 2019, pp. 243–261. DOI: 10.1007/978-3-030-32101-7_16.


David A. Basin, Sasa Radomirovic, and Michael Schläpfer. “A Complete Characterization of Secure Human-Server Communication”. In: *IEEE 28th Computer Security Foundations Symposium, CSF 2015*. Ed. by Cédric Fournet, Michael W. Hicks, and Luca Viganò. IEEE Computer Society, 2015, pp. 199–213. ISBN: 978-1-4673-7538-2. DOI: 10.1109/CSF.2015.21.


Bert den Boer. “More Efficient Match-Making and Satisfiability: The Five Card Trick”. In: *EUROCRYPT 1989*. Ed. by Jean-Jacques Quisquater and Joos Vandewalle. Vol. 434. LNCS. Springer, 1989, pp. 208–217. ISBN: 3-540-53433-4. DOI: 10.1007/3-540-46885-4_23.


Brandon Broadnax et al. “Fortified Multi-Party Computation: Taking Advantage of Simple Secure Hardware Modules”. In: *Proceedings on Privacy Enhancing Technologies* (4 2021), pp. 312–338. DOI: 10.2478/popets-2021-0072.

References II


Tal Moran and Moni Naor. “Basing cryptographic protocols on tamper-evident seals”. In: *Theor. Comput. Sci.* 411.10 (2010). Ed. by M. Yung, pp. 1283–1310. DOI: 10.1016/j.tcs.2009.10.023.


Ravikanth Pappu et al. “Physical One-Way Functions”. In: *Science* 297.5589 (2002), pp. 2026–2030. DOI: 10.1126/science.1074376.


Stefan Popoveniuc and Benjamin Hosp. “An Introduction to PunchScan”. In: *Towards Trustworthy Elections, New Directions in Electronic Voting*. Ed. by David Chaum et al. Vol. 6000. LNCS. Springer, 2010, pp. 242–259. DOI: 10.1007/978-3-642-12980-3_15.


Tom Verhoeff. *The Zero-Knowledge Match Maker*. June 18, 2014. URL: https://www.win.tue.nl/~wstomv/publications/liber-AMiCorum-arjeh-bijdrage-van-tom-verhoeff.pdf (visited on 08/23/2019).