PUFs, Protection, Privacy, PRNGs

an overview of physically unclonable functions

Pol Van Aubel
33rd Chaos Communication Congress, Hamburg, Germany

iCIS | Digital Security
Radboud University

Presenting

Pol Van Aubel
radboud@polvanaubel.com

Radboud University
iCIS|Digital Security

This lecture features work from many authors, a list of citations is provided on the final slides.

Outline

Outline

Unique identification and authentication of integrated circuits

Unique identification and authentication of integrated circuits

- distinguish chips

Unique identification and authentication of integrated circuits

- distinguish chips
- uniquely

Unique identification and authentication of integrated circuits

- distinguish chips
- uniquely
- from the same mask

Unique identification and authentication of integrated circuits

- distinguish chips
- uniquely
- from the same mask
- with high accuracy

Unique identification and authentication of integrated circuits

- distinguish chips
- uniquely
- from the same mask
- with high accuracy
- unforgably

Outline

Counterfeiting

Counterfeiting

- Money

Counterfeiting

- Money
- Magstripe cards

Counterfeiting

- Money
- Magstripe cards
- Identity documents

Counterfeiting

- Money
- Magstripe cards
- Identity documents
- Nuke Counters

Counterfeiting

- Money
- Magstripe cards
- Identity documents
- "Treaty Limited Item" identifiers

Money

Money

- Highly intricate imagery

Money

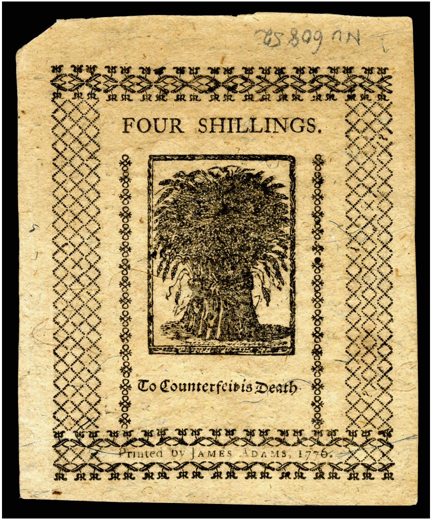
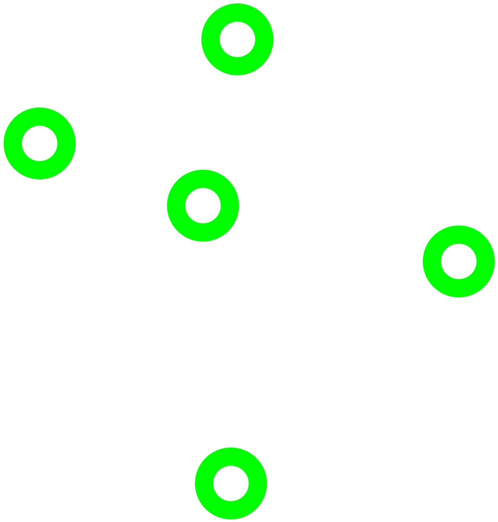


Image from the National Numismatic Collection at the Smithsonian Institution, U.S.A.

Money



Money

- Highly intricate imagery
- Photocopiers and the EURion constellation[1]

[1] M. Kuhn, *The eurion constellation*, Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/eurion.pdf.

Money

- Highly intricate imagery
- Photocopiers and the EURion constellation[1]
- Common theme: same mark for valid bills

[1] M. Kuhn, *The eurion constellation*, Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/eurion.pdf.

Money

- Highly intricate imagery
- Photocopiers and the EURion constellation[1]
- Common theme: same mark for valid bills
- Alternative: different marks for valid bills and *sign the marking*

[1] M. Kuhn, *The eurion constellation*, Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/eurion.pdf.

Money

- Highly intricate imagery
- Photocopiers and the EURion constellation[1]
- Common theme: same mark for valid bills
- Alternative: different marks for valid bills and *sign the marking*
- Sprinkle random-length optical fibres into the paper pulp, sign the dot pattern caused by a lightbar scan[2,3]

---

[1] M. Kuhn, *The eurion constellation*, Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/eurion.pdf.

[2] D. W. Bauder, "An anti-counterfeiting concept for currency systems", *Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990*, 1983.

[3] G. J. Simmons, "Identification of data, devices, documents and individuals", in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

Cards

Cards

- Magnetic stripes + PIN

Cards

- Magnetic stripes + PIN
- Surely nobody knows how to copy... oh.

Cards

- Magnetic stripes + PIN
- Surely nobody knows how to copy... oh.
- Holograms?

Cards

- Magnetic stripes + PIN
- Surely nobody knows how to copy... oh.
- Holograms?
- Randomly disperse magnetic fibers, scan them, turn into pulses, AND the pulses with clock. . . [4]

[4] J. Brosow and E. Furugard, *Method and a system for verifying authenticity safe against forgery*, US Patent 4,218,674, Aug. 1980. [Online]. Available: https://www.google.com/patents/US4218674.

Cards

- Magnetic stripes + PIN
- Surely nobody knows how to copy... oh.
- Holograms?
- Randomly disperse magnetic fibers, scan them, turn into pulses, AND the pulses with clock... [4]
- Randomly disperse conductive particles in insulating material, scan with a microwave.[5]

---

[4] J. Brosow and E. Furugard, *Method and a system for verifying authenticity safe against forgery*, US Patent 4,218,674, Aug. 1980. [Online]. Available: https://www.google.com/patents/US4218674.

[5] J. Samyn, *Method and apparatus for checking the authenticity of documents*, US Patent 4,820,912, Apr. 1989. [Online]. Available: https://www.google.com/patents/US4820912.

(Identity) documents

(Identity) documents

- Translucency[6]

[6] R. Goldman, *Verification system for document substance and content*, US Patent 4,689,477, Aug. 1987. [Online]. Available: https://www.google.com/patents/US4689477.

(Identity) documents

- Translucency[6]
- Exact 3-dimensional cotton fibre pattern[7]

[6] R. Goldman, *Verification system for document substance and content*, US Patent 4,689,477, Aug. 1987. [Online]. Available: https://www.google.com/patents/US4689477.

[7] G. J. Simmons, "Identification of data, devices, documents and individuals", in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

(Identity) documents

- Translucency[6]
- Exact 3-dimensional cotton fibre pattern[7]
- Texture hash of postal envelope[8]

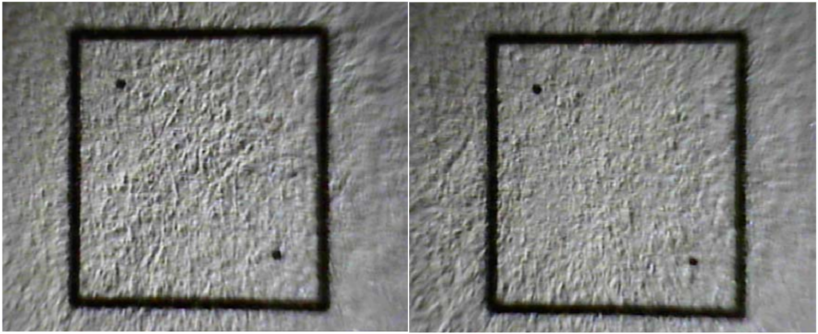
---

[6] R. Goldman, *Verification system for document substance and content*, US Patent 4,689,477, Aug. 1987. [Online]. Available: https://www.google.com/patents/US4689477.

[7] G. J. Simmons, "Identification of data, devices, documents and individuals", in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

[8] J. R. Smith and A. V. Sutherland, "Microstructure based indicia", in *Proceedings of the Second Workshop on Automatic Identification Advanced Technologies*, 1999, pp. 79–83.

Paper texture hash



Treaty Limited Items

Treaty Limited Items

- Reflective Particle Tags[9]

[9] G. J. Simmons, "Identification of data, devices, documents and individuals", in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

Treaty Limited Items

- Reflective Particle Tags[9] (for if you ever have a bunch of nukes to count)

[9] G. J. Simmons, “Identification of data, devices, documents and individuals”, in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

The common theme

The common theme

1. Intrinsic aspect

The common theme

1. Intrinsic aspect
2. Infeasible to copy

The common theme

1. Intrinsic aspect
2. Infeasible to copy
3. Easily readable

The common theme

1. Intrinsic aspect
2. Infeasible to copy
3. Easily readable
4. Unpredictable

The common theme

1. Intrinsic aspect
2. Infeasible to copy
3. Easily readable
4. Unpredictable
5. Unchanging

Outline

Physical One-Way Functions

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser
- Captured 320x240 pixel speckle pattern

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser
- Captured 320x240 pixel speckle pattern
- Turned into 2400-bit key with Gabor transform

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser
- Captured 320x240 pixel speckle pattern
- Turned into 2400-bit key with Gabor transform
- Drilling a hole causes half the bits to flip →tamper-resistant

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser
- Captured 320x240 pixel speckle pattern
- Turned into 2400-bit key with Gabor transform
- Drilling a hole causes half the bits to flip →tamper-resistant
- Reading structure? Feasible. Submicron reproduction? Not so much.

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Physical One-Way Functions

- Epoxy with miniscule glass spheres[10]
- Illuminated by laser
- Captured 320x240 pixel speckle pattern
- Turned into 2400-bit key with Gabor transform
- Drilling a hole causes half the bits to flip →tamper-resistant
- Reading structure? Feasible. Submicron reproduction? Not so much.
- Emulation requires storage: huge challenge/response space

[10] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Protocol

1. Read on trusted terminal

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal
4. Send challenge to terminal

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal
4. Send challenge to terminal
5. Receive response-key

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal
4. Send challenge to terminal
5. Receive response-key
6. Reject if key differs too much (941 bits)

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal
4. Send challenge to terminal
5. Receive response-key
6. Reject if key differs too much (941 bits)
7. Repeat steps 4–6 a few times

Protocol

1. Read on trusted terminal
2. Collect random challenge/response pairs
3. Authentication request from untrusted terminal
4. Send challenge to terminal
5. Receive response-key
6. Reject if key differs too much (941 bits)
7. Repeat steps 4–6 a few times
8. Goto 1

Physical One-Way Functions

Physical One-Way Functions

- Connection with cryptography

Physical One-Way Functions

- Connection with cryptography
- Defined protocol

Physical One-Way Functions

- Connection with cryptography
- Defined protocol
- “Special” equipment required

Physical One-Way Functions

- Connection with cryptography
- Defined protocol
- “Special” equipment required
- Same possibility in silicon?

Physical One-Way Functions

- Connection with cryptography
- Defined protocol
- "Special" equipment required
- Same possibility in silicon?
- "it may become possible to employ a similar mesoscopic approach in an electronic system by using the scattering of electrons from atomic-scale inhomogeneities within their coherence length."[11]

[11] R. Pappu, B. Recht, J. Taylor *et al.*, "Physical one-way functions", *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

Outline

The old days

The old days

"In the fuel rod placement monitor ... high radiation levels in the "hot" cell provided the general tamper resistance ..."[12]

[12] D. W. Bauder, "An anti-counterfeiting concept for currency systems", *Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990*, 1983.

The old days

"In the fuel rod placement monitor . . . high radiation levels in the "hot" cell provided the general tamper resistance . . . "[12]

"The seismic sensors . . . would detect any attempt to gain physical access to the package long before the information security is in jeopardy."

[12] D. W. Bauder, "An anti-counterfeiting concept for currency systems", *Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990*, 1983.

RSA in 1984

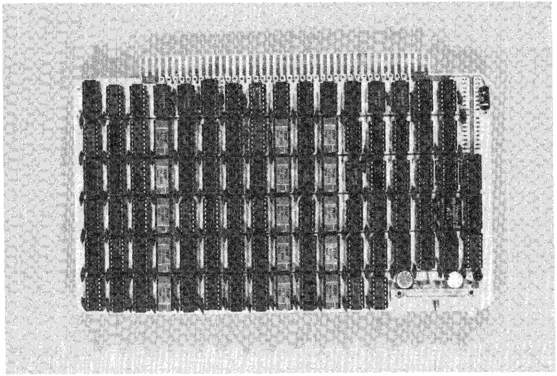


Figure 7. RSA Cryptoboard for PPIV.

The bottom line to this discussion is that equipment exists to measure various individual attributes to implement the identification technique described before. The first reduction to practice by the Sandia National Laboratories in the PPIV, using hand geometry measurements, illustrates the general principle.

Other solutions

Other solutions

- Hardware security modules (HSM)

Other solutions

- Hardware security modules (HSM)
- Smart Cards

Other solutions

- Hardware security modules (HSM)
- Smart Cards
- Trusted Platform Modules

Aspects

Aspects

- Key never leaves the device

Aspects

- Key never leaves the device
- How does the key enter the device?

Aspects

- Key never leaves the device
- How does the key enter the device?
- What can the key do?

Aspects

- Key never leaves the device
- How does the key enter the device?
- What can the key do?
- Possible to emulate once you have the key?

Outline

The case for PUFs

The case for PUFs

- Tamper-resistance: expensive and difficult

The case for PUFs

- Tamper-resistance: expensive and difficult
- Process Variations across "identical" Integrated Circuits[13]

[13] K. Lofstrom, W. R. Daasch and D. Taylor, "Ic identification circuit using device mismatch", in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No.00CH37056)*, 2000, pp. 372–373. DOI: 10.1109/ISSCC.2000.839821.

The case for PUFs

- Tamper-resistance: expensive and difficult
- Process Variations across “identical” Integrated Circuits[13]
- Use for secure device identification / authentication[14]

---

[13] K. Lofstrom, W. R. Daasch and D. Taylor, “Ic identification circuit using device mismatch”, in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No.00CH37056)*, 2000, pp. 372–373. DOI: 10.1109/ISSCC.2000.839821.

[14] B. Gassend, D. Clarke, M. van Dijk *et al.*, “Silicon physical random functions”, in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02, Washington, DC, USA: ACM, 2002, pp. 148–160, ISBN: 1-58113-612-9. DOI: 10.1145/586110.586132. [Online]. Available: http://doi.acm.org/10.1145/586110.586132.

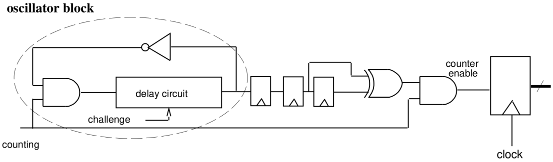


Figure 1: Self-Oscillating Loop Circuit.

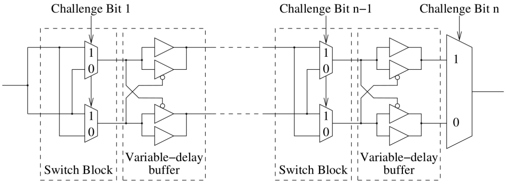


Figure 2: Non-Monotonic Delay Circuit. [15]

[15] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Silicon physical random functions", in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02, Washington, DC, USA: ACM, 2002, pp. 148–160, ISBN: 1-58113-612-9. DOI: 10.1145/586110.586132. [Online]. Available: http://doi.acm.org/10.1145/586110.586132.

Attacks

Attacks

- Duplication

Attacks

- Duplication
- Emulation from measuring

Attacks

- Duplication
- Emulation from measuring
- Emulation from modelling

Attacks

- Duplication
- Emulation from measuring
- Emulation from modelling
- Control algorithm attack

Controlled Physically Unclonable Functions

Controlled Physically Unclonable Functions

- As before, with bells on![16]

[16] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

Controlled Physically Unclonable Functions

- As before, with bells on![16]
- Access function for the PUF as part of the PUF

[16] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

Controlled Physically Unclonable Functions

- As before, with bells on![16]
- Access function for the PUF as part of the PUF
- Proof of execution on specific device

[16] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

Controlled Physically Unclonable Functions

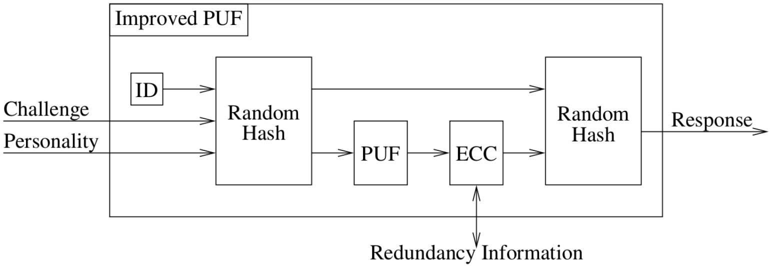
- As before, with bells on![16]
- Access function for the PUF as part of the PUF
- Proof of execution on specific device
- Code that only runs on specific device

[16] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

Controlled Physically Unclonable Functions

- As before, with bells on![16]
- Access function for the PUF as part of the PUF
- Proof of execution on specific device
- Code that only runs on specific device
- Whatever you need a secure cryptographic key for...

[16] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.



[17]

[17] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Controlled physical random functions", in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

Formal model

Formal model

- Robustness[18]

[18] F. Armknecht, R. Maes, A. R. Sadeghi *et al.*, "A formalization of the security features of physical functions", in *2011 IEEE Symposium on Security and Privacy*, 2011, pp. 397–412. DOI: 10.1109/SP.2011.10.

Formal model

- Robustness[18]
- Physical unclonability

[18] F. Armknecht, R. Maes, A. R. Sadeghi *et al.*, "A formalization of the security features of physical functions", in *2011 IEEE Symposium on Security and Privacy*, 2011, pp. 397–412. DOI: 10.1109/SP.2011.10.

Formal model

- Robustness[18]
- Physical unclonability
- Unpredictability

[18] F. Armknecht, R. Maes, A. R. Sadeghi *et al.*, "A formalization of the security features of physical functions", in *2011 IEEE Symposium on Security and Privacy*, 2011, pp. 397–412. DOI: 10.1109/SP.2011.10.

Proposals (& attacks!)

Proposals (& attacks!)

- Arbiter PUFs[19]

[19] J. W. Lee, D. Lim, B. Gassend *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication applications", in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, 2004, pp. 176–179. DOI: 10.1109/VLSIC.2004.1346548.

Proposals (& attacks!)

- Arbiter PUFs[19]
- . . . with modelling attacks[20,21,22]

---

[19] J. W. Lee, D. Lim, B. Gassend *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication applications", in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, 2004, pp. 176–179. DOI: 10.1109/VLSIC.2004.1346548.

[20] U. Rührmair, J. Sölter and F. Sehnke, "On the foundations of physical unclonable functions.", *IACR Cryptology ePrint Archive*, vol. 2009, p. 277, 2009.

[21] M. Majzoobi, F. Koushanfar and M. Potkonjak, "Testing techniques for hardware security", in *2008 IEEE International Test Conference*, 2008, pp. 1–10. DOI: 10.1109/TEST.2008.4700636.

[22] F. Ganji, S. Tajik and J.-P. Seifert, "Pac learning of arbiter pufs", *Journal of Cryptographic Engineering*, vol. 6, no. 3, pp. 249–258, 2016, ISSN: 2190-8516. DOI: 10.1007/s13389-016-0119-4. [Online]. Available: http://dx.doi.org/10.1007/s13389-016-0119-4.

Proposals (& attacks!)

- Arbiter PUFs
- . . . with modelling attacks

Proposals (& attacks!)

- Arbiter PUFs
- . . . with modelling attacks
- . . . and now also measuring delays at 6ps accuracy![23]

[23] S. Tajik, E. Dietz, S. Frohmann *et al.*, "Photonic side-channel analysis of arbiter pufs", *Journal of Cryptology*, pp. 1–22, 2016, ISSN: 1432-1378. DOI: 10.1007/s00145-016-9228-6. [Online]. Available: http://dx.doi.org/10.1007/s00145-016-9228-6.

Proposals (& attacks!)

Proposals (& attacks!)

- Memory-based (bistable) PUFs[24,25,26,27,28]

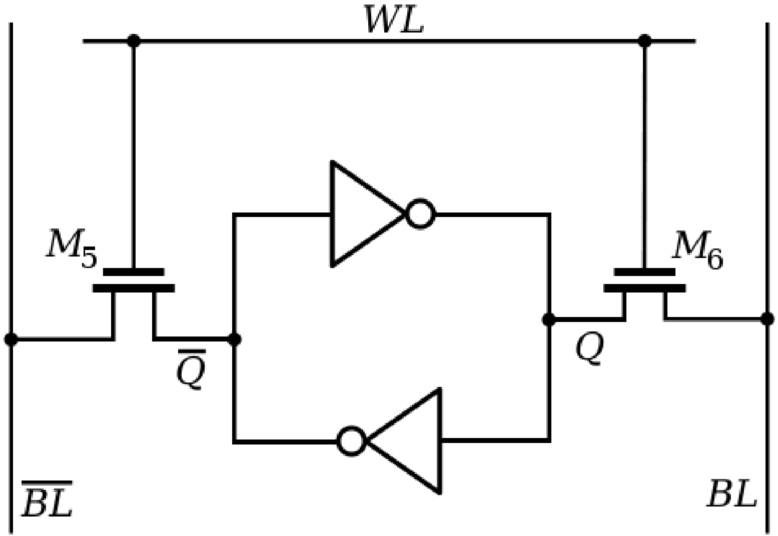
[24] J. Guajardo, S. S. Kumar, G.-J. Schrijen *et al.*, "Fpga intrinsic pufs and their use for ip protection", in *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 63–80, ISBN: 978-3-540-74735-2. DOI: 10.1007/978-3-540-74735-2_5.

[25] D. E. Holcomb, W. P. Burleson and K. Fu, "Initial sram state as a fingerprint and source of true random numbers for rfid tags", in *In Proceedings of the Conference on RFID Security*, 2007.

[26] R. Maes, P. Tuyls, I. Verbauwhede *et al.*, *Intrinsic pufs from flip-flops on reconfigurable devices," in wissec*, 2008.

[27] V. van der Leest, G.-J. Schrijen, H. Handschuh *et al.*, "Hardware intrinsic security from d flip-flops", in *Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing*, ser. STC '10, Chicago, Illinois, USA: ACM, 2010, pp. 53–62, ISBN: 978-1-4503-0095-7. DOI: 10.1145/1867635.1867644.

[28] S. S. Kumar, J. Guajardo, R. Maes *et al.*, "Extended abstract: The butterfly puf protecting ip on every fpga", in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 67–70. DOI: 10.1109/HST.2008.4559053.


WL
M5
M6
Q̄
Q
B̄L̄
BL

Proposals (& attacks!)

- Memory-based (bistable) PUFs

Proposals (& attacks!)

- Memory-based (bistable) PUFs
- . . . with cloning[29]

[29] C. Helfmeier, C. Boit, D. Nedospasov *et al.*, "Cloning physically unclonable functions", in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 1–6. DOI: 10.1109/HST.2013.6581556.

Proposals (& attacks!)

- Memory-based (bistable) PUFs
- ... with cloning[29] and emulation attacks

[29] C. Helfmeier, C. Boit, D. Nedospasov *et al.*, "Cloning physically unclonable functions", in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 1–6. DOI: 10.1109/HST.2013.6581556.

Proposals (& attacks!)

Proposals (& attacks!)

- Decay-based PUFs[30]

[30] W. Xiong, A. Schaller, N. A. Anagnostopoulos *et al.*, "Run-time accessible dram pufs in commodity devices", in *Cryptographic Hardware and Embedded Systems – CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, B. Gierlichs and A. Y. Poschmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 432–453, ISBN: 978-3-662-53140-2. DOI: 10.1007/978-3-662-53140-2_21. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-53140-2_21.

Proposals (& attacks!)

- Decay-based PUFs[30]
- ...

[30] W. Xiong, A. Schaller, N. A. Anagnostopoulos *et al.*, "Run-time accessible dram pufs in commodity devices", in *Cryptographic Hardware and Embedded Systems – CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, B. Gierlichs and A. Y. Poschmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 432–453, ISBN: 978-3-662-53140-2. DOI: 10.1007/978-3-662-53140-2_21. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-53140-2_21.

Outline

Academic cop-out

This is trivial and left as an exercise for the reader.

J/K

Why? It's hopeless!

Why? It's hopeless!

- Protection: Some > None

Why? It's hopeless!

- Protection: Some > None
- No silver bullets

If nothing else

Read *this*[31] paper about using a PUF to create a secure boot loader on small embedded ARM and other SoC devices (the following slides contain material from this paper),

[31] A. Schaller, T. Arul, V. van der Leest *et al.*, "Lightweight anti-counterfeiting solution for low-end commodity hardware using inherent pufs", in *Trust and Trustworthy Computing: 7th International Conference, TRUST 2014, Heraklion, Crete, June 30 – July 2, 2014. Proceedings*, T. Holz and S. Ioannidis, Eds. Cham: Springer International Publishing, 2014, pp. 83–100, ISBN: 978-3-319-08593-7. DOI: 10.1007/978-3-319-08593-7_6. [Online]. Available: http://www2.seceng.informatik.tu-darmstadt.de/assets/schaller-2/docs/trust2014.pdf.

If nothing else

and *this*[32] more recent paper on hardware-assisted software protection.

[32] F. Kohnhäuser, A. Schaller and S. Katzenbeisser, "Puf-based software protection for low-end embedded devices", in *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings*, M. Conti, M. Schunter and I. Askoxylakis, Eds. Cham: Springer International Publishing, 2015, pp. 3–21, ISBN: 978-3-319-22846-4. DOI: 10.1007/978-3-319-22846-4_1. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-22846-4_1.

What you'll need

A device with:

What you'll need

A device with:

- a masked ROM to hold the boot loader

What you'll need

A device with:

- a masked ROM to hold the boot loader
- modifiable startup code (1st stage bootloader)

What you'll need

A device with:

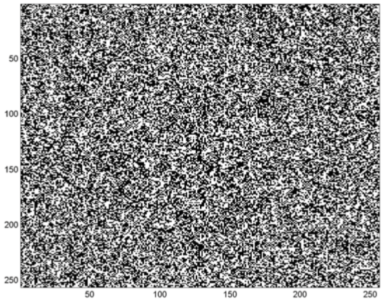
- a masked ROM to hold the boot loader
- modifiable startup code (1st stage bootloader)
- on-board SRAM

What you'll need

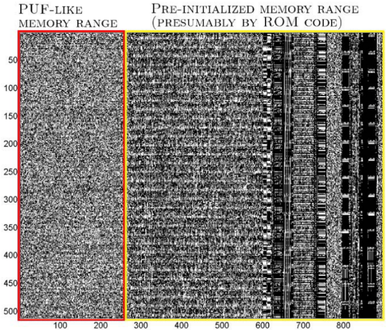
A device with:

- a masked ROM to hold the boot loader
- modifiable startup code (1st stage bootloader)
- on-board SRAM
- non-volatile memory for encrypted firmware & helper data

Analyze the PUF

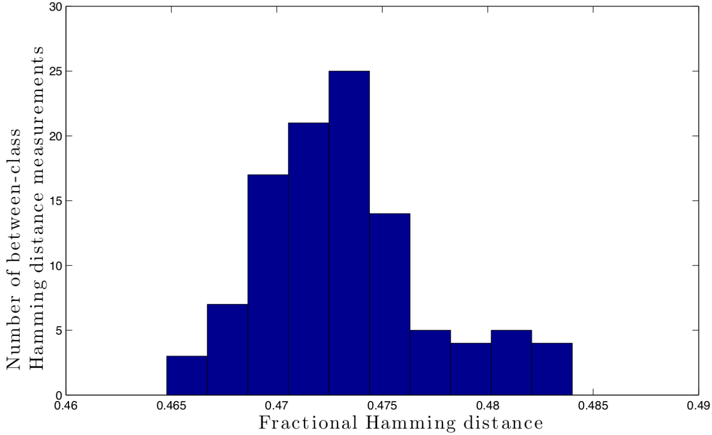


(a) STM32F100B



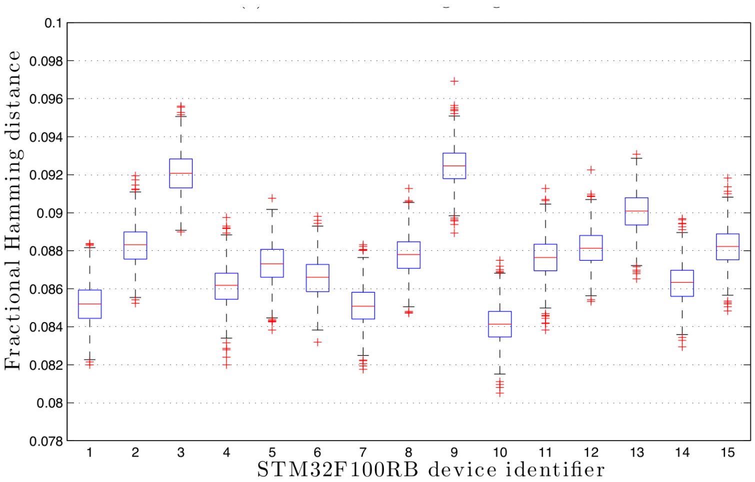
(b) PandaBoard

Analyze the PUF



(c) Between-class Hamming distance

Analyze the PUF

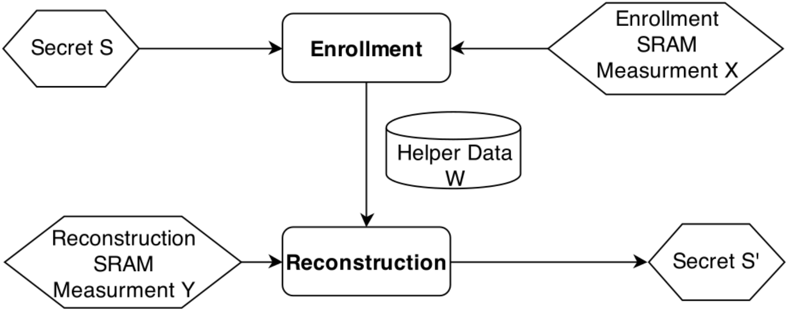


Analyze the PUF

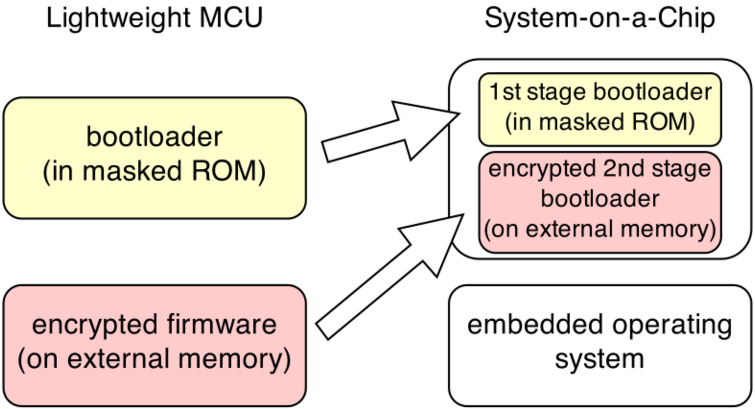
Will need error correction, e.g. using Golay codes

Fuzzy extractor enrollment / usage described in paper

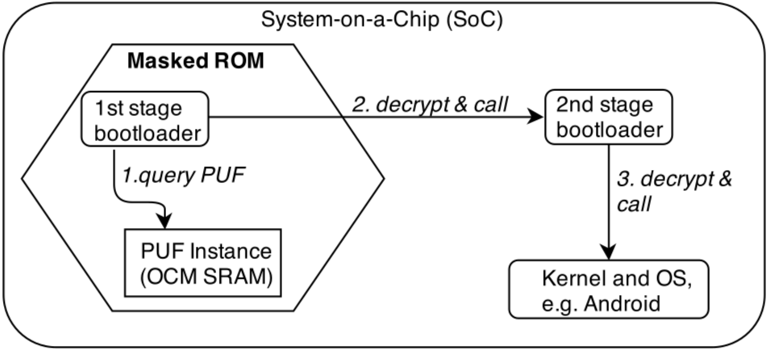
Now build this

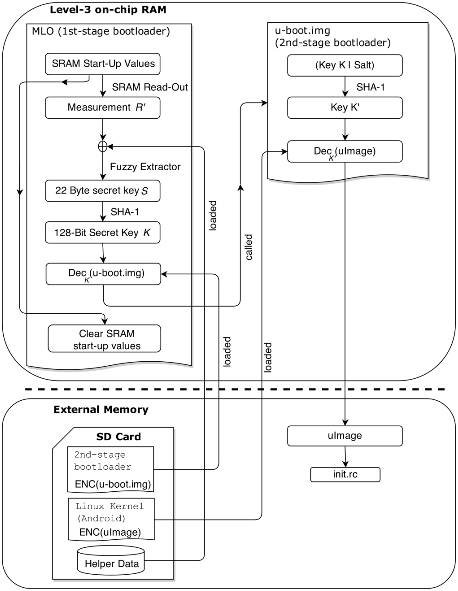


Now build this



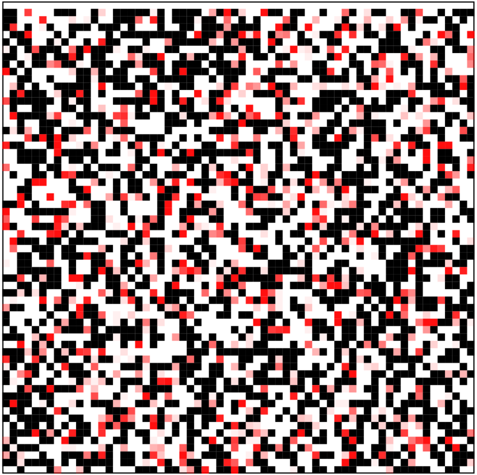
Now build this



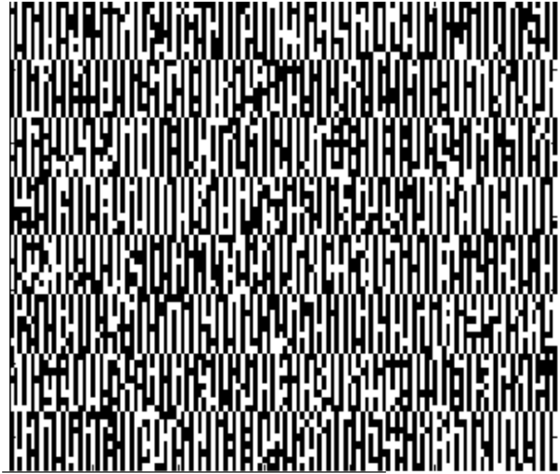


Level-3 on-chip RAM
MLO (1st-stage bootloader)
SRAM Start-Up Values
SRAM Read-Out
Measurement R'
Fuzzy Extractor
22 Byte secret key S
SHA-1
128-Bit Secret Key K
Dec K (u-boot.img)
Clear SRAM start-up values
u-boot.img (2nd-stage bootloader)
(Key K I Salt)
SHA-1
Key K'
Dec K' (uImage)
loaded
called
loaded
loaded
External Memory
SD Card
2nd-stage bootloader
ENC(u-boot.img)
Linux Kernel (Android)
ENC(uImage)
Helper Data
uImage
init.rc

And you'll also have this



But hopefully not this

 [33]

[33] A. Van Herrewege, V. van der Leest, A. Schaller *et al.*, "Secure prng seeding on commercial off-the-shelf microcontrollers", in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, ser. TrustED '13, Berlin, Germany: ACM, 2013, pp. 55–64, ISBN: 978-1-4503-2486-1. DOI: 10.1145/2517300.2517306. [Online]. Available: http://doi.acm.org/10.1145/2517300.2517306.

x86_64?

Unfortunately, won't be possible[34]

[34] P. Van Aubel, D. J. Bernstein and R. Niederhagen, "Investigating sram pufs in large cpus and gpus", in *Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings*, R. S. Chakraborty, P. Schwabe and J. Solworth, Eds. Cham: Springer International Publishing, 2015, pp. 228–247, ISBN: 978-3-319-24126-5. DOI: 10.1007/978-3-319-24126-5_14. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-24126-5_14.

Outline

Out of time, but. . .

Privacy concerns: "past experience shows that users feel uncomfortable with processors that have unique identifiers, because they ***feel*** that they can be tracked. Users could have the same type of concern with the use of PUFs, given that PUFs are a form of unique identifier."[35] (emphasis added)

[35] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Silicon physical random functions", in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02, Washington, DC, USA: ACM, 2002, pp. 148–160, ISBN: 1-58113-612-9. DOI: 10.1145/586110.586132. [Online]. Available: http://doi.acm.org/10.1145/586110.586132.

Out of time, but...

Privacy concerns: "past experience shows that users feel uncomfortable with processors that have unique identifiers, because they ***feel*** that they can be tracked. Users could have the same type of concern with the use of PUFs, given that PUFs are a form of unique identifier."[35] (emphasis added)

Damn users, being paranoid and all...

[35] B. Gassend, D. Clarke, M. van Dijk *et al.*, "Silicon physical random functions", in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02, Washington, DC, USA: ACM, 2002, pp. 148–160, ISBN: 1-58113-612-9. DOI: 10.1145/586110.586132. [Online]. Available: http://doi.acm.org/10.1145/586110.586132.

Controlled PUF

with multiple personalities.

Outline

Google

Seriously. Google Scholar is your friend.

References I

M. Kuhn, *The eurion constellation*, Feb. 2002. [Online]. Available: http://www.cl.cam.ac.uk/~mgk25/eurion.pdf.

D. W. Bauder, “An anti-counterfeiting concept for currency systems”, *Sandia National Labs, Albuquerque, NM, Tech. Rep. PTK-11990*, 1983.

G. J. Simmons, “Identification of data, devices, documents and individuals”, in *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on Security Technology*, 1991, pp. 197–218. DOI: 10.1109/CCST.1991.202215.

References II

- J. Brosow and E. Furugard, *Method and a system for verifying authenticity safe against forgery*, US Patent 4,218,674, Aug. 1980. [Online]. Available: https://www.google.com/patents/US4218674.
- J. Samyn, *Method and apparatus for checking the authenticity of documents*, US Patent 4,820,912, Apr. 1989. [Online]. Available: https://www.google.com/patents/US4820912.
- R. Goldman, *Verification system for document substance and content*, US Patent 4,689,477, Aug. 1987. [Online]. Available: https://www.google.com/patents/US4689477.
- J. R. Smith and A. V. Sutherland, "Microstructure based indicia", in *Proceedings of the Second Workshop on Automatic Identification Advanced Technologies*, 1999, pp. 79–83.

References III

R. Pappu, B. Recht, J. Taylor and N. Gershenfeld, “Physical one-way functions”, *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, ISSN: 0036-8075. DOI: 10.1126/science.1074376. [Online]. Available: http://science.sciencemag.org/content/297/5589/2026.

K. Lofstrom, W. R. Daasch and D. Taylor, “Ic identification circuit using device mismatch”, in *2000 IEEE International Solid-State Circuits Conference. Digest of Technical Papers (Cat. No.00CH37056)*, 2000, pp. 372–373. DOI: 10.1109/ISSCC.2000.839821.

References IV

B. Gassend, D. Clarke, M. van Dijk and S. Devadas, “Silicon physical random functions”, in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, ser. CCS '02, Washington, DC, USA: ACM, 2002, pp. 148–160, ISBN: 1-58113-612-9. DOI: 10.1145/586110.586132. [Online]. Available: http://doi.acm.org/10.1145/586110.586132.

B. Gassend, D. Clarke, M. van Dijk and S. Devadas, “Controlled physical random functions”, in *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, 2002, pp. 149–160. DOI: 10.1109/CSAC.2002.1176287.

References V

- F. Armknecht, R. Maes, A. R. Sadeghi, F. X. Standaert and C. Wachsmann, "A formalization of the security features of physical functions", in *2011 IEEE Symposium on Security and Privacy*, 2011, pp. 397–412. DOI: 10.1109/SP.2011.10.
- J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications", in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, 2004, pp. 176–179. DOI: 10.1109/VLSIC.2004.1346548.
- U. Rührmair, J. Sölter and F. Sehnke, "On the foundations of physical unclonable functions.", *IACR Cryptology ePrint Archive*, vol. 2009, p. 277, 2009.

References VI

M. Majzoobi, F. Koushanfar and M. Potkonjak, "Testing techniques for hardware security", in *2008 IEEE International Test Conference*, 2008, pp. 1–10. DOI: 10.1109/TEST.2008.4700636.

F. Ganji, S. Tajik and J.-P. Seifert, "Pac learning of arbiter pufs", *Journal of Cryptographic Engineering*, vol. 6, no. 3, pp. 249–258, 2016, ISSN: 2190-8516. DOI: 10.1007/s13389-016-0119-4. [Online]. Available: http://dx.doi.org/10.1007/s13389-016-0119-4.

References VII

S. Tajik, E. Dietz, S. Frohmann, H. Dittrich, D. Nedospasov, C. Helfmeier, J.-P. Seifert, C. Boit and H.-W. Hübers, "Photonic side-channel analysis of arbiter pufs", *Journal of Cryptology*, pp. 1–22, 2016, ISSN: 1432-1378. DOI: 10.1007/s00145-016-9228-6. [Online]. Available: http://dx.doi.org/10.1007/s00145-016-9228-6.

J. Guajardo, S. S. Kumar, G.-J. Schrijen and P. Tuyls, "Fpga intrinsic pufs and their use for ip protection", in *Cryptographic Hardware and Embedded Systems - CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings*, P. Paillier and I. Verbauwhede, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007, pp. 63–80, ISBN: 978-3-540-74735-2. DOI: 10.1007/978-3-540-74735-2_5.

References VIII

D. E. Holcomb, W. P. Burleson and K. Fu, "Initial sram state as a fingerprint and source of true random numbers for rfid tags", in *In Proceedings of the Conference on RFID Security*, 2007.

R. Maes, P. Tuyls, I. Verbauwhede and L. Esat-cosic, *Intrinsic pufs from flip-flops on reconfigurable devices," in wissec*, 2008.

V. van der Leest, G.-J. Schrijen, H. Handschuh and P. Tuyls, "Hardware intrinsic security from d flip-flops", in *Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing*, ser. STC '10, Chicago, Illinois, USA: ACM, 2010, pp. 53–62, ISBN: 978-1-4503-0095-7. DOI: 10.1145/1867635.1867644.

References IX

S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen and P. Tuyls, "Extended abstract: The butterfly puf protecting ip on every fpga", in *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, 2008, pp. 67–70. DOI: 10.1109/HST.2008.4559053.

C. Helfmeier, C. Boit, D. Nedospasov and J. P. Seifert, "Cloning physically unclonable functions", in *2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 1–6. DOI: 10.1109/HST.2013.6581556.

References X

W. Xiong, A. Schaller, N. A. Anagnostopoulos, M. U. Saleem, S. Gabmeyer, S. Katzenbeisser and J. Szefer, "Run-time accessible dram pufs in commodity devices", in *Cryptographic Hardware and Embedded Systems – CHES 2016: 18th International Conference, Santa Barbara, CA, USA, August 17-19, 2016, Proceedings*, B. Gierlichs and A. Y. Poschmann, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 432–453, ISBN: 978-3-662-53140-2. DOI: 10.1007/978-3-662-53140-2_21. [Online]. Available: http://dx.doi.org/10.1007/978-3-662-53140-2_21.

References XI

A. Schaller, T. Arul, V. van der Leest and S. Katzenbeisser, "Lightweight anti-counterfeiting solution for low-end commodity hardware using inherent pufs", in *Trust and Trustworthy Computing: 7th International Conference, TRUST 2014, Heraklion, Crete, June 30 – July 2, 2014. Proceedings*, T. Holz and S. Ioannidis, Eds. Cham: Springer International Publishing, 2014, pp. 83–100, ISBN: 978-3-319-08593-7. DOI: 10.1007/978-3-319-08593-7_6. [Online]. Available: http://www2.seceng.informatik.tu-darmstadt.de/assets/schaller-2/docs/trust2014.pdf.

References XII

F. Kohnhäuser, A. Schaller and S. Katzenbeisser, "Puf-based software protection for low-end embedded devices", in *Trust and Trustworthy Computing: 8th International Conference, TRUST 2015, Heraklion, Greece, August 24-26, 2015, Proceedings*, M. Conti, M. Schunter and I. Askoxylakis, Eds. Cham: Springer International Publishing, 2015, pp. 3–21, ISBN: 978-3-319-22846-4. DOI: 10.1007/978-3-319-22846-4_1. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-22846-4_1.

References XIII

A. Van Herrewege, V. van der Leest, A. Schaller, S. Katzenbeisser and I. Verbauwhede, "Secure prng seeding on commercial off-the-shelf microcontrollers", in *Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices*, ser. TrustED '13, Berlin, Germany: ACM, 2013, pp. 55–64, ISBN: 978-1-4503-2486-1. DOI: 10.1145/2517300.2517306. [Online]. Available: http://doi.acm.org/10.1145/2517300.2517306.

References XIV

P. Van Aubel, D. J. Bernstein and R. Niederhagen, "Investigating sram pufs in large cpus and gpus", in *Security, Privacy, and Applied Cryptography Engineering: 5th International Conference, SPACE 2015, Jaipur, India, October 3-7, 2015, Proceedings*, R. S. Chakraborty, P. Schwabe and J. Solworth, Eds. Cham: Springer International Publishing, 2015, pp. 228–247, ISBN: 978-3-319-24126-5. DOI: 10.1007/978-3-319-24126-5_14. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-24126-5_14.

Presenting

Pol Van Aubel
radboud@polvanaubel.com

Radboud University
iCIS|Digital Security