Daniel Genkin

Curriculum Vitae

Last Updated: January 16, 2018

PERSONAL DETAILS

Birth	August 1, 1989
Address	121 S 43rd St. Apt. 406, Philadelphia, PA 19104
Phone	+001 267 916 7939 ; +972 544 385 893
Mail	danielg30@gmail.com
Homepage	https://www.cis.upenn.edu/~danielg3/

CURRENT POSITION

Postdoctoral Fellow 09.2016-present

University of Pennsylvania and University of Maryland

Field of Research: Cryptography and Information Security

Host: Prof. Nadia Heninger and Prof. Jonathan Katz

EDUCATION

Ph.D. in Computer Science 2011-2016

Technion — Israel Institute of Technology

Field of Research: Cryptography and Information Security

Thesis Title: Secure Computation in Hostile Environments

Thesis Advisor: Prof. Yuval Ishai and Prof. Eran Tromer

M.Sc. in Computer Science 2008-2011

Technion — Israel Institute of Technology

Field of Research: Automata Theory

Thesis Title: Radical Lexicalization of Mildly Context-Sensitive Languages

Thesis Advisor: Prof. Michael Kaminski

B.A. in Computer Science 2004-2008

The Open University of Israel

Cum Laude

SCHOLARSHIPS AND AWARDS

- **Warren Center Postdoctoral Fellowship.** Warren Center for Network and Data Sciences, 2017.
- **Paper selected as one of top 4 papers in CHES 2016 conference.** CHES, 2016.
- **Rothschild Postdoctoral Fellowship.** Rothschild Foundation, 2016-2017.
- **Jacobs Outstanding Publication Award.** Technion, 2015.
- **Paper selected as one of top 3 papers in CHES 2014 conference.** CHES, 2014.
- **Paper selected as one of top 3 papers in CRYPTO 2014 conference.** CRYPTO, 2014.
- **Pwnie Award for Most Innovative Research.** Black Hat, 2014.
- **CS Department Excellence Fellowship.** Technion, 2014.
- **1st Place, Research day.** Technion, 2014.
- **2nd Place, Research day.** Technion, 2013.

TEACHING EXPERIENCE

Teaching Assistant (TA) in the following courses:

Algorithms 1 2013-2016
Lecturers: Prof. Eli Ben-Sasson, Prof. Shlomo Moran, Prof. Seffi Naor, Prof. Hadas Shachnai

Automata and Formal Languages 2011-2012
Lecturers: Prof. Michael Kaminski, Prof. Shmuel Zaks

Digital Computer Architecture 2010
Lecturer: Dr. Lihu Rappoport

Theory of Compilation 2008-2010
Lecturers: Dr. Shirley Halevy Ginsburg, Dr. Ayal Zaks

PROFESSIONAL SERVICE

- Program Committee member: Crypto 2018, ACM Conference on Computer and Communications Security (CCS) 2017, Smart Card Research and Advanced Application Conference (CARDIS) 2017.
- External Reviewer for: Crypto 2017, Usenix Security 2017, Eurocrypt 2016, IEEE Security and Privacy (Oakland) 2016.

PUBLICATIONS

"AR" and "IF" are the venue's acceptance rate or impact factor, respectively (in relevant year if available, otherwise average over recent years if available).

Preprints

- Paul Kocher, Daniel Genkin, Daniel Gruss, Werner Haas, Mike Hamburg, Moritz Lipp, Stefan Mangard, Thomas Prescher, Michael Schwarz, Yuval Yarom. **Spectre Attacks: Exploiting Speculative Execution**. `https://spectreattack.com/`
- Moritz Lipp, Michael Schwarz, Daniel Gruss, Thomas Prescher, Werner Haas, Stefan Mangard, Paul Kocher, Daniel Genkin, Yuval Yarom, Mike Hamburg. **Meltdown**. `https://meltdownattack.com`

Publications in Refereed Conferences

1. Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou. **vRAM: Faster Verifiable RAM With Program-Independent Preprocessing**. To appear in *IEEE Symposium on Security and Privacy 2018*.
2. Daniel Genkin, Yuval Ishai, and Mor Weiss. **How to Build a Leakage-Resilient (Stateless) Trusted Party.** In *Theory of Cryptography Conference (TCC) 2017*, pages 209-244, Springer, 2017. (AR. 0.30)
3. Daniel Genkin, Luke Valenta, and Yuval Yarom. **May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519.** In *ACM Conference on Computer and Communications Security (CCS) 2017*, pages 845-858, ACM, 2017. (AR. 0.18)
4. Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, and Yuval Yarom. **Sliding Right Into Disaster: Left-to-right sliding windows leak.** In *Cryptographic Hardware and Embedded Systems (CHES) 2017*, pages 555-576, Springer, 2017. (AR. 0.25)

5. Yang Su, Daniel Genkin, Damith Ranasinghe, and Yuval Yarom. **USB Snooping Made Easy: Crosstalk Leakage Attacks on USB Hubs.** In *Usenix Security Symposium 2017*, pages 1145-1161, Usenix Association, 2017. (AR. 0.16)

6. Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou. **vSQL: Verifying General SQL Queries over Dynamic Outsourced Databases.** In *IEEE Security & Privacy (Oakland) 2017*, pages 863-880, IEEE, 2017. (AR. 0.14)

7. Eli Ben-Sasson, Iddo Ben-Tov, Alessandro Chiesa, Ariel Gabizon, Daniel Genkin, Matan Hamilis, Evgenya Pergament, Michael Riabzev, Mark Silberstein, Eran Tromer, and Madars Virza. **Computational Integrity with a Public Random String from Quasi-Linear PCPs.** In *Eurocrypt 2017*, pages 551-579, Springer, 2017. (0.23)

8. Daniel Genkin, Yuval Ishai, and Mor Weiss. **Binary AMD Circuits from Secure Multiparty Computation.** In *Theory of Cryptography Conference (TCC 2016-B) 2016*, pages 336-366, Springer, 2016. (AR. 0.4)

9. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Eran Tromer, and Yuval Yarom. **ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels.** In *ACM Conference on Computer and Communications Security (ACM CCS) 2016*, pages 1626-1638, ACM, 2016. (AR. 0.16)

10. Yuval Yarom, Daniel Genkin, and Nadia Heninger. **CacheBleed: A Timing Attack on OpenSSL Constant Time RSA.** In *Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2016*, pages 346-367, Springer, 2016.
    - ◇ Selected by the PC as one of the conference's top 4 papers and invited to the Journal of Cryptographic Engineering (JCEN).

11. Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. **ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs.** In *RSA Conference — The Cryptographer's Track 2016*, pages 219-235, Springer, 2016. (AR. 0.294)

12. Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. **Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation.** In *Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2015*, pages 207-228, Springer, 2015. (AR 0.19)

13. Daniel Genkin, Antigoni Polychroniadou, and Yuval Ishai. **Efficient Multi-party Computation: From Passive to Active Security via Secure SIMD Circuits.** In *CRYPTO 2015, Part 2*, pages 721-741, Springer, 2015. (AR 0.28)

14. Daniel Genkin, Itamar Pipman, and Eran Tromer. **Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs.** In *Workshop on Cryptographic Hardware and Embedded Systems (CHES) 2014*, pages 242-260, Springer, 2014. (AR. 0.26)
    - ◇ Selected by the PC as one of the conference's top 3 papers and invited to the Journal of Cryptographic Engineering (JCEN).

15. Daniel Genkin, Adi Shamir, and Eran Tromer. **RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis.** In *CRYPTO 2014, Part 1*, pages 444-461, Springer, 2014. (AR 0.26)
    - ◇ Selected by the PC as one of the conference's top 3 papers and invited to the Journal of Cryptology (JoC).
    - ◇ Won Black Hat 2014 Pwnie Award for Most Innovative Research.

16. Daniel Genkin, Yuval Ishai, Manoj M. Prabhakaran, Amit Sahai, and Eran Tromer. **Circuits Resilient to Additive Attacks with Applications to Secure Computation.** In *Symposium on Theory of Computing (STOC) 2014*, pages 495-504, ACM, 2014. (AR. 0.28)

17. Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. **SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge.** In *CRYPTO 2013, Part 2*, pages 90-108, Springer, 2013. (AR. 0.27)

18. Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, and Eran Tromer. **Fast reductions from RAMs to delegatable succinct constraint satisfaction problems.** In *Innovations in Theoretical Computer Science (ITCS) 2013*, pages 404-414, ACM, 2013. (AR. 0.40)

19. Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, and Eran Tromer. **On the concrete efficiency of probabilistically-checkable proofs.** In *Symposium on Theory of Computing (STOC) 2013*, pages 585-594, ACM, 2013. (AR. 0.28)

20. Daniel Genkin, Nissim Francez, and Michael Kaminski. **Mildly Context-Sensitive Languages via Buffer Augmented Pregroup Grammars.** In *Time for Verification, Essays in Memory of Amir Pnueli*, pages 144-166, Springer, 2010.

Journal Publications

1. Daniel Genkin, Dimitrios Papadopoulos, and Charalampos Papamanthou. **Privacy in Decentralized Cryptocurrencies**. To appear in *Communications of the ACM*.

2. Yuval Yarom, Daniel Genkin, and Nadia Heninger. **CacheBleed: A Timing Attack on OpenSSL Constant Time RSA - Extended Version.** In *Journal of Cryptographic Engineering (JCEN)*, vol. 7 no. 2 pages 99-112, Springer, 2017.

   ◇ Selected by the PC as one of the conference's top papers and invited to the Journal of Cryptographic Engineering (JCEN).
   ◇ This is an extended version of conference publication 10.

3. Daniel Genkin, Lev Pachmanov, Itamar Pipman, Adi Shamir, and Eran Tromer. **Physical Key Extraction Attacks on PCs.** In *Communications of the ACM*, vol 59 no. 6 pages 70-79, ACM 2016. (IF. 3.42)

4. Daniel Genkin, Adi Shamir, and Eran Tromer. **Acoustic Cryptanalysis.** In *Journal of Cryptology*, vol. 30 no. 2 pages 392-443, Springer, 2017.

   ◇ Invited as a top paper in CRYPTO 2014 conference.
   ◇ This is an extended version of conference publication 15.

5. Daniel Genkin, Itamar Pipman, and Eran Tromer. **Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs - Extended Version.** In *Journal of Cryptographic Engineering*,vol. 5 no. 2 pages 95-112, Springer, 2015.

   ◇ Invited as a top paper in CHES 2014 conference.
   ◇ This is an extended version of conference publication 14.

6. Daniel Genkin, Michael Kaminski, and Liat Peterfreund. **A note on the emptiness problem for alternating finite-memory automata.** In *Theoretical Computer Science*,vol. 526 pages 97-107, Elsevier, 2014. (IF 0.657)

7. Tamar Aizikowitz, Nissim Francez, Daniel Genkin, and Michael Kaminski. **Extending Free Pregroups with Lower Bounds.** In *Studia Logica*,vol. 95 no. 3 pages 417-441, Springer, 2010. (IF 0.598)

COMMON VULNERABILITIES EXPOSURES (CVE)

CVE is a dictionary of publicly known information security vulnerabilities and exposures. Each security vulnerability is assigned a unique identifier for future reference.

- **CVE-2017-5754** for Meltdown.

- **CVE-2017-5715** and **CVE-2017-5753** for Spectre Attacks: Exploiting Speculative Execution.
- **CVE-2017-0379** for May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519.
- **CVE-2017-7526** for Sliding Right Into Disaster: Left-to-right sliding windows leak.
- **CVE-2016-0702** for CacheBleed: A Timing Attack on OpenSSL Constant Time RSA.
- **CVE-2015-7511** for ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs.
- **CVE-2014-5270** for Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs.
- **CVE-2014-3591** for Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation.
- **CVE-2013-4576** for RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis.