Weak-point bitstream

Constantin Piber

November 17, 2023

Bitstream Lifecycle

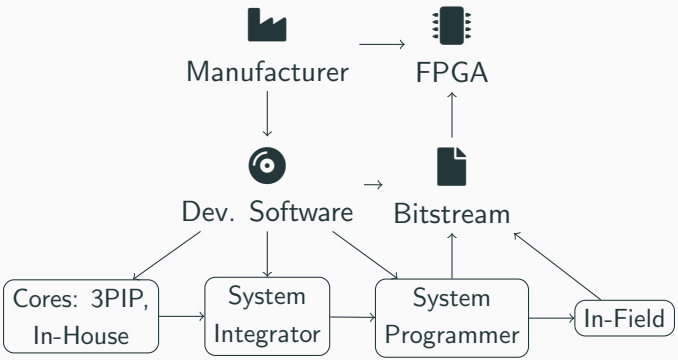

Figure 1: FPGA Design flow [1]

Bitstream Lifecycle

What is a bitstream? [2], [3]

- Produced by Vendor-specific software
- Result of translation from HDL
- Usually proprietary
- Encrypted, Authenticated or Unencrypted
- Configures logic blocks/cores of FPGA

Bitstream Lifecycle

Phases of the bitstream cycle [1]:

1. **Bitstream-Generation**:
   Generation of bitstream file via FPGA design tools
2. **Bitstream-at-Rest**:
   Bitstream has been generated, stored on disk/cloud/...
3. **Bitstream-Loading**:
   Loading of bitstream from non-volatile memory to FPGA configuration
4. **Bitstream-Running**:
   Running FPGA, with bitstream configured
5. **Bitstream-EOL**:
   End of life, after bistream and/or FPGA is decomissioned

Bitstream Generation

IP-level threats [1], [4]

- **Trojan Attacks**:
  Post-synthesis modifications, change placement – Power consumption, profile rarely activated logic [5]–[7]
- **IP Piracy**:
  IP theft, overuse, reverse engineering – Watermarking, PUF-challenge to unlock core, logic obfuscation [8]–[10]
- **Vulnerabilities**:
  Unintended vulnerabilities during conversion, malicious tooling – Randomize placement, check for equivalence [11]–[13]

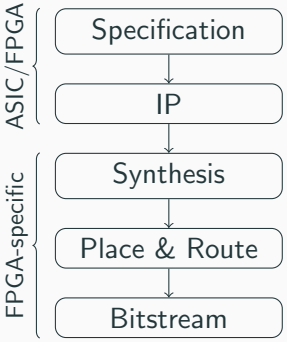

Figure 2: Bitstream Generation Flow [1]

Bitstream at Rest

Attacks on stored bistream files [1], [4]

- **Bitstream Tampering**:
  Plaintext manipulations – Logic locking (PUF), obfuscation [14]–[16]
- **Bitstream Encryption**:
  Prevents manipulation [14]
- **Red/Black Encryption**:
  Black key on FPGA generates decryption via PUF [17]
- **IP Piracy**:
  Reverse engineering – Watermarking [18]

Bitstream at Rest

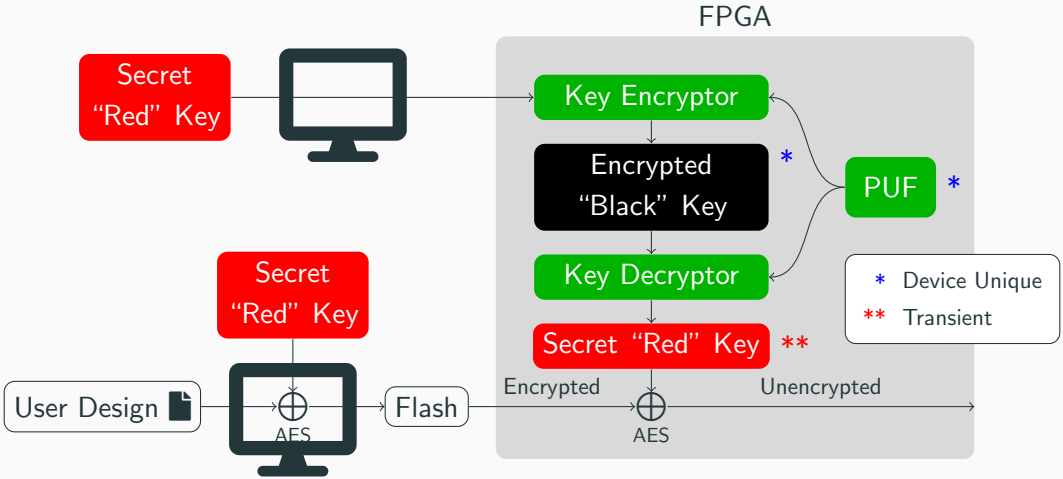

Figure 3: Red/Black Encryption [17]

Bitstream Loading

During configuration of silicon [1], [4]

- **Side Channel Threats**:
  Collect information, extract keys – Key rolling, optical reflectance [17], [19], [20]
- **FPGA-based SoCs**:
  Boot process loads bitstream – Authentication [17], [21]
- **Bitstream Replay Threats**:
  Configuration downgrade – Versioning, critical switch [22], [23]

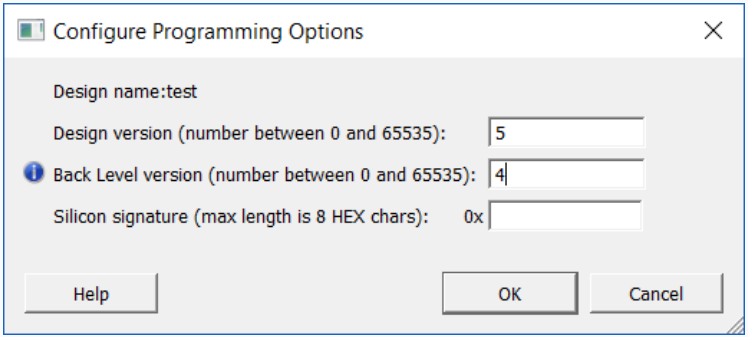

Figure 4: Bitstream Versioning [22]

Bistream Running

FPGA is operating [1], [4]

- **Fault Injection**:
  Glitches – Detect bitflips via reconfiguration core [24]–[26]
- **Run-time Attacks**:
  Leak or corrupt information on shared systems – Vendor screening, sensors to detect glitches [27]–[29]

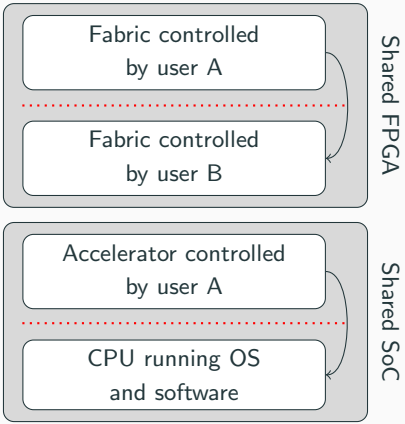

Figure 5: Attack over logical separation [27]

Bitstream End-of-Life

FPGA/Bitstream decomissioned [1]

- **Bitstream Remanence**:
  Bitstream remains on board – Zeroise memory [22], [29]
- **Device Counterfeiting**:
  Selling of used devices, bootleg – Device-specific markings [30]–[32]

References i

[1] A. Duncan, F. Rahman, A. Lukefahr, F. Farahmandi, and M. Tehranipoor, **Fpga bitstream security: A day in the life,** in 2019 IEEE International Test Conference (ITC), 2019, pp. 1–10. DOI: 10.1109/ITC44170.2019.9000145.

[2] R. K. Soni, **Open-source bitstream generation for fpgas,** Ph.D. dissertation, Virginia Tech, 2013.

[3] Xilinx, **Embedded hardware components: Fpga bitstream,** [Online]. Available: https://www.xilinx.com/htmldocs/xilinx2018_1/SDK_Doc/SDK_concepts/concept_fpgabitstream.html.

[4] M. Moraitis, **Fpga bitstream modification: Attacks and countermeasures,** IEEE Access, pp. 1–1, 2023. DOI: 10.1109/ACCESS.2023.3331507.

[5] M. Tehranipoor and F. Koushanfar, **A survey of hardware trojan taxonomy and detection,** IEEE Design & Test of Computers, vol. 27, no. 1, pp. 10–25, 2010. DOI: 10.1109/MDT.2010.7.

References ii

[6] S. Mal-Sarkar, A. Krishna, A. Ghosh, and S. Bhunia, **Hardware trojan attacks in fpga devices: Threat analysis and effective counter measures,** in Proceedings of the 24th Edition of the Great Lakes Symposium on VLSI, ser. GLSVLSI '14, Houston, Texas, USA: Association for Computing Machinery, 2014, pp. 287–292, ISBN: 9781450328166. DOI: 10.1145/2591513.2591520. [Online]. Available: https://doi.org/10.1145/2591513.2591520.

[7] K. Xiao and M. Tehranipoor, **Bisa: Built-in self-authentication for preventing hardware trojan insertion,** in 2013 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2013, pp. 45–50. DOI: 10.1109/HST.2013.6581564.

References iii

[8] A. K. Jain, L. Yuan, P. R. Pari, and G. Qu, **Zero overhead watermarking technique for fpga designs,** in Proceedings of the 13th ACM Great Lakes Symposium on VLSI, ser. GLSVLSI '03, Washington, D. C., USA: Association for Computing Machinery, 2003, pp. 147–152, ISBN: 1581136773. DOI: 10.1145/764808.764847. [Online]. Available: https://doi.org/10.1145/764808.764847.

[9] J. Zhang, Y. Lin, Y. Lyu, and G. Qu, **A puf-fsm binding scheme for fpga ip protection and pay-per-device licensing,** Trans. Info. For. Sec., vol. 10, no. 6, pp. 1137–1150, Jun. 2015, ISSN: 1556-6013. DOI: 10.1109/TIFS.2015.2400413. [Online]. Available: https://doi.org/10.1109/TIFS.2015.2400413.

[10] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, **Security analysis of logic obfuscation,** in DAC Design Automation Conference 2012, 2012, pp. 83–89. DOI: 10.1145/2228360.2228377.

References iv

[11] C. Krieg, C. Wolf, and A. Jantsch, **Malicious lut: A stealthy fpga trojan injected and triggered by the design flow,** in 2016 IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2016, pp. 1–8. DOI: 10.1145/2966986.2967054.

[12] Z. Zhang, L. Njilla, C. A. Kamhoua, and Q. Yu, **Thwarting security threats from malicious fpga tools with novel fpga-oriented moving target defense,** IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 3, pp. 665–678, 2019. DOI: 10.1109/TVLSI.2018.2879878.

[13] A. Sengupta, S. Bhadauria, and S. P. Mohanty, **TI-hls: Methodology for low cost hardware trojan security aware scheduling with optimal loop unrolling factor during high level synthesis,** IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 36, no. 4, pp. 655–668, 2017. DOI: 10.1109/TCAD.2016.2597232.

[14] P. Swierczynski, G. T. Becker, A. Moradi, and C. Paar, **Bitstream fault injections (bifi)–automated fault attacks against sram-based fpgas,** IEEE Transactions on Computers, vol. 67, no. 3, pp. 348–360, 2018. DOI: 10.1109/TC.2016.2646367.

[15] H. Mardani Kamali, K. Zamiri Azar, K. Gaj, H. Homayoun, and A. Sasan, **Lut-lock: A novel lut-based logic obfuscation for fpga-bitstream and asic-hardware protection,** in 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2018, pp. 405–410. DOI: 10.1109/ISVLSI.2018.00080.

[16] R. Karam, T. Hoque, S. Ray, M. Tehranipoor, and S. Bhunia, **Robust bitstream protection in fpga-based systems through low-overhead obfuscation,** in 2016 International Conference on ReConFigurable Computing and FPGAs (ReConFig), 2016, pp. 1–8. DOI: 10.1109/ReConFig.2016.7857187.

[17] E. Peterson, **Developing tamper-resistant designs with zynq ultrascale+ devices,** Xilinx, Tech. Rep., 2018. [Online]. Available: https://xilinx.com/support/documents/application_notes/xapp1323-zynq-usp-tamper-resistant-designs.pdf.

[18] M. Schmid, D. Ziener, and J. Teich, **Netlist-level ip protection by watermarking for lut-based fpgas,** in 2008 International Conference on Field-Programmable Technology, 2008, pp. 209–216. DOI: 10.1109/FPT.2008.4762385.

[19] S. Tajik, H. Lohrke, J.-P. Seifert, and C. Boit, **On the power of optical contactless probing: Attacking bitstream encryption of fpgas,** in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '17, Dallas, Texas, USA: Association for Computing Machinery, 2017, pp. 1661–1674, ISBN: 9781450349468. DOI: 10.1145/3133956.3134039. [Online]. Available: https://doi.org/10.1145/3133956.3134039.

[20] Nanopyramid: An Optical Scrambler Against Backside Probing Attacks, vol. ISTFA 2018: Conference Proceedings from the 44th International Symposium for Testing and Failure Analysis, International Symposium for Testing and Failure Analysis, Oct. 2018, pp. 280–289. DOI: 10.31399/asm.cp.istfa2018p0280. eprint: https://dl.asminternational.org/istfa/proceedings-pdf/ISTFA2018/81009/280/607688/istfa2018p0280.pdf. [Online]. Available: https://doi.org/10.31399/asm.cp.istfa2018p0280.

[21] E. Peterson, **Leveraging asymmetric authentication to enhance security-critical applications using zynq-7000 all programmable socs,** Xilinx, Tech. Rep., 2015. [Online]. Available: https://xilinx.com/content/dam/xilinx/support/documents/white_papers/wp468_asym-auth-zynq-7000.pdf.

[22] Microsemi, **User guide polarfire fpga security,** Microsemi, Tech. Rep., 2019. [Online]. Available: https://www.microsemi.com/document-portal/doc_view/1245814-polarfire-fpga-and-polarfire-soc-fpga-security-user-guide.

[23] R. Kuramoto, **Quickboot method for fpga design remote update,** Xilinx, Tech. Rep., 2014. [Online]. Available: http://www.xilinx.com/support/documentation/application_notes/xapp1081-quickboot-remote-update.pdf.

[24] H. Li, G. Du, C. Shao, L. Dai, G. Xu, and J. Guo, **Heavy-ion microbeam fault injection into sram-based fpga implementations of cryptographic circuits,** IEEE Transactions on Nuclear Science, vol. 62, no. 3, pp. 1341–1348, 2015. DOI: 10.1109/TNS.2015.2423672.

[25] J. Heiner, B. Sellers, M. Wirthlin, and J. Kalb, **Fpga partial reconfiguration via configuration scrubbing,** in 2009 International Conference on Field Programmable Logic and Applications, 2009, pp. 99–104. DOI: 10.1109/FPL.2009.5272543.

[26] T. Güneysu, I. Markov, and A. Weimerskirch, **Securely sealing multi-fpga systems,** in Proceedings of the 8th International Conference on Reconfigurable Computing: Architectures, Tools and Applications, ser. ARC'12, Hong Kong, China: Springer-Verlag, 2012, pp. 276–289, ISBN: 9783642283642. DOI: 10.1007/978-3-642-28365-9_23. [Online]. Available: https://doi.org/10.1007/978-3-642-28365-9_23.

[27] F. Schellenberg, D. R. Gnad, A. Moradi, and M. B. Tahoori, **An inside job: Remote power analysis attacks on fpgas,** in 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), 2018, pp. 1111–1116. DOI: 10.23919/DATE.2018.8342177.

[28] M. Zhao and G. E. Suh, **Fpga-based remote power side-channel attacks,** in 2018 IEEE Symposium on Security and Privacy (SP), 2018, pp. 229–244. DOI: 10.1109/SP.2018.00049.

[29] Xilinx, **Security monitor ip core product brief,** Product Brief, 2015. [Online]. Available: https://www.xilinx.com/support/documents/product-briefs/security-monitor-ip-core-product-brief.pdf.

[30] Xilinx, **Ultrascale architecture and product data sheet: Overview,** Product Data Sheet, 2022. [Online]. Available: https://www.mouser.com/datasheet/2/903/ds890_ultrascale_overview-1591529.pdf.

[31] M. M. Alam, M. Tehranipoor, and D. Forte, **Recycled fpga detection using exhaustive lut path delay characterization and voltage scaling,** IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2897–2910, 2019. DOI: 10.1109/TVLSI.2019.2933278.

[32] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, **Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain,** Proceedings of the IEEE, vol. 102, no. 8, pp. 1207–1228, 2014. DOI: 10.1109/JPROC.2014.2332291.