СЕКЦИЯ «АКТУАЛЬНЫЕ ВОПРОСЫ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЭЛЕКТРОННОЙ ЭКОНОМИКИ» (НА ИНОСТРАННЫХ ЯЗЫКАХ)

UDC 621.396 + 004.4

1. THE PROBLEM OF FPGA CLONING

Burko L. A., Master's degree student, group 455801

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Liakh Y.V. – Senior Lecturer

Annotation. This article explores the challenges and security risks associated with FPGA cloning, where unauthorised parties replicate FPGA-based designs. It describes the impact on intellectual property, competitive advantage, and security. Various countermeasures, including bitstream encryption, physical unclonable functions (PUFs), watermarking, and blockchain for IP protection, are presented. The study also highlights emerging trends in FPGA security to combat cloning and unauthorised replication.

Keywords. FPGA cloning, intellectual property protection, bitstream encryption, PUF, watermarking, hardware security, anti-tamper mechanisms, supply chain security, blockchain, runtime authentication, hardware metering, FPGA security challenges, reverse engineering prevention, counterfeit detection.

Richard Hamming, in his well-known speech "You and Your Research", mentioned himself asking scientists at Bell Labs a simple question: "What are the important problems of your field?" In FPGA (Field-programmable gate arrays) sphere scientists and engineers ask the same question: what are the important problems in FPGA engineering? There are many answers: inherent parallelism, timing closure, synchronisation and metastability, very complex hard silicon IP, build times limit iteration cycle, cost of chips and their sizes, and many other unknown words for simple users. FPGA engineering has many complex and at the same time interesting challenges, but engineers have found the ways to simplify solutions over time. They use hardware description languages (HDLs) like Verilog or VHDL and high-level synthesis (HLS) tools to make parallelism easier to manage, use double-flop synchronisers and clock domain crossing (CDC) techniques to handle signal transitions safely, choose the right FPGA for the job – there are low-cost, power-efficient options for simpler applications.

FPGA engineers and scientists spend years developing innovative architectures, optimising performance, and fine-tuning designs. They solve complex problems like timing closure, power efficiency, and hardware-software co-design. Their work results in cutting-edge FPGA-based solutions for industries like telecommunications, AI, and embedded systems. But then cloning comes. Competitors or counterfeiters extract bitstreams, reverse-engineer hardware, or replicate entire FPGA-based products – often without understanding the effort behind them.

FPGAs are widely used in various industries due to their flexibility, performance, and reconfigurability. Engineers and scientists invest significant effort into designing FPGA-based systems, optimising them for efficiency, security, and reliability. However, one major challenge that has emerged in this field is FPGA cloning, where unauthorised parties replicate FPGA-based designs without proper authorisation. This not only results in intellectual property (IP) theft but also introduces serious security risks. This article describes the problems associated with FPGA cloning, the impact on the industry, and the countermeasures that engineers can implement to mitigate these threats. Instead of reviewing a specific topic on FPGA-based system design, we examine the FPGA supply and demand model in Figure 1, the key players in the FPGA market, and the security and trust challenges they face [1].

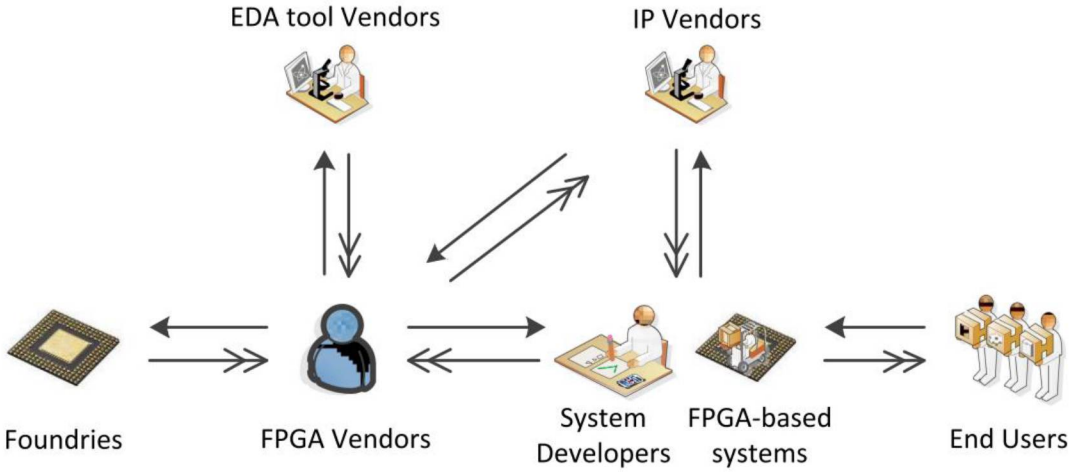

Figure 1 – The description of the supply-and-demand flows in the FPGA-based system market. "→": service requesting; "→→": service providing [1]

For instance, the intellectual property (IP) infringement to high-end chips such as cloning and reverse engineering brings the loss of approximately $250 billion dollars and 750,000 jobs annually. It was reported by IEEE Spectrum that in 2007 the Syrian radar defense system did not provide necessary warning against the guided missiles from Israel. According to scientists' analysis, it happened because a commercial chip used in Syrian radar defense systems was implanted with a hardware Trojan or backdoor in the fabrication process.

The 2004 paper by Wollinger et al. is the first survey on FPGA security covering the following three topics: the advantages of using FPGA for cryptographic applications; the security vulnerabilities and existing attacks to FPGAs; and the available countermeasures against these attacks [1, 2].

FPGA cloning occurs when attackers extract the configuration bitstream of an FPGA, reverse-engineer its design, and replicate the system. Unlike ASICs, which have a fixed hardware structure, FPGAs use a reconfigurable fabric that loads a bitstream to define the circuit's functionality. This bitstream, however, is highly vulnerable to interception, duplication, and tampering.

Scientists and engineers dedicate years to developing complex FPGA architectures, ensuring optimal performance, and securing their systems against various threats. However, once a design is finalised and deployed, it becomes an attractive target for attackers who aim to clone it for financial gain or malicious purposes. Cloning leads to direct financial losses for developers and compromises the security of applications using the cloned technology.

Cloning allows malicious actors to bypass this effort, directly copying a working solution without investing in development. Companies that innovate in FPGA technology lose their competitive edge when their designs are copied and sold at lower prices. Cloned FPGA-based systems may contain vulnerabilities due to a lack of proper verification and security measures, leading to risks in sensitive applications such as military, financial, and industrial sectors. Unauthorised cloned FPGAs may enter the supply chain, potentially affecting system reliability and introducing unknown security backdoors. The global semiconductor industry loses billions of dollars due to IP theft and counterfeiting, which stifles innovation and reduces incentives for new research and development efforts. Enforcing intellectual property rights in FPGA technology can be difficult due to jurisdictional differences, making it challenging for companies to take legal action against counterfeiters [2].

The consequences of FPGA cloning are severe and multifaceted:

1. Intellectual property theft.
2. Loss of competitive advantage.
3. Compromised security.
4. Supply chain risks.
5. Economic consequences.
6. Legal and Regulatory Challenges.

FPGA vendors and system developers spend substantial resources in research and development. To protect FPGA designs from cloning and unauthorised use, engineers can implement several countermeasures.

1. Bitstream encryption. Encrypting the FPGA bitstream ensures that even if an attacker intercepts it, they cannot deploy it on another device without the correct decryption key. This method is widely used in modern FPGA families from Xilinx and Intel [3].

In Figure 2a FPGA replay attacks are still successful even if the bitstream is locked and the key (PUF response) is reconfigured to recompute the new license (license2) in the binding mechanisms. In Figure 2b

FPGA replay attacks are defeated when both the locking mechanism and the key (PUF response) are reconfigured to recompute the new license (license2) in the binding mechanism.

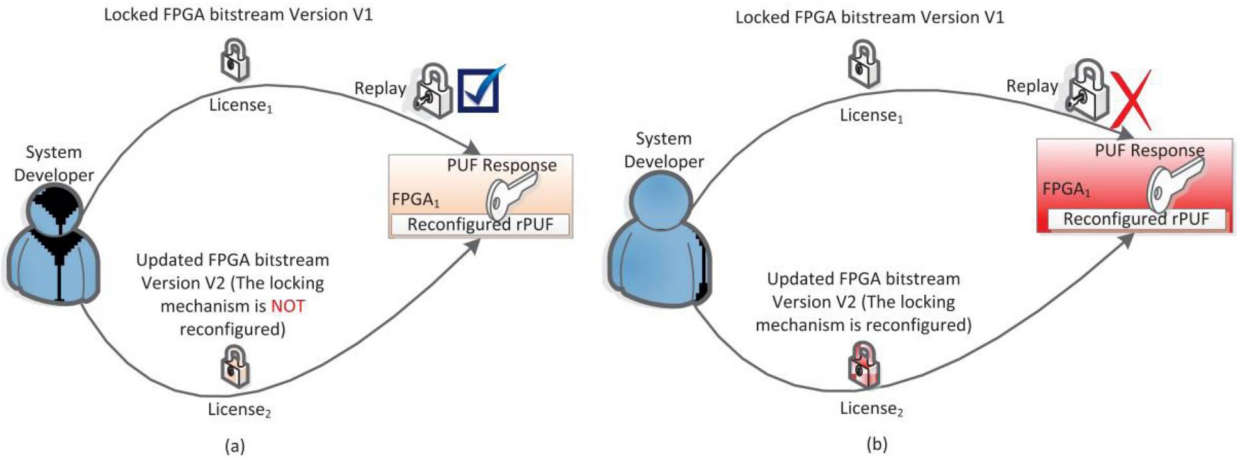

Figure 2 – Effect of Reconfiguration on FPGA Replay Attacks: Success vs. Prevention [1, 3]

2. Physical unclonable functions (PUFs), a simple PUF circuit is shown in Figure 3. PUFs exploit inherent variations in silicon manufacturing to generate unique device identifiers. By integrating PUF-based authentication, engineers can bind bitstreams to specific FPGA hardware, preventing unauthorised copies from functioning [4,5].

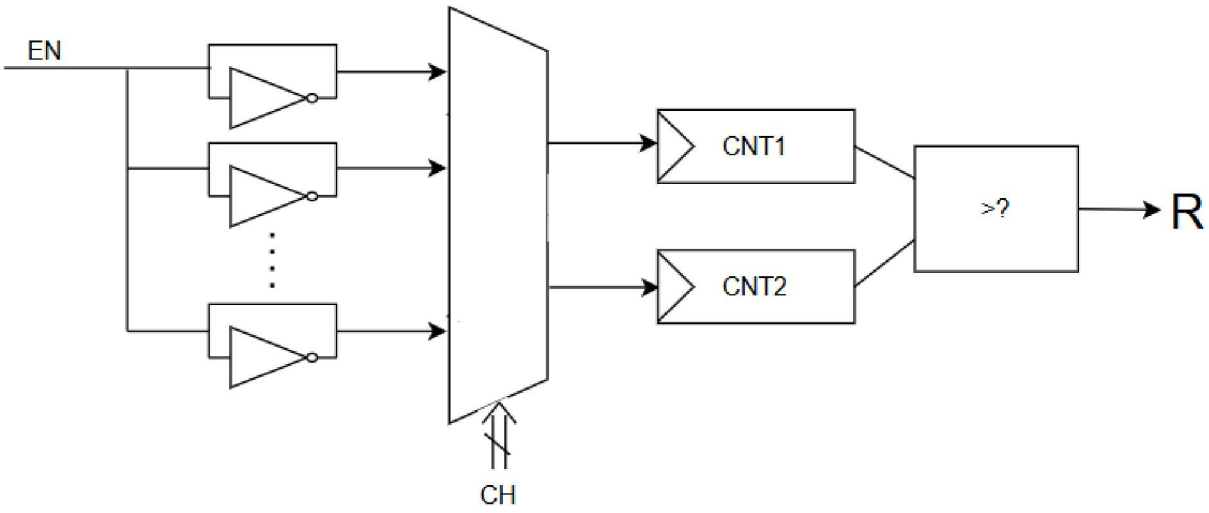

Figure 3 – The structure of RO PUF

3. Watermarking and Fingerprinting. Watermarking techniques embed hidden signatures within the FPGA design to prove ownership. Fingerprinting extends this by embedding unique identifiers in each distributed copy, allowing engineers to trace unauthorised duplicates.

4. Anti-Tamper Mechanisms. Secure boot processes, runtime authentication, and integrity checks can prevent unauthorised bitstream modifications and cloning attempts.

5. Hardware Obfuscation. By designing FPGA logic with redundant or misleading elements, engineers can make reverse engineering more challenging, reducing the effectiveness of cloning attempts.

6. Secure Supply Chain Practices. Ensuring a trusted manufacturing process by working with verified suppliers and implementing supply chain audits can help prevent overbuilding and unauthorised production of FPGA-based designs.

7. Blockchain for IP Protection. Blockchain technology can be used to record and verify FPGA designs, ensuring authenticity and traceability throughout the design lifecycle.

8. Hardware Metering. Implementing hardware metering techniques can help track the usage of FPGA designs, ensuring that unauthorised duplications are detected and prevented.

9. Runtime Authentication and Remote Attestation. Secure authentication protocols can be implemented to verify FPGA integrity at runtime, ensuring that only authorised configurations are loaded onto the device.

The battle against FPGA cloning is an ongoing challenge that requires continuous research and the development of advanced security techniques. As FPGAs become more prevalent in cloud computing, artificial intelligence, and edge computing applications, the need for robust protection mechanisms will increase. Emerging technologies such as AI-based anomaly detection, post-quantum cryptography, and trusted execution environments (TEEs) may offer new ways to strengthen FPGA security against cloning and unauthorised replication.

Additionally, collaboration between industry leaders, academia, and regulatory bodies is crucial in establishing standards and best practices for FPGA security. Governments and organisations should also invest in awareness programs and legal frameworks to address the growing threat of hardware counterfeiting and intellectual property theft.

FPGA cloning poses a significant challenge to the industry, threatening innovation, security, and financial sustainability. However, engineers can adopt robust security measures such as encryption, PUFs, watermarking, and obfuscation to protect their designs. Furthermore, new advancements in blockchain, hardware metering, and runtime authentication provide additional layers of security. As FPGA technology continues to evolve, securing these systems against cloning and unauthorised access will remain a priority to ensure long-term trust and reliability in FPGA-based applications. By staying ahead of potential threats and implementing proactive security measures, the industry can safeguard its intellectual property and maintain a secure FPGA ecosystem.

Cloning undermines innovation, leads to security risks, and devalues genuine engineering work. Engineers must combat this with encryption, authentication, and unique hardware IDs to protect their designs from unauthorised duplication.

References:

1. Security on FPGAs: State-of-the-art implementations and attacks. / T. Wollinger, J. Guajardo, and C. Paar. // ACM Trans. Embed. Comput. Syst. 3, 3 (2004), – p. 534–574.

2. Recent Attacks and Defenses on FPGA-based Systems / Jiliang Zhang and Gang Qu. // ACM Trans. Reconfigurable Technol. Syst. 12, 3, Article 14 (August 2019), – p. 24 pages.

3. Extracting secret keys from integrated circuits. / J. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas // IEEE Trans. Very Large Scale Integr. Syst. 13, 10 (2005), – p. 1200–1205.

4. Reconfigurable binding against FPGA replay attacks / J. Zhang, Y. Lin, and G. Qu. // ACM Trans. Des. Autom. Electron. Syst. 20, 2 (2015)

5. Physical unclonable functions for device authentication and secret key generation / G. E. Suh and S. Devadas. // In Proceedings of the ACM/IEEE Design Automation Conference. – p. 9–14.