DOI: 10.35598/mcfpga.2025.022

Application of Physical Unclonable Functions (PUFs) to Provide Hardware Trust and Counter Spoofing in ATC/STOL/IFF Systems Under Noisy Channels and Non-Deterministic Delays

Oleksandr Vorgul
Scientific adviser
ORCID 0000-0002-7659-8796
dept.Microprocessor Technologies and System
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
oleksandr.vorgul@nure.ua

Anton Serikov
dept.Microprocessor Technologies and System
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
anton.serikov@nure.ua

***Abstract*— The article considers the problem of ensuring trust in equipment and data in critical air traffic control (ATC), airspace control (ASC) and identification friend or foe (IFF) systems operating in complex electronic environments. The main attention is paid to the threats of spoofing and equipment compromise. The application of Physical Unclonable Functions (PUF) as a key hardware technology for creating a root of trust (Root of Trust). The principles of PUF operation, their integration into onboard and ground equipment, and the mechanisms for their use for generating and protecting cryptographic keys, authenticating devices, and ensuring secure boot are analyzed in detail. It is shown that PUFs provide a fundamentally new level of physical invulnerability to cloning and key extraction, significantly increasing the resistance of systems to spoofing and unauthorized access, even in conditions of noisy communication channels and non-deterministic signal propagation delays.**

Keywords*— *Physical Unclonable Functions, PUF, ATC, Airspace Control, Stol, Identification Friend Or Foe, IFF, Spoofing, Hardware Trust, Root Of Trust, Secure Boot, Hardware Security, Noisy Channels, Non-Deterministic Delays.

I. INTRODUCTION

Air traffic control (ATC), airspace monitoring (ASM), and identification friend or foe (IFF) systems are critical infrastructure for national security. Their reliable and secure operation depends on data integrity, authenticity of information sources, and resistance to malicious influences [1, 2]. The operating conditions of these systems are particularly challenging: a dense electronic environment with multiple protocols (Mode S, ADS-B, military IFF standards), random and intentional interference, and non-deterministic propagation delays of pulse signals [3]. In such conditions, traditional, primarily software-based approaches to ensuring security, especially to protecting cryptographic keys and device authentication, demonstrate their vulnerability to attacks, including spoofing, physical opening and extraction of keys, and the introduction of malicious code [4, 5]. There is an urgent need for hardware-centric solutions capable of providing a fundamental level of trust in the equipment and its functioning. Physical Unclonable Functions (PUFs) offer unique properties that make them a promising technology for addressing these challenges. The objective of this paper is to analyze the application of PUFs to provide hardware trust and counter key security threats in ATC/STOP/IFF systems operating in noisy channels and non-deterministic latency environments.

II. CHARACTERISTICS OF THE OPERATING CONDITIONS OF THE ATC, STOL AND IFF SYSTEMS

ATC, STOL and IFF systems operate in a highly dynamic , distributed and potentially hostile environment. Their key features include:

- Distributed: Interaction of multiple geographically dispersed objects: aircraft (onboard IFF transponders, navigation systems), ground radar stations (RLS), IFF interrogators , ATC control centers, repeaters [1, 6].
- Real-time mode: The need to process and transmit critical data (coordinates, identification, commands) with minimal and predictable delay to ensure flight safety and rapid response [2].
- Complex Electronic Environment: Simultaneous use of multiple radio frequency communication, navigation and identification protocols (e.g., secondary radars, ADS-B, tactical communications channels), resulting in mutual interference and airwave saturation [3].
- Presence of interference: The impact of both random electromagnetic interference (atmospheric , industrial) and intentional interference (electronic suppression) [3, 7].
- Non-deterministic delays: Variability in signal propagation times due to multipath, retransmissions, channel congestion, and processing, which is critical for synchronization and time-sensitive protocols [3, 8].
- High security requirements: Systems are a target for attackers, and the consequences of successful attacks (spoofing, false targets, control disruption) are catastrophic [1, 4, 5].

III. Key safety issues of ATC/STOL/IFF systems

In the context of complex operating conditions, the following key safety issues stand out:

- IFF/Transponder Spoofing: An attacker generates false "friend" responses, impersonating a legitimate aircraft or ground object, using protocol vulnerabilities or intercepted data [4, 5, 9]. Traditional non-cryptographic IFF methods are vulnerable to interception and replay.
- Equipment compromise: Physical access to remote or poorly secured ground assets (radars, interrogators) or attempts to introduce counterfeit/compromised onboard equipment to steal keys, modify firmware or introduce a backdoor [1, 4, 5].
- Vulnerability of encryption and authentication keys: Storing long-term cryptographic keys in memory (ROM, flash) makes them vulnerable to extraction by physical opening or using exploits. Compromised keys allow spoofing and data interception [4, 5, 10].
- Software and Configuration Integrity Compromise: The possibility of unauthorized modification of the firmware or configuration of onboard terminals, ground stations, or control centers, which may lead to incorrect operation, data leakage, or malicious actions [1, 5].
- Difficulty of authentication in noisy environments with delays: Traditional authentication methods that are time-sensitive or based on simple identifiers become unreliable in the presence of noise and variable delays [3, 8].

IV. Hardware security mechanisms: Physical Unclonable Functions (PUF)

Physical Unclonable Functions (PUFs) are hardware structures that exploit the inevitable microscopic variations in semiconductor manufacturing process parameters (oxide thickness, doping, transistor channel length, etc.) to generate a unique, unpredictable, but stable "digital fingerprint" for each specific chip instance [10, 11, 12]. Operating principle and key properties:

- Mechanism of operation: PUF is implemented as a specialized circuit on a crystal. When an electrical stimulus (a "challenge") is applied, the circuit produces an output signal (a "response"), which is deterministic for a given chip, but externally unpredictable, since it is determined by a unique combination of physical variations in its structure [11, 12].
- Uniqueness: PUF responses are statistically unique for each chip instance, even those manufactured using the same technology on the same wafer [10, 11, 12] .
- Unclonability: It is physically impossible to create an exact copy of a chip with identical physical variations and hence identical PUF responses [10, 11, 12].
- Unpredictability: The value of a key generated from a PUF is not explicitly stored in memory. It is dynamically generated on each request and destroyed after use. Even knowing the exact design of a PUF, it is impossible to predict or compute its response without access to the specific physical chip [10, 11, 12].
- Attack Resistance: The properties of PUFs make them resistant to a wide range of attacks, including many side-channel attacks (power analysis, timing attacks) and physical attacks (probing, opening the case) aimed at extracting keys, since the key as such is not present statically [10, 11, 12].

Implementation: PUFs can be implemented on various hardware platforms, but are most effectively integrated into FPGAs and specialized secure microcontrollers (Secure Elements, Hardware Security Modules - HSM). Modern secure FPGAs (e.g. Xilinx Zynq UltraScale+, Intel Agilex) often contain built-in PUFs or easily allow the integration of PUF IP cores [2, 12].

V. Effect of using PUF in ATC/STOL/IFF systems

The implementation of PUF in on-board (IFF transponders, navigation systems) and ground (IFF interrogators, radars, processing centers) equipment of ATC/STOL/IFF systems allows achieving the following key effects in conditions of noise and non-deterministic delays:

- Creating a Hardware Root of Trust (Hardware Root of Trust): PUF serves as a unique and non-extractable source of entropy for generating cryptographic keys directly on the chip [10, 11, 12]. This forms an unshakable basis for building chains of trust.
- Reliable protection of cryptographic keys: Encryption and authentication keys for IFF protocols (including cryptographically strong modes), protection of ATC communication channels and KVP telemetry are generated and used dynamically, without being stored in vulnerable memory. This dramatically increases resistance to physical hacking and equipment compromise [4, 5, 10, 12]. The key can only be compromised by stealing a specific physical device.
- Effective counteraction to spoofing: The uniqueness and non-extractability of the key associated with the PUF *of a specific* transponder or interrogator makes it economically and technically unprofitable to create exact clones to generate valid "own" responses [4, 5, 9]. Cryptographic authentication based on PUF keys provides reliable verification of the authenticity of the signal source.
- Ensuring secure boot and software integrity: Keys derived from (or signed using) PUFs are used to verify the digital signatures of bootloaders, firmware, and FPGA configurations before they are executed [2, 10, 12]. This ensures that the device only runs trusted, untampered code, preventing the introduction of malware, even after crashes or attacks.
- Delay-tolerant device authentication: Challenge-response authentication protocols based on unique PUF responses are cryptographically strong and do not directly depend on absolute signal propagation time (although the protocol must account for acceptable delay variations) [3, 8, 10]. The control center can authenticate *a specific* ground station by its unique PUF response despite interference and delay variations.
- Physical invulnerability to cloning: The unclonability property of PUF makes it impossible to create a functionally identical and trusted copy of a critical system component (transponder, radar processing

board) without possessing the original chip with its unique physical characteristics [10, 11, 12].

VI. Conclusions

The use of Physical Unclonable Functions (PUF) offers a fundamentally new approach to solving fundamental security problems in ATC, STOL and IFF systems, especially in complex electronic environments with noisy channels and non-deterministic delays. Integrating PUF into the hardware platform of onboard and ground equipment allows for the creation of a reliable Hardware Root of Trust, ensuring:

Dynamic generation and protection of cryptographic keys, eliminating their static storage and extraction during physical hacking.

A qualitatively new level of protection against spoofing due to the rigid binding of cryptographic authentication to the unique physical properties of a specific chip in the transponder or interrogator.

Guaranteeing software and configuration integrity through secure boot mechanisms based on PUF keys.

The ability to securely authenticate devices using cryptographically strong protocols that are resistant to latency variations.

Physical invulnerability to cloning of critical system components.

Thus, PUFs act not just as a key protection technology, but as a fundamental element for building stable, trusted and physically protected airspace management and control systems in today's saturated and potentially hostile electronic environment. Their implementation is a strategic direction for improving the security of critical aviation infrastructure.

References

[1] Kayton , M., & Fried , W. R. (Eds .). (1997). *Avionics navigation systems* (2nd ed .). John Wiley & Sons .

[2] Xilinx . (2022). *Security Solutions in Zynq UltraScale+ MPSoCs* (White Paper WP509). Retrieved from https://www.xilinx.com/support/documentation/white_papers/wp509-ultrascale-plus-security.pdf

[3] Stevens, M. C. (1988). *Secondary surveillance radar* . Artech House.

[4] Strohmeier, M., Schafer, M., Lenders , V., & Martinovic , I. (2014). *Realities and challenges of nextgen air traffic management : The case of ADS-B* . IEEE Communications Magazine , 52(5), 111–118.

[5] McCallie , D., Butts , J., & Mills , R. (2011). *Security analysis of ADS -B implementation in the next generation air transportation system* . International Journal of Critical Infrastructure Protection , 4(2), 78–87.

[6] International Civil Aviation Organization (ICAO). (2018). *Doc 4444: Procedures for Air Navigation Services — Air Traffic Management* (16th ed .).

[7] Pace, P. E. (2009). *Detecting and classifying low probability of intercept radar* (2nd ed .). Artech House .

[8] Kayton , M. (Ed .). (1990). *Navigation : Land , sea , air , and space* . IEEE Press .

[9] Costin , A., & Francillon , A. (2012). *Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices* . Black Hat USA.

[10] Maiti, A., & Schaumont , P. (2011). *Physical unclonable functions and applications : A tutorial* . Proceedings of IEEE , 99(7), 1126–1141.

[11] Gassend , B., Clarke , D., van Dijk , M., & Devadas , S. (2002). *Silicon physical random functions* . Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS '02), 148–160.

[12] Herder , C., Yu , M., Koushanfar , F., & Devadas , S. (2014). *Physical unclonable functions and applications : A review* . Proceedings of the IEEE, 102(8), 1126–1141.

[13] GOST R 58766-2019. Aviation systems. Information security requirements. Data integrity and authenticity control.

[14] Skorobogatov , S. P. (2011). *Physical attacks and tamper resistance* . In *Introduction to Hardware Security and Trust* (pp . 143–173). Springer .

[15] RTCA. (2020). *DO-356A: Airworthiness Security Methods and Considerations *. Radio Technical Commission for Aeronautics