INTISARI

IMPLEMENTASI *ARBITER PHYSICAL UNCLONABLE FUNCTION* PADA *FIELD PROGRAMMABLE GATE ARRAY* SEBAGAI *AUTHENTICATOR* PERANGKAT BERBASIS *CHALLENGE-RESPONSE*

Oleh

Achmad Husein
21/473553/PA/20403

Keamanan perangkat keras menjadi pondasi kritis dalam era digital seiring meningkatnya ancaman serangan siber sehingga membutuhkan keamanan yang andal dan efisien. Sistem autentikasi dapat menjadi salah satu solusi keamanan perangkat. Namun, sistem keamanan berbasis perangkat lunak memiliki kerentanan terhadap serangan seperti *Man-in-the-Middle* melalui metode *cloning*, *counterfeiting*, dan *backdoor* yang dapat menyalin dan mencuri data melalui memori. Penelitian ini bertujuan untuk membuat sistem keamanan berbasis perangkat keras yang mengimplementasikan *Arbiter Physical Unclonable Function* (PUF) pada *Field Programmable Gate Array* (FPGA) sebagai sistem autentikasi perangkat berbasis *challenge-response* yang aman dan efisien.

Sistem dirancang menggunakan FPGA Nexys A7-100T dengan arsitektur *Arbiter PUF* 8 *stage* yang memanfaatkan perbedaan *delay path* mikroskopis dari proses manufaktur untuk menghasilkan *response* unik dan tidak dapat dikloning. Sistem autentikasi ini terintegrasi dengan modul komunikasi UART untuk koneksi PC dan FPGA, database SQLite untuk penyimpanan 256 *Challenge-Response Pair* (CRP), dan antarmuka pengguna *Graphical User Interface* (GUI) berbasis *Python* untuk proses *enrollment* dan *verification*. Hasil pengujian menunjukkan distribusi *uniformity* sebesar 44,53% bit '0' dan 55,47% bit '1' dengan deviasi 5,47% dari distribusi ideal. Pengujian *randomness* menggunakan NIST *Statistical Test Suite* menunjukkan sistem lulus seluruh pengujian dengan *p-value Runs Test* sebesar 0,34 dan *Serial Test* (*m*=3) sebesar 0,27 dan 0,66, serta *Serial Test* (*m*=4) sebesar 0,11 dan 0,10, semuanya di atas threshold 0,01. Implementasi sangat ringan dengan utilisasi LUT 0,15% (94 dari 63.400), Flip-Flop 0,06% (78 dari 126.800), dan konsumsi daya total hanya 0,092 W. Dengan demikian, implementasi *Arbiter PUF* pada FPGA terbukti efektif sebagai sistem autentikasi perangkat keras yang aman karena memiliki kualitas CRP yang bagus serta efektif penggunaan sumber daya logika dan konsumsi daya.

Kata kunci: *Arbiter PUF*, Autentikasi Perangkat, *Challenge-Response Pair,* FPGA

ABSTRACT

IMPLEMENTATION OF AN ARBITER PHYSICAL UNCLONABLE FUNCTION ON AN FIELD PROGRAMMABLE GATE ARRAY FOR CHALLENGE-RESPONSE BASED DEVICE AUTHENTICATION

By

Achmad Husein
21/473553/PA/20403

Hardware security has become a critical foundation in the digital era as cyber-attack threats increase, requiring reliable and efficient security. Authentication systems can be one of the device security solutions. However, software-based security systems have vulnerabilities to attacks such as Man-in-the-Middle through cloning, counterfeiting, and backdoor methods that can copy and steal data through memory. This research aims to develop a hardware-based security system that implements Arbiter Physical Unclonable Function (PUF) on Field Programmable Gate Array (FPGA) as a secure and efficient challenge-response-based device authentication system.

The system is designed using Nexys A7-100T FPGA with an 8-stage Arbiter PUF architecture that exploits microscopic delay path differences from the manufacturing process to generate unique and unclonable responses. This authentication system is integrated with UART communication modules for PC-FPGA connection, SQLite database for storing 256 Challenge-Response Pairs (CRPs), and a Python-based graphical user interface (GUI) for enrollment and verification processes. Test results show a uniformity distribution of 44.53% '0' bits and 55.47% '1' bits with a 5.47% deviation from the ideal distribution. Randomness testing using the NIST Statistical Test Suite shows the system passes all tests with a Runs Test p-value of 0.34 and Serial Test (m=3) p-values of 0.27 and 0.66, and Serial Test (m=4) p-values of 0.11 and 0.10, all above the 0.01 threshold. The implementation is highly lightweight with LUT utilization of 0.15% (94 out of 63,400), Flip-Flop utilization of 0.06% (78 out of 126,800), and total power consumption of only 0.092 W. Thus, the implementation of Arbiter PUF on FPGA proves to be effective as a secure hardware authentication system due to its excellent CRP quality and efficient use of logic resources and power consumption.

Keywords: *Arbiter PUF*, *Device Authentication*, *Challenge-Response Pair, FPGA*