UNIVERSITAS
GADJAH MADA
**Implementasi Hardware Signature Authenticator Berbasis Algoritma ECDSA Terakselerasi SHA-256 Engine
Pada FPGA**
Irfansyah Peradeniya, Prof. Dr. Ir. Jazi Eko Istiyanto, M.Sc., IPU., ASEAN Eng.; Oskar Natan, S.ST., M.Tr.T., Ph.D.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN ..... **ii**
PERNYATAAN BEBAS PLAGIASI ..... **iii**
KATA PENGANTAR ..... **iv**
DAFTAR ISI ..... **vi**
DAFTAR GAMBAR ..... **viii**
DAFTAR TABEL ..... **ix**
INTISARI ..... **x**
ABSTRACT ..... **xi**
BAB I PENDAHULUAN **1**
1.1. Latar Belakang 1
1.2. Rumusan Masalah 4
1.3. Batasan Masalah 4
1.4. Tujuan Penelitian 4
1.5. Manfaat Penelitian 5
1.6. Metodologi Penelitian 5
1.7. Sistematika Penulisan 7
BAB II TINJAUAN PUSTAKA **8**
2.1. Hardware Signature Authenticator 8
2.1.1. IC-Security 10
2.2. Elliptic Curve Digital Signature Algorithm 11
2.2.1. Pembuatan Tanda Tangan 14
2.2.2. Verifikasi Tanda Tangan 15
2.3. Field Programable Gate Array 16
2.3.1. Xilinx Ultrascale+ MPSOC XCZU3EG 17
2.3.2. Verilog 18
2.4. Secure Hashing Algorithm 19
2.4.1. Pustaka SHA256 Verilog 22
2.5. Petalinux 23
2.5.1. Pustaka Kriptografi OpenSSL 25
2.6. Model Akselerasi Hybrid Hardware-Software 26
2.7. Korelasi Penelitian Terdahulu 27
BAB III METODE PENELITIAN **31**
3.1. Analisis Sistem 31
3.2. Tahapan Penelitian 32
3.3. Rancangan Implementasi 33
3.3.1. Arsitektur Hardware-Software Co-Design 34
3.3.2. Rancangan Top Module SHA256 Engine pada PL 35
3.3.3. Rancangan Aplikasi Userspace pada PS 38
3.4. Pengujian Sistem 40
3.5. Alat dan bahan 44
BAB IV IMPLEMENTASI **46**
4.1. Gambaran Implementasi 46
4.1.1. Implementasi Fisik Perangkat Keras 47
4.2. Implementasi SHA256_Engine 48
4.2.1. Input Output 48

Implementasi Hardware Signature Authenticator Berbasis Algoritma ECDSA Terakselerasi SHA-256 Engine
Pada FPGA
Irfansyah Peradeniya, Prof. Dr. Ir. Jazi Eko Istiyanto, M.Sc., IPU., ASEAN Eng.; Oskar Natan, S.ST., M.Tr.T., Ph.D.
Universitas Gadjah Mada, 2025 | Diunduh dari http://etd.repository.ugm.ac.id/

4.2.2. Implementasi FSM 49
4.2.3. Implementasi Protokol AXI_Stream 52
4.2.4. Implementasi Partial Data Processor 53
4.2.5. Implementasi Padding dan Bit Counter 55
4.3. Implementasi Block Design dan Interkoneksi AXI 57
4.4. Implementasi PetaLinux pada Processing System 58
4.4.1. Konfigurasi Kernel dan Rootfs 59
4.4.2. Device Tree dan IOMMU 60
4.4.3. First Stage Bootloader dan Boot Image 62
4.5. Implementasi Perangkat Lunak HSA 64
4.5.1. Transfer DMA menggunakan VFIO 65
4.5.2. Implementasi Fungsi Hardware Hash 66
4.5.3. Implementasi IC-Security 67
4.5.4. Integrasi dengan ECDSA OpenSSL 68
4.5.5. Aplikasi Web dan Antarmuka Pengguna 69
4.6. Pengujian Sistem 71
4.6.1. Simulasi SHA256_Engine 71
4.6.2. Sintesis PL dengan Vivado 72
4.6.3. Pengujian Validitas SHA256_Engine 74
4.6.4. Dataset Uji 74
4.6.5. Pengukuran Latensi dan Throughput 75
4.6.6. Pengukuran Beban CPU dan Resource FPGA 76
4.6.7. Pengukuran Power Consumption 77
BAB V HASIL DAN PEMBAHASAN 78
5.1. Analisis Validitas SHA256_Engine 78
5.2. Analisis Throughput dan Performa 80
5.2.1. Throughput SHA256_Engine 80
5.2.2. Kecepatan Signing dan Verifikasi HSA 82
5.3. Analisis Sumber Daya 84
5.3.1. Sumberdaya Processing System 84
5.3.2. Sumberdaya Programmable Logic 85
5.4. Analisis Power Consumption 87
5.5. Komparasi dan Pembahasan 88
BAB VI KESIMPULAN DAN SARAN 91
6.1. Kesimpulan 91
6.2. Saran 93
DAFTAR PUSTAKA 94