UNIVERSITAS
GADJAH MADA
LOGIC LOCKING KUNCI DINAMIS PER-SESI BERBASIS ALGORITMA HMAC KEY DERIVATION FUNCTION (HKDF) TERINTEGRASI AUTENTIKASI DS28E50 PADA MIKROKONTROLER
Mellia Putri, Prof. Dr. Ir. Jazi Eko Istiyanto, M.Sc.; Oskar Natan, S.ST., M.Tr.T., Ph.D.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

DAFTAR ISI

HALAMAN PENGESAHAN ii
PERNYATAAN BEBAS PLAGIASI iii
PRAKATA iv
DAFTAR ISI vi
DAFTAR GAMBAR ix
DAFTAR TABEL xi
INTISARI xii
ABSTRACT xiii
BAB I 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 3
1.3 Batasan Masalah 3
1.4 Tujuan Penelitian 4
1.5 Manfaat Penelitian 5
1.6 Metodologi Penelitian 5
1.7 Sistematika Penulisan 7
BAB II 9
2.1 *Logic Locking* 9
2.1.1 Prinsip dan mekanisme dasar 9
2.1.2 Pemodelan dan evaluasi berbasis RTL 11
2.2 Serangan *Oracle* pada *Logic Locking* 11
2.2.1 SAT *attack* 12
2.2.2 *Dishonest oracle* sebagai mekanisme pertahanan 13
2.3 Autentikasi Perangkat Keras Berbasis PUF 15
2.3.1 *Physically Unclonable Function* (PUF) 15
2.3.2 *Secure authenticator* DS28E50 16
2.4 Kriptografi HMAC dan SHA-3 17
2.5 Derivasi Kunci dan Manajemen Siklus Hidup 19
2.6 Platform Implementasi 21
2.6.1 Protokol komunikasi 1-*Wire* 22
2.6.2 Mikrokontroler STM32F103C8 23
2.7 Korelasi Penelitian Terdahulu 23
BAB III 26

UNIVERSITAS GADJAH MADA
LOGIC LOCKING KUNCI DINAMIS PER-SESI BERBASIS ALGORITMA HMAC KEY DERIVATION FUNCTION (HKDF)
TERINTEGRASI AUTENTIKASI DS28E50 PADA MIKROKONTROLER
Mellia Putri, Prof. Dr. Ir. Jazi Eko Istiyanto, M.Sc.; Oskar Natan, S.ST., M.Tr.T., Ph.D.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

3.1 Analisis Sistem 26
3.2 Alat dan Bahan 27
3.3 Tahapan Penelitian 29
3.4 Rancangan Model Sistem 30
3.4.1 Rancangan perangkat keras 31
3.4.2 Mekanisme autentikasi dan alur sesi 32
3.4.3 Rancangan KDF per sesi dan manajemen kunci 34
3.4.4 Rancangan *logic locking* pada ALU dengan variasi lebar bit 36
3.5 Rencana Implementasi Sistem 38
3.6 Metode Pengujian Sistem 40
3.6.1 Pengujian fungsionalitas sistem secara *end-to-end* 40
3.6.2 Pengujian keunikan dan independensi kunci sesi 41
3.6.3 Analisis ketahanan terhadap serangan SAT 43
3.6.4 Pengujian *corruptibility* rangkaian ALU dengan variasi lebar bit 46
3.6.5 Pengujian keamanan siklus hidup kunci 48
3.6.6 Pengujian *overhead* sumber daya dan *timing* 50
BAB IV 52
4.1 Gambaran Implementasi 52
4.2 Implementasi Perangkat Keras 53
4.3 Implementasi *Firmware* STM32 55
4.3.1 Implementasi protokol komunikasi 1-*Wire* dan *driver* DS28E50. 56
4.3.2 Pembacaan *memory page* dan eksekusi *challenge* TRNG 57
4.3.3 Komputasi autentikasi internal 58
4.3.4 Alur autentikasi dan *handshake* serial dengan PC 59
4.3.5 Implementasi derivasi kunci 61
4.3.6 Implementasi *secure zeroize* dan manajemen *buffer* sensitif 63
4.4 Implementasi Perangkat Lunak PC *Verifier* 65
4.4.1 *Handshake* sinkronisasi serial 65
4.4.2 Ekstraksi *frame* DATA dan verifikasi HMAC 66
4.4.3 Injeksi kunci ke simulasi verilog 67
4.5 Implementasi *Logic Locking* ALU 8-bit 68
4.5.1 Implementasi *golden* ALU 69
4.5.2 Implementasi ALU terkunci dengan XOR *key-gate* 70
4.5.3 Implementasi *testbench* dan injeksi kunci sesi 71

UNIVERSITAS
GADJAH MADA
LOGIC LOCKING KUNCI DINAMIS PER-SESI BERBASIS ALGORITMA HMAC KEY DERIVATION FUNCTION (HKDF) TERINTEGRASI AUTENTIKASI DS28E50 PADA MIKROKONTROLER
Mellia Putri, Prof. Dr. Ir. Jazi Eko Istiyanto, M.Sc.; Oskar Natan, S.ST., M.Tr.T., Ph.D.
Universitas Gadjah Mada, 2026 | Diunduh dari http://etd.repository.ugm.ac.id/

4.6 Implementasi Pengujian Sistem 73
4.6.1 Implementasi pengujian fungsionalitas sistem secara *end-to-end* 73
4.6.2 Implementasi pengujian keunikan dan independensi kunci sesi... 75
4.6.3 Implementasi analisis ketahanan terhadap serangan SAT 76
4.6.4 Implementasi pengujian *corruptibility* rangkaian ALU 8-bit 78
4.6.5 Implementasi pengujian keamanan siklus hidup kunci..... 79
4.6.6 Implementasi pengujian *overhead* sumber daya dan *timing*..... 81
BAB V..... 84
5.1 Pengujian Fungsionalitas Sistem secara *End-to-end*..... 84
5.2 Pengujian Keunikan dan Independensi Kunci Sesi..... 89
5.2.1 Pengujian keunikan kunci sesi 89
5.2.2 Pengujian independensi kunci sesi..... 91
5.3 Analisis Ketahanan terhadap Serangan SAT 93
5.3.1 Penolakan autentikasi perangkat tidak sah..... 94
5.3.2 *Bypass* perangkat lunak dan ketidakkonsistenan *oracle* 95
5.3.3 Sintesis keamanan berlapis 97
5.4 Pengujian *Corruptibility* Rangkaian ALU 8-bit..... 98
5.4.1 Kondisi kunci valid 99
5.4.2 Kondisi kunci salah 100
5.4.3 Kondisi tanpa kunci..... 103
5.4.4 Perbandingan dan analisis 106
5.5 Pengujian Keamanan Siklus Hidup Kunci..... 107
5.5.1 Hasil verifikasi *zeroize* 108
5.5.2 Analisis *oracle window* 110
5.5.3 Keterkaitan dengan prinsip manajemen kunci 111
5.6 Pengujian *Overhead* Sumber Daya Dan *Timing* 112
5.6.1 Hasil *overhead* sumber daya 112
5.6.2 Hasil *timing overhead* 113
BAB VI 115
6.1 Kesimpulan 115
6.2 Saran..... 116
DAFTAR PUSTAKA 118