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/

INTISARI

Logic locking adalah teknik proteksi kekayaan intelektual sirkuit terpadu yang mengunci fungsi logika sehingga beroperasi normal hanya apabila kunci yang benar dimuat. Skema konvensional berbasis kunci statis rentan terhadap serangan *Boolean Satisfiability* (SAT) yang mengeksploitasi konsistensi *oracle* untuk memulihkan kunci secara iteratif. Penelitian ini mengimplementasikan mekanisme *logic locking* kunci dinamis per sesi pada sistem tertanam yang mengintegrasikan *secure authenticator* DS28E50 berteknologi *ChipDNA* PUF dengan mikrokontroler STM32F103C8. Setiap sesi autentikasi menghasilkan kunci unik melalui HKDF-SHA256 yang dipetakan ke model RTL ALU dengan variasi lebar 4-bit, 8-bit, dan 16-bit berbasis XOR *key-gate*, diikuti prosedur *zeroization* terhadap seluruh material kriptografis di memori volatil. Hasil pengujian menunjukkan bahwa 100 kunci sesi yang dibangkitkan bersifat unik dengan entropi rata-rata 0,99 bit per posisi dan *Hamming Distance pairwise* 50,02%, mengonfirmasi ketiadaan korelasi lintas sesi. *Corruptibility* ALU pada variasi 4-bit, 8-bit, dan 16-bit menunjukkan pola yang konsisten, yaitu HD ≈ 0% pada kunci valid dan HD ≈ 50% pada kunci tidak valid maupun mode *fallback*, dengan mode *fallback* menghasilkan HD deterministik 50% pada seluruh variasi lebar ALU. *Overhead* implementasi terkendali dengan utilisasi *Flash* 29% dan RAM 6% dari kapasitas platform serta latensi sesi 1,06 detik. Prosedur *zeroization* mencapai keberhasilan 100% dengan jendela eksposur kunci deterministik 3 ms, dan verifikasi empiris mengonfirmasi bahwa kunci dari jalur tidak sah tidak mampu memulihkan fungsi ALU, mewujudkan prinsip *dishonest oracle* yang mengeliminasi prasyarat konvergensi SAT *solver*.

Kata kunci: *Logic Locking,* Serangan SAT*,* Pembuatan Kunci Dinamis*,* Autentikasi Perangkat Keras*, Dishonest Oracle.*

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/

ABSTRACT

*Logic locking is an intellectual property protection technique for integrated circuits that restricts circuit functionality to operate correctly only when the correct key is loaded. Conventional static-key-based schemes are vulnerable to Boolean Satisfiability (*SAT*) attacks that exploit oracle response consistency to iteratively recover the key. This research implements a per-session dynamic key logic locking mechanism on an embedded system integrating the DS28E50 secure authenticator with ChipDNA PUF technology and an STM32F103C8 microcontroller. Each authentication session generates a unique key via HKDF-SHA256, which is mapped into RTL ALU models with 4-bit, 8-bit, and 16-bit width variations using XOR key-gate architecture, followed by zeroization of all cryptographic material from volatile memory. Evaluation results show that 100 generated session keys exhibit zero duplication with an average bit-level entropy of 0.99 bits per position and a pairwise Hamming Distance of 50.02%, confirming negligible inter-session correlation. ALU corruptibility across the 4-bit, 8-bit, and 16-bit variations shows a consistent pattern, with HD ≈ 0% under valid key conditions and HD ≈ 50% under invalid key and fallback mode conditions, while fallback mode deterministically produces 50% HD across all tested ALU widths. Implementation overhead is manageable, with Flash utilization at 29% and RAM at 6% of platform capacity, and a total session latency of 1.06 seconds. Zeroization achieves a 100% success rate with a deterministic 3 ms key exposure window, and empirical verification confirms that keys derived through unauthorized bypass paths fail to restore ALU functionality, realizing the dishonest oracle principle that eliminates* SAT *solver convergence prerequisites.*

Keywords: *Logic Locking,* SAT *Attack, Dynamic Key Generation, Hardware Authentication, Dishonest Oracle.*