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 PUSTAKA

Analog Devices, 2021. *DS28E50 DeepCover Secure Authenticator with ChipDNA PUF Datasheet*. San Jose, CA: Analog Devices. Available at: https://www.analog.com/media/en/technical-documentation/data-sheets/DS28E50.pdf

Analog Devices, n.d. Reading and Writing 1-Wire® Devices Through Serial Interfaces. Available at: https://www.analog.com/en/resources/app-notes/reading-and-writing-1wirereg-devices-through-serial-interfaces.html (Accessed: 28 May 2026).

ARM Limited, 2010. *ARM Cortex-M3 Technical Reference Manual*. Cambridge: ARM Limited. Available at: https://developer.arm.com/documentation/100165/latest/

Barker, E., 2020. *Recommendation for Key Management Part 1: General (NIST SP 800-57 Part 1 Rev. 5)*. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-57pt1r5

Barker, E., Chen, L. and Davis, A., 2020. *Recommendation for Key-Derivation Methods Part 1: (NIST SP 800-56C Rev. 2)*. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-56Cr2

Bellare, M., 2006. New Proofs for NMAC and HMAC: Security against Collision Attacks. In: *Advances in Cryptology – CRYPTO 2006*. Berlin: Springer, pp. 631-648. DOI: 10.1007/11818176_42

Bellare, M., Canetti, R. and Krawczyk, H., 1996. Keying *Hash* Functions for Message Authentication. In: *Advances in Cryptology – CRYPTO '96*. Berlin: Springer, pp. 1-15. DOI: 10.1007/3-540-68697-5_1

Dupuis, S., Flottes, M.L. and Rouzeyre, B., 2019. Logic Locking: A Survey. *Journal of Electronic Testing*, 35(2), pp. 115-125. DOI: 10.1007/s10836-019-05794-9

Gandhi, A., et al., 2023. Logic locking for IP security: A comprehensive analysis on *challenge*s, techniques, and trends. *Microprocessors and Microsystems*, 98, p. 104775. DOI: 10.1016/j.micpro.2023.104775

Herder, C., Yu, M., Koushanfar, F. and Devadas, S., 2014. Physical Unclonable Functions and Applications: A Tutorial. *IEEE Design & Test*, 31(4), pp. 26-36. DOI: 10.1109/MDAT.2014.2329571

Hori, Y., Yoshida, T., Katashita, T. and Satoh, A., 2010. Evaluating the security of physical unclonable functions from the viewpoint of information theory. In: *2010 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, pp. 1084-1089. DOI: 10.1109/DATE.2010.5457013

Internet Engineering Task Force (IETF), 1997. *RFC 2104: HMAC: Keyed-Hashing for Message Authentication*. Reston, VA: IETF. DOI: 10.17487/RFC2104

Kamali, H.M., Kim, K., Lee, S. and Tehranipoor, M., 2022. Advances in Logic Locking: Past, Present, and Prospects. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 41(11), pp. 4050-4063. DOI: 10.1109/TCAD.2022.3197537

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/

Krawczyk, H., 2010. Cryptographic Extraction and Key Derivation: The HKDF Scheme. In: *Advances in Cryptology – CRYPTO 2010*. Berlin: Springer, pp. 631-648. DOI: 10.1007/978-3-642-14623-7_39

Krawczyk, H. and Eronen, P., 2010. *RFC 5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF)*. Reston, VA: Internet Engineering Task Force. DOI: 10.17487/RFC5869

Kurra, V.R. and Nelakuditi, S., 2019. Secure and Efficient Key Generation and Storage for IoT Devices. *IEEE Internet of Things Journal*, 6(5), pp. 8000-8010. DOI: 10.1109/JIOT.2019.2928582

Limaye, N., Karmakar, S., et al., 2021. Thwarting All Logic Locking Attacks: Dishonest *Oracle* with Truly Random Logic Locking. In: *2021 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Washington, DC: IEEE, pp. 1-11. DOI: 10.1109/HOST51478.2021.9533832

Maxim Integrated, 2018. *DS28E50 DeepCover Secure Authenticator User Guide (UG6724)*. San Jose, CA: Maxim Integrated. Available at: https://www.analog.com/media/en/technical-documentation/application-notes/UG6724.pdf

Mirmohammadi, S. and Etemadi Borujeni, S., 2023. A New Optimal Method for the Secure Design of Combinational Circuits against Hardware Trojans Using Interference Logic Locking. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 31(5), pp. 700-713. DOI: 10.1109/TVLSI.2023.3248981

National Institute of Standards and Technology, 2015. *FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Gaithersburg, MD: NIST. DOI: 10.6028/NIST.FIPS.202

Rajendran, J., Pino, Y., Sinanoglu, O. and Karri, R., 2013. Logic encryption: A new paradigm for IP protection. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 32(2), pp. 248-260.

Rostami, M., Koushanfar, F. and Karri, R., 2014. A Primer on Hardware Security: Models, Methods, and Metrics. *Proceedings of the IEEE*, 102(8), pp. 1208-1229. DOI: 10.1109/JPROC.2014.2336744

Software Engineering Institute, 2021. MSC06-C. Beware of compiler optimizations. In: *CERT C Coding Standard*. Pittsburgh, PA: Carnegie Mellon University. Available at: https://wiki.sei.cmu.edu/confluence/display/c/MSC06-C.+Beware+of+compiler+optimizations

STMicroelectronics, 2015. *STM32F103x8 / STM32F103xB Datasheet*. Geneva: STMicroelectronics. Available at: https://www.st.com/resource/en/datasheet/stm32f103c8.pdf

Subramanyan, P., Ray, S. and Malik, S., 2015. Evaluating the Security of Logic Encryption Algorithms. In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. Washington, DC: IEEE, pp. 134-139. DOI: 10.1109/HST.2015.7141368

Suh, G.E. and Devadas, S., 2007. Physical Unclonable Functions for Device Authentication and Secret Key Generation. In: *Proceedings of the 44th*

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/

Annual Design Automation Conference (DAC). New York: ACM, pp. 9-14. DOI: 10.1145/1278480.1278484

Turan, M.S., Barker, E., Kelsey, J., McKay, K.A., Baish, M.L. and Boyle, M., 2018. *Recommendation for the Entropy Sources Used for Random Bit Generation (NIST SP 800-90B)*. Gaithersburg, MD: National Institute of Standards and Technology. DOI: 10.6028/NIST.SP.800-90B

Xie, Y. and Srivastava, A., 2019. Anti-SAT: Mitigating SAT Attack on Logic Locking. *IEEE Transactions on Information Forensics and Security*, 14(9), pp. 2360-2373. DOI: 10.1109/TIFS.2019.2909159

Yang, Y., et al., 2019. SFLL-hd: A Secure Logic Locking Scheme against SAT Attack. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38(10), pp. 1850-1863. DOI: 10.1109/TCAD.2019.2898438

Yasin, M., Mazumdar, B., Rajendran, J.J. and Sinanoglu, O., 2016. SARLock: SAT Attack Resistant Logic Locking. In: *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. Leuven: EDAA, pp. 1369-1374. DOI: 10.1109/DATE.2016.7452941

Zhong, H. and Guin, U., 2023. Complexity Analysis of the SAT Attack on Logic Locking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 42(1), pp. 200-213. DOI: 10.1109/TCAD.2022.3187333