A Keccak-Based Wireless Authentication Tag with per-Query Key Update and Power-Glitch Attack Countermeasures

16.2 A Keccak-Based Wireless Authentication Tag with per-Query Key Update and Power-Glitch Attack Countermeasures

Chiraag S Juvekar[1], Hyung-Min Lee[1], Joyce Kwong[2], Anantha P Chandrakasan[1]

[1]Massachusetts Institute of Technology, Cambridge, MA, [2]Texas Instruments, Dallas, TX

Counterfeiting is a major problem plaguing global supply chains. While small low-cost tagging solutions for supply-chain management exist, security in the face of fault-injection [1] and side-channel attacks [2] remains a concern. Power glitch attacks [3] in particular attempt to leak key-bits by inducing fault conditions during cryptographic operation through the use of over-voltage and under-voltage conditions. This paper presents the design of a secure authentication tag with wireless power and data delivery optimized for compact size and near-field applications. Power-glitch attacks are mitigated through state backup on FeRAM based non-volatile flip-flops (NVDFFs) [4]. The tag uses Keccak [5] (the cryptographic core of SHA3) to update the key before each protocol invocation, limiting side-channel leakage to a single trace per key. Fig. 1 shows the complete system including the tag, reader, and backend server implemented in this work. Tags are seeded at manufacture and this initial seed is stored in the server database before a tag is affixed to an item. A wireless power and data transfer (WPDT) frontend harvests energy from the reader (433 MHz inductive link) and powers the on-chip authentication engine (AE). On startup the AE updates its key using a PRNG (seeded with the old key) and increments the key index. The AE then responds to the subsequent challenge, by encrypting the challenge under the new key. These challenge-response pairs can be validated by a trusted server to authenticate the tag. Additionally, the server can use the key-index to resynchronize with the tag in the event of packet loss.

The AE, shown in Fig. 2, implements PRNG and encryption modes using the Keccak-f[400] permutation. Two 400-bit state-arrays are implemented, each with 25 16-bit lane shift-registers allowing us to access the state one slice at a time over 16 cycles. Of the 5 operations used in a Keccak round, four (θ, π, χ and ı [5]) act on the full slice and hence are implemented by a common combinational block acting on the output of the state shared by both modes. The ρ operation acts on lanes and is implemented with lane-specific hard-coded muxes. Since, each NVDFF is 3.2x larger than a DFF and needs 3.4pJ from on-chip energy storage for backup [4], the design stores only the PRNG state, tag ID, and key index in NVDFFs and DFFs are used for all other state-elements. This reduces back-up energy by 57% and AE area by 26%. The 128-bit security level desired for our application is guaranteed using Keccak-f[400], saving 62% backup-energy and 67% area when compared to Keccak-f[1600] (used in SHA3) due to the smaller internal state of the algorithm.

The WPDT architecture shown in Fig. 3 can harvest up to 1mW power from a mm-sized RF coil. A proposed regulating voltage multiplier (RVM) combines the AC-DC voltage multiplier and regulator into a single structure, which simultaneously rectifies, boosts, and regulates a small AC coil voltage to the supply voltage, V_{DD} (1.5V). The RVM uses four AC-coupled adaptive regulating rectifiers (ARRs) connected in series to charge an on-chip decoupling capacitor, C_L. Each ARR consists of a cross-coupled NMOS/PMOS rectifier 0 and regulating switches to adjust DC output level. Negative feedback signals, V_{FBN} and V_{FBP}, adaptively control dropout voltages across the regulating switches to regulate V_{DD}. Built-in regulation in the ARRs limits their DC outputs below V_{DD} for overvoltage self-protection. The proposed RVM needs only one decap compared to a conventional voltage multiplier, which typically needs a following regulator and two decaps. The RVM was measured to generate a 1.5V regulated voltage (supplying 60μW) for all AC input amplitudes >0.55V at 433MHz with <1.1% line/load regulation ($\Delta V_{DD}/V_{DD}$), voltage conversion ratio (VCR, $V_{DD}/V_{AC,PEAK}$) up to 2.73, and simulated power conversion efficiency (PCE, $P_{LOAD}/P_{AC,IN}$) up to 60% (Fig. 6). An active clamp circuit limits the AC input amplitude below 1.2V, and the RVM provides further overvoltage glitch protection to limit the transient overshoot on V_{DD} to 110mV within a safe margin (10% of V_{DD}) for the AE (Fig. 6). A separate rail, V_{DDNV}, is provided for NVDFF backup/restore [4]. The RVM trickle charges V_{DDNV} to 1.5V to avoid charge-sharing when connecting it to V_{DD} before NVDFF restore.

The pulse-based wireless telemetry circuits that minimize wireless power dead-time on the inductive link are shown in Fig. 3. The tag transmits a clock-recovery message to help the reader set the downlink data bit period to compensate for tag-reader clock drift. An all-digital pulse-position (PP) demodulator extracts this at 125kbps by comparing position ratio among three (12.5% duty-cycle) on-off-keying (OOK) demodulated pulses (4x lower dead-time energy loss compared to 50% duty-cycle pulse-width modulation 0). Load-shift-keying (LSK) by shorting the L_2C_2-tank for 0.5μs (per high bit) at 125kbps is used for uplink.

The energy backup unit (EBK) is shown in Fig. 4. When wireless power is interrupted, the tag needs 3.5nJ energy (including 40% margin) to complete safe shutdown. Stable operation of NVDFFs necessitates that supply droop be regulated within 10%. Simply increasing C_L (1.5V FeCap) requires a total 0.4mm^2 silicon area. A more compact EBK is implemented by using a backup decap, C_{BK} (3.3V FeCap), which has lower capacitance per area but can be charged to higher voltage than 1.5V FeCap. On startup a cross-coupled switched-capacitor voltage doubler charges C_{BK} to 2.75V (V_{BK}). If the input power sensing circuit detects loss of wireless power, C_{BK} powers V_{DD} through a linear regulator until safe shutdown is complete. A minimum decap (C_{Lmin}) of 0.11mm^2 is still needed to limit V_{DD} drop from instantaneous NVDFF energy consumption (up to 1nJ). Due to 3.4x higher energy density of C_{BK} (at 2.75V including average 79% regulator efficiency) compared to C_L (at 1.5V), the EBK, C_{BK}, and C_{Lmin} together need just 0.24mm^2 (40% less area than using C_L alone). Safe shutdown operation (verified with worst-case power interruption events) is shown in the measured waveforms. Wireless power is interrupted just after V_{DDNV} reaches 1.5V and before NVDFF restore is started. In response the WPDT enters sleep mode, and the energy from C_{BK} is sufficient for the AE to restore state, run a key-update step, and complete the backup to the NVDFFs.

Power-glitch countermeasures mitigate power-loss at arbitrary times due to a malicious reader or if the reader is pulled away inadvertently. In particular, the PRNG needs 3.1ms for key-update, and care needs to taken to avoid state corruption due to power loss. Moreover, a part of the key-update is forced between successive power glitches to avoid side-channel leakage resulting from the same key being restored and backed up. Fig. 5 presents these countermeasures in detail. On power-up the AE is first held in reset by the WDPT until C_{BK} charges to 2.75V. Next, the AE requests charging of the V_{DDNV} for NVDFF restore. If power is lost before V_{DDNV} reaches 1.5V, no action needs to be taken, as the NVDFFs have not been accessed yet. Once V_{DDNV} charges to 1.5V, the NVDFF restore is started. Power-loss before restore completion necessitates that restore, at least one key-update step, and backup all be performed from C_{BK}. After the NVDFFs are restored, the AE tries to complete the key-update before running the challenge-response protocol. Power-loss at this point is handled separately based on whether the AE was running in PRNG mode or encryption mode. The former indicates that a key-update was in progress and must be resumed later, while the latter indicates that an encryption was aborted and a new key-update must be started. Finally glitches during a backup operation are ignored, and power-ups are deferred until after WPDT shutdown. Successful operation in the presence of 2 successive power-glitch events is shown in the measured waveforms. Key-update guarantees the use of unique keys for the two tag responses.

The authentication tag was fabricated in a 130nm CMOS process and occupies 0.77mm^2 area including C_L and C_{BK}. The tag consumes 7.5μW for standby and total 16.1μW during authentication. The AE occupies 17.9k NAND Gate Equivalents (GE). Novel countermeasures for power-glitch and side-channel attack mitigation are summarized in Fig. 6. Fig. 7 shows die photo of the authentication tag.

Acknowledgement:

The authors thank Sudipto Chakraborty for advice, Denso and Texas Instruments for funding this work and Texas Instruments for chip fabrication.

Reference:

I. Verbauwhede, et al, "Circuit Challenges from Cryptography," *IEEE ISSCC*, pp. 1-2, Feb. 2015.

C. Tokunaga, et al, “Secure AES engine with a local switched-capacitor current equalizer,” *IEEE ISSCC*, pp. 64–65, Feb. 2009.

K. Gomina, et al, “Power supply glitch attacks: Design and evaluation of detection circuits”, *IEEE HOST*, pp. 136-141, May 2014.

M. Qazi, et al, "A 3.4pJ FeRAM-enabled DFF in 0.13μm CMOS for Nonvolatile Processing in Digital Systems," *IEEE ISSCC*, pp.192-193, Feb. 2013.

G. Bertoni, et al, “The Keccak Reference, ” *Round 3 Submission to NIST*, 2011.

N. Desai, et al, "A Scalable 2.9mW 1 Mb/s eTextiles Body Area Network Transceiver with Remotely-Powered Sensors and Bi-Directional Data Communication," *IEEE ISSCC,* pp. 206-207, Feb. 2013.

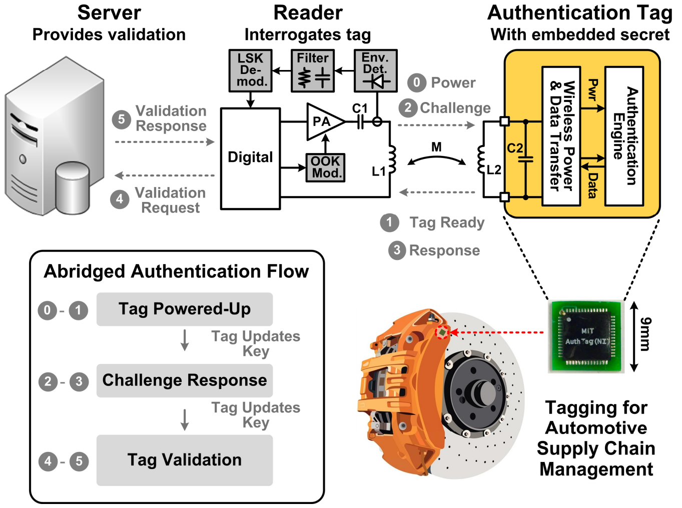


Figure 16.2.1: System architecture, authentication protocol, and applications for the proposed authentication tag

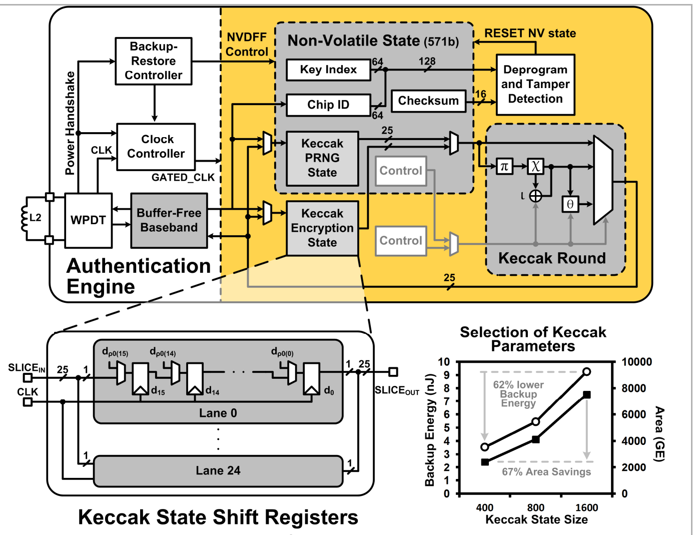


Figure 16.2.2: Architecture of the Keccak authentication engine (AE) with non-volatile state optimization for area and energy savings

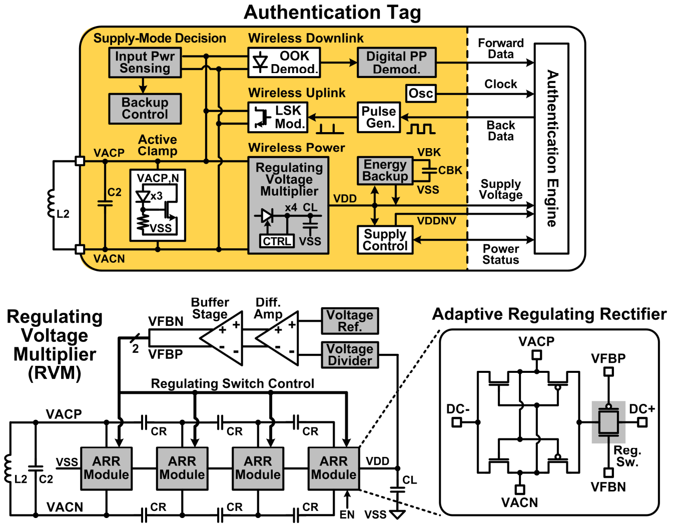


Figure 16.2.3: Architecture of the wireless power and data transfer (WPDT) circuits with the proposed regulating voltage multiplier

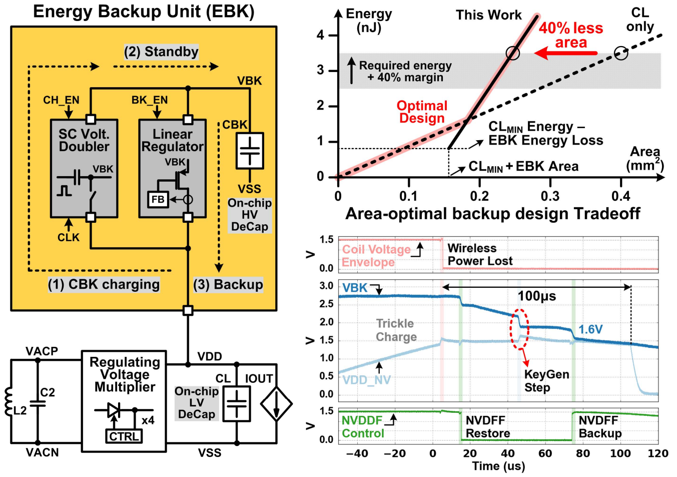


Figure 16.2.4: Energy backup unit to provide sufficient energy from minimally-sized on-chip capacitors and measured waveform of safe shutdown during worst-case power interruption event

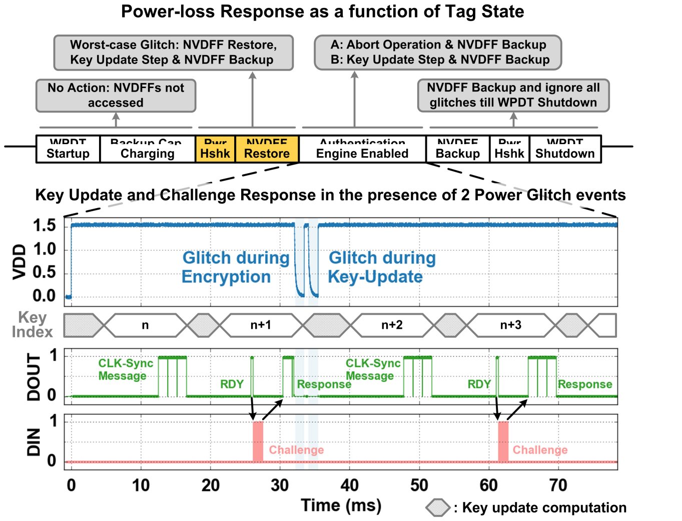
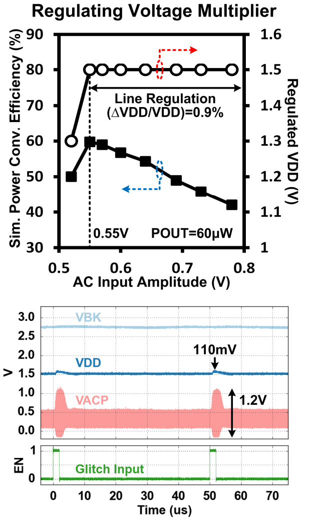


Figure 16.2.5: Power-glitch attack countermeasures and measured waveform of successful operation in the presence of two glitches



Authentication Tag Specification

Overall System	
Process	130nm CMOS
VDD/VBK/PSB	1.5V / 2.75V / 7.5μW^A
Die Area^B	0.77mm^2
Wireless Power/Data Transfer	
Source	Inductive Link
L1 / L2	23.5nH / 46nH
Downlink	0.5μs-PW OOK-PPM, 125kbps
Uplink	0.5μs-PW LSK, 125kbps
Authentication Engine	
Modes	PRNG + Auth-Encryption
Throughput	30 Tags/sec
Power	3.6μW(Standby), 8.6μW(Auth)
Area	17.9k GE (Incl. 571 NVDFF)
Attack Mitigation	
Glitching	Backup Cap + NVDFF
Side-Channel	Per Query Key Refresh

^{A} Standby static power
^{B} Including on-chip decaps, CL and CBK

Figure 16.2.6: Authentication tag specification including measured RVM performance and overvoltage power-glitch waveform

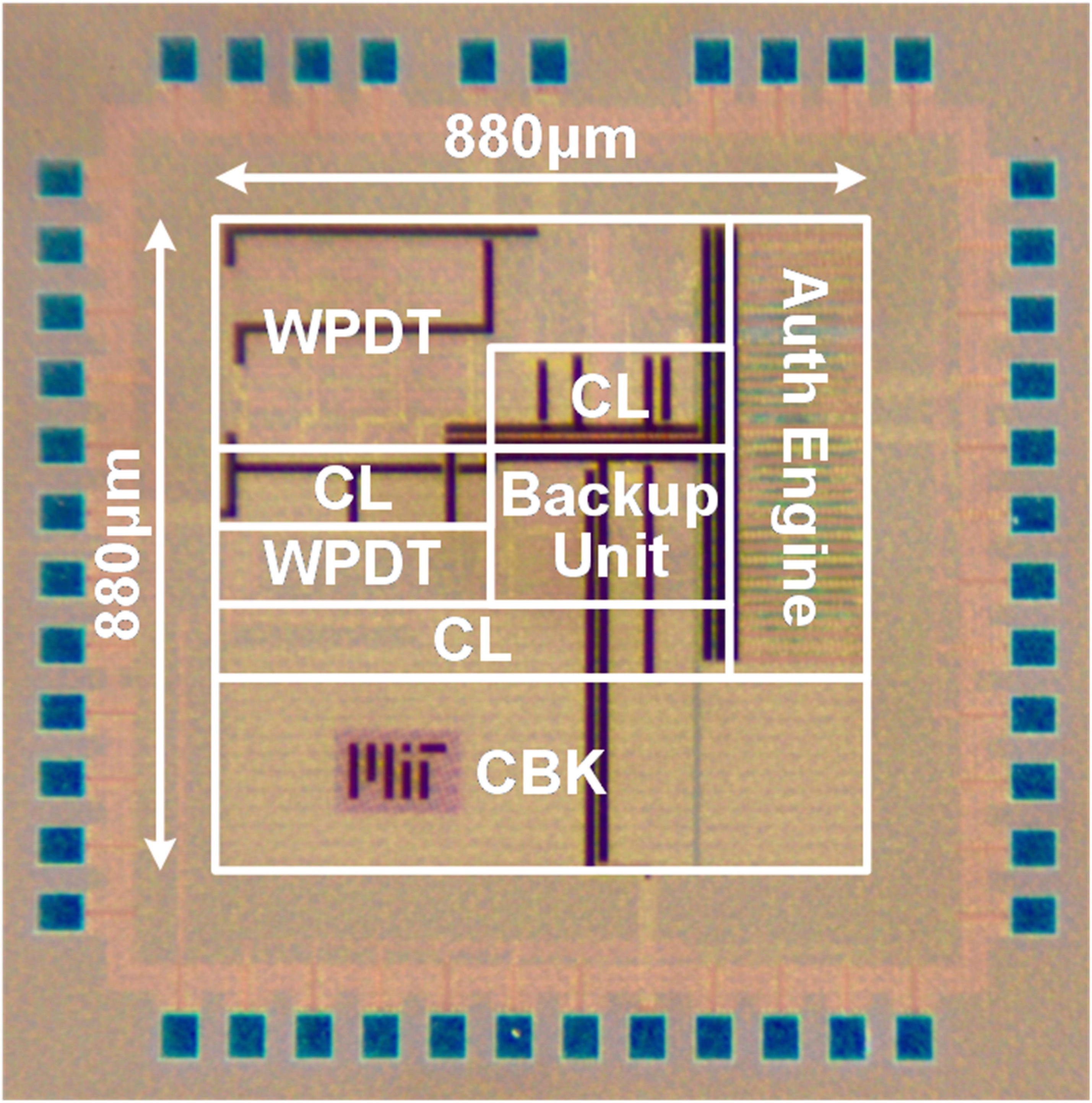


Figure 16.2.7: Die photo of the authentication tag