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

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>As Published</td>
<td><a href="https://submissions.mirasmart.com/isscc2016/PDF/ISSCC2016AdvanceProgram.pdf">https://submissions.mirasmart.com/isscc2016/PDF/ISSCC2016AdvanceProgram.pdf</a></td>
</tr>
<tr>
<td>Publisher</td>
<td>Institute of Electrical and Electronics Engineers (IEEE)</td>
</tr>
<tr>
<td>Version</td>
<td>Author's final manuscript</td>
</tr>
<tr>
<td>Accessed</td>
<td>Tue Nov 13 14:18:47 EST 2018</td>
</tr>
<tr>
<td>Citable Link</td>
<td><a href="http://hdl.handle.net/1721.1/101188">http://hdl.handle.net/1721.1/101188</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>Creative Commons Attribution-Noncommercial-Share Alike</td>
</tr>
<tr>
<td>Detailed Terms</td>
<td><a href="http://creativecommons.org/licenses/by-nc-sa/4.0/">http://creativecommons.org/licenses/by-nc-sa/4.0/</a></td>
</tr>
</tbody>
</table>
16.2 A Keccak-Based Wireless Authentication Tag with per-Query Key Update and Power-Glitch Attack Countermeasures

Chiraag S Juvetakari, Hyung-Min Lee, Joyce Kwong, Anantha P Chandrakasan

1Massachusetts Institute of Technology, Cambridge, MA, 2Texas 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 (NVDDFs) [4]. The tag uses Keccak [5] (the cryptographic core of SHA3) to update the key before each power glitch, by invoking 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) front-end 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-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, χ, η and σ [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 p operation acts on lanes and is implemented with lane-specific hard-coded mixtures. Since, each NVDDFF 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 NVDDFFs 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 use of unique keys for the two tag responses. 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 WPDT until CIN charges to 2.75V. Next, the AE requests charging of the VDDH for NVDDF restore. If power is lost before VDDH reaches 1.5V, no action needs to be taken, as the NVDDFFs have not been accessed yet. Once VDDH charges to 1.5V, the NVDDF restore is started. Power-loss before restore completion necessitates that restore, at least one key-update step, and backup all be performed from CBK. After the NVDDFFs 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 0.77m² area including CIN and CBK. The tag consumes 7.5pW 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:
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

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