A Nonvolatile Flip-Flop-Enabled Cryptographic Wireless Authentication Tag with Per-Query Key Update and Power-Glitch Attack Countermeasures

Chiraag Juvekar\textsuperscript{1}, Hyung-Min Lee\textsuperscript{2}, Joyce Kwong\textsuperscript{3}, and Anantha Chandrakasan\textsuperscript{1}

\textsuperscript{1}Massachusetts Institute of Technology
\textsuperscript{2}Korea University, \textsuperscript{3}Texas Instruments

$30$ million worth fake wines were seized in 2012

In 2014, Aston Martin recalled 18,000 cars due to counterfeit brake pedals

Fake malaria drugs caused 100,000 deaths in Africa
Threat Model:

- **Passive attacks** against the tag such as DPA/DEMA
- **Non-invasive active attacks** like power glitch attacks
Key Features

- Regulating Voltage Multiplier
- Pulse-based Telemetry
- Key Update Protocol
- Keccak Cryptographic Core
- NV-DFF Key-storage
- FeCap-based Energy Backup

Wireless power/data for compact-size tag
To prevent side-channel attack
To limit power-glitch attack
Area-Optimal Energy Backup Unit

- **3.5nJ** backup energy requirement
- **$C_{BK}$** (HV FeCap) has **3.4x higher energy density** including regulator efficiency than **$C_L$** (LV FeCap)
- Energy Backup Unit needs **2.2x less area** compared to single output cap
Power-Glitch Countermeasures

Power Glitch Causes:
- Reader is pulled away
- Malicious Reader

Guaranteed safe backup and key update

Backup w/ Worst-Case Glitch Event

The tag safely performs:
- NVDDFF restore
- Key update
- NVDDFF backup