Secure Mode Register Cell: Hardware Enforcement of Privileged Context Isolation

Shivam Kak, Isaac Gyamfi
Princeton University
sk3686@princeton.edu, ig8214@princeton.edu

I. Introduction

HYPERVISORS in virtualized systems typically have full access to VM register state, creating security risks if compromised. This is critical in cloud computing where multiple tenants share hardware. Traditional software-based isolation relies on trusted hypervisors, but a compromised hypervisor can access all VM state, including cryptographic keys.

The ZION architecture [1] addresses this by isolating vCPU state from untrusted software. We explore implementing similar protection at the storage cell level: a transistor-level register with dual read ports (public and secure) that enforces read access control. When secure mode is disabled, the secure port returns logic 0 regardless of stored data, providing hardware-level guarantees that sensitive results are erased when transitioning contexts.

II. Circuit Design and Methodology

We designed a 1-bit secure register cell in Cadence Virtuoso (Fig. 7) with: (1) cross-coupled inverter pair, (2) transmission gate write path (WE control), (3) secure read port (Q_SEC) with direct buffered access, and (4) public read port (Q_PUB) with SEC-gated access. The design uses positive edge-triggered architecture [2] (Fig. 1). Both designs were implemented in 1-bit and 16-bit versions using 45nm GPDK. Transient simulations verified functionality across all SEC, WE, D $\in \{0, 1\}$ combinations (Table I).

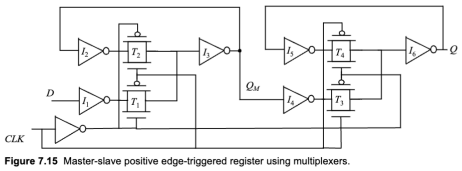

Fig. 1: **Positive edge-triggered register [2].**

III. Analysis and Results

A. Functional Behavior

The dual-port architecture enables independent control of secure and public data paths. **SEC = 0 (Public Mode):** Q_PUB operates as a normal register (writes D when WE=1, retains state when WE=0), while Q_SEC is forced to 0 regardless of inputs, ensuring secure data cannot leak to unprivileged contexts. **SEC = 1 (Secure Mode):** Q_PUB holds its previous state regardless of inputs, preventing public access during secure operations, while Q_SEC operates normally (writes D when WE=1, retains state when WE=0).

Transient analysis (Figs. 2, 3) confirms correct operation. When SEC transitions to 1, Q_PUB retains previous state (0 or 1 depending on timing). The 16-bit implementation shows identical behavior.

TABLE I: Truth Tables for SEC = 0 and SEC = 1

SEC = 0 (Public Mode)				**SEC = 1 (Secure Mode)**			
D	WE	Q_PUB$_n$	Q_SEC$_n$	D	WE	Q_PUB$_n$	Q_SEC$_n$
0	0	Q_{n-1}	0	0	0	Q_{n-1}	Q_{n-1}
0	1	0	0	0	1	Q_{n-1}	0
1	0	Q_{n-1}	0	1	0	Q_{n-1}	Q_{n-1}
1	1	1	0	1	1	Q_{n-1}	1

B. Timing and Energy

Setup time is 1ns for both Q_SEC and Q_PUB outputs (Figs. 4, 5), matching baseline performance. Hold time is 0s for all configurations (Fig. 6). As noted in [2], the transmission gate turns off when clock goes high, so D-input changes after the rising edge are not seen, resulting in zero hold time.

Energy consumption (Table II) shows linear scaling: 68.21 fJ for 1-bit and 1.084 pJ for 16-bit. The 15.9× increase matches expected 16× scaling. Secure and normal registers consume identical energy, demonstrating minimal overhead for security features.

TABLE II: Energy Consumption Comparison

Design	1-bit	16-bit
Secure Register	68.21 fJ	1.084 pJ
Normal Register	68.21 fJ	1.084 pJ

C. Area Analysis

Layout area analysis (Table III) shows the secure register requires 2.36× more area than the normal register due to dual-port architecture (Q_PUB and Q_SEC), which is required here to enable effective resource management with hardware-enforced isolation.

IV. Conclusion

We successfully demonstrated a dual-port secure register with hardware-enforced isolation, showing correct functionality with 1ns setup time, 0s hold time, and minimal energy overhead. Future work includes: (1) PVT characterization for robust operation, (2) side-channel attack analysis to verify data erasure prevents leakage, (3) scaling to larger structures for secure processor integration, and (4) formal security verification.

References

[1] J. Wang, J. Wang, and Y. Zhang, "Zion: A practical confidential virtual machine architecture on commodity risc-v processors," in *2025 62nd ACM/IEEE Design Automation Conference (DAC)*, 2025, pp. 1–7.

[2] J. M. Rabaey, A. Chandrakasan, and B. Nikolic, *Digital integrated circuits*. Prentice hall Englewood Cliffs, 2002, vol. 2.

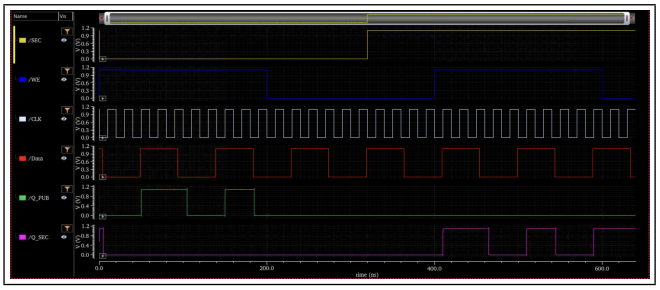

Fig. 2: **Transient Case 1: Q_PUB retains 0**

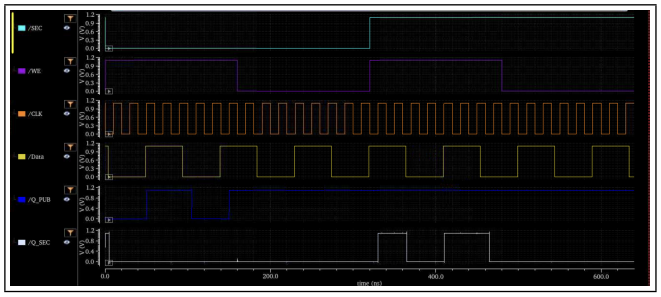

Fig. 3: **Transient Case 2: Q_PUB retains 1**

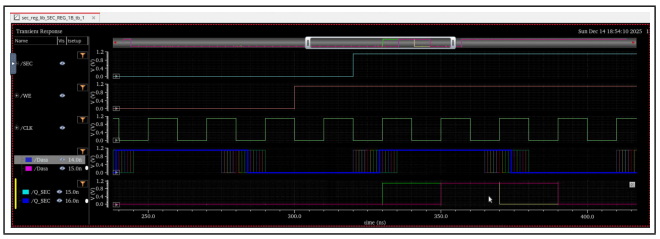

Fig. 4: **Setup time for Q_SEC: 1ns**

Fig. 5: **Setup time for Q_PUB: 1ns**

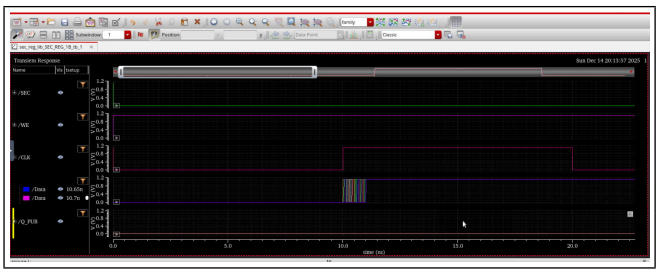

Fig. 6: **Hold time: 0s for all configurations**

Design	**Area (μm^2)**	**Overhead**
Normal Reg	2.04	1.00×
Secure Reg	4.82	2.36×

TABLE III: **Area Comparison for 1-bit Registers**

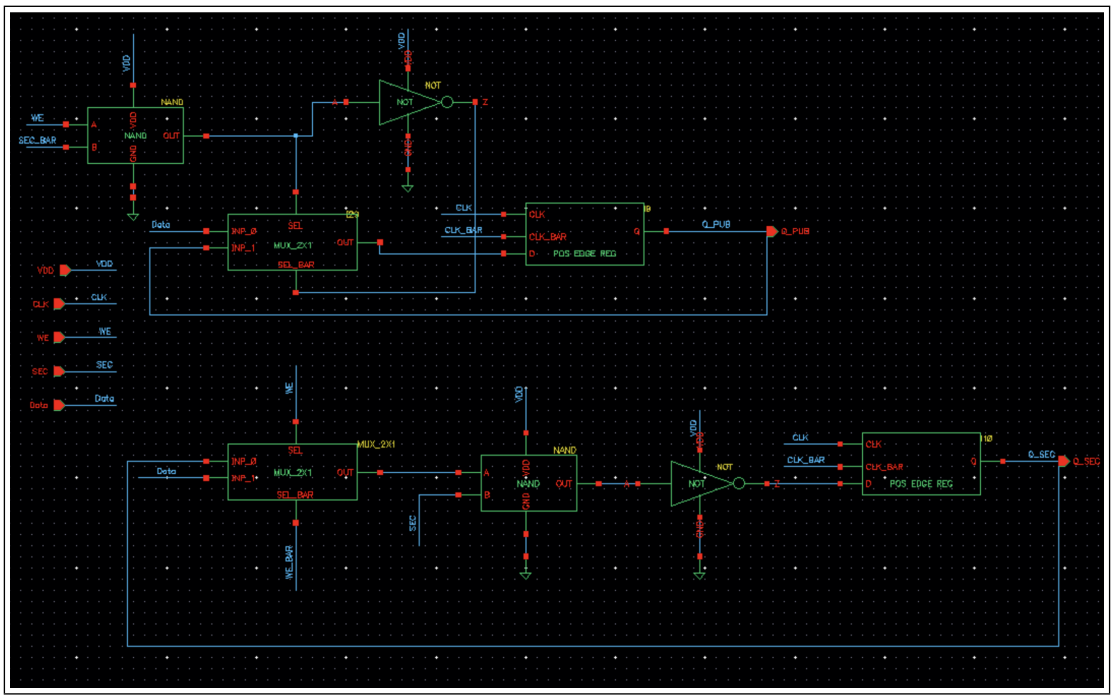

Fig. 7: **Secure register schematic with dual-port architecture**