

Hertzbleed & DVFS Cryptographic Side-Channel Vulnerabilities

Microarchitectural Security Audit on Dynamic Voltage/Frequency Throttling Leakage

Published by **Lesty Tech Security Research Lab** | Date: October 19, 2026 | Reference: LESTY-ENG-2026-B5

1. The Fundamental Vulnerability: Power-to-Frequency Conversion

Constant-time cryptographic implementations (e.g., constant-time AES, Montgomery laddering in RSA, and post-quantum ML-KEM/Kyber) guarantee identical execution cycles regardless of input data secret bits. However, modern x86-64 and ARM processors employ aggressive Dynamic Voltage and Frequency Scaling (DVFS) algorithms to remain within strict Thermal Design Power (TDP) envelopes. These algorithms dynamically modulate CPU clock frequency based on instantaneous current draw ($I_{dd} = C_{dyn} \cdot V_{dd} \cdot f$). Operands with higher Hamming weight (higher bit transitions) trigger larger dynamic capacitance switching, forcing immediate 50–150 MHz frequency drops.

2. Wall-Clock Leakage in Constant-Cycle Instructions

Security Disclosure: Even if two operations require the exact same number of clock cycles (e.g., exactly 1,000,000 cycles), if Operation A executes at 4.2 GHz due to low Hamming weight and Operation B throttles the core to 4.0 GHz due to high Hamming weight, Operation B takes 11.9 microseconds longer in real wall-clock time! Remote attackers measuring network packet round-trip latencies can extract full cryptographic keys without local execution privileges.

3. Hardware Mitigations vs. Workload Performance Penalties

Mitigating DVFS-induced side channels requires either disabling hardware DVFS (forcing static frequency scaling at severe energy costs) or injecting software power-equalization masking routines. Modern Linux kernel patches provide per-process core throttling lockouts, but cross-core power budget sharing on multi-tenant cloud instances (Intel Running Average Power Limit - RAPL) leaves containerized workloads vulnerable to co-tenant frequency sniffing.

ARCHITECTURAL BENCHMARK & PARAMETER TELEMETRY

Architectural Metric	Standard Fixed Frequency	Active DVFS (Unmitigated)	Masked Constant-Time HW
Cycle Count Consistency	Exact (Cycle-accurate)	Exact (Cycle-accurate)	Exact (Cycle-accurate)
Wall-Clock Jitter per Op	< 0.05 ns	12–85 ns (Data dependent)	< 0.12 ns
Hamming Weight Sensitivity	None (Zero frequency shift)	50–150 MHz throttle drop	Equalized switching dummy noise
Key Recovery Time (AES-256)	Infeasible (>10 ¹⁸ probes)	36 Hours (Remote HTTP probes)	Infeasible (>10 ¹⁵ probes)
CPU Energy Efficiency Impact	-22% (Fixed high clock)	Baseline Max Efficiency	-8% (Power-equalizing overhead)

