

GoFetch: Microarchitectural Analysis of Apple Silicon DMP

Breaking Constant-Time Cryptographic Primitives via Data Memory-Dependent Prefetching

Research Desk: Lesty Tech Hardware Security Lab | Date of Assessment: October 2026 | Distribution: Public Technical Release

1. The Classical Constant-Time Paradigm

Modern cryptographic algorithms (OpenSSL, RSA, ECDSA, Kyber, Dilithium) enforce strict constant-time execution: instruction cycle count and memory access patterns must be mathematically independent of secret key bits, neutralizing timing-based cache attacks.

Architectural security models assumed that while prefetchers monitor memory access strides, they never interpret raw memory payloads as pointers.

2. Data Memory-Dependent Prefetcher (DMP) Mechanics

Apple M1, M2, and M3 microarchitectures incorporate an aggressive Data Memory-Dependent Prefetcher (DMP) inside the CPU load-store unit to accelerate pointer-heavy pointer-chasing workloads.

CRITICAL: The DMP inspects memory contents directly. If a data value within a cache line matches an address falling within the application's virtual address space, the DMP autonomously executes an out-of-order prefetch for that address.

GoFetch crafts chosen-ciphertext inputs that cause intermediate cryptographic secrets to be treated as pointers. When the prefetcher dereferences the secret, it evicts cache lines from the L2 cache, leaking the secret key bits through side-channel timing analysis.

3. Microcode Immutability and Software Mitigation Costs

Because DMP logic is hardwired directly into the performance core (P-core) load queues on M1 and M2, it cannot be disabled via software or firmware updates without running cryptography exclusively on Icestorm efficiency cores (E-cores) or injecting expensive memory fence instructions that degrade cryptographic throughput by 120% to 260%.

Empirical Laboratory & Architectural Benchmark Telemetry

Cryptographic Primitive	Target Key Size	GoFetch Extraction Latency
OpenSSL 3.0.7 RSA	2048-bit Private Key	Under 54 minutes (Full Key Recovery)
Go crypto/elliptic P-256	256-bit Scalar Key	Under 18 minutes (Complete Key Extraction)
CRYSTALS-Kyber-512 (Post-Quantum)	Post-Quantum KEM	Under 140 minutes

Software Mitigation Penalty (DIT)	Data-Independent Timing	Available only on M3+ (Zero M1/M2 support)
E-Core Execution Overhead	Crypto Offloading to E-cores	+185% to +240% Latency Penalty