DEFY: A Deniable, Encrypted File System for Log-Structured Storage

Tim Peters, Cal Poly San Luis Obispo
Mark Gondree, Naval Postgraduate School
Zachary N J Peterson, Cal Poly San Luis Obispo




Erase vs. write granularity

Wear leveling

DEFY

the Deniable Encrypted File System from YAFFS

Contributions

log-structured design
deniability levels
authenticated encryption
efficient **secure deletion**
snapshot resistent

Deniability

Levels imply **privacy equivalence**

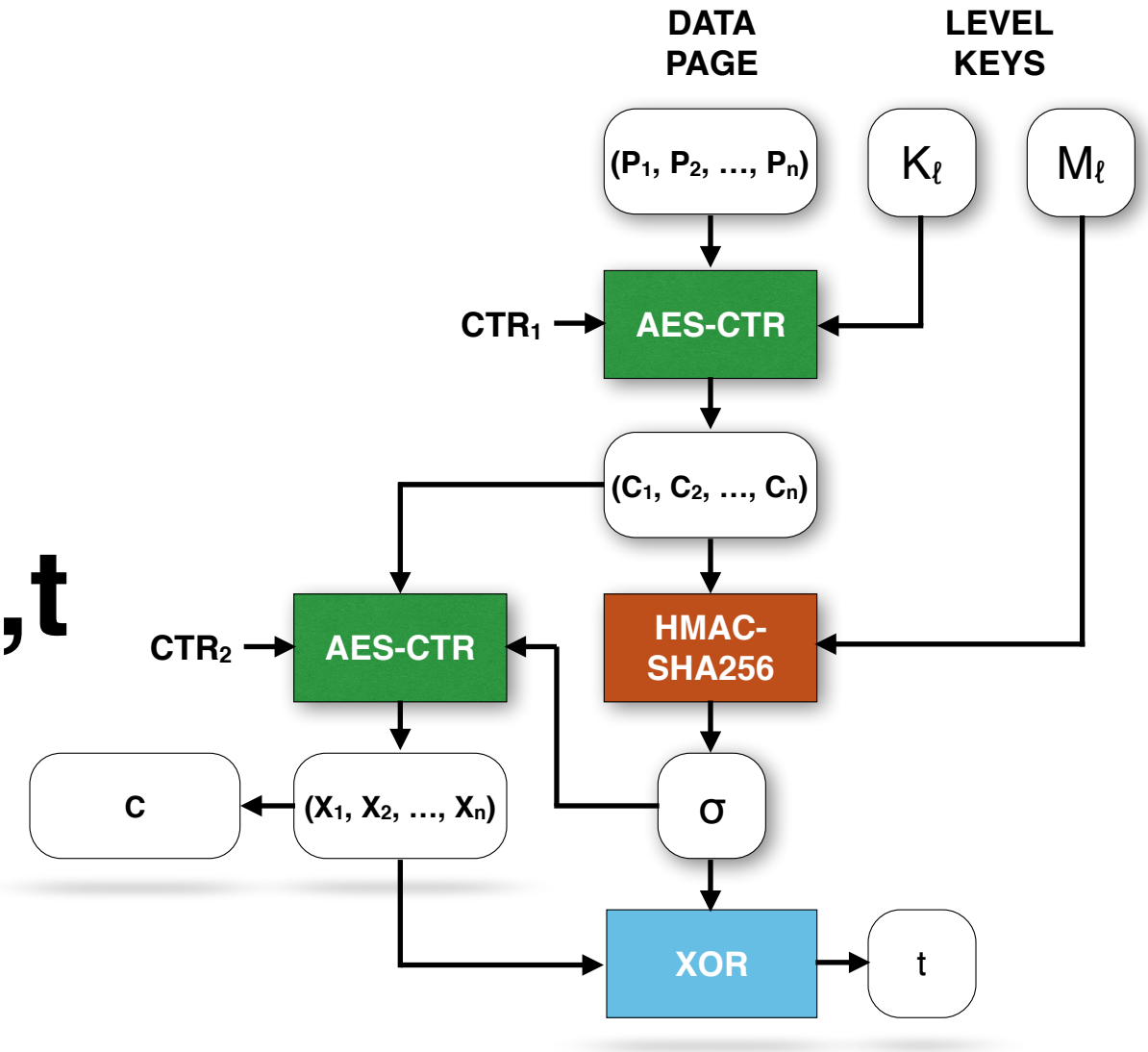
Levels provide a **total order**

Higher levels reveal lower levels

Revealing a level provides **no information about unrevealed levels**

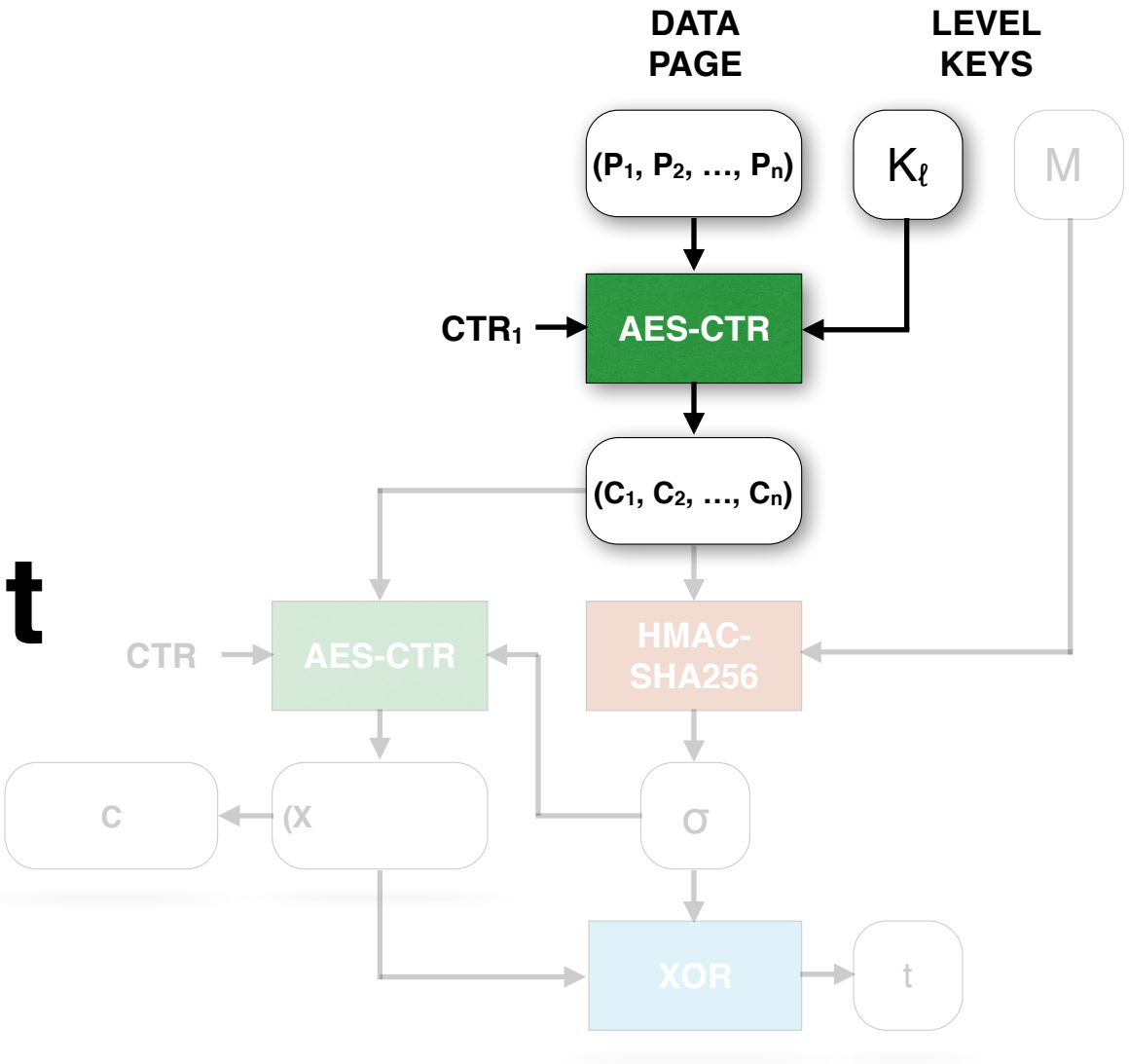
Transform

$$f(K_\ell, M_\ell, P) = C, t$$



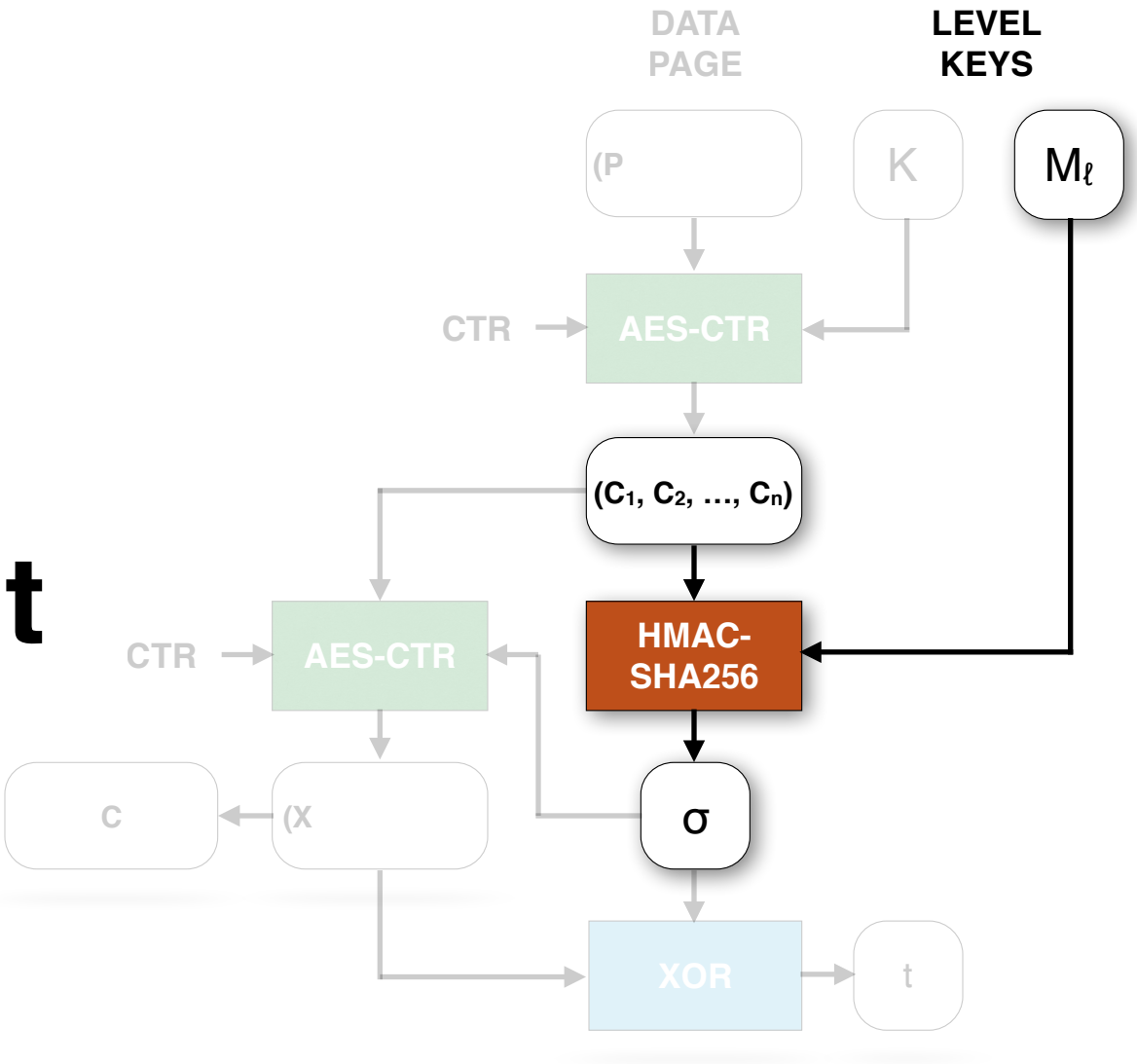
Transform

$$f(K_\ell, M_\ell, P) = C, t$$



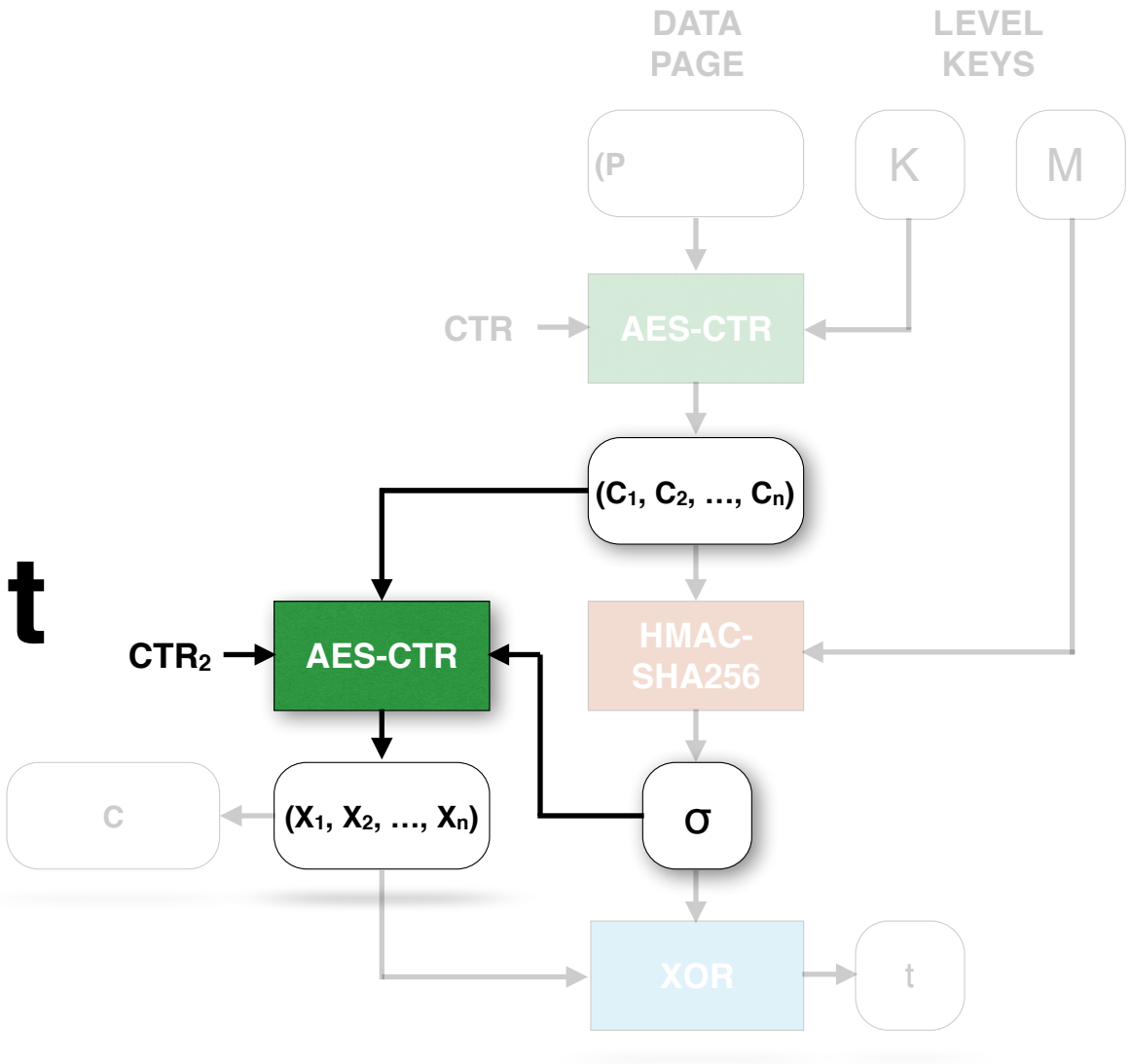
Transform

$$f(K_\ell, M_\ell, P) = C, t$$



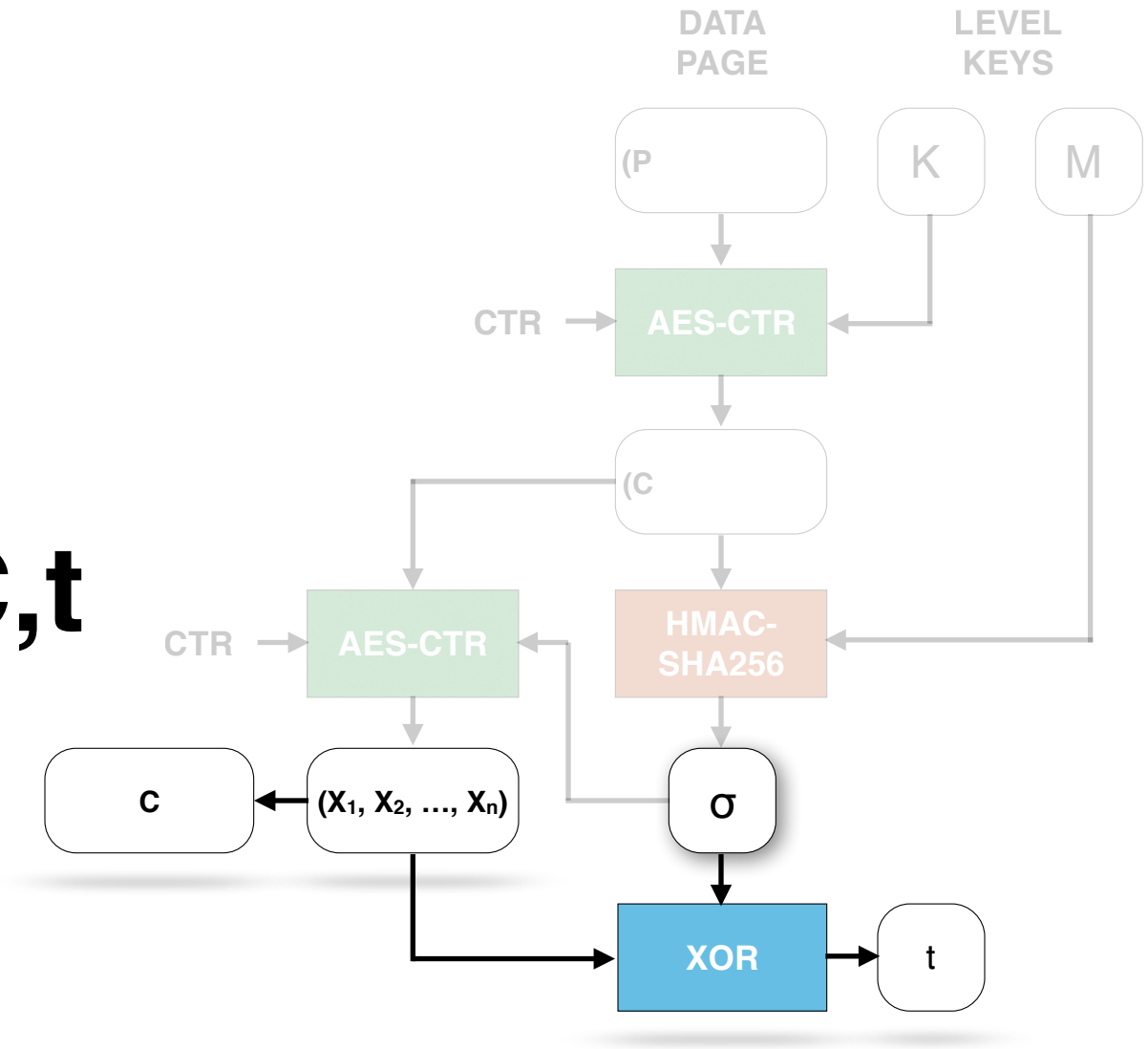
Transform

$$f(K_\ell, M_\ell, P) = C, t$$



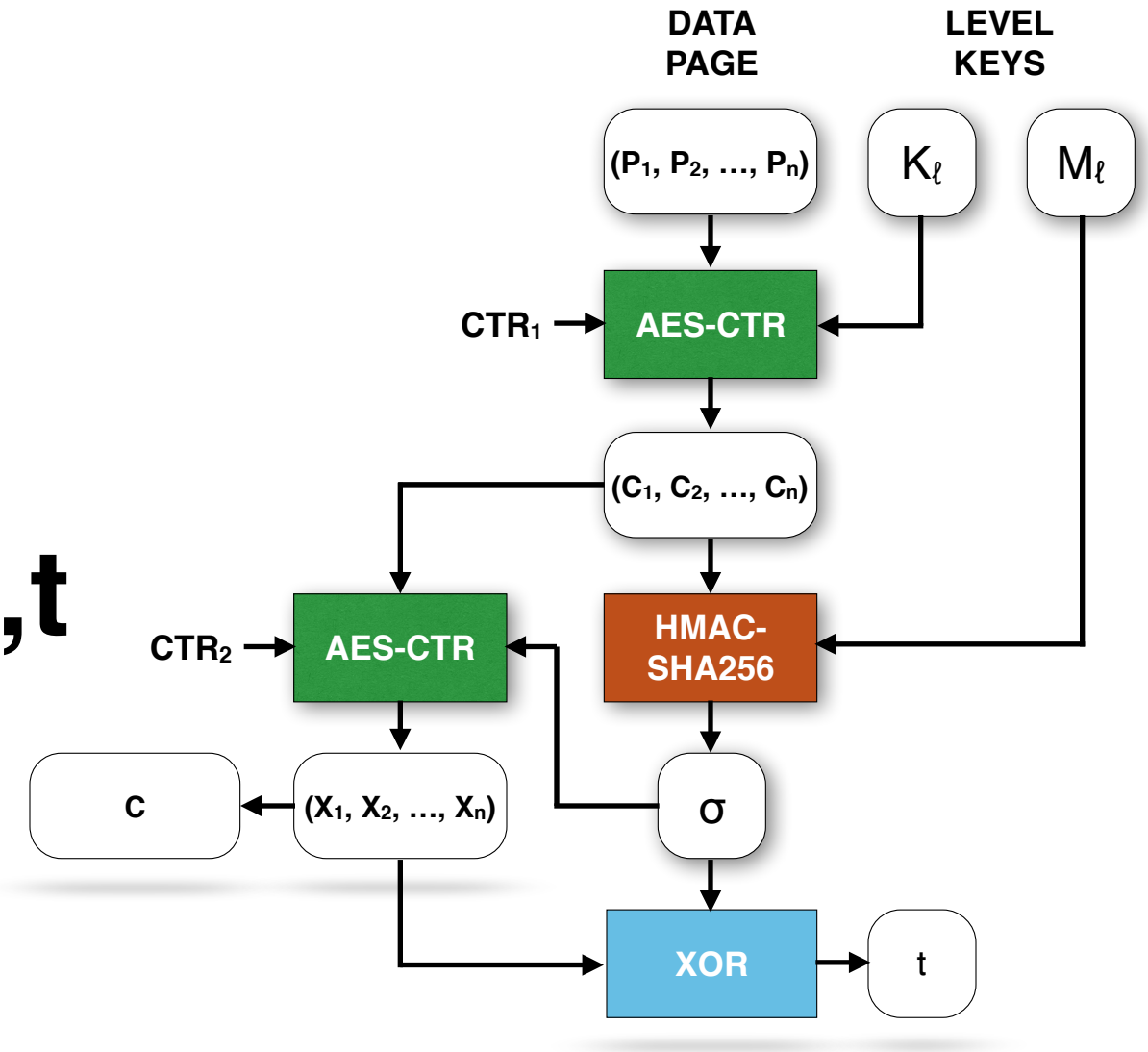
Transform

$$f(K_\ell, M_\ell, P) = C, t$$



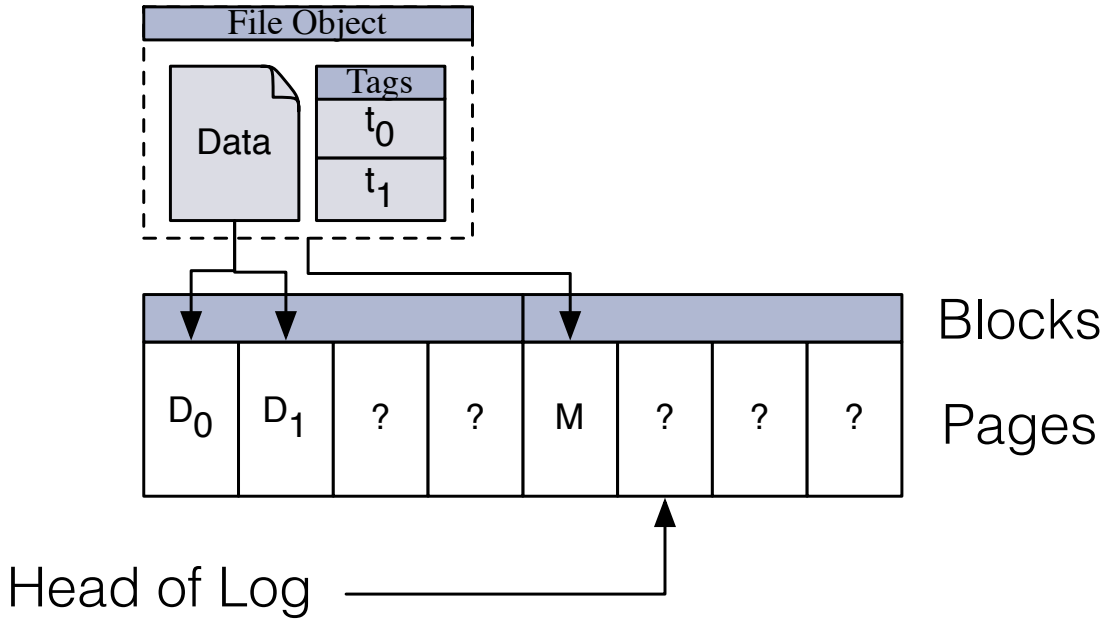
Transform

$$f(K_\ell, M_\ell, P) = C, t$$

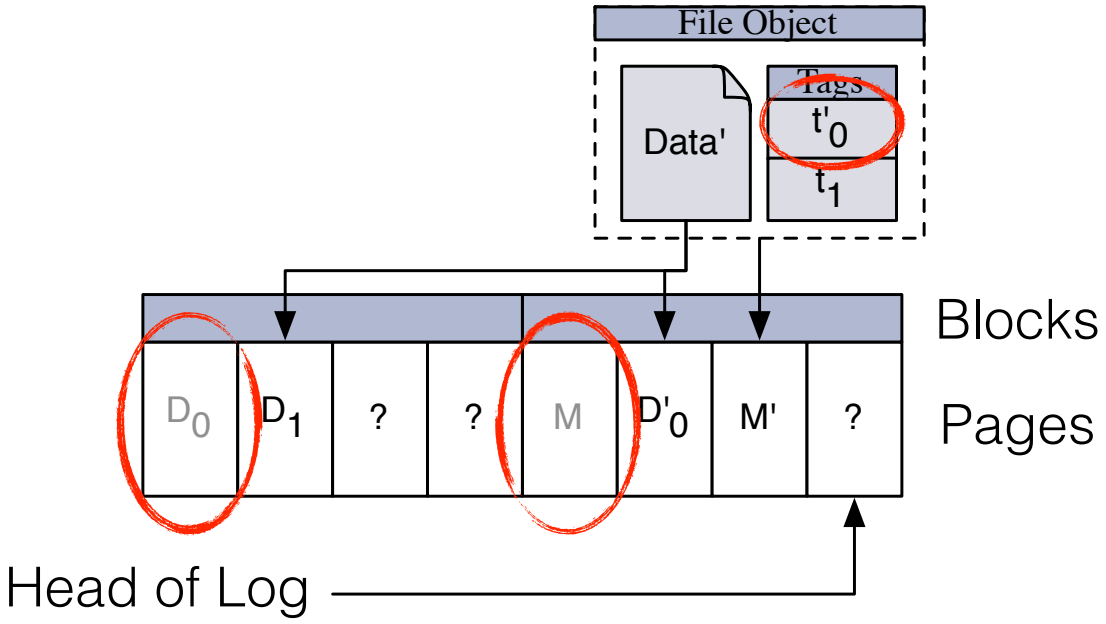


Deniable Writes

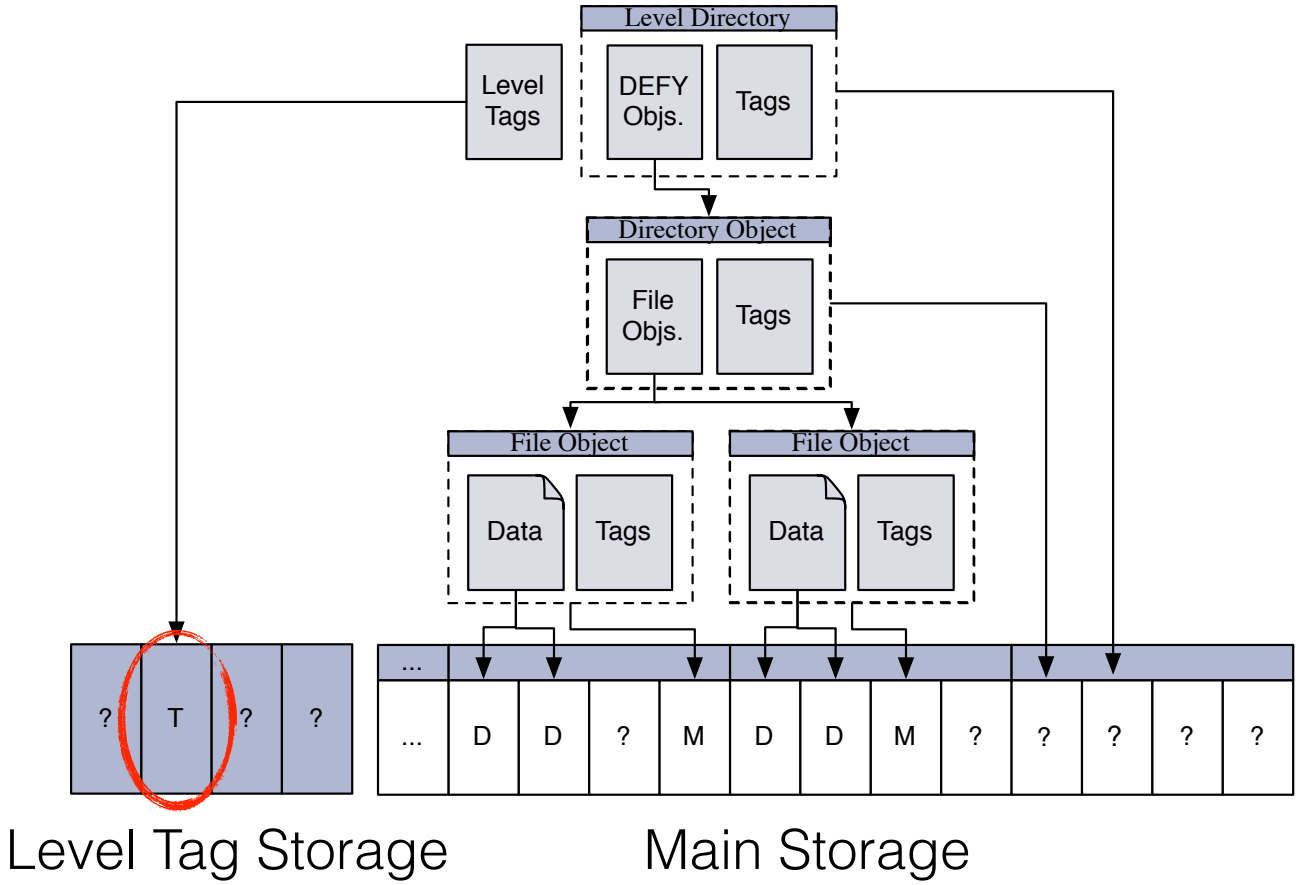
write(D',0)



Deniable Writes



Deniable Writes

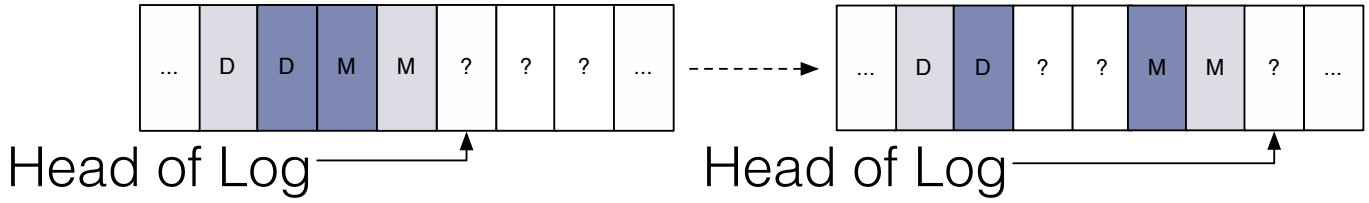


Security

deniability **lacks formality**

prior, single-view, solutions consider **indistinguishability over pages**

snapshot adversary requires **indistinguishability over file system states**

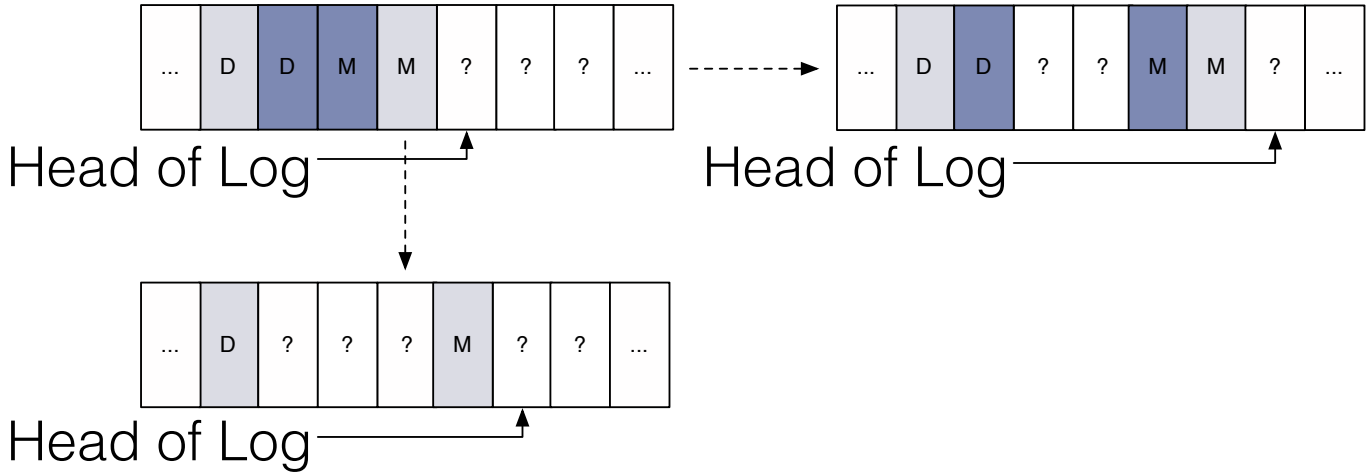


Security

update@ℓ_1

Security

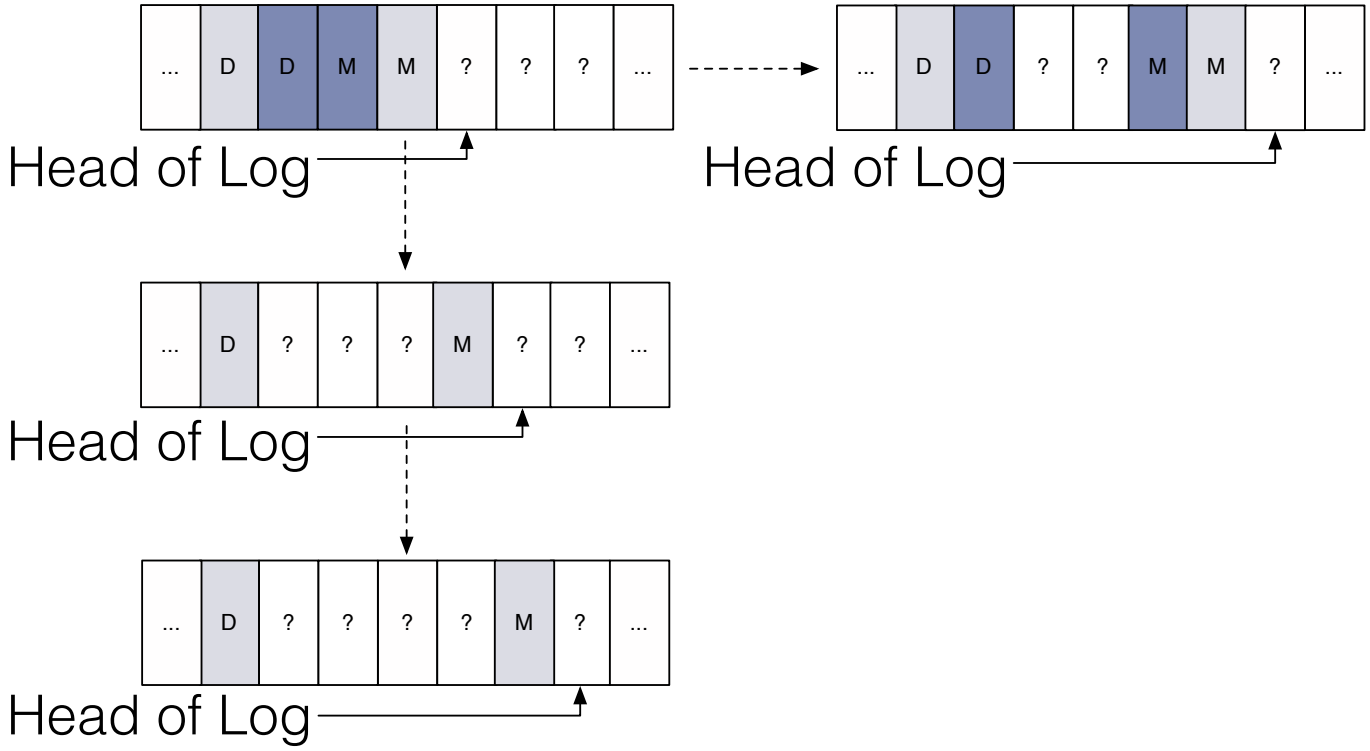
update@ℓ_0



Security

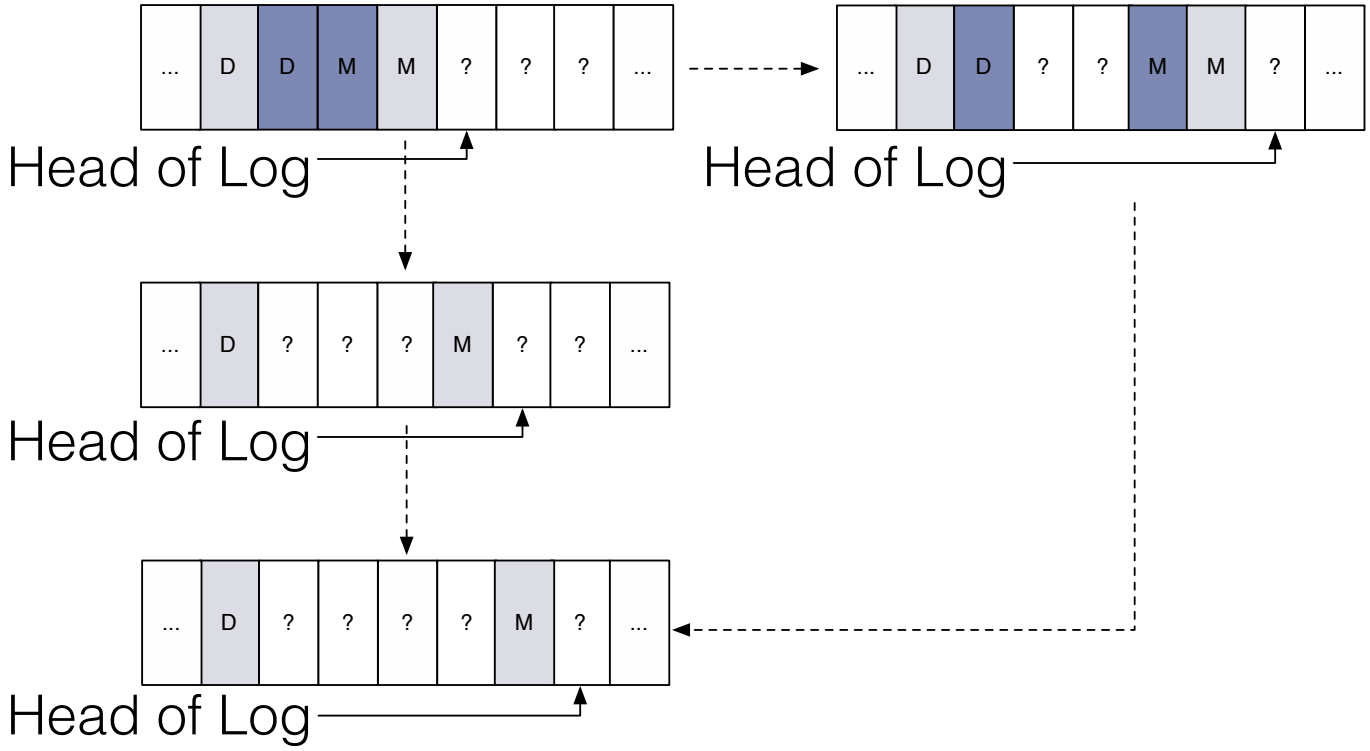
update@ℓ_0

update@ℓ_0



Security

update@ℓ_0
update@ℓ_0
hide@ℓ_1



DEFY
In Real Life

users must use system **correctly**

doesn't protect against **malware**

or **colluding carriers**

few have explored deniability OPSEC against **coercive adversaries**

Status & Future Work

DEFY is released as **free** and **open source** software

Confirm loss of **semantic security** in flash

Formalize notions of **deniability**

thanks