# RansomAir Filled with Clouds

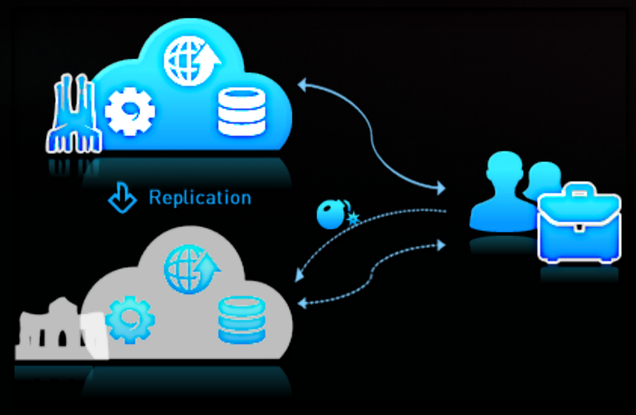
Dusko Pavlovic, Univesity of Hawaii

C3E, 23 October 2017, Atlanta GA

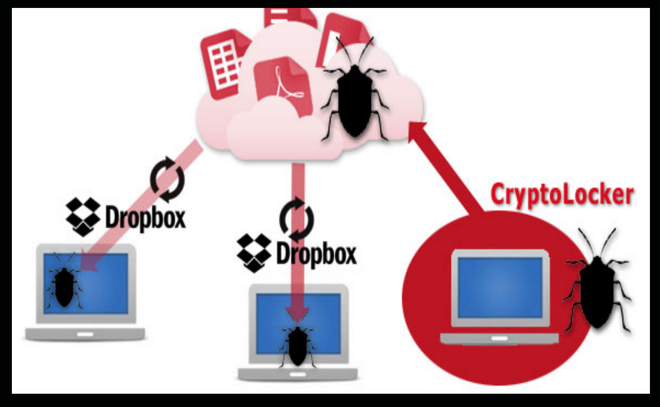
- Problem: ransom attacks

- Insight: data are different


- Solution: cloud storage



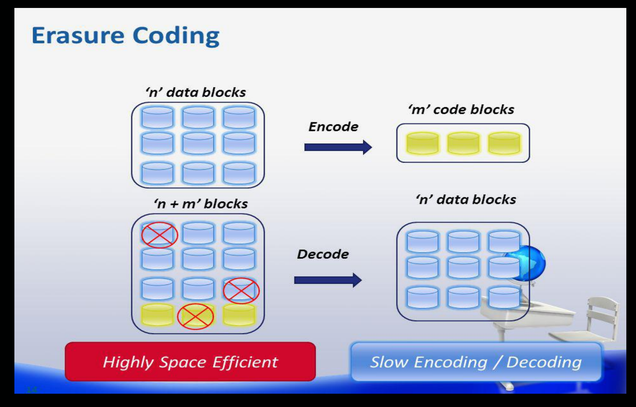

- PROBLEM: cloud security




Even lightweight encryption incurs **slowdown**

- INSIGHT: slow recovery ok
  - crypto requires ongoing fast decryption
  - data attacks are not ongoing
  - data recovery is rarely needed

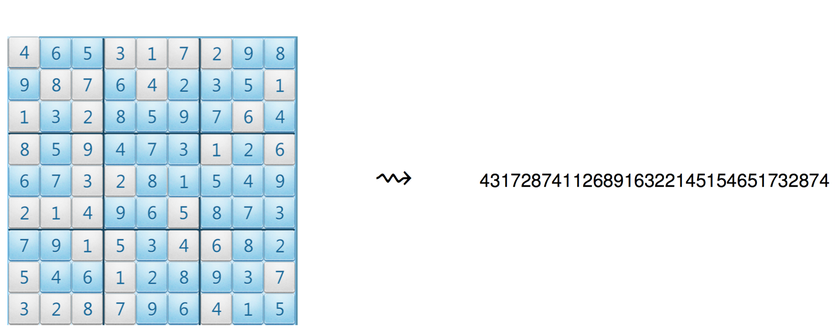
- SOLUTION: code, not crypto




Coding incurs **speedup**

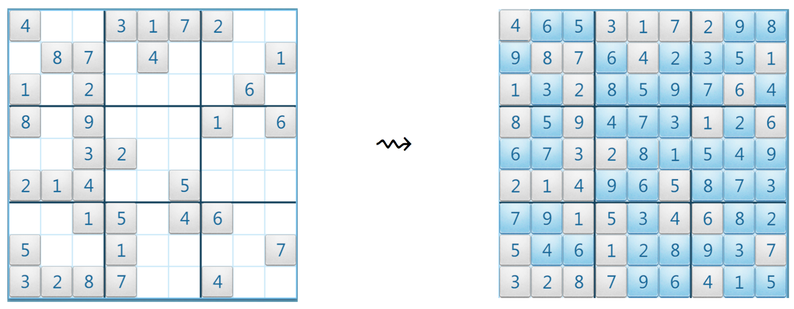
- **SOLUTION: deletion channel security**

Encoding (using sudoku)



$\rightsquigarrow$ 431728741126891632214515465173 2874

Decoding



Eavesdroping

431728741126891632214515465173 2874 $\rightsquigarrow$ Pr(*guess* 45 *digits*) $= 9^{-45}$

SPECIAL CYBER OPERATIONS RESEARCH AND ENGINEERING