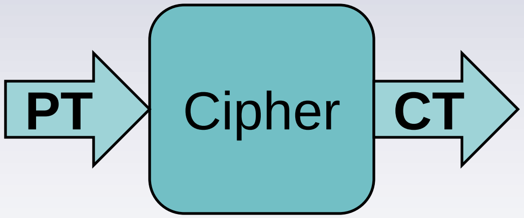
High Throughput Encryption for Flash Memories

Dmitri Varsanofiev, IP Cores, Inc.

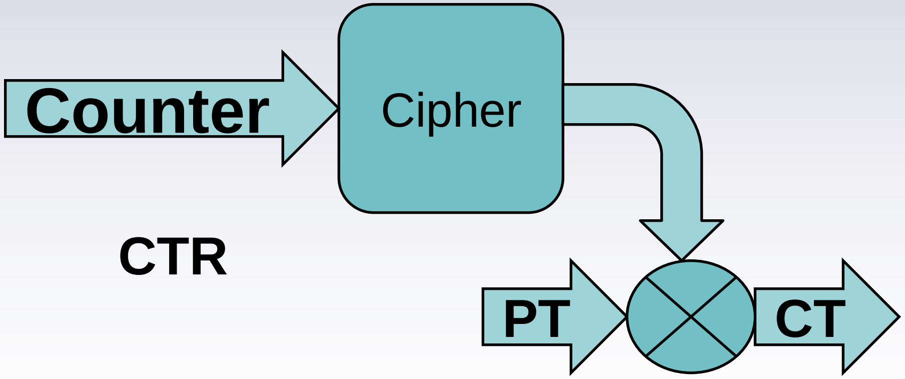
dima@ipcores.com

Terminology To-Go

- Block cipher encrypts its input arranged in “blocks” (usually 128 bits in size)
- Way to apply unencrypted data *(plaintext, PT)* to the cipher and use the output for to produce *ciphertext* (CT) is called **mode.**



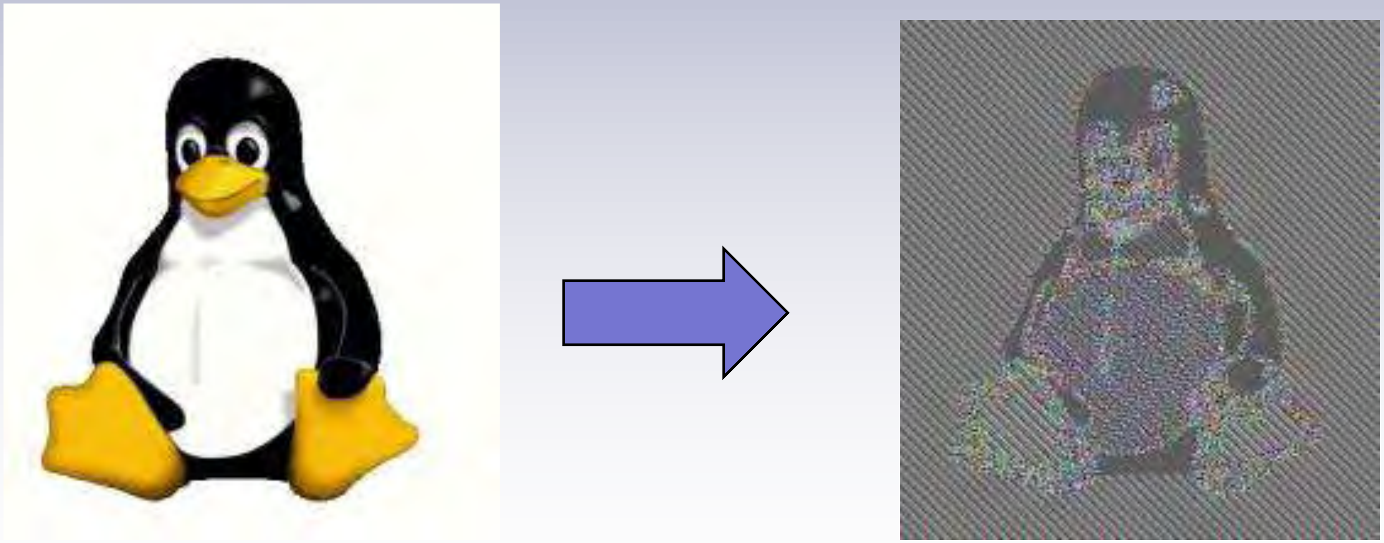
ECB



CTR

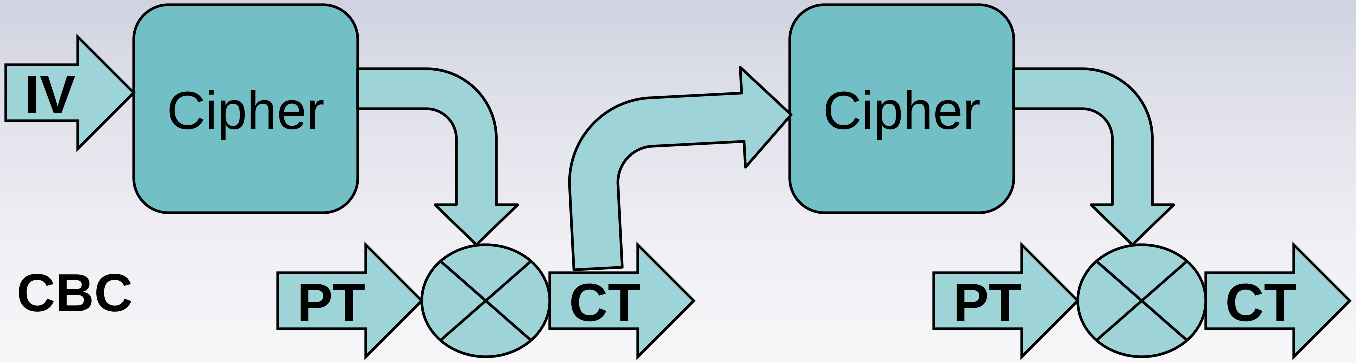
Terminology Continued

- Cipher will always convert same input into same output; thus the need to “tweak” the data for each location using initialization vector, IV
- Otherwise …



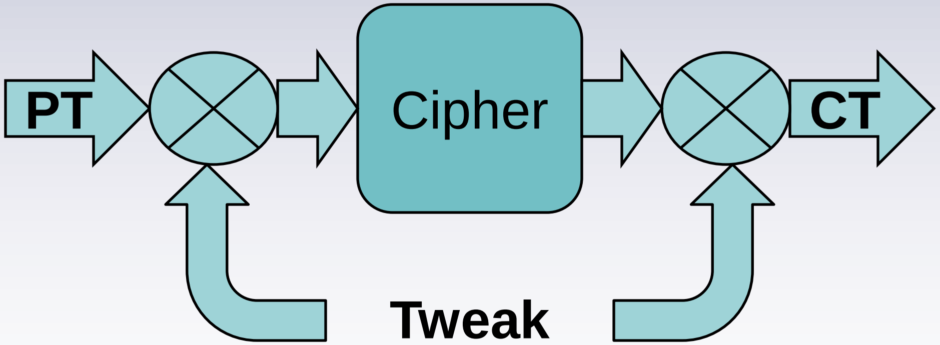
Tweaking: The Old Way

- Apply IV at the beginning and introduce the feedback: CBC mode
- Feedback limits the speed
  - 128 bits in the block / 10 rounds per block = 12.8 bits per clock maximum = 1.28 Gbps at 100 MHz clock



Tweaking: The New Way

- IEEE P1619
  - “XOR with a tweak-Encrypt-XOR”
  - ~~XEX~~ / ~~XTC~~ / XTS
    - – Strange hits on www.ipcores.com website ☺



PT

Cipher

CT

Tweak

Based on location

XTS

- Official name: XEX-based Tweaked codebook mode with ciphertext Stealing
- Completely parallel, no speed limit
  - 10-100 Gbps rates are easy even in FPGA
- “Narrow-block” (can independently rewrite as few as 128 bits)
- 100% utilization, no extra storage space required for IV

Authentication

- Ability to detect that the ciphertext was tampered with (without decryption)
  - The need depends on the threats
- For flash memory, main threat is media getting lost; tampering is therefore not a problem
- Authentication needs cryptographic “checksum”, *Message Authentication Code*, MAC – usually 128 bits

Authentication Continued

- Due to storage overhead required for MAC, “wide-block” (typically, page-sized) methods are used
- Modern high-speed method is Galois/Counter Mode (GCM)
  - Completely parallel, no speed limit
  - Requires storage for 96 bit IV and 128 bit MAC
- Never reuse GCM IV with the same key
  - Cannot use location as IV (unlike XTS)

Summary

- Add XTS encryption to your next flash design
- The silicon cost is very low; scalable cores start at just 15-20 thousands of ASIC gates for multiple Gbps of throughput
- Or …

References

- Wikipedia:
  - http://en.wikipedia.org/wiki/Disk_encryption_theory
  - http://en.wikipedia.org/wiki/Galois/Counter_Mode
- IP Cores, Inc. site:
  - http://ipcores.com/xts_aes_p1619_ip_core.htm
  - http://ipcores.com/macsec_802.1ae_gcm_aes_ip_core.htm