Data Security with SSD

Chris Tsu

Hangzhou Dianzi University

Lloyd Liu

Sage Microelectronics Corp. Hangzhou

Self-Encrypting Drive (SED)

- With a circuit build in disk drive controller
    - Encrypts all data into drive media
        - All SED encrypted all the time
        - Decrypt data automatically
    - Advanced Encryption Standard (AES) is de facto algorithm

- Transparent or invisible to the user once encryption key established
    - Key lost will equivalent to a full erase of media .

Encrypting Bridge Approach

- SED can be made with a interface bridge
  - Convert a commodity drive to SED for cost reason
  - Input and output interface not necessary to be the same
    - Example : USB to SATA bridge with encryption

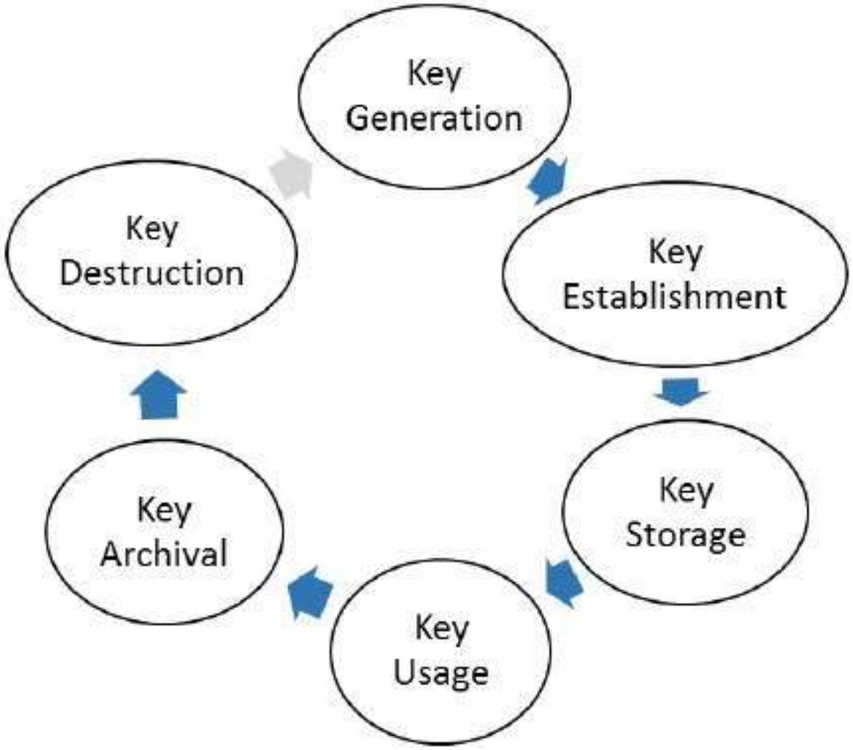
- Encrypting bridge can introduce more advanced function
  - Change SED encrypting algorithm from AES
  - Dynamic change drive partition with key protection
  - Help to establish new crypto standard to SED with min cost

Media Key and Key Encrypt Key

- **Synchronous and Asynchronous Key encryption**
- Media Encryption Key (MEK) is a Synchronous key
    - Data is encrypted by Media Key
    - Whole Data sectors group can only have one media key
    - Once Data is encrypted, It will stay with the Key
    - In general, Media key is hide inside the SSD
    - Attacker is always to break media key, not the data itself

- MEK has to protect by asynchronous key
    - Key encrypt Key (KEK) is the major challenge

Life Cycle of a SED Key Diagram



Life Cycle of a SED Media Key

- Generation of Media Key
  - Either by on board SED controller or third party pre load
- Backup and Storage
  - Hide within SED security boundary or remote backup
  - Distribution and Loading if remotely
- Normal Use and Replacement
  - Media Key can not be replaced during life cycle,
- Archival – For data no longer been active
- End of Key's Life Cycle – Change MEK = Erasure

Key Management(KMS) & Escrow

- Local Key management (WannaCry Proven?)
  - KEK is store on hide section, should not contact any OS
  - Usually use password to retrieve MEK from KEK

- Centralized key management
  - MEK is Encrypt by public key, and store in KMS at key generation phase
  - At boot time, SED acquired KEK from KMS, then decode by private key
  - X.509 certification is most common practice to transport KEK

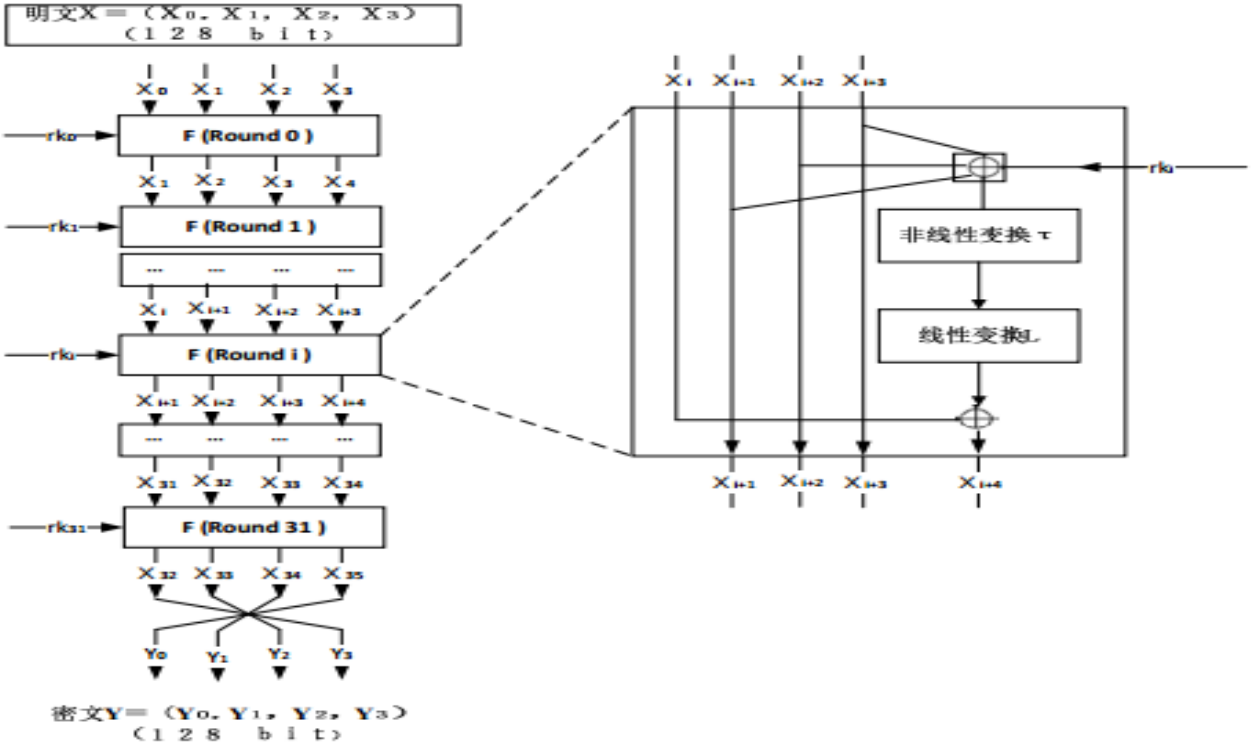
Chinese Crypto Standard

- China pushed its own encryption standard 1999
- Establish “commercial cryptography” testing lab 2006
  - Only certified products are allowed to be sold in China
  - Implements Commercial Cryptographic algorithms
  - Affect core function such as hardware such as
    - Hardware Security Module (HSM)
    - Smart Card Chip, Trust Platform Module(TPM)
    - USB token and flash driver.HDD/SSD
    - Software and firmware product are not affected
- Lawfully, no foreign encryption products are allowed to be sold or used in China

Published Algorithms

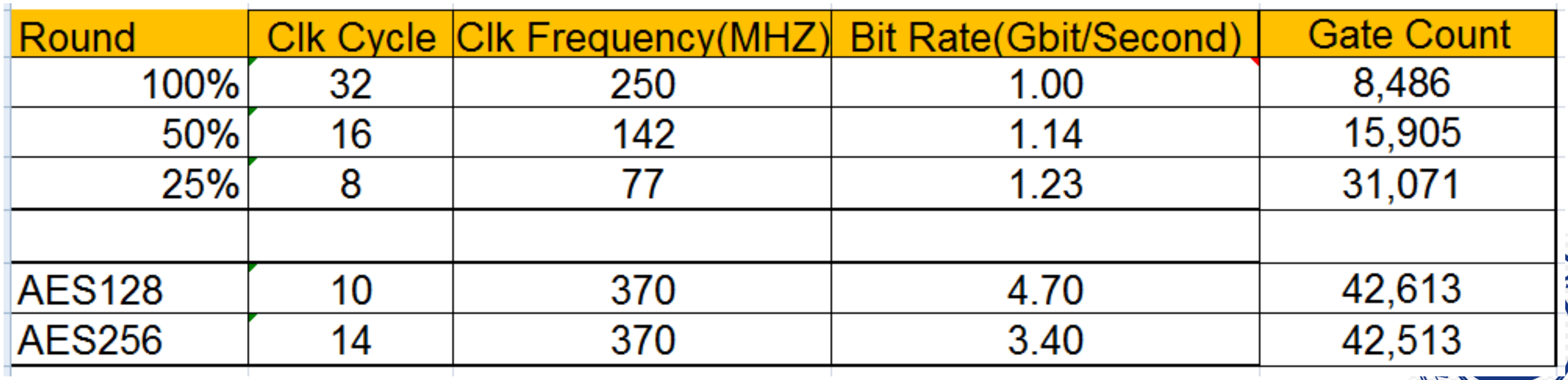
- SM2 – Elliptic Curve Cryptography (ECC)
  - Competitor of ECDSA
  - Use on Key Encryption Key (KEK)
- SM3 – Hash Function
  - Competitor of SHA-256
  - Together with SM2 and a Key Derivation function(KDF)
  - Use for Key transportation such as X.509
- SM4 – Block cipher symmetric algorithm
  - Competitor of AES-128
  - Use on Media Encryption Key (MEK)

SM4 Encryption Flow


明文X＝（X_0，X_1，X_2，X_3）
（128 bit）
X_0 X_1 X_2 X_3
rk_0
F (Round 0)
X_1 X_2 X_3 X_4
rk_1
F (Round 1)
--- --- --- ---
X_i X_{i+1} X_{i+2} X_{i+3}
rk_i
F (Round i)
X_{i+1} X_{i+2} X_{i+3} X_{i+4}
--- --- --- ---
X_{31} X_{32} X_{33} X_{34}
rk_{31}
F (Round 31)
X_{32} X_{33} X_{34} X_{35}
Y_0 Y_1 Y_2 Y_3
密文Y＝（Y_0，Y_1，Y_2，Y_3）
（128 bit）
X_i X_{i+1} X_{i+2} X_{i+3}
rk_i
非线性变换τ
线性变换L
X_{i+1} X_{i+2} X_{i+3} X_{i+4}

MEK SM4/AES 128 Efficiency

- Analysis is based on SMIC 55nm Proess.
- SM4 is 5 times slower due to its long logic chain delay
- AES logic counts are five times as SM4



Round	Clk Cycle	Clk Frequency(MHZ)	Bit Rate(Gbit/Second)	Gate Count
100%	32	250	1.00	8,486
50%	16	142	1.14	15,905
25%	8	77	1.23	31,071
AES128	10	370	4.70	42,613
AES256	14	370	3.40	42,513