Some properties of one mode of operation of block ciphers

Dmitriy Bogdanov, Vladislav Nozdrunov

2 June 2021 г.

Introduction

FDE

FDE – Full Disk Encryption.

Introduction

[1] DATA STORAGE SECURITY AND FULL DISK ENCRYPTION // E.K. Alekseev, L.R. Akhmetzyanova, A.A. Babueva, S.V. Smyshlyaev // Prikladnaya Diskretnaya Matematika, — V. 49, —- Pp. 78—97, 2020. (In Russian)

Introduction

FDE

FDE – Full Disk Encryption.

Features

Sectors – bit strings of fixed length l.

- Read and write in whole sectors
- No empty or incomplete sectors can exist

What has been studied?

DEC

DEC – Disk Encryption with Counter mode.

Who is mister DEC?

2020 г. Report to the TC 26 working group .

2021 г. RusCrypto'2021, Report «Encryption of data storage. DEC Mode » .

Features

DEC

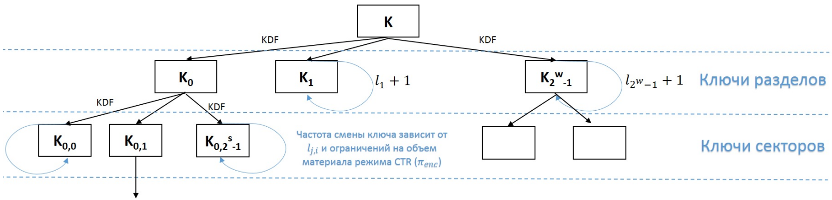
DEC – Disk Encryption with Counter mode.

Features

Partition — the set of s sectors.

- Data storage is represented as a set of partitions.
- Mechanisms from the documents of the national standardization system
- Need to store service information

KDF



Keys

K – master-key

From $K \rightarrow K_j$ by dint of KDF, j, l_j.

From $K_j \rightarrow K_{i,j}$ by dint of KDF, $j, i, l_{j,i}$

KDF From P 1323565.1.022-2018

How it encrypted?

How it encrypted?

Gamming. Keystream blocks are generated according to the rule

$$\Delta_t = e_{K_{j,i,l_{j,i}}}(CTR(i, l_{j,i}, t)),$$

где

$$CTR(i, l_{j,i}, t) = i || (l_{j,i} \cdot q) \boxplus t,$$

What means my name to you?..

CTR

$$CTR(i, l_{j,i}, t) = i||(l_{j,i} \cdot q) \boxplus t.$$

Parameters

j – section number

i – sector number in the partition

$l_{j,i}$ – count of number of encryptions

q – sector size in blocks

$t \in \{0, 1, \cdots, q-1\}$ – block number in sector

$\boxplus$ – addition in ring $\mathbb{Z}_{2^{\frac{n}{2}}}$

Remark

CTR

$$CTR(i, I_{j,i}, t) = i||(I_{j,i} \cdot q) \boxplus t.$$

Attention!

Sets $\{CTR(i, I_{j,i}, 0), CTR(i, I_{j,i}, 1), \cdots, CTR(i, I_{j,i}, q-1)\}$ either do not intersect or coincide.

Attention! coincide $\{CTR\}$ **not equal** coincidence of Keystream blocks.

Sector Key $= KDF(i, j, I_{j,i}, I_j)$.

Remarks and Problems

Attention!

If sets $\{CTR\}$ with different parameters are equal,
$\Rightarrow$ keys $K_{j,i,l_{j,i}}$ and $K_{j,i,l'_{j,i}}$ are different .
With a high probability . This probability must be estimated.

Problems: How many keys can we generate?

1. Based on the properties of KDF?
2. What a probability of coincidence $\{\Delta_t = e_{K_{j,i,l_{j,i}}}(CTR(i, l_{j,i}, t))\}$?

Remarks and Problems

Attention!

If sets $\{CTR\}$ with different parameters are equal,
$\Rightarrow$ keys $K_{j,i,l_{j,i}}$ and $K_{j,i,l'_{j,i}}$ are different .
With a high probability . This probability must be estimated.

Problems: How many keys can we generate?

1. **Based on the properties of KDF?**
2. What a probability of coincidence $\{\Delta_t = e_{K_{j,i,l_{j,i}}}(CTR(i, l_{j,i}, t))\}$?

Properties of KDF

Lemma 6 [2]

$$Adv_{kdf^2}^{prf^*}(t, q) \leq Adv_f^{prf}(t, \beta q) + \frac{\beta q(\beta q - 1)}{2^d}.$$

Estimate from work [3]

$$Adv_{CMAC}^{prf}(t, q, \rho n) \leq \frac{(5\rho^2 + 1)q^2}{2^n} + Adv_E^{prp}(t', q').$$

[2] Cryptographic Research Results and Rationale cryptographic qualities. Key Derivation Mechanisms // TK 26 // 2017. // (In Russian)
[3] OMAC: One-Key CBC MAC // T. Iwata, K. Kurosawa // Lecture Notes in Computer Science, — V. 2887, — Pp. 129–153, 2003

Advantages of block cipher

Magma [2]

$$Adv^{prp}_{E=\text{Magma}}(t, q) \leq \frac{t}{2^{192}} + \frac{q}{2^{64}}.$$

Kuznechik [2]

$$Adv^{prp}_{E=\text{Kuznechik}}(t, q) \leq \frac{t}{2^{256}} + \frac{q}{2^{128}}.$$

[2] Cryptographic Research Results and Rationale cryptographic qualities. Key Derivation Mechanisms // TK 26 // 2017. // (In Russian)

Catch them all!

Magma

In total for «Magma»

$$Adv^{prf^*}_{kdf^2}(t, q) \leq \frac{46096q^2}{2^{64}} + \frac{t'}{2^{192}} + \frac{96q+1}{2^{64}} + \frac{4q(4q-1)}{2^{1536}}.$$

Kuznechik

In total for «Kuznechik»

$$Adv^{prf^*}_{kdf^2}(t, q) \leq \frac{2884q^2}{2^{128}} + \frac{t'}{2^{256}} + \frac{24q+1}{2^{128}} + \frac{2q(2q-1)}{2^{1536}}.$$

Example

Magma

Let $t \le 2^{128}$, $q \le 2^{17}$. Then

$$Adv_{kdf^2}^{prf^*}(t, q) \le 10^{-3}.$$

Kuznechik

Let $t \le 2^{128}$, $q \le 2^{51}$. Then

$$Adv_{kdf^2}^{prf^*}(t, q) \le 10^{-3}.$$

Example

Kuznechik

Let $t \leq 2^{128}$, $q \leq 2^{51}$. Then

$$Adv_{kdf^2}^{prf^*}(t, q) \leq 10^{-3}.$$

Example

Typical 1TB consumer SSD drive. Record / rewrite resource is 1200 TB $\approx 2^{54}$ bits. Size of sector is 2^{12} or 2^{15} bits.

Example

Kuznechik

Let $t \leq 2^{128}$, $q \leq 2^{51}$. Then

$$Adv_{kdf^2}^{prf^*}(t, q) \leq 10^{-3}.$$

Example

Typical 1TB consumer SSD drive. Record / rewrite resource is 1200 TB $\approx 2^{54}$ bits. Size of sector is 2^{12} or 2^{15} bits.
$\Rightarrow$ One partition key is enough for the entire lifetime, even if a new sector key is generated for each write to the sector.

Problems

Problems: How many keys can we generate?

1. Based on the properties of KDF?
2. **What a probability of coincidence** $\{\Delta_t = e_{K_{j,i,l_{j,i}}}(CTR(i, l_{j,i}, t))\}$?

Model

Mathematical model

$x_1, \cdots, x_N \in \mathcal{X}$, where $\mathcal{X}$ – some set, $x_i \neq x_j$ if $i \neq j$.

$\mathcal{E} : \overline{x} \to \mathcal{X}$ – injective functions .

$E_1, \cdots, E_K \in \mathcal{E}$ – ordered set .

Model

Mathematical model

$x_1, \cdots, x_N \in \mathcal{X}$, where $\mathcal{X}$ – some set, $x_i \neq x_j$ if $i \neq j$.

$\mathcal{E} : \overline{x} \to \mathcal{X}$ – injective functions .

$E_1, \cdots, E_K \in \mathcal{E}$ – ordered set .

$\xi_{i,j}$, $i \in \{1, \cdots, M\}$, $j \in \{1, \cdots, N\}$ – independent random variables uniformly distributed on set $\{1, \cdots, K\}$.

Event $A : \exists i, i' \in \{1, \cdots, M\}$, $j, j' \in \{1, \cdots, N\}$, $(i, j) \neq (i', j')$, such that $E_{\xi_{i,j}}(j) = E_{\xi_{i',j'}}(j')$

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

What is what?

$x_j \leftrightarrow \{CTR(i, l_{j,i}, t),\ \ t = 0, \cdots, q-1\}$

$\xi_{i,j} \leftrightarrow$ sector key $K_{i,j}$

$E_{\xi_{i,j}}(j) \leftrightarrow \{\Delta_0, \Delta_1, \cdots, \Delta_{q-1}\}$ — keystream blocks.

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

What are we estimating?

$$A = \bigcup_{k \leq l}^{N} A^{k,l}, \text{ and } Pr[A] \leq \sum_{k \leq l}^{N} Pr[A^{k,l}]$$

$A^{k,l}$ – collision between elements of k-th and l-th column.

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

How are we estimating

Events $A^{k,l}_{i,i'}$: $E_{\xi_{i,k}}(x_k) = E_{\xi_{i',l}}(x_l)$
2 cases: collision in one column, collision in different columns .

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

How are we estimating?

1 case. Collision in one column

$A^{k,k}$: either the «keys» match, or the «keys» are different.

$Pr[A^{k,k}_{i,i'}] = \frac{1}{K} + \frac{K-1}{|Q| \cdot K}$.

Sum by (i, i').

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

How are we estimating?

2 case. collision in different columns

$A^{k,l}$: either the «keys» match, or the «keys» are different.

$Pr[A^{k,k}_{i,i'}] = \frac{K-1}{|Q|\cdot K}$.

Sum by (i, i').

Model

x_1	x_2	x_3	$\cdots$	x_N
$E_{\xi_{1,1}}(x_1)$	$E_{\xi_{1,2}}(x_2)$	$E_{\xi_{1,3}}(x_3)$	$\cdots$	$E_{\xi_{1,N}}(x_N)$
$E_{\xi_{2,1}}(x_1)$	$E_{\xi_{2,2}}(x_2)$	$E_{\xi_{2,3}}(x_3)$	$\cdots$	$E_{\xi_{2,N}}(x_N)$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$E_{\xi_{M,1}}(x_1)$	$E_{\xi_{M,2}}(x_2)$	$E_{\xi_{M,3}}(x_3)$	$\cdots$	$E_{\xi_{M,N}}(x_N)$

How are we estimating?

2 case. collision in different columns

$A^{k,l}$: either the «keys» match, or the «keys» are different.

$Pr[A^{k,k}_{i,i'}] = \frac{K-1}{|Q| \cdot K}$.

Sum by (i, i').

Model

In total

$$Pr[A] \leq \frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}$$

What is what?

K – cardinality of the set of keys (2^{256})
Q – cardinality of the keystream blocks (2^{qn})
N – number of different sets $\{CTR(i, l_{j,i}, t),\ t = 0, \cdots, q-1\}$ M – number of encryptions per set CTR (depends from the number of sections).
NM – total number of encryptions.

Model

In total

$$Pr[A] \leq \frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}$$

Example

typical 1TB consumer SSD drive. Record / rewrite resource is 1200 TB $\approx 2^{54}$ bits. Size of sector is 4096 bits.

$NM \leq 2^{54}$

$M \leq 2^{54}$

$$Pr[A] \leq \frac{2^{104}}{2^{256}} + \frac{2^{104}}{2^{4096}}$$

Consequence

In total

$$Pr[A] \leq \frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}$$

Question

With $NM = const$ what is the «worst» situation?

Consequence

In total

$$Pr[A] \leq \frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}$$

Question

With $NM = const$ what is the «worst» situation?

Consequence

Fix $NM = const$. Sturm's method. Consider $N' = \frac{N}{\Delta}$, $M' = \Delta \cdot M$, $\Delta > 1$.

Consequence

In total

$$Pr[A] \leq \frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}$$

Question

With $NM = const$ what is the «worst» situation?

Consequence

Fix $NM = const$. Sturm's method. Consider $N' = \frac{N}{\Delta}$, $M' = \Delta \cdot M$, $\Delta > 1$.

How will the estimate is change?

Consequence

Consequence

$$\frac{NM(\Delta \cdot M - 1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K} >$$
$$\frac{NM(M-1)}{2K} + \frac{NM(K-1)(NM-1)}{2|Q| \cdot K}.$$

Conclusions

Consequence

A decrease of the number of sections leads to a decrease in the score for the probability of collisions (as well as to a decrease in the amount of service information) .

Conclusions

1.An approach for determining the maximum allowable number of generated keys for sectors with predetermined cryptographic properties is presented.
2.An estimate of the probability of collision of gammas is given, provided that the keys are equally probable.

Some properties of one mode of operation of block ciphers

Dmitriy Bogdanov, Vladislav Nozdrunov

2 June 2021 г.