Some properties of one mode of operation of block ciphers

Dmitriy Bogdanov, Vladislav Nozdrunov

2 June 2021 r.
Some properties of one mode of operation of block ciphers
FDE and DEC

Introduction

FDE
FDE – Full Disk Encryption.

Introduction

Some properties of one mode of operation of block ciphers
FDE and DEC

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
Some properties of one mode of operation of block ciphers
FDE and DEC

What has been studied?

DEC
DEC – Disk Encryption with Counter mode.

Who is mister DEC?

2020 г. Report to the TC 26 working group.
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
Some properties of one mode of operation of block ciphers

FDE and DEC

**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
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

$$CTR(i, l_j,i, t) = i \parallel (l_j,i \cdot q) \oplus t,$$
CTR

\[ CTR(i, l_j, i, t) = i \|(l_j, i \cdot q) \oplus t. \]

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
- \( \oplus \) – addition in ring \( \mathbb{Z}_{2^n} \)
Some properties of one mode of operation of block ciphers
FDE and DEC

Remark

$$CTR(i, l_j, i, t) = i || (l_j, i \cdot q) ⊕ t.$$  

Attention!

Sets \{CTR(i, l_j, i, 0), CTR(i, l_j, i, 1), \ldots, CTR(i, l_j, i, q - 1)\} either do not intersect or coincide.

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

Sector Key = KDF(i, j, l_j, i, l_j).
Some properties of one mode of operation of block ciphers
FDE and DEC

Remarks and Problems

Attention!
If sets \( \{ \text{CTR} \} \) 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
\( \{ \Delta_t = e_{K_{j,i,l_{j,i}}(\text{CTR}(i, l_{j,i}, t))} \} \)?
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
   \[ \{\Delta_t = e_{K_{j,i,l_{j,i}}} (CTR(i, l_{j,i}, t))\} \]?
Some properties of one mode of operation of block ciphers

KDF

Properties of KDF

Lemma 6 [2]

\[ \text{Adv}^{\text{prf}^*}_{\text{kdf}^2}(t, q) \leq \text{Adv}^{\text{prf}}_f(t, \beta q) + \frac{\beta q(\beta q - 1)}{2^d}. \]

Estimate from work [3]

\[ \text{Adv}^{\text{prf}}_{\text{CMAC}}(t, q, \rho n) \leq \frac{(5\rho^2 + 1)q^2}{2^n} + \text{Adv}^{\text{prp}}_E(t', q'). \]


Advantages of block cipher

<table>
<thead>
<tr>
<th>Property</th>
<th>Formula</th>
</tr>
</thead>
<tbody>
<tr>
<td>Magma [2]</td>
<td>( \text{Adv}_{E=\text{Magma}}^{\text{prp}}(t, q) \leq \frac{t}{2^{192}} + \frac{q}{2^{64}} )</td>
</tr>
<tr>
<td>Kuznechik [2]</td>
<td>( \text{Adv}_{E=\text{Kuznechik}}^{\text{prp}}(t, q) \leq \frac{t}{2^{256}} + \frac{q}{2^{128}} )</td>
</tr>
</tbody>
</table>

Some properties of one mode of operation of block ciphers

KDF

Catch them all!

**Magma**

In total for «Magma»

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

**Kuznechik**

In total for «Kuznechik»

$$Adv_{kdf^2}^{prf^*}(t, q) \leq \frac{2884q^2}{2^{128}} + \frac{t'}{2^{256}} + \frac{24q + 1}{2^{128}} + \frac{2q(2q - 1)}{2^{1536}}.$$
Some properties of one mode of operation of block ciphers

KDF

Example

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

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

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

$$\text{Adv}_{kdf^2}^{prf^*}(t, q) \leq 10^{-3}.$$
Some properties of one mode of operation of block ciphers

KDF

Example

Kuznechik

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

$$\text{Adv}_{prf^*}^{kdf_2}(t, q) \leq 10^{-3}.$$  

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.
Some properties of one mode of operation of block ciphers

KDF

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.
Some properties of one mode of operation of block ciphers

Collision probability

Problems

Problems: How many keys can we generate?

1. Based on the properties of KDF?
2. What a probability of coincidence
   \[ \{\Delta_t = e_{\kappa_{j,i,l_j,i}}(CTR(i, l_j,i, t)) \} \]?
Mathematical model

\( x_1, \cdots, x_N \in X, \) where \( X \) – some set, \( x_i \neq x_j \) if \( i \neq j \).

\( \mathcal{E} : \overline{X} \rightarrow X \) – injective functions.

\( E_1, \cdots, E_K \in \mathcal{E} \) – ordered set.
Some properties of one mode of operation of block ciphers

Collision probability

Mathematical model

Model

Mathematical model

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

\( \mathcal{E} : \mathcal{X} \rightarrow \mathcal{X} \) - 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 \( E_{\xi_{i,j}}(j) = E_{\xi_{i',j'}}(j') \)
Some properties of one mode of operation of block ciphers

Collision probability

Mathematical model

Model

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$\cdots$</th>
<th>$x_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{\xi_{1,1}}(x_1)$</td>
<td>$E_{\xi_{1,2}}(x_2)$</td>
<td>$E_{\xi_{1,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{1,N}}(x_N)$</td>
</tr>
<tr>
<td>$E_{\xi_{2,1}}(x_1)$</td>
<td>$E_{\xi_{2,2}}(x_2)$</td>
<td>$E_{\xi_{2,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{2,N}}(x_N)$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$E_{\xi_{M,1}}(x_1)$</td>
<td>$E_{\xi_{M,2}}(x_2)$</td>
<td>$E_{\xi_{M,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{M,N}}(x_N)$</td>
</tr>
</tbody>
</table>

What is what?

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

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

$E_{\xi_{i,j}}(j) \leftrightarrow \{ \Delta_0, \Delta_1, \cdots, \Delta_{q-1} \} — \text{keystream blocks.}$
Some properties of one mode of operation of block ciphers
Collision probability
Mathematical model

Model

What are we estimating?

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

\( A^{k,l} \) – collision between elements of \( k \)-th and \( l \)-th column.
Some properties of one mode of operation of block ciphers

Collision probability
Mathematical model

Model

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$\cdots$</th>
<th>$x_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{\xi_{1,1}}(x_1)$</td>
<td>$E_{\xi_{1,2}}(x_2)$</td>
<td>$E_{\xi_{1,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{1,N}}(x_N)$</td>
</tr>
<tr>
<td>$E_{\xi_{2,1}}(x_1)$</td>
<td>$E_{\xi_{2,2}}(x_2)$</td>
<td>$E_{\xi_{2,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{2,N}}(x_N)$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$E_{\xi_{M,1}}(x_1)$</td>
<td>$E_{\xi_{M,2}}(x_2)$</td>
<td>$E_{\xi_{M,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{M,N}}(x_N)$</td>
</tr>
</tbody>
</table>

How are we estimating

Events $A_{i,j}^{k,l}$: $E_{\xi_{i,k}}(x_k) = E_{\xi_{i',l}}(x_l)$

2 cases: collision in one column, collision in different columns.
Some properties of one mode of operation of block ciphers

Collision probability

Estimate

Model

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>...</th>
<th>$x_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{\xi_{1,1}}(x_1)$</td>
<td>$E_{\xi_{1,2}}(x_2)$</td>
<td>$E_{\xi_{1,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{1,N}}(x_N)$</td>
</tr>
<tr>
<td>$E_{\xi_{2,1}}(x_1)$</td>
<td>$E_{\xi_{2,2}}(x_2)$</td>
<td>$E_{\xi_{2,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{2,N}}(x_N)$</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$E_{\xi_{M,1}}(x_1)$</td>
<td>$E_{\xi_{M,2}}(x_2)$</td>
<td>$E_{\xi_{M,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{M,N}}(x_N)$</td>
</tr>
</tbody>
</table>

How are we estimating?

1 case. Collision in one column

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

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

Sum by $(i, i')$. 
Some properties of one mode of operation of block ciphers

Collision probability

Estimate

Model

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$\cdots$</th>
<th>$x_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{\xi_{1,1}}(x_1)$</td>
<td>$E_{\xi_{1,2}}(x_2)$</td>
<td>$E_{\xi_{1,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{1,N}}(x_N)$</td>
</tr>
<tr>
<td>$E_{\xi_{2,1}}(x_1)$</td>
<td>$E_{\xi_{2,2}}(x_2)$</td>
<td>$E_{\xi_{2,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{2,N}}(x_N)$</td>
</tr>
<tr>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\vdots$</td>
<td>$\cdots$</td>
<td>$\vdots$</td>
</tr>
<tr>
<td>$E_{\xi_{M,1}}(x_1)$</td>
<td>$E_{\xi_{M,2}}(x_2)$</td>
<td>$E_{\xi_{M,3}}(x_3)$</td>
<td>$\cdots$</td>
<td>$E_{\xi_{M,N}}(x_N)$</td>
</tr>
</tbody>
</table>

How are we estimating?

2 case. collision in different columns

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

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

Sum by $(i, i').$
Some properties of one mode of operation of block ciphers

Collision probability

Estimate

Model

<table>
<thead>
<tr>
<th>$x_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>...</th>
<th>$x_N$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$E_{\xi_{1,1}}(x_1)$</td>
<td>$E_{\xi_{1,2}}(x_2)$</td>
<td>$E_{\xi_{1,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{1,N}}(x_N)$</td>
</tr>
<tr>
<td>$E_{\xi_{2,1}}(x_1)$</td>
<td>$E_{\xi_{2,2}}(x_2)$</td>
<td>$E_{\xi_{2,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{2,N}}(x_N)$</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>$E_{\xi_{M,1}}(x_1)$</td>
<td>$E_{\xi_{M,2}}(x_2)$</td>
<td>$E_{\xi_{M,3}}(x_3)$</td>
<td>...</td>
<td>$E_{\xi_{M,N}}(x_N)$</td>
</tr>
</tbody>
</table>

How are we estimating?

2 case. collision in different columns

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

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

Sum by $(i, i')$. 
Some properties of one mode of operation of block ciphers

Collision probability

Model

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

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 \(\{CTR(i, l_{ij}, t), t = 0, \cdots, q - 1\}\)
- \( M \) – number of encryptions per set \(CTR\) (depends from the number of sections).
- \( NM \) – total number of encryptions.
Some properties of one mode of operation of block ciphers
Collision probability
Estimate

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.
\( NM \leq 2^{54} \)
\( M \leq 2^{54} \)

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

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?
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 $N' = \frac{N}{\Delta}$, $M' = \Delta \cdot M$, $\Delta > 1$. 

Some properties of one mode of operation of block ciphers

Collision probability

Consequence

In total

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

Question

With \( NM = \text{const} \) what is the «worst» situation?

Consequence

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

How will the estimate change?
Some properties of one mode of operation of block ciphers
Collision probability

\[ \text{Consequence} \]

\[
\frac{NM(\Delta \cdot M - 1)}{2K} + \frac{NM(K - 1)(NM - 1)}{2|Q| \cdot K} > \frac{NM(M - 1)}{2K} + \frac{NM(K - 1)(NM - 1)}{2|Q| \cdot K}.
\]
Some properties of one mode of operation of block ciphers

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

Collision probability

Consequence

Dmitriy Bogdanov, Vladislav Nozdrunov

2 June 2021 r.