# An approach to the analysis of CryptoPro KeyMeshing

Anton Naumenko

Yaroslavl, 2016

# Specification of CryptoPro Key Meshing

Let we have

*C = {0x22720069L, 0x2304C964L, 0x96DB3A8DL, 0xC42AE946L, 0x94ACFE18L, 0x1207ED00L, 0xC2DC86C0L, 0x2BA94CEFL}.*

and a random key

$$K_0 \in \{0,1\}^{256}$$

Key Meshing is

$$K_{r+1}(K_0) = Decrypt_{K_r(K_0)}(C), r = 0,1,\ldots$$

# Basic properties of CryptoPro Key Meshing

For any $r \geq 1$ *and* $K_0$

$$K_r(K_0) \in B, B = \{(x_0||x_1||x_2||x_3); x_i \in \{0,1\}^{64}, x_i \neq x_j, i \neq j\}.$$

*Denote*

$$B_r = \bigcup_{K_0} \{K_r(K_0)\}.$$

***Property 1***

$$B \supseteq B_1 \supseteq B_2 \supseteq \ldots \supseteq B_r \supseteq B_{r+1} \supseteq \ldots$$

# Main results

If we consider CryptoPro Key Meshing as ***random mapping*** then (see Odlyzko 1990, Mironkin 2014):

$$E(|B_r|) = (1-\tau_r)|B|; \; where \; \tau_1 = e^{-1}; \; \tau_{i+1} = e^{-1+\tau_i}.$$

**Proposition 1**

$$1-\tau_r = \frac{2}{r} + \frac{2}{3r^3} + O\left(r^{-4}\right).$$

**Note**

Elements of the set $B_r$ have different probabilities (in considering model)

Let $\Psi_r$ - probability distribution on elements of key set $B_r$ .

Denote Shannon entropy as $H(\Psi_T)$ .

**Proposition 2**

$$H(\Psi_r) \approx \log_2 |B| - 2 \cdot \ln 2 \cdot \log_2 r - C,$$

$$C = 1.61...$$

infotecs

# Thanks for Attention!

# Questions?