

Особенности шифра Belt
Ф.М. Малышев

СТCrypt 2026 Минск

$$F_\theta: V_{128} \rightarrow V_{128}, \quad \theta = (\theta_1, \dots, \theta_8) \in V_{32}^8 = V_{256}$$

$$(\theta, \theta, \theta, \theta, \theta, \theta, \theta) = (\tau^{(1)}, \dots, \tau^{(8)}) \in (V_{32}^7)^8,$$

$$\tau^{(1)} : \theta_1 \ \theta_2 \ \theta_3 \ \theta_4 \ \theta_5 \ \theta_6 \ \theta_7$$

$$\tau^{(2)} : \theta_8 \ \theta_1 \ \theta_2 \ \theta_3 \ \theta_4 \ \theta_5 \ \theta_6$$

$$\tau^{(3)} : \theta_7 \ \theta_8 \ \theta_1 \ \theta_2 \ \theta_3 \ \theta_4 \ \theta_5$$

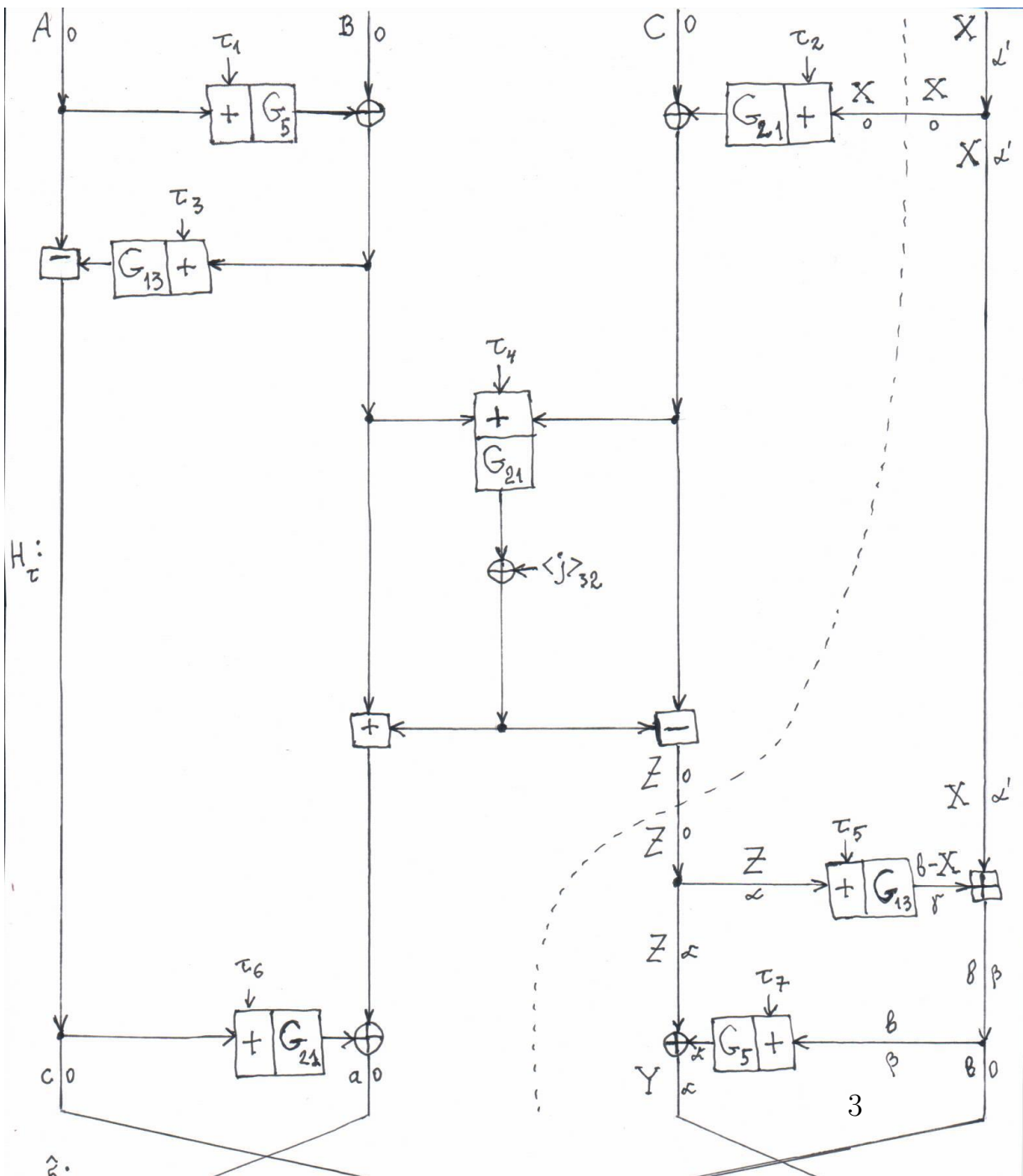
$$\tau^{(4)} : \theta_6 \ \theta_7 \ \theta_8 \ \theta_1 \ \theta_2 \ \theta_3 \ \theta_4$$

$$\tau^{(5)} : \theta_5 \ \theta_6 \ \theta_7 \ \theta_8 \ \theta_1 \ \theta_2 \ \theta_3$$

$$\tau^{(6)} : \theta_4 \ \theta_5 \ \theta_6 \ \theta_7 \ \theta_8 \ \theta_1 \ \theta_2$$

$$\tau^{(6)} : \theta_3 \ \theta_4 \ \theta_5 \ \theta_6 \ \theta_7 \ \theta_8 \ \theta_1$$

$$\tau^{(8)} : \theta_2 \ \theta_3 \ \theta_4 \ \theta_5 \ \theta_6 \ \theta_7 \ \theta_8$$



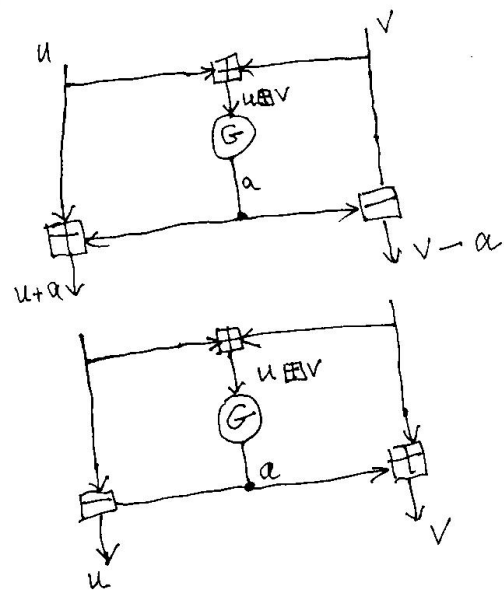
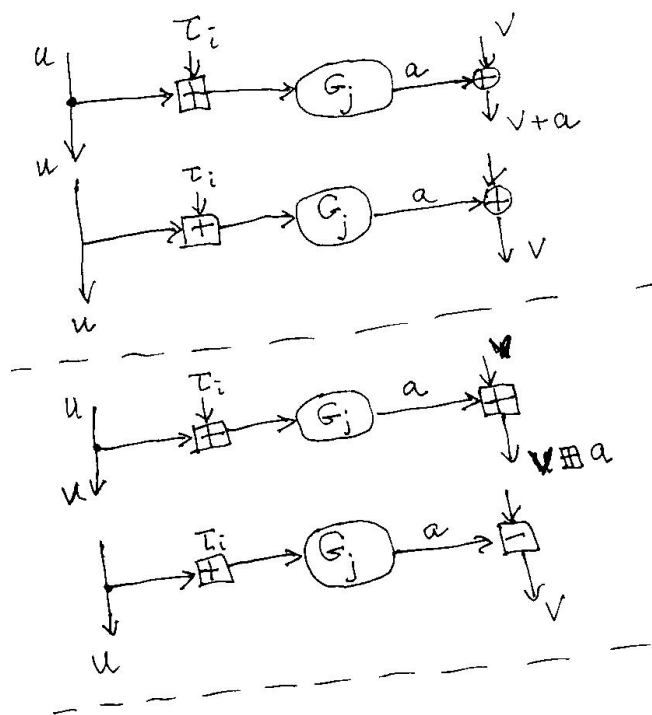
$$\sigma: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}, \quad (1, 3, 4, 2)$$

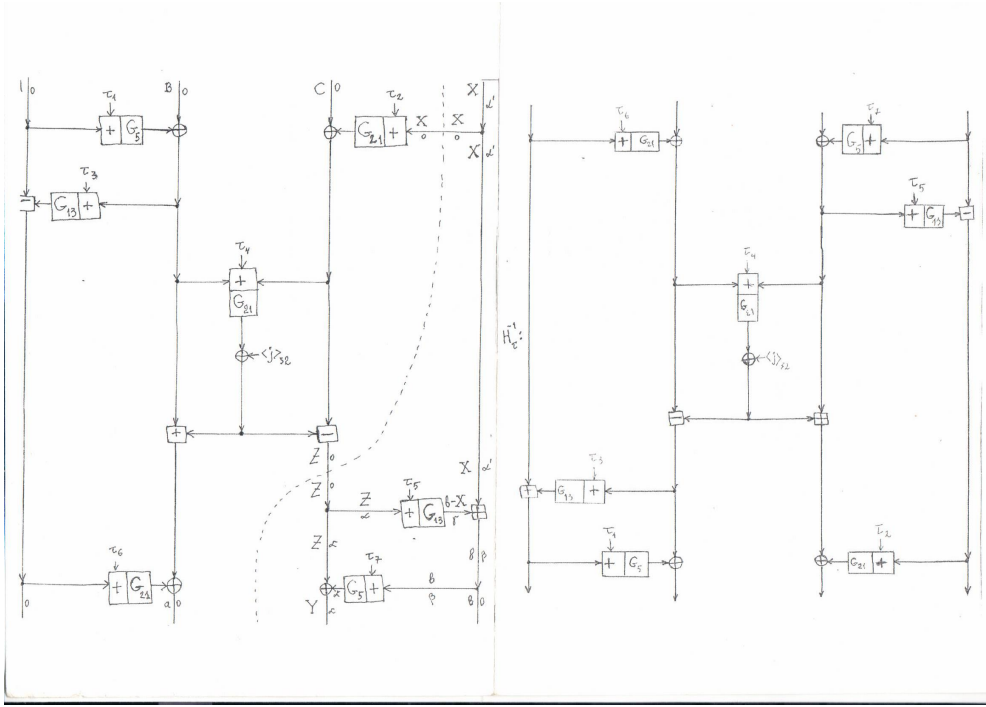
$$H_\tau: V_{32}^4 \rightarrow V_{32}^4 = V_{128}$$

$$G_k: V_{32} \rightarrow V_{32}, \quad k \in \{5, 13, 21\}$$

$$F_\theta = H_{\tau(1)}\sigma H_{\tau(2)}\sigma...\sigma H_{\tau(7)}\sigma H_{\tau(8)}\hat{\mathcal{S}}, \quad \mathcal{S} = \sigma^2 = (1, 4)(2, 3).$$

$$H_{\tau(i)}^{-1}$$





$$H_{\tau}^{-1} = \mathcal{S} H_{\bar{\tau}} \mathcal{S}, \quad \mathcal{S} H_{\bar{\tau}}^{-1} \mathcal{S} = H_{\tau}, \quad \mathcal{S} = \sigma^2$$

$$\bar{\tau} = (\tau_7, \tau_6, \dots, \tau_2, \tau_1), \quad \tau = (\tau_1, \tau_2, \dots, \tau_6, \tau_7)$$

$$F_{\theta,\chi} = H_{\tau(1)}\chi H_{\tau(2)}\chi\cdots\chi H_{\tau(7)}\chi H_{\tau(8)}\mathcal{S}, \quad \chi \in S_4$$

$$F_{\theta,\sigma} = F_{\theta}, \quad F_{\theta}^{-1} = F_{\bar{\theta},\sigma^{-1}}$$

$$F_{\theta,\chi}^{-1} = F_{\bar{\theta},\mathcal{S}\chi^{-1}\mathcal{S}}.$$

$$F_{\theta,\chi}^{-1} = \mathcal{S}H_{\tau(8)}^{-1}\chi^{-1}H_{\tau(7)}^{-1}\chi^{-1}\cdots\chi^{-1}H_{\tau(2)}^{-1}\chi^{-1}H_{\tau(1)}^{-1}.$$

$$H_{\tau}^{-1} = \mathcal{S}H_{\bar{\tau}}\mathcal{S}, \quad \mathcal{S}H_{\bar{\tau}}^{-1}\mathcal{S} = H_{\tau}$$

$$F_{\theta,\chi}^{-1} = H_{\tau(8)}\chi'H_{\tau(7)}\chi'\cdots\chi'H_{\tau(2)}\chi'H_{\tau(1)}\mathcal{S}, \quad \chi' = \mathcal{S}\chi^{-1}\mathcal{S}$$

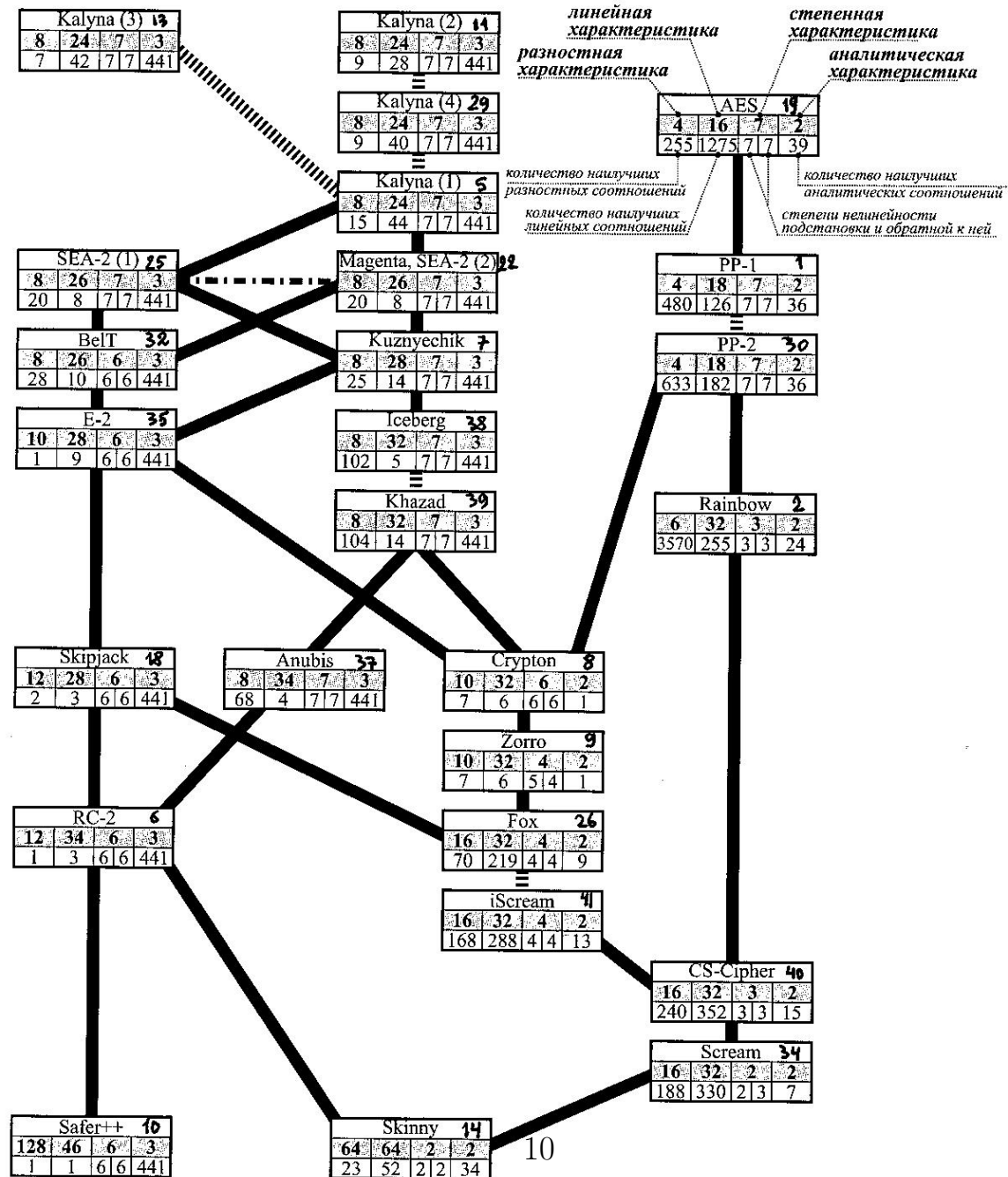
$$\chi' = \chi, \quad \mathcal{S}\chi^{-1}\mathcal{S} = \chi, \quad (\chi\mathcal{S})^2 = \text{id}_{\overline{1,4}}$$

$$\chi_1 = (1, 3)(2, 4); \quad \chi_2 = (1, 2)(3, 4); \quad \chi_3 = (1, 3, 2, 4);$$

$$\chi_4 = (1, 4, 2, 3); \quad \chi_5 = (1, 2, 3, 4); \quad \chi_6 = (1, 4, 3, 2);$$

$$\chi_7 = (2, 3); \quad \chi_8 = (1, 4); \quad \chi_9 = \sigma^2;$$

$$\chi_{10} = \text{id}_{\overline{1,4}}$$



References

- [1] Государственный стандарт республики Беларусь. Криптографические алгоритмы шифрования и контроля целостности. СТБ 34.101.31 – 2011 г. Дата введения 2011–07–01.
- [2] Шнайер Б. Прикладная криптография. М., "ТРИУМФ" , 2003.
- [3] Воробьёв Н.Н. Числа Фибоначчи. М.: Наука, 1978. 144 с.
- [4] Matsui M. Linear Cryptanalysis Method for DES Cipher // Proc. Eurocrypt – 1993. Lect. Notes Comput. Sci. 1994. *N* 765. P. 386–397.
- [5] Daemen J., Rijmen V. The Design of Rijndael: AES - The Advanced Encryption Standard. Springer Verlag. 2002.
- [6] Malyshev F.M., Trishin A.E. Linear and Differential Cryptanalysis: Another Viewpoint. Mathematical Aspects of Cryptography, **11**:2 (2020), 83–98.
- [7] Малышев Ф.М. Методы линейных и разностных соотношений в криптографии. Дискрет. матем. 34: 1 (2022), 36–63.