BETA-Klasse, BOA-Algorithmus

Grundlage für die Untersuchung und Entwicklung der BETA-Klasse ist der Zufallszahlengenerator von Hull und Dobell(1962).
Die Entwicklung der BETA-Klasse begann 1974 und endete nach umfassender Analyse 1979.
Im Jahr 1988 wurde die Geheimhaltung des Verfahrens aufgehoben.
Der Algorithmus wurde 1974 bis 1975 spezifiziert und bis 1979 wurden statistische Untersuchungen unternommen in denen die Kryptologische Sicherheit der Klasse nachgewiesen wird.
Ziel war es, wie es in der ALPHA-Klasse realisiert wurde, einen sicheren Algorithmus zu erstellen mit dem man Zufallsfolgen, Wurmgruppen, für den Chiffrieralgorithmus bereitstellt.
Geplant war bis zur Schließung der Akte, den BOA Algorithmus ür weitere Chiffriersysteme zu nutzen.

Die Folge a = (a_n) n € η_0 ist die Additionsreihe.

$$a^{3i} = {}^{*i}t_6\,{}^{*i}t_5 \ \ldots\ {}^{*i}t_0$$

$$a^{3i+1} = {}^{*i}t_{14}\,{}^{*i}t_{14} \ \ldots\ {}^{*i}t_8$$

$$a^{3i+2} = {}^{*i}t_{21}\,{}^{*i}t_{22} \ \ldots\ {}^{*i}t_{15}$$

$$T^{*i} = {}^{*i}t_{21}\ {}^{*i}t_{20} \ \ldots\ {}^{*i}t_0$$

$$T_i = {}^{i}s_p{}^{i} \otimes {}^{i}s_q{}^{i}$$

$$S^{\circ} = ({}^{\circ}s_0, {}^{\circ}s_1, \ldots, {}^{\circ}s_{31}) \in \eta$$ **ist der Schlüssel**

p = $(p^i)_i$, q = $q^i)_i$, r = $(r^i)_i$ heißen Steuerfolgen.

$$p_i = {}^{i}v_{21}\,{}^{i}v_{20}\,{}^{i}v_{19}\,{}^{i}v_{18}\,{}^{i}v_{17};$$

$$q_i = {}^{i}v_9\,{}^{i}v_8\,{}^{i}v_7\,{}^{i}v_6\,{}^{i}v_5;$$

$$r_i = {}^{i}v_4\,{}^{i}v_3\,{}^{i}v_2\,{}^{i}v_1\,{}^{i}v_0;$$

$$c_i = {}^{i}v_{14}\,{}^{i}v_{13};$$

$$V^i = E^i \otimes {}^{i}s_k \text{ mit } k \equiv i \pmod{32}$$

$$E^{i+1} = 33\ E^i \otimes Y$$

$$F^{i+1} = 9\ F^i \otimes Z$$

Das Schlüsselsystem umfaßt:

$$({}^{\circ}s_0, {}^{\circ}s_1, \ldots, {}^{\circ}s_{31}, {}^{E}, {}^{Y}, {}^{F}, {}^{Z}) \in [N(2^{22})]^{32}$$

$\otimes$ **entspricht mod(2^{22})**

Die Additionsreihen werden wie bei der T-310 nicht direkt mit dem Klartext, bzw. Chiffrat XOR-Verknüpft.

Bei entsprechender Wahl des Schlüssels, große Primzahlen, können bis zu 600 Millionen Zufallszahlen erzeugt werden, dann beginnt der Zyklus. (Periodizität)

In der Häufigkeitsverteilung konnte nachgewiesen werden das diese paarweise verschieden sind.