# 2. РЕАЛИЗАЦИЯ И ИЗСЛЕДВАНЕ НА ГРУПА ГЕНЕРАТОРИ НА СЛУЧАЙНИ ПОСЛЕДОВАТЕЛНОСТИ В ПАРАЛЕЛНА ИЗПЪЛНИТЕЛНА СРЕДА

В първата точка на раздела се разглеждат няколко предложения на реализации на алгоритмически генератори, използващи *LFSR*, както и вариант на реализация на *Алгоритъм-М* на Кнут.

Във втора точка е представен ефективен генератор на псевдослучайна последователност чрез примитивната функция *crc32* на паралелната среда.

Архитектурата *XS1* съдържа физически ентропиен източник. Това дава възможност да се реализира генератор на действително-случайна последователност (*RRNG*), което е направено в следващата точка.

Операторът *select* от езика *XC* е аналог на алтернативната команда на *CSP*. В четвърта точка от раздела е изследвана възможността за генериране на случайна последователност чрез вградения в командата за алтернативен избор недетерминизъм. Изходното предположение е, че реализацията на алтернативната команда също трябва да притежава недетерминизъм. Противно на очакванията обаче, операторът *select* не проявява подобно свойство. Затова в следващата точка се прилага техника за вграждане на недетерминизъм, с оглед адекватността на оператора *select* на алтернативната команда.

Контролиращият блок на физическия генератор от фиг. 1.4 за следене на статистическите качества на изработената случайна последователност трябва да присъства при всяко критично приложение. Съответно, шеста точка от раздела се спира на една възможна реализация на монобитния тест, като характерен представител на методите за оценка на случайната последователност. Оценката се прави в реално време и е основана на критерия $\chi^2$. Приведени са получените в хода на работата експериментални статистически данни.