

Реферат

Изобретение реализует способ генерации динамических ID для блокчейн-систем по формуле:

$$ID = (T_{[2N]} \oplus \Delta k) \bmod (P + H).$$

где:

$P = 0xFFFFFFFF$ (32-битная константа);

$H = 0x5A827999$ (константа SHA-1).

Технический результат

Генерация ID со сложностью $O(1)$ через:

Параллельный расчёт Δk на GPU (`atomicAdd()`);

Кэширование T_k в shared memory;

Аппаратно-оптимизированные операции (AVX512, `umulhi`).

Показатели безопасности. $P_{атаки} = 10^{-9}$ при $N \geq 40$ узлов.