Politechnika Wrocławska

Opracowanie publikacji Danila Gorodocky'ego i Tiziano Villa'y - sumatory modularne

Łukasz Wdowiak 264026
Damian Jabłoński 264025

Prowadzący: dr inż. Piotr Patronik
Grupa: K03-47a, Pon 15:15-16:55 TN

Wydział Informatyki i Telekomunikacji
Informatyka Techniczna
IV semestr

Spis treści

1 Cele projektu

2 Przebieg projektu

3 Algorytmy

3.1 Modulo dla dowolnych X i P - bit po bicie

3.1.1 Opis algorytmu

W artykule autorzy zaproponowali sposób obliczania oparty na następującej reprezentacji:

$$X = P \cdot Q + R = \tag{1}$$
$$= P \cdot 2^{\delta} \cdot q_{\delta} + P \cdot 2^{\delta-1} \cdot q_{\delta-1} + \ldots + P \cdot 2^{0} \cdot q_0 + R \tag{2}$$

$X(\mathrm{mod}P) = R$, gdzie $X = (x_{\psi}, x_{\psi-1}, \ldots, x_1)$ i δ jest określona nierównością $P \cdot 2^{\delta} < 2^{\psi} - 1 \leq P \cdot 2^{\delta+1}$.

Na przykład, $X = (x_{10}, x_9, \ldots, x_1)$ i $P = 21$, przy $\delta = 5$. Wynosi:

$$X = 21 \cdot Q + R =$$
$$= 21 \cdot 2^5 \cdot q_5 + 21 \cdot 2^4 \cdot q_4 + 21 \cdot 2^3 \cdot q_3 +$$
$$+ 21 \cdot 2^2 \cdot q_2 + 21 \cdot 2^1 \cdot q_1 + 21 \cdot 2^0 \cdot q_0 + R.$$

Każdy kolejny iloczyn częściowy jest wejściem kolejnego bloku obliczeniowego. R jest wynikiem szóstego bloku oraz resztą z dzielenia przez 21. Jeśli chcemy policzyć $X(\mathrm{mod}P) = R$, gdzie $X = 888$, a $P = 21$, to:

$X_5 \geq 21 \cdot 2^5$, $888 \geq 672$, $X_4 = 888 - 21 \cdot 2^5 = 216$;
$X_4 < 21 \cdot 2^4$, $216 < 336$, $X_3 = 216$;
$X_3 \geq 21 \cdot 2^3$, $216 \geq 168$, $X_2 = 216 - 21 \cdot 2^3 = 48$;
$X_2 < 21 \cdot 2^2$, $48 < 84$, $X_1 = 48$;
$X_1 \geq 21 \cdot 2^1$, $48 \geq 42$, $X_0 = 48 - 21 \cdot 2^1 = 6$;
$X_0 < 21 \cdot 2^0$, $6 < 21$, $R = 6$.

W pierwszym kroku porównujemy X z $21 \cdot 2^5$. Następnie odejmujemy $21 \cdot 2^5$ od X i otrzymujemy $X_4 = 216$. W kolejnym kroku porównujemy X_4 z $21 \cdot 2^4$ i otrzymujemy $X_3 = 216$. Następnie odejmujemy $21 \cdot 2^3$ od X_3 i otrzymujemy $X_3 = 48$. W kolejnym kroku porównujemy X_2 z $21 \cdot 2^2$ i

otrzymujemy $X_1 = 48$. Następnie odejmujemy $21 \cdot 2^1$ od X_1 i otrzymujemy $X_0 = 6$. W kolejnym kroku porównujemy X_0 z $21 \cdot 2^0$ i otrzymujemy $R = 6$.

Jak widać powyżej jest to prosta operacja odejmowania i porównywania, która jest wykonywana w pętli.

3.1.2 Implementacja algorytmu

Algorytm został zaimplementowany za pomocą trzech funkcji.

- **calc_length** - oblicza długość binarną liczby 'number' poprzez przesuwanie jej bitów w prawo i zliczanie ilości przejść, zwracając ostateczną długość.
- **get_delta** - funkcja obliczająca δ na podstawie parametrów l i P, sprawdzając warunek związanym z potęgami dwójki.
- **mod_bit_by_bit** - funkcja obliczająca resztę z dzielenia - w pętli obliczane są kolejne wartości X. Jeżeli $X_i \geq P \cdot 2^i$, to $X_{i-1} = X_i - P \cdot 2^i$, w przeciwnym wypadku $X_{i-1} = X_i$. Pętla kończy się, gdy wartość δ wynosi 0 ,a funkcja zwraca R jako reszte z dzielenia.

Literatura

[1]