

INTISARI

PENENTUAN EKSPLISIT POLINOMIAL MINIMAL DARI BARISAN DE BRUIJN BINER TERMODIFIKASI

Oleh

MUSTHOFA

19/450317/SPA/00699

Barisan de Bruijn biner order n merupakan suatu barisan siklik dengan panjang 2^n atas $\mathbb{F}_2$ dan setiap n -tuple sebagai suatu sub barisan muncul tepat satu kali dalam satu periode barisan tersebut. Barisan ini memiliki sifat acak yang sesuai untuk diimplementasi pada kriptografi stream cipher. Kompleksitas linear barisan de Bruijn adalah derajat polinomial minimal yang membangun barisan tersebut. Jika pada deretan nol terpanjang dari barisan de Bruijn dihapus satu nol-nya, maka dihasilkan barisan de Bruijn termodifikasi. Para peneliti telah menunjukkan bahwa untuk mengukur kompleksitas barisan de Bruijn akan lebih tepat melalui barisan de Bruijn termodifikasi. Pada penelitian ini dihasilkan suatu metode untuk menentukan polinomial minimal dari barisan de Bruijn biner termodifikasi. Langkah pertama yang dilakukan dalam penelitian ini adalah membentuk suatu graf Γ_n yang isomorfis dengan graf D_n , yaitu graf yang diperoleh dengan menghilangkan titik nol pada graf de Bruijn. Setiap siklus Hamiltonian $\mathcal{H}$ pada graf Γ_n akan berkorespondensi dengan suatu barisan de Bruijn biner termodifikasi order n . Selanjutnya ditentukan polinomial kanonik pembangun siklus Hamiltonian $\mathcal{H}$. Polinomial minimal barisan de Bruijn biner termodifikasi yang berkorespondensi dengan $\mathcal{H}$ dapat ditentukan dengan menghitung $\frac{F(x)}{d(x)}$ dengan $F(x)$ merupakan hasil kali semua polinomial irreduksibel dengan derajat $d \mid n$, $d \neq 1$ dan $d(x)$ adalah faktor persekutuan terbesar dari $g(x)$ dan $F(x)$ dengan $g(x)$ adalah polinomial generator dari $\mathcal{H}$. Pada penelitian ini juga dihasilkan algoritma yang dinamakan dengan algoritma *Prefer Complement* untuk menentukan $\mathcal{H}$ yang secara *heuristik* berhasil memilih barisan de Bruijn termodifikasi dengan kompleksitas yang besar ataupun mencapai nilai maksimalnya yaitu $2^n - 2$.

Kata-kata kunci: barisan de Bruijn biner termodifikasi, polinomial minimal, kompleksitas linear, graf de Bruijn, siklus Hamiltonian, algoritma *prefer complement*.

ABSTRACT

EXPLICIT DETERMINATION OF THE MINIMAL POLYNOMIALS OF MODIFIED BINARY DE BRUIJN SEQUENCES

By

MUSTHOFA

19/450317/SPA/00699

A binary de Bruijn sequence is a periodic sequence over $\mathbb{F}_2$ with a period of 2^n , where each n -tuple appears exactly once within a period of the sequence. This sequence possesses a random-like property suitable for implementation in stream cipher cryptography. The linear complexity of the de Bruijn sequence is the degree of the minimal polynomial that generates the sequence. If the longest run of zeros in the de Bruijn sequence has one of its zeros removed, the modified binary de Bruijn sequence is obtained. Researchers have demonstrated that measuring the complexity of the de Bruijn sequence is more accurate through the modified version. In this work, we develop a method to determine the minimal polynomials of the modified binary de Bruijn sequences. The first step is constructing a graph Γ_n that is isomorphic to the graph D_n , obtained by removing the zero node from the de Bruijn graph. Each Hamiltonian cycle $\mathcal{H}$ in the graph Γ_n corresponds to a modified binary de Bruijn sequence of order n . The next step is to determine the canonical polynomial that generates the Hamiltonian cycle $\mathcal{H}$. The minimal polynomial of the modified binary de Bruijn sequence corresponding to $\mathcal{H}$ can be determined by calculating $\frac{F(x)}{d(x)}$, where $F(x)$ is the product of all irreducible polynomials of degree $d|n, d \neq 1$, and $d(x)$ is the greatest common divisor of $g(x)$ and $F(x)$, where $g(x)$ is the generator polynomial of $\mathcal{H}$. This research also introduces an algorithm called the *Prefer Complement* algorithm to determine $\mathcal{H}$, which heuristically produces modified de Bruijn sequences with high complexities or reaches its maximum value of $2^n - 2$.

Keywords: binary modified de Bruijn sequence, minimal polynomial, linear complexity, de Bruijn graph, Hamiltonian cycle, *prefer complement* algorithm.