Review Paper

Judul	Heterogeneous Rainbow Table Widths Provide Faster Cryptanalyses
Jurnal/Prosiding	In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security
Halaman	815 - 822
Tahun	2017
Tempat	Abu Dhabi, United Arab Emirates
Penulis	Gildas Avoine dan Xavier Carpent
Reviewer	1. Sang Putu Febri Wira Pratama (1808561012) 2. Muhammad Akbar Hamid (1808561064)
Tanggal	10 Mei 2021

Tujuan Penelitian	Tujuan yang ingin dicapai pada panelitian adalah untuk menunjukkan bahwa ranbow table tidak harus dieksploitasi karena didasarkan pada pertimbangan tabel dengan lebar yang sama masih jauh dari konfirgurasi optimal. Penelitian yang ingin ditunjukkan bahwa lebar setiap tabel dan memori yang dialokasikan untuk masing-masing tabel harus dihitung secara individual (tetapi tidak secara independen) untuk setiap tabel. Pendekatan yang dilakukan mengarah pada pembuatan apa yang disebut "tabel heterogen" yang bertentangan dengan "tabel homogen". Penulis juga ingin menunjukkan bahwa aturan yang banyak digunakan terdiri dari mengunjungi tabel secara berurutan bukanlah hal yang optimal saat mempertimbangkan pada tabel heterogen.
Metode Penelitian	Pendekatan yang digunakan pada penelitian ini adalah menggunakan algoritma optimasi untuk mencari konfigurasi dari ukuran tabel yang meminimalkan waktu pencarian rata-rata. Pada persamaan (1) merupakan ekspresi matematika untuk waktu rata-rata dalam kasus tabel homogen.

	$$T = \sum_{k=1}^{t}\sum_{i=1}^{\ell}\frac{m}{N}\left(1-\frac{m}{N}\right)^{(k-1)\ell+i-1}\left(\ell\sum_{j=1}^{k-1}C_j+iC_k\right) + e^{-2\ell}\ell\sum_{k=1}^{t}C_k. \quad (1)$$ Sedangkan persamaan (2) merupakan ekspresi waktu rata-rata dalam kasus tabel heterogeny. $$T = \sum_{k=1}^{t}\frac{[m]_{V_k}}{N}\prod_{j=1}^{k-1}\left(1-\frac{[m]_{V_j}}{N}\right)\sum_{j=1}^{k}[CS_j]_{V_j} + e^{-2\ell}\sum_{i=1}^{\ell}\sum_{s=1}^{[t]_i}[C_s]_i, \quad (2)$$ Kemudian pada masalah minimisasi dapat menggunakan persamaan berikut. $$\min_{[t]_1,\ldots,[t]_\ell} \quad T([t]_1,\ldots,[t]_\ell) \quad \text{s.t.} \quad \sum_{i=1}^{\ell}M_i \le M, \quad (3)$$
Hasil Penelitian	Hasil penelitian yang diperoleh penulis adalah dengan efek yang dimungkikan dari ukuran heterogen dalam satu set rainbow table, dan memberikan urutan eksplorasi yang optimal. Hal tersebut menghasilkan percepatan waktu rata-rata yang tidak bergantung pada ukuran masalah atau memori, tetapi bergantung pada jumlah tabel (dipengaruhi oleh kemungkinan keberhasilan yang diinginkan). Dalam aplikasi tipikal yang digunakan (misalnya l = 4, yaitu sebesar P^*=99.97%) tabel heterogen sekitar 40% lebih cepat daripada tabel homogennya. Pada kasus terburuk, waktu terkena dampak negatif: ≈ 2.13 perlambatan dengan parameter yang sama, di mana kurang dari 1% kasus adalah tabel heterogen lebih buruk daripada tabel homogen.
Kesimpulan Paper	Kesimpulan pada penelitian ini adalah penulis memilih $N = 2^{40}$ karena ini merupakan ukuran ruang input yang dianggap mengevaluasi TMTOs. Biaya prakomputasi kira-kira setara untuk tabel heterogen dan homogen, alasannya biaya prakomputasi untuk tiap tabel sebanding dengan *mt*. Kelemahan dari tabel heterogen adalah bahwa kasus terburuk lebih buruk dari tabel

	homogen. Kasus terburuk muncul ketika nilai yang dicari tidak tercakup pada salah satu tabel. Ini terjadi dengan probabilitas $1 - e^{-2t}$.