Kamil Kulesza
Instytut Podstawowych Problemów Techniki PAN, Warszawa
Department of Applied Mathematics and Theoretical Physics
University of Cambridge[*]
E-mail: Kamil.Kulesza@damtp.cam.ac.uk

Zastosowania grafów w kryptografii

Grafy znajdują zastosowanie praktycznie w każdej części kryptografii. Wiele z tych zastosowań wywodzi się obszarów, w obrębie których grafy są tradycyjnie stosowane w informatyce. W naszej prezentacji ograniczymy się do przykładów z zakresu kryptografii opartej na problemach trudnych obliczeniowo (*complexity based cryptography*) oraz wybranych zagadnień związanych z protokołami kryptograficznymi. W tym celu na początku przedstawimy podstawowe pojęcia z teorii złożoności obliczeniowej. Następnie omówimy wybrane problemy trudne obliczeniowo związane z grafami ze szczególnym uwzględnieniem zagadnień ich kolorowania. Przyjrzymy się też przykładom zastosowań grafów w określonym powyżej zakresie.

Na koniec zarysujemy możliwości wynikające z nowego, opartego na grafach podejścia do projektowania i analizy systemów kryptograficznych, zwłaszcza protokołów.

[*] Praca nad częścią zagadanień omawianych w tej prezentacji miała miejsce w czasie pobytu autora na stażu naukowym w Cambridge.