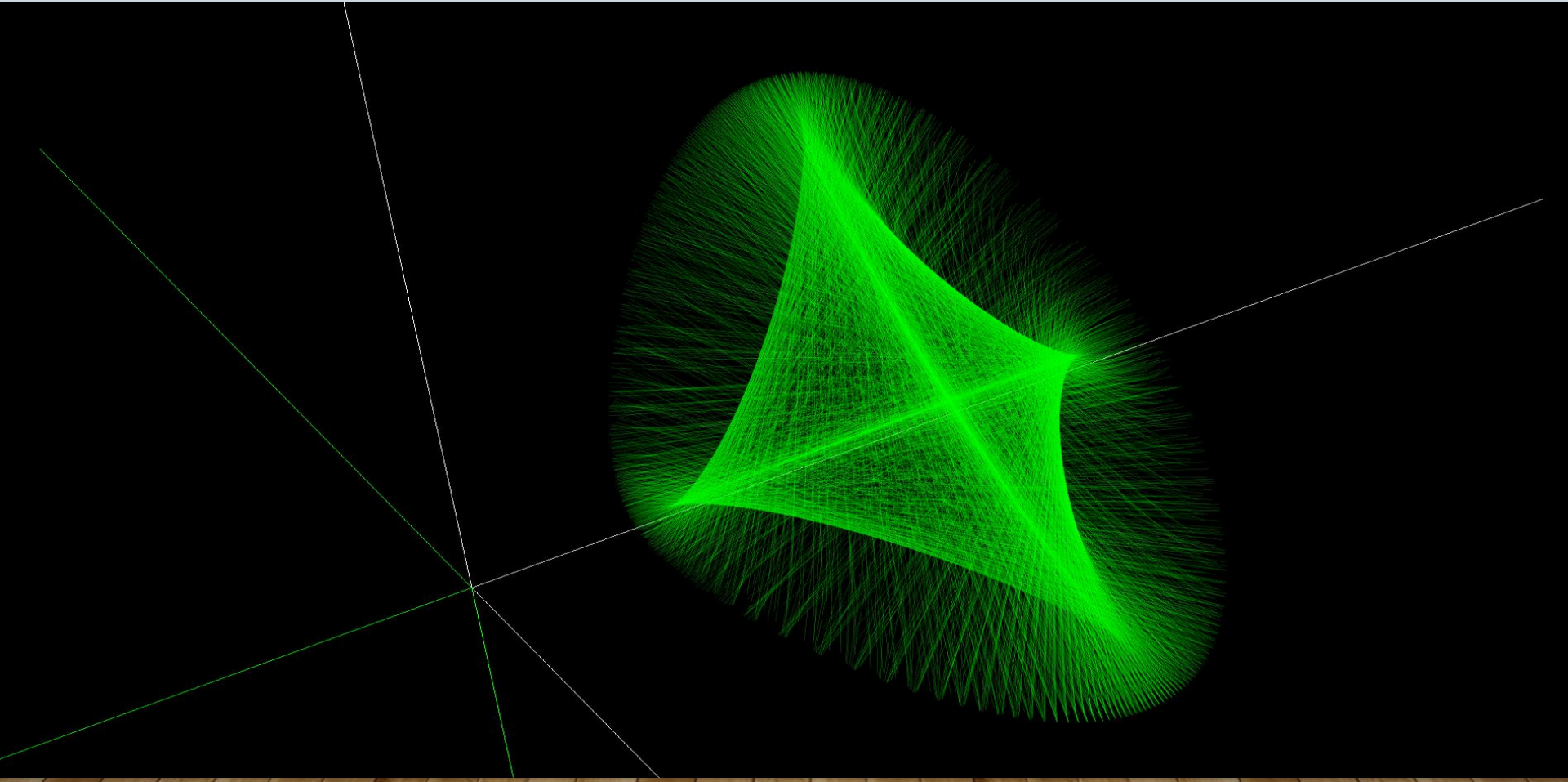
PREZENTACJA SPECJALNOŚCI

MCB

26 MAJA 2022R.

SPECJALNOŚĆ

MATEMATYKA W CYBERBEZPIECZEŃSTWIE



Wydział Matematyki i Nauk Informacyjnych PW

Obraz: M. Zwierzyński


DANGER
DON'T RUN
BEWARE!
DEEP
SHAFTS
DON'T WALK
BACKWARDS
UNMARKED HOLES
DEPARTMENT OF
PRIMARY INDUSTRIES
AND RESOURCES

WSPÓŁCZESNE WYZWANIA

- **Kryptografia postkwantowa**
- **Kryptowaluty**
- **Łączność międzyplanetarna**
- **Oszustwa cyfrowe**
- **Dezinformacja w sieci**

METODY MATEMATYCZNE W BEZPIECZEŃSTWIE TELE - INFORMATYCZNYM

- KRYPTOLOGIA
- BEZPIECZNA TRANSMISJA DANYCH
- POPRAWNOŚĆ I BEZPIECZEŃSTWO OPROGRAMOWANIA

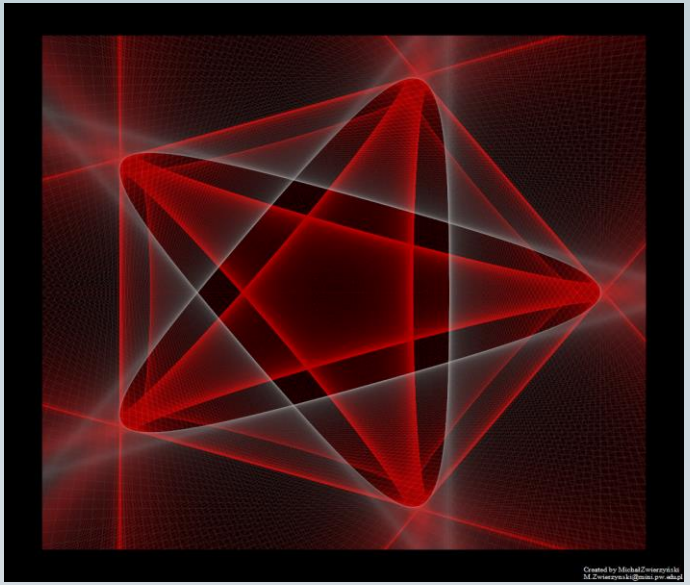
NASZA OFERTA

- Poznanie metod matematycznych stosowanych w weryfikowaniu bezpieczeństwa cyfrowego
- Poznanie głównych idei matematycznych algorytmów stosowanych w cyberbezpieczeństwie
- Zdobycie umiejętności rozwiązywania problemów we współpracy z informatykami i inżynierami zapewniającymi bezpieczeństwo systemów i sieci teleinformatycznych

ZAPRASZAMY OSOBY ZAINTERESOWANE WYKORZYSTANIEM W BEZPIECZEŃSTWIE METOD MATEMATYCZNYCH Z ZAKRESU:

- **Algebry**
- **Logiki**
- **Teorii liczb**
- **Teorii kategorii**
- **Matematyki dyskretnej**
- **Rachunku prawdopodobieństwa**

Algebra



Obraz: M. Zwierzyński

Klasyczne struktury algebraiczne:

- pierścienie
- ciała skończone
- kraty i algebry Boole'a

oraz mniej klasyczne:

- półgrupy i monoidy
- quasigrupy
- quandle
- algebry relacji

- Algebra w kryptografii
- Nieprzemienne struktury algebraiczne i ich zastosowania w kryptografii
- Algebra w naukach informacyjnych

Matematyka jest królową nauk,

a teoria liczb królową matematyki.

Carl Friedrich Gauss

Krypto……

- Algorytmiczna teoria liczba
- Wprowadzenie do współczesnej kryptologii
- Teoria złożoności

- Liczby pierwsze
- Testy pierwszości
- Problemy faktoryzacji
- Logarytm dyskretny

- Szyfrowanie asymetryczne
- Podpis cyfrowy
- Funkcje skrótu
- Krzywe eliptyczne
- Protokoły kryptograficzne
- Kryptografia na kratach

- Klasy problemów P i NP
- NP-zupełność
- Złożoność obliczeniowa w teorii liczb i w kryptografii

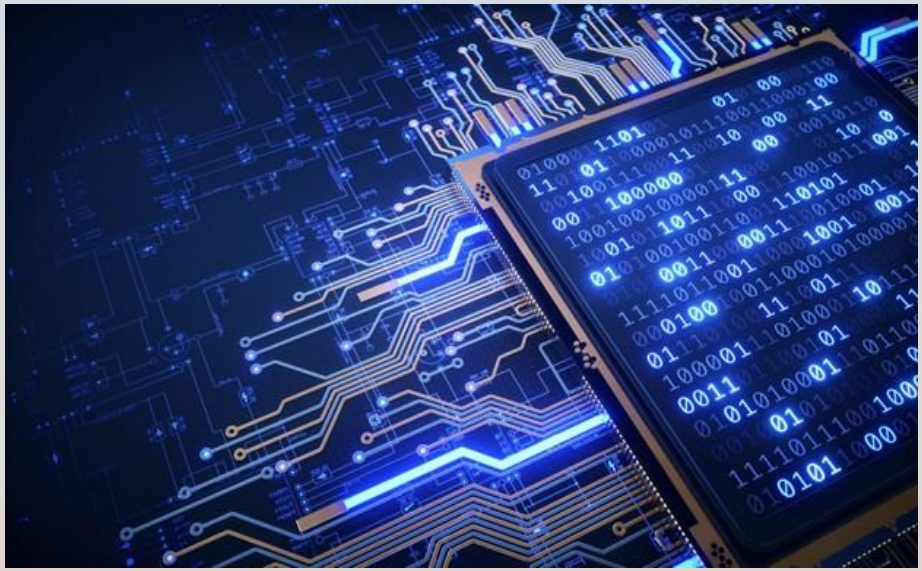
Cyber w praktyce

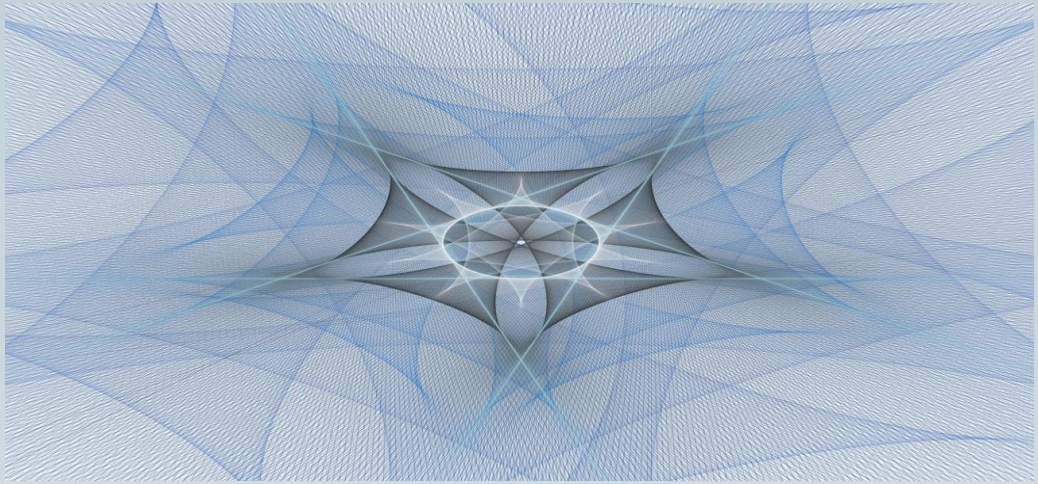
- Cyberprzestrzeń: sieci i systemy
- Zagrożenia w cyberprzestrzeni
- Planowanie i sterowanie atakami
- Przełamywanie zabezpieczeń
- Pozyskiwanie danych
- Zarządzanie ryzykiem

- Entropia
- Bezstratna kompresja danych
- Źródła informacji
- Kanały komunikacyjne
- Tajność doskonała systemu kryptograficznego

- Kody liniowe nad ciałami
- Kody BCH
- System McEliece

- Wprowadzenie do cyberbezpieczeństwa
- Teoria informacji i podstawy bezpieczeństwa cyfrowego
- Kody korekcyjne i transmisja danych





Obraz: M. Zwierzyński + D. Kaczmarska

Logika i nie tylko

- Teoria kategorii
- Metody formalne i weryfikacja protokołów kryptograficznych

Mathematics	*Programming*
theorem	type
proof	program
correctness verification	type checking
cut elimination	computation

- Teoria automatów i języków formalnych

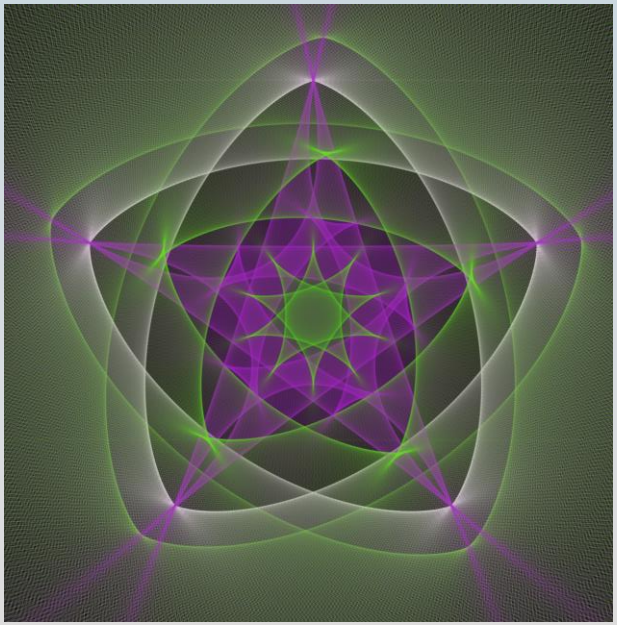
- Funktory
- Diagramy
- Monady
- Algebry Eilenberga-Moore'a

- Logika intuicjonistyczna
- Rachunek lambda
- Teoria typów
- Dowodzenie programów (Agda)
- ProVerif

- Gramatyki i języki
- Automaty
- Maszyny Turinga

Programowanie i warsztaty

- Programowanie funkcyjne (Haskell)
- Programowanie dyskretne
- Programowanie dyskretne projekt
- Warsztaty matematycznych metod cyberbezpieczeństwa
- Algorytmy zaawansowane
- Projekt zespołowy



Obraz: M. Zwierzyński + D. Kaczmarska

PERSPEKTYWY ZAWODOWE

Firmy telekomunikacyjne i energetyczne	**Banki, Firmy ubezpieczeniowe**	**Firmy projektujące sprzęt elektroniczny oraz oprogramowanie**
Agencje do spraw bezpieczeństw	**Branża E-Commerce – handel elektroniczny**	**Branża Adtech – rynek reklam internetowych**

DIAMOND SPONSORS

aws

Meta

intel.

GOLD SPONSORS

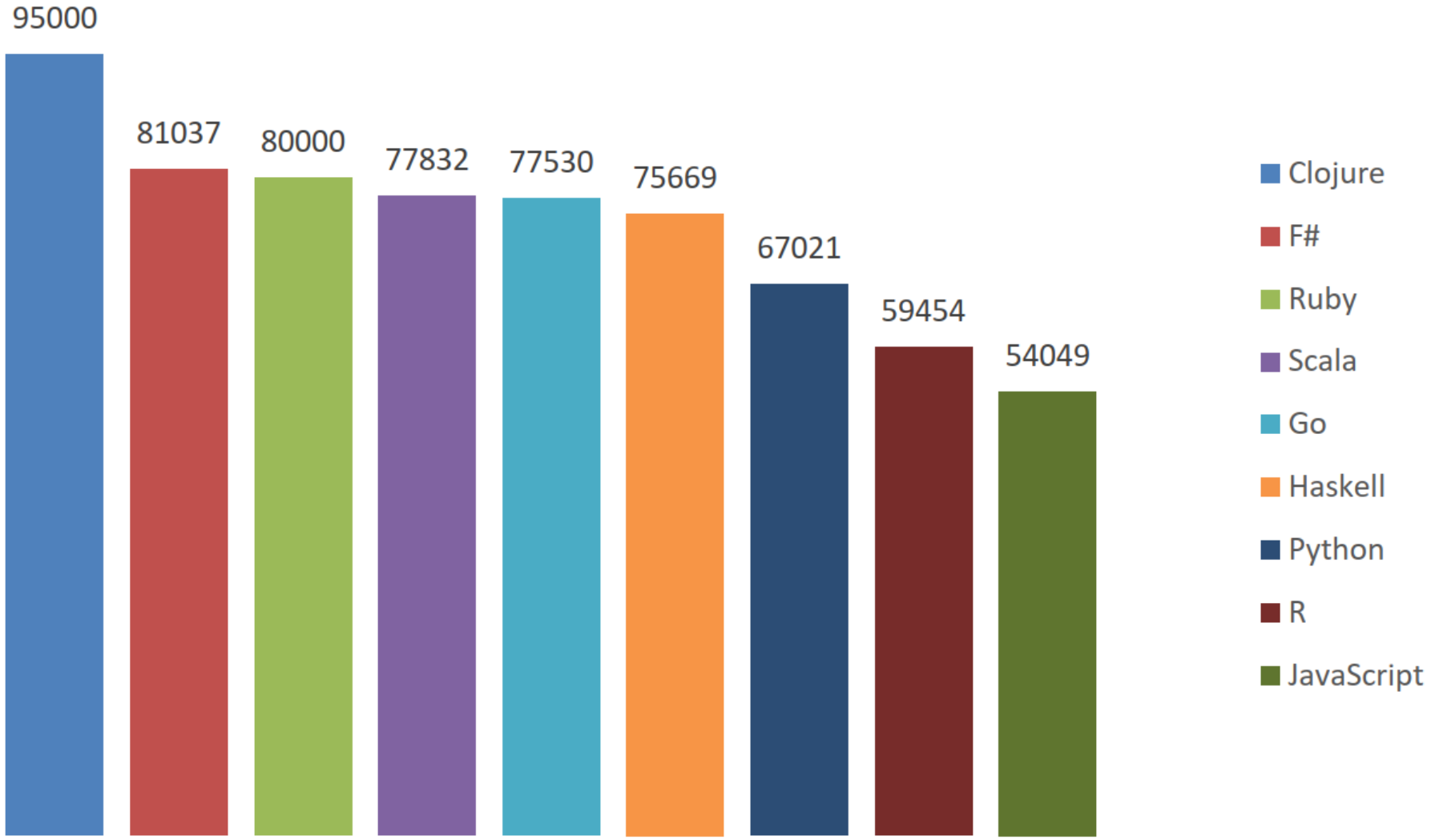
Google

NVIDIA.

SYNOPSYS®

Top Highly Paid Programming Languages to Learn in 2022

https://lvivity.com/top-highly-paid-programming-languages



KARIERA NAUKOWO-BADAWCZA

- Projekty
- Szkoły doktorskie
- Doktoraty wdrożeniowe
- Uczelnie, instytucje badawcze

KONTAKT

Zakład Algebry i Kombinatoryki

dr hab. inż. Agata Pilitowska

agata.pilitowska@pw.edu.pl

dr Tomasz Brengos

tomasz.brengos@pw.edu.pl

dr hab. inż. Konstanty Junosza-Szaniawski

konstanty.szaniawski@pw.edu.pl

ZAPRASZAMY

NA

MCB