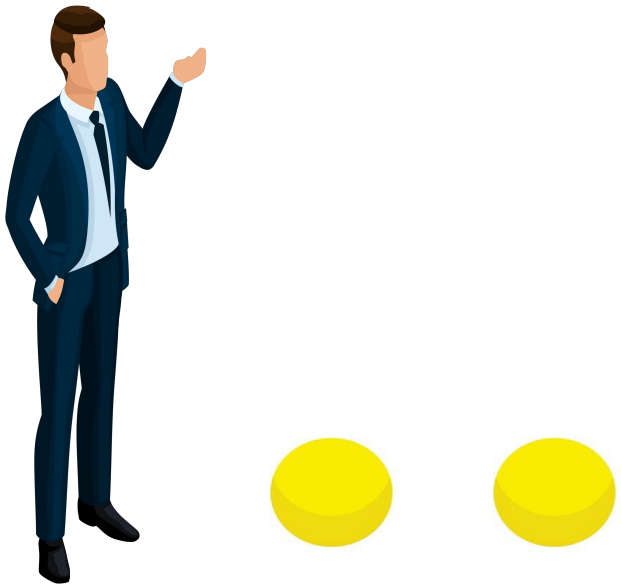
Zero Knowledge Proofs

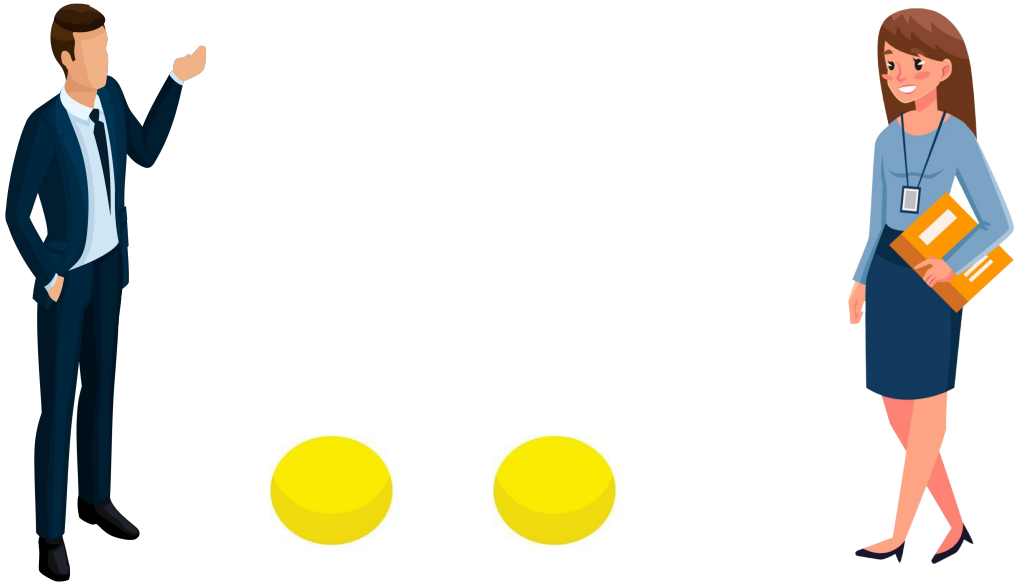
„Wiem, ale nie powiem”

Tomasz Gogacz

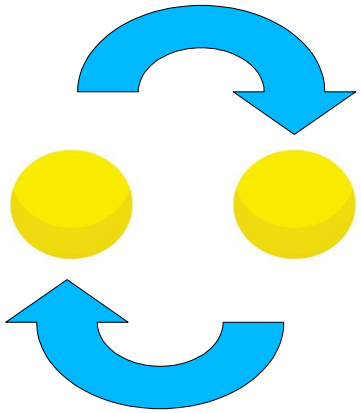
Kolor Kulek



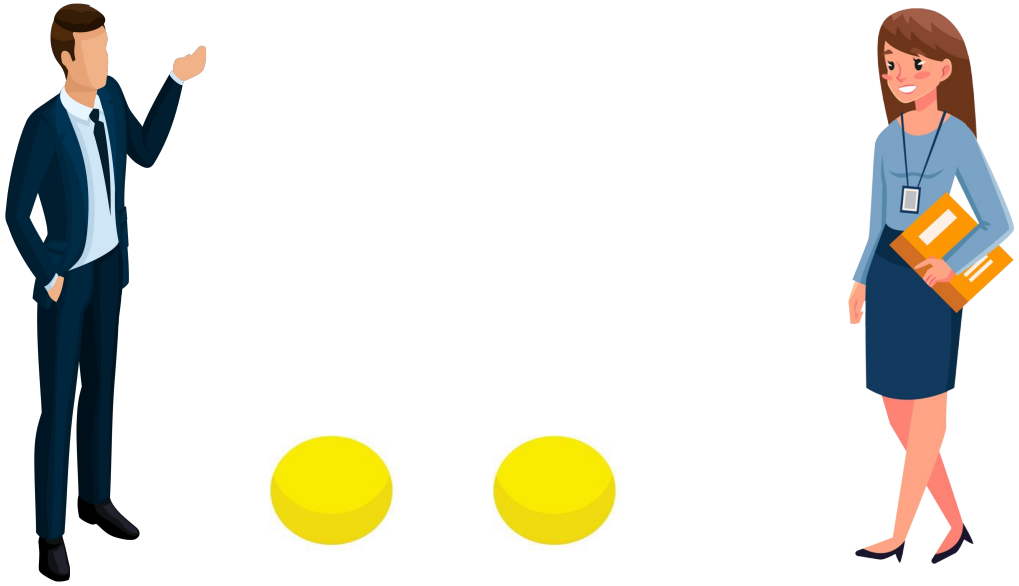
Kolor Kulek



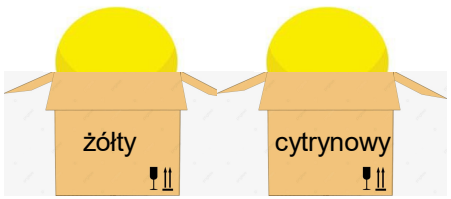
Kolor Kulek



Kolor Kulek



Kolor Kulek



Protokół

- Interaktywny: Adam (verifier), Ewa (prover)
- Adam może używać losowości

Protokół

- Interaktywny: Adam (verifier), Ewa (prover)
- Adam może używać losowości

- Jeśli stwierdzenie jest prawdziwe,

  to Ewa zawsze odpowie poprawnie
- Jeśli stwierdzenie jest fałszywe,

  to Ewa odpowie źle z nietrywialnym prawdopodobieństwem
- Adam jest ograniczony umysłowo
- Adam nie dowie się nic poza statusem stwierdzenia

Pierwiastek Dyskretny

$$Z_p = \langle \{0,1,2,3,\ldots p-1\}, 0,1,+,* \rangle$$

Pierwiastek Dyskretny

$$Z_p = \langle \{0,1,2,3,\ldots p-1\}, 0,1,+,* \rangle$$

$$3^2 = 4 \pmod 5$$

Pierwiastek Dyskretny

$$Z_p = \langle \{0,1,2,3,\ldots p-1\}, 0, 1, +, * \rangle$$

$$3^2 = 4 \pmod 5$$

$$x^2 = 57 \pmod{59} \; ?$$

Pierwiastek Dyskretny

$$x^2 = 57 \pmod{59}$$

- Wylosuj liczbę a ze zbioru {1,2,...,58}
- Ustal b = x / a
- Podaj wartość c = a^2
- Chcesz znać a czy b?

c*b^2=57

a^2=c

Logarytm Dyskretny

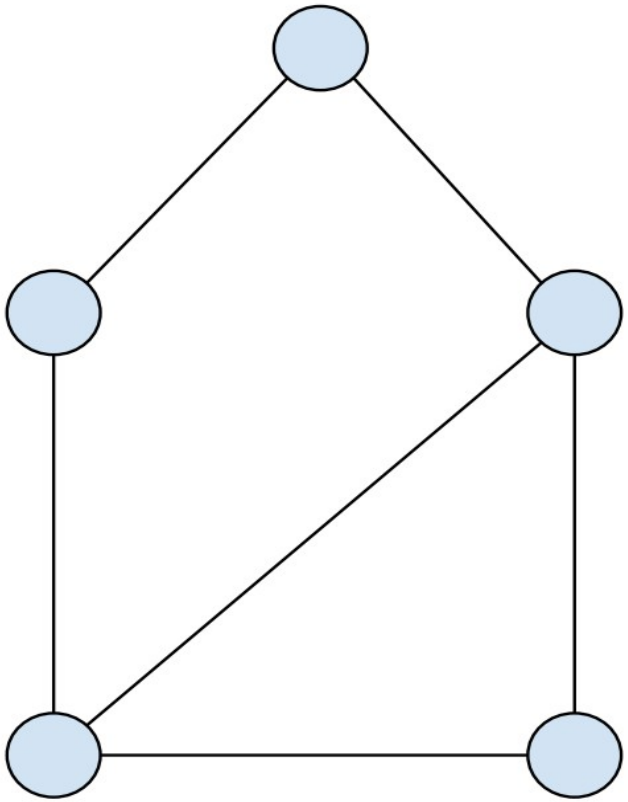
$$2^{y} = 11 \left(mod\ 59 \right)$$

- Wylosuj liczbę a ze zbioru {1,2,...,58}
- Ustal b = y - a
- Podaj wartość c = 2^a
- Chcesz znać a czy b?

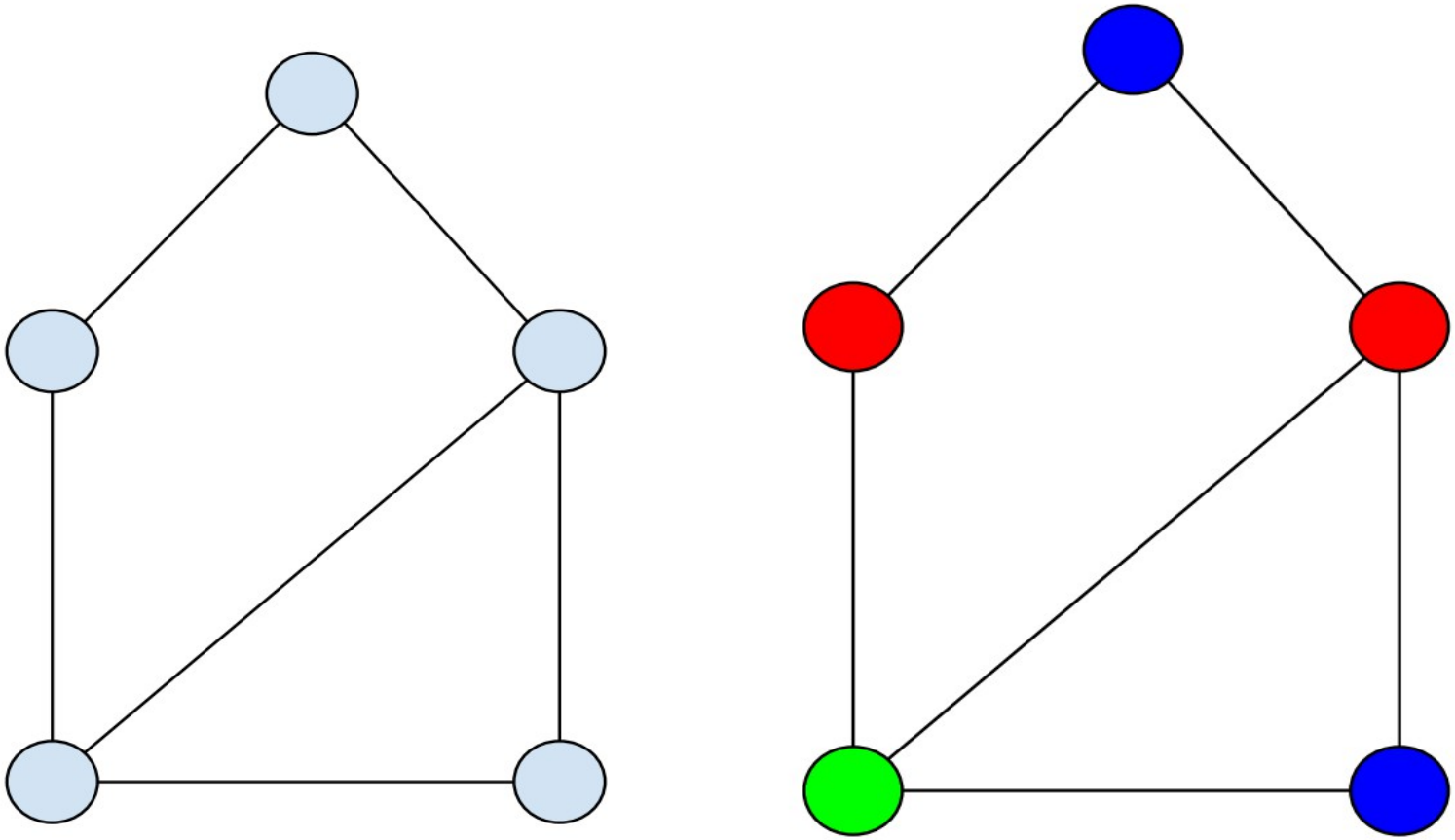
c*2^b=11

2^a=c

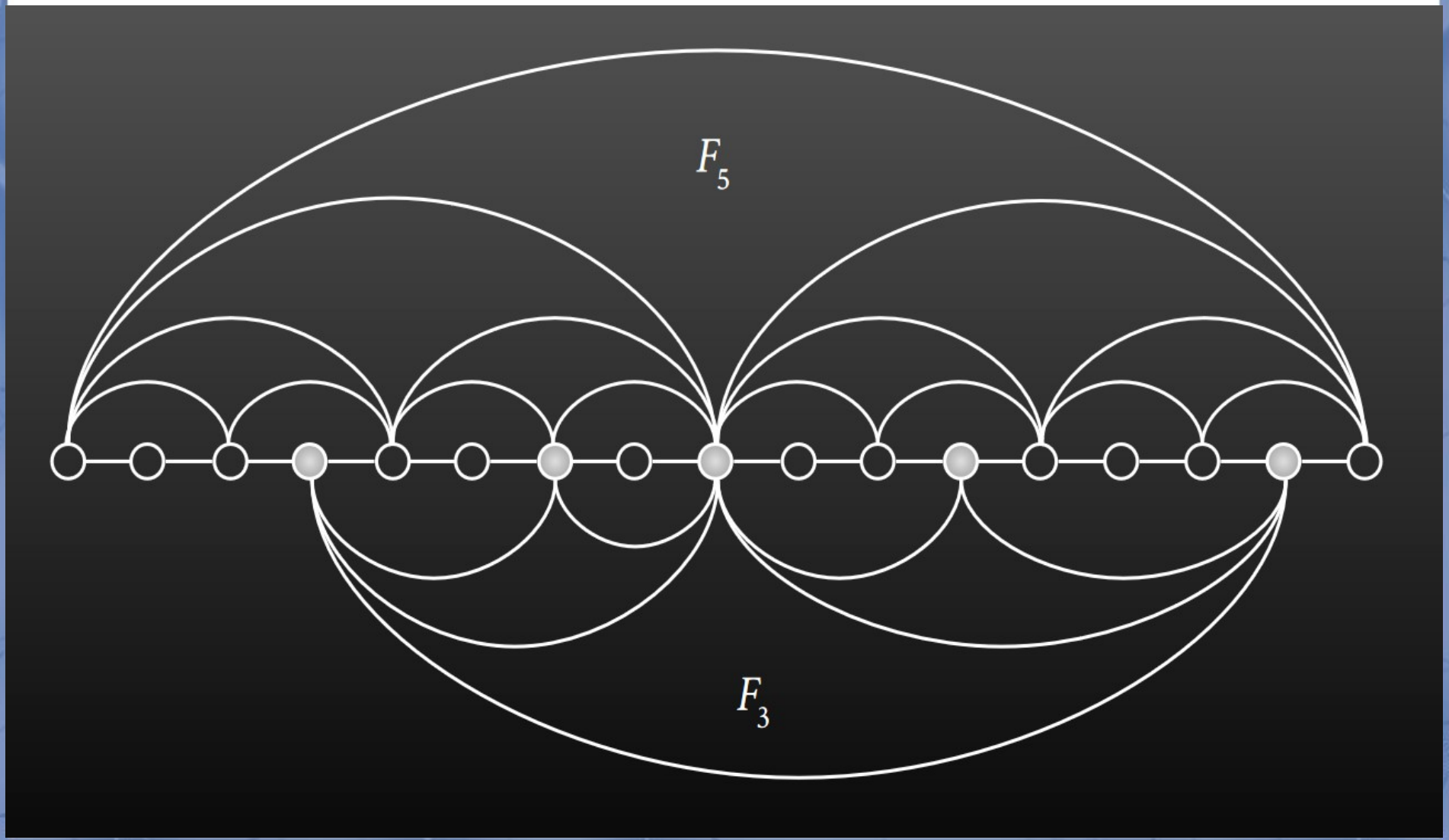
4-kolorowanie Grafu



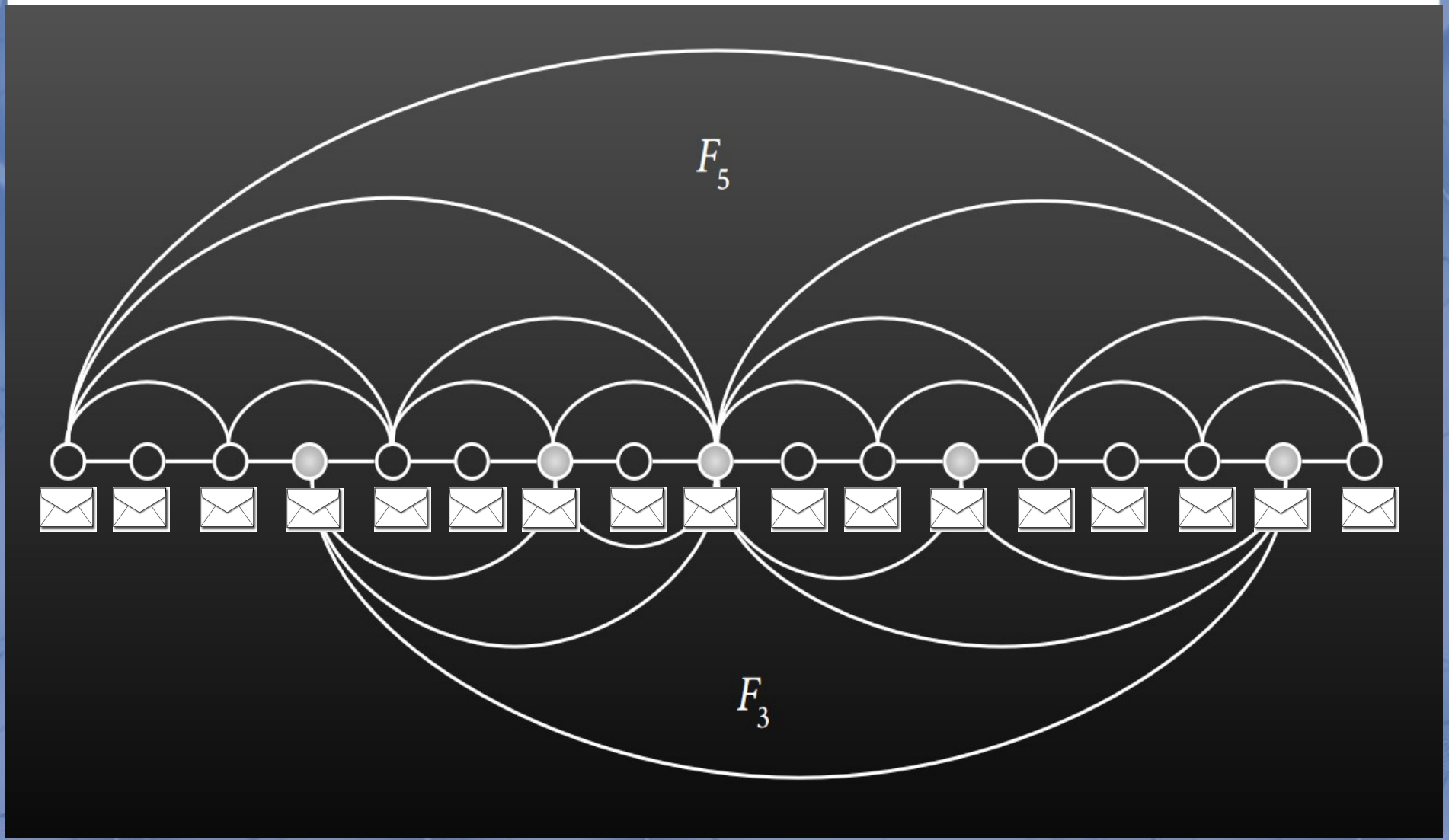
4-kolorowanie Grafu



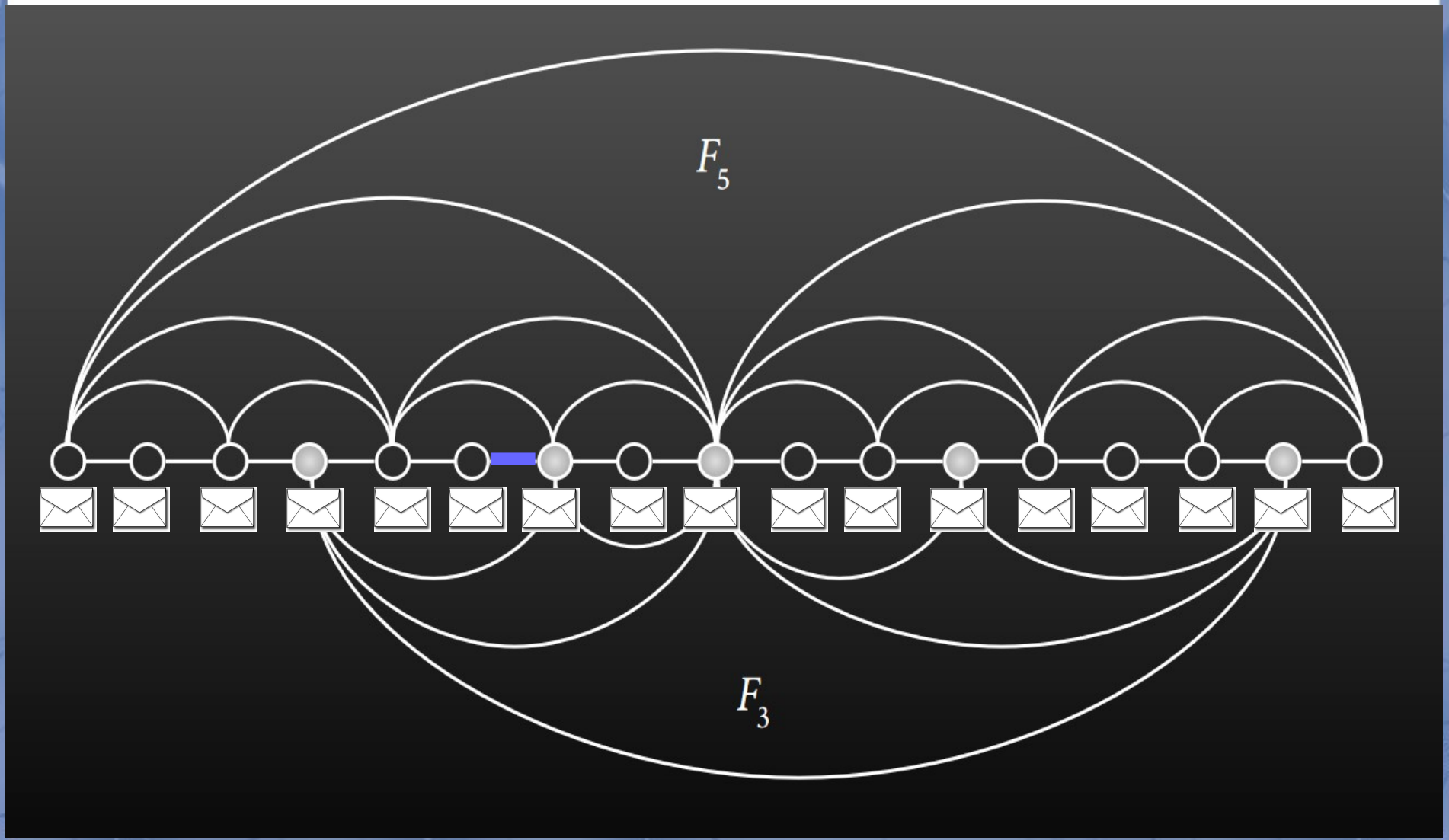
4-kolorowanie Grafu



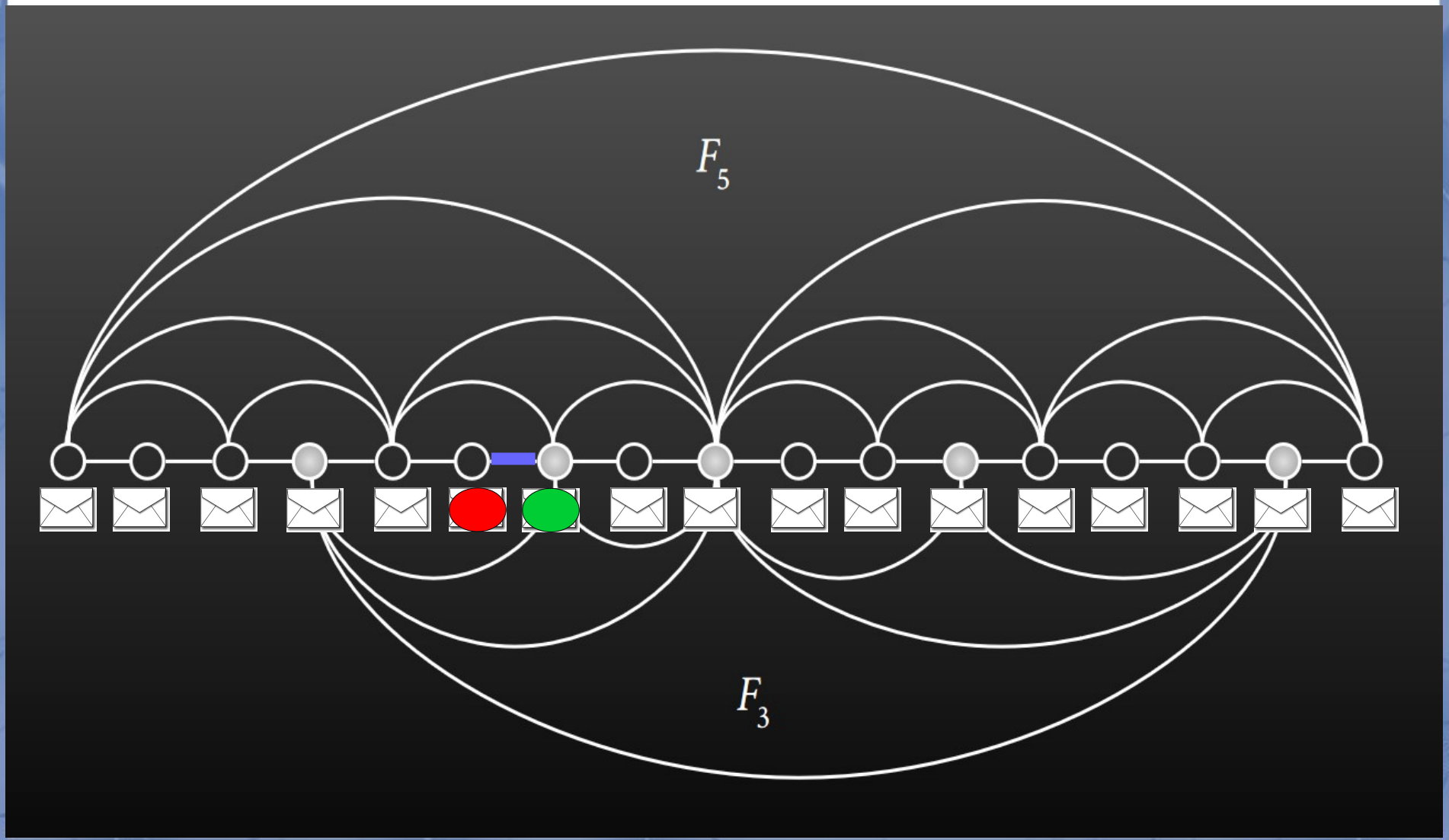
4-kolorowanie Grafu



4-kolorowanie Grafu



4-kolorowanie Grafu



4-kolorowanie Grafu

- Jesli graf jest 3-kolorowalny, zawsze sukces
- Jeśli graf nie jest 3-kolorowalny, mamy szansę co najmiej 1/m na wykrycie tego

4-kolorowanie Grafu

- Jesli graf jest 3-kolorowalny, zawsze sukces
- Jeśli graf nie jest 3-kolorowalny, mamy szansę co najmiej 1/m na wykrycie tego

- Powtarzamy procedurę k*m razy
- Szansa na oszukanie nas spada do e^{-k}
- Musimy permutować kolory!!!

O Złożoności

- 4-kolorowanie jest NP-zupełne
- Kazdy problem w NP ma zero knowledge proof
- Używamy funkcji jednostronnych jako kopert