Wręczenie Nagrody im. Witolda Lipskiego

Marek Klonowski

Marek.Klonowski@pwr.wroc.pl

Politechnika Wrocławska
Instytut Matematyki i Informatyki

Zainteresowania naukowe

Marek
Klonowski

- anonimowa komunikacja
- bezpieczeństwo dla urządzeń o silnie ograniczonych zasobach
- sieci P2P i ad hoc
- technologie podpisów cyfrowych
- e-wybory
- . . .

Anonimowa komunikacja

Marek
Klonowski

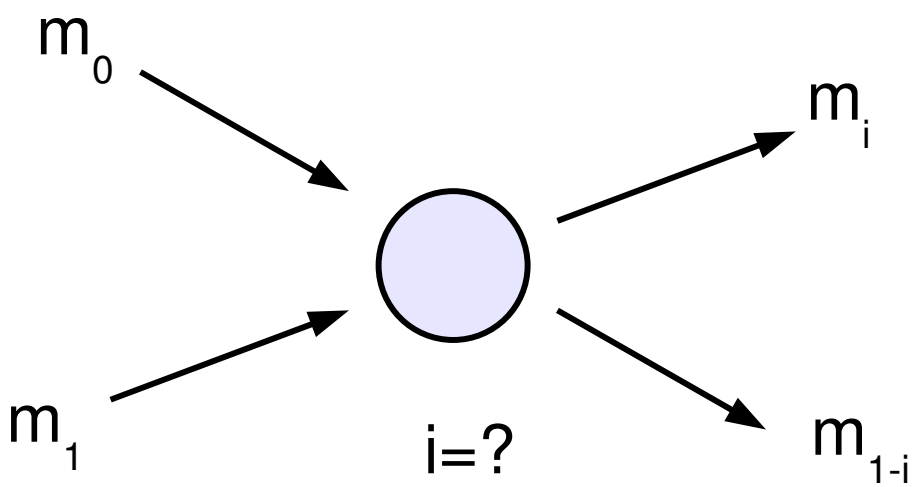
Idea

W dużym skrócie - w sieci komunikacyjnej chcemy, aby adwersarz obserwujący połączenia pomiędzy węzłami nie był w stanie ustalić, które węzły się ze sobą komunikują.

MIX Davida Chauma

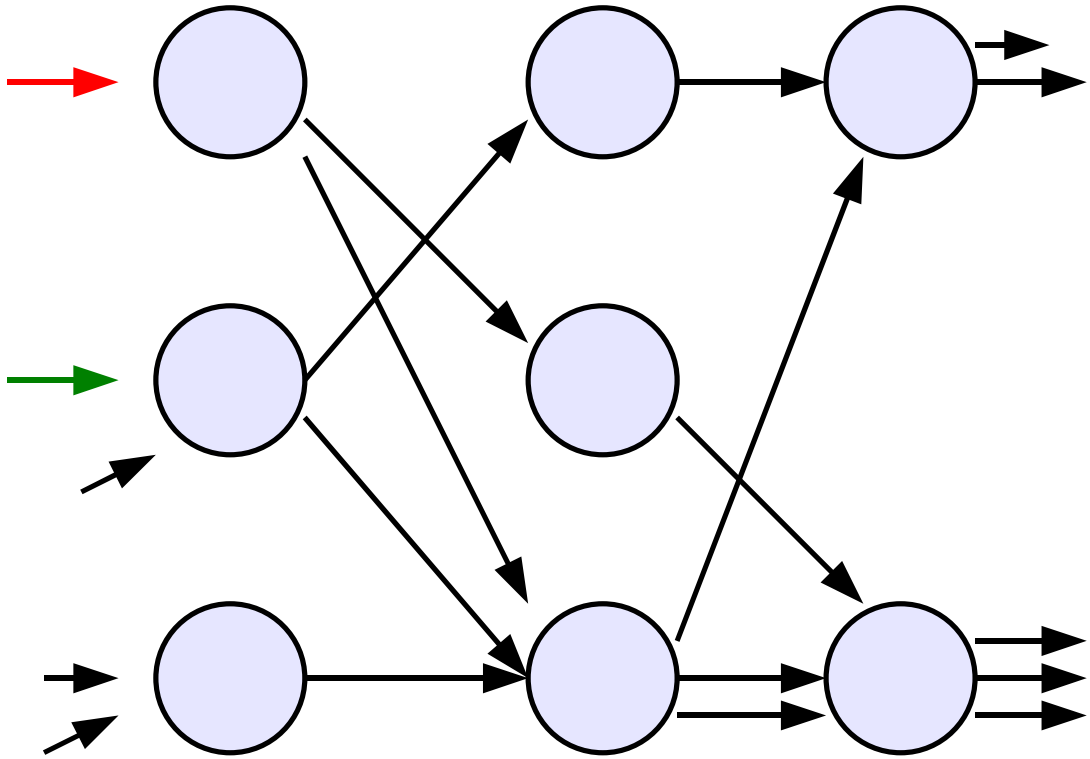
Marek Klonowski

Dzięki specjalnemu kodowaniu dwie wiadomości, które wchodzą do tego samego węzła, stają się nierozróżniane.



Sieć anonimizująca

Marek
Klonowski



Analiza modelu BFT

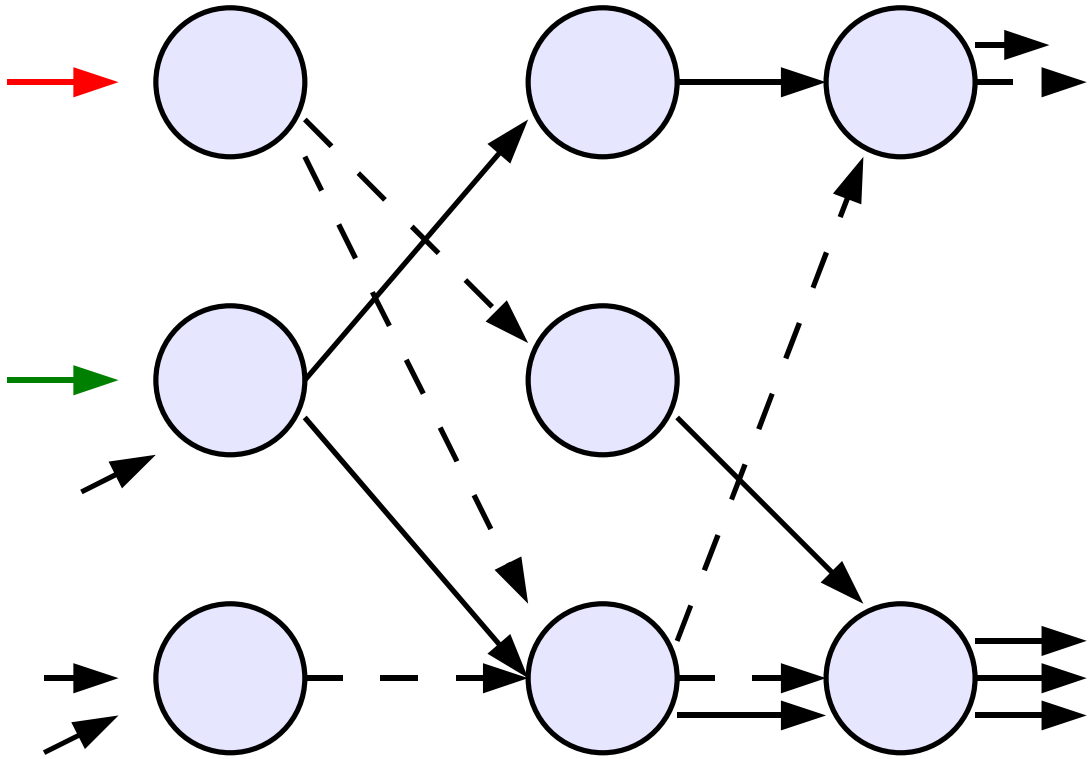
Marek
Klonowski

M. Gomułkiewicz, M. Klonowski, M. Kutyłowski, „Provable Unlinkability Against Traffic Analysis already after $\mathcal{O}(\log(n))$ steps!”.

- Adwersarz obserwuje jedynie frakcję $1 - f$ wszystkich połączeń.
- Wiadomości przesyłane są przez sieć. Intuicyjnie im dłuższa ścieżka, po której przesyłana jest wiadomość, tym anonimowość jest lepsza.

Sieć anonimizująca

Marek
Klonowski



Analiza modelu BFT

Marek Klonowski

Główny wynik

Π_t - rozkład możliwych permutacji wiadomości (z punktu widzenia adwersarza), U- permutacja losowa o rozkładzie jednostajnym. Wtedy

$$\|\Pi_t - U\| < \frac{1}{n}$$

dla wszystkich $t > \tau$, gdzie

$$\tau = \frac{6}{\ln(1-f^4)^{-1}} \ln(n) = \Theta(\log n).$$

Wykorzystane techniki:

- wiedza adwersarza jako łańcuch Markowa + coupling
- zliczanie grafów

Analiza modelu BFT

Marek Klonowski

Główny wynik

Π_t - rozkład możliwych permutacji wiadomości (z punktu widzenia adwersarza), U- permutacja losowa o rozkładzie jednostajnym. Wtedy

$$\|\Pi_t - U\| < \frac{1}{n}$$

dla wszystkich $t > \tau$, gdzie

$$\tau = \frac{6}{\ln(1-f^4)^{-1}} \ln(n) = \Theta(\log n).$$

Wykorzystane techniki:

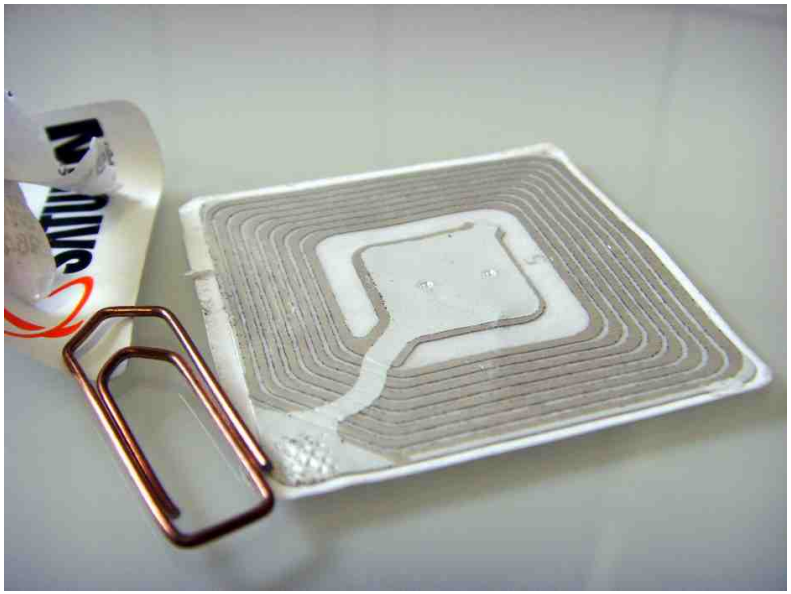
- wiedza adwersarza jako łańcuch Markowa + coupling
- zliczanie grafów

RFID - ochrona prywatności

Marek
Klonowski

RFID-tag

urządzenie z pamięcią, która może być odczytana z pewnej odległości; bardzo tanie i małe. (zd. Wikipedia)



Zastosowania i problemy

Marek
Klonowski

Zastosowania:

- następcy kodów kresowych
- *inteligentne* przedmioty
- kontrola fizycznego i logicznego dostępu
- logistyka

Problemy:

- klonowanie
- szpiegostwo przemysłowe
- **ochrona prywatności** - śledząc taga, śledzimy osobę

Zastosowania i problemy

Marek
Klonowski

Zastosowania:

- następcy kodów kresowych
- *inteligentne* przedmioty
- kontrola fizycznego i logicznego dostępu
- logistyka

Problemy:

- klonowanie
- szpiegostwo przemysłowe
- **ochrona prywatności** - śledząc taga, śledzimy osobę

Ochrona prywatności dla użytkowników RFID

Marek
Klonowski

CELE:

- Tylko uprawniona strona może śledzić taga.
- ALTERNATYWNIE: tag może być ROZPOZNANY (i śledzony), gdy użytkownik się na to zgadza.

Problem: ograniczone moce obliczeniowe

Ochrona prywatności dla użytkowników RFID

Marek
Klonowski

CELE:

- Tylko uprawniona strona może śledzić taga.
- ALTERNATYWNIE: tag może być ROZPOZNANY (i śledzony), gdy użytkownik się na to zgadza.

Problem: ograniczone moce obliczeniowe

Ochrona prywatności dla użytkowników RFID

Marek
Klonowski

CELE:

- Tylko uprawniona strona może śledzić taga.
- ALTERNATYWNIE: tag może być ROZPOZNANY (i śledzony), gdy użytkownik się na to zgadza.

Problem: ograniczone moce obliczeniowe

Rozwiązanie

Marek
Klonowski

Privacy Protection for RFID with Hidden Subset Identifiers
[J. Cichoń, M. Klonowski, M. Kutyłowski, PERVASIVE 2008]

- Wymagania sprzętowe po stronie taga:
  - kilkadziesiąt bramek logicznych
  - PRNG - fizyczne źródło, rozwiązanie standardowe

Idea (n, k)-taga

Marek
Klonowski

- Tag T składa się z n-elementowej *części niezależnej* X_T oraz k-elementowej *części zależnej* Y_T.
- Z każdym tagiem T związanych jest k losowo wybranych *zbiorów charakterystycznych* $(C_T^1, \ldots, C_T^k \subseteq \{1, \ldots, n\})$. W najprostszym przypadku każdy element jest załączany do każdego ze zbiorów z prawdopodobieństwem p.
- Znajomość zbiorów charakterystycznych umożliwia rozpoznanie taga.

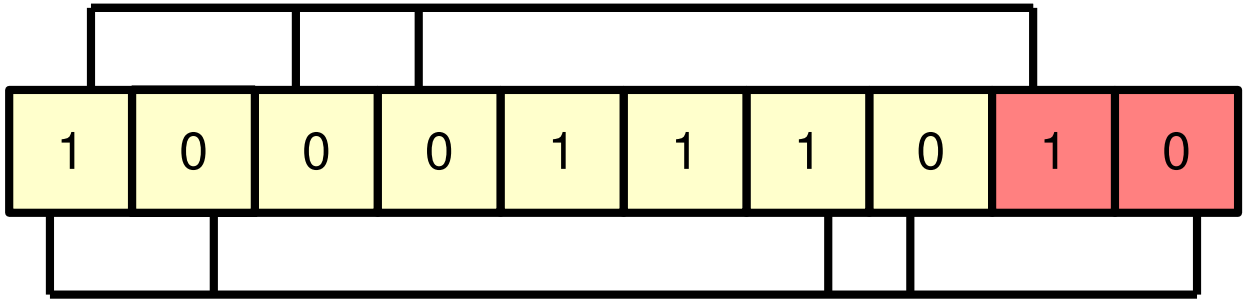
Procedura Update

Marek
Klonowski

procedure Update(T)
begin
  $X_T \in_R \{0,1\}^n$;
  for $i = 1$ to k
    $Y_T(i) := \bigoplus_{C_T^i} X_T$;
end;

RFID - ochrona prywatności

Marek
Klonowski



Odpowiedzi taga

Marek
Klonowski

	Zależna	Niezależna
1:	11001111	11
2:	01101111	11
3:	10010111	00
4:	11111011	00
5:	01111011	10
6:	11000100	00
7:	00000101	01
8:	10110110	10
9:	10000110	01

Unlinkability

Marek Klonowski

Adwersarz obserwuje t odczytów z L tagów $\{T_1, T_2, \ldots, T_L\}$. Następnie przedstawiany jest mu nowy, $t+1$. odczyt z jednego losowo wybranego taga T_i. Zadaniem adwersarza jest znalezienie i.

Twierdzenie

Prawdopodobieństwo znalezienia właściwego i przez **dowolnego** adwersarza jest mniejsze niż

$$\frac{1}{L} + L \cdot \frac{2^{t+1}}{2^n}(1 + (1-2p)^{t+1})^n \ .$$

Unlinkability

Marek Klonowski

Adwersarz obserwuje t odczytów z L tagów $\{T_1, T_2, \ldots, T_L\}$. Następnie przedstawiany jest mu nowy, $t+1$. odczyt z jednego losowo wybranego taga T_i. Zadaniem adwersarza jest znalezienie i.

Twierdzenie

Prawdopodobieństwo znalezienia właściwego i przez **dowolnego** adwersarza jest mniejsze niż

$$\frac{1}{L} + L \cdot \frac{2^{t+1}}{2^n}(1 + (1-2p)^{t+1})^n \, .$$

Analiza rozwiązania

Marek
Klonowski

Tagi w praktyce

- Ochrona prywatności – adwersarz, aby śledzić taga musi zebrać kilkaset (kilka tysięcy) odczytów z pojedynczego taga.
- Uprawniona strona może rozpoznać tag w pojedynczym odczycie z wysokim prawdopodobieństwem. ($\approx 1 - 2^{-k}$)

Analiza

- Część twierdzeń może być sprowadzona do analizy rzędu losowej macierzy.

Trwałe usuwanie danych

Marek Klonowski

Data deletion with provable security (Praca z M. Przykuckim i T. Strumińskim)

Dotychczasowe podejście

- heurystyki - nadpisywanie zawartości dysków; brak formalnej analizy.
- Adwersarz posiadający bardzo czułe urządzenie może dane odzyskać.
- Bezpieczeństwo zależy od fizycznych własności nośników danych.

Nowe podejście

- Specjalne kodowanie umożliwia usunięcie danych niezależnie od własności nośnika; dowodliwe bezpieczeństwo

Marek
Klonowski

Dziękuję bardzo!