Kryptosystem z generacją skrzynek podstawieniowych w czasie rzeczywistym wykorzystujący dyskretne chaotyczne układy dynamiczne

Seminarium

Michał Łazicki

Opiekun:
dr hab. Z. Kotulski, prof. PW

Cel pracy

- Wykorzystanie dyskretnych układów dynamicznych z własnością chaosu do budowy wydajnego i bezpiecznego kryptosystemu

Co to jest szyfr blokowy?

- Strumień informacji (bitów) dzielony na bloki o skończonej długości
- Szyfrowanie – przekształcenie bloku bitów (tekst odkryty) w inny blok bitów o tej samej długości (szyfrogram)
- Formalnie:

$$F_K(\cdot) : \{0,1\}^l \rightarrow \{0,1\}^l$$

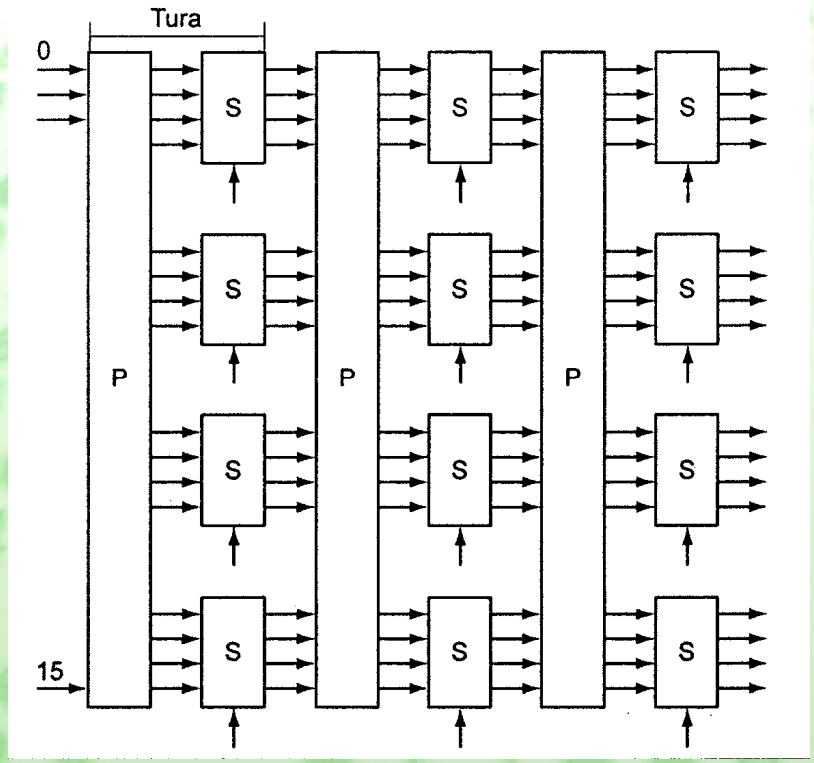
Wymagania dla szyfrów blokowych

- Funkcja *F* powszechnie znana
- Legalny użytkownik powinien łatwo wykonywać operację szyfrowania F_K i odszyfrowania F_K^{-1} o ile zna tajny klucz *K*
- Potencjalny przeciwnik ma trudności z:
  - szyfrowaniem i deszyfrowaniem, gdy nie zna klucza *K*
  - znalezieniem klucza na podstawie pary tekstów: odkryty i zaszyfrowany
  - uzyskaniem jakiejkolwiek informacji na podstawie znajomości tekstu zaszyfrowanego.

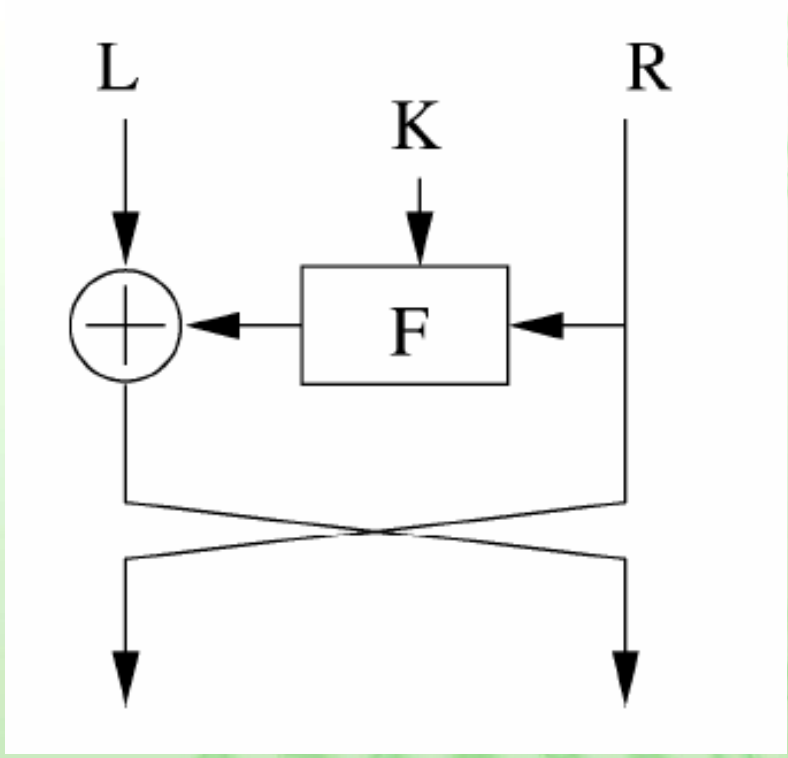
Budowa szyfru blokowego

- Funkcja F_K – n-krotne złożenie pewnego przekształcenia f_{Ki} nazywanego funkcją rundową
  - K_i – klucze rundowe otrzymane z klucza K
  - $i = 1, \ldots, n$ – numer rundy
- Funkcja rundowa f_{Ki} złożona z:
  - operacji nieliniowych, czyli podstawień
  - operacji liniowych, czyli permutacji

Struktury szyfrów blokowych



Struktura S-P



Struktura Feistela

Wymagania konstrukcyjne

- Mieszanie i rozpraszanie
- Lawinowość i zupełność
- Dyfuzja i konfuzja

Mieszanie i rozpraszanie

- Mieszanie – losowe i równomierne rozprowadzanie wiadomości tekstu jawnego po zbiorze wiadomości tekstu zaszyfrowanego
- Rozpraszanie – bity znajdujące się obok siebie przed wejściem do rundy, po wyjściu z tej rundy wpływają na bity odległe od siebie (każdy bit wejściowy wpływa na wiele bitów wyjściowych)

Lawinowość i zupełność

- Lawinowość – zmiana jednego bitu na wejściu rundy wywołuje zmianę co najmniej dwóch bitów na wyjściu rundy
- Zupełność – każdy bit bloku wyjściowego jest skomplikowaną funkcją wszystkich bitów bloku wejściowego

Dyfuzja i konfuzja

- Dyfuzja – rozmycie wszelkich związków pomiędzy bitami tekstu jawnego lub klucza w całym bloku
  - Miarą dyfuzji jest prawdopodobieństwo aproksymacji różnicowej *DP*
- Konfuzja – maksymalne wymieszanie bitów bloku klucza z bitami bloku tekstu szyfrowanego i uczynienie ich związku skomplikowanym
  - Miarą konfuzji jest prawdopodobieństwo aproksymacji liniowej *LP*

Teoria chaosu

- Dział matematyki zajmujący się opisem układów zdeterminowanych, które jednak zachowują się w sposób kapryśny, nieprzewidywalny i na pozór przypadkowy
- Dla pewnych wartości parametrów równania zachowują się chaotycznie, podczas gdy dla pozostałych - regularnie

Teoria chaosu – pojęcia (1/3)

- Dyskretny układ dynamiczny – para (X, φ) :
  - X – przestrzeń stanów (przestrzeń metryczna)
  - φ – ciągłe odwzorowanie z X do X
- Trajektoria (startująca z punkt x_0) – ciąg elementów X uzyskanych przez iteracje:

$$x_{n+1} = \varphi(x_n) \; lub \; x_n = \varphi^n(x_0)$$

Teoria chaosu – pojęcia (2/3)

- Niestabilność – wrażliwość na warunki początkowe („efekt motyla”)
- Matematycznie: dodatni wykładnik Lapunowa
- Cecha systemu niestabilnego to wykładniczy wzrost między sąsiednimi punktami przestrzeni fazowej
  - $x_{n+1} = ax_n$ => po n krokach otrzymujemy zależność: $x_{n+1} = a^n x_0 = x_0 e^{nlna}$
  - *lna* – pokazuje, jak zmienia się odległość między punktami

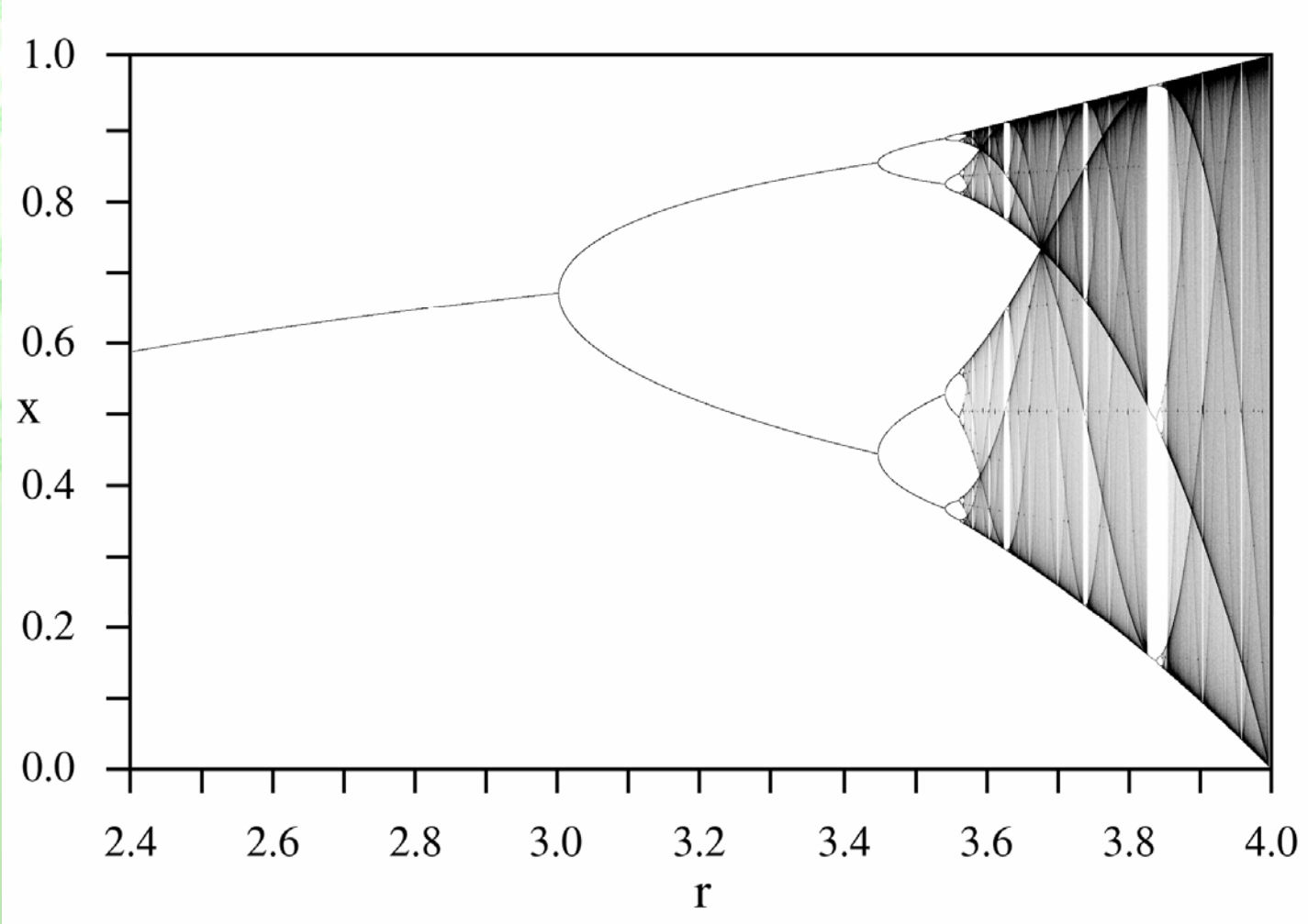
Teoria chaosu – pojęcia (3/3)

- Ergodyczność – trajektoria startująca z dowolnego $x_0 \in X$ nigdy nie lokalizuje się w pewnym podzbiorze przestrzeni
- Mieszanie – własność silniejsza niż ergodyczność; startując z dowolnego $x_0 \in X$, w wyniku iteracji osiągamy dowolny podzbiór X z prawdopodobieństwem proporcjonalnym do rozmiaru tego zbioru w całej przestrzeni stanów

Odwzorowanie logistyczne (1/2)

- $x_{n+1} = rx_n(1-x_n)$ na odcinku jednostkowym [0,1]
- Dla wartości $r \in [0,4]$ odwzorowanie przeprowadza odcinek jednostkowy w siebie
- Dla różnych wartości r, układ generuje różne trajektorie
  - $0<r\leq 1$ – wszystkie ciągi $x_1, x_2,\ldots,x_n$ zbiegają do zera
  - $1<r\leq 3$ – punkt $1-1/r$ jest atraktorem – zbiegają do niego wszystkie ciągi $x_1, x_2,\ldots,x_n$
  - $r>3$ – atraktor staje się wielopunktowy

Odwzorowanie logistyczne (2/2)



Między chaosem a kryptografią

System chaotyczny	Algorytmy kryptograficzne
Przestrzeń fazowa: zbiór liczb rzeczywistych	Przestrzeń fazowa: zbiór liczb naturalnych
Iteracje	Rundy

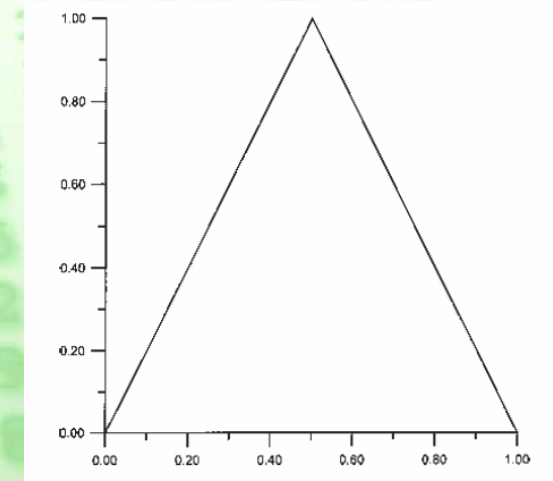
Między chaosem a kryptografią

Parametry	Klucze
Wrażliwość na zmianę warunków początkowych	Dyfuzja
?	Bezpieczeństwo i wydajność

Pierwszy szyfr blokowy oparty o chaos dyskretny (1/4)

- Propozycja Toshiki Habutsu na konferencji EUROCRYPT'91

$$F: \begin{cases} x_{n+1} = \dfrac{x_n}{\alpha} & dla\ 0 \le x_n \le \alpha \\ x_{n+1} = \dfrac{x_n - 1}{\alpha - 1} & dla\ \alpha < x_n \le 1 \end{cases}$$



- Wykładnik Lapunowa dla danego α:

$$\lambda = -\alpha \log \alpha - (1 - \alpha) \log(1 - \alpha)$$

Pierwszy szyfr blokowy oparty o chaos dyskretny (2/4)

- Odwzorowanie odwrotne ma postać:

$$F^{-1}: \begin{cases} x_{n-1} = \alpha x_n \\ \text{lub} \\ x_{n-1} = (\alpha - 1)x_n + 1 \end{cases}$$

- Odwzorowania F i F^{-1} mają właściwości:
  - *F* jest odwzorowaniem 2:1
  - F^{-1} jest odwzorowaniem 1:2
  - F^n jest odwzorowaniem 2^n:1
  - F^{-n} jest odwzorowaniem $1:2^n$

Pierwszy szyfr blokowy oparty o chaos dyskretny (3/4)

- Dla każdego n i dla każdego $x \in X = [0,1]$ spełniona jest równość: $X = F^n(F^{-n}(X))$
- Tajnym kluczem jest parametr $\alpha \in [0,1]$
- Szyfrowaną wiadomością (blokiem) jest liczba $P \in [0,1]$
- Szyfrowanie:

$$C=F^{-n}(P)=F^{-1}(F^{-1}(\ldots F^{-1}(P)))$$

- Deszyfrowanie:

$$P=F^{n}(C)=F(F(\ldots F(C)))$$

Pierwszy szyfr blokowy w oparty o chaos dyskretny (4/4)

- Zalety:
  - Bezpieczeństwo szyfru oparte na ścisłej teorii matematycznej: teorii dyskretnych w czasie układów dynamicznych z własnością chaosu
- Wady:
  - Nieodporny na różne rodzaje ataków, m. in. atak wybranym szyfrogramem, atak wybranym tekstem jawnym
  - Operuje na liczbach rzeczywistych, zatem wynik obliczeń zależy od implementacji sprzętowej

Chaotyczny szyfr blokowy

- Propozycja budowy szyfru z użyciem S-boxów wygenerowanych przy pomocy chaotycznych układów dynamicznych

Chaotyczny szyfr blokowy

- Propozycja szyfru:
  - Dane wejściowe: blok bitów o długości 64 bitów
  - Klucz: blok bitów o długości 128 bitów
  - Dane wyjściowe: blok bitów o długości 64 bitów
  - Liczba rund: r

Chaotyczny szyfr blokowy

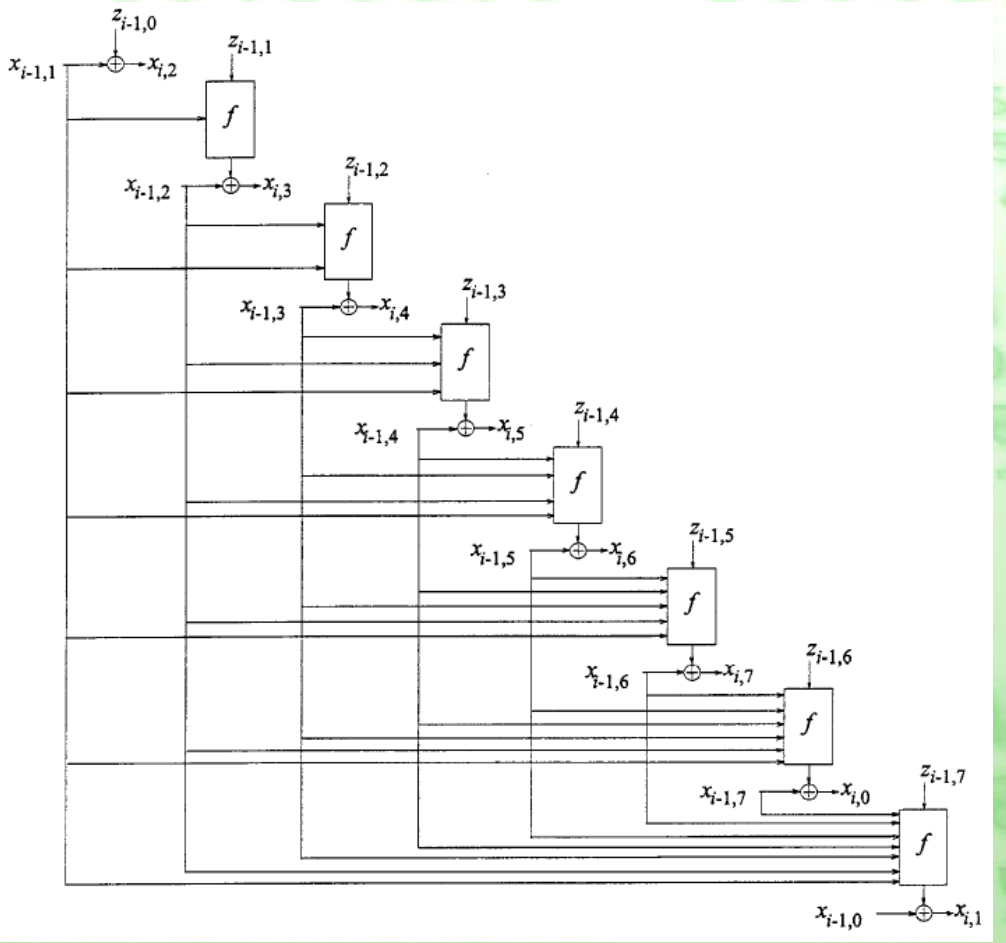
- Generacja kluczy rundowych:
  - K – klucz: $K=K_0K_1\ldots K_{15}$
  - $K_{i,k+1}=K_{i-1,k} \oplus f_{k-1}[K_{i-1,1}, \ldots, K_{i-1,k-1}, c_{k-1}]$
  - z_i – klucz i-tej rundy, $z_i=RH(K_i)$
  - gdzie:
    - $i=1,\ldots,r$
    - $k=1,\ldots,16$
    - $f_0=c_0$, $K_{i,16}=K_{i,0}$, $K_{i,17}=K_{i,1}$
    - $c_0,\ldots,c_{15}$ – stała liczba
    - $f_{k-1}[K_{i-1,1}, \ldots, K_{i-1,k-1}, c_{k-1}] = f_{k-1}[K_{i-1,1} \oplus \ldots \oplus K_{i-1,k-1} \oplus c_{k-1}]$
    - RH – funkcja, która zwraca prawą połowę klucza K_i

Chaotyczny szyfr blokowy

- Szyfrowanie:
  - X – dane wejściowe: $X=X_0X_1\ldots X_7$
  - $X_{i,k+1}=X_{i-1,k} \oplus f_{k-1}[X_{i-1,1}, \ldots, X_{i-1,k-1}, z_{i,k-1}]$
  - gdzie:
    - $i=1,\ldots,r$
    - $k=1,\ldots,8$
    - $f_0=z_{i,0}$, $X_{i,8}=X_{i,0}$, $X_{i,9}=X_{i,1}$
    - z_i – klucz i-tej rundy
    - $f_{k-1}[X_{i-1,1}, \ldots, X_{i-1,k-1}, z_{i,k-1}] = f_{k-1}[X_{i-1,1} \oplus \ldots \oplus X_{i-1,k-1} \oplus z_{i,k-1}]$

Chaotyczny szyfr blokowy

Runda szyfrowania danych



Chaotyczny szyfr blokowy

- Deszyfrowanie:
  - X – dane wejściowe: $X=X_0X_1\ldots X_7$
  - $X_{i-1,k}=X_{i,k+1} \oplus f_{k-1}[X_{i-1,1}, \ldots, X_{i-1,k-1}, z_{i,k-1}]$
  - gdzie:
    - $i=r,\ldots,1$
    - $k=1,\ldots,8$
    - $f_0=z_{i,0}$, $X_{i,8}=X_{i,0}$, $X_{i,9}=X_{i,1}$
    - z_i – klucz i-tej rundy
    - $f_{k-1}[X_{i-1,1}, \ldots, X_{i-1,k-1}, z_{i,k-1}] = f_{k-1}[X_{i-1,1} \oplus \ldots \oplus X_{i-1,k-1} \oplus z_{i,k-1}]$

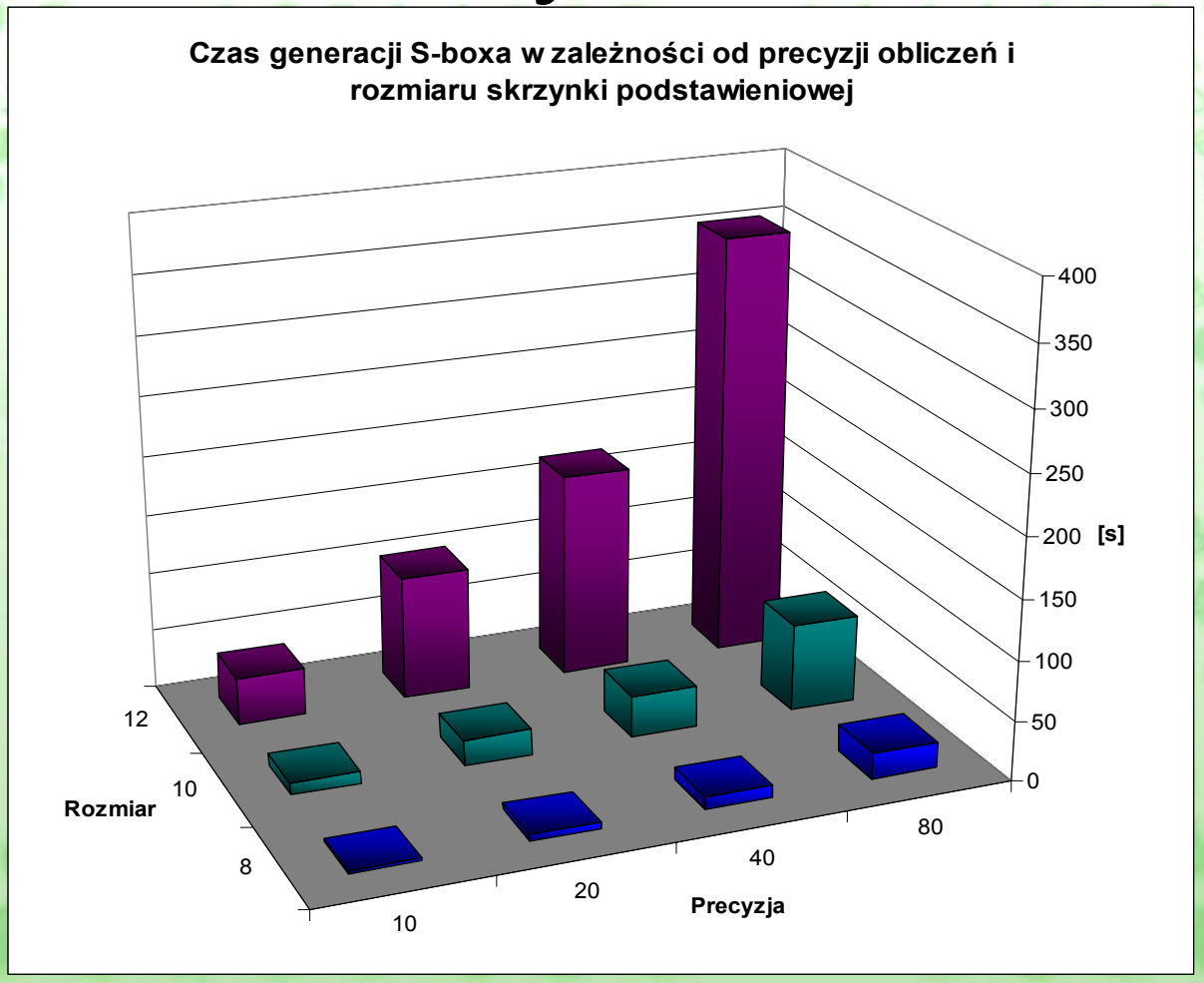
Metoda generacji S-boxów

- Propozycja generacji S-boxów przy użyciu chaotycznych układów dynamicznych:
  - odwzorowanie logistyczne: $x_{n+1} = 4x_n(1-x_n)$
  - Procedura generacji S-boxa o m wartościach:
    1. Dzielimy przestrzeń stanów na n+1>me obszarów i każdemu z obszarów przypisujemy liczbę od 0 do n
    2. Punkt w obszarze i ma wartość i
    3. Wybieramy losowo z każdego obszaru punkt i poddajemy go N przekształceniom
    4. Znajdujemy zbiór punktów startowych S, które mają unikalny obraz (tzn. do jednego przedziału wpada tylko jeden punkt) oraz wybieramy podzbiór A o m elementach
    5. Przypisujemy mu nowe wartości od 0 do m-1 i tak samo ich obrazom, zachowując porządek starych wartości

Metoda generacji S-boxów - problemy

- Dokładność obliczeń
  - Zmienna double 0.1 → 0.1000000000000000055511151231257827021181583404541015625
  - Rozwiązanie: obiekt reprezentujący liczbę z odcinka (0,1) ze skończoną dokładnością
- Czas obliczeń

Metoda generacji S-boxów - wyniki



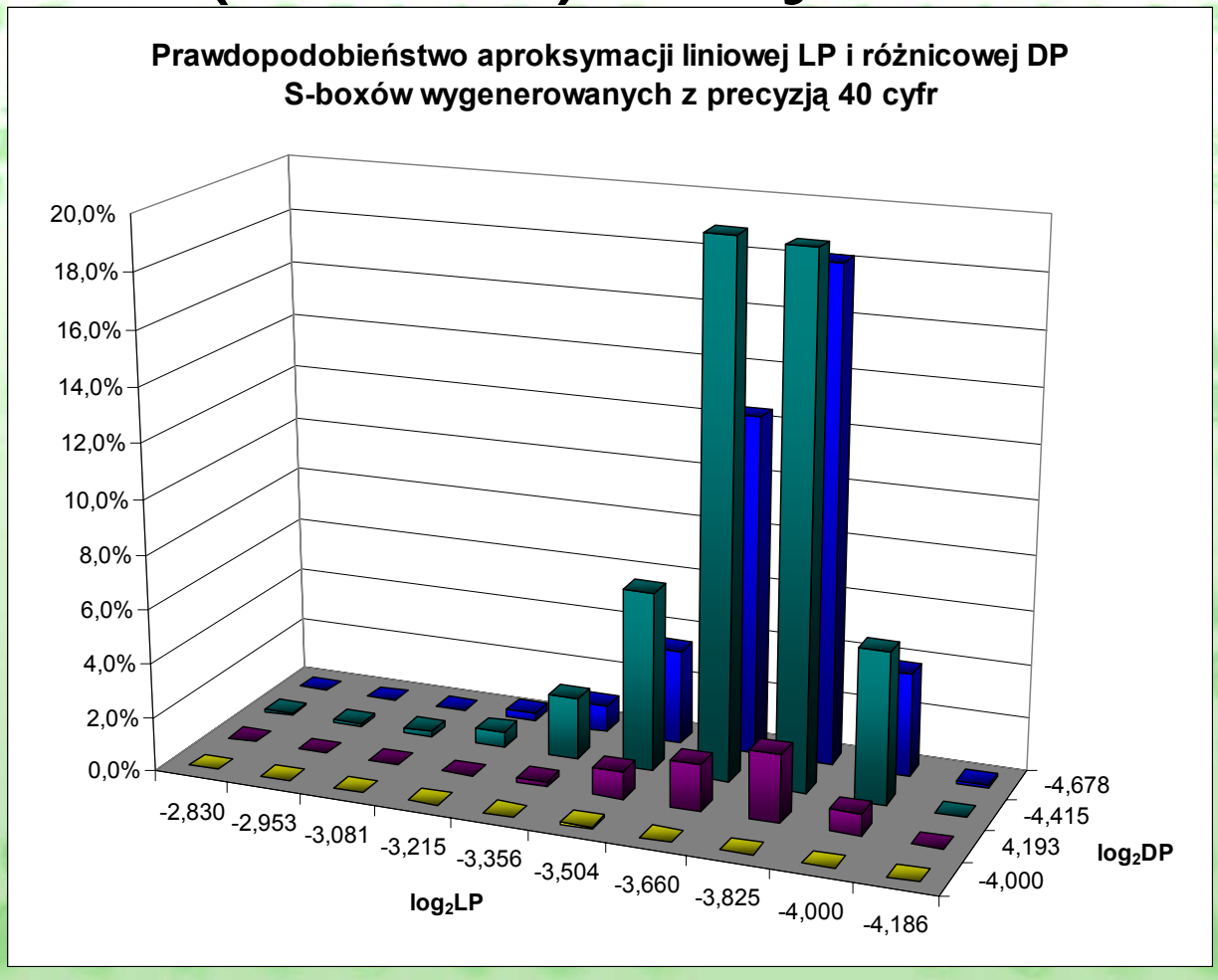
Metoda generacji S-boxów - wyniki

Parametry S-boxa 8 bitowego dla generacji z precyzją 40 cyfr				
	DP	LP	SAC	Czas [s]
Min.	$2^{-4,678}$	$2^{-4,186}$	0,4841	10,540
Max.	$2^{-4,000}$	$2^{-2,712}$	0,5127	10,771
Średnia	$2^{-4,513}$	$2^{-3,726}$	0,5017	10,611

Parametry S-boxa 10 bitowego dla generacji z precyzją 40 cyfr				
	DP	LP	SAC	Czas [s]
Min.	$2^{-6,415}$	$2^{-5,660}$	0,4943	34,858
Max.	$2^{-5,678}$	$2^{-4,953}$	0,5068	35,750
Średnia	$2^{-6,258}$	$2^{-5,375}$	0,5007	35,185

Parametry S-boxa 12 bitowego dla generacji z precyzją 40 cyfr				
	DP	LP	SAC	Czas [s]
Min.	$2^{-8,193}$	$2^{-7,320}$	0,4988	170,294
Max.	$2^{-7,660}$	$2^{-6,922}$	0,5011	172,958
Średnia	$2^{-8,036}$	$2^{-7,143}$	0,4998	171,396

Metoda generacji S-boxów (8 – bit) - wyniki



Właściwości S-boxów (8 – bit)

- Dobre właściwości kryptograficzne S-boxów:

$$2^{-4} \leq DP \leq 2^{-5}$$

$$2^{-3} \leq LP \leq 2^{-4}$$

- Dla całego szyfru:

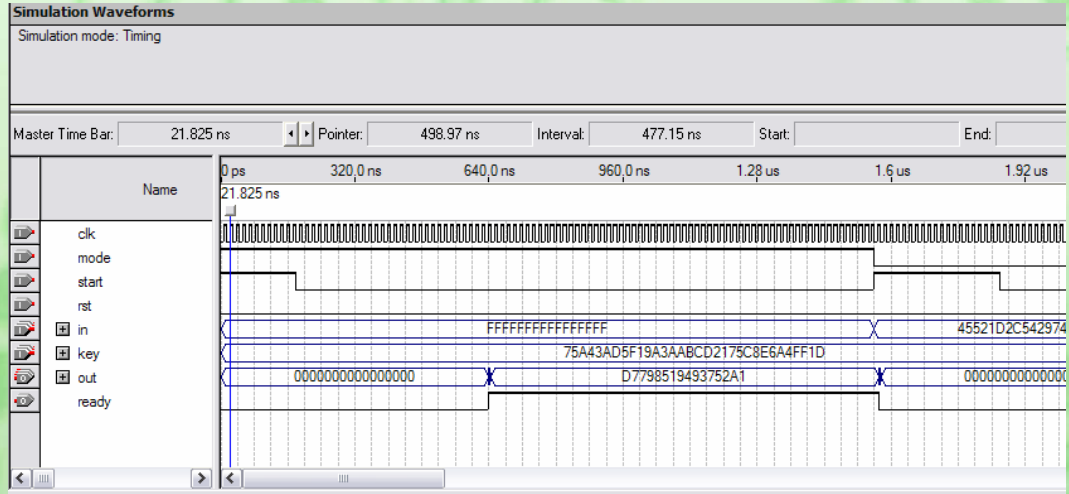
$$2^{-68} \leq DP \leq 2^{-85}$$

$$2^{-51} \leq LP \leq 2^{-68}$$

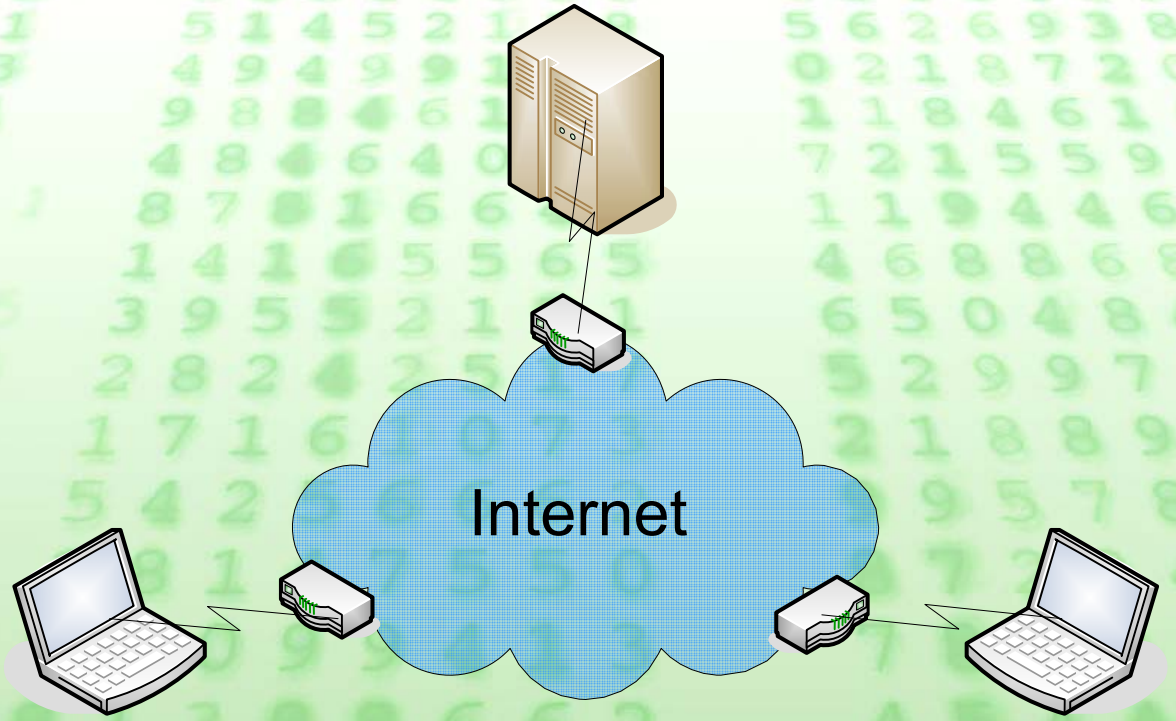
- Złożoność ataków:
  - różnicowego: $\sim 1/DP$
  - liniowego: $\sim 1/LP$

Realizacja w układzie FPGA

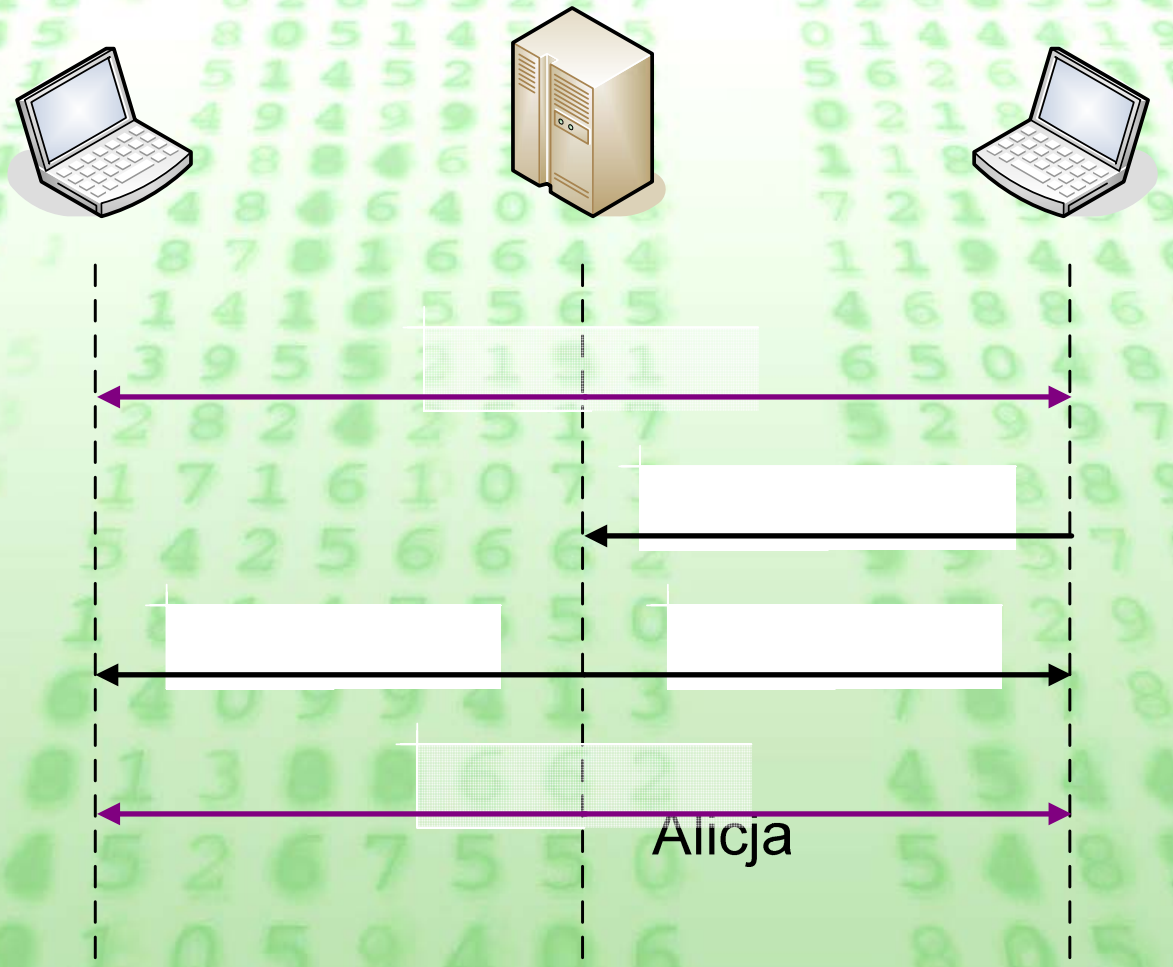
- Układ zaimplementowany w układzie FPGA Stratix z rodziny EP1S20
- Przepływność: 195 Mbit/s
- Przepływność dla szyfru AES: 365 Mbit/s



Propozycja kryptosystemu (1)



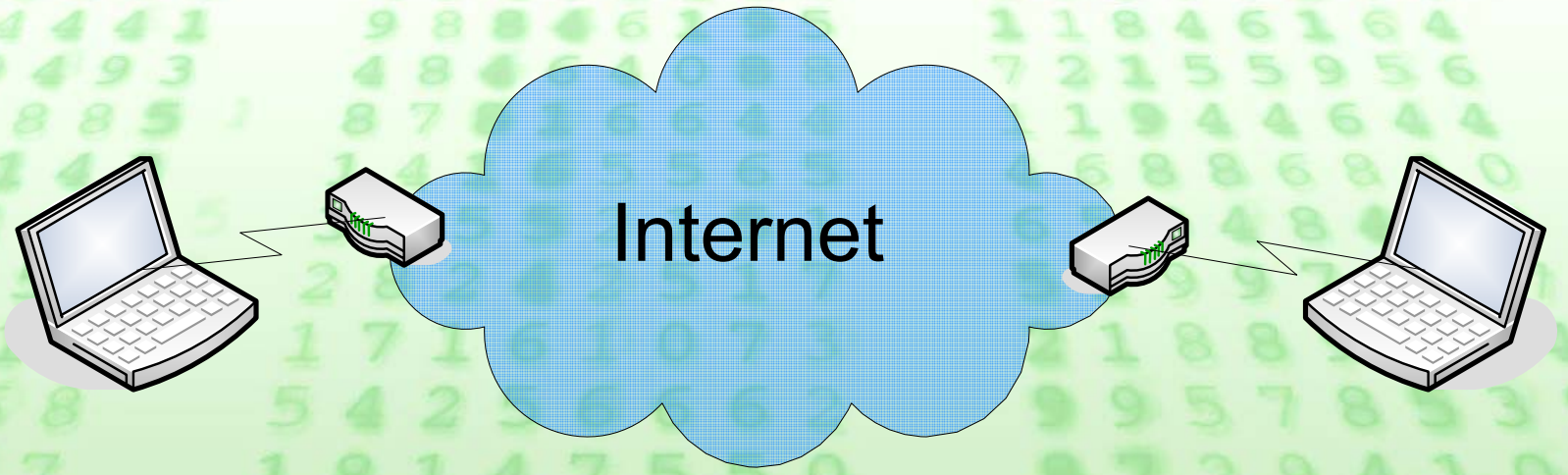
Propozycja kryptosystemu (1)



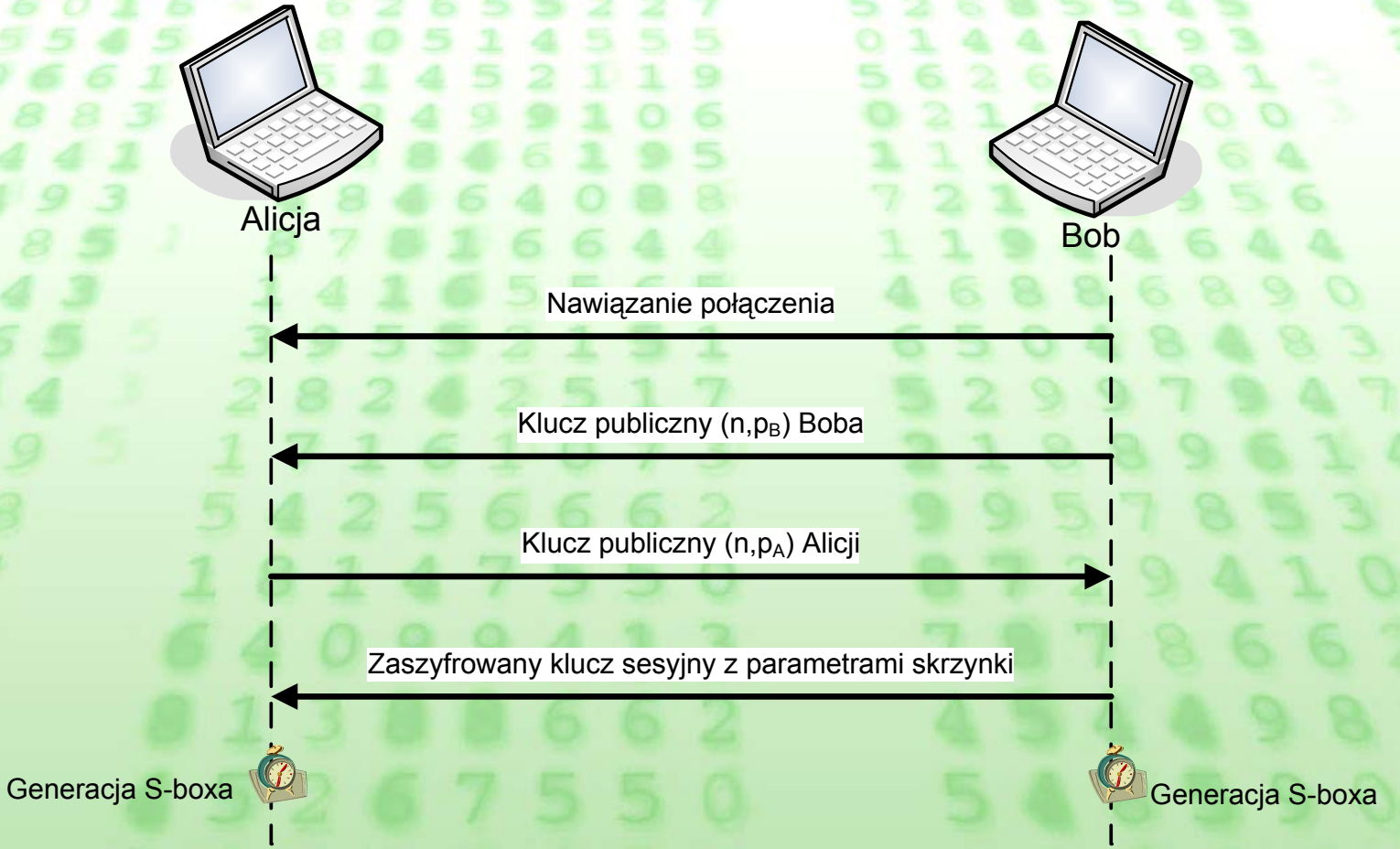
Trzecia Za

Dys

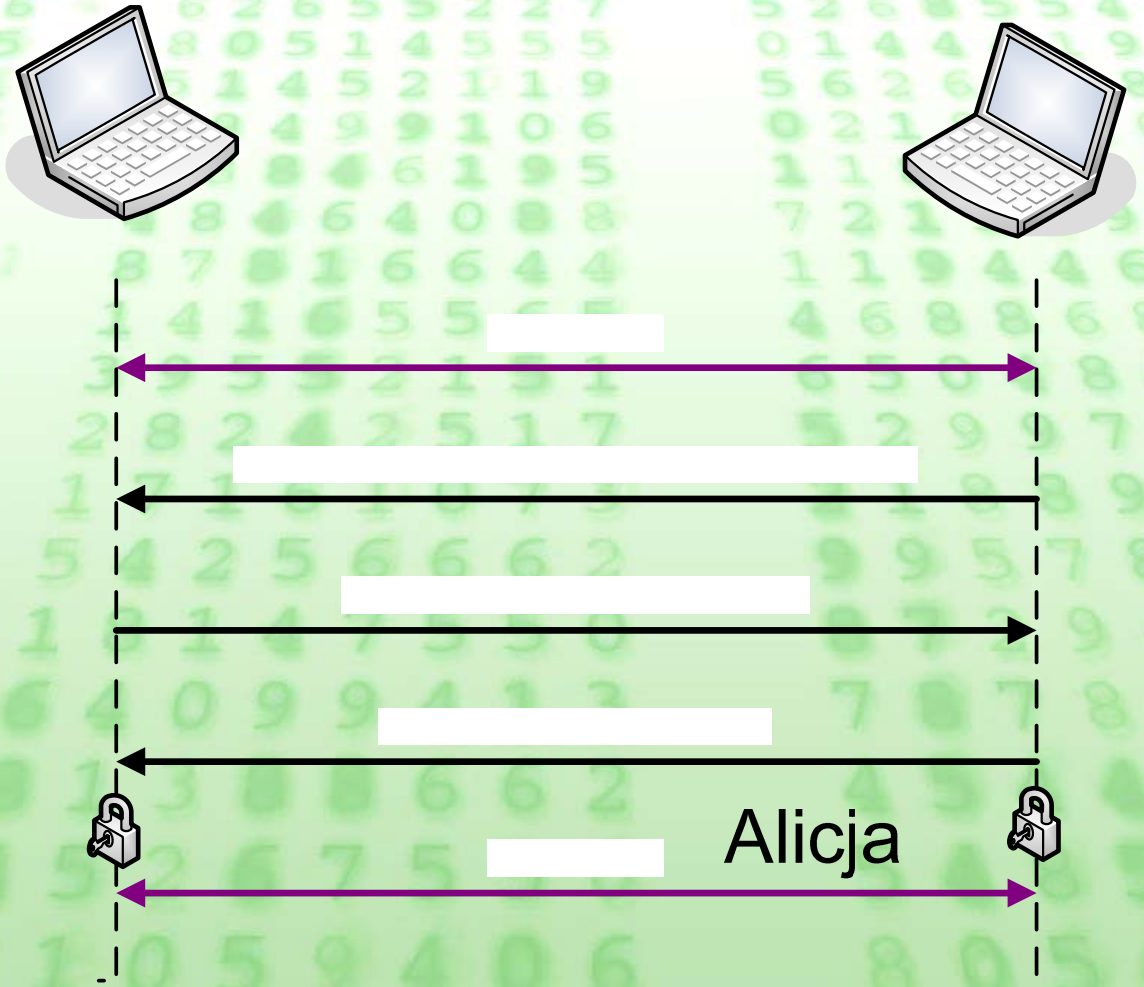
Propozycja kryptosystemu (2)



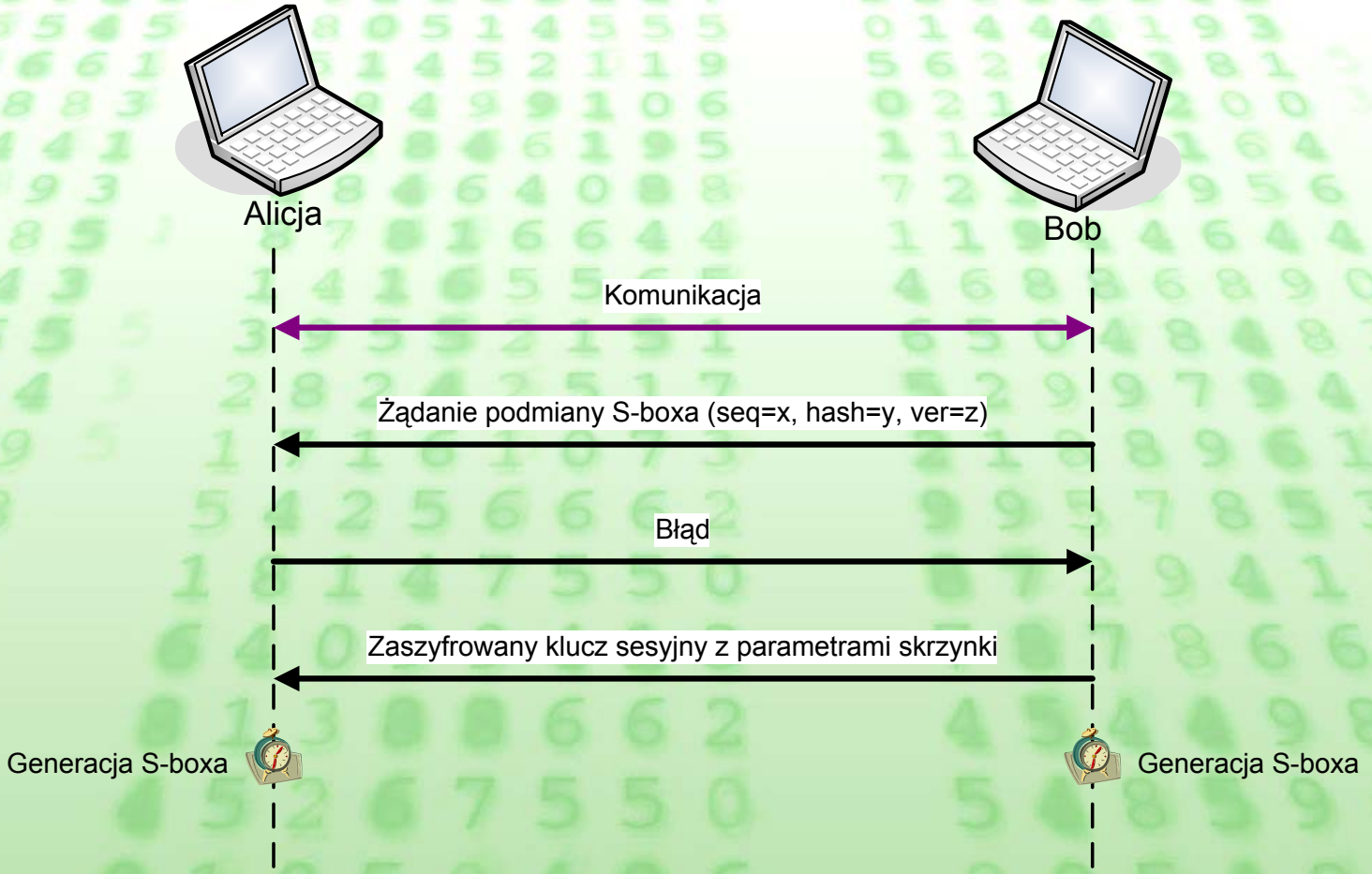
Propozycja kryptosystemu (2)



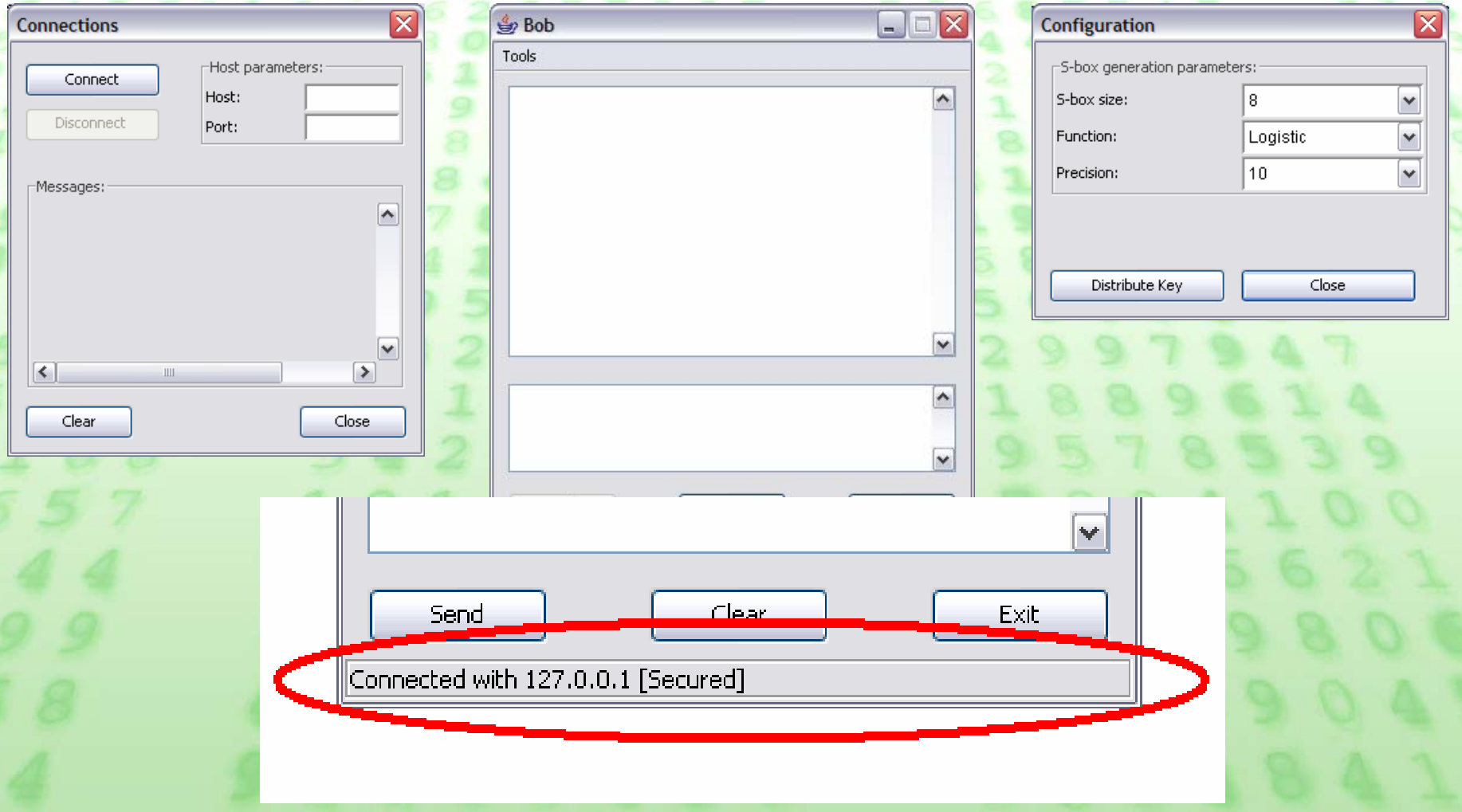
Propozycja kryptosystemu (2)



Propozycja kryptosystemu (2)



Implementacja kryptosystemu



Kryptosystem -zagrożenia

- Atak „man in the middle”
- Odkrycie klucza sesyjnego przy pierwszej turze wymiany wiadomości sygnalizacyjnych

Podsumowanie

- „Ktoś z bardzo dobrą znajomością kryptoanalizy i teorii chaosu jest w stanie skonstruować bezpieczny, aczkolwiek wolny algorytm kryptograficzny”

  L. Kocarev

- Kryptosystem z generacją skrzynek podstawieniowych w czasie rzeczywistym oparty na chaosie
- Implementacja sprzętowa i programowa

Dziękuję za uwagę.