Hybrydowy system służący do kryptoanalizy szyfrów opartych na krzywych eliptycznych

Piotr Majkowski

Politechnika Warszawska – Wydział Elektroniki i Technik Informacyjnych Instytut Telekomunikacji

System rozpraszania obliczeń z zastosowaniem w rozwiązywaniu zagadnienia logarytmu dyskretnego na krzywych eliptycznych

Piotr Majkowski

Praca inżynierska pod opieką: prof Zbigniewa Kotulskiego

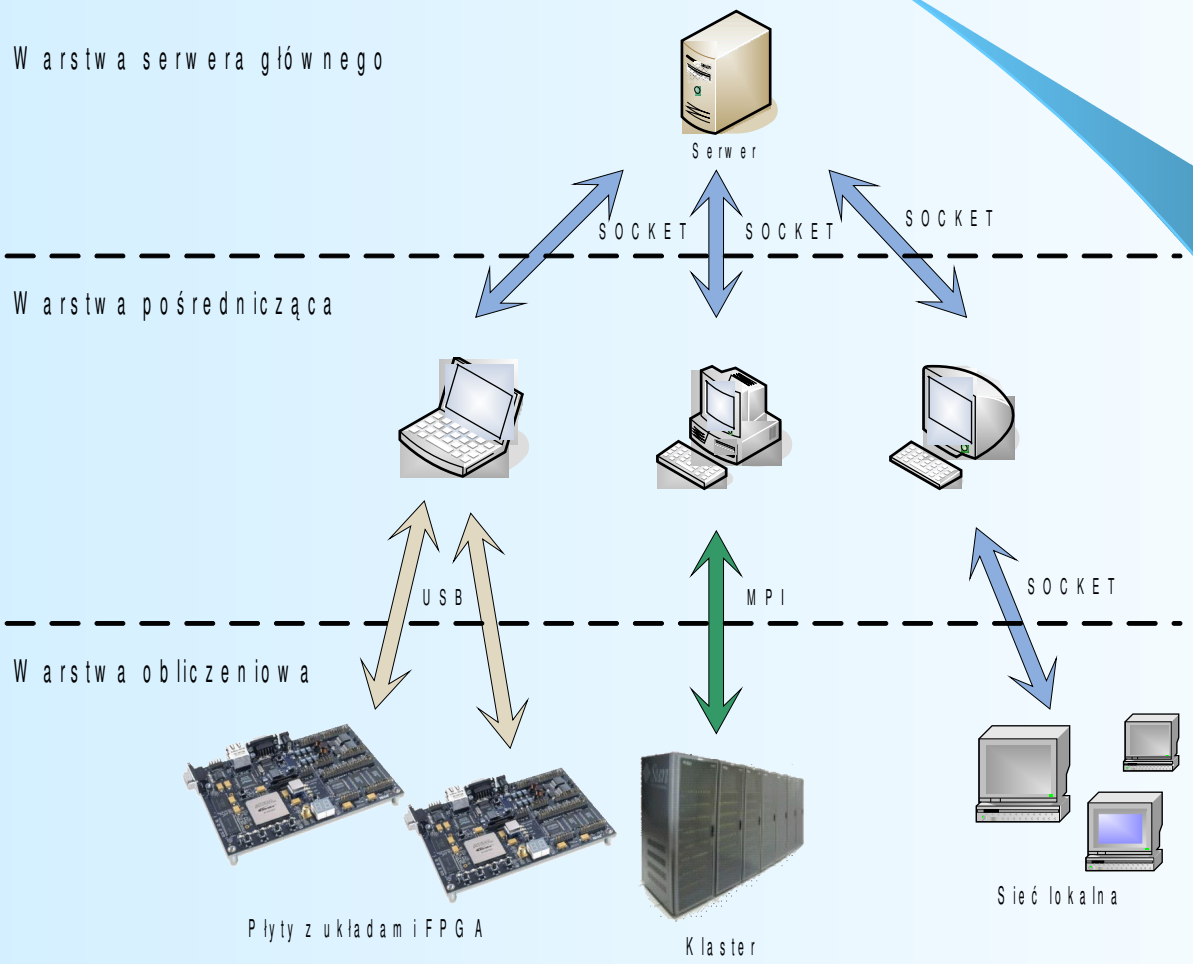
Cechy stworzonego systemu

- Niezależność od przeprowadzanych obliczeń.
- Niezależność od technologii przesyłania danych.
- Niezależność od środowiska systemowego.
- Skalowalność.
- Umożliwienie dynamicznych zmian liczby klientów obliczeniowych niezauważalnie dla algorytmu obliczeniowego

Wyniki implementacji

- Implementacja systemu w języku C
- Biblioteka krzywych eliptycznych oparta na MIRACL
- Obliczenia przeprowadzono:
  - Sieć lokalna (Windows i Unix / Socket i MPI).
  - Internet (Windows i Linux / Socket).
  - Klaster w ICM (Linux / MPI)

Heterogeniczny system obliczeniowy



Cel

Certicom ECC Challenge

http://www.certicom.com

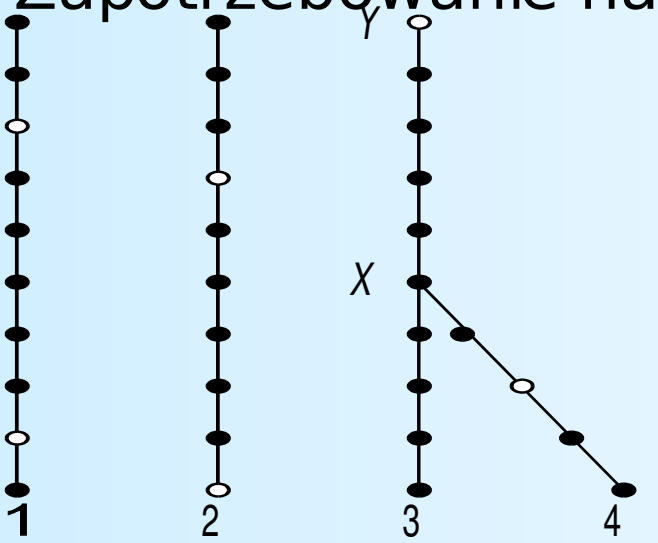
10 lat temu krzywą ECC2-89 złamano za pośrednictwem 70 komputerów w ok. 16 dni

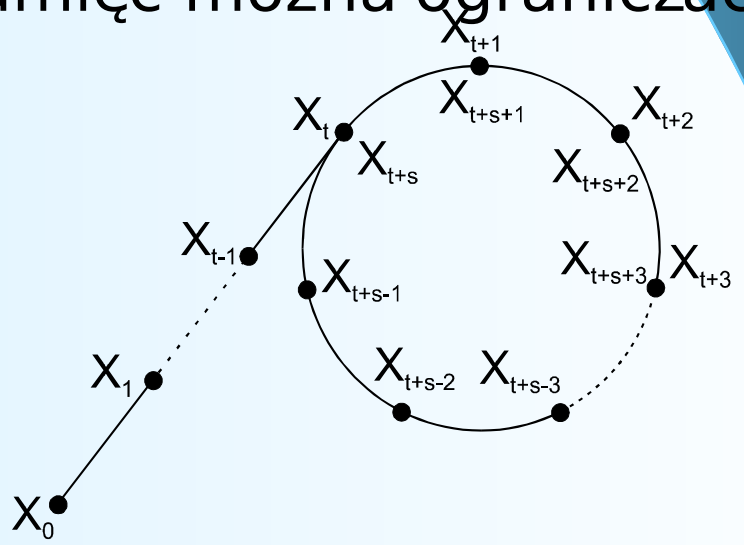
Dlaczego krzywe eliptyczne?

- Obecnie najpoważniejszy konkurent dla RSA
- Mniejsza długość klucza przy tym samym poziomie bezpieczeństwa
- Nowy standard, coraz więcej zastosowań
- Rekomendowane do stosowania w kartach EMV
- Istnieją odpowiedniki tradycyjnych technik kryptograficznych operujące na krzywych eliptycznych np. wymiana kluczy Diffie-Hellmana, szyfrowanie ElGamala

Algorytm rho Pollarda

- Najlepszy znany obecnie algorytm rozwiązywania ECDLP
- Algorytm probabilistyczny oparty na błądzeniu przypadkowym
- Istnieje wersja równoległa
- Zapotrzebowanie na pamięć można ograniczać



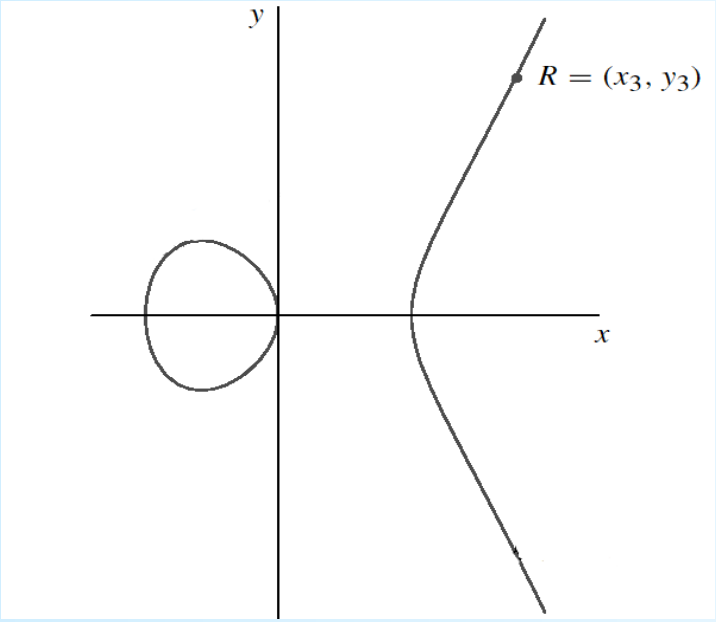


Krzywe eliptyczne nad $GF(2^n)$

Krzywa eliptyczna *E* nad ciałem ***GF(2ⁿ)*** jest zdefiniowana przez następujące równanie:

$$y^2 + xy = x^3 + ax^2 + b$$

gdzie $a,b \in$ ***GF(2ⁿ)***.



Ciało *GF(2ⁿ)* – ang. *Galois Field* - elementami ciała są binarne, *n* wymiarowe wektory współrzędnych w ustalonej bazie.

Bazy

Baza potęgowa

$$(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \ldots, \alpha^{n-1})$$

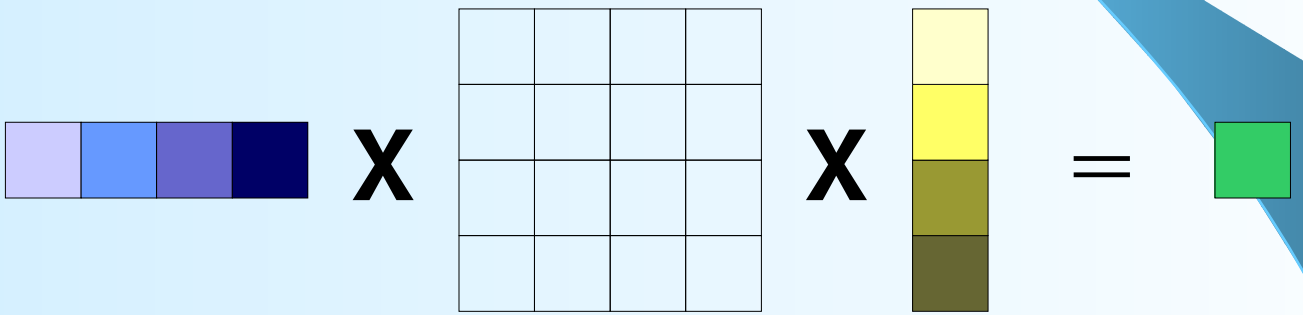
Baza normalna

$$(1, \beta, \beta^2, \beta^4, \beta^8, \ldots, \beta^{2^{n-1}})$$

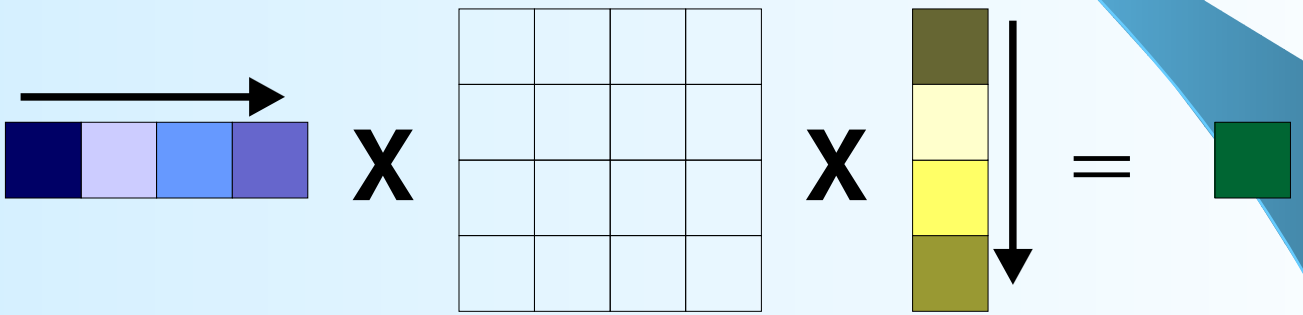
Operacje w ONB

- Dodawanie → XOR po wszystkich współrzędnych
- Podnoszenie do kwadratu → Cykliczna rotacja
- Mnożenie → Za pomocą macierzy mnożenia

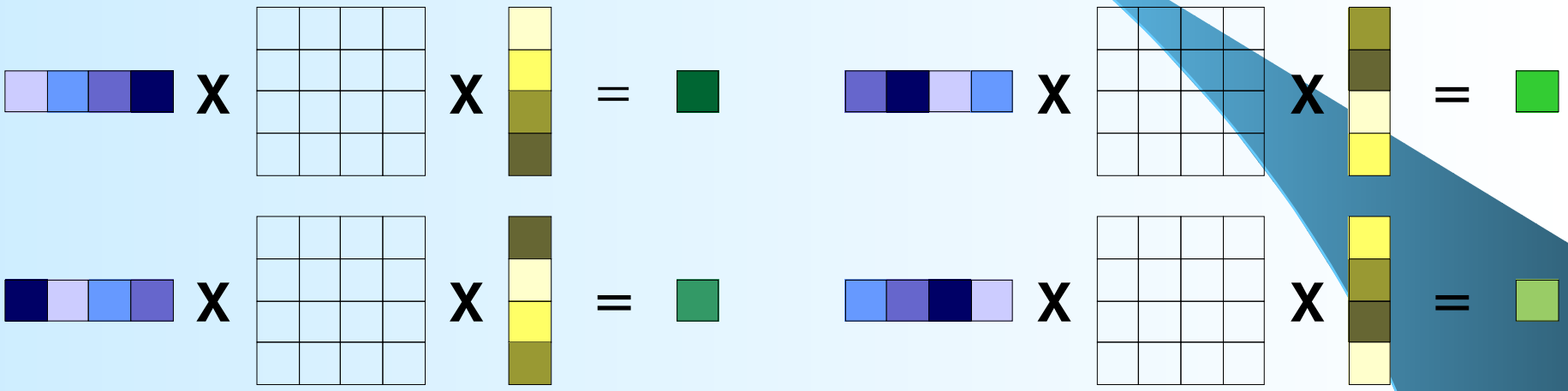
Mnożenie w ONB



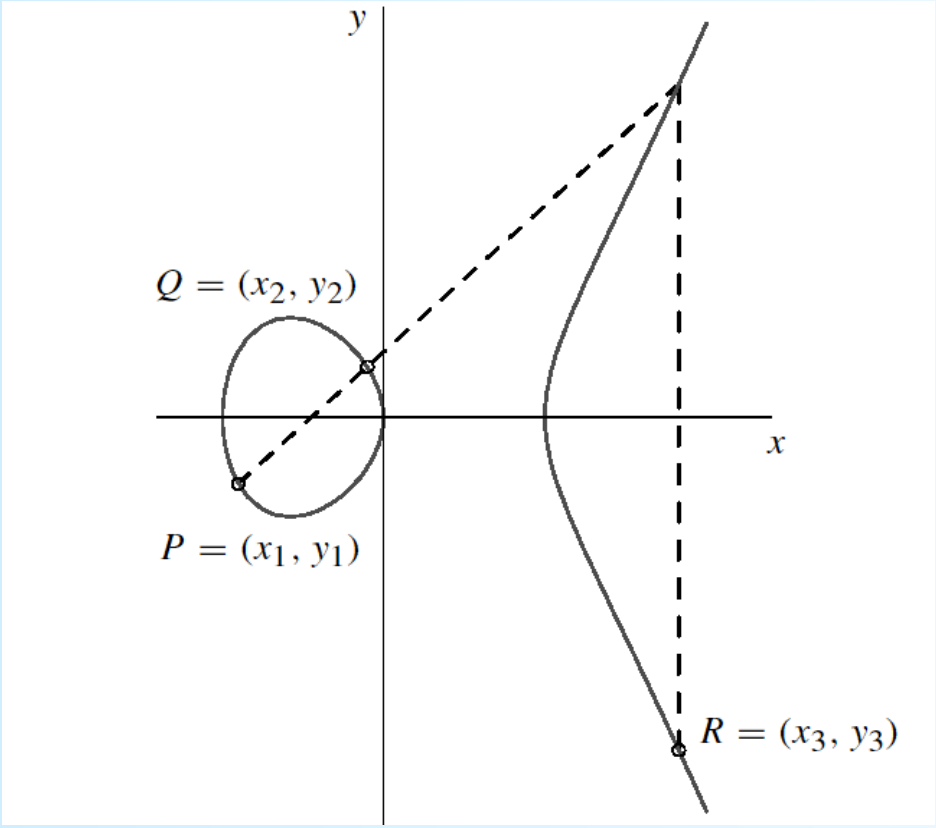
Mnożenie w ONB architektura szeregowa



Mnożenie w ONB architektura równoległa

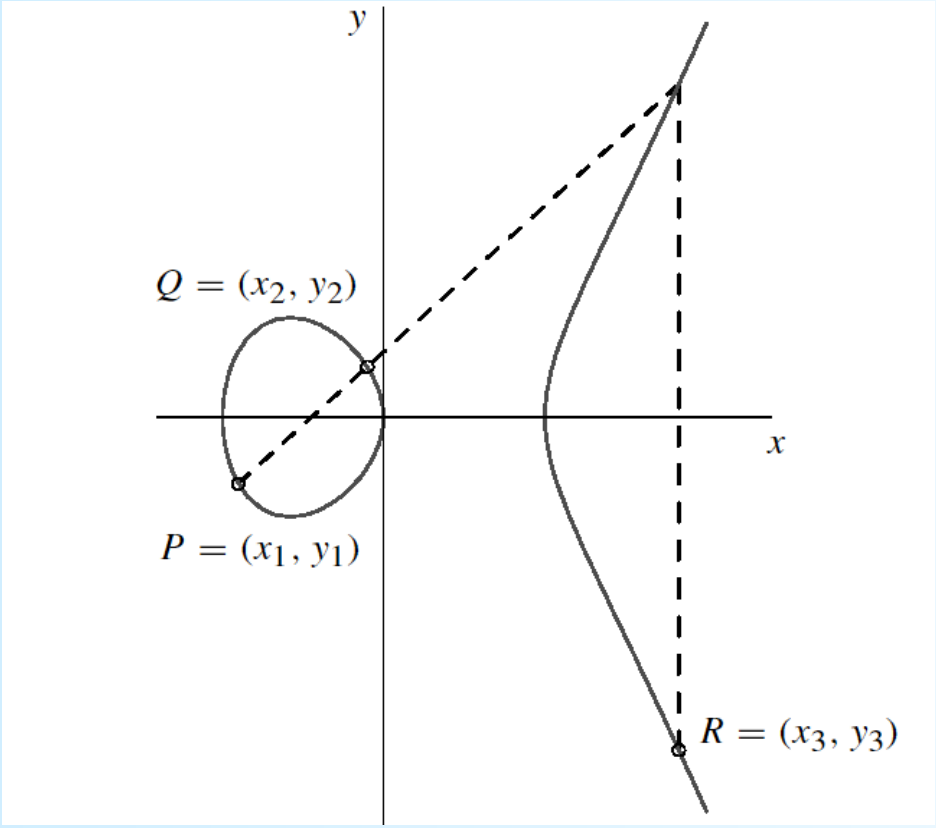


Dodawanie punktów na krzywej eliptycznej



$$
\begin{aligned}
U_0 &= X_0 \cdot Z_1^2 \\
S_0 &= Y_0 \cdot Z_1^3 \\
U_1 &= X_1 \cdot Z_0^2 \\
W &= U_0 + U_1 \\
S_1 &= Y_1 \cdot Z_0^3 \\
R &= S_0 + S_1 \\
L &= Z_0 \cdot W \\
V &= R \cdot X_1 + L \cdot Y_1 \\
Z_2 &= L \cdot Z_1 \\
T &= R + Z_2 \\
X_2 &= a \cdot Z_2^2 + T \cdot R + W^3 \\
Y_2 &= T \cdot X_2 + V \cdot L^2
\end{aligned}
$$

Dodawanie punktów na krzywej eliptycznej



$$U_0 = X_0 \cdot Z_1^2$$
$$S_0 = Y_0 \cdot Z_1^3$$
$$U_1 = X_1 \cdot Z_0^2$$
$$W = U_0 + U_1$$
$$S_1 = Y_1 \cdot Z_0^3$$
$$R = S_0 + S_1$$
$$L = Z_0 \cdot W$$
$$V = R \cdot X_1 + L \cdot Y_1$$
$$Z_2 = L \cdot Z_1$$
$$T = R + Z_2$$
$$X_2 = a \cdot Z_2^2 + T \cdot R + W^3$$
$$Y_2 = T \cdot X_2 + V \cdot L^2$$

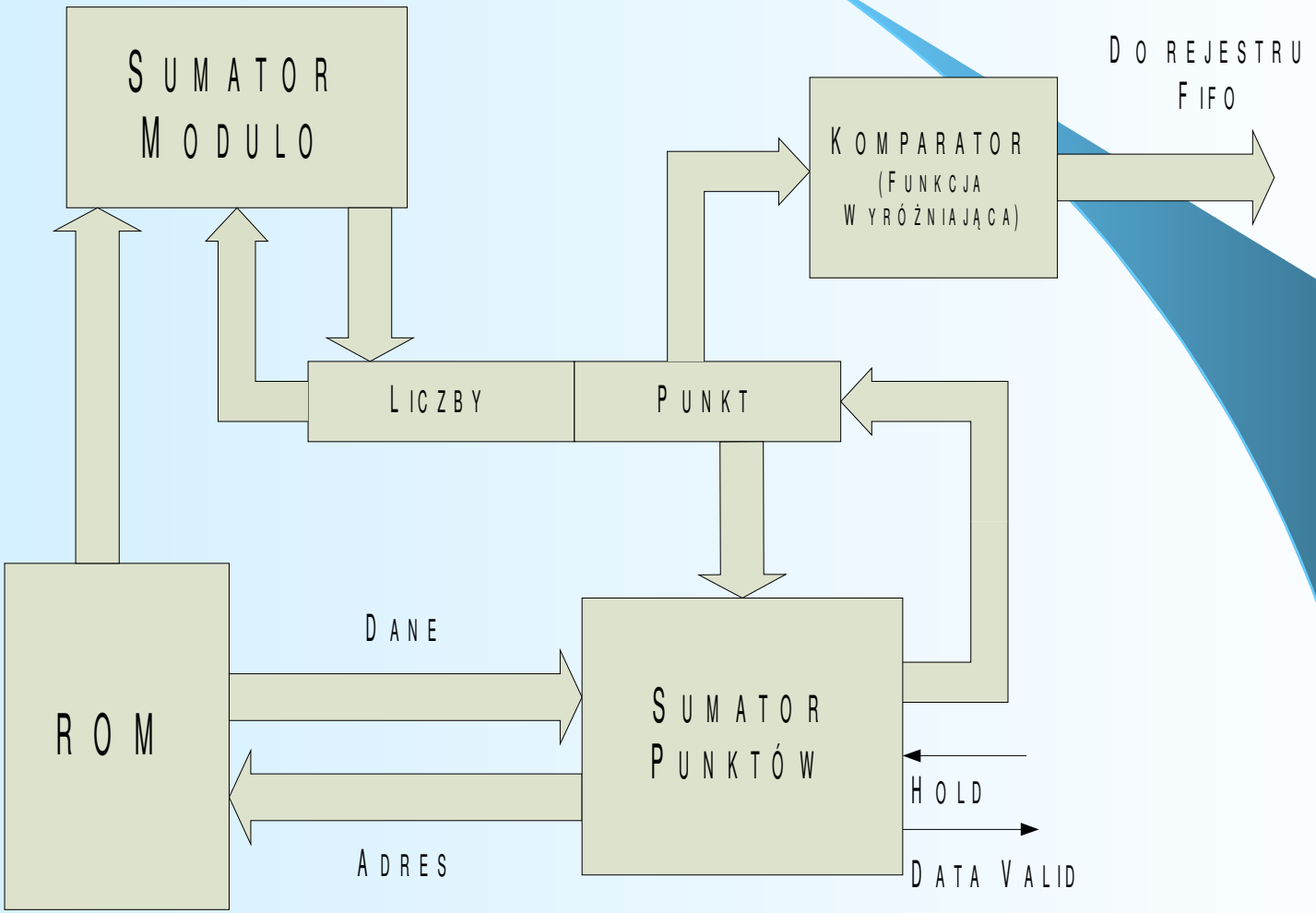
Algorytm Rho

INPUT: punkt $P \in E(F_q)$, o rzędzie n oraz punkt $Q \in \langle P \rangle$

OUTPUT: logarytm dyskretny $l = \log_P(Q)$

1. Wybierz ilość gałęzi L
2. Zdefiniuj funkcję pozycjonującą $H(X)$
3. Zdefiniuj kryterium wyróżnialności punktów
4. Od $j=1$ do L wykonuj
   a. Wybierz losowo $a_j, b_j \in (0, n-1)$
   b. Oblicz $R_j = a_j P + b_j Q$
5. Każdy z procesorów wykonuje
   a. Wybierz losowo c' oraz d' z $[0, n-1]$ i oblicz $X' = c'P + d'Q$
   b. Wykonuj
      i. Jeśli X spełnia warunek wyróżnienia to wyślij trójkę (c, d, X) do serwera
      ii. Oblicz $j = H(X')$
      iii. $X \leftarrow X + R_j$
      iv. $c \leftarrow c + a_j \pmod n, \quad d \leftarrow d + b_j \pmod n$
   c. Tak długo aż serwer nie znajdzie tego samego wyróżnionego punktu ponownie
6. Serwer sprawdza czy $d' = d''$ i w wypadku powodzenia zwraca „**Błąd**”
7. W przeciwnym wypadku oblicza i zwraca $l = (c' - c'')(d'' - d')^{-1} \pmod n$

Układ HardRho



Wyniki implementacji

Układ EP2S60F1020C4 z rodziny Stratix II (Altera)

Wykorzystane komórki logiczne:		
	9216	27593
Całkowite zużycie zasobów:		
	20%	58%
Czestotliwość zegara:		
	138 MHz	116 MHz
Efektywność obliczeń:		
	12.5 mln iter/sec	31,6 mln iter/sec

Porównanie z Certicom

Stacja Alpha 500 Mhz => 187 tysięcy iter/sec

Hard Rho 116 MHz => 31600 tysięcy iter/sec

Stosunek: HardRho/Alpha = 169

Szacowana długość obliczeń to około 8 dni.

Plany na przyszłość

- Prace na zwielokrotnieniem
- Przeprowadzenie obliczeń
- Podłączenie układów FPGA do Systemu Rozproszonych Obliczeń

RUC 2007

Realizacja jednostki wspomagającej kryptoanalizę szyfrów opartych na krzywych eliptycznych w strukturach reprogramowalnych

ENIGMA 2007

System sprzętowo - programowy do rozproszonej kryptoanalizy szyfrów opartych na krzywych eliptycznych

Piotr Majkowski, Tomasz Wojciechowski, Maciej Wojtyński, Mariusz Rawski

Dziękuję za uwagę