Kryptologia Bankowa

Spis Treści

1. Grupowe struktury dwuliniowe

1.1 Grupowe struktury dwuliniowe

G_1, G_2 - grupy skończone cykliczne o rzędzie będącym zadanym liczbą pierwszą

Działanie dwuliniowe (iloczyn)
$e: G_1 \times G_2 \to G_2$ spełniający warunki: $G_1 = (G_1, +)$ $G_2 = (G_2, *)$
1)dwuliniowość $e(aP, bP) = e(P, Q)^{ab}$ $a, b \in \mathbb{Z}$ $P, Q \in G_1$
2)nietrywialność(nie zdegenerowalność) to oznacza, że $e(G_1 \times G_1) \neq (\mathbf{1}_{G_2})$, gdzie **1** oznacza element neutralny grupy multiplikatywnej.
3)obliczalność

$\forall P, Q \in G_1$ istnieje efektywny obliczeniowo algorytm pozwalający obliczyć $e(P, Q)$

Wniosek 1

Jeśli P jest generatorem G_1 to element $e(P, P)$ jest generatorem G_2

Dowód

Każdy element G_1 jest postaci aP . Zatem niech Q, R takie punkty G_2 , że $e(Q, R) \neq (\mathbf{1}_{G_2})$, $e(P, P)^{ab} \neq (\mathbf{1}_{G_2}) \Rightarrow e(P, P) \neq (\mathbf{1}_{G_2})$. Zatem $e(P, P)$ - generuje nietrywialną podgrupę w G_2 rzędu dzielącego liczbę pierwszą P. Zatem jest całą grupą G_2 .

Trójkę (G_1, G_2, e) nazywamy strukturą z działaniem dwuliniowym

Protokół Difiego-Helmana

$P, Q \in G_1$ punkty znane publicznie

A → B
aP - publ. bP – publ.

aQ – prywatne bQ – prywante
a,b – losowe

Każda strona oblicza wspólny klucz wymiany obliczając
$e(bP, aQ)=e(aP, bQ)$
$e(P, Q)^{ba}=e(P, Q)^{ab}=k_{AB}$ - klucz wymiany

Analiza złożoności protokołu

Niech T – operacja transmisji, O – operacja obliczeniowa
Złożoność protokołu D-H dla struktury dwuliniowej wynosi 2T + 6O
Teraz możemy wykorzystać klucz $k_{AB}=e(P, Q)^{a, b}$ do szyfrowania i deszyfrowania wiadomości "m" co daje łącznie 3T +8O operacji

1.2 System "szyfrowanie ze wskazówką" (odpowiada kryptosystemowi ElGamala)

A "m" B
rP - publ. bP – publ.
rQ – prywatne bQ – prywante
(2O+1T)
r – losowe

1. $[e(bP, rQ)\cdot m, rP]$ – otrzymuje dzieląc pierwszą współrzędną przekazu przez $e(rP, bQ)$ - koszt 4O+1T + 2O
B – oblicza $e(rP, bQ)$
Łączny koszt to 8O +2T

1.3 Podpis cyfrowy w strukturze dwuliniowej

A B
aP - publ. rP – publ.
aQ – prywatne rQ – prywante
r – losowe

Podpis $\sigma a, r(m)=[(mr+a), rP]$
$[m, \sigma_{a, r}(m)]\rightarrow B$

Weryfikacja

Strona B sprawdza czy : $e((mr+a)Q, P)=e(mQ, rP)\cdot e(Q, aP)$

Poprawność wynika z własności iloczynu

Uzasadnienie

Iloczyn ma własność $e(P+Q,R)=e(P,R)e(Q,R)$ bo
$e(mrQ,P)\cdot e(aQ,P)=e(Q,P)^{mr}\cdot e(Q,P)^{a}=e(mQ,rP)\cdot e(Q,aP)$ ckd

1.4 System szyfrowania oparty na identyfikacji
1.4.1 Podpis Schnorra w strukturze dwuliniowej

A “m” **B**
składa podpis → weryfikuje podpis

Podpisywanie wiadomości “m” (wybieramy losowe *r* i obliczamy)
$\sigma_{r,a}(m)=[r+ah,rP]$ gdzie $h=h(m,mP)$ jest publicznie znaną funkcją haszującą.

Weryfikacja polega na sprawdzeniu czy zachodzi równość:
(*) $e((r+ah)Q,P)=e(Q,rP)e(Q,r\,aP)^{h}$

Poprawność: jeśli podpis przebiega prawidłowo to weryfikacja powiedzie się.

Sprawdzamy (*)
Na mocy własności dzielenia (dwuliniowości) mamy:
$lewa=\langle(r+ah)Q,P\rangle=\langle rQ,P\rangle\langle ahQ,P\rangle=\langle a,rP\rangle\langle Q,P\rangle^{ah}=\langle Q,rP\rangle\langle Q,aP\rangle^{h}=prawa$

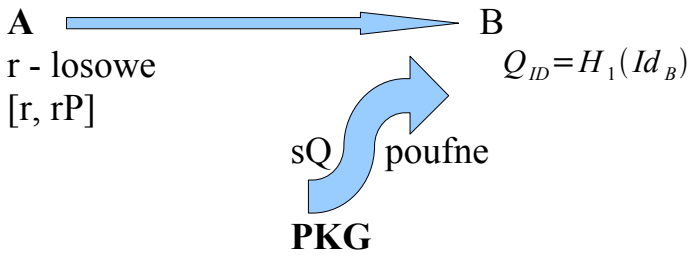
Bezpieczeństwo podpisu $\sigma_{r,a}(m)$ sprowadza się odpowiednio do trudności obliczenia wartości $a\,lub\,r$, mając dane punkty $aP\,lub\,rP$ na krzywej eliptycznej – jest to problem logarytmu dyskretnego w grupie punktów wymiernych na krzywej eliptycznej $E(K)$, gdzie *K* – ciało skończone.

1.4.2 Schemat szyfrowania opartego na identyfikacji:

A → B
$m\to m\circ k$ $k=k(Id_B)$

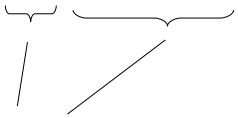
PKG (private key generator)
dostarcza klucz deszyfrujący $m\circ k$

E – publicznie znana krzywa
P, Q – zadane punkty na E
H_1, H_2 – publicznie znane funkcje haszujące



sQ – klucz deszyfrujący dla *B*
sD – klucz publiczny dla *B*
s – master key

Szyfrogram wiadomości "m" generowany przez *A* jest parą:
$c=[rP, m\oplus H_2(g_{ID}^r)]$ gdzie $g_{ID}=\langle Q_{ID}, sP\rangle$; $\oplus$ - dodawanie mod 2



c = [X, Y]
Odbiorca używający kluczy sQ oraz $c=[X, Y]$, najpierw oblicza $H_2(g_{ID}^r)$ potem dodaje $H_2(t)\,Y=m\oplus H_2\oplus H_2=m$.
Wystarczy pokazać, że *R* może obliczyć g_{ID} , mianowicie $g_{ID}^r=\langle Q_{ID}, sP\rangle^r=\langle sQ_{ID}, rP\rangle$ co kończy wnioskowanie.

2. Problemy obliczeniowe w strukturze dwuliniowej

Struktura (grupowa) dwuliniowa (G_1, G_2, e) , $e: G_1 \times G_1 \to G_2$,
$ord\, G_1 = ord\, G_2 = q$ q – liczba pierwsza.

Problemy:

1) Problem logarytmu dyskretnego DLG (ang. Discrete Logarithm Problem)
2) Problem obliczeniowy Diffie-Hellmana CDH (ang. Computational Diffie-Hellman Problem)
3) Problem decyzyjny Diffie-Hellmana DDH (ang. Decisional Diffie-Hellman Problem)

Założenia

1) Problem DDL w G_2 jest trudny
2) Problem CDH w G_1 jest trudny

Problemy CDH w G_1 :
Dane $[P, aP, bP]$, obliczyć Q = abP
Problemy CDH w G_2 :
Dane $[g, g^a, g^b]$, obliczyć g^{ab}
Problem DDH w G_2 :
Czy czwórka $[g, g^a, g^b, g^c]$ jest czwórka Diffiego – Hellmana
tzn. taką, że $g^c = g^{ab}$
Problem DDH w G_1 :
Czy czwórka $[P, aP, bP, cP]$ jest czwórką Diffiego – Hellmana
tzn. taką, że $abP = cP$

Twierdzenie

Redukcja MOV (Menezes, Okamoto, Vanstone)
Niech (G_1, G_2, e) - struktura dwuliniowa. Wtedy problem DLG w G_1 nie jest trudniejszy niż problem DLG w G_2

Dowód

Niech $P, Q \in G_1$. Szukamy $a: aP = Q$.
Niech $g = e(P, P)$, $h = e(P, Q)$. P,a – generatory G_2 . Pokażemy, że rozwiązując problem DLG w G_2 , rozwiązujemy DLG w G_1 .
Dane :

$g, h \in G_2$

Znajdź :

$\alpha : g^{\alpha} = h$

Niech α będzie rozwiązaniem tego problemu w G_2 tzn. $g^{\alpha} = h$.

Zauważmy, że $a = \alpha$ jest rozwiązaniem problemu DLG w G_1 , bo jeśli $Q = \alpha P$ to $h = e(P, \alpha P) = e(P, P)^{\alpha} = g^{\alpha}$, cnd.

2.1 Problem jednokierunkowości

Twierdzenie 2

Odwzorowania $\psi_Q : G_1 \to G_2$ zadane wzorem:

$\psi_Q(P) = e(P, Q)$ jest homomorfizmem jednokierunkowym o ile problem DDH w G_2 jest trudny.

Dowód

Załóżmy, że "odwróciliśmy" $\psi_Q(P)$ tzn. Mając dany iloczyn e(P, Q) możemy wyznaczyć P. Pokażemy, że wtedy DDH w G_2 jest łatwy. Zauważmy, że DDH w G_1 jest łatwy bo dla stwierdzenia czy czwórka $[P, aP, bP, cP]$ jest właściwą czwórką D-H wystarczy sprawdzić czy $e(P, cP) = e(aP, bP) = e(P, P)^c = e(P, P)^{ab}$.

Niech (g, g^a, g^b, g^c) będzie dane. Mamy stwierdzić czy jest to czwórka D-H w G_2 wiadomo, że jeśli g-generator G_1 to $e(P, bP) = g^c = e(P, cP)$. Korzystając z założenia można obliczyć aP, bP, cP . Jeśli $[P, aP, bP, cP]$ jest czwórką D-H w G_1 to stwierdzić można, że $[g, g^a, g^b, g^c]$ jest właściwą czwórką D-H w G_2 .

A zatem rozwiązanie problemu DDH w G_2 jest niemożliwe bo założyliśmy, że jest on trudny. A zatem ψ jest jednokierunkowe c.k.d.

Problem BDH (dwuliniowy Diffie-Hellman)

Niech P – generator w G_1 rzędu q

Dane: $[P, aP, bP, cP] gdzie a, b, c \in \boldsymbol{Z}_q$

Obliczyć: $e(P, P)^{abc}$

Algorytm *A* ma przewagę ε w rozwiązaniu problemu BDH jeśli $Pr[A(P, aP, bP, cP) = e(P, P)^{abc}] \geq \varepsilon$ gdzie prawodopodobieństwo jest wyznaczane po "losowych" wyborach $a, b, c \in \boldsymbol{Z}_q$ i losowych bitach algorytmu *A*.

Generatorem parametrów (IG) dla struktury $(G_{1,} G_{2,} e)$ nazywamy algorytm zrandomizowany spełniający warunki:

1. Na wyjściu dane $k \in N$
2. (IG) działa w czasie $O(k^c)$
3. (IG) daje na wyjściu strukturę $(G_{1,} G_{2,} e)$ taką, że $|G_i|=q$ dla i = 1, 2. oznacza ze generator parametrów ma na wyjściu parametr bezpieczeństwa złożony z k jedynek. $IG(1^k)$

Definicja

(IG) spełnia założenia BDH jeśli dowolny zrandomizowany i działający w czasie wielomianowym (od k) algorytm *A* rozwiązuje problem BDH z przewagą co najwyżej 1/f(k) dla dowolnego wielomianu f.

3. Iloczyn WEILA

Definicja 1

Niech $E=E/\bar{K}$ ($\bar{K}$ – algebraicznie domknięte ciało)
Wtedy $E[n]=\{P\in E: nP=\theta\}$ nazywamy grupą punktów n-torsyjnych na krzywej $E/\bar{K}$ (θ punkt neutralny w grupie).
Dalej zakładamy, że $e: E[n]\times E[n]\rightarrow(\bar{K})^*$

Definicja 2

Iloczynem Weila nazywamy działanie dwuliniowe trywialne na przekątnej tzn. spełniające warunek : $e(P,P)=1$ dla dowolnego $P\in E(n)$.

Twierdzenie 1

Niech $e: H\times H\rightarrow G$ będzie nietrywialnym działaniem dwuliniowym takim, że $e(P,P)=1$ dla dowolnego $P\in H$ oraz niech $\phi: H\times H\rightarrow G$ – homomorfizm taki, że grupa $<P,\phi(P)>$ generowana przez P i $\phi(P)$ jest równa H . Wtedy odwzorowanie $\hat{e}=H\times H\rightarrow G$ określone następująco: $\hat{e}(P,Q)=e(P,\phi(Q))$ jest działaniem dwuliniowym nietrywialnym na przekątnej.

Dowód

Niech $Q\in H$ takie, że $(P,Q)\neq 1$ Ponieważ $<P,\Phi(P)>=H$ to $Q=aP+b\phi(P)$. Zatem $1\neq e(P,Q)=e(P,aP+b\phi(P))=e(P,P)^a e(P,\phi(P))^b$ $=e(P,\phi(P))^b$ c.k.d.

Przypomnienie

Niech $E/K\simeq Div^0(E)/Prin(E)$. Zatem, każdy punkt P na krzywej E będziemy identyfikować z dywizorem (P) > (Q) stopnia 0 z dokładnością do dywizorów głównych. Co więcej $A=\sum a_P(P)$ jest dywizorem głównym, wtedy i tylko tedy gdy :

$$\begin{cases}\sum a_P=0 \ oraz\\ \sum a_P P=\theta\end{cases}$$

w sensie struktury grupowej na *E*. Dywizor główny nazywamy często - dywizorem funkcji i oznaczamy $(f)=\sum ord_P f(P)$

3.1 Dywizory funkcji liniowych

Niech l: ax + by + c = 0 i niech P, Q, R będą punktami przecięcia krzywej *E* z

prostą l, wtedy $Div(l)=(P)+(Q)+(\overline{P+Q})-3(\theta)$
Jeśli $b=0$ to $l: x+c=0$ wtedy dywizor $Div(l^*)=(P)+(\bar{P})-2(\theta)$

Definicja

Jeśli f jest funkcja na krzywej E oraz $A=\sum a_P(P)$ jest dywizorem to
$f(A)=\prod_{P\in A} f(P)^{a_P}$

Przykład:

$f(x,y)=x-x_R$
$A=(P)-(Q)$
$f(A)=(x_P-x_R)^1\cdot(x_Q-x_R)^{-1}=\frac{x_P-x_R}{x_Q-x_R}$
$f((P)-(Q))=f(P)\cdot f(Q)^{-1}=\frac{f(P)}{f(Q)}$

Definicja

Iloczynem Weila $e: E[n]\times E[n]\to(\bar{K})^*$ nazywamy przekształcenie zadane wzorem:

$e_n=(P,Q)=\frac{f_p{}^n(A_Q)}{f_Q{}^n(A_Q)}$, gdzie $(f_p^n)\sim n(P)-n(\theta)\quad A_Q\sim(Q)-(\theta)$

$(f_Q^n)\sim n(Q)-n(\theta)\quad A_P\sim(P)-(\theta)$

Wnioski

Wartość $e_n(P,Q)$ nie zależy od wyboru reprezentantów klas dywizorów modulo dywizory główne.

Dowód

Niech $\tilde{A}_P$ będzie dywizorem równoważnym A_P *tzn.* $\tilde{A}_P=A_P+(g)$
g – funkcja wymierna na krzywej E oraz $\tilde{f_P}{}^n=f_P{}^n\cdot g^n$ bo
$\mathrm{div}(f_P{}^n\cdot g^n)=\mathrm{div}\, f_P{}^n+n(\mathrm{div})g$ oraz $\tilde{A}_P\sim(P)-(\theta)+(g)$ (bo
$(\tilde{f_P}{}^n)\sim n\tilde{A}_P\sim n[(P)-(\theta)+g]=n(P)-n(\theta)+n(g)=(f_P{}^n)+(g^n)$).

Zatem mamy :

$$e_n(P,Q)=\frac{f_P{}^n(\tilde{A}_Q)}{f_Q{}^n(\tilde{A}_P)}=\frac{f_P(A_Q)g(A_Q)^n}{f_Q(A_P)f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}\cdot\frac{g(nA_Q)}{f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}\cdot\frac{g(f_Q{}^n)}{f_Q(g)}=\frac{f_P(A_Q)}{f_Q(A_P)}$$

ostatnia równość zachodzi na mocy wzoru wzajemności $f((g))=g((f))$

Lemat

Istnieje efektywny algorytm D , który dla danych wejściowych $f_b(A_Q), f_c(A_q)$ oraz $bP, cP, (b+c)P \ (b, c \in N)$ oblicza wartość $f_{b+c}(A_Q)$ gdzie $f_a \quad a \in \{b, c, b+c\}$ jest funkcją wymierną której dywizor jest równoważny dywizorowi.

$A_Q = a(P+R_1) - a(R_1) - (aP) + (\Theta)$

Dowód

Zdefiniujemy dwie funkcje liniowe g_1, g_2 na krzywej E

$g_1 : (g_1) = (bP) + (cP) + (\overline{(b+c)P}) - 3(\Theta)$

$g_2 : (g_2) = ((b+c)P + \overline{(b+c)P}) - 2(\Theta)$

Zatem g_1 jest prostą przechodzącą przez punkty $bP, cP.$ Jeżli $b = c$ to g_1 jest styczną do krzywej E w punkcie bP. Niech $g_1(x, y) = a_1 x + b_1 y + c_1$. Dalej g_2 jest prostą pionować przechodzącą przez punkt $(b+c)P$. Niech $g_2(x, y) = x + c_2$.

Zdefinicji mamy, że

$A_b = b(P+R_1) - b(R_1) - (bP) + (\Theta)$

$A_c = c(P+R_1) - c(R_1) - (cP) + (\Theta)$

$A_{c+b} = (b+c)(P+R_1) - (b+c)(P+R_1) - [(b+c)(P+R_1)] + (\Theta)$

Zatem otrzymujemy, że $A_{c+b} = A_b + A_c + g_1 - g_2$ skąd

$f_{b+c}(A_Q) = f_b(A_Q) + f_c(A_Q) + g_1 - g_2$

Wniosek

Jeśli p jest punktem n-torsyjnym , to dywizory funkcji $f_n \ i \ f_P^n$ są równoważne.

Dowód

$(f_p^n) \sim n A_P \sim n(P) - n(\Theta)$. Z definicji A_n wiemy, że (f_n) jest dywizorem równoważnym $A_n \sim n(P+R_1) - n(P_1) - (nP) + \Theta$, który jest równoważny dywizorowi $n(P) - n(\Theta)$.

Wniosek 2

Dla rekurencyjnego obliczenia f_{b+c} rozpoczniemy do obliczenia f_1 takiego,że $(f_1) = (P+R_1) - (R_1) - (P) + \Theta$; taka funkcja jest ilorazem funkcji $g_2`(x, y) / g_1`(x, y)$ gdzie $g_2`(x, y)$ jest prostą pionową przchodzącą przez $(P+R_1)$ natomiast $g_1`(x, y)$ jest prostą przechodzącą przez punkty $P \ i \ R_1$.

Wniosek 3

Obliczanie iloczynu Weil`a $e_n(P,Q)$ wykonuje się w czasie $O(\log^c n)$ gdzie *c* jest pewną stałą dodatnią.

4. Testy Pierwszosci

1)Szybkość

-wielomianiowe, czas działania $\Theta(g|n|)$ g-pewny wielomian

-podwykładnicze (Adleman, Rumely, Pomerance) czas działania $\Theta(\exp\frac{|n|}{f|n|})$

-wykładnicze (Eratostenes), czas działania $\Theta(n^{\frac{1}{2}+\epsilon})$

Aspekt praktyczny

Nieefektywność stałej w oznaczeniu $\Theta(.)$ może powodować, że test podwykładniczy jest w praktyce bardziej wydajny niż wielomianowy (np. testy AKS, APR)

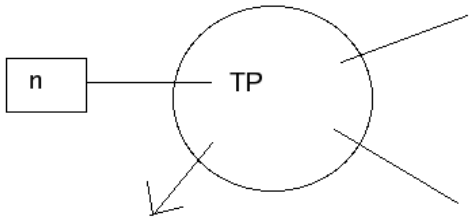
2) Ogólność

-testy specyficzne , działają efektywnie dla danych wejściowych specjalnej postaci np. Dla liczb "n" postaci $n=2^m-1$ *lub* $n=2^{2^n}+1$. Liczby pierwsze tej postaci to odpowiednio liczy pierwsze Mersenne`a i Fermata

-testy uniwersalne, działają dobrze na dowolnych danych (np. AKS, APR)

3)Pewność

Potrafimy podać dowód pierwszości (złożoność danej częsci)



pierwsze
Testy Millera-Rabina
Test Lehmana

złożone
Fellowsa – Koblitza (deterministyczny)

<u>Wniosek</u>

Najlepsze testy to takie, które spełniaja wszystkie trzy warunki.

<u>Testy warunkowe lub hipotetyczne</u>

Działają szybko jeśli spełnione są pewne warunki.

<u>Przykład 1</u>

Test Fellowsa – Koblitza działa szybki jeśli znamy rozkład n-1 na czynniki pierwsze.

Przykład 2

Testy Soloray'a Strassena działa szybko jeśli prawdziwa jest uogólniona hipoteza Riemanna

Schemat(testu pierwszości)

Załóżmy , że potrafimy udowodnić twierdzenie typu : Jeśli n jest liczbą pierwszą to … Wtedy druga część implikacji (teza) może być traktowana jako warunek konieczny pierwszości.

Przykład

Jeśli n- pierwsze $|Z_n^*| = n-1$

$\forall\, a \perp n \qquad a^{n-1} = 1 (mod\ n)$

Taki test nazywamy testem Fermata. Jest szybki , ogólny ale nie poprawny bo nie można dowieść , że liczba po przejściu przez test jest pierwsza.

KONTRPRZYKŁAD (z ustalonym świadkiem a = 4)

Mamy $4^{14} = 1$ (mod n)

KONTRPRZYKŁAD (dla dowolnego świadka „ a ”)

$a^{560} = 1 (mod\ 561)$

Definicja.

Liczbę n nazywamy pseudopierwszą przy podstawie „ a ” jeśli jest złożona i zachodzi warunek Fermata ze świadkiem a .

Definicja

Liczbę złożoną , która przechodzi pomyślnie test Fermata dla wszystkich świadków $a \in (\ Z_n^*$)nazywamy liczbą Carmichaela .

Twierdzenie (Heath - Brown 1980’s)

{ n x : n jest liczbą Carmichaela } x $2/7$

Testy propabilistyczne (warunek pewności osłabiony)

Twierdzenie

Niech n ∈ P i niech r-1=2^R S ,gdzie S jest nieparzyste.
Wtedy dla każdego a ∈ zachodzą warunki :

1.) $a^{n-1} = 1 \,(mod\, n)$

2.) $a^S = 1 \,(mod\, n)$ lub istnieje takie 0r < R ,że a $a^{2^r S}$ = -1 (mod n)

Dowód

Warunek 1) wynika z twierdzenia Fermata. Dla dowodu drugiego zauważmy że pierwszość n pociąga za sobą , że

$$a^{\frac{n-1}{2}} = a^{2^{R-1}S} = \pm 1 (\mathrm{mod}\, n)$$

Zatem w ciągu potęg $a^{2^r S}$ modulo n r =R-1,R-2,..0 albo będzie potęga dająca resztę -1 modulo n albo $a^S = 1 \,(mod\, n)$ co dowodzi tezy.
Na powyższych argumentach oparty jest następujący algorytm (Test pierwszości Millera -Rabina).

Szkic algorytmu

1.) Dla losowo wybranego $a \in Z_n^* (a \neq 1)$

Oblicz $a^{n-1} (mod\, n)$
Jeśli wynik ≠ 1 (mod n) to algorytm daje na wyjściu odpowiedź n∉P.
W przeciwnym razie przechodzimy do drugiego kroku.

2.) Zapisz n-1 = 2^RS , S – nieparzyste.
Jeśli $a^S = 1 \,(mod\, n)$ lub istnieje takie 0≤ r < R ,że a $a^{Z^r S} = -1 \,(mod\, n)$

Algorytm daje na wyjściu odpowiedź n ∈ P.
W przeciwnym przypadku algorytm daje odpowiedź n∉ P.

UWAGA

Z powyższego twierdzenia wynika ,że odpowiedź n∉ P jest pewna.
Natomiast n ∈ P jest obarczona (prawdopodobnym) błędem.
Jak pokazali Miller i Rabin prawdopodobieństwo omyłki nie przekracza jednak 1/4 .
Zatem przy l - iteracjach algorytmu prawdopodobieństwo omyłki jest ⩽¼^l , tzn. mamy :

Wniosek 1

Jeśli *n* przechodzi pomyślnie test Millera-Rabina *l* –razy, to n jest liczbą pierwszą z prawdopodobieństwem $\geqslant 1 - \frac{1}{4}^l$.

Definicja

n -nazywamy liczbą silnie pseudopierwszą przy podstawie $a \Leftrightarrow n$ -złożone i spełnia warunki 1.) i 2.).

4.1 Liczby pseudopierwsze Eulera

Niech *g* –generator Z_P^* , *p* –liczba pierwsza. Wtedy każde $a \in (Z_P^*)$ jest postaci $a = g^x (mod\ p)$
Jeśli *x* jest parzyste to $a \in (Z_P^*)$ nazywamy resztą kwadratową , w przeciwnym przypadku nieresztą kwadratową (mod p).

Łatwo zauważyć, że jest resztą kwadratową równanie $a \in (Z_P^*)$ jest resztą kwadratową (mod p) $\Leftrightarrow$ równanie $a = y^2 (mod\ p)$ ma rozwiązanie .

Wniosek 2

Zbiory reszt i niereszt kwadratowych mają tę samą moc $= \frac{p-1}{2}$.

Definicja

Symbol Legendre'a $\left(\frac{a}{p}\right)$ definiujemy następująco:

Wniosek 3

Jeśli *g* -generator to Z_P^* to
$g^{\frac{p-1}{2}} = -1 (mod\ p)$

Warunek Eulera

$\forall\, a \in Z_P^*$ mamy $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} (mod\ p)$

Dowód

Jeśli *a* -reszta kwadratowa (mod p) to obie strony są równe 1(mod p).
Jeśli *a* -niereszta kwadratowa (mod p) to

$a = g^{2y+1}$ *skąd* $a^{\frac{p-2}{2}} = (g^{p-1})^y g^{\frac{p-1}{2}} = -1 (mod\ p)$ i lewa strona także -1, co należało dowieść.

Definicja

Liczbę *n* nazywamy liczbą pseudopierwszą Eulera przy podstawie $a \Leftrightarrow n$ - złożone i spełnia warunek:

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) (mod\ n)$$

Twierdzenie

(charakterystyka liczb złożonych przechodzących pomyślnie test Millera-Rabina)

Liczba $n \equiv 3 (mod\ 4)$ jest liczbą pseudopierwszą Eulera(przy podstawie *a*)⇔ jest liczbą silnie pseudopierwszą (przy podstawie *a*).

Mamy zatem klasyfikację;

1.) Liczby pseudo-pierwsze przy podstawie a spełniają warunek Fermata :

$$a^{n-1} = 1 (mod\ n)$$

2.) Liczby silnie pseudo-pierwsze spełniają warunek Millera-Rabina : j.w.

3.) Liczby pseudo-pierwsze Eulera spełniają warunek Eulera :

$$a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right) (mod\ n)$$

gdzie left $\left(\frac{a}{n}\right)$ jest symbolem Jacobiego.

Jeśli dla $O(\log^2 n)$ losowych świadectwo $a \in Z_P^*$ przy założeniu hipotezy RIEMANNA możemy wnioskować , że $n \in P$.

Odpowiedni test nazywamy testem SOLOVAYA – STRASSENA.

Powyższy symbol Jacobiego jest uogólnieniem symbolu Legenre'a ,a mianowicie jeśli

$n = P_1^{a_1} P_2^{a_2} \ldots P_r^{a_r}$ (założenie a , n – nieparzyste) to

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{a_1} \ldots \left(\frac{a}{p_r}\right)^{a_r}$$

Dalej jeśli :

$a = q_1^{\beta_1} \ldots q_s^{\beta_s}$ to

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{\beta_1} \ldots \left(\frac{q_s}{p}\right)^{\beta_s}$$

Pozostaje umieć obliczać $\left(\frac{p}{q}\right)$, p i q –liczby pierwsze ,q – nieparzyste

Prawo wzajemności Gaussa pokazuje związek symboli Legendre'a $\left(\frac{p}{q}\right)$ i $\left(\frac{q}{p}\right)$ mianowicie $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{2}}$

Jeśli p=2 to obliczamy $\left(\frac{2}{p}\right)=(-1)^{\frac{(q^2-1)}{2}}$

oraz $\left(\frac{-1}{q}\right)=(-1)^{\frac{(q-1)}{2}}$

Wniosek

Powyższe wzory pozwalają na efektywne obliczenie symbolu Jacobiego i w konsekwencji otrzymujemy wielomianowy, deterministyczny test pierwszości Solovay'a Stressena .

4.2 Algorytm Lehmana

Twierdzenie(kryterium pierwszosci Lehmana – efektywne obliczeniowo):

Liczba $n \in N$ jest pierwsza wtedy i tylko wtedy, gdy zbiór

$$\left\{a^{\frac{n-1}{2}}(\mathrm{mod}\, n), a \in Z_n^*\right\}=\{-1,1\} \qquad (*)$$

Dowód

„⇒" Jeśli *n* jest pierwsze to $a^{n-1}=1(mod\, n)$ na mocy twierdzenia Fermata. Co więcej jest ciałem *n*-elementowym. Więc równanie x^2-1 na tym ciele ma dokładnie dwa rozwiązania: $x=\pm 1(mod\, n)$.

Kładąc $x=a^{\frac{n-1}{2}}$ otrzymujemy, że $x^2=1(mod\, n)$ zatem $a^{\frac{n-1}{2}}\in\{-1,1\}$ dla dowolnego

$$a \in Z_n^* \text{ tzn } \left\{a^{\frac{n-1}{2}},\ a \in Z_n\right\} \in \{-1,\ 1\}$$

Ale mamy, że $1^{\frac{n-1}{2}}=1(mod\, 1)$. Z drugiej strony: ponieważ Z_n^* jest cykliczna to biorąc a równe generatorowi Z_n^* otrzymujemy, że najmniejszy wykładnik *k* taki, że $a^k=1(mod\, n)$ jest równy $n-1$ i wtedy

$a^{\frac{n-1}{2}} \neq 1 \,(mod\, n)$ a więc $1^{\frac{n-1}{2}} = -1 \,(mod\, 1)$.

„⇐" Załóżmy, że $n \in P$, gdzie *P* to zbiór liczb pierwszych.
Pokażmy, że nie zachodzi następująca równość (*)

I) $n \notin n_1 n_2, \quad n_2 \perp n_1, \quad (n_1, n_2 > 1)$
Zakładamy że nie zachodzi (*)
Istnieje $a \in Z_n^*$ takie że $a^{\frac{n-1}{2}} = -1 \,(mod\, 1)$

Niech $b \in Z_n^*$ będzie rozwiązaniem układu konkurencji.

$$b = a \,(\mathrm{mod}\, n_1)$$
$$b = 1 (\mathrm{mod}\, n_2)$$

(także *b* istnieje na mocy twierdzenia chińskiego o resztach gdyż $n_1 \perp n_2$)
Wtedy

$$b^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} = -1 (\mathrm{mod}\, n_1)$$
$$b^{\frac{n-1}{2}} = a^{\frac{n-1}{2}} = 1 (\mathrm{mod}\, n_2)$$

Zatem $b^{\frac{n-1}{2}} \neq \pm 1 \,(mod\, n)$ wbrew założeniu (*)

II) $n = p^a$, *p*-liczba pierwsza
Gdy $n = p^a$ gdzie $a \geq 2$, to w grupie $Z_{p^a}^*$ której rząd równy jest

$$\varphi\left(p^{\alpha}\right) = p^{\alpha-1}(p-1)$$

istnieje element *a* rzędu *p*. Niech będzie tym elementem, wtedy:

$$\left.\begin{array}{l} a^{n-1} = 1 (\mathrm{mod}\, n) \\ a^{p} = 1 (\mathrm{mod}\, n) \end{array}\right\} \text{ ponieważ } p \mid n \text{ więc } \operatorname{rzad} a = 1 \text{ co niemożliwe.}$$

Otrzymana sprzeczność dowodzi implikacji „⇐". c.k.d.

<u>Algorytm Lehmana</u>

Dla losowo wybranych $a_j, j = 1, 2, \ldots, k$ obliczamy $a_j^{\frac{n-1}{2}} (mod\, n)$, wtedy:

1) jeżeli istnieje $j \le k, a_j^{\frac{n-1}{2}} \neq \pm (mod\ n)$ to odpowiedź: $n \notin P$.

2) jeśli $\forall\ j \le k \quad a_j^{\frac{n-1}{2}} = 1 (mod\ n)$ to odpowiedź: $n \notin P$

3) w przeciwnym wypadku odpowiedź: $n \in P$

Odpowiedź 1) jest pewna, odpowiedź 2) z prawdopodobieństwem $\ge 1 - 2^{-k}$, 3) z prawdopodobieństwem $\ge 1 - 2^{-k}$.

4.3 Test pierwszości AKS

Wymyślony w 2002 roku przez Agravala, Keyala i Saxenę.
Algorytm AKS jest algorytmem deterministycznym i działa w czasie wielomianowym(!!!) od rozmiaru liczby.

Lemat 1

Jeśli *n* jest liczbą pierwszą nieparzystą, to
$(x-a)^n = x^n - a (mod\ n)$, gdzie $a \perp n$

Dowód

Dwumian Newtona dla $(x-a)^n$ ma postać:

$$\sum x^k (-a)^{n-k} \binom{n}{k}$$

Z twierdzenia Fermata wynika, że $a^n \equiv a (mod\ n)$. Tylko dwa wyrazy, pierwszy i ostatni są różne od $0 (mod\ n)$. Wszystkie pozostałe są równe $0 (mod\ n)$ bo

$$n \left| \frac{n!}{k!(n-k)!} \right.$$

Lemat 2

Jeśli zachodzi równość, że $(x-a)^n = x^n - a (mod\ n)$ (gdzie *n* jest nieparzyste), to jest *n* liczbą pierwszą.

Dowód

Niech q^k będzie najwyższą potęgą liczby pierwszej *q*, która dzieli *n*.
Jeśli: $n = q^k l$, gdzie $k \ge 1\ i\ l \perp q$,

to wtedy:

$$\binom{n}{q} = \binom{q^k l}{q!(q^k l - q)!} = \frac{(q^k l)(q^k l - 1)\cdot \ldots \cdot (q^k l - q - 1)}{q!} = q^{k-1} l .$$

tylko ten czynnik dzieli się przez q — ten i następne już nie bo q nie dzieli $q - m$

$$\left.\begin{array}{l} q \mid q^k l - (q - m) \\ q \mid q^k l \end{array}\right\} \Rightarrow q \mid (q - m)$$

sprzeczność!!!

$$(x-a)^n - (x^n - a) = \sum_{i=1}^{n-1} \binom{n}{i} (-a)^{n-i} x^i$$

Weźmy teraz $i = q$. Wtedy $\binom{n}{i}$ nie jest wielokrotnością q^k , więc także nie jest wielokrotnością *n*. Zatem różnica $(x-a)^n - (x^n - a) \neq 0 \,(mod\ n)$. Stąd *n* jest liczbą pierwszą (na mocy dowodu nie wprost).

Twierdzenie AKS

Załóżmy że $n \in N$, *q r* są liczbami pierwszymi, gdzie $q | r-1$ oraz spełnione są cztery poniższe założenia:

1) $n^{\frac{r-1}{q}} \,(mod\ r) \notin \{0, 1\}$
2) ***S*** - skończony zbiór liczb całkowitych taki, że
   $\forall\, b \neq b \in S$ zachodzi: $b - b' \perp n$
3) $\binom{q + |S| - 1}{|S|} > n^{2\sqrt{(r)}}$
4) $\forall\, b \in S \quad (x+b)^n = x^n + b \,(mod\ x^r - 1, n)$ tzn.
   $(x+b)^n - x^n + b = f(x)(x^r - 1) + n g(x)$ Gdzie, $f, g \in Z[x]$

Wtedy *n* jest potęgą liczby pierwszej.

Przykład

$n\, g(x) = 0 \,(mod\ n)$

$x^{2r} - 1 = 0 \,(mod\ x^r - 1, n)$, gdyż $x^{r-1} | x^{2r} - 1 = (x^r + 1)(x^r - 1)$

Szkic dowodu twierdzenia AKS.

I. Warunki 1, 2, 3 można traktować jako koszt spełnienia założenia z

lematu 2.

II. Jeśli zachodzi $(x+b)^n=(x^n-b)(mod\ x^r-1,n)$ to zachodzi to także dla liczb *m* w postaci $m=n^i p^j$, gdzie *p* jest dzielnikiem pierwszym liczby *n*, tzn. $(x+b)^m=x^m+b(mod\ x^r-1,n)$ (jest to propagacja równości z warunku 4 na liczby postaci).

a) Bierzemy $m=n^i$. Otrzymamy wtedy $(x+b)^{n^i}=x^{n^i}+b(mod\ x^r-1,n)$

Dla dowodu zauważmy, że:

$$(x+b)^{n^i}=[(x+b)^n]^{n-1}=(x^n+b)^{n^{i-1}}=[(x^n+b)^n]^{n^{i-2}}=(x^{n^2}+b)^{n^{i-2}}=...=$$
$$=(x^{n^i}+b)^0=x^{n^i}+b$$

b) Bierzemy $n=p^j$ tzn. $(x+b)^{p^j}=x^{p^j}+b(mod\ x^r-1,n)$ Zauważmy teraz, że

$(x+b)^n=(x^n+b)(\mathrm{mod}\,x^{r-1},n)$, więc także $(x+b)^n=(x^n+b)(\mathrm{mod}\,x^{r-1},p)$, gdyż $p\mid n$.

Mamy $(x+b)^P=x^P+b^P(mod\ p)=x^P+b(mod\ p)$

Pozostałe współczynniki znikną, gdyż są podzielne przez *p*.

Na mocy twierdzenia Fermata mamy:
Jeśli $b\perp p$, to $b^{p-1}=1(mod\ p)\Rightarrow b^P=b(mod\ p)$
Jeśli $p|b$, to $b^P=b(mod\ p)$, gdyż $p|b^P-b$
Zatem:

$$(x+b)^{p^j}=((x+b)^p)^{p^{j-1}}=(x^p+b)^{p^{j-1}}=[(x^p+b)^p]^{p^{j-2}}=(x^{p^2}+b)^{p^{j-2}}=...=$$
$$=x^{p^j}+b(\mathrm{mod}\,p).$$

Udowodniliśmy więc, że zachodzi $(x+b)^{p^j}=x^{p^j}+b(mod\ x^r-1,n)$

Jest to o słabszy warunek niż $(\mathrm{mod}\,n)$, więc jeśli równanie jest prawdziwe $(\mathrm{mod}\,n)$, to jest też prawdziwe dla $(\mathrm{mod}\,x^r-1,n)$.

Połączenie kroków a) i b).

$$\begin{cases}(x+b)^{n^i}=x^{n^i}+b(\mathrm{mod}\,x^r-1,n)\\(x+b)^{p^j}=x^{p^j}+b(\mathrm{mod}\,x^r-1,n)\end{cases}\qquad m=n^i p^j$$

$$(x+b)^{n^i p^j}=[(x+b)^{n^i}]^{p^j}=[x^{n^i}]^{p^j}+b=x^{n^i p^j}+b(mod\ x^r-1,n)$$

krok a) krok b)

III. Załóżmy, że $b<a$. Jeżeli $a=b(modr)$, to $x^a=x^b(mod\, x^r-1,n)$.

Dowód:

$x^a-x^b=x^b(x^{a-b}-1)$. Pokażemy, że $x^b(x^{a-b}-1)$ jest wielokrotnością x^r-1 .

Połóżmy $a-b=lr$. Wtedy

$$x^{lr}-1=(x^r)^l-1=y^l-1=(y-1)(y+y^2+...+y^{l-1})=$$
$$=(x^r-1)(1+x^r+x^{2r}+...+x^{r(l-1)}).$$ C.N.D.

IV. Zasada szufladkowa Dirichleta.

Jeśli $0\le i,\ j\le|\sqrt{(r)}|$, to wtedy istnieją pary $(i,j)\neq(i',j')$ takie, że $n^i p^j=n^{i'} p^{j'}(mod\, r)$

(Są to liczby dające tą samą resztę. Dzieje się tak dlatego, gdyż możliwości wyboru par (ij) jest o jeden więcej niż istnieje reszt.)

V. Ekstrapolacja kroku II.

Krok II można zapisać

że dla $q_1(x)=x+b_1$ mamy równość $q_1(x)^m=q_1(x^m)(mod\, x^r-1,n)$,

a dla $q_2(x)x+b_2$ mamy $q_2(x)^m=q_2(x^m)(mod\, x^r-1,n)$.

Wtedy równość $q(x^m)=q(x)^m(mod\, x^r-1,n)$ zachodzi dla $q=q_1q_2$

Dowód.

$$(*)\begin{cases} q_1(x^m)=q_1(x)^m \bmod(x^r-1,n) \\ q_2(x^m)=q_2(x)^m \bmod(x^r-1,n) \end{cases}$$

$$q_1q_2(x^m)\overset{?}{=}q_1(x)^m q_2(x)^m$$

Ale lewa strona powyższego równania jest równa $q_1(x^m)q_2(x^m)=q_1(x)^m q_2(x)^m$ ma mocy (*). C.K.D.

VI. Konstrukcja elementu dużego rzedu w $Z[x]/x^r-1$.

Rozważmy grupę *G* generowaną przez dwumiany $x+b$, gdzie $b\in S$, w ciele $Z_P[x]/h(x)$, gdzie $b(x)$ jest wielomianem nierozkładalnym w $Z_P[x]$ dzielącym $\frac{x^r-1}{x-1}$

Zatem:

$$|G|\ge\left|\{\prod_{b\in S}(x+b)^{\alpha_b},\sum_{b\in S}\alpha_b\le q-1,\alpha_b\ge 0\}\right|$$

Grupa multiplikatywna ciała $Z_P[x]/h(x)$ jest cykliczna, zatem grupa *G* też jest cykliczna.

Jeśli *g* jest jej generatorem, to rząd $g=|G|\geq\left(\frac{q+|S|-1}{|S|}\right)$

VII. Zakończenie dowodu.

Niech *g* - generator grupy *G*, oraz m, m' będą elementami zbioru $\{n^i p^j : 0\leq i, j\leq|\sqrt{(n)}|\}$ takimi, że $m\equiv m'(mod\, r)$ wtedy prawdziwe jest:

$(*)\quad q(x^m)=q(x^{m'})(mod\, x^r-1, n)$

Jeśli q_1, q_2 spełniają (*) $\Rightarrow$ $q_1 * q_2$ też spełniają (*)

Zatem równanie (*) zachodzi dla generatora *g* w grupie *G*, tj.

$q(x^m)=p(x)^m mod\,(x^r-1, n)$

Ponieważ $m=m'(mod\, r)$ więc $(x+b)^m=(x+b)^{m'}(mod\, x^r-1)$ i na mocy multiplikatywności $(\prod_{b\in S}(x+b)^{a_b})^m=(\prod_{b\in S}(x+b)^{a_b})^{m'}(mod\, x^r-1, n)$

Czyli $q(x)^m=q(x)^{m'}$ w grupie G. Wtedy mamy

$$|G|\leq|m-m'|\leq n^{2\lfloor\sqrt{n}\rfloor}<\left|\begin{matrix}q+|S|-1\\|S|\end{matrix}\right|\leq|G|$$

Otrzymaliśmy sprzeczność z wnioskiem płynącym z zasady szufladkowej Dirichleta, czyli sprzeczność z $m\neq m'$. Sprzeczne więc jest $n^i p^j\neq n^{i'} p^{j'}$, czyli

$$n^i p^j = n^{i'} p^{j'}$$

$$n^{i-i'} = n^{j-j'} \Rightarrow n = p^{\alpha}$$

C.N.D

Algorytm AKS:

1) Znajdź liczbę pierwszą *r* rzędu $\mathcal{L}\hat{}c(n)$. Znajdź *q* – największy dzielnik pierwszy liczby *r-1* taki, że $n^{\frac{r-1}{q}}(mod\, r)\notin\{0,1\}$
2) Znajdź , takie że $\binom{q+s-1}{s}\geq n^{2|\sqrt{(r)}|}$
3) Sprawdź, czy *n* ma dzielnik pierwszy w zbiorze {2, 3, ..., s}
4) Jeśli nie, to sprawdź następującą kongruencję:
   $(x+b)^n=x^n+b(mod\, x^r-1, n)$
5) Sprawdź jaką potęgą liczby pierwszej jest *n*

5. Przekształcenia aproksymacyjne (przybliżające)

W praktycznych zastosowaniach dobrze jest reprezentować klucze częściowe $L \in P$ w postaci konkatenacji $l_0 * l_1 * ... * l_t$

Definicja

Podkluczem klucza $P = l_0 * l_1 * ... * l_t$ nazywamy dowolny klucz postaci $l_{i1} * l_{i2} * ... * l_{iS}$ gdzie $(l_1, l_2 ... l_{is})$ jest podciągiem ciągu (0, 1, ..., t).

W dalszym ciągu P oznaczać będziemy zbiór dowolnych kluczy częściowych w powyższym sensie.

Dla przybliżenia kluczy kompletnych przez niekompletne, wykorzystywać będziemy funkcję aproksymacyjną $\alpha : L \to P(U)$, który rozszerzamy do podzbiorów kluczy wejściowych $\tilde{\alpha} : P(L) \to P(U)$ w następujący sposób $\tilde{\alpha}(l_{i1} * l_{i2} * ... * l_{iS}) = \alpha(l_{i1}) \circ \alpha(l_{i2}) \circ ... \circ \alpha(l_{iS})$. W dalszym ciągu α będzie oznaczało funkcję rozszerzoną $\tilde{\alpha}$. Operacja "$\circ$" oznacza jedną z dwóch operacji mnogościowych "$\cup$" lub "$\cap$". Będziemy zakładać, że dziedziną funkcji α jest zbiór kluczy częściowych $\tilde{L}$ takich, że $\tilde{\alpha}(\tilde{L}) \neq \varnothing$

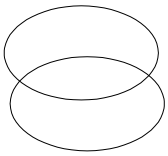
Przykład

" $\circ$ " = "$\cap$" L = { $l_1 * l_2$ } P = { $l_1, l_2, l_1 * l_2$ }

$\alpha : L \to P^+(U)$

$\alpha(l_1) \to$

$\alpha(l_2) \to$



$\leftarrow \alpha(l_1 * l_2) = \alpha(l_1) \cap \alpha(l_2)$

$l_1 * l_2$ – klucz kompletny

l_1, l_2 – klucze niekompletne

Definicja

Odległością pomiędzy kluczami częściowymi $L, L' \in P$ nazywamy wielkość $|L - L'| = card(\alpha(L) \div \alpha(L'))$.

Wygodnie jest rozpatrywać czwórkę (U, P, α , $\circ$) w przestrzeni kluczy częściowych $\alpha : P \to P^+(U)$ gdzie H = (U, P, α) jest odpowiednim hipergrafem. Język hipergrafów bardzo przydatny jest przy badaniu relacji pojęcia doskonałości.

Definicja

Strukturą przydziału kluczy nazywamy czwórkę (R, U, α , $\circ$) gdzie $R \subset K \times C$ $\tilde{R} \subset K \times P$ $\alpha : P \to P^{+}(U)$ oraz " $\circ$ " = "$\cup$" lub "$\cap$".

Jeśli $\circ = \cup$ to strukturę nazywamy strukturą dostępu. Jeśli $\circ = \cup$ to strukturę nazywamy, strukturą selekcji

6. Systemy kryptograficzne wykorzystujące krzywe eliptyczne i hipotezy o liczbach pierwszych.

Zagadnienia omówione na tym wykładzie:
1. Kryptosystemy „eliptyczne”
2. Kodowanie na krzywej
3. Problem logarytmu w E (Fq)
4. Aspekt bezpieczeństa - działanie Weila

6.1 Kryptosystemy eliptyczne:

1. Protokół Diffie-Hellmana na krzywej
P – punkt dużego rzędu (np.: generator) na krzywej E(Fq).
$|E(F\_q)| \approx\sim q$
A aP → B
(a) → bP (b)
Q = abP jest tajnym kluczem wymiany Diffiego-Hellmana

2. System Massey’a – Omury na krzywej eliptycznej
N = |E(Fq)| znane de = 1(mod N)

M → $P = P_m$
A w, P → B
← eBeaP
$d_A e_A e_B P$ B mnoży d_a i otrzymuje P.

3. Systemy eliptyczne ElGamala (szyfrowanie ze wskazówką).
M → P= Pm E(Fq),Q- znane publiczne

Wartość N=|E(Fq)| nie musimy znać.
A B
xA – tajny klucz xB – tajny klucz
xBQ – jawny
Do przekazania wiadomości P,A używając losowej wartości k ∈ Z przekazuje
$(kPQ, P + kx_B Q)$
gdzie Q jest publicznie znanym punktem krzywej E(Fq).
B
$x_B kQ = kx_B Q$ i odejmując od drugiej współrzędnej dostaje wiadomość P.

6.2 Kodowanie wiadomości na punktach krzywej

Zakładamy, że E (Fp) jest zadana przez równanie Weierstrasse

$y^2 = x^3 + Ax + B$

Gdzie p / Δ i AB = 0(mod p) (ale A i B nie są jednocześnie podzielne przez p).

Kodowanie punktów krzywej E(mod p).
Kodowanie musi być JEDNOZNACZNE i PRZEJRZYSTE
m – wiadomość (np. binarna)

P_m - punkt na E(mod p) odpowiadający wiadomości m.

Wtedy mamy następujące procesy

m → P_m → Q_m → P_m → m
kodowanie szyfrowanie deszyfrowanie dekodowanie

Przejrzystość kodowania zapewniamy określając
m→x : ∃y : (x, y) ∈ E

Mankament: dla wybranego x odpowiednie y może nie istnieć!

Dlatego algorytm A : m → A → x będzie PROBABILISTYCZNY, jeśli dla x nie powiedzie się to
x → x + 1. Dokładniej niech p > Mk (k = 50), gdzie M jest ograniczeniem wiadomości m tj.
m ∈ [0, M>.
Kodowanie K_j określamy następująco

$K_j(m) = m(k) + j$, j=1, 2, ……, k.

Jeśli $K_1(m)=x$ jest „złe” to sprawdzamy $K_2(m)$ itd.
Załóżmy, że dla pewnego j < k mamy

$K_j(m)$ dobre tj. ∃y : (x, y) ∈ E (mod p)

$K\, f(x)=x^3+Ax+B=E(mod\ p)$

tzn.
dla $x=K_j(m)$. Wtedy przyjmujemy:

$P_m(x,y)=(K_j(m), \sqrt[2]{f(K_j(m))}\ mod\ p >$

Dekodowanie ma zwrócić wartość wiadomości m, więc obliczamy je wyznaczając część całkowitą liczby

$K\frac{K_j(m)-1}{k}=\frac{mk+j-1}{k}=m+\frac{j-1}{k}$, która wynosi m, gdyż $K\frac{j-1}{k}=\frac{k-1}{k}<1$

Prawdopodobieństwo, ze kodowanie powiedzie się najdalej w k-tej próbie wynosi: $K\,1-2^{-k}\geqslant 1-2^{-50}$, gdyż dla 50% wartości x(mod p)dokładnie $\frac{p-1}{2}$ wartości $K\,x\in(p^{\perp}),f(x)=k(\ mod\,p)$ na mocy założenia że AB=O(mod p).

Dla krzywych szczególnej postaci KODOWANIE można określić deterministycznie. Tak jest na przykład dla krzywych rodziny $K\,E:y^2=x^3+Ax\ mod\,F_p$ gdzie p ≡ 3(mod 4) . Jak pokazaliśmy, jedna z wartości $K\,x^3+Ax\,lub\,(-x)^3+A(-x)$ jest kwadratem w ciele F_p gdyż ich symbole Legendre'a różnią się znakiem. W takim przypadku kodowanie można określićnastępująco:

$$m\rightarrow P_m=(\pm m(mod\,p),\sqrt{\pm(m3+Am)(mod\,p)})$$

gdzie znak ± wybieramy w zależności od tego czy $m^3+Am(mod\,p)$ jest resztą kwadratową czy nie (odpowiednio).

DEKODOWANIE

$$P=(x,y)\rightarrow\begin{array}{ll}x\,gdy & x^3+Ax=k(mod\,p)\\ & -x\,w.\,p.\,p.\end{array}$$

6.3 Logarytm dyskretny na krzywej $E(F_q)$

Metody znajdowania wartości logarytmu dyskretnego na krzywej E(Fq) :

1.) Metoda naiwna. Wybieramy kolejne wartości x= 2,3,4 i sprawdzamy, czy x P = Q?
2.) Algorytm Pohlig'a – Hellmana
3.) Metoda wielkich wielkich małych kroków (baby - step ,giant - step)
4.) Algorytm ρ -Pollarda
5.) Analogon metody indeksu

<u>Problem</u>

Dane P i Q ∈ $E(F_q)$. Znaleźć (o ile istnieje) x całkowite: xP=Q

Większość algorytmów obliczających logarytm dyskretny w grupie punktów wymiernych na krzywej $E(F_q)$ to algorytmy uniwersalne, a więc nie wykorzystujące szczególnej struktury grupy $E(F_q)$. W latach 90'tych MENEZES, VANSTONE i OKAMOTO wykorzystali działania WEILA, aby zanurzyć $E(F_q)$ w $F_{q^k}*$ i tym samym

zredukować problem L.D. do grupy G= $G=F_{q^k}*$.

Efektywność redukcji wymaga, aby k – było małe a to może się zdarzyć tylko dla krzywych SUPEROSOBLIWYCH (o jakich była mowa w rozważanych przypadkach, AB=0 mod p). Jeśli więc będziemy rozważać krzywe niesuperosobliwe i takie, że $E(F_q)$ ma duży dzielnik pierwszy to odpowiedni system kryptograficzny dla krzywej będzie bardziej BEZPIECZNY niż dla $G=Z_p*$ (przy porównywalnych wielkościach parametrów grupy).

Bezpieczeństwo na krzywej $E(F_q)$ przewyższa bezpieczeństwo w grupie F_q* , gdyż jak dotąd nie mamy odpowiedniego algorytmu imitującego metodę indeksu dla grupy F_q* .

Dla pokazania przyczyny za to odpowiedzialnej rozważmy krzywą $E(Q): y^2+y=x^3-x$.

Grupa punktów wymiernych na niej leżących jest nieskończona, generowana przez punkt P=(0,0).

Łatwo obliczamy, że jeśli $kP=(x,y)$ ¿ $(k+1)P=((\frac{y}{x})^2-x,-(\frac{y}{x})^3+y-1)$.

Ponieważ x,y są wymierne to możemy dla $x=\frac{a}{b}, y=\frac{c}{d}$ zdefiniować wysokość punktu P=(x,y) jako $H(P)=\log max\{|a|,|b|,|c|,|d|\}$

Spełnia ona równość H(P) = h(P)+O(1), gdzie h(P) to tzw. kanoniczna wysokość
NERONA – TATE'A
h(P) spełnia warunek
h(P+Q)+h(P-Q)=2(h(P)+h(Q))
skąd w szczególności
h(2P)=4h(P)
a więc H(2P)=4H(P)+O(1)
i podobnie

$$H(2^kP)=H(2\cdot 2^{k-1}P)=4\,H(2^{k-1}P)+O(1)=.....=4^kH(P)+O(k)=(2^k)^2\cdot H(P)+O(k)$$

co dowodzi, że wzrost wysokości punktu (przy k-tym podwojeniu punktu) następuje w tempie kwadratowym!

Reasumując mamy:

1. Wysokość punktu przy k-tej iteracji rośnie szybszej w grupie $E(F_q)$ niż grupie F_q* .

2. Na krzywej $E(F_q)$ liczba punktów o „małej" wysokości jest relatywnie mniejsza niż w grupie F_q^* ,

tj. $\#\{Q=\sum x_i P_i : H(x_i P_i)<t\} <$ ¿ Q = prod{ b_{i} ^{x_i} : b_{i} ^{x_i} < t}

Przykład

$E(Q): y^2+y=x^3-x$

P = (0, 0), 2P = (1, 0), …..

Dla k = 1, 2, …… otrzymamy dla współrzędnych y-tych kolejnych wielokrotności punktu P.

$\frac{8}{7}$

$\frac{69}{125}$

$\frac{435}{343}$

$\frac{2065}{64}$

$\frac{3612}{12167}$

Mianowniki wzrastają w tempie $O(e^{k^2})$, więc ilość odpowiadającym im cyfr w tempie $O(k^2)$. Metoda indeksu dla krzywej $E(F_q)$ T,S ∈ $E(F_q)$.

Dane:

Znaleźć: n: S = n T

Q – ciało liczb wymiernych

1.) Wybieramy krzywą E(Q) , która redukuję się do krzywej $E(F_q)$, która ma dużą ilość niezależnych punktów p1,p2,…,pr (generatorów grupy $E(F_q)$).

2.) Wyliczamy wielokrotności S,2S,3S,… ∈ $E(F_q)$ i dla każdego takiego punktu znajdujemy odpowiedni punkt S_i ∈ E(Q) redukujący się do punktu i S ∈ $E(F_q)$.

3.) Rozwiązujemy równanie :

$$S_i = \sum_{r}^{j=1} n_j p_j \qquad \text{w E(Q)}$$

4.) r – krotne powtórzenie punktu 3 daje r- równań:

$$j = \sum_{r}^{j=1} n_j \log_S(P_i)$$

które można rozwiązać dla danych P.

5.) Podnosimy T + j S $\in$ $E(F_q)$.(dla pewnego j) do Tj $\in$ E(Q) (tzn. znajdując punkt z E(Q)),

który redukuje się do T + jS $\in$ $E(F_q)$.

Rozkładamy :

$$T_j = \sum_{r}^{i=1} m_i \log_S(P_i)$$

6.) Mając już wszystkie dane możemy policzyć n korzystając ze wzoru :

$$\log_S(T_j) + j = \sum_{r}^{i=1} P_i$$

Wniosek

Tak zmodyfikowana metoda indeksu , ma 3 „słabe” punkty :

1.) Trudno jest znaleźć krzywe E(Q) z wysoką rangą (nieznane są krzywe z rangą większą niż 2 ,3)

2.) Trudno jest znaleźć krzywe E(Q) generowane przez punkty o małej wysokości.

3.) Mając daną krzywą E(Q) i liczbą pierwszą p ,oraz punkt S $\in$ E(Q) który redukuje się do punktu S.

6.4 Działanie Weila

Działanie Weila (które redukuje problem logarytmu dyskretnego na krzywej $E(F_q)$ do analogicznego problemu dla F_q^*) to przyporządkowanie $E(Q)^2 \ni (P,Q) \rightarrow <P,Q>,$

które spełnia następujący warunek dwuliniowości

$<P1+P2,Q> = <P1,Q> + <P2,Q>$ ¿

Wysokość h(P) punktu P to z definicji wartość $h(P)=<P, P>$

Wniosek

$$< P, Q > = \frac{1}{2}(h(P+Q)-h(P)-h(Q))$$

Dowód

h(P + Q) =< P + Q, P + Q >= (P, P) + < Q, Q > +2(P, Q) = h(P) + h(Q) + 2 < P, Q >

WŁASNOŚCI h(P)

Zachodzi następujący związek pomiędzy wysokością punktu i jego rzędem (w grupie E (Q)).

h(P) = 0 ⇔ rzP < ∞ gdzie h(P) jest kanoniczną wysokością Nerona-Tate'a.

n = 1,2,... jest okresowy jeśli rzP < ∞ i

Dla dowodu zauważmy, że ciąg punktów $2^n P$ wtedy jest też odpowiedni ciąg wysokości $h(2^n P)$ jest ograniczony, skąd na mocy własności

$h(2^n P)=4^n h(P)+O(1)$

otrzymujemy, że h(P) = 0 .

Odwrotnie jeśli h(P) = 0 to 0 = 4 n h(P) = h(2 n P) + 0(1)

Skąd $h(2^n P)$ ograniczony, więc ciąg $2^n P$, n = 1,2,... jest w istocie skończony. Zatem punkt P ma rząd skończony.

Uwaga

Powyższa równoważność pozwala na ignorowanie części torsyjnej przy badaniu grupy Mordella-Weila.

Niech G ' = {2 P, P ∈ E (Q)}

Ponieważ działanie dodawania punktów jest przemienne więc G ' jest podgrupą grupy E (Q) .

Zachodzi następujące (słabe twierdzenie Mordella):

Twierdzenie

Grupa ilorazowa E (Q) / 2 E (Q) jest skończona.

W oparciu o nie pokażemy teraz, że dowolny punkt grupy E (Q) jest kombinacją liniową punktów o wysokościach ograniczonych przez wysokości reprezentantów powyższej grupy ilorazowej.

Dowód

Niech $P_1, P_2, \ldots, P_r$ generuje wszystkie elementy modulo 2 E (Q) i niech

$M = max\, h(P_i). Jeśli\ S = \{ P \in E(Q) : h(P) \le M \}$ to pokażemy, że S = E (Q) .

Niech $P \in E(Q) - <S>$ będzie takim punktem, że h(P) jest minimalne.

Wtedy $P = P_i + 2R$ gdzie i≤r oraz $R \notin <S>$

Na mocy minimalności mamy, że gdzie h(P)

$$h(P) \le h(R) = \frac{1}{4} h(2R) = \frac{1}{4} h(P - P_i) \le \frac{1}{2}(h(P) + h(P_i)) \le \frac{1}{2}(h(P_i) + M)$$ skąd h(P) < M

otrzymana sprzeczność kończy dowód.

I.) Efektywna arytmetyka na krzywej $E(F_q)$.

Krzywe eliptyczne izomorficzne.

1.) K- ciało ,E(k) krzywa e eliptyczna nad K w ogólnej postaci Weierstrassa.

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \ \ gdzie\ a_i \in K$$

Powiemy ,że dwie krzywe E i E' są izomorficzne wtedy i tylko wtedy gdy jedna da się otrzymać z drugiej przez (dopuszczalną) zamianę zmiennych postaci :

$(x, y) \to (u^2 x + r, u^3 y + u^2 sx + t)$ podzielenie otrzymanego równania przez u^6 , gdzie u∈K\{0}., r , s ,t ∈K.

Wniosek

Jeśli char k ≠ 2 ,3 to dopuszczalna zamiana zmiennych prowadzi od (szczególnej) postaci Weierstrassa $E : y^2 = x^3 + A + B$

Wtedy mamy następujące wzory na podwojenie i dodawanię punktów.

(1.) P = Θ to -P = Θ

(2.) P = (x,y) to -P = (x , -y)

(3.) P ≠ -P i P = (x,y) to

$$x(2P) = \frac{3\,x(P)^2 + A}{2y(P)} - 2x(P) \quad \text{i} \quad y(2P) = \left(\frac{3\,x(P)^2 + A}{2y(P)}\right)^2 - 2x(P) - y(P)$$

(4.) Jeśli P ≠ ± Q to

$$x(P\, xor \oplus Q) = \left[\frac{y(Q) - y(P)}{x(Q) - x(P)}\right]^2 - x(P) - x(Q)$$

$$(P\,xor\,\oplus Q)=[\frac{y(Q)-y(P)}{x(Q)-x(P)}]-x(P)-x(P+Q)-y(P)$$

Przykład

$E(F_{23}): y^2=x^3+x+4$ $E(F_{23})$ jest grupą rzędu 29 generowaną przez punkt P = (0,2).

Przykład

$E(Q): y^2+y=x^3-x$ Punkt (0,0) jest jej generatorem nieskończonego rzędu. Dopuszczalna zmiana zmiennych prowadzi do krzywej w szczególnej postaci Weierstrassa : $y^2=x^3+Ax+B$ i wykorzystując wzory na podwojenie i dodawanie punktów
otrzymujemy :

$2P=(\frac{1,1}{2})$ i ogólnie jeśli $kP=(x,y)$ to $(k+1)P=[(\frac{x}{y})^2-x;-(\frac{x}{y})^3+y-1\ ]$

Zamieniana układu współrzędnych $(x,y)\rightarrow(x,y-\frac{1}{2})$ przeprowadza krzywą E na

$E': y^2=x^3-x+\frac{1}{4}$ oraz punkt $P=(0,0)$ na $P'=(0,\frac{1}{2})$. Układ współrzędnych przesuwamy o
wektor $(0,-\frac{1}{2})$. współrzędne punktu przesunięte są o wektor $(0,\frac{1}{2})$.

$2P'=(1,\frac{1}{2})\Rightarrow 2P=(1,\frac{1}{2})+(0,-\frac{1}{2})=(1,0)$

Niech $kP=(x,y)$ wtedy $(kP)'=(x,y)+(0,\frac{1}{2})=(x,y+\frac{1}{2})$

$$(k+1)'=kP'\,xor\,\oplus P'=P'\,xor\,\oplus kP'=(x,y+\frac{1}{2})\oplus xor\,(0,\frac{1}{2})=((\frac{y}{x})^2-x,-(\frac{y}{x})^3+y-\frac{1}{2})$$

Zatem

$$(k+1)P=(k+1)P'+(0,-\frac{1}{2})=((\frac{y}{x})^2-x,-(\frac{y}{x})^3+y-1)$$

krzywe eliptyczne nad ciałem Fq .

Uwaga

Istnieje wiele systemów kryptograficznych wykorzystujemy arytmetykę w skończonej grupie abelowej G.

(np. $G=Z_p^*$ * lub G = $G=E(F_q)$) ,których bezpieczeństwo jest oparte na problemie logarytmu dyskretnego w G. (np. system Diffiego-Hellmana , ElGamala i inne). Aby uniemożliwić atak oparty na algorytmie Pohliga-Hellmana, rząd grupy G musi być podzielny przez dużą liczbę pierwszą.

W przypadku grupy $G=E(F_q^r)$ powstaje pytanie: „Dla jakich r możemy spodziewać się ,że $\# E(F_q^r)$ jest podzielny przez dużą liczbę pierwszą.

Po pierwsze zauważmy ,że jeżeli P = (x,y) ∈ $E(F_q^r)$ to x= x(t), y = y(t) gdzie x (t) ,y(t) ∈Fu[Fq] są wielomianami st ≤ r -1 .W szczególności wielomiany stałe (stopnia 0) dają punkty (x,y) ∈ $E(F_q)$. Ponieważ F_q jest zbiorem zamkniętym, że względem na branie punktu przeciwnego, dodawanie punktów więc $E(F_q)$ jest podciałem $E(F_q^r)$ .Podobnie jeśli F_q^S jest podciałem ciała F_q^r to

$F_q^s=\{\sum_{0\le i\le k} a_i t^i, a_i\in (F_q^s)\}$, a zatem $\# F_q^r=(q^s)^k$ i w konsekwencji s| r.

Odwrotnie jeśli s|r to F_q^s jest podciałem F_q^r ,zatem $S(F_q^s)$ jest podgrupą grupy $E(F_q^r)$ jeśli s|r i z tw. Lagrange'a wynika , że

$\frac{\# E(F_q^r)}{\# E(F_q^s)}$ jest liczbą całkowitą. Zatem dużych dzielników pierwszych dzielących rząd grupy $\# E(F_q^r)$ powinniśmy raczej szukać dla r będących liczbami pierwszymi , niż złożonymi . Niech zatem r będzie liczbą pierwszą.

Rozważmy iloraz :

$\frac{\# E(F_q^r)}{\# E(F_q)}$ Na mocy twierdzeń Hasse-Weila mamy, że $Nr=|\alpha^r-1|$ dla r ∈ N

gdzie α ,α to pierwiastki trójmianu $T^2+aT+qa=q+1-N_1$ operujące w twierdzeniu Hassego.

Reasumując mamy $\frac{N_r}{N}=|\frac{\alpha^r-t}{\alpha-1}|^2$

Hipoteza

$|\frac{\alpha^r-t}{\alpha-1}|$ jest liczbą pierwszą dla nieskończenie wielu r ∈N.

Teraz pokażemy w jaki sposób możemy wybierać krzywe i punkty na niej

leżące do konstrukcji systemów kryptograficznych.

Wybór krzywej i punktu w konstrukcji kryptosystemu

Metoda 1:
Losowy wybór krzywej E i punktu P :
(E, P) , $E = E(F_q)$, q -ustalone

Wybieramy losowy x , y , A należące do ciała i definiujemy $B = y^2 - (x^3 + ax)$
wtedy punkt P = (x, y) leży na krzywej zadanej równaniem $y^2 = x^3 + Bx + B$.

Metoda 2:
Redukcja krzywej globalnej

a) wybieramy krzywą eliptyczną E (Q) taką, że jej rząd jest nieskończony (ranga krzywej >0). Można to osiągnąć znajdując punkt na krzywej i dowodząc, że E_{tors} jest trywialne.
b) wyznaczamy punkt P leżący na E (Q) nieskończonego rzędu.
c) Wybieramy dużą liczbę pierwszą p i rozważamy redukcję krzywej E(mod p)

Uwaga

Dla prawie wszystkich p tak określona redukcja daje dobrze określoną krzywą eliptyczną

d) Zmieniając p generujemy wiele par (E p , Pp) , gdzie Pp - redukcja punktu P (mod p)

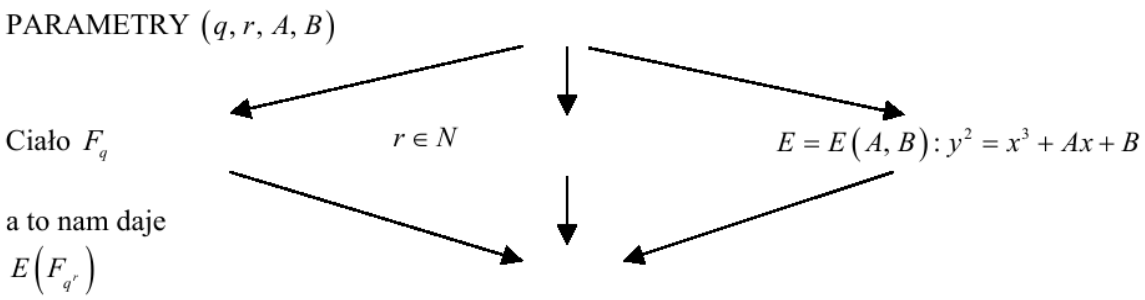
Przykład

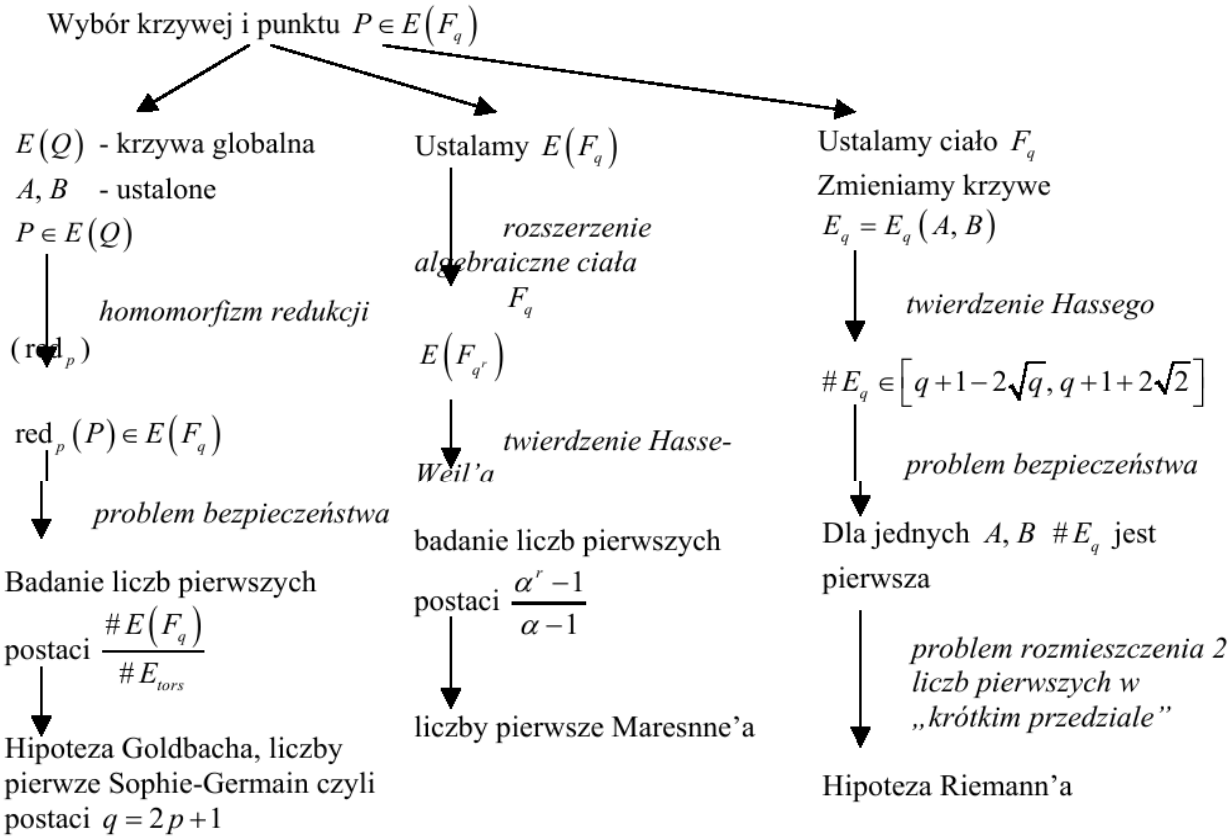
Załóżmy α = 2. Wtedy liczby pierwsze postaci

$\frac{w^r - t}{2 - 1} = 2^r - 1$ nazywamy liczbami pierwszymi Marsenne'a

Podsumowanie
Q - ciało liczb wymiernych
E_q - ciało skończone

Systemy kryptograficzne wykorzystujące krzywe $E\left(F_{q^r}\right)$





Znajdywanie punktów na krzywej $E\left(F_q\right)$

Rozkład krzywej nad ciałem liczb wymiernych

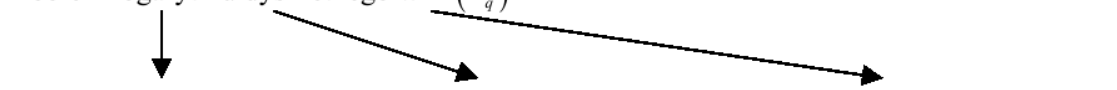
$E(q) = E_{tors} \oplus Z^r$, r - generator

działanie Weil'a twierdzenie Nagelle-Lutza homomorfizm redukcji red_p

Bezpieczeństwo

Jeśli uda się złamać problem logarytmu dyskretnego to te systemy stracą zastosowanie.

Problem logarytmu dyskretnego w $E(F_q)$



Wysokość Neron'a-Tate'a i działanie Weil'a

Wybór parametrów A, B, q, r takich że ilość punktów n krzywej $\#E(F_{q^r})$ ma duży dzielnik pierwszy.

Znane algorytmy znajdujące logarytm dyskretny na krzywej $E(F_q)$ („metoda indeksu")

7. Relacje rozkładu

K, L - skończone zbiory

L^* - rodzina wszystkich skończonych ciągów z L (z uwzględnieniem ciągu pustego)

Elementy L^* oznaczamy sembolem $L=l_{i1}*...*l_{ir}$, l_{ik} różne dla k=1,...,r

Niech $L' \in L^* \; L'=l_{j1}*...*l_{is}$ l_{ik} - różne , k=1,...,s

Definicja

$L^* L'=l_{m1}*...*l_{mt}$ gdzie $m_{1,}...,m_t$ jeśli podciągiem ciągu $(l_{1,}...,l_r, j_{1,}...,j_s)$ złożony ze wszystkich różnych wyrazów. Z definicji przyjmujemy, że $L^* \emptyset = L$. Zapis $L \subset L'$, oznacza, że wszystkie wyrazy l_i występują w L pojawiają się też w L' .

Relacje rozkładu

$R \subset K \times L$ bez zmniejszenia ogólności zakładamy, że

$\forall k \in K \; \exists l \in L : (k,l) \in R$

$\forall l \in L \; \exists k \in K : (k,l) \in R$

Definicja 1

Relacje rozkładu (odpowiadającego R) nazywamy relację S zdefiniowaną następująco $S \subset K^* L^*$.

1. $L=(k, l_1 * l_2 * ... l_r) \in S \Leftrightarrow (k, l_1) \in R$ dla i=1,2,...,r. Z definicji przyjmujemy, że $(k, \emptyset) \in S$. W dowolnym ciągu będziemy ograniczać się do relacji : $S \subset K^*$ gdzie dla dowolnego $L \in P$ istanieje $k \in K$ takie, że $(k,l) \in S$

Do budowy relacji rozkładu podstawowe znaczenie mają zbiory:

2. $A(l)=k \in K : (k,l) \in S$
3. $B(k)=L \in P : (k,l) \in S$

Wniosek

Rodzina zbiorów A(l) jest monotoniczna tzn. zachodzi implikacja

$$L \subset L' \Rightarrow (k, L') \in S \Rightarrow (k, L) \in S$$

Definicja 2

L, L' są równoważne wtt gdy A(L) = A(L')

Definicja 3

Powiemy, że $L \in P$ jest kompletnym rozkładem klucza k (odpowiadającego L) wtt gdy, żaden element L' nierównoważny L tzn. że $L^T \gg L$ nie jest relacją zk.

Wniosek

Jeśli $|A(L)|=1$ to L jest kluczem kompletnym odpowiadający k takiemu, że $(k,l) \in S$

Definicja 4

Niech $K_m \subset K$ bedzie podzbiorem K takim, że dowolny klucz kompletny $L \in P$ odpowiadający $k \in K$ ma długośćm. Obliczając relację S do odpowiedniej relacji:

$S_m \subset K_m * P$ otrzymujemy relację m-rozkładów. Niech $X = X_m$ - funkcje charakterystyczne relacji S_m .

Twierdzenie

Niech $|K|^{1/m} \geq M \geq |L|^{1/2}$ żałóżmy, że istnieje funkcja $u: L \Rightarrow [0,1]$ taka, że

1. $\sum_{\mu \in L} \mu(l) = \mu + O(1)$ dla pewnego $\mu = \mu(K,L)$ gdy $K \Rightarrow \infty$
2. $\forall L \in P \; A(L) = \mu(L)|K|(1+O(\frac{1}{\mu}))$ gdzie $\mu(l) = \mu(l_1 * \ldots * l_s) = \mu(l_1)\mu(l_2)\ldots\mu(l_s)$

wtedy $card\,\{k : (B^{|m|}{}_r(k) - M^r| > \epsilon M^r)\} = O_s(\frac{|K|}{M\epsilon^2})$ dla każdego $r \leq m-1$

Definicja 5

$B_r^{(m)}(k) = \{L \in P : |L| = r, (k,L) \in S_m\}$

Mamy, po zmienie kolejności sumowania:

$$\sum_1 = \sum_{l_1, l_2} \sum_K \chi_m(k, l_1)\chi(k, l_2) =$$

$$\sum_{l_1, l_2} \sum_K \chi_m(k, l_1 * l_2) =$$

$$\sum_{l_1, l_2} |A(l_1 * l_2)| =$$

sprawdzić, że

$$\sum_{l_1, l_2} (\mu(l_1 * L_2)|itak\,K| + O(1)) =$$

$$M^2|K|(1+O(\frac{1}{M})) + O(|K|^2) + O(|K|)$$

$|K|^2 \le M|K|$ *ponieważ* $m \ge 2$ to

$|L|^2 \le M^4 \le M * M^3 = M(|K|^{1/m})^3 \le M|K|$ c.k.d.

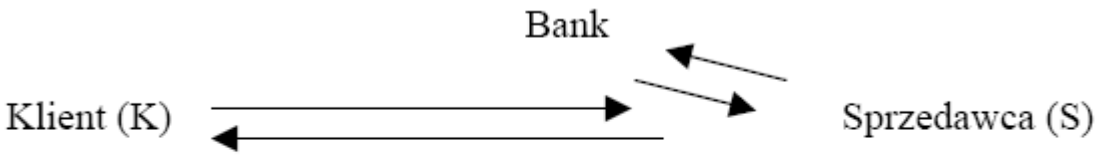
Podobnie pokażemy, że

$$\sum_2 = |K| M^2 (1 + O(\frac{1}{M})) = \sum_3$$

Zatem

$$\sum = O(|K|M)$$

8. Schematy płatności internetowych i model pieniądza cyfrowego



on-line $2N + 2N = 4N$
off-line $2N + \varepsilon$

Koszty transakcji:
- sprzęt
- połączenie (ilość)
- obsługa ludzka
- ubezpieczenie

Zagrożenia

PROCES rozliczania transakcji (płatność + autoryzacja)

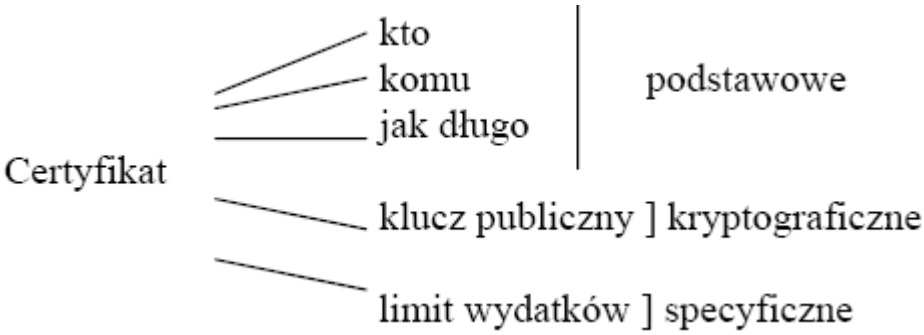
klient	- przekroczenie salda, limitu dziennego
	- pranie brudnych pieniędzy
	- oszustwa
sprzedawca	- powielanie zleceń (zamówień)
Bank	- monitorowanie klienta

Zewnętrzne	- wykorzystywanie przerw w połączeniach
	- ataki hackerskie

Korzyści:

- zakupy wirtualne
- bezpieczeństwo fizyczne
- większa anonimowość

Podstawowe wymogi
(zawarcie transakcji)



Postać certyfikatu

$$C_u = \{\underbrace{Id_B, Id_M, X_U, Exp, LIM}_{m}\}_{\sigma_B(m)}$$

Weryfikacja podpisu Banku

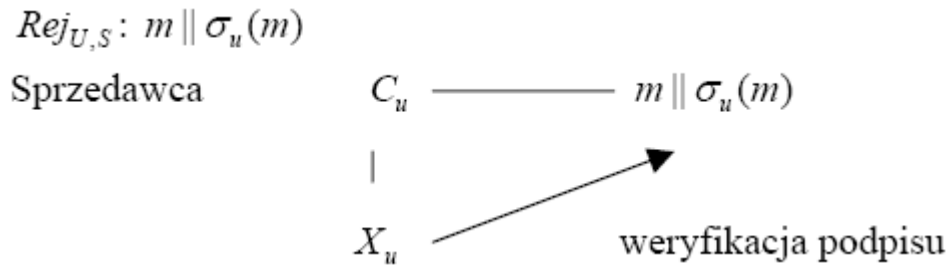
$$x_B(H(m)) \rightarrow X_B x_B(H(m)) = H(m)$$

H – funkcja haszujące (silna kryptograficznie)
(x, X) para kluczy: prywatny, publiczny

Rejestracja (aspekt płatności)
Założenie: S zna $X_B!$

$$Rej_{U,S} = \{\underbrace{C_u, Id_s, T, P}_{m}\}_{\sigma_u(m)}$$

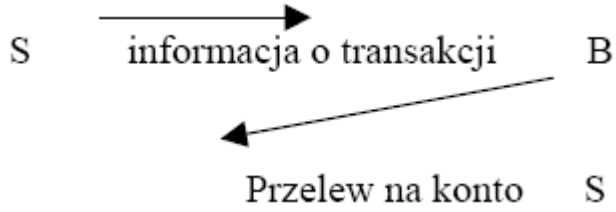
T – data i czas zakupu
P – pole płatności (forma płatności)
Model graficzny (|| oznacza konkatenację)



Sprzedawca wykonuje:
- sprawdza wartość certyfikatu (Exp!)
- weryfikuje autentyczność klienta (sprawdza, że $U = U(C_U)$)
- akceptuje płatność (po połączeniu z Bankiem)

Realizacja kolejnych płatności
- ograniczenie: LIM (dzienny) zawarty w
- na koniec (dnia) – raport do Banku

Rozliczenie z Bankiem



Anonimowość w aspekcie płatności
E – czek (imienny) np. ikp
ma postać
$m \| \sigma_B(m)$

gdzie m zawiera dane: emitentna, właściciela, ew. kwoty.

Deponując czek Bank identyfikuje klienta. Anonimowość klienta wobec Banku polegałaby na tym, że Bank deponując autoryzowany swoim podpisem cyfrowym banknot elektroniczny nie mógłby powiązać go z tożsamością klienta-właścicielka banknotu. Inaczej bank nie może oznaczyć banknotu, który podpisuje.

Realizuje: ślepy podpis
Aby zapobiec oszustwom ze strony klienta Bank sprawdza „duże" próbkę banknotów do ślepego podpisu. Jeśli są zgodne ze standardem pozostałe

podpisując na „ślepo”.

Kryptografia cyfrowego pieniądza (idea)
M – Dane Banku, Identyfikacyjny numer banknotu.
Podpis $\sigma_B(m) = x_B \circ m$

Podpis ślepy:
Maska dla m postaci ($r \circ X_B$)m
gdzie r – losowy czynnik (maskujący)
Podpis pod maską

$$[(r \circ X)m]_{\sigma_B} = [(X \circ r)m]_{\sigma_B} = x(X \circ r)(x \circ m) =$$
$$((xX) \circ r)(x \circ m) = r(x \circ m) = r \cdot \sigma_B(m)$$

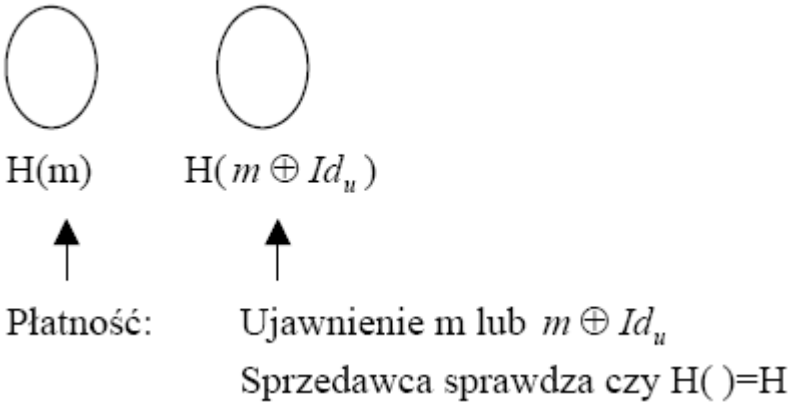
Uwaga

Wykorzystaliśmy homomorfizm przekształcenia podpisu (np. deszyfrowanie RSA). W praktyce (bezpieczeństwo) rozważamy
$[(X \circ r)H(m)]_\sigma$

Systemy anonimowe z certyfikacją

Założenia
$C_u = \{C.A., X_u, p, q, \gamma\}, \quad X_u = \gamma^{x_u} (\mathrm{mod}\, p)$
Certyfikat zawiera X_U i stałe protokołu (bez danych U). Jeśli Bank obliczy x_u to C.A. podaje dane użytkownika (demaskuje oszusta!)

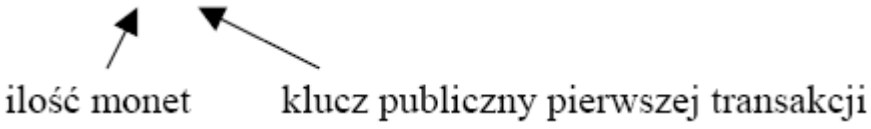
1. Moneta cyfrowa
- Odkrycie strony monety to ujawnienie wartości m lub odpowiednio



Jeśli dwukrotnie U płaci tą samą monetę z szansą 1:2 odkryje różne strony monety i wtedy m⊕m⊕Id = Id

2. Podpis Banku (ślepy). Załóżmy, że wszystkie monety są tego samego nominału (uproszczenie!)

Bank podpisuje na ślepo $\{n, R_1, C_u\}_B$



Transakcje

Podpis transakcyjny składa się z trójki (h, z_k, R_k): $z_k = r_k + xh (\mathrm{mod}\, q)$

gdzie

$h = H(Id_s, R_{k+1}, n')$

n' – ilość monet pozostałych do wydania zatem podpis pod kolejną transakcją zależy od wcześniejszej.

r_k - losowo wybrany przez klienta klucz prywatny k-tej transakcji.

Klient nie może bezkarnie powielić transakcji u, tego samego sprzedawcy. Jeśli $s \neq s' \; to \; h \neq h'$ i Bank obliczy

$$\frac{z - z'}{h - h'} = \frac{x(h - h')}{h - h'} = x \quad \text{i w połączeniu z C.A. zdemaskuje oszusta}$$

$$r_k = r_k'$$

9. Mikropłatności. System Bankowości Internetowej PLANET

System MicroMint (mennica elektroniczna)
Ekwiwalentem pieniądza jest *k* - kolizja to jest wektor
$(x_1,...,x_k): \quad h(x_1) = ... = h(x_k)$.

Zakładamy, że Sprzedawca zna Bank i parametry (h,k).
System nie wykorzystuje certyfikatów cyfrowych.

Porównanie kosztów
Obliczenie h : $100^2 x$ szybsze niż generowanie RSA
$10^2 x$ szybsze niż weryfikacja podpisu RSA

Faza wstępna (Klient-Bank)
Bank przydziela (sprzedaje) użytkownikowi *l k*- kolizji (na przykład do końca danego miesiąca).
(Można zakładać, że ciągi $(x_1,...,x_K)$ różnią się istotnie !). Są przechowywane w bazie danych Banku.

Płatność: $(x_1,...,x_k)$= jednostka płatnicza K. S sprawdza, czy
$h(x_1) = ... = h(x_k)$.

raport S na koniec dnia (S przekazuje ciągi do B).

Bank sprawdza, że kolizje nie powtarzają się (powtórzenie stanowi tą samą monetę!) i powiększa saldo na rachunku Sprzedawcy

Generacja (kolizji)
Bank wcześniej przygotowuje kolizję (proces opłacalny w kosztach obliczeniowych). Na dany miesiąc akceptuje szczególne typy np.

$$x_i = (....., \overbrace{01.....1}^{e\ bitów}).$$

To utrudnienie generowanie ciągów kolizji ewentualnym oszustom. Koszt generowania kolizji odpowiedniego nominału czyni oszustwo nieopłacalnym.

Bezpieczeństwo
$h(x_i)$ - ciągi n – bitowe

Paradoks urodzinowy:

$\sqrt{2^n} = 2^{n/2}$ przeszukiwań znajduje 2 – kolizję z dużym prawdopodobieństwem.

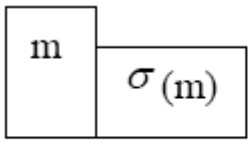
Podejście probabilistyczne
Mamy k – kostek 2^n ściennych
Kolizje: na każdej kostce wypada taka sama liczba „oczek"

k = 2 Średni czas oczekiwania na tę samą liczbą oczek to $2^{n/2}$.

Ogólnie $2^{n\cdot\frac{k-1}{k}}$

System Payword

h - funkcja haszująca
Rejestracja:



gdzie
$m = \{C_U, \quad h^{n-1}(x_0), h^n(x_0)\}$

x_0 - losowo wybrany przez U

$\left[h^{n-1}, h^n\right]$ - pierwsza płatność płatność rejestracji.

KOLEJNE PŁATNOŚCI

Klient płaci *i* – jednostkami podając wartość h^{n-i-1} . Sprzedawca sprawdza czy $h^i h^{n-i-1} = h^{n-1}$
Akceptacja płatności dopóki $\sum i \le n$.

Payword – wielokrotne zakupy u jednego sprzedawcy
Koszt: *n* iteracji funkcji *h*
Bezpieczeństwo:
$h^n \nrightarrow h^{n-1} \nrightarrow h^{n-2} ...itd$.

WARIACJA

Sprzedawca losowo raportuje do Banku żądając potwierdzenia salda

Ten wariant pośredni (on / off) jest tańszy niż klasyczny „on".

System PLANET bankowości internetowej

KLIENT
• Klient wchodzi na stronę internetową oddziału banku
• Za pomocą appletu wypełnia wniosek (następuje generacja pary kluczy prywatny / publiczny)
• Klucz prywatny i publiczny zapisywany jest na dyskietce klienta.
• wypełniony wniosek wraz z kluczem publicznym przesyłany jest za pośrednictwem internetu do banku (dane klienta są przesyłane w postaci zaszyfrowanej).
• Poprawny przekaz implikuje wyświetlanie potwierdzeń dostarczenia wniosku zawierając „odciski palca" klucza publicznego użytkownika (np. ciąg 32 bitowy w systemie PLANET).
• Klient zapisuje „odcisk palca" lub drukuje potwierdzenie dla późniejszej weryfikacji poprawności certyfikatu wydawanego przez oddział banku.

ADMINISTRATOR systemu w centrali banku po otrzymaniu wniosku i weryfikacji jego poprawności wykonuje:
• Pobiera odpowiadający wnioskowi plik żądania wytworzenia certyfikatu i generuje certyfikat dla naszego użytkownika.
• Utworzony certyfikat dołącza do właściwego wniosku w module administracji wnioskami.
• Akceptując wniosek zostaje automatycznie wysłany do obsługi infolinii.

ADMINISTRATOR systemu w zespole obsługi infolinii po otrzymaniu wniosku z certyfikatem:
• Wprowadza nowego użytkownika do systemu.
• Nadaje użytkownikowi identyfikator.
• Akceptując wniosek automatycznie jest przekazywany do odpowiedniego oddziału.

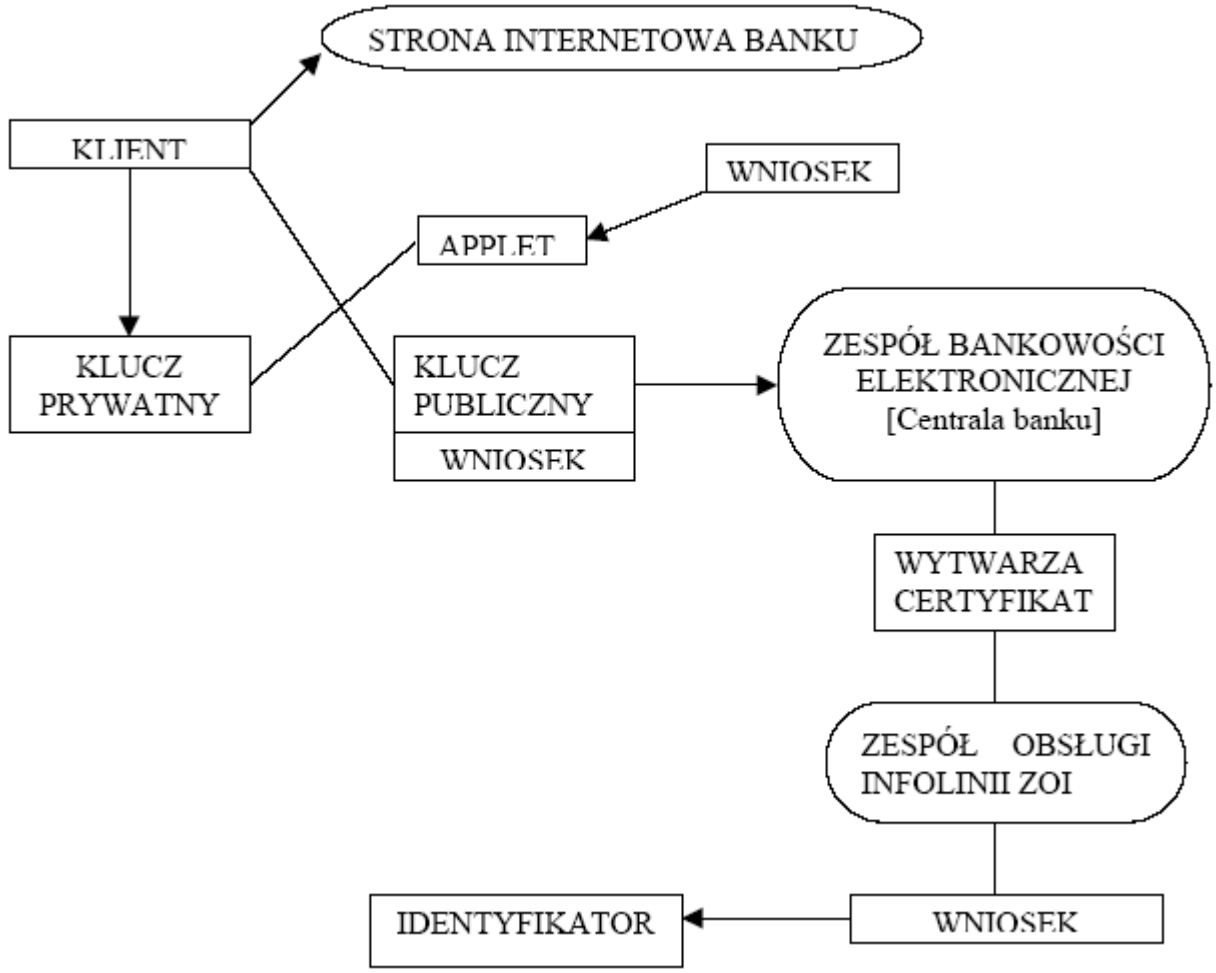
PRACOWNIK oddziału kontaktuje się z klientem i ustala:
• Datę podpisania wniosku i odbioru certyfikatu

• Przygotowuje dyskietkę z zapisanym certyfikatem i instrukcją

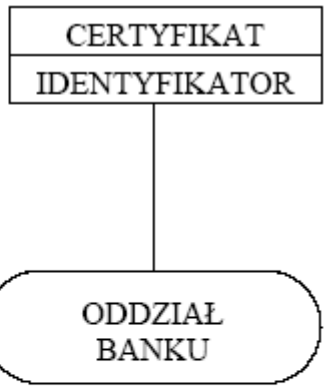
KLIENT przed podpisaniem wniosku w oddziale:
• Porównuje „odcisk palca" klucza publicznego obliczony przez klienta z odciskiem palca klucza publicznego zawartego w certyfikacie.
• Otrzymuje swój identyfikator.

SYSTEM BANKOWOŚCI INTERNETOWEJ

• Staje się dostępny po kilku godzinach, po wprowadzeniu go do systemu w aplikacji administratora.
• Po zakończeniu obsługi klienta przez pracownika oddziału wniosek jest przekazywany do ZOI.
• Jeśli nie ma konieczności wprowadzenia zmian w konfiguracji konta użytkownika ZOI przekazuje wniosek automatycznie do archiwum.



Klucz prywatny zabezpieczony hasłem klient wykorzystuje do tworzenia PODPISU ELEKTRONICZNEGO pod wszelkimi dyspozycjami składanymi w ramach SYSTEMU B.I.



POROWNANIE
Odcisków palca, klucza publicznego klienta i wartość klucza zawartego w certyfikacie klienta
PRZYDZIELENIE
Dyskietki z certyfikatem.
PODPISANIE
Wniosku