6. Grupowe struktury dwuliniowe

6.1 Grupowe struktury dwuliniowe

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

Działanie dwuliniowe (iloczyn dwuliniowy)
$e: G_1 \times G_2 \to G_2$ 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 (niezdegenerowalność) 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 w strukturze dwuliniowej

$P, Q \in G_1$ punkty znane publicznie

A → B
aP - publ. bP – publ.

aQ – prywatne bQ – prywante
a,b – losowe

Każda strona wyznacza 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

6.2 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

6.3 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

6.3.1 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 $h=h(m, rP)$ 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.

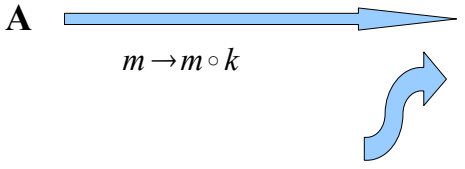
Sprawdzamy (*)

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.

6.4 System szyfrowania oparty na identyfikacji



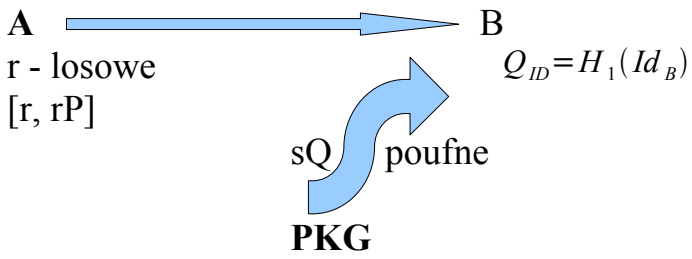
PKG (private key generator)

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*

sP – 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.

7. Problemy obliczeniowe w strukturze dwuliniowej

7.1 Problem Diffie-Hellmana

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 $abP = cP$

7.2 Redukcje MOV

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.

7.3 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.

8. Iloczyn WEILA

8.1 Wprowadzenie

W tym rozdziale zdefiniujemy działanie dwuliniowespełniające warunki: nietrywialności i obliczalności.

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 $\hat{e}=H\times H\to G$ 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.

8.2 Grupa klas dywizorów krzywej eliptycznej

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 $(f)=\sum ord_P f(P)$

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:

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

$$f((P)-(Q))=f(P)\cdot f(Q)^{-1}=\frac{f(P)}{f(Q)}$$

8.3 Określenie iloczynu Weila

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 $(f_p^n)\sim n(P)-n(\theta)$ $A_Q\sim(Q)-(\theta)$

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

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

$\operatorname{div}(f_P{}^n\cdot g^n)=\operatorname{div} f_P{}^n+n(\operatorname{div})g$ 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 $a\in\{b,c,b+c\}$ 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 Weila $e_n(P,Q)$ wykonuje się w czasie $O(\log^c n)$ gdzie c jest pewną stałą dodatnią.