Krzywe eliptyczne i kryptografia

Wojciech GUZICKI

Z artykułu J. Konarskiego dowiedzieliśmy się, że każda krzywa eliptyczna jest tzw. grupą przemienną, co oznacza, że punkty tej krzywej można elegancko dodawać.

Działanie dodawania w grupie przemiennej E ma następujące własności:
1. jeśli $P \in E$ i $Q \in E$, to $P + Q \in E$,
2. $P + Q = Q + P$,
3. $(P + Q) + R = P + (Q + R)$,
4. istnieje taki punkt $O \in E$, że $P + O = P$ dla każdego $P \in E$,
5. dla każdego $P \in E$ istnieje taki punkt $-P \in E$, że $P + (-P) = O$.

Warto wspomnieć, że punkty krzywej eliptycznej można również dość łatwo reprezentować w komputerze (za pomocą ich współrzędnych, tzn. jako pary liczb) oraz że działanie dodawania jest opisane stosunkowo prostymi wzorami, a więc czas wykonania działania dodawania dwóch punktów przez komputer nie jest bardzo długi.

Te własności krzywych eliptycznych pozwalają wykorzystać je w kryptografii. Spróbujmy zatem popatrzeć, jak można wykorzystać dowolną grupę E do szyfrowania. Częstym problemem, z jakim muszą zmierzyć się osoby korespondujące w sposób tajny, jest przesłanie klucza. Jeśli, na przykład, osoba A często wysyła do osoby B zaszyfrowane komunikaty i każdy z tych komunikatów szyfruje za pomocą innego klucza (a w przypadku wielu systemów kryptograficznych jest to niezbędny warunek bezpieczeństwa), to osoba B musi równie często przesyłać osobie A klucze używane do szyfrowania. Oczywiście, osoba A mogłaby sama tworzyć te klucze, ale musiałaby przesyłać je osobie B w sposób całkowicie bezpieczny – tylko po co wtedy całe to szyfrowanie, jeśli można po prostu przesłać w ten bezpieczny sposób każdy list? Na ogół jednak jest tak, że używamy szyfrowania wtedy, gdy nie jesteśmy w stanie przesłać bezpiecznie wiadomości w żadną stronę i osoba B nie będzie mogła przesłać kluczy osobie A. Co w takim razie zrobić? Odpowiedzią może być zastosowanie metody wymiany klucza Diffiego i Hellmana, opracowanej w 1976 roku, pozwalającej ponadto na jednakowy wpływ osoby A i B na tworzenie klucza.

Osoby A i B uzgadniają wspólnie pewną grupę E i wybierają element $P \in E$. Mogą to zrobić jawnie. Następnie osoba A wybiera dowolną liczbę naturalną a i osoba B wybiera liczbę b. Te liczby są wybierane w sposób tajny i nieujawniane nikomu. Następnie osoba A tworzy element $a \cdot P$ grupy E (używamy tu oczywistego skrótu: $2 \cdot P = P + P$, $3 \cdot P = P + P + P$ itd.) i podobnie osoba B tworzy element $b \cdot P$. Teraz osoby A i B wysyłają do siebie tak utworzone elementy. Na końcu osoby A i B tworzą element $Q = a \cdot b \cdot P$. Każda z nich ma wystarczającą ilość informacji potrzebnych do tego: osoba A zna liczbę a i element $b \cdot P$, osoba B zna liczbę b i element $a \cdot P$.

Na ogół wybiera się bardzo dużą grupę E, np. mającą około 10^{100} elementów i odpowiednio duże liczby a i b.

Mimo tego, że te liczby są bardzo duże, istnieją sposoby pozwalające dość szybko wyznaczyć element $a \cdot P$. Teraz cała korespondencja między osobami A i B może odbywać się w sposób jawny. Każdy będzie znał grupę E, element P oraz elementy $a \cdot P$ i $b \cdot P$. Nie będzie jednak mógł poznać elementu $a \cdot b \cdot P$. Do tego, gdyby chciał powtórzyć postępowanie którejś z osób A i B, musiałby poznać jedną z liczb a i b, a te liczby są przecież trzymane w tajemnicy! Okazuje się, że nie znamy dotychczas żadnej wystarczająco szybkiej metody obliczania liczby a, gdy znane są elementy P i $a \cdot P$. Podobnie nie znamy żadnej wystarczająco szybkiej metody wyznaczania $a \cdot b \cdot P$, gdy znane są $a \cdot P$ i $b \cdot P$. Na tym polega bezpieczeństwo tej metody wymiany klucza.

Żeby szybko wyznaczyć element $a \cdot P$, obliczamy elementy

$$2 \cdot P,\ 4 \cdot P,\ 8 \cdot P,\ \ldots,\ 2^n \cdot P$$

dla takiej liczby n, by $2^{n+1} > a$. Następnie dodajemy pewne z tak wyznaczonych elementów (w zależności od postaci rozkładu dwójkowego liczby a), otrzymując $a \cdot P$. Jeśli, na przykład, chcemy wyznaczyć element $11 \cdot P$, to obliczamy $2 \cdot P$, $4 \cdot P$ i $8 \cdot P$, a następnie dodajemy $8 \cdot P$, $2 \cdot P$ i P: bowiem

$$11 = 8 + 2 + 1 = 2^3 + 2^1 + 2^0.$$

Ta metoda obliczania wielokrotności elementu P jest bardzo szybka: wymaga liczby dodawań równej co najwyżej podwojonej liczbie cyfr w rozwinięciu dwójkowym liczby a.

Teraz, gdy obie osoby A i B wspólnie stworzyły tylko im znany sekret, mogą wykorzystać go w taki sam, wcześniej uzgodniony, sposób do stworzenia klucza szyfrującego. Można powiedzieć, że element $a \cdot b \cdot P$ grupy E jest tym kluczem. System wymiany klucza Diffiego i Hellmana został stworzony dla grupy reszt z dzielenia przez dużą liczbę pierwszą p z działaniem mnożenia, ale, oczywiście, może być zastosowany do dowolnej grupy. Warunkiem jest to, by grupa była duża (a dokładniej, by istniały takie elementy P, że jest dużo różnych elementów postaci P, $2P$, $3P$ itd. – mówimy wtedy, że element P ma duży rząd). Oczywiście, wszystkie te działania muszą być wykonywane za pomocą komputera, więc elementy grupy muszą się dawać łatwo reprezentować i działanie grupowe musi być wykonywane łatwo i szybko. Grupy punktów krzywych eliptycznych mają te wszystkie własności i dlatego już dość dawno (w końcu lat osiemdziesiątych) dostrzeżono ich zalety kryptograficzne.

Wielką zaletą krzywych eliptycznych jest to, że jest ich bardzo dużo. Można się obawiać, że systemy kryptograficzne wykorzystujące wyłącznie grupę reszt z dzielenia przez p z działaniem mnożenia zostaną kiedyś złamane. Ta grupa ma stosunkowo najlepiej poznaną strukturę i dlatego najbardziej możemy się obawiać o bezpieczeństwo systemów wykorzystujących ją. Różnych rodzajów krzywych eliptycznych jest bardzo wiele i możemy mieć nadzieję, że będzie znacznie trudniej znaleźć jakąś metodę ogólną pozwalającą złamać wszystkie systemy kryptograficzne wykorzystujące te krzywe.