

## Dowody o wiedzy zerowej

**Dowody o wiedzy zerowej** (inaczej: dowody z wiedzą zerową, protokoły wiedzy zerowej, z ang. zero-knowledge proofs, zero-knowledge protocols) to takie procedury kryptograficzne, za pomocą których udowadniamy fakt posiadania pewnej informacji, bez ujawniania jej. Innymi słowy: wykazujemy prawdziwość pewnego stwierdzenia bez ujawniania niczego poza tą prawdziwością.

### Przykład 1.

Peggy twierdzi, że zna hasło do sejfów jej rodziców. Victor nie daje temu wiary i prosi ją o udowodnienie tego faktu. Peggy przedstawia mu te hasła. Ale teraz zna je też Victor i może wykorzystać w nieuczciwych celach.

Niestety jedynym sposobem na udowodnienie faktu posiadania tej informacji jest jej przedstawienie.



## Przykład 2b.

Założmy teraz, że Victor ma kamerę i nagrywa wszystko, co widzi. Rejestruje to, jak Peggy znika w jaskini; rejestruje to, co krzyczy do Peggy, gdy żąda by wyszła z jaskini; oraz moment, kiedy Peggy z niej wychodzi. W ten sposób zapisuje na taśmie wszystkie  $n$  prób.

Postawmy pytanie: Czy jeśli pokaże ten zapis Carol, to na podstawie filmu uwierzy ona, że Peggy zna tajemne hasło?

Na pewno nie. Peggy i Victor mogli przecież ustalić wcześniej kolejność poleceń wydawanych przez Victora, lub w innym wypadku zmontować film z udanych prób odgadnięcia polecenia Victora przez Peggy (gdy nie zna ona zaklęcia).

Victor nie może więc przekonać trzeciej strony o poprawności dowodu.

**Dowód o wiedzy zerowej** musi spełniać trzy warunki:

1. **Zupełność** – jeśli twierdzenie jest prawdziwe, uczciwy weryfikator (czyli taki, który postępuje dokładnie według protokołu) zostanie przekonany o tym fakcie przez uczciwą osobę udowadniającą.
2. **Słuszność** – jeśli twierdzenie jest fałszywe, nieuczciwa (oszukująca) osoba udowadniająca nie przekona weryfikatora o jego prawdziwości, poza przypadkiem, gdy „dopisze jej szczęście” (jednak z minimalnym prawdopodobieństwem).
3. **Wiedza zerowa** – jeśli twierdzenie jest prawdziwe, nieuczciwy weryfikator nie dowie się na jego temat nic więcej poza tym faktem. W dodatku każdy nieuczciwy weryfikator może zasymulować protokół, który będzie wyglądał jak interakcja między udowadniającym a weryfikatorem.

Badania nad dowodami o wiedzy zerowej zostały prowadzone przede wszystkim na potrzeby systemów uwierzytelniania. Przy uwierzytelnianiu jedna strona chce udowodnić drugiej swoją tożsamość przy pomocy jakiejś tajnej informacji (np. hasła), ale nie chce, by ta druga dowiedziała się czegokolwiek na jej temat.

Dowody wiedzy zerowej nie są dowodami w ścisłym matematycznym sensie. Zawsze istnieje bowiem minimalna szansa (*błąd słuszności*), że nieuczciwa osoba udowadniająca przekona weryfikatora o fałszywym twierdzeniu. Istnieją jednak techniki zmniejszające ten błąd do tak niskich wartości, że można je pominąć.

## Izomorfizm grafowy

Grafy  $G_1$  i  $G_2$  nazywamy izomorficznymi, jeżeli istnieje bijekcja zbioru wierzchołków grafu  $G_1$  na zbiór wierzchołków grafu  $G_2$ , która zachowuje strukturę grafu (krawędzie). Wiemy, że dla skrajnie dużych grafów stwierdzenie, czy dwa dane grafy są izomorficzne, zajęłoby wieki pracy komputera (jest to problem NP-zupełny).

Przy pomocy izomorfizmu grafów także można przedstawić dowód o wiedzy zerowej. Zakładamy, że Peggy zna izomorfizm między grafami  $G_1$  i  $G_2$ . Oto, jaki protokół przekona Victora co do wiedzy Peggy:

1. Peggy dokonuje losowej permutacji wierzchołków grafu  $G_1$  i w ten sposób tworzy graf  $H$  izomorficzny do  $G_1$ . Ponieważ zna izomorfizm pomiędzy  $G_1$  a  $H$ , zna izomorfizm pomiędzy  $H$  a  $G_2$ . Dla każdej innej osoby znalezienie izomorfizmu pomiędzy  $G_1$  a  $H$  albo  $H$  a  $G_2$  jest równie trudne co znalezienie izomorfizmu pomiędzy  $G_1$  a  $G_2$ .
2. Peggy przekazuje Victorowi kopię grafu  $H$ .
3. Victor żąda od niej wykonania jednej z dwóch rzeczy:
  - a) udowodnienia, że  $G_1$  i  $H$  są izomorficzne, albo
  - b) udowodnienia, że  $H$  i  $G_2$  są izomorficzne.
4. Peggy wykonuje polecenie. Robi jedną z dwóch rzeczy:
  - a) udowadnia, że  $G_1$  i  $H$  są izomorficzne bez udowadniania, że  $H$  i  $G_2$  są izomorficzne; albo
  - b) udowadnia, że  $H$  i  $G_2$  są izomorficzne bez udowadniania, że  $G_1$  i  $H$  są izomorficzne.
5. Peggy i Victor powtarzają kroki 1.-4.  $n$ -krotnie.

Jeśli Peggy nie zna izomorfizmu pomiędzy  $G_1$  i  $G_2$ , to nie utworzy grafu  $H$  izomorficznego z oboma grafami. Może jedynie utworzyć taki, który jest izomorficzny albo z jednym albo z drugim. Ma więc wtedy tylko 50% szans w każdym cyklu na odgadnięcie tego, którego dowodu zażąda Victor w kroku 3.

Protokół ten nie zdradza Victorowi żadnej informacji, potrzebnej do znalezienia izomorfizmu pomiędzy  $G_1$  a  $G_2$ . Peggy generuje graf  $H$  w każdym cyklu protokołu, nie istnieje więc żadna taka informacja, którą Victor może uzyskać nawet po kilku cyklach. Nawet dzięki wielu odpowiedziom Peggy nie odnajdzie on izomorfizmu pomiędzy  $G_1$  a  $G_2$ .

W każdym cyklu Victor otrzymuje nową permutację losową  $H$  wraz z izomorfizmem między  $G_1$  lub  $G_2$ . Równie dobrze może je wygenerować osobiście. Ponieważ może on utworzyć symulację protokołu, można dowiedzieć, że jest dowodem o wiedzy zerowej.

### Cykle Hamiltona

Cykl Hamiltona to taki cykl w grafie, w którym występuje każdy wierzchołek grafu i występuje jeden raz.

Znalezienie cyklu Hamiltona dla grafu jest kolejnym „trudnym problemem”.

Peggy zna cykl Hamiltona w grafie  $G$ , Victor zna  $G$ , ale nie zna cyklu Hamiltona. Peggy chce mu udowodnić, że zna cykl, bez jego ujawniania. Istnieje protokół, dzięki któremu tego może dokonać.

**Przedstawione** dowody wiedzy zerowej zawierały n wymian informacji między Peggy i Victorem. Można stworzyć takie protokoły, które będą je wykonywały równolegle. Dla nich jednak zapis protokołu jest niewygodny do symulacji, dalej jednak są to dowody o wiedzy zerowej.

**Aby** przekonać osobę trzecią, należy użyć niekonwersacyjnego dowodu o wiedzy zerowej (poprzednie były konwersacyjne). Te dowody nie wymagają konwersacji, przykładowo Peggy mogłaby je opublikować i tym samym dowiedzieć prawdziwości twierdzenia. Protokół taki podobny jest do wspomnianego przed chwilą dowodu równoległego, rolę Victora odgrywa funkcja jednokierunkowa (spełniająca rolę bezstronnego losowego generatora bitowego). Aby Peggy mogła oszukać, musiałaby przewidzieć wynik takiej funkcji. Nie ma bowiem żadnego sposobu, aby Peggy mogła wymusić na funkcji wygenerowanie określonych bitów, albo odgadnąć jaki ciąg bitów ona wytworzy.

W takim protokole musi wystąpić znacznie więcej cykli związanych z sekwencją zapytanie/odpowiedź. W protokole konwersacyjnym wykonanie 10 iteracji (prawdopodobieństwo  $1/1024$ , że Peggy oszukuje) jest świetnym zabezpieczeniem. W przypadku niekonwersacyjnego to nie wystarcza. Potrzebuje 64 lub 128 iteracji, aby uznać go za poprawny.

Ten protokół może być stosowany do schematów podpisów cyfrowych.

**Manuel Blum** udowodnił, że dowolne twierdzenie matematyczne może być przekształcone w graf w taki sposób, że dowód tego twierdzenia jest równoważny z drogą hamiltona w grafie. Przy zastosowaniu dobrej jakości funkcji jednokierunkowych i algorytmów szyfrujących dowolny dowód matematyczny może być przekształcony w dowolny dowód o wiedzy zerowej. Za pomocą tego można dowiedzieć, że zna się dowód konkretnego twierdzenia bez ujawniania jaki to jest dowód.

### Klasyfikacja dowodów o wiedzy zerowej:

**doskonałe** – istnieje przekształcenie (symulator), które umożliwia uzyskanie zapisów identycznie rozproszonych jak rzeczywiste (przykłady – cykl Hamiltona i izomorfizm grafów),

**statystyczne** - istnieje przekształcenie (symulator), które umożliwia uzyskanie zapisów identycznie rozproszonych jak rzeczywiste oprócz pewnej stałej liczby wyjątków,

**obliczeniowe** - istnieje przekształcenie (symulator), które umożliwia uzyskanie zapisów nieodróżnialnych od rzeczywistych,

**nieformalne** – przekształcenie (symulator) może nie istnieć, ale możemy dowiedzieć, że weryfikator nie uzyska żadnej wiedzy z dowodu (przykład dowodu równoległego).

Źródła:

Bruce Schneier - "Kryptografia dla praktyków", Wydawnictwa Naukowo-Techniczne 2002

Wikipedia