# Schemat podpisu cyfrowego z wykorzystaniem heurystyki Fiata Shamira

Temat polega na wybraniu problemu NP i następnie wykorzystanie go w schemacie podpisu cyfrowego. Należy znaleźć dowód o wiedzy zerowej dla danego problemu, a następnie zastosować heurystykę Fiata-Shamira. W tej pracy został wybrany problem znadywania pierwiastka reszty kwadratowej modulo złożona liczba. Pierwiastkiem kwadratowym jest liczba całkowita x, dla której istnieje całkowite rozwiazanie równania kongruencyjnego:

$x^2 \equiv$ a (mod n), gdzie $n = p * q$, dla liczb pierwszych p oraz q.

Problem znajdywania pierwiastka kwadratowego modulo liczba złożona n, uznawany jest za równoważny problemowi faktoryzacji liczby n, który jest w klasie NP.

## 1 Podpisy cyfrowe

Podpisy cyfrowe są matematycznym sposobem zapewnienia autentyczności przesyłanych wiadomości oraz dokumentów. Mają na celu:

- uwierzytelnienie oraz potwierdzenie tożsamości autora wiadomości,
- zapewnienie niezaprzeczalności, że to dany autor nadał wiadomość,
- zapewnienie integralności danych, przez co jakakolwiek modyfikacja wiadomości zostanie wykryta.

Schemat podpisu cyfrowego zwykle składa się z 3 algorytmów:

- generacji kluczy, prywatnego i publicznego,
- algorytmu podpisującego, który produkuje podpis na podstawie wiadomości oraz klucza prywatnego,
- algorytmu weryfikującego, który za pomocą klucza publicznego i wiadomości potwierdza, bądź odrzuca autentyczność wiadomości.

## 2 Dowody o wiedzy zerowej

Dowód o wiedzy zerowej jest jest procedurą, w której jedna ze stron jest w stanie udowodnić drugiej, że posiada pewną tajną informację, bez zdradzania jakichkolwiek informacji, które mogłyby wpłynąć na ujawnienie treści sekretu. Każdy dowód o wiedzy zerowej musi spełniać trzy własności:

- kompletność: jeżeli zdanie jest prawdziwe, uczciwy weryfikator będzie przekonany tym faktem przez uczciwą osobę udowadniającą.
- solidność: jeżeli zdanie jest fałszywe, weryfikator akceptuje zdanie z prawdopodobieństwem $\leqslant 1/2$.
- wiedza zerowa: jeżeli zdanie jest prawdziwe, weryfikator nie dowie się niczego poza tym, że osoba udowadniająca mówi prawdę. Możliwe jest stworzenie symulatora, który potrafi sporządzić transkrypt interakcji między uczciwą osobą udowadniającą, a weryfikatorem.

## 2.1 Schemat dowodu o wiedzy zerowej

**Publiczne dane:** x, n.
**Prywatne dane (Alicji):** s, takie że x = $s^2$ (mod n).
**P → V:** Alicja wybiera losową liczbę r ∈ $Z_n^*$ i wysyła y = $r^2$ (mod n) do Boba.
**P ← V:** Bob wybiera losowo b ∈ {0, 1} i wysyła do Alicji.
**P → V:** Jeżeli b = 0, Alicja wysyła r do Boba, jeżeli b = 1 wysyła $w * r$ (mod n).
**Weryfikacja:** Niech z oznacza liczbe wysłaną przez Alicję w ostatnim kroku. Bob akceptuje dowód w przypadku b = 0, jeśli $z^2$ = y (mod n). W przypadku b = 1, Bob akceptuje dowód, jeśli $z^2$ = xy (mod n).

1. Kompletność.
Jeżeli x ∈ $QR_n$, a Alicja posiada s, takie, że x = $s^2$ (mod n) oraz Alicja i Bob postępują zgodnie z protokołem, to Bob zaakceptuje dowód z prawdopodobieństwem 1.

2. Solidność.
Jeżeli x ∉ $QR_n$, wtedy niezależnie od tego co zrobi Alicja, Bob odrzuci dowód z prawdopodobieństwem przynajmniej 1/2.
Załóżmy, że x ∉ $QR_n$. Wtedy nie jest możliwe, aby y oraz y*x były naraz resztami kwadratowymi. Jeżeli y = $u^2$ (mod n) oraz $w^2$ = y *x, wtedy x = $w^2(y^-1)^2$ (mod n). Sprzeczność.

3. Wiedza zerowa.
Można stworzyć następującą symulację:

1. **Dane wejściowe:** x, n takie, że x ∈ $QR_n$.
2. Wybranie losowo b' ∈ {0, 1}.
3. Wybranie losowo z ∈ $QR_n$.
4. Jeżeli b' = 0, obliczenie y = $z^2$. W przeciwnym wypadku obliczenie y = $z^2x^{-1}$.
5. Symulacja losowości weryfikatora. Wybranie losowo b ∈ {0, 1}.
6. Jeżli b = b' to zwrócenie $< y, z >$. W przeciwnym przypadku powrót do punktu 2.

# 3 Podpis cyfrowy z heurystyką Fiata-Shamira

Niech I - identyfiaktor Alicji(np. jej nazwisko), m - wiadomość do podpisania, f - funkcja hashująca.

## 3.1 Generowanie sekretu s, takiego że x = $s^2$ (mod n)

1. Obliczenie wartości $v_j$ = f(I, j) dla małych wartości j.
2. Wybranie k różnych wartości j, dla których $v_j$ jest resztą kwadratową (mod n) i obliczenie najmniejszego pierwiastka kwadratowego $s_j$ z liczby $v_j^{-1}$ (mod n), gdzie $v_j^{-1}$ to odwrotność $v_j$ modulo n.

Odwrotność $v_j$ modulo n, można obliczyć przy pomocy rozszerzonego algorytmu Euklidesa, o ile NWD($v_j$, n) = 1.

Znając rozkład n = p*q, gdzie p, q to liczby pierwsze, możliwe jest wyznaczenie najmniejszego pierwiastka kwadratowego $s_j$ (mod n). Załóżmy, że p = 3 (mod 4). Wtedy liczba a ∈ $Z_p^*$ jest resztą kwadratową, jeśli 1 = $J_p(a) = a^{\frac{p-1}{2}}$ mod p. $J_p(a)$ jest symbolem Legendre'a. Jeśli $J_p(a) = 1$, to liczba a jest resztą kwadratową, jeśli 0 to a jest wielokrotnością p, jeśli -1 to to nie istnieje żadne b, takie że $b^2$ = a (mod p).

Jeśli powyższe warunki są spełnione można obliczyć pierwiastki kwadratowe a, za pomocą formuły $s_{p1}$ = SQR(a) = $a^{\frac{p+1}{4}}$ mod p. Drugi pierwiastek posiada przeciwny znak. Analogicznie należy postępować, aby znaleźć pierwiastki kwadratowe a mod q.

Posiadając równania:
x ≡ $s_{p1}$ (mod p)
x ≡ $s_{p2}$ (mod p)
x ≡ $s_{q1}$ (mod q)
x ≡ $s_{q2}$ (mod q)

Przy pomocy chińskiego twierdzenia o resztach możliwe jest wyznaczenie najmniejszego pierwiastka kwadratowego mod n.

### 3.2 Podpis wiadomości m

1. Alicja wybiera losowe $r_1, ..., r_t \in [0, n)$ i oblicza $x_i = r_i^2$ (mod n).

2. Alicja oblicza f(m, $x_1, ..., x_t$) i używa pierwsze $kt$ bitów hashu jako wartości $e_{ij}$, gdzie ($1 \leqslant i \leqslant t$, $1 \leqslant j \leqslant k$).

3. Alicja oblicza $y_i = r_i \prod_{e_{ij}=1} s_j$ (mod n) dla i = 1, ..., t

i publikuje I, m, $e_{ij}$, $y_i$.

### 3.3 Weryfikacja wiadomości m

1. Bob oblicza $v_j$ = f(I, j) dla j = 1, ..., k.

2. Bob oblicza $z_i = y_i^2 \prod_{e_{ij}=1} v_j$ (mod n) for i = 1, ..., t.

3. Bob weryfikuje że pierwsze $kt$ bitów f(m, $z_1, ..., z_t$) to $e_{ij}$.

Z definicji:

$z_i = y_i^2 \prod_{e_{ij}=1} v_j = r_i^2 \prod_{e_{ij}=1} (s_j^2 v_j) = r_i^2 = x_i$(mod n), więc f(m, $z_1, ..., z_t$) = f(m, $x_1, ..., x_t$).

## 4 Atak na protokół

Możliwy jest atak na protokół, poprzez losowe wygenerowanie macierzy y oraz v, a następnie zgadywanie kolejnych możliwych macierzy $e_{ij}$. Atak działa dla dowolnej wiadomości m. Prawdopodobieństwo podrobienia podpisu wynosi T * $2^{-kt}$, gdzie T to ilość prób zgadniecia odpowiedniej macierzy $e_{ij}$.

Wynik ataku dla przykładowych parametrów:

Dla parametrów t = 3, k = 4 oraz 1000 pełnych przeszukań wszystkich możliwości macierzy $e_{ij}$ dla losowo wygenerowanych macierzy y oraz v, algorytmowi udało się podrobić podpis w 62.5% przypadków, średnia potrzebna ilość zgadnięć macierzy $e_{ij}$ w przypadku poprawnego podrobienia podpisu wynosiła: 979 na 4096 możliwych.