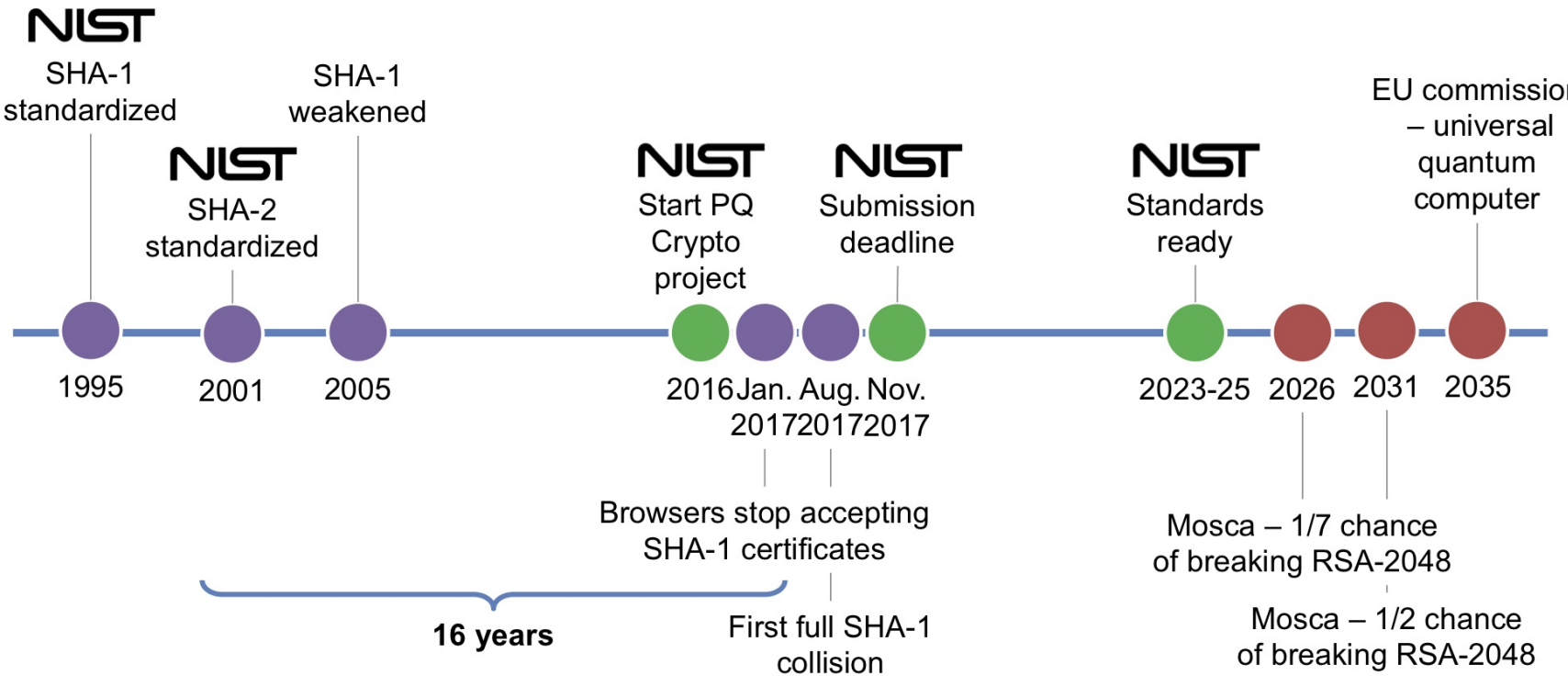
Post-kwantowy algorytm podpisu cyfrowego Kryptosystem NTRU

Janusz Szmidt, Marcin Barański

Wojskowy Instytut Łączności

13 XII 2018

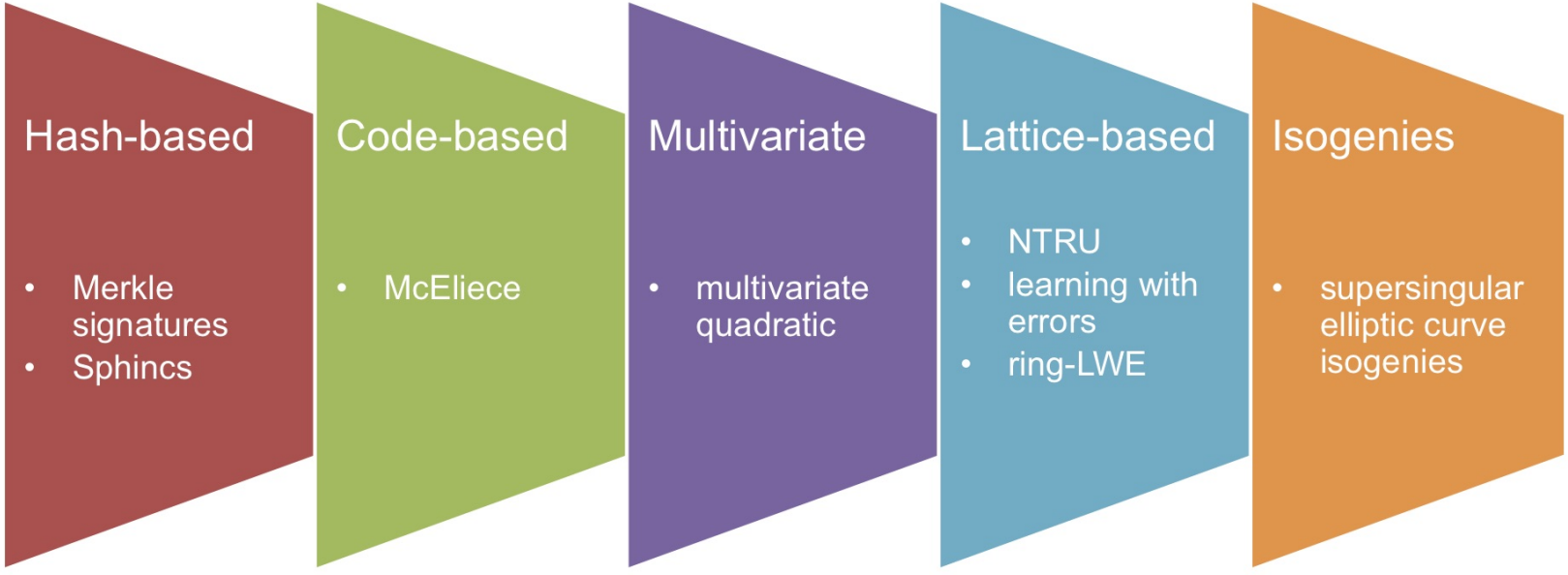
Timeline


NIST
SHA-1 standardized
1995
NIST
SHA-2 standardized
2001
SHA-1 weakened
2005
16 years
NIST
Start PQ Crypto project
2016
Jan. 2017
Browsers stop accepting SHA-1 certificates
Aug. 2017
First full SHA-1 collision
NIST
Submission deadline
Nov. 2017
NIST
Standards ready
2023-25
2026
Mosca – 1/7 chance of breaking RSA-2048
2031
Mosca – 1/2 chance of breaking RSA-2048
EU commission – universal quantum computer
2035

Post-quantum crypto

a.k.a. quantum-resistant algorithms

Classical crypto with no known exponential quantum speedup



NTRU - abstract

- We describe NTRU, a new public key cryptosystem. NTRU features resonably short, easly created keys, high speed, and low memory requirements.
- NTRU encryption and decryption use a mixed system suggested by polynomial algebra combined with a clustering principle based on elementary probability theory.
- The security of the NTRU cryptosysyem comes from the iteraction of the polynomisl mixing system with the independence of reduction modulo two relatively prime integers p and q.

Pierścienie wielomianów

- Z - pierścień liczb całkowitych
- $Z[x]$ - pierścień wielomianów o współczynnikach całkowitych
- q - liczba pierwsza
- Z_q - zbiór reszt modulo q
  $Z_q = \{0, \ldots, q-1\}$ - ciało q-elementowe
- $Z_q[x]$ - pierścień wielomianów o współczynnikach z ciała Z_q
- N - liczna naturalna
- $R = Z[x]/(x^N - 1)$ - pierścień ilorazory wielomianów splotowych rzędu N (convolution polynomials of rank N)
- $R_q = Z_q[x]/(x^N - 1)$ - pierścień ilorazory wielomianów splotowych rzędu N modulo q (convolution polynomials of rank N modulo q)

Pierścienie wielomianów

- Wielomian

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{N-1} x^{N-1} \quad \mathrm{R}$$

będziemy identyfikowali z wektorem współczynników

$$(a_0, a_1, a_2, \ldots, a_{N-1}) \quad \mathrm{Z}^N$$

- Dodawaniu wielomianów odpowiada dodawanie wektorów

$$a(x) + b(x) \leftrightarrow (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_{N-1} + b_{N-1})$$

- Iloczyn dwóch wielomianów jest dany wzorem

$$a(x) \quad b(x) = c(x) \quad \text{gdzie} \quad c_k = \square \quad a_i b_{k-i},$$

$$i+j=k \ \mathrm{mod}\ N$$

Pierścienie wielomianów

Definicja 1
Niech $a(x)$ R_q. Centrycznym podniesieniem (*centered lift*) wielomianu $a(x)$ do R jest jedyny wielomian $a\,(x)$ R spełniający:

$$a\,(x)\ mod\ q = a(x)$$

którego współczynniki wybrane są z przedziału

$$-\frac{q}{2} < a_i \quad \frac{q}{2}$$

Np. Jeśli $q = 2$ to *centered lift* $a\,(x)$ wielomianu $a(x)$ jest wielomianem binarnym.

Pierścienie wielomianów

Definicja 2

Niech $a(x)$ R_q. Multiplikatywną odwrotnością wielomianu $a(x)$ nazywamy wielomian $a^{-1}(x)$ R_q taki, że $x(x)$ $a^{-1}(x) = 1$ w pierścieniu R_q, tzn.

$$a(x)a^{-1}(x) = 1 \; mod \; (x^N - 1).$$

Stwierdzenie 1

Niech q będzie liczbą pierwszą. Wielomian $a(x)$ R_q ma multiplikatywną odwrotność w pierścieniu R_q wtedy i tylko wtedy gdy

$$gcd(a(x), x^N - 1) = 1 \;\; \text{w} \;\; R_q.$$

Kryptosystem NTRU - Jaffrey Hoffstein, Jill Pipher, Joseph Silverman - 1996

Definicja 3

Dla liczb naturalnych d_1, d_2 definiujemy zbiór wielomianów $a(x) \quad R$, które spełniają:

$$T(d_1, d_2) = \begin{cases} a(x) \text{ ma } d_1 \text{ współczynników równych } 1, \\ a(x) \text{ ma } d_2 \text{ współczynników równych } -1, \\ a(x) \text{ ma pozostałe współczynniki równe } 0. \end{cases}$$

Wielomiany te nazywamy *trójkowymi*, w analogii do wiemianów binarnych.

Kryptosystem NTRU - specyfikacja

Generacja kluczy:

- Zaufana trzecia strona wybiera zestaw parametrów (N, p, q, d), gdzie N, p są liczbami pierwszymi, $gcd(p, q) = gcd(N, q) = 1$ oraz $q > (6d + 1)p$.
- Niech R, R_p, R_q oznaczają wprowadzone powyżej pierścienie wielomianów.
- Klucz prywatny Alicji to dwa losowo wybrane wielomiany:

$$f(x) \quad T(d+1, d), \quad g(x) \quad T(d, d).$$

- Alicja oblicza odwrotności wielomianów:

$$F_q(x) = f^{-1}(x) \bmod q \quad R_q \text{ oraz } F_p(x) = f^{-1}(x) \bmod p \quad R_p.$$

Kryptosystem NTRU - specyfikacja

- Jeśli któraś z odwrotności nie istnieje, to Alicja wybiera inne $f(x) \quad T(d+1, d)$ i sprawdza istnieie odwrotności.
- Żaden element z $T(d, d)$ nie ma odwrotności (dowód !), stąd wybierane jest $f(x) \quad T(d+1, d)$.
- Kluczem prywatnym Alicji potrzebnym do deszyfrowania jest para $(f(x), F_p(x))$. Alicja może zachować tylko $f(x)$ i obliczać $F_p(x)$ kiedy potrzebuje.
- Kluczem publicznym Alicji jest wielomian

$$h(x) = F_q(x) \quad g(x) \quad \text{w} \quad R_q.$$

Kryptosystem NTRU - specyfikacja

Szyfrowanie:

- Tekstem jawnym Boba jest wielomian $m(x) \quad R$, którego współczynniki są zawarte miądzy $-\frac{p}{2}$ a $\frac{p}{2}$. Czyli $m(x)$ jest wielomianem w R, który jest *central lift* wielomianu z R_p.
- Bob wybiera losowo wielomian (*klucz ulotny - ephemeral key*) $r(x) \quad T(d, d)$ i oblicza szyfrogram

$$e(x) = ph(x) \quad r(x) + m(x) \ mod \ q,$$

który jest elementem pierścienia R_q.

Kryptosystem NTRU - specyfikacja

Deszyfrowanie:

- Alicja zaczyna proces deszyfrowania obliczając

$$a(x) = f(x) \quad e(x) \ mod \ q.$$

- Następnie podnosi centrycznie $a(x)$ do elementu z R i oblicza

$$b(x) = F_p(x) \quad a(x) \ mod \ p.$$

Stwierdzenie 2

Jeśli parametry (N, p, q, d) kryptosystemu NTRU spełniają warunek

$$q > (6d + 1)p$$

to wielomian $b(x)$ równy jest tekstowi jawnemu $m(x)$.

Public Parameter Creation	
A trusted party chooses public parameters (N, p, q, d) with N and p prime, $\gcd(p, q) = \gcd(N, q) = 1$, and $q > (6d + 1)p$.	
Alice	**Bob**
Key Creation	
Choose private $\mathbf{f} \in \mathcal{T}(d + 1, d)$ that is invertible in R_q and R_p. Choose private $\mathbf{g} \in \mathcal{T}(d, d)$. Compute $\mathbf{F}_q$, the inverse of $\mathbf{f}$ in R_q. Compute $\mathbf{F}_p$, the inverse of $\mathbf{f}$ in R_p. Publish the public key $\mathbf{h} = \mathbf{F}_q \star \mathbf{g}$.	
Encryption	
	Choose plaintext $\mathbf{m} \in R_p$. Choose a random $\mathbf{r} \in \mathcal{T}(d, d)$. Use Alice's public key $\mathbf{h}$ to compute $\mathbf{e} \equiv p\mathbf{r} \star \mathbf{h} + \mathbf{m} \pmod{q}$. Send ciphtertext $\mathbf{e}$ to Alice.
Decryption	
Compute $\mathbf{f} \star \mathbf{e} \equiv p\mathbf{g} \star \mathbf{r} + \mathbf{f} \star \mathbf{m} \pmod{q}$. Centerlift to $\mathbf{a} \in R$ and compute $\mathbf{m} \equiv \mathbf{F}_p \star \mathbf{a} \pmod{p}$.	

NTRU - przykład

- Parametry publiczne

$$(N, p, q, d) = (7, 3, 41, 2).$$

- Spełniony jest warunek

$$41 = q > (6d + 1)p = 39,$$

co zapewnia poprawność deszyfrowania.

- Alicja wybiera

$$f(x) = x^6 - x^4 + x^3 + x^2 - 1 \quad T(3, 2),$$

$$g(x) = x^6 + x^4 - x^2 - x \quad T(2, 2).$$

NTRU - przykład

- Następnie oblicza odwrotności w R_q i w R_p:

$$F_q(x) = f^{-1}(x) \; mod \; q = 8x^6 + 26x^5 + 31x^4 + 21x^3 + 40x^2 + 2x + 37,$$

$$F_p(x) = f^{-1}(x) \; mod \; p = x^6 + 2x^5 + x^3 + x^2 + x + 1.$$

- Alicja zachowuje $(f(x), F_p(x))$ jako swój klucz prywatny.
- Alicja oblicza swój klucz publiczny jako element R_q

$$h(x) = F_q(x) \; g(x) = 20x^6 + 40x^5 + 2x^4 + 38x^3 + 8x^2 + 26x + 30.$$

- Bob decyduje się wysłać Alicji wiadomość

$$m(x) = -x^5 + x^3 + x^2 - x + 1.$$

- Bob wybiera losowo klucz ulotny

$$r(x) = x^6 - x^5 + x - 1.$$

NTRU - przykład

- Bob szyfruje wiadomość $m(x)$:

$$e(x) = pr(x) \quad h(x) + m(x) =$$

$$31x^6 + 19x^5 + 4x^4 + 2x^3 + 40x^2 + 3x + 25 \ mod \ q.$$

- W procesie deszyfrowania Alicja oblicza:

$$f(x) \quad e(x) = x^6 + 10x^5 + 33x^4 + 40x^3 + 40x^2 + x + 40 \ mod \ q.$$

- Następnie stosuje opercję *center lift* modulo q otrzymując:

$$a(x) = x^6 + 10x^5 - 8x^4 - x^3 - x^2 + x - 1 \quad R.$$

NTRU - przykład

- Z kolei Alicja redukuje $a(x)$ modulo p i oblicza

$$F_p(x) \quad a(x) = 2x^5 + x^3 + x^2 + 2^x + 1 \ mod \ p).$$

- W końcu stosuje operację *center lift* modulo p w celu odzyskania tekstu jawnego

$$m(x) = -x^5 + x^3 + x^2 - x + 1.$$

NTRU - kryptoanaliza

- Odzyskanie klucza w kryptosystemie NTRU można sformułować jako problem znalezienia najkrótszego wektora w kratach specjalnego typu.
- Odzyskanie tekstu jawnego w NTRU można sformułować jako problem znalezienia najbliższego wektora w pewnego typu kratach.
- Niech

$$h(x) = h_0 + h_1 x + \cdots + h_{N-1} x^{N-1}$$

będzie kluczem publicznym systemu NTRU. Tworzymy macierz M_h wymiaru $2N \times 2N$. Z macierzy M_h budujemy $2N$-wymiarową kratę L_h rozpiętą na wierszach tej macierzy.

NTRU - macierz M_h

$$M_{\mathbf{h}}^{\mathrm{NTRU}} = \left(\begin{array}{cccc|cccc} 1 & 0 & \cdots & 0 & h_0 & h_1 & \cdots & h_{N-1} \\ 0 & 1 & \cdots & 0 & h_{N-1} & h_0 & \cdots & h_{N-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & h_1 & h_2 & \cdots & h_0 \\ \hline 0 & 0 & \cdots & 0 & q & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & q & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & q \end{array}\right)$$

NTRU - kryptoanaliza

- Macierz M_h zapisujemy w skrócie jako

$$M_h = \begin{array}{cc} 1 & \mathbf{h} \\ 0 & qI \end{array}$$

gdzie $\mathbf{h}$ jest macierzą $N \times N$ cyklicznych permutacji współczynników wielomianu $h(x)$. M_h rozpatrujemy jako macierz wymiaru 2×2 o elementach z pierścienia R.

- Parę wielomianów

$$a(x) = a_0 + a_1 x + \cdots + a_{N-1} x^{N-1},\ b(x) = b_0 + b_1 x + \cdots + b_{N-1} x^{-1}$$

utożsamiamy z $2N$-wektorem

$$(a, b) = (a_0, a_1, \ldots, a_{N-1}, b_0, b_1, \ldots, b_{N-1}) \quad Z^{2N}.$$

NTRU - kryptoanaliza

Przypominamy, że klucz publiczny $h(x)$ był wygenerowany z wielomianów prywatnych $f(x), g(x)$.

Stwierdzenie 3

Załóżmy, że $f(x) \quad h(x) = g(x) \ mod \ q$. Niech $u(x) \quad R$ będzie wielomianem, który spełnia

$$f(x) \quad h(x) = g(x) + qu(x).$$

Wtedy

$$(f, -u)M_h = (f, g),$$

tzn. wektor (f, g) należy do NTRU kraty L_h.

Dowód

$$(f, -u) \begin{bmatrix} 1 & \mathbf{h} \\ 0 & qI \end{bmatrix} = (f, f \quad h - qu) = (f, g).$$

NTRU - kryptoanaliza

Stwierdzenie 4

Niech (N, p, q, d) będą parametrami NTRU, które spełniają

$$d \approx N/3, \quad q \approx 6d \approx 2N.$$

Niech L_h będzie NTRU kratą związaną z kluczem prywatnym (f, g). Wtedy

1. $det(L_h) = q^N$.
2. $||(f, g)|| \approx \sqrt{4d} \approx \sqrt{4N/3} \approx 1.155N$.
3. Heurystyka Gaussa przepowiada, że najkrótszy wektor w NTRU kracie L_h ma długość

$$\sigma(L_h) \approx \sqrt{Nq/\pi e} \approx 0.484N.$$

Zatem, jeśli N jest duże to jest znaczące prawdopodobieństwo, że najkrótszym wektorem w kracie L_h jest wektor (f, g) lub jego rotacje $x^k \quad f(x), x^k \quad g(x), \ 0 < k < N$.

NTRU - kryptoanaliza

- Stwierdzenie 4 mówi, że kryptoanalityk Ewa może znaleźć klucz prywatny Alicji jeśli znajdzie najkrótszy wektor w NTRU kracie L_h.
- Ogólniej, jeśli Ewa potrafi rozwiązać *apprSVP* w kracie L_h z dokładnością do czynnika aproksymacyjnego N^{ϵ} dla pewnego $< \frac{1}{2}$, wtedy najkrótszy wektor, który ona znajdzie, jest prawdopodobnie kluczen deszyfrującym.
- W celu znalezienia najkrótszych wektorów w kracie mamy do dyspozycji algorytm LLL i jego uogólnienie algorytm BKZ-LLL.
- Badania i eksperymenty przeprowadzone do roku 2003 stwierdzają, że wartości N w zakresie od 250 do 1000 odpowiadają poziomowi bezpieczeństwa algorytmów RSA, ElGamal i ECC.

Podpis cyfrowy NTRU

- W pierwszej kolejności Zaufana Trzecia Strona lub Samanta (podpisujący) wybierają odpowiednie parametry (N, q, d) dla systemu NTRU. Wybór oparty jest na teorii krat.
- Samanta wybiera losowo *tajne* wielomiany trójkowe $f(x), g(x) \quad T(d+1, d)$ i oblicza jej klucz publiczny (sprawdzający)

$$h(x) = f^{-1}(x) \quad g(x) \ mod \ q.$$

Konstrukcja ta podobna jest do szyfrowania w kryptosystemie NTRU.

Podpis cyfrowy NTRU

- W celu podpisania dokumentu $D = (D_1, D_2)$, gdzie $D_1, D_2 \quad R$, potrzebujemy wybranej wyżej pary f, g oraz obliczonej drugiej pary (F, G) spełniającej warunek

$$f(x) \quad G(x) - g(x) \quad F(x) = q \quad \text{oraz}$$

$$||F|| = O(N), \quad ||G|| = O(N).$$

  Dowodzi się, że taka para F, G istnieje.

- Samanta oblicza dwa wielomiany

$$v_1(x) = \quad (D_1(x) \quad G(x) - D_2(x) \quad F(x))/q$$

$$v_2(x) = \quad (-D_1(x)g(x) + D_2(x) \quad f(x))/q$$

  gdzie $p(x)$ oznacza wielomian $p(x)$, którego wszystkie współczyniki zostały zaokrąglone do najbliższych liczb całkowitych.

Podpis cyfrowy NTRU

- **Podpisem** dokumentu $D(x)$ jest wielomian

$$s(x) = v_1(x) \quad f(x) + v_2(x) \quad F(x).$$

- **Weryfikacja podpisu:**
  Victor bierze klucz publiczny Samanty $h(x)$ i oblicza

$$t(x) = h(x) \quad s(x) \ mod \ q \ .$$

  Następnie Victor sprawdza, że wektor (s, t) jest *'dostatecznie blisko'* wektora $D = (D_1, D_2)$.

Public Parameter Creation	
A trusted party chooses NTRU parameters (N, q, d)	
Samantha	**Victor**
Key Creation	
Choose ternary $\mathbf{f}, \mathbf{g} \in \mathcal{T}(d+1, d)$. Compute small $\mathbf{F}$ and $\mathbf{G}$ satisfying $\mathbf{f} \star \mathbf{G} - \mathbf{g} \star \mathbf{F} = q$ as described in Table 7.6. Compute $\mathbf{h} \equiv \mathbf{f}^{-1} \star \mathbf{g} \pmod{q}$. Publish verification key $\mathbf{h}$.	
Signing	
Choose document $\mathbf{D} = (\mathbf{D}_1, \mathbf{D}_2) \bmod q$. Compute $\mathbf{v}_1 = \lfloor (\mathbf{D}_1 \star \mathbf{G} - \mathbf{D}_2 \star \mathbf{F})/q \rceil$, $\mathbf{v}_2 = \lfloor (-\mathbf{D}_1 \star \mathbf{g} + \mathbf{D}_2 \star \mathbf{f})/q \rceil$. Compute $\mathbf{s} = \mathbf{v}_1 \star \mathbf{f} + \mathbf{v}_2 \star \mathbf{F}$. Publish signature $(\mathbf{D}, \mathbf{s})$.	
Verification	
	Compute $\mathbf{t} \equiv \mathbf{h} \star \mathbf{s} \pmod{q}$. Verify that $(\mathbf{s}, \mathbf{t})$ is close to $\mathbf{D}$.