ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2014
Seria: ORGANIZACJA I ZARZĄDZANIE z. 74 Nr kol. 1921

Jacek GRUBER, Dawid IWANICKI, Monika JACAK, Ireneusz J. JÓŹWIAK,
Piotr P. JÓŹWIAK, Jacek KOWALCZYK
Wydział Informatyki i Zarządzania
Politechnika Wrocławska

KRYTERIA BUDOWY KOMPUTERA KWANTOWEGO I ALGORYTMY KRYPTOGRAFII POSTKWANTOWEJ

Streszczenie. W artykule dokonano zwięzłego wprowadzenia do kryptografii postkwantowej. Wyjaśniono podstawowe pojęcia związane z tą dziedziną. Przyczyną rozwoju kryptografii postkwantowej jest zagrożenie wynikające z możliwości zbudowania komputera kwantowego dużej mocy. Zdefiniowano pojęcie komputera kwantowego i omówiono kryteria DiVincenzo konstrukcji takiego komputera. Przedstawiono cztery grupy algorytmów uważanych za odporne na ataki przy użyciu komputera kwantowego.

Słowa kluczowe: kryptografia postkwantowa, komputer kwantowy, podpis cyfrowy Merkle, algorytm McEliece, system NTRU, kryptosystem HFE.

QUANTUM COMPUTER CONSTRUCTION CRITERIA AND POST-QUANTUM CRYPTOGRAPHY ALGORITHMS

Summary. The article concise introduction to cryptography post-quantum. It explains the basic concepts related to the field. The reason for the development of cryptography is the threat posed by the possibility of building a quantum computer with high computing power. Defined the term "quantum computer". DiVincenzo criteria conditioning the possibility of constructing such a computer are discussed. Several groups of algorithms, which can be considered as resistant to attack by a quantum computer has been discussed.

Keywords: post-quantum cryptography, quantum computer, Merkle signature scheme, McEliece cryptosystem, NTRU public key cryptosystem, HFE cryptosystem.

1. Wprowadzenie

Zagrożenia wynikające ze zbudowania komputera kwantowego o dużej mocy są powodem rozwoju badań i kryptografii postkwantowej. Już obecnie istnieją takie algorytmy kwantowe, jak algorytm „poszukiwania igły w stogu siana" Grovera [2] lub algorytm faktoryzacji liczb Petera Shora [1], które są zagrożeniem dla kryptografii kwantowej. Używając komputera kwantowego o rozbudowanej architekturze i o wystarczającej mocy obliczeniowej, można znacznie skrócić czas potrzebny do rozwiązania wielu problemów matematycznych, na których opierają się powszechnie stosowane dziś kryptosystemy, np. RSA. Kryteria DiVincenzo określają warunki, jakie konstrukcja takiego urządzenia musi spełniać [4].

Z drugiej strony, znanych jest wiele algorytmów uważanych za odporne na ataki przy użyciu komputera kwantowego. Dla tych algorytmów nie podano dotychczas algorytmów kwantowych pozwalających na ich kompromitację, co jednak nie oznacza, że są one bezwzględnie bezpieczne. Algorytmy te można zaklasyfikować do czterech grup: algorytmy opierające się na funkcji haszującej, oparte na kodach liniowych, oparte na kratach oraz algorytmy opierające się na wielomianach drugiego stopnia o wielu zmiennych. Do każdej z grup algorytmów podano algorytm przykładowy wraz z opisem jego działania. Są to odpowiednio: system podpisu cyfrowego Merkle'a [8], algorytm McEliece'a [2, 3], asymetryczny system NTRU [6], a także kryptosystem publicznego klucza HFE [9, 10].

Kryptografia postkwantowa jest nową dziedziną, jednak ze względu na zagrożenie wynikające z algorytmów kwantowych jest dostępnych w literaturze wiele pozycji na jej temat. Na potrzeby niniejszego artykułu wiadomości dotyczące komputerów kwantowych zostały zaczerpnięte z [7] oraz raportu [1]. Doskonałym kompendium z kryptografii post-kwantowej są wykłady [4], z których wiedza również została wykorzystana przez autorów niniejszego artykułu. Do lepszego wyjaśnienia zasad działania omawianych algorytmów pomocne były przegląd [10], wykłady [3] i [6], a także raport [2].

2. Wstęp do kryptografii postkwantowej

Geneza i rozwój kryptografii postkwantowej są związane z możliwością sukcesu technologicznego w konstrukcji dużego komputera kwantowego. Oznacza to, że stanie się możliwe wykorzystanie zaawansowanego technologicznie, architektonicznie i obliczeniowo komputera kwantowego do różnych celów – łącznie z przestępczymi. Istnieje realne ryzyko, że zostaną złamane wszystkie znane dotychczas algorytmy kryptograficzne klucza publicznego. Łatwo sobie wyobrazić powstanie paniki w skali światowej w obawie

o bezpieczeństwo ludzi, danych i panika w obliczu groźby unicestwienia walut, pieniądza elektronicznego i systemów finansowych narodowych, wspólnotowych i globalnych.

Komputery kwantowe, korzystając z kwantowych algorytmów, będą w stanie łamać takie zabezpieczenia, jak RSA, DSA ECDSA, i w ten sposób współczesna kryptografia stanie się martwa. Naturalnie, nie chcemy wracać do czasów, kiedy dane były ukrywane w sejfach, a dostęp do nich mieli tylko najbardziej zaufani ludzie. Z tym zagrożeniem wiążą się dodatkowe problemy, np. kompromitacja zabezpieczeń fizycznych, generująca znaczne koszty – o wiele większe niż w przypadku zabezpieczeń cyfrowych.

Jednakże w pewnym stopniu jesteśmy zabezpieczeni przed takimi pesymistycznymi scenariuszami, ponieważ z wyprzedzeniem opracowano algorytmy, które są w stanie oprzeć się próbom złamania przez komputery kwantowe. Opracowano cztery grupy takich algorytmów [4] i są to:

1. algorytmy kryptograficzne oparte na funkcji skrótu bazującej na tablicy haszującej (*hash-based cryptography*). Przykładem takiego algorytmu jest system klucza publicznego opartego na drzewie skrótu Merkle'a. Algorytm powstał w 1979 roku. Został on zbudowany na podstawie idei jednorazowego podpisu Lamporta i Diffiego;
2. algorytmy oparte na kodach liniowych (*code-based cryptography*). Przykładem takiego algorytmu jest algorytm McEliece'a (1978), który wykorzystuje kody Goppa;
3. algorytmy kryptograficzne oparte na kratach (*lattice-based cryptography*). Przykładem bardziej szczegółowo opisanym dalej jest algorytm wzbudzający największe zainteresowanie – system szyfrowania klucza publicznego NTRU Hoffsteina-Piphera-Silvermana (1998);
4. algorytmy opierające się na wielomianach drugiego stopnia wielu zmiennych (*multivariate-quadratic-equations cryptography*). Przykładem może być system podpisu kluczem publicznym HFE Patriana (1996), uogólniający wniosek sformułowany przez Matsumotę i Imaiego.

Wymienione algorytmy kryptograficzne są uważane zarówno za odporne na ataki, których źródłem są komputery kwantowe, jak i na ataki kryptosystemów o architekturze klasycznej. Głównymi źródłami ataku są dwa algorytmy kwantowe: algorytm Shora, który pozwala na szybką faktoryzację liczb i atak bezpośredni na takie algorytmy jak RSA, oraz algorytm Grovera, który nie jest tak niebezpieczny z tej przyczyny, że nie jest tak szybki jak algorytm Shora i można uniknąć jego niepożądanego działania, wydłużając odpowiednio klucz.

Kryptografia postkwantowa odnosi się do badań nad prymitywami kryptograficznymi, które z założenia mają być odporne na łamanie zarówno ze strony komputerów kwantowych, jak i ze strony klasycznych architektur komputerowych.

Badacze zauważyli problem zagrożenia bezpieczeństwa danych szyfrowanych po opracowaniu i opublikowaniu przez amerykańskiego matematyka Petera Shora niezwykle silnego algorytmu faktoryzacji liczb. Ten algorytm stanowi realne zagrożenie dla

współczesnych algorytmów i systemów szyfrowania opartych na kluczach tworzonych na podstawie dużych liczb pierwszych.

Możemy zatem sformułować stwierdzenie, że celem postkwantowej kryptografii jest ustrzeżenie się przed łamaniem zabezpieczeń przez wykorzystanie w tym celu komputerów kwantowych. Okazuje się, że można to osiągnąć, wykorzystując algorytmy z różnych dziedzin informatyki, a których powstanie i badania nad nimi sięgają okresu 1970-2000.

3. Komputer kwantowy

Komputer kwantowy jest układem fizycznym, do opisu i działania którego jest wymagana mechanika kwantowa. Układ ten jest zaprojektowany w taki sposób, aby wynik ewolucji tego układu reprezentował rozwiązanie określonego problemu obliczeniowego [7].

Ze względu na specyficzne własności przetwarzania informacji kwantowej komputer kwantowy umożliwiałby znaczne obniżenie złożoności obliczeniowej niektórych klas problemów trudnych, a tym samym umożliwiłby złamanie bezpieczeństwa kryptosystemów opartych na trudności problemów wywodzących się z teorii informacji.

Konstrukcja komputera kwantowego w realistycznym układzie fizycznym wymaga spełnienia następujących warunków, nazywanych kryteriami DiVincenzo [1]:

1. Odpowiednio zdefiniowany qubit – dwa stany kwantowe oddzielone od pozostałych stanów układu (względnie duże odległości energetyczne, wzbronione przejścia), tak by informacja w niego wpisana nie ulegała wypływowi.
2. Określenie możliwości wpisywania informacji w qubit – tj. możliwości uzyskania dowolnej superpozycji dwóch stanów qubitu za pomocą zewnętrznego, makroskopowo regulowanego pola (np. oscylacje Rabiego w realistycznym obszarze pól).
3. Możliwość skalowania qubitu do urządzenia wieloqubitowego.
4. Zaprojektowanie i zaimplementowanie podstawowej operacji dwuqubitowej, na której można by oprzeć wykonanie dowolnej kwantowej operacji logicznej. W każdym przypadku konieczne jest opanowanie techniki włączania i wyłączania oddziaływania qubitów w sposób precyzyjny, w bardzo krótkich odstępach czasu, tj. sterowanie splątaniem dwóch qubitów.
5. Zapewnienie stosunku rzędów czasu potrzebnego na wykonanie elementarnych operacji logicznych i czasu dekoherencji na poziomie nie mniejszym niż 6.
6. Zapewnienie możliwości oddziaływania dużej liczby qubitów albo bezpośrednio, (co jest trudne), albo przez qubit pośredniczący (np. foton) w celu skalowania komputera i implementacji korekty błędów.

7. Zapewnienie możliwości odczytu informacji na wyjściu.
8. Zapewnienie możliwości resetowania całego układu.

Współcześnie trudno jest spełnić wszystkie wymienione wyżej warunki, dlatego praktyczna konstrukcja dużego komputera kwantowego wydaje się nierealistyczna w najbliższym czasie. Jednak gwałtowny postęp w eksperymentalnej mechanice kwantowej z pewnością doprowadzi do wielu ważnych odkryć i praktycznych zastosowań.

Biorąc pod uwagę istnienie algorytmów kwantowych, które mogą skompromitować używane obecnie algorytmy kryptograficzne, np. RSA, nie można ignorować zagrożenia dla bezpieczeństwa informacji, jakim byłoby zbudowanie dużego komputera kwantowego. Dlatego stale wzrasta zapotrzebowanie na wyniki badań nad kryptografią postkwantową, czyli na badania takich klasycznych algorytmów szyfrowania, w których złamanie szyfru będzie tak samo trudne przy użyciu komputera kwantowego, jak jest obecnie trudne przy użyciu komputerów klasycznych.

Za pomocą komputera kwantowego można efektywnie rozwiązać problemy matematyczne oparte na bardzo dużej złożoności obliczeniowej. To strona pozytywna rozwijających się badań podstawowych i technologii zmierzających do zbudowania komputera kwantowego dużej mocy [5].

Jednak istnieją poważne zagrożenia wynikające z coraz wyraźniej zbliżającej się perspektywy zbudowania komputera kwantowego dużej mocy. Największym zagrożeniem jest to, że natychmiast na takich komputerach będzie można wykonywać wiele znanych już algorytmów kwantowych, które rozwiązują wiele trudnych do rozwiązania matematycznych problemów. Są one podstawą powszechnie stosowanych dziś kryptosystemów klucza publicznego, np. mocnego algorytmu RSA. Do najbardziej znanych ofensywnych algorytmów kwantowych należą algorytm „poszukiwania igły w stogu siana" Grovera [2] i algorytm faktoryzacji liczb Petera Shora [1]. Kryptoanaliza znanych krypto systemów klasycznych i kwantowych wykazała, że możliwe jest znaczne skrócenie czasu potrzebnego do łamania szyfrów klasycznych i kwantowych za pomocą tych algorytmów. Zatem po powstaniu komputera kwantowego dużej mocy kryptosystemy kryptograficzne dotychczas powszechnie stosowane zostaną skompromitowane. Z matematycznego, kryptoanalitycznego punktu widzenia kryptosystemy klasyczne i kwantowe są już skompromitowane. Okazało się zatem, że znane kryptosystemy klasyczne oparte na kryptografii kwantowej i sama kryptografia kwantowa wobec możliwości zastosowania komputerów kwantowych nie będą tworzyć bezwzględnie bezpiecznych kanałów komunikacyjnych. Poza tym z naciskiem należy podkreślić, że infrastruktury i platformy realizacyjne kryptografii kwantowej z takimi protokołami kryptografii kwantowej, jak BB84 lub E91 (i naturalnie starszymi), są w istocie podatne na ataki na ich bezpieczeństwo. Z braku miejsca nie omawiamy w niniejszym artykule zagadnień i protokołów kryptografii kwantowej.

W tych okolicznościach powstała konieczność znalezienia algorytmów bardziej odpornych na ataki kryptograficzne możliwe do wykonania za pomocą komputera

kwantowego dużej mocy. Takie algorytmy oraz badanie ich właściwości i odporności kryptoanalitycznej matematyczną kryptoanalizą i potencjalne ataki kryptograficzne za pomocą algorytmów kwantowych na platformie koncepcyjnej komputera kwantowego są przedmiotem badań tzw. kryptografii postkwantowej. Istnieją cztery klasy matematycznych algorytmów trudnych lub odpornych kryptoanalitycznie nawet za pomocą komputera kwantowego dużej mocy. Należy jednak podkreślać, że stopniowo i te algorytmy są kompromitowane kryptoanalitycznie. Jednakże niektóre z nich wydają się bardzo odporne na kryptoanalizę jakąkolwiek metodą. W artykule omawiamy te cztery klasy algorytmów i ich reprezentantów.

4. Przykładowe algorytmy kryptografii postkwantowej

Obecnie opiszemy zwięźle kilka przykładowych systemów kryptograficznych. Takie systemy i algorytmy wydają się bardzo trudne do złamania, nawet dla kryptoanalityka uzbrojonego w duży komputer kwantowy.

Omawiane tu przykładowe algorytmy kryptograficzne dotyczą podpisów w systemie klucza publicznego i szyfrowania w systemie klucza publicznego. Wszystkie z opisywanych systemów przykładowych są parametryzowane za pomocą pożądanego przez użytkownika poziomu bezpieczeństwa. Większość źródeł literaturowych i doniesień w publikacjach naukowych skupia się na przykładach systemów z kluczem publicznym, ponieważ komputery kwantowe wydają się mieć niewielki wpływ na kryptografię klucza tajnego, funkcje skrótu i na inne systemy kryptograficzne. Algorytm Grovera wymusza nieco większe rozmiary kluczy do szyfrów z kluczem tajnym, ale wymagania odnośnie do zwiększania kluczy kryptograficznych są w zasadzie podobne w różnych systemach kryptograficznych i dla różnych szyfrów. Najszybszymi obecnie prekwantowymi szyframi 256-bitowymi są również najszybsi kandydaci na szyfry postkwantowe przy założeniu rozsądnego poziomu bezpieczeństwa. Istnieje kilka specjalnie skonstruowanych tajnych kluczy szyfrujących, które mogą być złamane przez algorytm Shora, ale te szyfry z pewnością nie należą obecnie do najszybszych. Zagadnienia związane z wielkością kluczy w algorytmach i systemach kryptograficznych są omówione w dobrze opracowanym wprowadzeniu do teorii szyfrów z kluczem tajnym w [11].

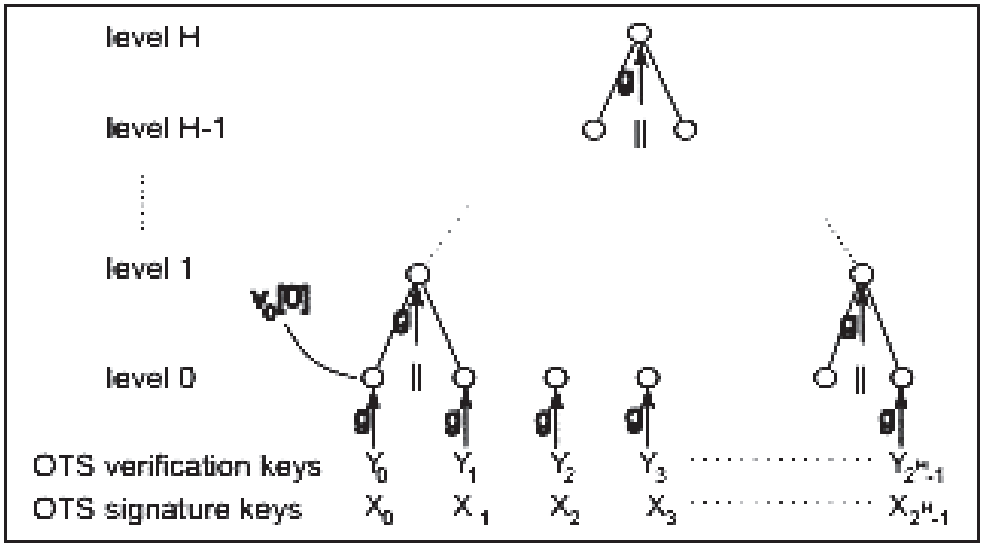
4.1. Algorytmy opierające się na funkcji haszującej – system podpisu cyfrowego Merkle'a

Ideą systemu podpisu cyfrowego Merkle'a jest redukcja walidowania wielu kluczy do walidacji jednego klucza publicznego przy skorzystaniu przy tym z konstrukcji drzewa

haszującego. Korzeniem tego drzewa jest klucz publiczny podpisu szyfrowego Merkle'a, liściom odpowiada hash klucza weryfikującego jednorazową sygnaturę [4, 8].

Działanie algorytmu:

1. Niech G(n) = {g : {0, 1}*} → {0, 1}^{n}|kϵK} będzie rodziną kryptograficznych funkcji haszujących. Dla systemu podpisu cyfrowego Merkle'a wybieramy parametry bezpieczeństwa: (KeyGen$_{OTS}$, Sign$_{OTS}$,Verify$_{OTS}$). Dodatkowo wybieramy wartość całkowitą dodatnią H. System podpisu cyfrowego będzie w stanie podpisać 2^H wiadomości mϵ {0, 1}* jednym kluczem publicznym, gdyż buduje on drzewo binarne o wysokości H.
2. Generowanie klucza przebiega następująco. Najpierw 2^H par kluczy OTS (X_i,Y_i) z $0 \leq i < 2^H$ jest generowanych przez funkcje KeyGen$_{OTS}$ – X to klucz sekretny, a Y to klucz publiczny. Potem następuje losowy wybór funkcji haszującej i utworzenie binarnego drzewa haszującego Merkle'a o długości H.



Rys. 1. Przykładowa struktura drzewa [4]
Fig. 1. Example of tree structure [4]

Wierzchołki o długości i są opisane przez $v_i[j]$, gdzie $0 \leq j < 2^{H-i}$. Zaczynamy od budowy liści drzewa Merkelego. Są to hasze kluczy weryfikujących OTS, np. $v_0[j] = g(Y_j)$, $0 \leq j < 2^H$. Wewnętrzne liście są budowane według następującej zasady: wierzchołek rodzica to hasz będący konkatenacją jego lewego i prawego dziecka, co oznacza: $v_i[j] = g(v_{i-1}[2j]||v_{i-1}[2j + 1])$ dla $0 \leq i \leq H$ i $0 \leq j < 2^i$, gdzie || oznacza konkatenację. Na koniec licznik C, który będzie inkrementowany za każdą operacją podpisu – będący jednocześnie numerem ostatnio używanego klucza OTS – zostaje inicjalizowany przez podstawienie C←−1. Dodajemy także pole statusu S, które zawiera ten licznik (może zawierać także dodatkowe informacje): S=(C). Klucz publiczny w systemie podpisu cyfrowego Merkle'a pk

jest korzeniem $v_H[0]$ drzewa Merkele'a i funkcji haszującej g, np. pk = ($v_H[0]$, g). Klucz sekretny sk zawiera sekwencje ($X_0, \ldots, X_{2H-1}$) kluczy sekretnych OTS i pola statusu S, np. sk = (($X_0, \ldots, X_{2H-1}$), S).

3. Podpis: Niech $d \in \{0, 1\}^*$ będzie dokumentem lub wiadomością do podpisu. Na początku podpisujący zwiększa licznik C – C ← C + 1 i odświeża pole statusu S. Następnie generuje jednorazową sygnaturę σ_{OTS} z d, używając klucza OTS do podpisu – X_C – jako argumentu funkcji $Sign_{OTS}$. Ponieważ klucz Y_C służący do weryfikacji może nie być poprawny dla weryfikującego, podpisujący tworzy tzw. ścieżkę autentykacji, która pozwala weryfikującemu zredukować walidację klucza Y_C do walidacji pierwszej części klucza publicznego pk. Uściślając, można stwierdzić, że ścieżka autentykacji pozwala na skonstruowanie ścieżki z liścia $g(Y_C) = v_0[C]$ do korzenia drzewa – $v_H[0]$. Jest to ścieżka autentykacji do sekwencji wierzchołków drzewa.

4. Weryfikacja: Procedura weryfikacji podpisu przebiega następująco: weryfikujący otrzymuje dokument lub wiadomość d, klucz publiczny pk i sygnaturę σ, następnie używa klucza weryfikującego Y_C jako argumentu funkcji $Verify_{OTS}$, by zweryfikować sygnaturę σ_{OTS}. Jeżeli weryfikacja się powiedzie, weryfikujący używa ścieżki autentykacji, by stworzyć ścieżkę od korzenia do liścia $g(Y_C)$. Jeżeli ostatni element ścieżki jest równy pierwszej części klucza publicznego pk – sygnatura jest przyjmowana. W przeciwnym wypadku sygnatura jest odrzucana.

4.2. Algorytmy oparte na kodach liniowych: algorytm McEliece'a

Algorytm McEliece'a to asymetryczny algorytm szyfrowania, opracowany w 1978 roku przez Roberta McEliece'a. Jest on oparty na trudności dekodowania kodów liniowych. Sam algorytm po adaptacji parametrów bezpieczeństwa nie został złamany. Przed adaptacją był obiektem wielu ataków [2, 3]. Klucz prywatny do tego algorytmu opiera się na kodach Goppa.

Działanie algorytmu:

1. Parametry: $n, t \in N$, gdzie $t << n$
2. Generowanie klucza: Biorąc parametry n,t, wygeneruj poniższe macierze:
   - G k x n macierz generującą kod G na F k wymiarową o najmniejszej odległości $d \geq 2t+1$ (binarnie nieskracalny kod Goppa)
   - S k x k losowa macierz binarna, niejednostkowa
   - P n x n losowa macierz permutacji

Następnie należy wyliczyć macierz k x n $G^{pub} = SGP$

3. Klucz publiczny: (G^{pub}, t)

4. Klucz prywatny: (S, D_g, P), gdzie: D_g to algorytm dekodujący dla G

5. Szyfrowanie: ($E_{(G^{pub},t)}$), aby zaszyfrować tekst jawny $m \in F^k$, wybierz losowo wektor $z \in F^n$ o wadze t oraz wylicz tekst tajny c według wyrażenia:
$$c = mG^{pub} \oplus z$$

6. Deszyfrowanie: $D_{(S,D_g,P)}$, aby odszyfrować tekst tajny c, wylicz:
$$cP^{-1} = (mS)G \oplus zP^{-1}$$
a następnie zastosuj algorytm dekodowania D_{Gpub} od G. Z racji że cP^{-1} ma odległość Hamminga od t do G, uzyskujemy słowo kodowe:
$$mSG = D_g(cP^{-1})$$
Niech $J \subseteq \{1,...,n\}$ będzie ciągiem, takim że G_J^{Pub} jest nieodwracalny, wtedy możemy wyliczyć tekst jawny: $m = (mSG)_J (G_J)^{-1} S^{-1}$

4.3. Algorytmy opierające się na kratach: asymetryczny system NTRU

System NTRU to asymetryczny pierścieniowy kryptosystem z kluczem publicznym i prywatnym. Jego pierwsza wersja powstała w 1996 roku, jego twórcami byli zaś J. Hoffstein, J. Pipger i J. Silverman. Działa on szybciej od RSA.

Możemy wyróżnić dwa algorytmy NTRU: NTRUEncrypt [5], NTRUSign [10].

Działanie algorytmu:

1. Parametry: Liczba pierwsza n, modulus q, granica całkowita d_f. Parametr liczbowy o małej wartości p = 3 ustawiony na stałe dla uproszczenia, są możliwe inne ustawienia.

2. Klucz prywatny: Wektory $f \in e_1 + \{p, 0-p\}^n$ oraz $g \in \{p, 0-p\}^n$, takie że każdy z $f - e_1$ i g zawiera dokładnie d_f+1 wartości pozytywnych i d_f wartości negatywnych, a także macierz [T*f] jako nieodwracalne modulo q.

3. Klucz publiczny: Kluczem publicznym jest wektor $h=[T*f]^{-1} g \bmod q \in Z_q^n$.

4. Szyfrowanie: Wiadomość jest kodowana przez wektor $m \in \{1,0,-1\}^n$. Jako wektor losowy wykorzystujemy wektor $r \in \{1,0,-1\}^n$, każdy z nich zawiera dokładnie d_f+1

wartości pozytywnych oraz d_f wartości negatywnych. Jako wyjście funkcja szyfrująca zwraca $c = m + [T * h]r \bmod q$.

5. Deszyfrowanie: Jako wejście funkcja przyjmuje tekst zaszyfrowany $c \in Z_q^n$, a jako wyjście zwraca $(([T * f]c) \bmod q) \bmod p$, gdzie redukowane jest modulo q, a p produkuje wektory o koordynatach [-q/2, +q/2] i [-p/2.p/2].

4.4. Algorytmy oparte na wielomianach drugiego stopnia wielu zmiennych: HFE

HFE to kryptosystem klucza publicznego oparty na wielomianach opisujących skończone pola Fq o różnych rozmiarach, aby ukryć zależność między kluczem prywatnym a publicznym. Opiera się na trudności problemu znalezienia rozwiązań dla systemu równań kwadratowych wielu zmiennych [9].

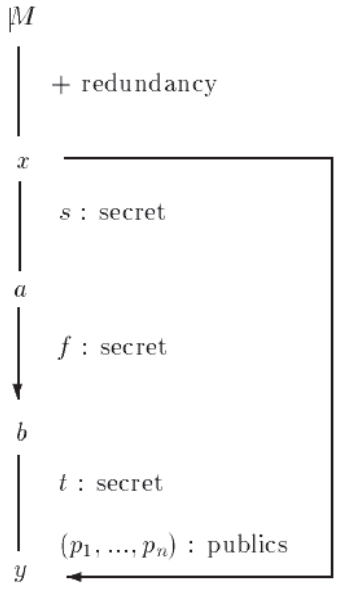
Reprezentacja x wiadomości M jest następująca:

Pole K, gdzie $q=p^m$ elementów jest publiczne. Każda wiadomość M jest reprezentowana przez wartość x, gdzie x jest ciągiem n elementów K (jeśli p=2, każda wiadomość będzie reprezentowana przez nm bitów).

Elementy tajne:

1. Rozszerzenie Ln pola K w stopniu n.
2. Funkcja f o stopniu d „nie za dużym” (np. d≤1024, a dokładniej zwykle d jest zawarte w 17≤d≤64).
3. Dwie afiniczne bijekcje s i t z $K^n \rightarrow K^n$ (mogą być reprezentowane jako wielomiany o całkowitym stopniu pierwszym i ze współczynnikiem w K).

Szyfrowanie jest opisane na rysunku 2. Tekst zaszyfrowany y jest wyznaczany funkcją: y=t(f(s(x))).



Rys. 2. Podstawowe szyfrowanie przy użyciu HFE [8]
Fig. 2. Basic encipher Rusing HFE cryptosystem [8]

Ważne jest to, że skoro s i T razem są stopnia pierwszego, a funkcja f jest stopnia drugiego, to kompozycja wszystkich operacji nadal będzie równaniem kwadratowym. Funkcja ta zatem może być przedstawiona jako n wielomianów ze współczynnikami w K, (p_1, ..., p_n). Wielomiany te pozwalają uzyskać komponenty y_1, ..., y_n tekstu do zaszyfrowania y z komponentów x_1, ..., x_n z x:

$$\begin{cases} y_1 = p_1(x_1, \dots, x_n) \\ y_2 = p_2(x_1, \dots, x_n) \\ \vdots \\ y_n = p_n(x_1, \dots, x_n) \end{cases}$$

Publiczne składniki to:

1. Pole K o $q=p^m$ elementach i długości n.
2. N wielomianów (p_1, ...,p_n) n zmiennych ze współczynnikami K.
3. Sposób na zawarcie redundancji w wiadomości (sposób na otrzymanie x z M).

5. Podsumowanie i wnioski

Problematyka algorytmów kryptografii postkwantowej będzie bardzo ważna w nadchodzących latach. W kontekście tempa rozwoju komputerów kwantowych bardzo realne jest zagrożenie, które płynie z mocy algorytmów Shore'a czy Grovera [2]. Według niektórych badaczy możliwe jest, że wkrótce ujrzymy nagłówki gazet głoszące, że wszystkie nasze dane nie są już bezpieczne i że transakcje w bankach tracą swoją pewność. Jest oczywiste, że tej sytuacji możemy uniknąć, jeżeli dalej będą rozwijane badania w obszarze kryptografii postkwantowej.

Algorytmy postkwantowej kryptografii mają wiele różnych źródeł i różne podstawy implementacji. Przykładem bardzo dobrego algorytmu może być NTRU, który jest szybszy od RSA i dodatkowo jest on odporny na ataki ze strony komputerów kwantowych [5, 6].

Świat nauki jest świadom zagrożenia dla bezpieczeństwa danych płynącego z komputerów kwantowych, dlatego odbywają się coroczne konferencje, których celem jest omawianie coraz nowszych i lepszych technik kryptograficznych.

Bibliografia

1. ARDA Report (Advanced Research & Development Activity – roadmap in Quantum Information 2002), http://www.qist.lanl.gov (20.05.2014).
2. Bernstein D.J., Grover vs. McEliece (Report 23 September 2009), http://cr.yp.to/codes/grovercode-20091123.pdf (20.05.2014).

3. Bernstein D.J., Lange T., Christiane P.: Attacking and defending the McEliece cryptosystem. Proc. 2nd International Workshop on Post-Quantum Cryptography. Lecture Notes In Computer Science (8 August 2008), 5299, p. 31-46.
4. Buchman J.: Post-Quantum Cryptography. Wykłady na Politechnice w Darmstadt, 2010, https://www-old.cdc.informatik.tu-darmstadt.de/lehre/WS09_10/vorlesung/pqc_files/PQC.pdf
5. Grzywak A., Klamka J. i inni: Klasyczne i kwantowe metody podniesienia bezpieczeństwa informacji w systemach komputerowych. Wydawnictwo Wyższej Szkoły Biznesu, Dąbrowa Górnicza 2010.
6. Hermans J., Vercauteren F., Preneel B.: Speed Records for NTRU. Pieprzyk J. (ed.): Topics in Cryptography - CT-RSA 2010. Lecture Notes in Computer Science San Francisco, CA: Springer, Berlin-Heidelberg, 5985, p. 73-88.
7. Jacak W., Donderowicz W., Jacak J.: Wstęp do informatyki i kryptografii kwantowej, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011, s. 4-16.
8. Merkle R.: Secrecy, authentication and public key systems / A certified digital signature. Ph.D. dissertation, Dept. of Electrical Engineering, Stanford University, 1979.
9. Patarin J.: Hidden Field Equations (HFE) and Isomorphisms of Polynomials (IP): two new Families of Asymmetric Algorithms (extended version); Eurocrypt 1996.
10. Perlner R.A., Cooper D.A.: Quantum resistant public key cryptography: a survey. Seamons K., McBurnett N., Polk T. (eds.): Proceedings of the 8th Symposium on Identity and Trust on the Internet New York, NY: ACM, p. 85-93.
11. Robshaw M., Billet O.: New stream cipher designs: the eSTREAM finalists. Lecture Notes in Computer Science, 4986, Springer, 2008.

Abstract

The purpose of this article is to present the subject of post-quantum cryptography. The first part explains the basic concepts and definitions related to the field. It also presents the reason behind the research in this area, which is the possible construction of quantum computer with high computational power. At present quantum algorithms, such as Grover's algorithm for searching an unsorted database or Shor's algorithm for integer factorization, already exist. It is possible, using quantum computer with enough computational power, to significantly reduce the time needed to solve many problems in mathematics on which most of used today cryptosystems, such as RSA, are based.

In the second part of the article the concept of „quantum computer" is defined. At this stage the conditions which such device should meet are listed, namely DiVincenzo criteria. In the third part four approaches are listed that are considered resistant to quantum computer

attacks. It means that up to today there was not developed such a quantum algorithm that would allow to discredit such cryptosystems. This approaches are as follows: hash-based cryptography, code-based cryptography, lattice-based cryptography and multivariate cryptography.

For each approach there is given an example of such an algorithm and its description is provided. Merkle signature scheme utilizes the hash tree construction in order to reduce the process of validating many keys to the validation of single public key. The public key of Merkle signature scheme is the root of such a tree, while the hashes of the key, which allow the verification of a one-time signature, are its leaves. McEliece cryptosystem is an asymmetric code-based algorithm created in 1978. The private key of this algorithm is based on the Goppa code. NTRU is a public-key cryptosystem which makes use of the lattice-based cryptography to encrypt and decrypt data. HFE, which also is public-key cryptosystem, is based on polynomials over finite fields F_q of different sizes to disguise the relationship between the private key and the public key.