Ewa Pośpiech

PODPISY NIEZAPRZECZALNE – PODPISY Z DODATKOWĄ FUNKCJONALNOŚCIĄ

Wprowadzenie

Powszechna informatyzacja powoduje, że w coraz większym stopniu są dostępne różne możliwości przeprowadzania operacji w sieci. Standardem jest komunikacja elektroniczna, gromadzenie i zarządzanie danymi, zakupy internetowe, transakcje w systemie bankowości elektronicznej, a coraz więcej użytkowników korzysta m.in. z różnego rodzaju usług e-urzędów. Jednym z najistotniejszych aspektów związanym z tego typu operacjami jest bezpieczeństwo; w kwestii tej znaczący udział ma współczesna kryptografia, która wykorzystuje narzędzia matematyczne, a której sprzyja dynamicznie rozwijająca się technika komputerowa.

W przypadku różnych transakcji zachodzi konieczność potwierdzenia ich wykonania, co jest realizowane przez składanie podpisu. W przypadku operacji wirtualnych jest składany podpis cyfrowy. Najpowszechniejszym zastosowaniem podpisów cyfrowych jest podpisywanie wiadomości przesyłanych drogą elektroniczną. Tą drogą odbywa się wymiana dokumentów z różnymi instytucjami i partnerami biznesowymi, składa się podania administracyjne, uwierzytelnia e-faktury, dokonuje się uwierzytelniania transakcji w systemie bankowości elektronicznej itp. Innym, równie istotnym zastosowaniem podpisów cyfrowych jest ich składanie w celu zabezpieczenia oprogramowania.

Celem składania podpisu cyfrowego jest przede wszystkim zagwarantowanie autentyczności, niezaprzeczalności i integralności wiadomości (dokumentu). Inną cechą, która w pewnych sytuacjach może być wymagana, jest dodatkowa funkcjonalność podpisu. Najczęściej oznacza to połączenie algorytmu podpisu cyfrowego z charakterystycznym protokołem w celu uzyskania dodatkowych własności, których zwykły algorytm nie zapewnia. Przykładem takich algorytmów są schematy podpisu niezaprzeczalnego. Schematy te, w odróżnieniu od zwykłych schematów podpisów cyfrowych, wymagają w procesie weryfikacji podpisu współpracy z podmiotem podpisującym.

Celem tego artykułu jest przedstawienie wybranych protokołów kryptograficznych umożliwiających składanie podpisów niezaprzeczalnych, które znajdują zastosowania m.in. w zabezpieczaniu oprogramowania przed kopiowaniem i rozpowszechnianiem wśród osób nieuprawnionych.

1. Podstawy teoretyczne

Bazą konstrukcji algorytmów kryptograficznych są pojęcia matematyczne. Głównie wykorzystuje się zagadnienia związane z teorią liczb oraz algebrą abstrakcyjną. Dlatego też przytoczono wybrane zagadnienia teoretyczne wykorzystywane przy formułowaniu prezentowanych protokołów podpisu niezaprzeczalnego (na podstawie [1; 3; 5]).

Definicja 1. Niech n jest liczbą całkowitą dodatnią oraz a, b są liczbami całkowitymi. Mówimy, że a przystaje do b modulo n, jeśli liczba a i liczba b dają takie same reszty przy dzieleniu przez n. Zależność tę zapisujemy w postaci wyrażenia zwanego kongruencją:

$$a \equiv b \pmod{n}.$$

Definicja 2. Niech n będzie liczbą naturalną oraz a liczbą całkowitą. Element $x \in \mathbf{Z}$ ($\mathbf{Z}$ – zbiór liczb całkowitych) nazywa się elementem odwrotnym do a modulo n, jeśli jest spełniona kongruencja:

$$ax \equiv 1 \pmod{n}.$$

Definicja 3. Grupą multiplikatywną grupy $\mathbf{Z}_n$, gdzie $\mathbf{Z}_n$ jest zbiorem w postaci $\mathbf{Z}_n = \{0, 1, 2, ..., n-1\}$, jest $\mathbf{Z}_n^* = \{a \in \mathbf{Z}_n : \mathrm{NWD}(a, n) = 1\}$. W szczególności gdy n jest liczbą pierwszą, wówczas $\mathbf{Z}_n^* = \{a \in \mathbf{Z} : 1 \le a \le n-1\}\}$.

Definicja 4. Rzędem grupy G lub podgrupy P nazywamy liczbę jej elementów.

Definicja 5. Jeśli $G = \{g^k : k \in \mathbf{Z}\}$ dla pewnego $g \in G$, gdzie G jest grupą, to G nazywamy grupą cykliczną, natomiast element g nazywamy generatorem grupy G.

Definicja 6. Niech G jest grupą oraz $g \in G$. Jeśli istnieje liczba całkowita dodatnia r taka, że zachodzi $g^r = 1$, to najmniejszą taką liczbę nazywa się rzędem elementu g w grupie G. Oznaczamy $r = \text{rząd}_G\, a$.

Definicja 7. Niech n będzie liczbą naturalną oraz a liczbą całkowitą taką, że NWD(a, n) = 1. Rzędem liczby a modulo n nazywamy najmniejszą liczbę naturalną r taką, że $a^r \equiv 1 \pmod{n}$.

Twierdzenie 1. Niech $g \in G$ (G – grupa multiplikatywna) i niech k, l będą liczbami całkowitymi. Wówczas $g^l = g^k$ wtedy i tylko wtedy, gdy $l \equiv k \pmod{\text{rząd}_G g}$.

Definicja 8. Niech n będzie liczbą naturalną. Funkcją Eulera $\varphi(n)$ nazywamy liczbę elementów naturalnych k takich, że $k \leq n$ oraz względnie pierwszych z n.

Definicja 9. Niech $g \in \mathbf{Z}_n^*$. Jeśli rząd g wynosi $\varphi(n)$, to o g mówimy, że jest generatorem lub elementem (pierwiastkiem) pierwotnym $\mathbf{Z}_n^*$. Jeśli $\mathbf{Z}_n^*$ ma generator, to o $\mathbf{Z}_n^*$ mówi się, że jest cykliczna.

Definicja 10. Niech n będzie liczbą naturalną oraz a liczbą całkowitą taką, że NWD(a, n) = 1. Jeśli rząd elementu a modulo n wynosi $\varphi(n)$, to a nazywamy pierwiastkiem pierwotnym modulo n.

Definicja 11. Niech p będzie liczbą pierwszą oraz niech g będzie pierwiastkiem pierwotnym modulo p. Dla każdej liczby całkowitej $A \in \{1, 2, \ldots, p-1\}$ istnieje wykładnik $a \in \{0, 1, \ldots, p-2\}$ taki, że:

$$A \equiv g^a \pmod{p}.$$

Wykładnik ten nazywamy logarytmem dyskretnym liczby A przy podstawie g ($a = \log_g A$).

2. Podpisy niezaprzeczalne

Podpisy niezaprzeczalne są rodzajem podpisu, którego weryfikacja wymaga współpracy z osobą podpisującą – składający podpis ma kontrolę nad sprawdzaniem podpisu oraz nad podmiotami sprawdzającymi (osoby trzecie nie mogą uzyskać potwierdzenia autentyczności informacji/dokumentu bez konfrontacji z osobą podpisującą). Takie określenie podpisów niezaprzeczalnych nie tłuma-

czy ich „niezaprzeczalności"; nazwa wywodzi się stąd, że jeśli podmiot podpisujący byłby zmuszony do potwierdzenia albo wyparcia się podpisu, to nie jest on w stanie fałszywie zaprzeczyć swojemu autentycznemu, poprawnemu podpisowi.

Podpisy niezaprzeczalne mogą być stosowane w różnych sytuacjach (na podstawie [2; 4]). Jedną z możliwości zastosowania jest np. ochrona prywatności osoby – sygnowanie podpisem niezaprzeczalnym informacji przekazanej danemu podmiotowi (np. prasie) uniemożliwia sprawdzenie autentyczności wiadomości osobom nieuprawnionym. Inną możliwością wykorzystania podpisów niezaprzeczalnych jest składanie ich na pakietach oprogramowania – sprzedając taki pakiet, podmiot sprzedający przeprowadza transakcję z konkretnym nabywcą, który może sprawdzić autentyczność oprogramowania; gdyby jednak nabywca zrobił kopię i sprzedał pakiet kolejnemu nabywcy, ten trzeci nie może zweryfikować autentyczności bez udziału w tym procesie podmiotu pierwotnie sprzedającego (pierwszy kupujący traci wiarygodność i jest „na cenzurowanym"). Kolejną możliwość zastosowania podpisu niezaprzeczalnego opisuje następująca sytuacja: klient posiada w banku skrzynkę depozytową; każdorazowe skorzystanie ze skrzynki musi być przez klienta potwierdzone, np. datą i godziną. Jeśli klient złoży na potwierdzeniu podpis niezaprzeczalny, bank nie jest w stanie nikomu udowodnić, bez skontaktowania się z właścicielem skrzynki (klientem), że ten ze skrzynki skorzystał.

Konstruowanie schematów pozwalających na składanie podpisów niezaprzeczalnych jest możliwe dzięki technikom kryptograficznym.

Schemat podpisu niezaprzeczalnego jest podzielony na etapy, a głównymi podmiotami są podmiot podpisujący i weryfikujący. Postać (wartość) podpisu niezaprzeczalnego jest uzależniona od dokumentu, pod którym ma być złożony, oraz od klucza prywatnego podmiotu podpisującego. Można wyszczególnić następujące etapy protokołu podpisu niezaprzeczalnego (na podstawie [1]):

1. Generowanie klucza – podmiot podpisujący generuje dwa klucze: podpisywania i weryfikacji. Pierwszy z nich jest kluczem prywatnym (tajnym), natomiast drugi z nich jest kluczem publicznym.
2. Generowanie podpisu – mając do dyspozycji dokument oraz klucz podpisywania, podmiot podpisujący oblicza podpis pod tym dokumentem.
3. Weryfikacja podpisu – dokonuje się jej z użyciem dokumentu, podpisu i klucza weryfikacji podmiotu podpisującego. Strona weryfikująca wysyła podpisującemu zapytanie. Podpisujący, posiadając dokument, zapytanie i tajny klucz, oblicza odpowiedź i przesyła ją podmiotowi weryfikującemu. Dysponując dokumentem, podpisem, kluczem weryfikacji podpisującego oraz otrzymaną odpowiedzią na zapytanie, weryfikujący przeprowadza weryfikację i podpis zostaje zaakceptowany albo odrzucony.

3. Schematy Chauma-van Antwerpena

3.1. Schemat Chauma-van Antwerpena podpisu niezaprzeczalnego

Bezpieczeństwo przedstawianego algorytmu wynika z trudności rozwiązywania zagadnienia znajdowania logarytmu dyskretnego w cyklicznej podgrupie rzędu q należącej do $\mathbf{Z}_p^*$ (według [2]):

1. Generuje się klucz prywatny i publiczny podpisującego – wybiera się liczby pierwsze p i q takie, że q dzieli $p - 1$. Wybiera się generator g grupy cyklicznej rzędu q w $\mathbf{Z}_p^*$: losuje się element $b \in \mathbf{Z}_p^*$ i oblicza wartość $g = b^{(p-1)/q} \text{MOD } p$, przy czym jeżeli $g = 1$, należy wylosować inną wartość $b \in \mathbf{Z}_p^*$, taką by $g \neq 1$. Następnie wybiera się losowo liczbę pierwszą a, $a \in (1, q - 1]$ i oblicza wartość $y = g^a \text{MOD } p$. Kluczem prywatnym podmiotu podpisującego jest a, natomiast kluczem publicznym jest czwórka (p, q, g, y).
2. Podpis s, generowany pod wiadomością (dokumentem) w przyjmuje postać $s = w^a \text{MOD } p$.
3. Weryfikacja podpisu przebiega etapami: podmiot weryfikujący otrzymuje klucz publiczny podpisującego, losuje tajne niezerowe wartości całkowite $u, v \in \mathbf{Z}_q$ i oblicza wartość zapytania $z = s^u y^v \text{MOD } p$, którą wysyła do podpisującego. Podmiot podpisujący oblicza $o = (z)^{a^{-1}} \text{MOD } p$, gdzie a^{-1} jest odwrotnością do a modulo q – odpowiedź jest odsyłana podmiotowi weryfikującemu, ten z kolei, oblicza wartość $o' = w^u g^v \text{ MOD } p$ i jeśli wartość ta jest równa wartości o – podpis jest akceptowany, w innym przypadku – odrzucany.

Poprawność powyższego schematu wynika z następujących przekształceń:

$$o = (z)^{a^{-1}} \text{MOD } p = (s^u y^v)^{a^{-1}} \text{MOD } p = (w^{au} g^{av})^{a^{-1}} \text{MOD } p =$$
$$= (w^u g^v)^{aa^{-1}} \text{MOD } p = w^u g^v \text{ MOD } p = z' \text{MOD } p = o'$$

Jeżeli podpis s jest sfałszowany, prawdopodobieństwo tego, że podmiot weryfikujący nie odrzuci podpisu, wynosi co najwyżej $\frac{1}{q}$, co w przypadku dostatecznie dużej wartości q jest małą liczbą.

Przykład 1

Niech $p = 47$ i $q = 23$ spełniają warunek, że q jest dzielnikiem $p - 1$. Dla wybranej wartości $b = 13 \in \mathbf{Z}_{47}^*$ generatorem grupy cyklicznej rzędu 23 w $\mathbf{Z}_{47}^*$ jest:

$$g = b^{(p-1)/q} \text{MOD } p = 13^2 \text{ MOD } 47 = 28 .$$

Niech dalej całkowita liczba a, $a \in (1, 22]$ jest równa $a = 11$. Wówczas wartość y wynosi:

$$y = g^a \text{MOD } p = 28^{11} \text{ MOD } 47 = 18 .$$

Kluczem publicznym podpisującego jest czwórka (47, 23, 28, 18), a jego kluczem prywatnym wartość $a = 11$.

Niech wiadomością w, pod którą ma być złożony podpis, jest $w = 110101$. Podpisem s, składanym pod wiadomością w, będzie wartość:

$$s = w^a \text{MOD } p = 110101^{11} \text{MOD} 47 = 17 .$$

Niech wartości $u, v \in \mathbf{Z}_q$, które losuje podmiot weryfikujący po uzyskaniu klucza publicznego, wynoszą $u = 9$, $v = 15$. Wartość zapytania przesyłana następnie do składającego podpis wynosi:

$$z = s^u y^v \text{ MOD } p = 17^9 \cdot 18^{15} \text{ MOD } 47 = 25 .$$

Podpisujący oblicza odpowiedź, uzyskując wartość:

$$o = (z)^{a^{-1}} \text{ MOD } p = 25^{21} \text{MOD} 47 = 37 ,$$

gdzie $a^{-1} = 21$ jest odwrotnością do $a = 11$ modulo 23. Wartość odpowiedzi jest wysyłana podmiotowi weryfikującemu, który dokonuje obliczenia:

$$o' = w^u g^v \text{ MOD } p = 110101^9 28^{15} \text{ MOD} 47 = 37 .$$

Ponieważ uzyskano równość wartości $o = o'$, więc podpis jest akceptowany.

Podmiot składający podpis, w jakiejś niedogodnej dla siebie sytuacji, mógłby chcieć wyprzeć się swojego poprawnego podpisu. Istnieje jednak możliwość sprawdzenia, za pomocą odpowiedniego algorytmu zabezpieczającego przed wyparciem, czy podmiot próbuje wyprzeć się ważnego podpisu; algorytm ten umożliwia także sprawdzenie, czy podpis nie jest sfałszowany.

Protokół Chauma-van Antwerpena chroniący przed wyparciem się podpisu

Protokół ten, dla danego podpisu *s* oraz klucza publicznego podmiotu podpisującego, wymaga m.in. dwukrotnego zastosowania schematu weryfikacji opisanego wyżej (na podstawie [2]):

1. Podmiot weryfikujący, po uzyskaniu klucza publicznego podmiotu podpisującego, losuje tajne niezerowe wartości całkowite $u_1, v_1 \in \mathbf{Z}_q$ i oblicza wartość $z = s^{u_1} y^{v_1} \text{ MOD } p$, którą przesyła podpisującemu. Podmiot podpisujący oblicza $o = (z)^{a^{-1}} \text{ MOD } p$ i odsyła ją podmiotowi weryfikującemu. Jeśli wartość *o* jest równa wartości wyznaczonej według wzoru $o = w^{u_1} g^{v_1} \text{ MOD } p$, podpis *s* jest akceptowany i protokół jest zatrzymywany.
2. Ponownie podmiot weryfikujący losuje tajne niezerowe wartości całkowite $u_2, v_2 \in \mathbf{Z}_q$ i oblicza wartość $z' = s^{u_2} y^{v_2}$ MOD *p*, którą przesyła podpisującemu. Podmiot podpisujący oblicza $o' = (z')^{a^{-1}} \text{ MOD } p$ i odsyła ją podmiotowi weryfikującemu. Jeśli zachodzi $o' = w^{u_2} g^{v_2} \text{ MOD } p$, podpis *s* jest akceptowany i protokół jest zatrzymywany.
3. Podmiot weryfikujący oblicza wartości $c = (og^{-v_1})^{u_2} \text{ MOD } p$ oraz $c' = (o' g^{-v_2})^{u_1} \text{ MOD } p$. Jeżeli wartości te są równe, wnioskuje się, że podpis *s* jest sfałszowany. W przeciwnym wypadku uznaje się, że podpis jest ważny, a podmiot podpisujący usiłuje się podpisu wyprzeć.

Przykład 2

Niech wartości niezbędne do złożenia i zweryfikowania podpisu są takie same, jak w przykładzie 1:
$p = 47$, $q = 23$,
$b = 13$, $g = 28$,
$a = 11$, $y = 18$.

Kluczem publicznym podpisującego jest czwórka (47, 23, 28, 18), a kluczem prywatnym wartość a = 11. Wiadomością w jest wartość w = 110101. Podpis, wyznaczony na podstawie schematu Chauma-van Antwerpena, wynosi 17. Założono jednak, że niepowołana osoba sfałszowała podpis i wysyła weryfikującemu wartość s = 16. W celu wykazania fałszerstwa jest przeprowadzany protokół Chauma-van Antwerpena chroniący przed wyparciem się podpisu.

Weryfikujący losuje niezerowe wartości całkowite $u_1, v_1 \in \mathbf{Z}_{23}$. Niech wartości te wynoszą $u_1 = 9, v_1 = 4$. Wartość zapytania wysyłana do składającego podpis wynosi:

$$z = s^{u_1} y^{v_1} \text{ MOD } p = 16^9 \cdot 18^4 \text{ MOD } 47 = 21.$$

Podpisujący oblicza następującą odpowiedź, którą odsyła weryfikującemu:

$$o = (z)^{a^{-1}} \text{ MOD } p = 21^{21} \text{ MOD } 47 = 34,$$

gdzie $a^{-1} = 21$ jest odwrotnością do a = 11 modulo 23. Podmiot weryfikujący porównuje tę wartość z odpowiadającą jej wartością obliczoną według wzoru:

$$o = w^{u_1} g^{v_1} \text{ MOD } p = 110101^9 28^4 \text{ MOD } 47 = 36.$$

Ponieważ wartości są różne, więc jest przeprowadzany kolejny etap protokołu.

Weryfikujący losuje kolejne niezerowe wartości całkowite $u_2, v_2 \in \mathbf{Z}_{23}$. Niech $u_2 = 8, v_2 = 5$. Wartość zapytania wysyłana do składającego podpis wynosi tym razem:

$$z' = s^{u_2} y^{v_2} \text{ MOD } p = 16^8 \cdot 18^5 \text{ MOD } 47 = 6.$$

Odpowiedź, którą ponownie oblicza podpisujący i odsyła weryfikującemu, wynosi:

$$o' = (z)^{a^{-1}} \text{ MOD } p = 6^{21} \text{ MOD } 47 = 17.$$

Podmiot weryfikujący porównuje tę wartość z wartością obliczoną za pomocą wzoru:

$$o' = w^{u_2} g^{v_2} \text{ MOD } p = 110101^8 28^5 \text{ MOD } 47 = 6.$$

Ponieważ wartości są różne, więc jest przeprowadzany ostatni etap protokołu. Podmiot weryfikujący oblicza elementy c i c':

$$c = (og^{-v_1})^{u_2} \text{ MOD } p = (34 \cdot 28^{-4})^8 \text{ MOD } 47 = (34 \cdot 14)^8 \text{ MOD } 47 = 24,$$

gdzie 14 jest odwrotnością do 28^4 modulo 47 oraz:

$$c' = (o' g^{-v_2})^{u_1} \text{ MOD } p = (17 \cdot 28^{-5})^9 \text{ MOD } 47 = (17 \cdot 24)^9 \text{ MOD } 47 = 24,$$

gdzie 24 jest odwrotnością do 28^5 modulo 47. Ponieważ $c = c'$, więc na podstawie protokołu wnioskuje się, że podpis s = 16 jest sfałszowany.

4. Przekształcalne podpisy niezaprzeczalne

Podpis przekształcalny można weryfikować, zaprzeczać oraz przekształcać do postaci zwykłego podpisu cyfrowego. Przy jego konstrukcji wykorzystuje się algorytm podpisu ElGamala. Algorytm przekształcalnego podpisu niezaprzeczalnego przebiega następująco (na podstawie [4]):

1. Wybiera się liczby pierwsze p i q takie, że q dzieli $p - 1$, wybiera się generator g grupy cyklicznej rzędu q w $\mathbf{Z}_p^*$: losuje się element $b \in \mathbf{Z}_p^*$ i oblicza wartość $g = b^{(p-1)/q} \text{MOD } p$, przy czym jeżeli $g = 1$, należy wylosować inną wartość $b \in \mathbf{Z}_p^*$ taką, by $g \neq 1$. Wybiera się losowo liczby a i d, takie że $a, d \in (1, q - 1]$ i oblicza wartości $y = g^a \text{MOD } p$ oraz $x = g^d \text{MOD } p$. Kluczami prywatnymi podmiotu podpisującego są a i d, natomiast kluczem publicznym jest piątka liczb (p, q, g, y, x).
2. W celu obliczenia przekształcalnego podpisu cyfrowego składanego pod wiadomością w losuje się niezerową liczbę $t \in \mathbf{Z}_q$ i oblicza się wartości $T = g^t \text{MOD } p$ oraz $w' = Ttdw \text{MOD } q$.
3. Generuje się zwykły podpis ElGamala dla wiadomości w' – losuje się liczbę k, $k \leq p - 1$ taką, że NWD$(k, q - 1) = 1$. Oblicza się wartość l według reguły $l = g^k \text{MOD } p$ i za pomocą algorytmu Euklidesa wyznacza się podpis s z zależności:

$$w' \equiv la + ks \pmod q .$$

   Wartości (l, s) oraz T stanowią podpis ElGamala.
4. Podmiot podpisujący sprawdza swój podpis i pokazuje go weryfikującemu: podmiot weryfikujący losuje dwie liczby $\delta, \varepsilon \in \mathbf{Z}_p$, oblicza $c = T^{Tw\delta} g^{\varepsilon} \text{ MOD } p$ i przesyła wartość podpisującemu. Podpisujący wybiera liczbę losową γ i oblicza $h_1 = cg^{\gamma} \text{MOD } p$ oraz $h_2 = h_1^d \text{MOD } p$. Wartości te są wysyłane weryfikującemu, a ten przesyła podpisującemu wartości δ i ε. Podpisujący sprawdza równość $c = T^{Tw\delta} g^{\varepsilon} \text{ MOD } p$ i przesyła γ weryfikującemu. Ten z kolei sprawdza, czy zachodzi $h_1 = T^{Tw\delta} g^{\varepsilon+\gamma} \text{MOD } p$ oraz $h_2 = y^{l\delta} l^{s\delta} x^{\varepsilon+\gamma} \text{MOD } p$.

Poprawność powyższego schematu wynika z następujących przekształceń:

$$h_1 = T^{Tw\delta} g^{\varepsilon+\gamma} \text{MOD } p = cg^{\gamma} \text{MOD } p = h_1$$

$$h_2 = y^{l\delta} l^{s\delta} x^{\varepsilon+\gamma} \text{MOD } p = g^{al\delta} g^{ks\delta} g^{d(\varepsilon+\gamma)} \text{MOD } p = \left(g^{la+ks}\right)^{\delta} \left(g^{\varepsilon+\gamma}\right)^{d} \text{ MOD } p =$$

$$= \left(g^{w'}\right)^{\delta} \left(g^{\varepsilon+\gamma}\right)^{d} \text{ MOD } p = \left(g^{Ttdw}\right)^{\delta} \left(g^{\varepsilon+\gamma}\right)^{d} \text{ MOD } p =$$

$$= \left(g^{tTw\delta}\right)^{d} \left(g^{\varepsilon+\gamma}\right)^{d} \text{ MOD } p = \left(T^{Tw\delta} g^{\varepsilon+\gamma}\right)^{d} \text{ MOD } p = h_1^{d} \text{ MOD } p = h_2 .$$

Jeśli zostanie powszechnie udostępniona wartość d, podpisujący może przekształcić swoje podpisy niezaprzeczalne w zwykłe podpisy cyfrowe, a zatem takie, których weryfikacja nie wymaga interakcji z podpisującym.

Przykład 3

Niech początkowe wartości umożliwiające złożenie podpisu są takie same, jak w przykładzie 1, zatem:
$p = 47$, $q = 23$,
$b = 13$, $g = 28$,
$a = 11$, $y = 18$.

Ponadto niech $d = 17$, wówczas:

$$x = g^{d} \text{MOD } p = 28^{17} \text{ MOD } 47 = 21 .$$

Kluczem publicznym podpisującego jest piątka (47, 23, 28, 18, 21), a kluczem prywatnym są wartości $a = 11$ oraz $d = 17$. Wiadomością, którą podpisujący chce zatwierdzić, jest wartość $w = 110$.

Obliczenie podpisu wymaga wylosowania różnej od zera liczby $t \in \mathbf{Z}_{23}$; niech $t = 19$. Oblicza się wartości:

$$T = g^{t} \text{MOD } p = 28^{19} \text{ MOD } 47 = 14 ,$$

$$w' = Ttdw \text{ MOD } q = 14 \cdot 19 \cdot 17 \cdot 110 \text{ MOD } 23 = 22 .$$

Generowany jest podpis ElGamala dla wiadomości w'. Niech liczba k, $k \leq 46$ oraz względnie pierwsza z $q - 1 = 22$ jest równa $k = 41$. Wówczas wartość l wynosi:

$$l = g^{k} \text{MOD } p = 28^{41} \text{ MOD } 47 = 24 ,$$

a podpis s wyznacza się z zależności $w' \equiv la + ks \pmod{q}$, zatem:

$$22 \equiv 24 \cdot 11 + 41 \cdot s \pmod{23} ,$$

skąd $s = 7$. Podpisem jest para (24, 7) oraz wartość $T = 14$.

Weryfikacja podpisu dokonuje się etapami. Podmiot weryfikujący losuje dwie liczby: δ i ε; niech $\delta = 7$ oraz $\varepsilon = 12$. Wykorzystując te liczby, oblicza wartość:

$$c = T^{Tw\delta} g^{\varepsilon} \text{ MOD } p = 14^{14\cdot 110\cdot 7} 28^{12} \text{ MOD } 47 = 21,$$

którą przesyła podpisującemu. Ten z kolei losuje liczbę γ; niech γ = 16. Podpisujący oblicza dwie wartości:

$$h_1 = cg^{\gamma} \text{MOD } p = 21 \cdot 28^{16} \text{ MOD } 47 = 4,$$

$$h_2 = h_1^d \text{MOD } p = 4^{17} \text{ MOD } 47 = 27.$$

Wartości te wysyła weryfikującemu, a ten przesyła podpisującemu wartości δ i ε. Za pomocą tych wartości podpisujący sprawdza równość:

$$c = T^{Tw\delta} g^{\varepsilon} \text{ MOD } p$$

i przesyła γ weryfikującemu. Ostatecznie weryfikujący sprawdza, czy zachodzi:

$$h_1 = T^{Tw\delta} g^{\varepsilon+\gamma} \text{MOD } p = 14^{14\cdot 110\cdot 7} 28^{12+16} \text{ MOD } 47 = 4$$

oraz:

$$h_2 = y^{l\delta} l^{s\delta} x^{\varepsilon+\gamma} \text{MOD } p = 18^{24\cdot 7} 24^{7\cdot 7} 21^{12+16} \text{ MOD } 47 = 27.$$

Podsumowanie

Bezpieczeństwo implementowanych protokołów, a także ich funkcjonalność są jednymi z najistotniejszych zagadnień, jakimi zajmuje się współczesna kryptografia. Tworzenie bezpiecznych algorytmów jest możliwe dzięki stosowaniu pewnych trudnych do rozwiązania problemów dla dużych liczb całkowitych, takich jak np. znajdowanie logarytmu dyskretnego w cyklicznej podgrupie rzędu q należącej do $\mathbf{Z}_p^*$. Trudność rozwiązywania tych zagadnień daje gwarancję bezpieczeństwa wykorzystywanych protokołów, a zarazem bezpieczeństwa przeprowadzanych operacji.

Przedstawione w tej pracy protokoły Chauma-van Antwerpena oraz protokół przekształcalnych podpisów niezaprzeczalnych są protokołami podpisów ukazującymi zastosowanie zmodyfikowanych algorytmów podpisów cyfrowych, których weryfikacja wymaga bezpośredniej konfrontacji z podmiotem składającym podpis. Jest to użyteczne zwłaszcza wtedy, gdy podmiot podpisujący chce mieć kontrolę nad weryfikacją podpisu oraz nad podmiotami weryfikującymi.

Istnieją inne warianty podpisów niezaprzeczalnych (według [2; 4]). W niektórych rozgranicza się relacje: podpisujący – wiadomość i podpisujący – podpis – istnieje wówczas możliwość sprawdzenia przez dowolny podmiot, czy podpisujący złożył dany podpis, a konfrontacja z podpisującym jest wymagana

tylko w celu zweryfikowania, czy dany podpis jest właściwy dla konkretnej wiadomości. Pewnym wariantem podpisów niezaprzeczalnych są także powierzone podpisy niezaprzeczalne, które charakteryzują się tym, iż protokół zaprzeczający (wykonywany w przypadku wątpliwości dotyczących podpisu) może być przeprowadzony przez trzecią, niezależną stronę. Nieco innym wariantem są podpisy cyfrowe z wyznaczonym potwierdzającym – w tym wariancie weryfikacja podpisu może być dokonana przez osobę podpisującą, a także przez trzeci, specjalnie do tego celu wyznaczony podmiot. Takie podpisy mogą zapobiegać fałszywym zastosowaniom podpisu, stanowią ochronę w przypadku utraty klucza, dają możliwość zweryfikowania podpisu, gdy podmiot podpisujący jest aktualnie nieobecny. Jeszcze inną wersję podpisów można stworzyć łącząc niezaprzeczalne podpisy cyfrowe z algorytmami podziału sekretu – istniałaby wówczas możliwość scedowania weryfikacji podpisu na wybraną grupę n osób, z której do każdego protokołu weryfikacji byłaby potrzebna podgrupa złożona z co najmniej k, $k \leq n$, osób.

Można zauważyć, że możliwości zastosowań omawianych zagadnień są dosyć duże, a ich użyteczność znacząca. Tworzenie i stosowanie protokołów nie byłoby jednak możliwe bez implementacji pojęć matematycznych. Zatem znajomość pojęć, zwłaszcza z zakresu teorii liczb i algebry, jest kluczowym elementem współtworzenia współczesnej kryptografii.

Literatura

Wydawnictwa zwarte

1. Buchmann A.J.: *Wprowadzenie do kryptografii*. Wydawnictwo Naukowe PWN, Warszawa 2006.
2. Menezes A.J., Oorschot P.C. van, Vanstone S.A.: *Kryptografia stosowana*. Wydawnictwo Naukowo-Techniczne, Warszawa 2005.
3. Ross K.A., Wright C.R.B.: *Matematyka dyskretna*. Wydawnictwo Naukowe PWN, Warszawa 2003.
4. Schneier B.: *Kryptografia dla praktyków*. Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
5. Song Y. Yan: *Teoria liczb w informatyce*. Wydawnictwo Naukowe PWN, Warszawa 2006.

Strony internetowe

http://www.podpis.nordea.pl.

UNDENIABLE SIGNATURES – SIGNATURES WITH ADDITIONAL FUNCTIONALITY

Summary

Today, the role of digital signatures becoming more and more significant. The signature provides authentication and integrity of a message but quite often other features like additional functionality is required from the signature. Because of that the algorithms used in ordinary signing are not sufficient, they need to be special algorithms with some additional characteristics. Undeniable signatures are a form of digital signature that have two distinctive features: the verification process is interactive (the signatures cannot be verified without signer's cooperation), a disavowal protocol allows to determine whether a given signature is a forgery. These signatures can be used, for example, to protect a software against unauthorized persons. The safety of these signatures is guaranteed by techniques of modern cryptography which is based on advanced mathematical tools and computer technology.

The purpose of the article is to present selected schemes (protocols) of undeniable signatures (based on discrete log systems) such as Chaum-van Antwerpen protocol, Chaum-van Antwerpen protocol protecting against disavowal and a convertible undeniable signature protocol. Main definitions and theorems are presented and all described protocols are illustrated with examples.