Kryptografia

z elementami kryptografii kwantowej

Ryszard Tanaś

http://zon8.physd.amu.edu.pl/~tanas

Wykład 9

Spis treści

14 Podpis cyfrowy

14.1 Przypomnienie

- System kryptograficzny z kluczem publicznym może być wykorzystany do podpisywania dokumentów cyfrowych.
- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

14 Podpis cyfrowy

14.1 Przypomnienie

- System kryptograficzny z kluczem publicznym może być wykorzystany do podpisywania dokumentów cyfrowych.
- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

14 Podpis cyfrowy

14.1 Przypomnienie

- System kryptograficzny z kluczem publicznym może być wykorzystany do podpisywania dokumentów cyfrowych.
- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

14 Podpis cyfrowy

14.1 Przypomnienie

- System kryptograficzny z kluczem publicznym może być wykorzystany do podpisywania dokumentów cyfrowych.
- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

14 Podpis cyfrowy

14.1 Przypomnienie

- System kryptograficzny z kluczem publicznym może być wykorzystany do podpisywania dokumentów cyfrowych.
- Alicja szyfruje dokument używając swojego klucza prywatnego, podpisując w ten sposób dokument
- Alicja przesyła tak podpisany dokument do Bolka
- Bolek deszyfruje dokument używając klucza publicznego Alicji, weryfikując w ten sposób podpis Alicji

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.2 Cechy podpisu

- Podpis jest prawdziwy; Bolek weryfikuje go deszyfrując kryptogram kluczem publicznym Alicji
- Podpis nie może być sfałszowany;
  tylko Alicja zna jej klucz prywatny
- Podpis nie może być przeniesiony do innego dokumentu
- Podpisany dokument nie może być zmieniony; zmieniony dokument nie da się rozszyfrować kluczem publicznym Alicji
- Podpis jest niezaprzeczalny;
- Wada: podpis jest conajmniej tak długi jak sam dokument

14.3 Podpis z wykorzystaniem jednokierunkowej funkcji hashującej

- Alicja używa funkcji hashującej do dokumentu, który ma podpisać, otrzymując skrót („odcisk palca") dokumentu
- Alicja podpisuje skrót dokumentu szyfrując go swoim kluczem prywatnym
- Alicja przesyła Bolkowi dokument i podpisany skrót
- Bolek używa tej samej funkcji hashującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego Alicji; jeśli zdeszyfrowany skrót zgadza się z otrzymanym przez niego od Alicji to podpis jest prawdziwy

14.3 Podpis z wykorzystaniem jednokierunkowej funkcji hashującej

- Alicja używa funkcji hashującej do dokumentu, który ma podpisać, otrzymując skrót („odcisk palca") dokumentu
- Alicja podpisuje skrót dokumentu szyfrując go swoim kluczem prywatnym
- Alicja przesyła Bolkowi dokument i podpisany skrót
- Bolek używa tej samej funkcji hashującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego Alicji; jeśli zdeszyfrowany skrót zgadza się z otrzymanym przez niego od Alicji to podpis jest prawdziwy

14.3 Podpis z wykorzystaniem jednokierunkowej funkcji hashującej

- Alicja używa funkcji hashującej do dokumentu, który ma podpisać, otrzymując skrót („odcisk palca") dokumentu
- Alicja podpisuje skrót dokumentu szyfrując go swoim kluczem prywatnym
- Alicja przesyła Bolkowi dokument i podpisany skrót
- Bolek używa tej samej funkcji hashującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego Alicji; jeśli zdeszyfrowany skrót zgadza się z otrzymanym przez niego od Alicji to podpis jest prawdziwy

14.3 Podpis z wykorzystaniem jednokierunkowej funkcji hashującej

- Alicja używa funkcji hashującej do dokumentu, który ma podpisać, otrzymując skrót („odcisk palca") dokumentu
- Alicja podpisuje skrót dokumentu szyfrując go swoim kluczem prywatnym
- Alicja przesyła Bolkowi dokument i podpisany skrót
- Bolek używa tej samej funkcji hashującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego Alicji; jeśli zdeszyfrowany skrót zgadza się z otrzymanym przez niego od Alicji to podpis jest prawdziwy

14.3 Podpis z wykorzystaniem jednokierunkowej funkcji hashującej

- Alicja używa funkcji hashującej do dokumentu, który ma podpisać, otrzymując skrót („odcisk palca") dokumentu
- Alicja podpisuje skrót dokumentu szyfrując go swoim kluczem prywatnym
- Alicja przesyła Bolkowi dokument i podpisany skrót
- Bolek używa tej samej funkcji hashującej do otrzymania skrótu dokumentu, a następnie deszyfruje podpisany skrót używając klucza publicznego Alicji; jeśli zdeszyfrowany skrót zgadza się z otrzymanym przez niego od Alicji to podpis jest prawdziwy

- Podpis jest znacznie krótszy od dokumentu
- Można sprawdzić istnienie podpisu bez oglądania samego dokumentu

- Podpis jest znacznie krótszy od dokumentu
- Można sprawdzić istnienie podpisu bez oglądania samego dokumentu

14.4 Schemat ElGamala podpisu cyfrowego

14.4.1 Generowanie kluczy

- Alicja wybiera dużą liczbę pierwszą p oraz liczbę $g \in \mathbb{Z}_p$ (generator grupy multiplikatywnej $\mathbb{Z}_p^*$)
- Alicja wybiera liczbę losową $0 < a < p - 1$ oraz oblicza $b \equiv g^a \pmod{p}$
- Kluczem publicznym Alicji są liczby $\{b, g, p\}$ zaś kluczem prywatnym liczby $\{a, g, p\}$

14.4 Schemat ElGamala podpisu cyfrowego

14.4.1 Generowanie kluczy

- Alicja wybiera dużą liczbę pierwszą p oraz liczbę $g \in \mathbb{Z}_p$ (generator grupy multiplikatywnej $\mathbb{Z}_p^*$)
- Alicja wybiera liczbę losową $0 < a < p - 1$ oraz oblicza $b \equiv g^a \pmod{p}$
- Kluczem publicznym Alicji są liczby $\{b, g, p\}$ zaś kluczem prywatnym liczby $\{a, g, p\}$

14.4 Schemat ElGamala podpisu cyfrowego

14.4.1 Generowanie kluczy

- Alicja wybiera dużą liczbę pierwszą p oraz liczbę $g \in \mathbb{Z}_p$ (generator grupy multiplikatywnej $\mathbb{Z}_p^*$)
- Alicja wybiera liczbę losową $0 < a < p - 1$ oraz oblicza $b \equiv g^a \pmod{p}$
- Kluczem publicznym Alicji są liczby $\{b, g, p\}$ zaś kluczem prywatnym liczby $\{a, g, p\}$

14.4 Schemat ElGamala podpisu cyfrowego

14.4.1 Generowanie kluczy

- Alicja wybiera dużą liczbę pierwszą p oraz liczbę $g \in \mathbb{Z}_p$ (generator grupy multiplikatywnej $\mathbb{Z}_p^*$)
- Alicja wybiera liczbę losową $0 < a < p - 1$ oraz oblicza $b \equiv g^a \pmod{p}$
- Kluczem publicznym Alicji są liczby $\{b, g, p\}$ zaś kluczem prywatnym liczby $\{a, g, p\}$

14.4.2 Podpisywanie

- Alicja wybiera liczbę losową k (tajną), taką, że $0 < k < p-1$ oraz $NWD(k, p-1) = 1$
- Alicja oblicza

  $$r = g^k \pmod{p},$$

  $$k^{-1} \pmod{p-1},$$

  $$s = k^{-1}\left[H(M) - ar\right] \pmod{p-1}.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.4.2 Podpisywanie

- Alicja wybiera liczbę losową k (tajną), taką, że $0 < k < p-1$ oraz $NWD(k, p-1) = 1$
- Alicja oblicza

  $$r = g^k \pmod{p},$$

  $$k^{-1} \pmod{p-1},$$

  $$s = k^{-1}\left[H(M) - ar\right] \pmod{p-1}.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.4.2 Podpisywanie

- Alicja wybiera liczbę losową k (tajną), taką, że $0 < k < p-1$ oraz $NWD(k, p-1) = 1$
- Alicja oblicza

$$r = g^k \pmod{p},$$

$$k^{-1} \pmod{p-1},$$

$$s = k^{-1}\left[H(M) - ar\right] \pmod{p-1}.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.4.2 Podpisywanie

- Alicja wybiera liczbę losową k (tajną), taką, że $0 < k < p-1$ oraz $NWD(k, p-1) = 1$
- Alicja oblicza

  $$r = g^k \pmod{p},$$

  $$k^{-1} \pmod{p-1},$$

  $$s = k^{-1}\left[H(M) - ar\right] \pmod{p-1}.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.4.3 Weryfikacja

- Bolek aby stwierdzić prawdziwość podpisu Alicji pobiera klucz publiczny Alicji $\{b, g, p\}$
- Bolek sprawdza czy $0 < r < p$, jeśli nie, podpis nie jest prawdziwy
- Bolek oblicza

  $x_1 = b^r r^s \pmod{p}$,

  $x_2 = g^{H(M)} \pmod{p}$.
- Bolek akceptuje podpis jeśli $x_1 = x_2$

14.4.3 Weryfikacja

- Bolek aby stwierdzić prawdziwość podpisu Alicji pobiera klucz publiczny Alicji $\{b, g, p\}$
- Bolek sprawdza czy $0 < r < p$, jeśli nie, podpis nie jest prawdziwy
- Bolek oblicza

  $x_1 = b^r r^s \pmod{p}$,

  $x_2 = g^{H(M)} \pmod{p}$.
- Bolek akceptuje podpis jeśli $x_1 = x_2$

14.4.3 Weryfikacja

- Bolek aby stwierdzić prawdziwość podpisu Alicji pobiera klucz publiczny Alicji $\{b, g, p\}$
- Bolek sprawdza czy $0 < r < p$, jeśli nie, podpis nie jest prawdziwy
- Bolek oblicza

  $x_1 = b^r r^s \pmod{p}$,

  $x_2 = g^{H(M)} \pmod{p}$.
- Bolek akceptuje podpis jeśli $x_1 = x_2$

14.4.3 Weryfikacja

- Bolek aby stwierdzić prawdziwość podpisu Alicji pobiera klucz publiczny Alicji $\{b, g, p\}$
- Bolek sprawdza czy $0 < r < p$, jeśli nie, podpis nie jest prawdziwy
- Bolek oblicza

  $$x_1 = b^r r^s \pmod{p},$$

  $$x_2 = g^{H(M)} \pmod{p}.$$

- Bolek akceptuje podpis jeśli $x_1 = x_2$

14.4.3 Weryfikacja

- Bolek aby stwierdzić prawdziwość podpisu Alicji pobiera klucz publiczny Alicji $\{b, g, p\}$
- Bolek sprawdza czy $0 < r < p$, jeśli nie, podpis nie jest prawdziwy
- Bolek oblicza

  $x_1 = b^r r^s \pmod{p}$,

  $x_2 = g^{H(M)} \pmod{p}$.
- Bolek akceptuje podpis jeśli $x_1 = x_2$

14.4.4 Uzasadnienie

Ponieważ

$$s \equiv k^{-1}\left[H(M) - ar\right] \pmod{p-1},$$

to mnożąc stronami przez k mamy

$$ks \equiv H(M) - ar \pmod{p-1}$$

i po przekształceniu

$$H(M) \equiv ar + ks \pmod{p-1},$$

a co za tym idzie

$$g^{H(M)} \equiv g^{ar+ks} \equiv (g^a)^r r^s \equiv b^r r^s \pmod{p}.$$

Tak więc

$$x_1 = x_2.$$

14.5 DSA — Digital Signature Algorithm

- Algorytm podpisu cyfrowego zatwierdzony w 1994 r. przez NIST jako standard podpisu cyfrowego w USA (Digital Signature Standard — DSS).
- Wykorzystuje funkcję hashującą SHA-1.

14.5 DSA — Digital Signature Algorithm

- Algorytm podpisu cyfrowego zatwierdzony w 1994 r. przez NIST jako standard podpisu cyfrowego w USA (Digital Signature Standard — DSS).
- Wykorzystuje funkcję hashującą SHA-1.

14.5 DSA — Digital Signature Algorithm

- Algorytm podpisu cyfrowego zatwierdzony w 1994 r. przez NIST jako standard podpisu cyfrowego w USA (Digital Signature Standard — DSS).
- Wykorzystuje funkcję hashującą SHA-1.

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$
- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$
- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$
- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$
- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$
- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.1 Generacja klucza

- Alicja wybiera liczbę pierwszą q o długości 160 bitów
- Alicja wybiera liczbę pierwszą p o długości $512 \leq l \leq 1024$, przy czym $64|l$, taką, że $q|p-1$
- Alicja wybiera element $g \in \mathbb{Z}_p$ i oblicza
  $b = g^{(p-1)/q} \pmod{p}$;
  jeśli $b = 1$ to wybiera inne g.
- Alicja wybiera liczbę losową a, $0 < a < q$, i oblicza $c = b^a \pmod{p}$

- Kluczem publicznym Alicji jest zbiór liczb $\{b, c, p, q\}$

14.5.2 Podpisywanie

- Alicja wybiera tajną liczbę losową k, $0 < k < q$,
- Alicja oblicza

  $$r = (b^k \pmod p) \pmod q,$$

  $$k^{-1} \pmod q,$$

  $$s = k^{-1} \left[H(M) + ar \right] \pmod q.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.5.2 Podpisywanie

- Alicja wybiera tajną liczbę losową k, $0 < k < q$,
- Alicja oblicza

  $$r = (b^k \pmod p) \pmod q,$$

  $$k^{-1} \pmod q,$$

  $$s = k^{-1} \left[H(M) + ar \right] \pmod q.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.5.2 Podpisywanie

- Alicja wybiera tajną liczbę losową k, $0 < k < q$,
- Alicja oblicza

$$r = (b^k \pmod p) \pmod q,$$

$$k^{-1} \pmod q,$$

$$s = k^{-1} \left[H(M) + ar \right] \pmod q.$$

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.5.2 Podpisywanie

- Alicja wybiera tajną liczbę losową k, $0 < k < q$,
- Alicja oblicza

  $r = (b^k \pmod p) \pmod q$,

  $k^{-1} \pmod q$,

  $s = k^{-1} \left[H(M) + ar \right] \pmod q$.

- Podpisem Alicji dla wiadomości M jest para liczb $\{r, s\}$

14.5.3 Weryfikacja

- Bolek pobiera klucz publiczny Alicji $\{b, c, p, q\}$
- Bolek sprawdza czy $0 < r < q$ i $0 < s < q$, jeśli nie, to podpis jest fałszywy
- Bolek oblicza

  $H(M)$ i $w = s^{-1} \pmod{q}$,

  $u_1 = w\, H(M) \pmod{q}$,

  $u_2 = rw \pmod{q}$,

  $v = (b^{u_1} c^{u_2} \pmod{p}) \pmod{q}$.
- Bolek uznaje podpis za prawdziwy jeśli $v = r$.

14.5.3 Weryfikacja

- Bolek pobiera klucz publiczny Alicji $\{b, c, p, q\}$
- Bolek sprawdza czy $0 < r < q$ i $0 < s < q$, jeśli nie, to podpis jest fałszywy
- Bolek oblicza

  $H(M)$ i $w = s^{-1} \pmod{q}$,

  $u_1 = w\,H(M) \pmod{q}$,

  $u_2 = rw \pmod{q}$,

  $v = (b^{u_1} c^{u_2} \pmod{p}) \pmod{q}$.
- Bolek uznaje podpis za prawdziwy jeśli $v = r$.

14.5.3 Weryfikacja

- Bolek pobiera klucz publiczny Alicji $\{b, c, p, q\}$
- Bolek sprawdza czy $0 < r < q$ i $0 < s < q$, jeśli nie, to podpis jest fałszywy
- Bolek oblicza

  $H(M)$ i $w = s^{-1} \pmod{q}$,

  $u_1 = w\, H(M) \pmod{q}$,

  $u_2 = rw \pmod{q}$,

  $v = (b^{u_1} c^{u_2} \pmod{p}) \pmod{q}$.
- Bolek uznaje podpis za prawdziwy jeśli $v = r$.

14.5.3 Weryfikacja

- Bolek pobiera klucz publiczny Alicji $\{b, c, p, q\}$
- Bolek sprawdza czy $0 < r < q$ i $0 < s < q$, jeśli nie, to podpis jest fałszywy
- Bolek oblicza

  $H(M)$ i $w = s^{-1} \pmod{q}$,

  $u_1 = w\, H(M) \pmod{q}$,

  $u_2 = rw \pmod{q}$,

  $v = (b^{u_1} c^{u_2} \pmod{p}) \pmod{q}$.
- Bolek uznaje podpis za prawdziwy jeśli $v = r$.

14.5.3 Weryfikacja

- Bolek pobiera klucz publiczny Alicji $\{b, c, p, q\}$
- Bolek sprawdza czy $0 < r < q$ i $0 < s < q$, jeśli nie, to podpis jest fałszywy
- Bolek oblicza

  $H(M)$ i $w = s^{-1} \pmod{q}$,

  $u_1 = w\, H(M) \pmod{q}$,

  $u_2 = rw \pmod{q}$,

  $v = (b^{u_1} c^{u_2} \pmod{p}) \pmod{q}$.
- Bolek uznaje podpis za prawdziwy jeśli $v = r$.

14.5.4 Uzasadnienie

Jeśli $\{r, s\}$ jest prawdziwym podpisem Alicji dla wiadomości M, to

$H(M) \equiv -ar + ks \pmod{q}$.

Mnożąc stronami przez w i przekształcając otrzymujemy

$w\,H(M) + arw \equiv k \pmod{q}$,

co jest równoważne

$u_1 + au_2 \equiv k \pmod{q}$.

Podnosząc b do potęgi lewej i prawej strony tej kongruencji otrzymujemy

$(b^{u_1+au_2} \pmod{p}) \pmod{q} \equiv (b^k \pmod{p}) \pmod{q}$

i dalej mamy

$(b^{u_1} c^{u_2} \pmod{p}) \pmod{q} \equiv (b^k \pmod{p}) \pmod{q}$,

a to oznacza $v = r$.

14.6 Ślepe podpisy cyfrowe

- Zasadniczym założeniem protokołów podpisów cyfrowych jest, że podpisujący dokument wie co podpisuje. Nie należy podpisywać dokumentów wyglądających na losowy ciąg bitów.

- Od powyższej zasady są jednak odstępstwa.
  - Przypuśćmy, że Bolek jest notariuszem, zaś Alicja chce aby Bolek potwierdził notarialnie istnienie dokumentu, ale nie chce aby ten dokument obejrzał.
  - Mamy wtedy do czynienia z tzw. ślepym podpisem.

14.6 Ślepe podpisy cyfrowe

- Zasadniczym założeniem protokołów podpisów cyfrowych jest, że podpisujący dokument wie co podpisuje. Nie należy podpisywać dokumentów wyglądających na losowy ciąg bitów.

- Od powyższej zasady są jednak odstępstwa.
  - Przypuśćmy, że Bolek jest notariuszem, zaś Alicja chce aby Bolek potwierdził notarialnie istnienie dokumentu, ale nie chce aby ten dokument obejrzał.
  - Mamy wtedy do czynienia z tzw. ślepym podpisem.

14.6 Ślepe podpisy cyfrowe

- Zasadniczym założeniem protokołów podpisów cyfrowych jest, że podpisujący dokument wie co podpisuje. Nie należy podpisywać dokumentów wyglądających na losowy ciąg bitów.

- Od powyższej zasady są jednak odstępstwa.
  - Przypuśćmy, że Bolek jest notariuszem, zaś Alicja chce aby Bolek potwierdził notarialnie istnienie dokumentu, ale nie chce aby ten dokument obejrzał.
  - Mamy wtedy do czynienia z tzw. ślepym podpisem.

14.6 Ślepe podpisy cyfrowe

- Zasadniczym założeniem protokołów podpisów cyfrowych jest, że podpisujący dokument wie co podpisuje. Nie należy podpisywać dokumentów wyglądających na losowy ciąg bitów.

- Od powyższej zasady są jednak odstępstwa.
  - Przypuśćmy, że Bolek jest notariuszem, zaś Alicja chce aby Bolek potwierdził notarialnie istnienie dokumentu, ale nie chce aby ten dokument obejrzał.
  - Mamy wtedy do czynienia z tzw. ślepym podpisem.

14.6 Ślepe podpisy cyfrowe

- Zasadniczym założeniem protokołów podpisów cyfrowych jest, że podpisujący dokument wie co podpisuje. Nie należy podpisywać dokumentów wyglądających na losowy ciąg bitów.

- Od powyższej zasady są jednak odstępstwa.
  - Przypuśćmy, że Bolek jest notariuszem, zaś Alicja chce aby Bolek potwierdził notarialnie istnienie dokumentu, ale nie chce aby ten dokument obejrzał.
  - Mamy wtedy do czynienia z tzw. ślepym podpisem.

- Wyobraźmy sobie taką systuację:
  - Alicja wkłada list do koperty łącznie z kalką, zakleja kopertę, a potem prosi Bolka o złożenie podpisu na zaklejonej kopercie.
  - Po otwarciu koperty na liście będzie kopia podpisu Bolka.
- Cyfrowo ślepy podpis można zrealizować korzystając np. z algorytmu RSA.

- Wyobraźmy sobie taką systuację:
  - Alicja wkłada list do koperty łącznie z kalką, zakleja kopertę, a potem prosi Bolka o złożenie podpisu na zaklejonej kopercie.
  - Po otwarciu koperty na liście będzie kopia podpisu Bolka.
- Cyfrowo ślepy podpis można zrealizować korzystając np. z algorytmu RSA.

- Wyobraźmy sobie taką systuację:
  - Alicja wkłada list do koperty łącznie z kalką, zakleja kopertę, a potem prosi Bolka o złożenie podpisu na zaklejonej kopercie.
  - Po otwarciu koperty na liście będzie kopia podpisu Bolka.
- Cyfrowo ślepy podpis można zrealizować korzystając np. z algorytmu RSA.

- Wyobraźmy sobie taką systuację:
  - Alicja wkłada list do koperty łącznie z kalką, zakleja kopertę, a potem prosi Bolka o złożenie podpisu na zaklejonej kopercie.
  - Po otwarciu koperty na liście będzie kopia podpisu Bolka.
- Cyfrowo ślepy podpis można zrealizować korzystając np. z algorytmu RSA.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod n$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod n$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod n$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod n$, więc
  $z^d/k = M^d k/k \equiv M^d \pmod n$, czyli
  $s = M^d \pmod n$
  jest podpisem Bolka na wiadomości M.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod n$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod n$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod n$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod n$, więc
  $z^d/k = M^d k/k \equiv M^d \pmod n$, czyli
  $s = M^d \pmod n$
  jest podpisem Bolka na wiadomości M.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod n$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod n$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod n$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod n$, więc
  $z^d/k = M^d k/k \equiv M^d \pmod n$, czyli
  $s = M^d \pmod n$
  jest podpisem Bolka na wiadomości M.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod{n}$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod{n}$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod{n}$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod{n}$, więc
  $z^d/k = M^d k/k \equiv M^d \pmod{n}$, czyli
  $s = M^d \pmod{n}$
  jest podpisem Bolka na wiadomości M.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod n$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod n$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod n$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod n$, więc

  $z^d/k = M^d k/k \equiv M^d \pmod n$, czyli

  $s = M^d \pmod n$

  jest podpisem Bolka na wiadomości M.

14.6.1 Ślepy podpis z użyciem RSA

- Alicja pobiera klucz publiczny Bolka $\{e, n\}$
- Alicja wybiera liczbę losową k, $0 < k < n$,
- Alicja oblicza $z = M\,k^e \pmod n$ i przesyła z do Bolka
- Bolek oblicza $z^d = (M\,k^e)^d \pmod n$ używając swojego klucza prywatnego $\{d, n\}$ i wynik przesyła Alicji
- Alicja oblicza $s = z^d/k \pmod n$. Ponieważ $z^d \equiv (M\,k^e)^d \equiv M^d k \pmod n$, więc
  $z^d/k = M^d k/k \equiv M^d \pmod n$, czyli
  $s = M^d \pmod n$
  jest podpisem Bolka na wiadomości M.

14.7 Niezaprzeczalne podpisy cyfrowe

- Podpis niezaprzeczalny nie może być sprawdzony bez zgody osoby podpisującej.
- Podpisujący nie może się wyprzeć swojego podpisu,
- ale może także dowieść, że podpis jest fałszywy (jeśli jest).

14.7 Niezaprzeczalne podpisy cyfrowe

- Podpis niezaprzeczalny nie może być sprawdzony bez zgody osoby podpisującej.
- Podpisujący nie może się wyprzeć swojego podpisu,
- ale może także dowieść, że podpis jest fałszywy (jeśli jest).

14.7 Niezaprzeczalne podpisy cyfrowe

- Podpis niezaprzeczalny nie może być sprawdzony bez zgody osoby podpisującej.
- Podpisujący nie może się wyprzeć swojego podpisu,
- ale może także dowieść, że podpis jest fałszywy (jeśli jest).

14.7 Niezaprzeczalne podpisy cyfrowe

- Podpis niezaprzeczalny nie może być sprawdzony bez zgody osoby podpisującej.
- Podpisujący nie może się wyprzeć swojego podpisu,
- ale może także dowieść, że podpis jest fałszywy (jeśli jest).

14.7.1 Niezaprzeczalny podpis oparty na logarytmach dyskretnych

Przypuśćmy, że stroną podpisującą dokument jest Alicja.

- Generacja klucza

  Alicja posiada klucz prywatny $\{a, g, p\}$ oraz klucz publiczny $\{b, g, p\}$ wygenerowany jak w algorytmie ElGamala.

- Podpisywanie

  Alicja oblicza $z = M^a \pmod{p}$ i to jest jej podpis dla dokumentu M

14.7.1 Niezaprzeczalny podpis oparty na logarytmach dyskretnych

Przypuśćmy, że stroną podpisującą dokument jest Alicja.

- Generacja klucza

  Alicja posiada klucz prywatny $\{a, g, p\}$ oraz klucz publiczny $\{b, g, p\}$ wygenerowany jak w algorytmie ElGamala.

- Podpisywanie

  Alicja oblicza $z = M^a \pmod{p}$ i to jest jej podpis dla dokumentu M

14.7.1 Niezaprzeczalny podpis oparty na logarytmach dyskretnych

Przypuśćmy, że stroną podpisującą dokument jest Alicja.

- Generacja klucza

  Alicja posiada klucz prywatny $\{a, g, p\}$ oraz klucz publiczny $\{b, g, p\}$ wygenerowany jak w algorytmie ElGamala.

- Podpisywanie

  Alicja oblicza $z = M^a \pmod{p}$ i to jest jej podpis dla dokumentu M

- Weryfikacja
  1. Bolek wybiera dwie liczby losowe r i s mniejsze od p, oblicza $w = z^r b^s \pmod{p}$ i przesyła Alicji
  2. Alicja oblicza
     $$t = a^{-1} \pmod{p-1}$$
     $$v = w^t \pmod{p}$$
     i przesyła Bolkowi v
  3. Bolek sprawdza czy $v = M^r g^s \pmod{p}$
- Uzasadnienie

  Zauważmy, że

  $v = w^t = z^{rt} b^{st} = (z^t)^r (b^t)^s = (M^{at})^r (g^{at})^s = M^r g^s \pmod{p}$

- Weryfikacja
  1. Bolek wybiera dwie liczby losowe r i s mniejsze od p, oblicza $w = z^r b^s \pmod p$ i przesyła Alicji
  2. Alicja oblicza
     $$t = a^{-1} \pmod{p-1}$$
     $$v = w^t \pmod p$$
     i przesyła Bolkowi v
  3. Bolek sprawdza czy $v = M^r g^s \pmod p$
- Uzasadnienie

  Zauważmy, że

  $$v = w^t = z^{rt} b^{st} = (z^t)^r (b^t)^s = (M^{at})^r (g^{at})^s = M^r g^s \pmod p$$

- Weryfikacja
  1. Bolek wybiera dwie liczby losowe r i s mniejsze od p, oblicza $w = z^r b^s \pmod{p}$ i przesyła Alicji
  2. Alicja oblicza
     $$t = a^{-1} \pmod{p-1}$$
     $$v = w^t \pmod{p}$$
     i przesyła Bolkowi v
  3. Bolek sprawdza czy $v = M^r g^s \pmod{p}$
- Uzasadnienie

  Zauważmy, że

  $v = w^t = z^{rt} b^{st} = (z^t)^r (b^t)^s = (M^{at})^r (g^{at})^s = M^r g^s \pmod{p}$

- Weryfikacja
  1. Bolek wybiera dwie liczby losowe r i s mniejsze od p, oblicza $w = z^r b^s \pmod{p}$ i przesyła Alicji
  2. Alicja oblicza
     $$t = a^{-1} \pmod{p-1}$$
     $$v = w^t \pmod{p}$$
     i przesyła Bolkowi v
  3. Bolek sprawdza czy $v = M^r g^s \pmod{p}$
- Uzasadnienie

  Zauważmy, że

  $$v = w^t = z^{rt} b^{st} = (z^t)^r (b^t)^s = (M^{at})^r (g^{at})^s = M^r g^s \pmod{p}$$

- Weryfikacja
  1. Bolek wybiera dwie liczby losowe r i s mniejsze od p, oblicza $w = z^r b^s \pmod{p}$ i przesyła Alicji
  2. Alicja oblicza
     $$t = a^{-1} \pmod{p-1}$$
     $$v = w^t \pmod{p}$$
     i przesyła Bolkowi v
  3. Bolek sprawdza czy $v = M^r g^s \pmod{p}$
- Uzasadnienie

  Zauważmy, że

  $$v = w^t = z^{rt} b^{st} = (z^t)^r (b^t)^s = (M^{at})^r (g^{at})^s = M^r g^s \pmod{p}$$