19 kwietnia 2024

Zadania z kryptografii, lista nr 7

1. (Założenie DL) Niech $p = 2q + 1$ (p, q–pierwsze) i g rzędu q w $\mathbb{Z}_p^*$. Załóżmy, że istnieje wielomianowy algorytm probabilistyczny A obliczający dla losowego g^x liczbę x z prawdopodobieństwem co najmniej $1/w(l)$ gdzie w jest wielomianem a l długością p. Skonstruuj wielomianowy algorytm probabilistyczny obliczający X dla zadanego g^X z prawdopodobieństwem 0.9999. Czy zadanie to jest trudniejsze, jeśli algorytm A zwraca w przypadku niepowodzenia odpowiedź nieprawdziwą?

2. (Założenie CDH) Niech $p = 2q+1$ (p, q–pierwsze) i g rzędu q w $\mathbb{Z}_p^*$. Załóżmy, że istnieje wielomianowy algorytm probabilistyczny A obliczający dla losowych g^a, g^b liczbę g^{ab} z prawdopodobieństwem co najmniej $1/w(l)$ gdzie w jest wielomianem a l długością p. Jeśli mu to się nie uda nie zwraca żadnej odpowiedzi. Skonstruuj wielomianowy algorytm probabilistyczny obliczający g^{AB} dla zadanych g^A, g^B z prawdopodobieństwem 0.9999. Jak zmieni się rozwiązanie, gdy algorytm A w przypadku niepowodzenia zwraca nieprawdziwą odpowiedź?

3. (Założenie DDH) Niech $p = 2q+1$ (p, q–pierwsze) i g rzędu q w $\mathbb{Z}_p^*$. Załóżmy, że istnieje wielomianowy algorytm probabilistyczny A odróżniający dla losowych g^a, g^b liczby $z = g^{ab}$ i $z = g^r : r \in_R \mathbb{Z}_q$ z niezaniedbywalnym prawdopodobieństwem tzn., dla którego

$$\Pr(A(g^{ab}) = 1) - \Pr(A(g^r) = 1) \geq 1/w(l)$$

gdzie w jest wielomianem a l długością p. Skonstruuj wielomianowy algorytm probabilistyczny, który przy zadanych g^A, g^B, z dla $z = g^{AB}$ zwraca 1, dla jakiegokolwiek $z = g^R : R \neq AB$ zwraca 0 i myli się z prawdopodobieństwem poniżej 0.0001.

4. Nie jest znany wielomianowy algorytm sprawdzający czy reszta x modulo $n = pq$ (rozkład n jest nieznany) jest resztą kwadratową. Zbiór reszt kwadratowych w $\mathbb{Z}_n^*$ oznaczamy przez $QR(n)$, a zbiór niereszt kwadratowych $x \in \mathbb{Z}_n^*$ dla których $\left(\frac{x}{n}\right) = 1$ oznaczamy przez $NQR(n)$.

   (a) Pokaż, że $|NQR(n)| = |QR(n)|$. Opowiedz jak latwo stwierdzić, że $x \in \mathbb{Z}_n^* \setminus NQR(n)$ nie jest resztą kwadratową.

   (b) Załóżmy, że istnieje wielomianowy algorytm probabilistyczny A, który zwraca dla losowej reszty x wartość 0 lub 1, taki że

   $$\Pr(A(x) = 1 | x \in QR(n)) - \Pr(A(x) = 1 | x \in NQR(n)) \geq 1/w(l)$$

   dla pewnego wielomianu w gdzie l jest długością n. Skonsruuj wielomianowy algorytm probabilistyczny, który z prawdopodobieństwem powyżej 0.9999 prawidłowo stwierdza dla $x \in \mathbb{Z}_n^*$, czy x jest resztą kwadratową.

5. (Trudne bity RSA) Niech $n = pq, e$ będą publicznym kluczem RSA. Na wykładzie podany został dowód faktu, że jeśli istnieje wielomianowa funkcja HALF(m^e), gdzie

$$\text{HALF}(m^e) = \begin{cases} 0 \text{ gdy } m < n/2 \\ 1 \text{ gdy } m > n/2, \end{cases} .$$

   to RSA może być odszyfrowane w czasie wielomianowym Sprowadź obliczanie funkcji HALF(m^e) do obliczania funkcji LAST(m^e) wyliczającej ostatni bit m czyli m mod 2. Pokaż też redukcję w drugą stronę.

6. (Trudne bity logarytmu dyskretnego) Niech $p = 2q + 1$ (p, q–pierwsze) i g rzędu q w $\mathbb{Z}_p^*$. Niech też $y = g^x$ gdzie $x \in \mathbb{Z}_q^*$ jest nieznane. Pokaż, jak dysponując wielomianową procedurą znajdującą ostatni bit x wyliczyć w czasie wielomianowym całe x. Pokaż też jak dysponując procedurą zwracającą 1 wtedy i tylko wtedy gdy $x > q/2$, można wyliczyć całe x.