

## EGZAMIN

## Polecenia i pytania (100p)

1. Zdefiniuj problemy izomorfizmu (GI) i nieizomorfizmu grafów (GNI).
  - (a) Pokaż dowód interaktywny dla GNI (uzasadnij jego poprawność)
  - (b) Pokaż dowód z wiedzą zerową dla GI (uzasadnij jego poprawność oraz to, że jest z wiedzą zerową)

*Uwaga:* uzasadnienia mogą być nieformalne (parę zdań). Nie trzeba przeprowadzać pełnego dowodu.

2. Podaj protokół Shamira podziału sekretu.
3. Podaj specyfikację (definicję) protokołu *Transferu Utajnionego* (ang. *Oblivious Transfer, OT*) (w dowolnej wersji).

Niech  $f_{\vee} \{0, 1\} \times \{0, 1\} \rightarrow \{0, 1\}$  będzie *alternatywą*, czyli funkcją zdefiniowaną jako:

$$f_{\vee}(A, B) = A \vee B \quad (1)$$

Pokaż jak za można zredukować problem bezpiecznego obliczenia alternatywy między Alicją (z wejściem  $A$ ) i Bobem (z wejściem  $B$ ) do problemu transferu utajnionego.

4. Podaj specyfikację (definicję) protokołu *Weryfikowalnego Podziału Sekretu* (*VSS*).
5. Co to jest *szyfr progowy*?
6. Nieformalnie wyjaśnij co to jest *dowód z desygnowanym weryfikatorem*?
7. Omów różnicę pomiędzy definicjami protokołów PIR i OT.
8. Co to są *ślepe podpisy*?

## Zadanie dodatkowe

**Definicja 1** *Protokołem Uzgadniania Klucza* (ang. *Key Agreement, KA*) nazywamy protokół pomiędzy Alicją i Bobem (będącymi zrandomizowanymi maszynami działającymi w czasie wielomianowym) w wyniku którego obie strony zwracają identyczny wynik (dla uproszczenia załóżmy, że jest to bit  $B$ ). Alicja i Bob przed rozpoczęciem protokołu nie posiadają żadnego wspólnego sekretu.

*Bezpieczeństwo KA* definiujemy następująco. Jakikolwiek przeciwnik (będący zrandomizowaną maszyną działającą w czasie wielomianowym) mający dostęp do kanału komunikacyjnego między Alicją i Bobem nie jest w stanie (z prawdopodobieństwem znacząco lepszym niż  $\frac{1}{2}$ ) zgadnąć wartości  $B$ .

(„Znacząco lepszym niż  $\frac{1}{2}$ ” oznacza, że prawdopodobieństwo to jest mniejsze niż  $\frac{1}{2} + \epsilon(k)$ , gdzie pewną  $\epsilon$  jest funkcją zaniedbywalną, a  $k$  jest parametrem bezpieczeństwa.)

Pokaż jak zredukować problem Uzgadniania Klucza do problemu Transferu Utajnionego.

Powodzenia!