7.04.03

BDC- Infrastruktura Klucza Publicznego, 2003
WPPT, Politechnika Wrocławska

Lista nr 4

1. P posiada trzy atrybuty $x_1, x_2, x_3 \in \mathbb{Z}_q$. Jak dowieść, że

$$x_1 + 2x_2 - 10x_3 = 13$$

oraz

$$x_2 - 4x_3 = 5?$$

2. P posiada trzy atrybuty $x_1, x_2, x_3 \in \mathbb{Z}_q$. Jak dowieść, że

$$x_1 + 3x_2 + 5x_3 \neq 7$$

oraz

$$3x_1 + 10x_2 + 18x_3 = 23?$$

3. Jak wykazać, że spełniona jest jedna (lub obie) z formuł z zadań 1 i 2?

4. Łatwe pytanie na rozgrzewkę: Wiadomo, że jednemu kluczowi publicznemu RSA odpowiada wiele prywatnych. Czy można wykorzystać to do zbudowania schematu podpisów grupowych? (W schemacie tym każdy członek grupy otrzymałby jeden z kluczy prywatnych odpowiadających kluczowi K).

5. Spróbować zmodyfikować poznane schematy podpisów grupowych tak, aby identyfikacja podpisującego była możliwa jedynie przy współpracy dwóch Zaufanych Stron Trzecich.

6. Rozszerzyć schemat Chen-Pedersen podpisu grupowego opartego o dowód z wiedzą zerową:
   (a) dla dowolnej liczby uczestników grupy,
   (b) o możliwość identyfikacji osoby podpisującej,
   (c) o możliwość utworzenia k podpisów przez tę samą osobę bez zdradzania (w sensie teorio-informacyjnym), że podpisała ta sama osoba.

7. Co zmieniłoby się w bezpieczeństwie schematu podpisu rozważanego w poprzednim zadaniu, gdyby grupa, w której prowadzone są obliczenia nie byłą cykliczna? Czy procedura weryfikacji nadal będzie funkcjonować? Czy zmieniłoby się bezpieczeństwo teorioinformacyjne?

8. Zaprojektować sygnaturę wiedzy „2 z 3“ opierając się na sygnaturze „1 z 2“. Wskazówka: narysować trójkąt i wierzchołkom przyporządkować sygnowane sekrety.

/-/ Mirosław Kutyłowski