18.03.03

BDC- Infrastruktura Klucza Publicznego, 2003
WPPT, Politechnika Wrocławska

Lista nr 3

1. Tak zaprojektuj protokół ujawniania wiadomosci zawartych w ślepym certyfikacie, by ujawniający CA mógł uczynić to tylko raz bez zdradzenia zakodowanych w nim wartości $x_1, \ldots, x_l$.
   (Certyfikaty o tej własności nazywamy *one-show certificate*.)

2. W celu ułatwienia dowodów bezpieczeństwa ślepych certyfikatów modyfikuje sie nieco schemat wydawania ślepych certyfikatów (modyfikacja ta niestety zwiększa skomplikowanie metody i jej „elegancję"). CA generuje dodatkowo losowy element f z podgrupy G rzędu q, losowy bit $t \in \{0,1\}$ oraz kładzie $h_0 = g_0^{y_0} \cdot f^t$. Certyfikat dla h' przyjmuje wtedy postać c_0', r_0', r_1' i spełnia równość

   $$c_0' = H(h', g_0^{r_0'} f^{r_1'} (h_0 h')^{-c_0'})$$

   Pokaż jak zmodyfikować oryginalny protokół aby spełniał te zależność.

3. Alicja wybiera losowo a oraz $b \in \{0,1\}$ a następnie kładzie $h_0 = g_1^b g_2^a$. Jak Alicja może przekonać Boba, że użyty parametr b faktycznie należy do zbioru $\{0,1\}$? Wskazówka: ogólna procedura ujawniania ...

4. Istnieje wiele pojęć związanych z dowodami z wiedzą zerową i o podobnym znaczeniu. Jednym z nich jest dowód *ukrywający świadka*. Dla ustalenia uwagi załóżmy, że funkcja f jest jednostronna, oraz że Alicja pragnie wykazać, że zna x takie, że $f(x) = z$. Załóżmy, że Bob może wykonywać obliczenia o wielomianowej długości. Wtedy dowód P ukrywa świadka x, jeśli istnieje wielomianowy algorytm W, nazywany *ekstraktorem świadka* taki, że

   $$|\Pr(f(S(T, z, n, aux) = z) - \Pr(W(z, n, aux, V) = z)| < \frac{1}{n^c}$$

   gdzie n ozacza długość x, T oznacza zapis przebiegu dowodu między Alicją a Bobem, aux oznacza losowe ciągi wybierane podczas dowodu, V oznacza strategię Boba.
   Czy dowód ukrywający świadka jest automatycznie bezpieczny dla sekretu x?
   Czy protokół dowodzący wiedzy DL-reprezentacji ukrywa świadka?

/-/ Mirosław Kutyłowski