Jak się pozbyć dilerów ? Distributed Key Generation

Na podstwie pracy R.Gennaro, S.Jareckiego, H.Krawczyka, T.Rabina - „Distributed Key Generation for Discrete-Log Based Cryptosystems”

1 kwietnia 2003 roku

- **Secret Sharing** (SS) - protokół dzielenia tajemnic. Stworzony przez A.Shamira w 1979 roku. Umożliwia **dilerowi** (trusted party) rozdanie między n uczestników tzw. udziałów (shares), w taki sposób aby dowolnych t+1 uczestników mogło (a żadne t nie mogło) odtworzyć na ich podstawie sekretu dielra. $t < n$ jest tu tzw. progiem. Secret Sharing doczekał się wielu realizacji, zastosowań i modyfikacji Składa się z faz podziału i rekosntrukci sekretu. Protokół SS ma poważne wady:

  1. Diler może wysyłć uczestnikom niepoprawne wartości (np. udziały różnych grup mogą definiować różne sekrety, albo nawet być sprzeczne)
  2. W fazie rekonstrukcji sekretu, uczestnicy mogą podać inne wartości, niż te które otrzymali od dilera.
  3. Nie można nikomu udowodnić zachowania niezgodnego z protokołem.

- **Verifiable Secret Sharing** (VSS). Umożliwia weryfikację tego, ze diler przesyła spójne udziały (definiujące ten sam sekret) a także to, że uczestnicy w fazie rekonstrukcji podają to co od dilera wcześniej dostali. Protokół ten ma jedną istotsną wadę. Mianowicie diler posiada pełną wiedzę o sekrecie. Jeśli dostanie się pod kontroelę wroga (nawet pasywnego), sekret zostanie ujawniony. Jest to wada, które uniemożliwia użycie VSS w niektórych zastosowanich. (np.niektóre MIXy)

  Co robić ? Oto odpowiedź:

- **Distributed Key Generation**(DKG) Protokół ten umożliwia poprawne wygenerowanie pary kluczy, w taki sposób, aby nigdzie fizycznie nie istniał klucz prywatny odpowiadający kluczowi publicznemu (**Nie ma dilera !**).Ponadto protokół zapewnia poprawność i odporność (w sensie *robustness*) na dzaiałania wroga , który kontroluje część uczestników. Protokół ten ma wiele zastosowań. Dla systemów opartych na dyskretnym logarytmie DKG stowrzony był już na począku lat 90. Okazało się jednak, że ta pierwotna wersja umożliwia wrogowi kontrolującemu nawet niewielką część uczestników, duży wpływ na postać generownych kluczy.

- **Proactive Secret Sharing** Jest to protokół umożliwiający wygenerowanie na podstawie istniejących udziałów (shares), nowych definiujących ten sam sekret. Jest to bardzo przydatne przy przechowywaniu sekretów przez długi okres czasu. Wtedy wróg może sukcesywnie wykradać kolejne udziały uczestnikom, aż zdobędzie odpowiednią ilość, aby pozanć sekret. Poactiv SS, "odświerza" udziały i powoduje, że wykradzione informacje z poprzedniego okresu stają sie bezużyteczne.

Protokół DKG (R.Gennaro, S. Jarecki, H. Krawczyk, T.Rabin) Sytuacja początkowa: Jest n użytkowników $P_1, P_2..., P_n$ (agentów,serwerów). Chcą oni wygenerowć parę kluczy y, x, które spełniają zależność $y = g^x$ zgodnie z założeniami DKG. g,h generetory grupy $\mathbb{Z}_q$, takie że trudno jest policzyć $d\log_g(h)$

1. Każdy P_i przeprowadza Pedersen's-VSS jako diler.

   (a) Wybiera dwa wielomiany stopnia t nad $\mathbb{Z}_q$.

$$\begin{aligned} f_i(z) &= a_{i0} + a_{i1}z + a_{i1}z^2 + ... + a_{it}z^t \\ f_i'(z) &= b_{i0} + b_{i1}z + b_{i1}z^2 + ... + b_{it}z^t \end{aligned}$$

   (b) Publikuje $C_{ik} = g^{a_{ik}}h^{b_{ik}}$ dla $k = 0, 1...t$

   (c) Liczy:

$$\begin{aligned} s_{ij} &= f_i(j) mod\, q \\ s_{ij}' &= f_i'(j) mod\, q \end{aligned}$$

   (d) ...i wysyła s_{ij},s_{ij}' dla wszystkich j do P_j.

2. Każdy P_j sprawdza dla wszystkich $i = 1, ..., n$ czy zachodzi:

$$g^{s_{ij}}h^{s'_{ij}} = \prod_{k=0}^{t}(C_{ik})^{j^k} mod\, p \qquad (1)$$

   Jeśli dla jakiegoś i równość (1) nie jest spełniona, P_j składa **zażalenie** na P_i

3. Jeżeli na P_i złożono $t+1$ lub więcej zażaleń, jest usuwany. Jeśli otrzymał mniej, musi przedstwić s_{ij},s_{ij}', spełniające równość (1). Jeśli nie potrafi tego zrobić również jest usuwany z dalszej częśći protokołu.

4. $QUAL$- zbiór indeksów nie usuniętych uczestników. Klucz prywatny:

$$x = \sum_{i \in QUAL} a_{i0}\, mod\, q$$

   jest już zdefiniowany , chociaż nigdzie nie jest obliczony. Udziały, które otrzymują uczestnicy to:

$$\begin{aligned} x_i &= \sum_{i \in QUAL} s_{ji}\, mod\, q \\ x_i' &= \sum_{i \in QUAL} s_{ji}\, mod\, q \end{aligned}$$

5. **Wyliczanie** $y = g^x$.

   (a) Każdy Uczestnik Pj, $j \in QUAL$ publikuje:

$$A_{ik} = g^{a_{ik}} mod\, p$$

   (b) Każdy $P_j, j \in QUAL$ sprawdza czy zachodzi:

$$g^{s_{ij}} = \prod_{i \in QUAL}(A_{ik})^{j^k} mod\, p \ (2)$$

   Jeśli dla któregoś P_i (2) nie zachodzi, P_j wysyła **zażalenie** wraz z "załącznikiem" s_{ij}, s_{ij}', które spełniają (1) a nie spełniają (2).

   (c) Uczestnicy, na których nie zostało złożone zażalenie (z poprawnym "załączcnikiem" odtwarzają $f_i(z)$,A_{ik} dla tych P_i na które ktoś zażalenie złożył.

$$y = \prod_{i \in QUAL} g^{a_{i0}} mod\, p$$