Universidad Rey Juan Carlos

Grado en Ingeniería de la Ciberseguridad

Criptografía

Ejercicios prácticas autodirigidas. Bloque 4. Firmas y Protocolos.

---

1. Demuestra que el esquema de compartición de secretos de Shamir es lineal, es decir, si disponemos de dos shares s_1 y s_2 para dos secretos S_1 y S_2 (resp.) podemos construir a partir de s_1, s_2 una share para el secreto $S_1 + S_2$ y del mismo modo, dada una share para un secreto S y un escalar λ en el cuerpo en el que trabajamos, podemos construír una nueva share para el secreto λS.

2. Supongamos que $\mathcal{E} = (G, E, D)$ es un esquema de cifrado de clave pública seguro IND-CPA. Constuye a partir de $\mathcal{E}$ un esquema de compromiso.

3. Definimos un esquema de compromiso a partir de un esquema

$$\Pi = (KeyGen, Enc, Dec)$$

de cifrado de clave pública, correcto y determinista (que cifra siempre cada mensaje de la misma manera, sin involucrar aleatoriedad), haciendo:

   - Setup; con entrada el parámetro de seguridad λ, ejecuta $KeyGen(1^\lambda)$ y da como salida la clave pública pk que éste devuelve;
   - Commit; con entrada un mensaje m y la clave pública pk, llama $Enc(pk, m)$ y da como output su salida, el cifrado c
   - Open; con entrada c, pk da como salida m (si se cumple $c = Enc(pk, m)$) y $\perp$ en otro caso.

   Comenta si se cumplen las dos propiedades esenciales de este tipo de esquemas.

4. Supongamos que existe un esquema de firma digital con la propiedad de que dos usuarios distintos U_1 y U_2 son capaces de generar con sus claves secretas dos firmas idénticas σ de modo que, para todo mensaje m (que suponemos es un elemento de un cierto $\mathbb{Z}_p$ se tiene que (m, σ) es validado con la clave pública de verificación de U_1 y (m^2, σ) es validado con la clave pública de verificación de U_2. ¿Es este esquema seguro?