

# Secreto Compartido

Lic. Ana María Arias Roig

## Introducción

Adi Shamir y George Blakley conciben en 1979, aunque en forma separada, el concepto de Secreto Compartido como una manera de proteger claves.

Shamir, en su trabajo, justifica la creación del método, diciendo que

*“Para proteger los datos, los encriptamos, pero para proteger la clave de encriptación necesitamos un método diferente”.*

Plantea que guardar la clave en un solo lugar es altamente riesgoso y guardar múltiples copias en diferentes lugares sólo aumenta la brecha de seguridad. Concluye, entonces, que el secreto ( $D$ ) deberá dividirse en un número fijo de partes ( $D_1, D_2, \dots, D_n$ ) de forma tal que:

1. Conociendo un subconjunto de  $k$  cualesquiera de esas partes se pueda reconstruir  $D$ .
2. Conociendo un subconjunto de  $k-1$  cualesquiera de esas partes el valor  $D$  quede **indeterminado**.

En el mismo documento explica un método basado en interpolación polinómica que considera muy robusto para cumplir los objetivos anteriores:

*“Con  $n = 2k-1$ , obtenemos un esquema muy seguro de administración de la clave: podemos recuperar la clave aún cuando  $[n/2] = k-1$  de las  $n$  piezas hayan sido destruidas, mientras que los oponentes no pueden recuperar la clave aún cuando las brechas de seguridad expongan  $[n/2] = k - 1$  de las piezas restantes”*

Por su lado, Blakley considera también la cuestión de la protección de claves diciendo que, frente a la importancia de determinadas claves criptográficas, se presenta el dilema de hacer muchas copias y correr el riesgo de que algunas se extravíen o hacer pocas copias corriendo el riesgo de que se destruyan todas. Contempla tres tipos de incidentes de los cuales habrá que proteger a las piezas de información:

- a) **Abnegation - Repudio:** tras este incidente, una pieza de información ya no se puede reclamar a la persona a la que se había confiado en custodia. Comprende casos de **destrucción**, **degradación** y **deserción**.
- b) **Betrayal - Traición:** tras este incidente, la pieza de información es completamente conocida por el oponente. Comprende casos de **deserción** y **abandono**.
- c) **Combination - Combinación:** es un incidente que combina un repudio con una traición.

Estos tres tipos de incidentes ( $A, B, C$ ) generan un total  $d = a + b - c$  de incidentes que se espera que puedan ocurrir. Dado que se debe anticipar el máximo número de incidentes que puede ocurrir, que es  $a + b$ , el número de guardianes debería ser de  $g = a + b + 1$ . Por lo tanto, la sugerencia de Blakley es que la clave se distribuya en  $a + b + 1$  piezas a las que denomina **sombras**. La clave debe ser reconstruible a partir de cualquier conjunto de  $b + 1$  sombras, a la vez que con  $b$  de dichas sombras no se pueda obtener ningún tipo de información.

El documento de Blakley describe una forma de lograr el objetivo de distribuir las sombras de la manera exigida, utilizando conceptos de **geometría proyectiva**.

## Definiciones relativas a esquemas de secreto compartido

Con el fin de unificar el vocabulario y facilitar la comprensión del tema propuesto se exponen las siguientes definiciones:

- **S.S.S. Secret Sharing Scheme:** Esquema de Secreto Compartido. Es un método por el cual  $n$  piezas de información llamadas **sombras** (*shares o shadows*) son asignadas a una **clave secreta** ( $k$ ) de manera tal que:

1.  $k$  puede ser reconstruida a partir de ciertos **grupos autorizados** de sombras.
2.  $k$  no puede ser reconstruida a partir de los **grupos no autorizados** de sombras.

En términos de entropía, si las sombras son  $s_1, s_2, \dots, s_n$ :

1.  $H(k | s_{i_1}, s_{i_2}, \dots, s_{i_i}) = 0$ .
2.  $H(k | s_{i_1}, s_{i_2}, \dots, s_{i_{i-1}}) = H(k)$ .

- **Espacio de claves:** La clave se selecciona de un conjunto finito  $K$  de posibles claves, que es de público conocimiento. ( $k \in K$ ). En general, el valor de  $k$  lo elige un participante confiable, el dealer o distribuidor (D).
- **Espacio de sombras:** Es el conjunto  $S$  de todas las posibles sombras. El esquema de reparto del secreto permite obtener un conjunto de piezas de información, las sombras, que luego se repartirán a los participantes. Las piezas deben distribuirse de manera secreta.
- **Esquema Perfecto:** El esquema es perfecto si los **grupos no autorizados** de participantes, al reunir sus sombras no pueden obtener ningún grado de información acerca del secreto  $k$ . Por ejemplo, un esquema de secreto compartido podría ser, para la clave "password" dividirla en las sombras: "pa-----", "-ss-----" "----wo--" "-----rd". La concurrencia de las cuatro sombras permite obtener la clave. Sin embargo, poseer una sombra ya brinda algo de información. Y poseer dos sombras puede dar información suficiente como para adivinar la clave. Este no es un esquema perfecto.
- **Participantes:** Son los que reciben las sombras. El dealer  $D$  no pertenece a este conjunto. Si llamamos  $\wp$  al conjunto de participantes, entonces su cardinal es  $n$ . Es decir:  $\wp = \{P_1, P_2, \dots, P_n\} = \{P_i / 1 \leq i \leq n\}$  con  $\#\wp = n$ . El subconjunto  $S_i \subseteq S$  representa el conjunto de posibles sombras que el participante  $P_i$  podría recibir.
- **Estructura de acceso o Esquema de Concurrencia:** De los  $2^n$  subconjuntos de  $\wp$ , no todos estarán autorizados para reconstruir el secreto. La estructura de acceso  $\Gamma$  está formada por aquellos **subconjuntos autorizados** de participantes. Ejemplo: Si  $\wp = \{P_1, P_2, P_3, P_4\}$ , entonces  $n$  vale 4 y hay 16 subconjuntos de  $\wp$ . Una posible estructura de acceso podría ser  $\Gamma = \{\{P_1, P_2, P_3\}, \{P_1, P_4\}, \{P_3, P_4\}\}$  y otra podría ser  $\Gamma = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}\}$ . Cada participante debe aparecer por lo menos una vez en alguno de los subconjuntos del esquema.
- **Estructura de acceso monótona:** La estructura es monótona si, dados  $B$  y  $C$  subconjuntos de  $\wp$ , ocurre que siempre que  $B \in \Gamma$  y  $B \subseteq C$ , entonces  $C \in \Gamma$ . Es decir, si un conjunto de  $\wp$  pertenece a la estructura de acceso, también pertenece todo conjunto que lo contenga. Para el conjunto  $\wp$  del ejemplo anterior, una estructura monótona podría ser:  $\Gamma = \{\{P_1, P_2, P_3, P_4\}, \{P_1, P_2, P_3\}\}$ , porque  $\{P_1, P_2, P_3\}$  sólo está contenido en  $\{P_1, P_2, P_3, P_4\}$ , que también pertenece a la estructura de acceso.
- **Base de la Estructura de acceso:** Es el subconjunto de la estructura de acceso cuyos elementos son los subconjuntos autorizados minimales. Es decir, está formada por aquellos conjuntos de  $\Gamma$  cuyos subconjuntos ya no pertenecen a  $\Gamma$ .

$$\Gamma_0 = \{X \in \Gamma / X \text{ es minimal}\}$$

Es decir:

$$\Gamma_0 = \{X \in \Gamma / \forall Y \subset X : Y \notin \Gamma\}$$

En el ejemplo anterior,  $\Gamma_0 = \{\{P_1, P_2, P_3\}\}$

- **Rango de una estructura de acceso:** Es la máxima cardinalidad que presentan los subconjuntos minimales que conforman la base. En el caso anterior, es 3.
- **Esquema de Umbral o estructura de acceso umbral:** Un esquema de umbral  $(t, n)$  con  $t \leq n$  es un método para compartir una clave  $k$  entre un número finito de  $n$  participantes de manera tal que con un subconjunto cualquiera de  $t$  participantes o más se pueda reconstruir el valor de  $k$ , pero ningún grupo de  $t-1$  participantes pueda hacerlo.

Es decir:

$$\Gamma = \{A \subset \mathcal{P} / \# A \geq t\}.$$

En un esquema de umbral, la **Base** de la estructura de acceso consiste de todos los subconjuntos de exactamente  $t$  participantes. El rango, por lo tanto, es  $t$ .

Para el conjunto  $\mathcal{P} = \{P_1, P_2, P_3, P_4\}$  de participantes, el esquema:

$$\Gamma = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_2, P_3, P_4\}\}$$

no es de umbral, porque hay grupos de 3 participantes que no están autorizados.

Mientras que el esquema:

$$\Gamma = \{\{P_1, P_2, P_3\}, \{P_1, P_2, P_4\}, \{P_1, P_3, P_4\}, \{P_2, P_3, P_4\}, \{P_1, P_2, P_3, P_4\}\}$$

sí es una estructura de acceso de umbral 3, ya que cualquier subconjunto de  $\mathcal{P}$  de 3 o más participantes está autorizado para reconstruir el secreto. Es un esquema de umbral **(3, 4)**

- **Tasa de información de un SSS:** La clave puede representarse mediante una cadena de bits de longitud  $\log_2 |k|$ . Si el participante  $P_i$  recibe el conjunto  $S_i$  de sombras, entonces la información del participante puede medirse como  $\log_2 |S_i|$ . Por lo tanto la **tasa de información** para el participante  $P_i$  es la razón:

$$\rho_i = \frac{\log_2 |k|}{\log_2 |S_i|}$$

y para el SSS es:

$$\rho = \min\{\rho_i / 1 \leq i \leq n\}$$

mientras que la tasa de información promedio de un SSS es:

$$\bar{\rho} = \frac{n \log_2 |k|}{\sum_{i=1}^n \log_2 |S_i|}$$

En un esquema de Secreto Compartido Perfecto,  $\rho \leq \bar{\rho} \leq 1$ . Esto significa que el tamaño de la clave no puede ser superior al tamaño de la sombra.

- **Esquema de Secreto Compartido Ideal:** Aquél en que  $\rho = \bar{\rho} = 1$ . Los mejores esquemas son aquéllos en los que los fragmentos tienen casi la misma longitud que el secreto.

## Esquemas de Umbral.

Los primeros esquemas de secreto compartido de Shamir y de Blakley fueron de umbral. Luego hubo más esquemas de umbral que no tienen un aspecto geométrico (por ejemplo el que usa el teorema chino del resto).

### Esquema de umbral (t, n) de Shamir.

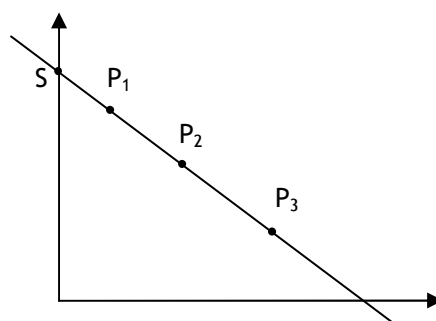
Dados  $t$  puntos en un plano bidimensional  $(x_1, y_1), (x_2, y_2), \dots, (x_t, y_t)$  con distintas coordenadas  $x_i$ , hay uno y sólo un polinomio  $q(x)$  de grado  $t-1$  que contiene a todos esos puntos. Es decir, un solo polinomio  $q(x)$  es tal que  $y_i = q(x_i)$ , para todos los  $i$  considerados. Teniendo en cuenta esto, para un secreto  $S$ , se elige un polinomio al azar de grado  $t-1$ , con  $t < n$  en el cual el término independiente  $a_0$  es igual al secreto  $S$ :

$$q(x) = S + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$$

Se evalúan las  $n$  sombras  $S_1 = q(1), S_2 = q(2), \dots, S_n = q(n)$  y se distribuyen a los participantes.

Para reconstruir el secreto  $S$ , deberá reunirse un suconjunto  $t$  de pares  $(i, S_i)$ . Mediante interpolación, o por la resolución del sistema de  $t$  ecuaciones lineales correspondiente se podrán obtener los coeficientes de  $q(x)$  y obtener finalmente  $q(0) = a_0 = S$

Un esquema de Shamir (2, 3) se representaría:



Es evidente que, con menos de 2 puntos no se puede obtener el polinomio (en este caso una recta) y por lo tanto no se puede hallar el valor de  $S$ .

Para su implementación, Shamir propone trabajar en un cuerpo finito:  $Z_p$ . El número primo elegido deberá ser  $p > S \wedge p > n$ .

Los coeficientes  $a_1, \dots, a_{t-1}$ , para el polinomio  $q(x)$  se eligen dentro de  $Z_p - \{0\}$ <sup>1</sup>. Es decir  $1 \leq a_i \leq p-1$ ,  $\forall i: 1 \leq i \leq t-1$ . Luego se calculan, módulo  $p$ , los valores  $S_i = q(i)$

---

<sup>1</sup> Shamir afirma que “**los coeficientes  $a_1, \dots, a_{t-1}$  en  $q(x)$  se eligen aleatoriamente de una distribución sobre los enteros en  $[0, p)$** ”, es decir incluye claramente al 0. Sin embargo, el coeficiente

$\forall i: 1 \leq i \leq n$  que se entregan a los participantes. Un grupo de  $t$  participantes con sus respectivas sombras pueden obtener el secreto resolviendo el sistema de  $t$  ecuaciones linealmente independientes<sup>2</sup>:

$$\sum_{i=0}^{t-1} a_i x_j^i = q(x_j) = y_j, (1 \leq j \leq t)$$

Es decir:

$$\begin{cases} a_0 + a_1 x_1^1 + a_2 x_1^2 + \dots + a_{t-1} x_1^{t-1} = y_1 \\ a_0 + a_1 x_2^1 + a_2 x_2^2 + \dots + a_{t-1} x_2^{t-1} = y_2 \\ \dots \\ a_0 + a_1 x_t^1 + a_2 x_t^2 + \dots + a_{t-1} x_t^{t-1} = y_t \end{cases}$$

Shamir propone usar la fórmula de interpolación de Lagrange para obtener los coeficientes:

$$q(x) = \sum_{j=1}^t y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x - x_k}{x_j - x_k}$$

Como sólo interesa  $a_0 = q(0) = S$ , lo que hay que calcular es:

$$\sum_{j=1}^t y_j \prod_{1 \leq k \leq t, k \neq j} \frac{x_k}{x_k - x_j}$$

Es decir,  $S$  resulta una combinación lineal de las sombras.

Stinson propone resolver el sistema de ecuaciones teniendo en cuenta que el mismo se corresponde, en términos de matrices, con:

$$\begin{pmatrix} 1 & x_1^1 & x_1^2 & \dots & x_1^{t-1} \\ 1 & x_2^1 & x_2^2 & \dots & x_2^{t-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_t^1 & x_t^2 & \dots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \dots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \dots \\ y_t \end{pmatrix}$$

Y como la matriz de coeficientes  $X = (x_i^j)$  es de Vandermonde su determinante es:

$$\Delta = \prod_{1 \leq k < j \leq t} (x_j - x_k)$$

que es distinto de 0 (ya que  $x_j \neq x_k \forall j, \forall k$ ) lo cual asegura que este sistema tenga una solución única en el cuerpo  $Z_p$

Si un grupo de  $t - 1$  participantes con sus sombras intentan obtener el secreto, deberán resolver un sistema de  $t - 1$  ecuaciones con  $t$  incógnitas, por lo cual la solución es

de  $a_{t-1}$  no puede ser 0 ya que en ese caso el polinomio dejaría de ser de grado  $t - 1$ , para ser de un grado menor.

<sup>2</sup> El sistema de ecuaciones resulta linealmente independiente porque se forma una matriz de Vandermonde cuyos valores de la segunda columna son todos distintos.

indeterminada. Los  $t-1$  participantes no pueden descubrir el secreto. En el caso de que se considere un valor al azar para  $a_0 = q(0) = y_0$ , el nuevo sistema de ecuaciones:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & x_1^1 & x_1^2 & \dots & x_1^{t-1} \\ 1 & x_2^1 & x_2^2 & \dots & x_2^{t-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_t^1 & x_t^2 & \dots & x_t^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \dots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ \dots \\ y_t \end{pmatrix}$$

Por tener también una matriz de Vandermonde con coeficientes  $x_j \neq x_k \forall j, \forall k$ , será de solución única. Es decir, para cada valor  $a_0$  existe un único polinomio posible. En consecuencia, hay tantos polinomios posibles como valores se puedan elegir en  $Z_p$ . Todas las claves del espacio de claves son equiprobables, lo que asegura que el esquema sea perfecto.

### Esquema de umbral (t, n) de Blakley.

La solución de Blakley usa geometría proyectiva finita.

Blakley describe en su documento una forma de distribuir la clave en  $a+b+1$ <sup>3</sup> sombras, de manera que pueda reconstruirse a partir de cualquier grupo de  $b+1$ <sup>4</sup> de esas sombras, pero que con  $b$  de ellos no se pueda obtener nada.

Previo al desarrollo de su esquema describe una serie de lemas y teoremas que le sirven para demostrar que el esquema es seguro.

La idea básica del esquema es la de considerar un espacio vectorial  $V$  de dimensión  $b+2$ , sobre un cuerpo finito  $Z_p$  donde  $p$  es un número primo. Es decir que  $V = Z_p^{(b+2)}$ . A cada uno de los  $(a+b+1)$  participantes (él los llama guardianes) se les asigna un subespacio de  $V$  de dimensión  $b+1: V(g) \subset V / \dim V(g) = b+1$ . Cuando  $b+1$  participantes intersectan sus sombras, es decir sus subespacios, el resultado es una recta  $L(k)$ . En realidad Blakley, considera a la recta como una clase de equivalencia, (es decir toma un **punto proyectivo**) cuyas coordenadas son una  $(b+2)$ -upla de valores en  $Z_p$ , uno de los cuales es la clave  $k$ .

Traducido a términos de espacio proyectivo, diremos que se toma un espacio proyectivo finito de dimensión  $b+1$ , y que cuando  $b+1$  hiperplanos de dimensión  $b$  se intersectan lo hacen en un punto, una de cuyas coordenadas es la clave  $k$ .

Lo primero que hay que hacer en este esquema es determinar los valores  $a$  y  $b$  y un valor  $Q$  suficientemente pequeño que será una medida del punto de partida para una completa aleatoriedad del procedimiento. Luego elegir un número primo  $p$ , impar, que satisfaga la inecuación que surge de uno de los lemas, que le permite asegurar una distribución adecuada de valores en la matriz:

$$0 < 2((a+b+2)(b+1)-1)^2 < 2pQ < 2p < ((a+b+2)(b+1)-1)p.$$

Para construir la matriz  $M$  con  $(a+b+2)$  filas y  $(b+2)$  columnas se coloca primero, en cada fila, una entrada en 1. En la primera fila, en una entrada al azar se guarda la clave  $k \in Z_p$ . Las restantes  $(a+b+2) \cdot (b+1) - 1$  entradas se eligen al azar de  $Z_p$ .

<sup>3</sup>  $a$  = cantidad de incidentes de **abnegation** (repudio)  $b$  = cantidad de incidentes de **betrayal** (traición)

<sup>4</sup> por si se da el peor de los casos: los  $b$  incidentes de traición.

Ejemplo:  $a = 1, b = 1, Q = 0,0001, p = 491$

$$\begin{bmatrix} 220 & 447 & 1 \\ 182 & 1 & 287 \\ 1 & 241 & 171 \\ 41 & 2 & 1 \end{bmatrix}$$

Para aceptar la matriz debe cumplirse que:

- 1) haya un sólo 1 en cada fila
- 2) no haya ningún 0
- 3) no haya dos entradas iguales (a menos que sean las colocadas en 1)
- 4) no debe tener ninguna submatriz  $(b+1) \times (b+1)$  cuyo determinante sea 0.
- 5) no debe tener ningún par de submatrices  $(b+1) \times (b+1)$  cuyos determinantes sean iguales.

Por cómo fueron elegidos los valores, la probabilidad de que la primera matriz que se produzca cumpla esas condiciones es alta.

Con dicha matriz se forman  $(a+b+1)$  submatrices  $b+1$  filas que contengan la primera fila de  $M$ :

$$N(1) = \begin{bmatrix} 220 & 447 & 1 \\ 182 & 1 & 287 \end{bmatrix}$$

$$N(2) = \begin{bmatrix} 220 & 447 & 1 \\ 1 & 241 & 171 \end{bmatrix}$$

$$N(3) = \begin{bmatrix} 220 & 447 & 1 \\ 41 & 2 & 1 \end{bmatrix}$$

Cada conjunto es linealmente independientes ya que cada submatriz  $(b+1) \times (b+1)$  es no inversible (su determinante es distinto de 0).

Sea  $N(j)$  la submatriz  $(b+1) \times (b+2)$  formada a partir del  $j$ -ésimo de estos  $(a+b+1)$  conjuntos de filas.

Si a la matriz  $N(j)$  se le agrega una última fila  $x$ , resulta una matriz  $Y(j, \vec{x})$ , de  $(b+2) \times (b+2)$ . El conjunto  $U(j) = \{\vec{x} \in V / \det Y(j, \vec{x}) = 0\}$  es un subespacio vectorial de dimensión  $b+1$ , al que pertenece la primer fila de  $M$ , que es la primera y última fila de  $Y(j, \vec{x}) \forall j$ .

En nuestro ejemplo:

$$U(1) = \{\vec{x} \in V / \det Y(1, \vec{x}) = 0\}$$

$$\det Y(1, \vec{x}) = 0 \Leftrightarrow \begin{vmatrix} 220 & 447 & 1 \\ 182 & 1 & 287 \\ x_1 & x_2 & x_3 \end{vmatrix} = 0$$

$$\Leftrightarrow x_1 \cdot \begin{vmatrix} 447 & 1 \\ 1 & 287 \end{vmatrix} - x_2 \cdot \begin{vmatrix} 220 & 1 \\ 182 & 27 \end{vmatrix} + x_3 \cdot \begin{vmatrix} 220 & 447 \\ 182 & 1 \end{vmatrix} = 0$$

$$\Leftrightarrow 137x_1 + 381x_2 + 372x_3 = 0$$

$$U(1) = \{\vec{x} \in V / \det Y(1, x) = 0\} = \{\vec{x} \in V / 137x_1 + 381x_2 + 372x_3 = 0\}$$

$$U(2) = \{\vec{x} \in V / \det Y(2, x) = 0\} = \{\vec{x} \in V / 91x_1 + 188x_2 + 36x_3 = 0\}$$

$$U(3) = \{\vec{x} \in V / \det Y(3, x) = 0\} = \{\vec{x} \in V / 445x_1 + 312x_2 + 280x_3 = 0\}$$

La ecuación  $\det Y(j, \vec{x}) = 0$  es una ecuación lineal de la forma  $C_{j1}x_1 + C_{j2}x_2 + \dots + C_{j(b+2)}x_{b+2} = 0$ , donde cada  $C_{ji}$  es el determinante de la matriz de tamaño  $(b+1) \times (b+1)$  que resulta de eliminar de  $Y(j, \vec{x})$  la fila  $b+2$  y la columna  $i$ . Esos determinantes ya vimos, por la forma en que se construyó la matriz, que son distintos de 0 y distintos de a pares, por lo que se obtiene una solución.

Cuando  $b$  de esos subespacios se intersectan, se resuelven simultáneamente  $b$  ecuaciones, de las que se obtiene un subespacio de dimensión 2 que no aporta información sobre cómo recuperar la clave.

Pero cuando  $b+1$  de estos subespacios se intersecta, su intersección es la línea a través del origen que también contiene a la primer fila de  $M$ , donde está  $k$ . Una base para esta línea es el vector  $\vec{g} = (g_1, g_2, \dots, g_{b+2})$ , que es algún **múltiplo no nulo** de la primer fila de  $M$ . Si se conoce  $\vec{g}$ , para cada entrada  $g_i$  se puede hallar el valor

$h_i \in \mathbb{Z}_p / g_i h_i \equiv 1 \pmod{p}$ . Los  $b+2$  vectores  $h_1 \vec{g}, h_2 \vec{g}, \dots, h_{b+2} \vec{g}$  son los **únicos múltiplos de  $\vec{g}$**  que tienen alguna entrada igual a 1, por lo tanto la primer fila de  $M$ , donde está  $k$  está entre ellos. Así que **una de las  $(b+2) \times (b+1)$  entradas distintas de 1, de los vectores es la clave**.

En el ejemplo, la intersección de dos subespacios permite obtener la solución  $S = \{(220x_3, 447x_3, x_3)\}$ , que contiene a  $(220, 447, 1)$  que es donde está la clave  $k = 447$ .

Como se ve, la solución es un punto proyectivo, y en la coordenada de uno de sus representantes está la clave.

### Dualidad en espacios proyectivos.

El **espacio proyectivo dual** de un espacio proyectivo  $P(E)$  es el **espacio proyectivo**  $P(E^*)$  deducido del espacio vectorial dual de  $E$

#### PRINCIPIO DE DUALIDAD:

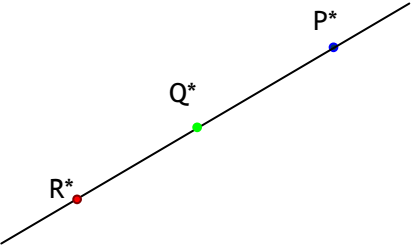
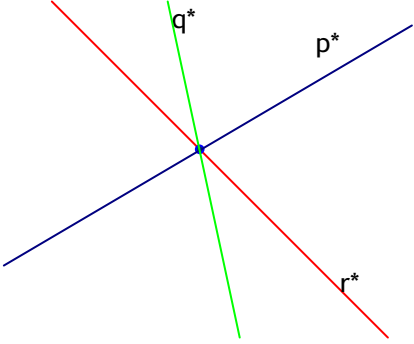
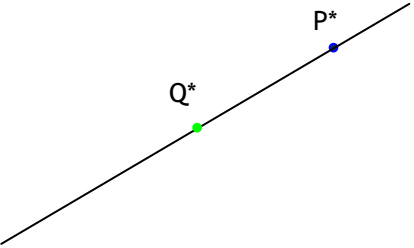
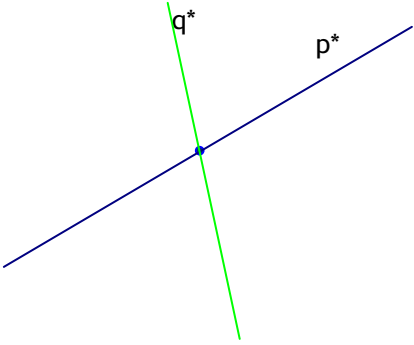
A todo teorema en  $P(E)$  que relacione puntos e hiperplanos y esté basado tan sólo en propiedades de intersección o suma de variedades proyectivas de  $P(E)$ , le corresponde un teorema en el espacio proyectivo  $P(E^*)$ , llamado **teorema dual** del anterior, cuyo enunciado se obtendrá simplemente permutando las palabras “punto” por “hiperplano” e “intersección” por “suma” y recíprocamente.

Un teorema  $T$  relativo a  $P(E)$  es cierto si y sólo si también lo es su teorema dual  $T^*$

#### Ejemplo:

Proposición o teorema	Proposición o teorema dual
“Los puntos $P, Q, R$ pertenecen a una misma recta” (están alineados)	“Las rectas $p^*, q^*, r^*$ se intersectan en el mismo punto” (son concurrentes). Un haz de rectas es el dual de una serie de puntos.



	
<p>“La <b>suma de puntos</b> distintos en el plano proyectivo es una y sólo una <b>recta</b>” o bien: “Dados dos <b>puntos</b> distintos existe una única <b>recta</b> que los <b>contiene a ambos</b>”</p> 	<p>“La <b>intersección de rectas</b> distintas en el plano proyectivo es uno y sólo un <b>punto</b>” o, lo que es equivalente: “Dadas dos <b>rectas</b> distintas existe un único <b>punto</b> que está <b>contenido en ambas</b>”.</p> 
<p>“Dados tres <b>puntos</b> distintos en <math>P^3</math>, existe un único <b>plano</b> que los <b>contiene a los tres</b>”</p>	<p>“Dados tres <b>planos</b> distintos en <math>P^3</math>, existe un único <b>punto</b> que está <b>contenido en los tres</b>”</p>
<p>“Dados <math>n</math> <b>puntos</b> distintos en <math>P^n</math>, existe un único <b>hiperplano</b> que los <b>contiene a todos</b>”</p>	<p>“Dados <math>n</math> <b>hiperplanos</b> distintos en <math>P^n</math>, existe un único <b>punto</b> que está <b>contenido en todos</b>”</p>

La importancia del principio de dualidad está en que permite duplicar toda la geometría al dar, para cada teorema, otro igualmente verdadero: su dual. Demostrar un teorema implica haber demostrado también su dual.

Si observamos los últimos tres teoremas del cuadro, son válidos en el espacio proyectivo pero no en el espacio afín. Dos rectas distintas, en el espacio afín, no siempre se intersectan en un punto, ya que las rectas que son paralelas no se intersectan nunca. La ampliación lograda mediante la geometría proyectiva permite que dos rectas distintas siempre se intersecten en un punto y que su dual también sea cierto.

De las proposiciones anteriores, la que dice “Dados dos **puntos** distintos existe una única **recta** que los **contiene a ambos**” se corresponde con un esquema de umbral  $(2, n)$  de Shamir, ya que en dicho esquema se necesitan 2 puntos para obtener un polinomio de grado 1, que sería una recta.

Por otro lado, su proposición dual “Dadas dos **rectas** distintas existe un único **punto** que está **contenido en ambas**” se corresponde con un esquema de umbral  $(2, n)$  de Blakley,

ya que en dicho esquema se necesitan 2 hiperplanos de dimensión 1 para obtener un **punto proyectivo**, en cuyas coordenadas está el secreto.

Entonces se tiene la siguiente relación de dualidad:

“Dados dos <b>puntos</b> distintos existe una única <b>recta</b> que los <b>contiene a ambos</b> ”	“Dadas dos <b>rectas</b> distintas existe un único <b>punto</b> que está <b>contenido en ambas</b> ”.
Esquema de secreto umbral $(2, n)$ de Shamir	Esquema de secreto umbral $(2, n)$ de Blakley

Sin embargo, un esquema umbral  $(t, n)$  de Blakley con  $t > 2$  ya no es dual de Shamir, aunque constituye otro esquema de secreto compartido.

## Bibliografía

- Shamir, Adi (1979) “*How to share a secret*”. Communications of the ACM 22(11): 612-613.
- Blakley, G. R. (1979). “*Safeguarding cryptographic keys*”. Proceedings of the National Computer Conference 48: 313 - 317
- Capítulo 15 de Computer Security - Art and Science, Matt Bishop, Addison-Wesley, 2004
- Capítulo 10 y 12 de Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, CRC Press, 1997