APPLICATION OF LINEAR ALGEBRA IN SHARING A SECRET

VITALIS KIMUTAI LAGAT

AIMS-SA

vitalis@aims.ac.za

January 22, 2015

Description

- The president of a company holds a secret S, that only him, knows;
- He wants to share it with his n Vice-Presidents incase he dies or become incapacitated;
- But he doesn't trust any of his Vice-Presidents with the secret;
- So he splits the secret and give parts of it to n Vice-Presidents;
- Only m (or more) of n Vice-Presidents can meet and combine their parts, to recover the secret.

Illustration

- As the president, you have $n = 6$ Vice-Presidents with $m = 3$ of them needed to recover the secret;
- All arithmetic done over $\mathbb{Z}_p$;
- Secret $S = 0212$ is a four-digit number chosen such that the prime number $p = 21101 > S$;
- Need a second-degree polynomial with S being its constant coefficient;
- The other coefficients constructed at random between 1 and p;
- The resulting polynomial is

$$P(x) = 212 + 3123x + 11921x^2$$

Continued...

- We will now build six pairs of inputs and outputs, where we will choose the inputs at random (not allowing duplicates) and we do all our arithmetic modulo p,

VP	x	P(x)
Finance	14921	15309
Human Resources	3618	18449
Marketing	12801	12768
Legal	7291	18156
Research	7239	18961
Manufacturing	19211	10466

- The two numbers of each row of the table are then given to the indicated Vice-President so that any three Vice-Presidents can jointly recover the secret.

Continued...

Let's test the recovery process.

- Suppose we write the unknown polynomial $P(x) = a_0 + a_1 x + a_2 x^2$ and the Vice-Presidents for Finance, Marketing and Legal all get together to recover the secret.
- The equations we arrive at are,

$$\begin{aligned} \text{Finance} \qquad 15309 &= P(14921) \\ &= a_0 + a_1(14921) + a_2(14921)^2 \\ &= a_0 + 14921a_1 + 20691a_2 \end{aligned}$$

Continued...

$$
\text{Marketing} \qquad \begin{aligned} 12768 &= P(12801) \\ &= a_0 + a_1(12801) + a_2(12801)^2 \\ &= a_0 + 12801a_1 + 16336a_2 \end{aligned}
$$

$$
\text{Legal} \qquad \begin{aligned} 18156 &= P(7291) \\ &= a_0 + a_1(7291) + a_2(7291)^2 \\ &= a_0 + 7291a_1 + 5262a_2 \end{aligned}
$$

Continued...

So they have a linear system, $\mathcal{LS}(A, \mathbf{b})$ with

$$A = \begin{pmatrix} 1 & 14921 & 20691 \\ 1 & 12801 & 16336 \\ 1 & 7291 & 5262 \end{pmatrix} \qquad \text{and} \qquad \mathbf{b} = \begin{pmatrix} 15309 \\ 12768 \\ 18156 \end{pmatrix}.$$

With a Vandermonde matrix as the coefficient matrix, they know there is a solution, and it is unique.

Continued...

By solving the system $A\mathbf{a} = \mathbf{b}$, they arrive at the solution,

$$
\begin{aligned}
\mathbf{a} &= A^{-1}\mathbf{b} \\
&= \begin{pmatrix} 12291 & 1173 & 7638 \\ 1254 & 21084 & 19864 \\ 16125 & 2678 & 2298 \end{pmatrix} \begin{pmatrix} 15309 \\ 12768 \\ 18156 \end{pmatrix} \\
&= \begin{pmatrix} 212 \\ 3123 \\ 11921 \end{pmatrix}
\end{aligned}
$$

So the President's secret is the number $S = a_0 = 212 = 0212$, as expected.

Other Secret sharing Scheme

- Uses hyperplane geometry to share a secret;
- The secret is a point in a m-dimensional space and n shares/portions are affine hyperplanes that pass through this point;
- Affine hyperplanes in a m-dimensional space with coordinates in a field $\mathbb{Z}_p$ have a linear equation of the form

$$a_1x_1 + a_2x_2 + ... + a_mx_m = b$$

- First coordinate of the point of intersection of any m hyperplanes is the secret.


THANK YOU
FOR YOUR
TIME