Threshold secret-sharing

All-or-nothing secret-sharing is a method to split the secret into two pieces so that both are required to recover the secret.

We could generalize to split the secret among four teaching assistants (TAs), so that jointly they could recover the secret but any three cannot.

However, it is risky to rely on all four TAs showing up for a meeting.

Instead we want a *threshold* secret-sharing scheme: share a secret among four TAs so that

- any three TAs could jointly recover the secret, but
- any two TAs could not.

There are such schemes that use fields other than $GF(2)$, but let's see if we can do it using $GF(2)$.

Threshold secret-sharing using five 3-vectors over $GF(2)$

Failing attempt: Here's an idea: select five 3-vectors over $GF(2)$ $\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4$.

These vectors are supposed to satisfy the following requirement:

Requirement: every set of three are linearly independent.

To share a one-bit secret s among the TAs, I randomly select a 3-vector $\mathbf{u}$ such that $\mathbf{a}_0 \cdot \mathbf{u} = s$. I keep $\mathbf{u}$ secret, but I compute the other dot-products:

$$\begin{aligned}
\beta_1 &= \mathbf{a}_1 \cdot \mathbf{u} \\
\beta_2 &= \mathbf{a}_2 \cdot \mathbf{u} \\
\beta_3 &= \mathbf{a}_3 \cdot \mathbf{u} \\
\beta_4 &= \mathbf{a}_4 \cdot \mathbf{u}
\end{aligned}$$

I give the bit β_1 to TA 1, I give β_2 to TA 2, I give β_3 to TA 3, and I give β_4 to TA 4. The bit given to a TA is her *share*.

Can any three TAs recover the secret? For example, suppose TAs 1, 2, and 3 want to recover the secret. They solve the matrix-vector equation

$$\begin{bmatrix} \mathbf{a}_1 \\ \hline \mathbf{a}_2 \\ \hline \mathbf{a}_3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{bmatrix}$$

Since the matrix is square and the rows $\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3$ are linearly independent, the matrix is is invertible, so $\mathbf{u}$ is the only solution. The TAs use `solve` to recover $\mathbf{u}$, and take the dot-product with $\mathbf{a}_0$ to get the secret $\mathbf{s}$.

Is the secret safe?

Now suppose two rogue TAs, TA 1 and TA 2, decide they want to obtain the secret without involving either of the other TAs. They know β_1 and β_2. Can they use these to get the secret s? The answer is no: their information is consistent with both $s = 0$ and $s = 1$. Since the matrix

$$\begin{bmatrix} \mathbf{a}_0 \\ \hline \mathbf{a}_1 \\ \hline \mathbf{a}_2 \end{bmatrix}$$

is invertible, each of the two matrix equations

$$\begin{bmatrix} \mathbf{a}_0 \\ \hline \mathbf{a}_1 \\ \hline \mathbf{a}_2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 0 \\ \beta_1 \\ \beta_2 \end{bmatrix}$$

$$\begin{bmatrix} \mathbf{a}_0 \\ \hline \mathbf{a}_1 \\ \hline \mathbf{a}_2 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \beta_1 \\ \beta_2 \end{bmatrix}$$

has a solution. The solution to the first equation is a vector $\mathbf{v}$ such that $\mathbf{a}_0 \cdot \mathbf{v} = 0$, and the solution to the second equation is a vector $\mathbf{v}$ such that $\mathbf{a}_0 \cdot \mathbf{v} = 1$.

Threshold secret-sharing with five pairs of 6-vectors

The proposed scheme seems to work. The catch is that first step:

- Select five 3-vectors over $GF(2)$ $\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_4$ satisfying

Requirement: every set of three are linearly independent.

Unfortunately, there are no such five vectors.

Instead, we seek ten 6-vectors $\mathbf{a}_0, \mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_1, \mathbf{a}_2, \mathbf{b}_2, \mathbf{a}_3, \mathbf{b}_3, \mathbf{a}_4, \mathbf{b}_4$ over $GF(2)$.

We think of them as forming five pairs:

- Pair 0 consists of $\mathbf{a}_0$ and $\mathbf{b}_0$,
- Pair 1 consists of $\mathbf{a}_1$ and $\mathbf{b}_1$,
- Pair 2 consists of $\mathbf{a}_2$ and $\mathbf{b}_2$, and
- Pair 3 consists of $\mathbf{a}_3$ and $\mathbf{b}_3$.
- Pair 4 consists of $\mathbf{a}_4$ and $\mathbf{b}_4$.

The requirement is as follows:

Requirement: For any three pairs, the corresponding six vectors are linearly independent.

To share two bits s and t:

- I choose a secret 6-vector $\mathbf{u}$ such that $\mathbf{a}_0 \cdot \mathbf{u} = s$ and $\mathbf{b}_0 \cdot \mathbf{u} = t$.
- I give TA 1 the two bits $\beta_1 = \mathbf{a}_1 \cdot \mathbf{u}$ and $\gamma_1 = \mathbf{b}_1 \cdot \mathbf{u}$, I give TA 2 the two bits $\beta_2 = \mathbf{a}_2 \cdot \mathbf{u}$ and $\gamma_2 = \mathbf{b}_2 \cdot \mathbf{u}$, and so on.

Each TA's share consists of a pair of bits.

Threshold secret-sharing with five pairs of 6-vectors: recoverability

Any three TAs jointly can solve a matrix-vector equation with a 6 × 6 matrix to obtain $\mathbf{u}$, whence they can obtain the secret bits s and t. Suppose, for example, TAs 1, 2, and 3 came together. Then they would solve the equation

$$\begin{bmatrix} \mathbf{a}_1 \\ \hline \mathbf{b}_1 \\ \hline \mathbf{a}_2 \\ \hline \mathbf{b}_2 \\ \hline \mathbf{a}_3 \\ \hline \mathbf{b}_3 \end{bmatrix} \begin{bmatrix} \\ \\ \mathbf{x} \\ \\ \\ \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \gamma_1 \\ \beta_2 \\ \gamma_2 \\ \beta_3 \\ \gamma_3 \end{bmatrix}$$

to obtain $\mathbf{u}$ and thereby obtain the secret bits. Since the vectors $\mathbf{a}_1, \mathbf{b}_1, \mathbf{a}_2, \mathbf{b}_2, \mathbf{a}_3, \mathbf{b}_3$ are linearly independent, the matrix is invertible, so there is a unique solution to this equation.

Threshold secret-sharing with five pairs of 6-vectors: recoverability

Suppose TAs 1 and 2 go rogue and try to recover s and t. They possess the bits $\beta_1, \gamma_1, \beta_2, \gamma_2$. Are these bits consistent with $s = 0$ and $t = 1$? They are if there is a vector $\mathbf{u}$ that solves the equation

$$\begin{bmatrix} \mathbf{a}_0 \\ \hline \mathbf{b}_0 \\ \hline \mathbf{a}_1 \\ \hline \mathbf{b}_1 \\ \hline \mathbf{a}_2 \\ \hline \mathbf{b}_2 \end{bmatrix} \begin{bmatrix} \\ \\ \mathbf{x} \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ \beta_1 \\ \gamma_1 \\ \beta_2 \\ \gamma_2 \end{bmatrix}$$

where the first two entries of the right-hand side are the guessed values of s and t.

Since the vectors $\mathbf{a}_0, \mathbf{b}_0, \mathbf{a}_1, \mathbf{b}_1, \mathbf{a}_2, \mathbf{b}_2$ are linearly independent, the matrix is invertible, so a solution exists.

Similarly, no matter what you put in the first two entries of the right-hand side, there is exactly one solution.

This shows that the shares of TAs 1 and 2 tell them nothing about the true values of s and t. The secret is safe.