

Let $\Omega = \{0, 1, \dots, n-1\}$ be a finite set, and let $s \in \Omega$ be the secret. Does there exist a system where we can give shares $s_1, s_2, s_3 \in \Omega$ to the three GSIs G_1, G_2, G_3 and a share $t \in \Omega$ to the professor, such that all three GSIs together, or the professor and any one GSI, can compute s ? We will show that the answer is no.

What does it mean for the professor and G_1 to ‘compute’ s ? We want a function f_1 that will take the professor’s share t and G_1 ’s share s_1 , and which will output the secret s . Since our scheme is public knowledge, this function $f_1 : \Omega \times \Omega \rightarrow \Omega$ should be known to everyone. What does this mean for the security of the system? Even though G_1 knows both f_1 and his share s_1 of the secret, he shouldn’t be able to deduce any information about the value of s . In particular, every value of s should still be possible. This means the sequence $f_1(s_1, 0), f_1(s_1, 1), \dots, f_1(s_1, n-1)$ should take on every possible value $0, 1, \dots, n-1$ in some order. In other words, the function $f_1(s_1, \cdot) : \Omega \rightarrow \Omega$ which takes $\Omega \rightarrow \Omega$ is surjective. Because the sequence has n elements and takes on n different values, it takes on each value precisely once. In other words, $f_1(s_1, \cdot)$ is injective. So $f_1(s_1, \cdot)$ is actually bijective. Similarly, we don’t want the professor to be able to deduce any information about s from his share alone, so the function $f_1(\cdot, t)$ should also be bijective. We’ll summarize this information by saying that f_1 is bijective in each variable.

Let $f_2(x_2, y)$ (respectively $f_3(x_3, y)$) be the function corresponding to the collaboration of G_2 (respectively G_3) and the professor, and let $g(x_1, x_2, x_3) : \Omega^3 \rightarrow \Omega$ be the function which corresponds to the collaboration of all three GSIs. By identical reasoning as above, these functions should all be bijective in each variable. (The fact that these functions are bijections are necessary, but not sufficient, to encapsulate all of the security issues present in this problem. In other words, there are more security issues that aren’t present in this mathematical formulation - but what we have is enough for the analysis below).

Suppose two GSIs, G_1 and G_2 , pool their shares so that they both know $x_1 = s_1, x_2 = s_2$. Since $f_1(s_1, t) = s$ and $f_2(s_2, t) = s$, they know $f_1(s_1, t) = f_2(s_2, t)$. If there was some value of y such that $f_1(s_1, y) \neq f_2(s_2, y)$, then G_1 and G_2 could deduce that $t \neq y$. This would give them information about s ; because $f_1(s_1, \cdot)$ is injective, they could conclude that $s \neq f_1(s_1, t)$. So we must have $f_1(s_1, y) = f_2(s_2, y)$ for all $y \in \Omega$.

Now consider the original problem, and suppose G_1 and G_2 do not share their information. G_1 knows that $f_1(s_1, y) = f_2(s_2, y)$ for all $y \in \Omega$. Then G_1 can determine s_2 . To do this, G_1 computes $f_1(s_1, 0)$. Since $f_2(\cdot, 0)$ is bijective, there is a unique value s_2 such that $f_2(s_2, 0) = f_1(s_1, 0)$. Thus G_1 can conclude that $x_2 = s_2$. Similarly, G_1 can compute s_3 . But then G_1 knows s_1, s_2 and s_3 , and can thus compute $g(s_1, s_2, s_3) = s$. This reasoning applies equally well to G_2 and G_3 , so we see that each of the GSIs can compute the secret without consulting anyone else!

Note: A function $f(x) : \Omega \rightarrow \Omega$ is called *injective* if $f(x) = f(x') \Rightarrow x = x'$. The function f is *surjective* if $\forall y \in \Omega. \exists x \in \Omega. f(x) = y$. A function is *bijective* if it is both injective and surjective.