3 Old secrets, new secrets

Bob$_1$ can achieve this by giving out $p'(1) = \frac{s'-s}{n+1} + p(1)$ instead of his actual number $p(1)$ when the Bobs gather to jointly discover the secret.

Consider the Lagrange interpolation process the Bobs would use once they gather together:

$$\Delta_1(x) = \frac{(x-2)(x-3)\cdots(x-(n+1))}{(1-2)(1-3)\cdots(1-(n+1))}$$
$$\Delta_2(x) = \frac{(x-1)(x-3)(x-4)\cdots(x-(n+1))}{(2-1)(2-3)(2-4)\cdots(2-(n+1))}$$
$$\cdots \quad \cdots$$
$$\Delta_n(x) = \frac{(x-1)(x-2)\cdots(x-(n-1))(x-(n+1))}{(n-1)(n-2)\cdots(n-(n-1))(n-(n+1))}$$
$$\Delta_{n+1}(x) = \frac{(x-1)(x-2)\cdots(x-n)}{(n+1-1)(n+1-2)\cdots(n+1-n)}$$

where the $\Delta_i(x) = \frac{(x-1)(x-2)\cdots(x-(i-1))(x-(i+1))\cdots(x-n)(x-(n+1))}{(i-1)(i-2)\cdots(i-(i-1))(i-(i+1))\cdots(i-n)(i-(n+1))}$

Thus, the original polynomial $f(x)$ is:

$$p(x) = p(1)\cdot\Delta_1(x) + p(2)\cdot\Delta_2(x) + p(3)\cdot\Delta_3(x) + \cdots + p(n+1)\cdot\Delta_{n+1}(x)$$

which gives that the secret $s = p(0) = p(1)\cdot\Delta_1(0) + p(2)\cdot\Delta_2(0) + \cdots + p(n+1)\cdot\Delta_{n+1}(0)$

Now, suppose Bob$_1$ wants to trick the other Bobs into believing that the secret is actually some fixed s'. Since the only thing he could lie about is $p(1)$, so let him say that he got the number $p'(1)$. Using Lagrange interpolation again, the Δ's would remain the same, and so new altered polynomial would be calculated as:

$$p'(x) = p'(1)\cdot\Delta_1(x) + p(2)\cdot\Delta_2(x) + p(3)\cdot\Delta_3(x) + \cdots + p(n+1)\cdot\Delta_{n+1}(x)$$

which means that the new secret $s' = p'(0) = p'(1)\cdot\Delta_1(0) + p(2)\cdot\Delta_2(0) + \cdots + p(n+1)\cdot\Delta_{n+1}(0)$

So, we have that:

$$s' - s = \Big(p'(1)\cdot\Delta_1(0) + p(2)\cdot\Delta_2(0) + \cdots + p(n+1)\cdot\Delta_{n+1}(0)\Big) - \Big(p(1)\cdot\Delta_1(0) + p(2)\cdot\Delta_2(0) + \cdots + p(n+1)\cdot\Delta_{n+1}(0)\Big) = p'(1)\cdot\Delta_1(0) - p(1)\cdot\Delta_1(0) = \big(p'(1) - p(1)\big)\cdot\Delta_1(0)$$

because we can cancel out all the other terms. Revisiting our definitions of $p'(1)$ and $p(1)$, so we have:

$$s' - s = \big(p'(1) - p(1)\big)\cdot\Delta_1(0)$$

Then, since $\Delta_1(0) = \frac{(0-2)(0-3)\cdots(0-(n+1))}{(1-2)(1-3)\cdots(1-(n+1))} = \frac{-2\cdot-3\cdots-n\cdot-(n+1)}{-1\cdot-2\cdot-3\cdots-(n-1)\cdot-n}$, which can be canceled out (as all terms are non-zero) into the form $\Delta_1(0) = \frac{-(n+1)}{-1} = n+1$. Thus, since $n+1 \neq 0$ by assumption, so we can divide both sides of the equation by $\Delta_1(0) = n+1$, which gives us that: $p'(1) - p(1) = \frac{s'-s}{n+1}$, which would then allow Bob$_1$ to calculate:

$$p'(1) = \frac{s'-s}{n+1} + p(1)$$

Thus, with s and $(n+1)$ being known by Bob$_1$ and s' being his goal in mind, so he can decide his fake value $p'(1)$ with the equation above and trick the other Bobs into believing that secret is actually some fixed s' instead of the original s.