# EVALUATION 2

Let $p$ be a prime, such that $|\mathbb{F}_p| > n$ where $\mathbb{F}_p$ is the finite field of integers modulo $p$ and $p \geq 2^b$.

## Security Through Finite Fields

We evaluate polynomials below "modulo a prime". If we use integer arithmetic, persistent attacker could get information about the polynomial we are using to create shares, since we are simply plotting a polynomial of degree $n$, where $n$ is the number of participants. The way to mitigate this is by using finite fields. We will derive our shares from a function that cannot be represented as a smooth curve on a 2-dimensional plane.

## Encoding the data

For a data of $k$-blocks, $d = d_0 d_1 \ldots d_{k-1}$ where each $d_i \in \mathbb{F}_p$, we fit it into a polynomial in this field.

$$f(x) = d_0 + d_1 x + d_2 x^2 + \cdots + d_{k-1} x^{k-1}$$

We know that a polynomial of degree $k-1$ is uniquely defined by $k$ evaluations.

Consider $k+e \leq n < k+2e$. Lets evaluate the above polynomial at n points.

$$E(d) = \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{k-1} \\ 1 & a_1 & a_1^2 & \cdots & a_1^{k-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \cdots & a_{n-1}^{k-1} \end{bmatrix} \begin{bmatrix} d_0 \\ d_1 \\ \vdots \\ d_{k-1} \end{bmatrix}$$

Now using digital signatures, we sign and store each of the encoded parts. We can choose group size so that the total number of blocks doesn't exceed or equal the total bits when using $k+2e$ blocks.

## Decoding the data

Since at most e blocks can be corrupted, that means we have $n - e \geq k$ blocks which are more than the required number of k points required to reconstruct the polynomial of $k-1$ degree.