Secret Sharing Schemes

Kyle Monette

CS556 Cryptography
Final Project

Spring 2022

Maximize Security & Convenience

Question: How can others recover my secret if I am not present or able to?

- Directly share secret: not secure, very convenient
- Distribute characters of secret: medium security, not convenient
- Don't share at all: very secure, not convenient

3 _ 4 _ _ _   _ 1 _ _ 5 _   _ _ _ 1 _ 9

What in math requires *at least* k objects to uniquely define it, and does not define it *uniquely* for less than k?

Shamir's Secret Sharing

1. Choose secret a_0, prime p, number of shares n, and threshold k so that $2 \leq k \leq n < p$.
2. Construct the polynomial

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1}.$$

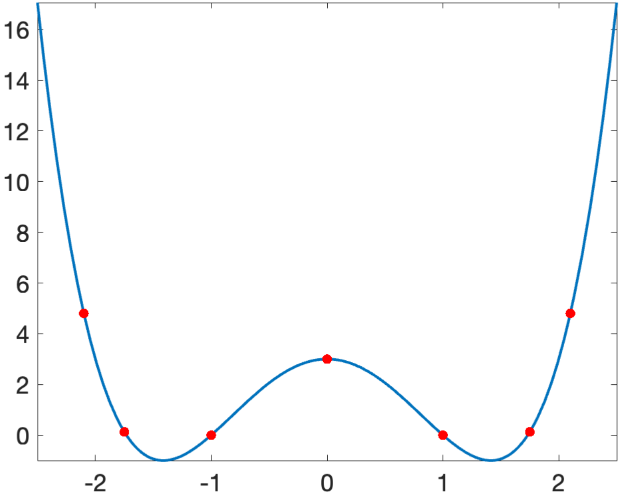
3. Distribute k together with n distinct shares

$$\{(x_1, f(x_1)), (x_2, f(x_2)), \ldots, (x_n, f(x_n))\}.$$

4. Given any subset of k shares, shareholders compute

$$a_0 = \sum_{j=0}^{k-1} f(x_j) \prod_{\substack{m=0 \\ m \neq j}}^{k-1} \frac{x_m}{x_m - x_j}.$$

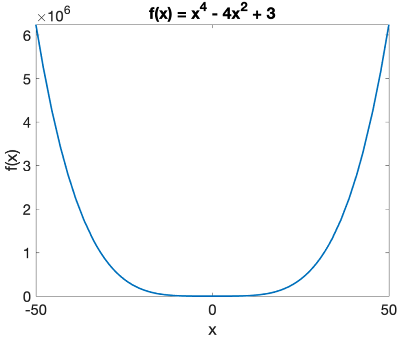
Continuity Attacks

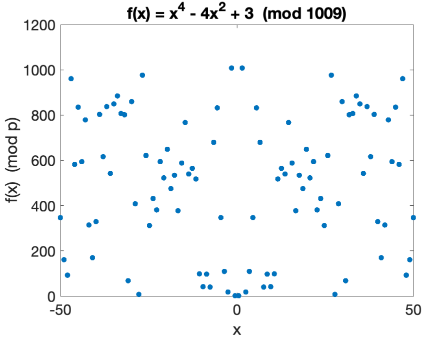


Remember: $k - 1$ is known!

Solution: Finite Fields

Construct $f(x)$ over $\mathbb{Z}_p$ for large prime p





Some Extensions

- Newton's Divided Difference: create additional shares easier (computationally)
- Chebyshev Nodes: eliminate Runge Phenomenon for integer arithmetic

Beyond SSS

There are three main issues in SSS:

1. The shareholders could contribute false shares.
2. The dealer could distribute false shares so that multiple secrets are generated.
3. The shareholders do not know if they received valid shares.

This is solved using *Verifiable Secret Sharing* (VSS) and *Publicly Verifiable Secret Sharing* (PVSS).

- Feldman's scheme: Auxiliary information is sent so they can check if their share is the discrete log of a public value.
- PVSS uses this together with ElGamal so anyone can verify anyone's share (without revealing it).

Asmuth-Bloom Scheme

1. Given a secret S and n and k such that $2 \leq k \leq n$, construct a sequence of pairwise coprime positive integers $S < p < m_1 < \cdots < m_n$ satisfying the property that

$$M := \prod_{i=1}^{k} m_i > p \prod_{i=1}^{k-1} m_{n-i+1}.$$

2. Choose $\alpha \in \mathbb{Z}$ and secretly compute $y = S + \alpha p$ such that $0 \leq y < M$.
3. Distribute shares (y_i, m_i) , where $y_i \equiv y \pmod{m_i}$.
4. Given k shares, shareholders can uniquely determine y from solving their system of congruences using the Chinese Remainder Theorem.
5. Shareholders recover $S \equiv y \pmod{p}$.

Questions?