Adi Shamir, "How to Share a Secret,"

CACM, November 1979.

How to share a secret [Shamir 1979]

(*K*, *N*) threshold scheme

- Secret D is represented by N pieces $D_1, \ldots, D_N$
  - D is easily computable from any K or more pieces
  - D cannot be determined with knowledge of K-1 or fewer pieces
- Tradeoff between reliability and security
  - Reliability: D can be recovered even if N-K pieces are destroyed
  - Security: foe can acquire K-1 pieces and still cannot uncover D
- Tradeoff between safety and convenience
  - Example—A company's checks must be (digitally) signed by three executives

(K, N) scheme by polynomial interpolation

- Given K points in 2-dimensional space, (x_1, y_1), … , (x_K, y_K), with *distinct* x_i's,
  - there is one and only one polynomial q(x) of degree K-1 such that $q(x_i)=y_i$ for all i.

- Let the secret D be a number.
  - Randomly select a K-1 degree polynomial

$$q(x) = a_0 + a_1 x + \ldots + a_{K-1} x^{K-1} \quad \text{where} \quad a_0 = D$$

  - Compute N values of q(x)

$$D_1 = q(1),\ \ldots, D_i = q(i),\ \ldots, D_N = q(N)$$

Scheme by polynomial interpolation (cont.)

- Given any subset of K of the (i, D_i) pairs, the coefficients of the unique $q(x)$ can be found by interpolation

  (such as, using the interpolation polynomial in the Lagrange form or by solving a set of K linear equations with K unknowns)

  - The secret D is $q(0)$

- Shamir's claim: Knowledge of just K-1 of the (i, D_i) pairs provides no information about D

Explanation of the previous claim

- Consider the special case of a finite field GF(p) where p is a large prime number larger than both D and N
  - The coefficients, $a_1, \ldots, a_{K-1}$, are randomly chosen from a uniform distribution over [0, p)
  - $D_1, \ldots, D_N$ are computed modulo p for distinct x values chosen from [0, p)

- Suppose K-1 of the (x_i, D_i) pairs are revealed to a foe. For each candidate value D' in [0, p) for the secret, the foe can construct one and only one polynomial $q'(x)$ of degree K-1 such that $q'(0) = D'$ and $q'(x_i)=D_i$ for the K-1 revealed pieces.
  - By construction, all possible polynomials are equally likely. So there is nothing the foe can deduce about the true value of D.

Useful properties

- Size of each piece D_i is not larger than size of secret D
- When K is kept fixed, D_i pieces can be dynamically added or "deleted"
- Individual D_i pieces can be changed without changing the secret D
  - Such changes enhance security over the long term.
  - How?

    Use a new polynomial with the same a_0 value (D)
- VIPs can be given more than one D_i pieces

Application to mobile ad hoc networks

Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, Lixia Zhang, "Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks," *Proceedings IEEE ICNP 2001.*

Comment - Shamir's method requires a secure and trusted server. This paper attempts to apply Shamir's method to mobile ad hoc networks which do not have access to a secure and trusted server when deployed in the field. The proposed solution is interesting but incomplete.

The end