Adi Shamir, "How to Share a Secret," CACM, November 1979.

2/23/2017

How to share a secret [Shamir 1979]

(K, N) threshold scheme

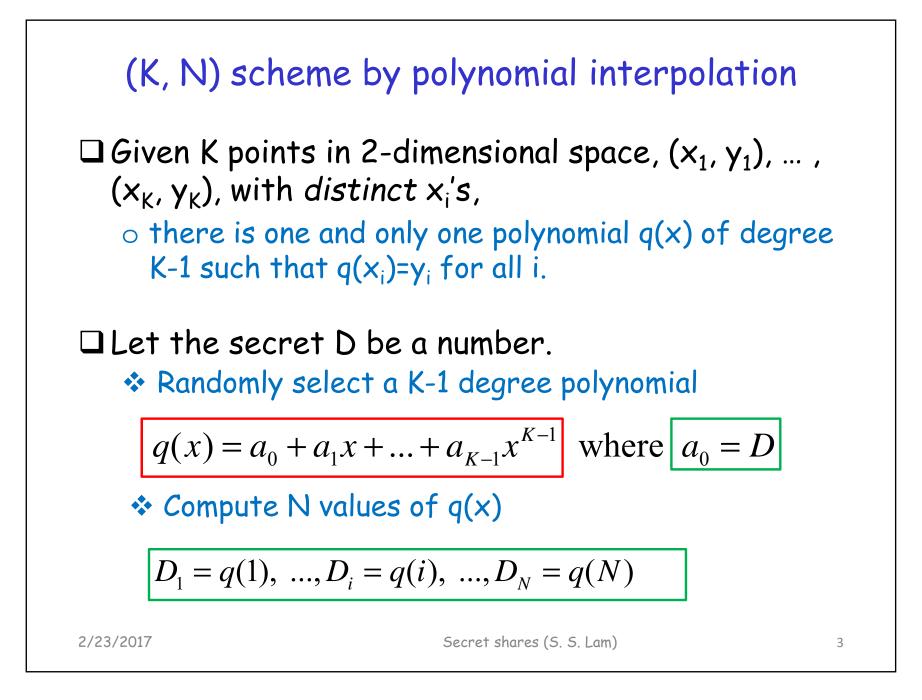
 \Box Secret D is represented by N pieces D₁, ..., D_N

- 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

2/23/2017



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

- \circ The coefficients, $a_1, ..., a_{K-1}$, are randomly chosen from a uniform distribution over [0, p)
- $\circ~D_1$, ..., 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.

2/23/2017



- □ 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"
- \Box 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)

 \Box VIPs can be given more than one D_i pieces

2/23/2017

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.

2/23/2017

Secret shares (S. S. Lam)

7

7

