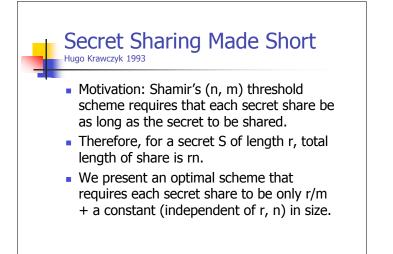


### Overview of the Talk

- Hugo Krawczyk. Secret Sharing Made Short, 1993.
- Josh Cohen Benaloh. Secret Sharing Homomorphisms: Keeping Shares of A Secret Secret, 1987.
- Josh Cohen Benaloh and Jerry Leichter. Generalized Secret Sharing and Monotone Functions, 1990.



### Perfect Secrecy

• Perfect Secrecy 1) In Shamir's (n, m) threshold scheme, no information about the secret is revealed in the information theoretic sense. If  $S_0$  is the secret, for every k < m, let  $S_1$ , ...,  $S_k$  be any k shares then

 $Pr(S_0 | S_1, ..., S_k) = Pr(S_0)$ 2) No bounds on the computation power of adversary are assumed.



### Computational Secrecy:

a) Adversary is resource bounded.

b) No information is revealed using only polynomial resources.

Polynomial Indistinguishability: Two probability distributions are polynomial time indistinguishable if any probabilistic polynomial time algorithm behaves essentially the same when its input is selected from either of the two distributions.

# Computation Secrecy: Formal definition

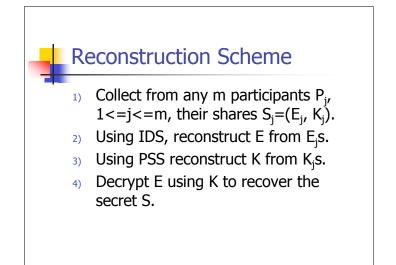
 An (n, m) threshold scheme is computationally secure if for any two secrets S' and S", for any k < m, the distributions on shares D(S'; S'<sub>1</sub>, ..., S'<sub>k</sub>) and D(S"; S"<sub>1</sub>, ..., S"<sub>k</sub>) introduced by the scheme are polynomially indistinguishable.

### Ingredients of the Scheme

- (n, m) Information Dispersal Scheme (IDS) introduced by Rabin. A piece of information (say a file F) is divided into n shares and transmitted over an unreliable channel. Any m shares suffice to reconstruct the file F. Size of each share is |F|/m.
- Secure private key encryption (ENC)
- Perfect (n, m) Secret Sharing Scheme (PSS) like Shamir's threshold scheme.

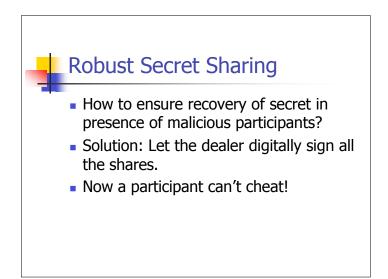
### **Distribution Scheme**

- 1) Choose a random encryption key K. Let  $E=ENC_{K}(S)$  where S=secret
- 2) Using IDS partition E into n fragments  $E_1, E_2, ..., E_n$ .
- <sup>3)</sup> Using PSS generate n shares of the key K:  $K_1$ ,  $K_2$ , ...,  $K_n$ .
- 4) Send to participant  $P_i$ , the share  $(E_i, K_i)$  privately.



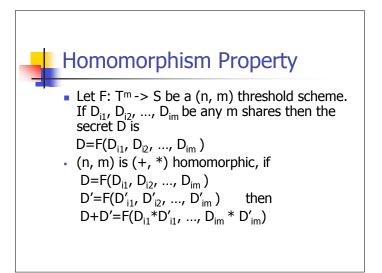
### Analysis

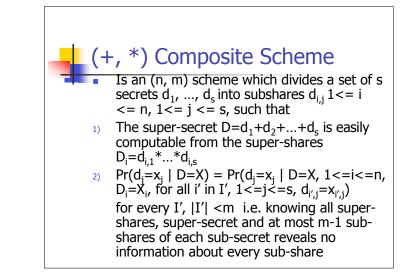
- Length of each share S<sub>i</sub>=(|S|/m, |K|).
- Correctness (Sketch):
- a) m-1  $E_js$  reveal no more information about S than E itself (by security of ENC).
- b) m-1 shares reveal absolutely no information about the encryption key K (by security of PSS).

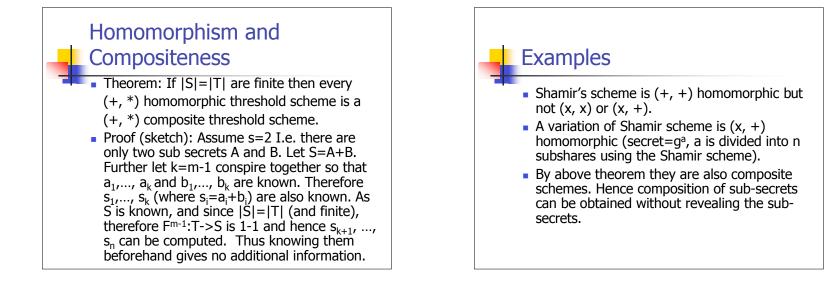


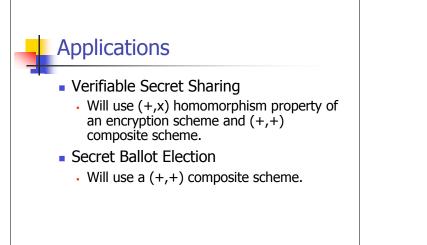
# Secret Sharing Homomorphisms: Josh Benaloh 1987

- Motivation:
- 1) Alice distributes a secret A to n agents using an (n, m) scheme.
- 2) Bob distributes secret B to the same n agents using an (n, m) scheme.
- 3) How can any m of the n agents determine A + B while revealing as little about A and B as possible.



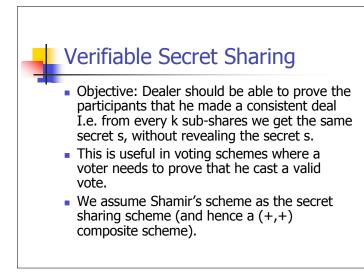






### **Encryption Scheme**

- Verifiable secret sharing scheme will use the following encryption scheme:
- Let r > |S| be prime, p and q also prime s.t. r divides p-1 but not q-1. N=pq. Let y be such that gcd(N, y) =1 and y is NOT the r<sup>th</sup> residue mod N (I.e.  $y \neq a^r \mod N$ , for any a). (N, y) are made public. To encrypt a secret s, choose a random x (relatively prime to N) and let E(s,x,y,N)=y<sup>s</sup>x<sup>r</sup> mod N.
- Knowing p and q, s can be easily determined.
- E is (+, x) homomorphic.



## Solution: Interactive Proof

- Interactive Proof (Probabilistic)
- Dealer will convince the participants that he made a consistent deal with high probability.
- For Shamir's scheme, this boils down for dealer to convince the participants that he used at most d=m-1 degree polynomial P.

### Algorithm

- 1. Encryptions of the values of the points that describe P are released by dealer.
- Similar encryptions of 100 more random polynomials of degree at most d are released to the verifiers.
- 3. A random subset of the random polynomials is selected by the verifiers.
- 4. The chosen subset of polynomials are decrypted by the prover and shown to verifiers. All these polynomials be of at most degree d.
- Each remaining polynomial is added to P. Each of these sum polynomials is decrypted by prover. They all must be of degree at most d.

### **Proof of Correctness**

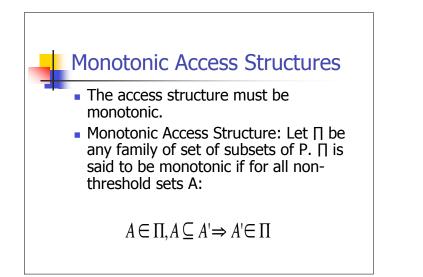
- Fact: If sum of two polynomials is of degree at most d, then either both polynomials are of degree at most d or both are of degree greater than d.
- Revealing a random subset of the set of random polynomials gives the confidence that the remaining polynomials are each of degree at most d.
- Since sum of each of the remaining polynomials with the polynomial P is of degree at most d, therefore P itself is of degree at most d.
- The homomorphism of E and Shamir's scheme helps in guaranteeing that sum of secrets can be revealed without revealing the constituent secret polynomial.

### Secret-Ballot Voting

- Each voter votes 0 or 1 (yes or no).
- N independent organizations hold the election. Assumption: at most m-1 of them collude.
- Voter uses an (+,+)-composite (n, m) threshold scheme and sends the shares to the organizations.
- After election, each organization sums up the shares that it received from different voters.
- Any m organization can get the vote count without compromising secrecy of each voter's vote.

### Generalized Secret Sharing and Monotone Functions: Josh Benaloh and Jerry Leicheter 1990

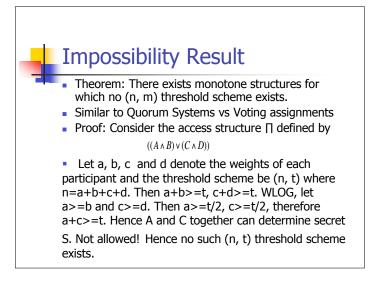
- Motivation: Let a secret S be shared among P, a set of trustees, such that any qualified subset of trustees is able to recover the secret and no unqualified subset of trustees is able to get any information about the secret.
- Example: Let access structure be Q={{a},{b,c},{d,e,f,g}<sub>3</sub> } I.e. either a can recover secret, or b and c together or any 3 of {d,e,f,g} together can recover secret.



### Facts

- Every monotone access structure can be represented by a boolean formula (containing only "and" and "or" and threshold gates) where each variable v<sub>i</sub> in formula corresponds to a participant P<sub>i</sub>.
- Therefore, it suffices to show how the secret should be shared across "and", "or" and threshold gates.
- Example: The access structure Q given earlier can be written as:

 $Q = a \lor (b \land c) \lor Thres3(d, e, f, g)$ 



## Generalized Secret Sharing

- Definition: Given a set P and a monotone access structure ∏, a generalized secret sharing scheme divides a secret s into shares s<sub>i,i</sub> such that :
- 1. When A is in  $\prod$ , s can be reconstructed from the shares  $s_{i,j}$  in A.
- 2. For A not in  $\Pi$ , shares  $s_{i,j}$  in A give no information about secret s.
- Notation: Let T<sub>m</sub>(s;p<sub>1</sub>,..,p<sub>n</sub>) denote a (n, m) threshold scheme.

### Intuition

- Suppose a secret s, 0 <= s < r, needs to be shared between P<sub>1</sub> and P<sub>2</sub> s.t.:
- a) Either of them should be able to determine the secret. Scheme: give s to both of them
- b) Only both of them together should be able to determine s: choose  $s_1$  and  $s_2$  randomly s.t.  $s = s_1 + s_2 \mod r$ . Give  $s_1$  to  $P_1$  and  $s_2$  to  $P_2$ .

### Scheme

- Let T(s,F) be our generalized secret scheme. We define it recursively:
- 1.  $T(s,v_p)$ =assign share s to p.
- 2.  $T(s, Or(F_1,...,F_n))=T(s, F_1),...,T(s, F_n)$  I.e divide s as s to all formula  $F_i$
- 3. T(s, And( $F_1,...,F_n$ ))=T(s<sub>i</sub>,  $F_i$ ) 1<=i<=n where s= $\sum_{1 < =i < =n} s_i$ ,  $s_i$  being random
- 4.  $T(s, THRES_m(F_1, ..., F_n)) = T(s_i, F_i) \ 1 \le i \le n$ where  $s = T_m(s; f_1, ..., f_n) = [s_i]_{1 \le i \le n}$

# Proof of Correctness We use structural induction on the length of access structure formula. Base case is trivial. Let the monotone formula f be of form Or(F<sub>1</sub>,...,F<sub>n</sub>). Since s is divided over each F<sub>i</sub> independently (by using T(s, F<sub>i</sub>)) therefore for any A not in Π, no joint information is conveyed by shares that belong to different T(s, F<sub>i</sub>). F=And(F<sub>1</sub>,...,F<sub>n</sub>). If A not in Π then there is an i s.t. shares of T(s<sub>i</sub>, F<sub>i</sub>) in A give no information about s<sub>i</sub>. Since all s<sub>i</sub> were chosen randomly s.t. s=∑s<sub>i</sub> therefore if s<sub>i</sub> is not known then no information about s is revealed. Similar argument applies for the threshold operator.

### Homomorphism

 Theorem: If the T<sub>m</sub>(s;p<sub>1</sub>,..,p<sub>n</sub>) is (+,+) homorphic then the generalized secret sharing scheme is also (+,+) homomorphic.

### Limitations

- Theorem: There exists monotone access structures for which the scheme is not efficient (formula size and hence number of shares is not polynomial in n)
- Proof (Sketch): Combinatorial Argument: There are doubly exponential monotonic access structures whereas there are only exponentially many polynomial sized access structures corresponding to polynomial sized formulae.