SECRET SHARING

SHARED CONTROL

THRESHOLD SCHEMES
- SHAMIR

ATTACKS ON KEY ESTABLISHMENT

ORIGINAL MOTIVATION

Safeguard cryptographic keys from loss,
create backup copies.
The more # copies, greater the exposure
Smaller # copies, greater risk of loss
Enhanced reliability w/o increased risk ⇒ secret sharing

SECRET SHARING: BASIC IDEA

Given secret, divide it into pieces called shares
and distribute amongst users
Pooled shares of specific subsets of users
allow reconstruction of original secret
- cooperation by t out of n users

SHARED CONTROL SCHEMES

Dual control by modular addition

Secret number S, $0 \leq S \leq m-1$ for some m

Trusted party generates random S_1, $1 \leq S_1 \leq m-1$ and gives S_1 and $S - S_1 \bmod m$ to A and B, respectively.

A and B are trusted not to collude

Unanimous consent control by modular addition

Divide secret S among t users, all of whom are required to recover S

Trusted party generates $t-1$ independent random numbers S_i, $0 \leq S_i \leq m-1$, $1 \leq i \leq t-1$

P_1 thru P_{t-1} are given S_i

P_t given $S_t = S - \sum_{i=1}^{t-1} S_i \bmod m$

(modulo m can be replaced with exclusive OR)

THRESHOLD SCHEMES

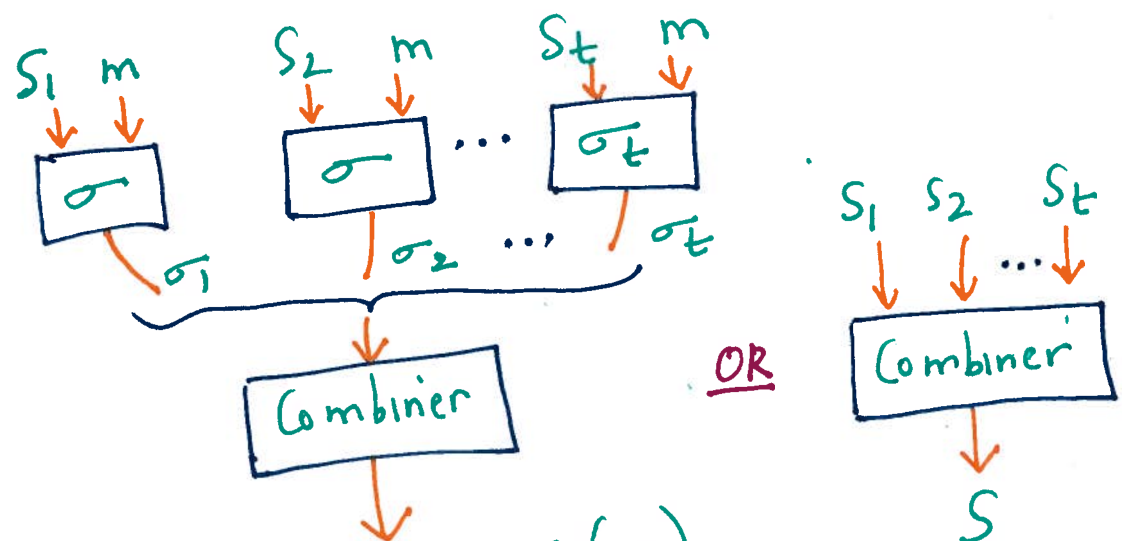
(t, n) threshold scheme $(t \leq n)$

Secret shares S_i, $1 \leq i \leq n$ computed by trusted party

Any t or more users who pool their shares may easily recover S. Any group of size $t-1$ or less may not.

Perfect threshold scheme: knowing only $t-1$ or fewer shares provides no advantage over knowing no shares

GENERAL THRESHOLD SYSTEM



$\sigma = \sigma_S(m)$

(Combiner keeps S hidden)

SHAMIR'S THRESHOLD SCHEME

Based on polynomial interpolation

Fact: A univariate polynomial $y = f(x)$ of degree $t-1$ is uniquely defined by t points (x_i, y_i) with distinct x_i (since these define t linearly independent eqns in t unknowns)

SETUP: Trusted party T has secret $S \geq 0$
n users, t is threshold

(a) Choose prime $p > \max(S, n)$
Set $a_0 = S$

(b) T selects $t-1$ random, independent coefficients $a_1, \ldots a_{t-1}$, $0 \leq a_j \leq p-1$ defining the random polynomial over $\mathbb{Z}_p$, $f(x) = \sum_{j=0}^{t-1} a_j x^j$

(c) T computes $S_i = f(i) \bmod p$, $1 \leq i \leq n$
(or for any n distinct points i, $1 \leq i \leq p-1$)

(d) Securely transmits S_i to user P_i, along with public index i.

POOLING: Any group of t or more users have t distinct points $(x, y) = (i, S_i)$, allowing computation of a_j, $0 \leq j \leq t-1$. $f(0) = a_0 = S$.

LAGRANGE INTERPOLATION

Coefficients of an unknown polynomial $f(x)$ of degree $t-1$, defined by points (x_i, y_i), $1 \le i \le t$ are given by:

$$f(x) = \sum_{i=1}^{t} y_i \prod_{\substack{1 \le j \le t, \\ j \ne i}} \frac{x - x_j}{x_i - x_j}$$

Since $f(0) = a_0 = S$, we can write:

$$S = \sum_{i=1}^{t} c_i y_i \text{ , where } c_j = \prod_{\substack{1 \le j \le t, \\ j \ne i}} \frac{x_j}{x_j - x_i}$$

PROPERTIES OF SHAMIR'S SCHEME

PERFECT: $t-1$ or fewer shares, all values of S possible

IDEAL: Size of one share is size of secret

EXTENDABLE FOR NEW USERS: New shares can be given to new users w/o affecting existing users.

VARYING LEVELS OF CONTROL POSSIBLE: Provide single user with multiple shares.

NO UNPROVEN ASSUMPTIONS: Does not rely on difficulty of particular problems.

ATTACKS ON KEY ESTABLISHMENT PROTOCOLS

Man-in-the-middle attack on unauthenticated
(i) Diffie Hellman

A		E		B
$\longrightarrow$	g^x	$\longrightarrow$	$g^{x'}$	$\longrightarrow$
$\longleftarrow$	$g^{y'}$	$\longleftarrow$	g^y	$\longleftarrow$

A forms session key $K_A = g^{xy'}$
B forms session key $K_B = g^{x'y}$
E. can compute both: $(g^x)^{y'}$ and $(g^y)^{x'}$.

Need to certify public keys!

(ii) Reflection attack

A and B share a symmetric key K
and authenticate each other.

A		B	
$\rightarrow$	r_A		(1)
	$E_K(r_A, r_B)$	$\leftarrow$	(2)
$\rightarrow$	r_B		(3)

is this secure?

What if E initiates a new protocol?

REFLECTION ATTACK.

A		E	
$\rightarrow$	r_A		(1)
	r_A	$\leftarrow$	(1′)
$\rightarrow$	$E_k(r_A, r_A')$		(2′)
	$E_k(r_A, r_B = r_A')$	$\leftarrow$	(2)
$\rightarrow$	r_B		(3)

A believes she has successfully authenticated B

Use distinct keys k & k' for $A \rightarrow B$ encryption and $B \rightarrow A$ encryption, or avoid message symmetry by including the identifier of originating party within the encrypted portion of (2).

INTERLEAVING ATTACK.

S_A denotes signature of party A.
All parties have authentic copies of all others' public keys

A		B	
$\rightarrow$	r_A		(1)
	$r_B, S_B(r_B, r_A, A)$	$\leftarrow$	(2)
$\rightarrow$	$r_A', S_A(r_A', r_B, B)$		(3)

Interleaving Attack (contd.)

E initiates one protocol with B (pretending to be A) and another with A (pretending to be B). Deceives B into believing E is A.

A	E	B	
	$\rightarrow$ r_A		(1)
	$r_B, S_B(r_B, r_A, A)$	$\leftarrow$	(2)
r_B	$\leftarrow$		(1')
$\rightarrow$ $r_A', S_A(r_A', r_B, B)$			(2)
Step 2 for A			
	$\rightarrow$	$r_A', S_A(r_A', r_B, B)$	(3)
		E uses A message in Step 3	

Attack possible due to the symmetry of (2) and (3)

Prevent by binding an identifier to each message indicating a message number, or requiring that the original r_A take the place of r_A' in (3)