secret sharing

LECTURE 9 WED 3/16

how do we share a secret securely?

let's suppose Alice has a secret s (e.g. a key) that she wants to securely share among n friends ($A_1, A_2, \ldots, A_n$) such that:

→ any t or more friends together can reconstruct s
→ any set of <t friends learn nothing about s

this is known as a threshold scheme (where t = threshold)

she'll give each friend A_i a "share" of the secret s_i such that the above security is held by the shares:

→ $\forall I \subseteq [n]$ $|I| \geq t$ given $\{s_i\}_{i \in I}$, s can be easily found
→ $\forall I \subseteq [n]$ $|I| < t$, $\{s_i\}_{i \in I}$ doesn't reveal anything about s (is independent of s)

let's look at how these shares will construct s given t. starting with easier cases

if $t=1$	$s_i = s$	each person knows s
if $t=n$	choose s_i at random but s.t. $s = s_1 \oplus \cdots \oplus s_n$	everyone must get together to find s

but how do we deal with a minimum # of people needed being $1 < t < n$? this is what Shamir's scheme details

Shamir secret sharing

lets gain some intuition first

The essential idea of Adi Shamir's threshold scheme is that 2 points are sufficient to define a line, 3 points are sufficient to define a parabola, 4 points to define a cubic curve and so forth. That is, it takes k points to define a polynomial of degree $k-1$.

Suppose we want to use a (k, n) threshold scheme to share our secret S, without loss of generality assumed to be an element in a finite field F of size P where $0 < k \leq n < P$; $S < P$ and P is a prime number.

Choose at random $k-1$ positive integers $a_1, \cdots, a_{k-1}$ with $a_i < P$, and let $a_0 = S$. Build the polynomial $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_{k-1} x^{k-1}$. Let us construct any n points out of it, for instance set $i = 1, \ldots, n$ to retrieve $(i, f(i))$. Every participant is given a point (a non-zero integer input to the polynomial, and the corresponding integer output) along with the prime which defines the finite field to use. Given any subset of k of these pairs, we can find the coefficients of the polynomial using interpolation. The secret is the constant term a_0.

(wikipedia)

now lets get to the nitty gritty

lets first get to how shares are generated
suppose $s \in GF[p]$ for some prime p. to share:

- → let $a_0 = s$
- → choose at random $a_1, \dots, a_{t-1} \leftarrow GF(P)$
- → let $f(x) = \sum_{i=0}^{t-1} a_i x^i$ } this is that polynomial
- → let $s_i = (i, \underbrace{f(i)}_{y_i})\ \forall i \in [n]$ ← an (x, y) point on

now to generate the key
given (x_i, y_i) where $1 \le i \le t$ given shares in threshold

$$f(x) = \sum_{i=1}^{t} f_i(x) \cdot y_i \quad \text{where } f_i(x) = \begin{cases} 1 & \text{at } x = x_i \\ 0 & \text{at } x \in \{x_j\}_{j \in [t] \setminus \{i\}} \end{cases}$$

↑ combining our points from shares

$$= \frac{\prod_{j \ne i} (x - x_j)}{\prod_{j = i} (x_i - x_j)}$$

product notation

and our secret

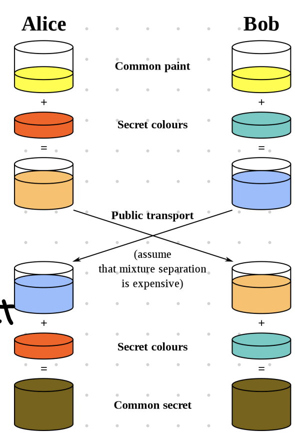
$$s = f(\emptyset) = \sum_{i=1}^{t} y_i \frac{\prod_{j \ne i} (-x_j)}{\prod_{j \ne i} (x_i - x_j)}$$

} constant of polynomial

diffie-hellman key exchange

but how does alice share secrets with bob when there's a passive eavesdropper (eve)?

alice & bob will generate a shared secret w/ individual secrets intuition →



[wikipedia]

let G be a cyclic group w/ generator g
both are fixed and public

A		B
choose random secret $x \leftarrow \{0, 1, \dots, \lvert G \rvert - 1\}$ and computes g^x	$\xleftarrow{g^y}$ $\xrightarrow{g^x}$	choose random secret y in the same way and computes g^y

computes $K = (g^y)^x$ computes $K = (g^x)^y$

now both have the same key while eve only has g^x & g^y
but how are we sure eve can't make K from that?

computational diffie hellman assumption (CDH)

def: given g^x and g^y it is hard to compute g^{xy}. there is only negligible chance of success

decisional diffie hellman assumption (DDH)

def: given g^x and g^y, it is hard to distinguish g^{xy} from g^u where u is random in $\{0, 1, \dots |G|-1\}$. the probability of successfully distinguishing is $\approx 1/2 +$ negligible ammount.

for which groups is it safe to assume DDH?

in generate groups $\langle g \rangle$ from some g of a subgroup of $\mathbb{Z}_p^*$ of order q, where p & q are primes such that q divides p-1 (safe prime)

DDH does not just hold in $\mathbb{Z}_p^*$