TOPIC: 6.857 Applied Cryptography

DATE: 3/9/22

FILE UNDER:

PAGE: L 12

Admin:

- Post project ideas on Piazza
- Post team memberships

Today:

- Finite Fields
- Shamir's Secret-Sharing
- RSA PK encryption
  invention, method, correctness, security

Readings:

- Shamir: secret-sharing paper
- DH paper
- RSA paper
- Boneh: 20 yrs of attacks on RSA

Finite fields: System $(S, +, \cdot)$ s.t.

- S is a finite set containing "0" & "1"
- $(S, +)$ is an abelian (commutative) group with identity 0

group laws:
- $((a+b)+c) = (a+(b+c))$ associative
- $a+0 = 0+a = a$ identity 0
- $(\forall a)(\exists b)\ a+b=0$ (additive) inverses $b=-a$
- $a+b = b+a$ commutative

- $(S^*, \cdot)$ is an abelian group with identity 1

S^* = nonzero elements of S

group laws:
- $(a \cdot b)\cdot c = a\cdot(b\cdot c)$ associative
- $a\cdot 1 = 1\cdot a = a$ identity 1
- $(\forall a \in S^*)(\exists b \in S^*)\ a\cdot b = 1$ (multiplicative inverses) $b = a^{-1}$
- $a\cdot b = b\cdot a$ commutative

- Distributive laws: $a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a$ (follows)

Familiar fields: $\mathbb{R}$ (reals) are infinite

$\mathbb{C}$ (complex)

For crypto, we're usually interested in finite fields, such as $\mathbb{Z}_p$ (integers mod prime p)

Over field, usual algorithms work (mostly).

E.g. solving linear eqns:

$$ax + b = 0 \pmod{p}$$

$$\Rightarrow x = a^{-1} \cdot (-b) \pmod{p} \text{ is soln.}$$

$$3x + 5 = 6 \pmod{7}$$

$$3x = 1 \pmod{7}$$

$$x = 5 \pmod{7}$$

Notation: $GF(q)$ is the finite field ("Galois field") with q elements

Theorem: $GF(q)$ exists whenever

$$q = p^k, \quad p \text{ prime}, \quad k \geq 1$$

Two cases:

① $GF(p)$ - work modulo prime p

Z_p = integers mod p = $\{0, 1, \ldots, p-1\}$

$Z_p^* = Z_p - \{0\} = \{1, 2, \ldots, p-1\}$

② $GF(p^k)$: $k > 1$

work with polynomials of degree $< k$
with coefficients from $GF(p)$
modulo fixed irreducible polynomial of degree k

Common case is $GF(2^k)$

Note: all operations can be performed efficiently
(inverses to be demonstrated)

construction of $GF(a^2) = GF(4)$

Has 4 elements.

Is not arithmetic mod 4. (where 2 has no mult inverse)

elements are polynomials of degree < 2 with coefficients mod 2 (i.e. in $GF(2)$):

	x	1
0	0	0
1	0	1
x	1	0
$x+1$	1	1

Addition is component-wise according to powers, as usual

$$(x) + (x+1) = (2x+1) = 1 \quad \text{(coefs. mod 2)}$$

Multiplication is modulo x^2+x+1 which is irreducible (doesn't factor)

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \bmod (x^2+x+1)$ is $x+1$ (note that $x \equiv -x$ coefs mod 2)

Key management

Start with "secret sharing" (threshold cryptography).

- Assume Alice has a secret s. (e.g. a key)
- She wants to protect s as follows:

  She has n friends $A_1, A_2, \ldots, A_n$

  She picks a "threshold" t, $1 \le t \le n$.

  She wants to give each friend A_i,

  a "share" s_i of s, so that

  - any t or more friends can reconstruct s
  - any set of $< t$ friends can not.

Also see bitcoin "multisig" as motivation

Easy cases:

$t = 1$: $s_i = s$

$t = n$: $s_1, s_2, \ldots, s_{n-1}$ random

s_n chosen so that

$$s = s_1 \oplus s_2 \oplus \cdots \oplus s_n$$

What about $1 < t < n$?

Shamir's method ("How to Share a Secret", 1979)

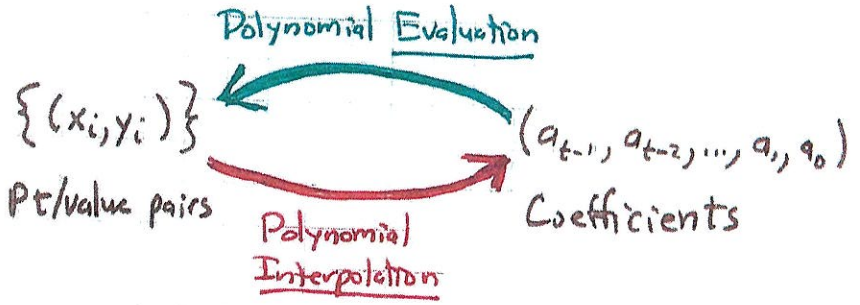
Idea: 2 points determine a line
3 points determine a quadratic
...
t points determine a degree $(t-1)$ curve

Let $f(x) = a_{t-1}x^{t-1} + a_{t-2}x^{t-2} + \cdots + a_1 x + a_0$

There are t coefficients. Let's work modulo prime p.

We can have t points: (x_i, y_i) for $1 \le i \le t$

They determine coefficients, and vice versa.



To share secret s (here $0 \le s < p$):

Let $y_0 = a_0 = s$

Pick $a_1, a_2, \ldots, a_{t-1}$ at random from $\mathbb{Z}_p$

Let share $s_i = (i, y_i)$ where $y_i = f(i)$, $1 \le i \le n$.

Evaluation is easy.

Interpolation

Given (x_i, y_i) $\quad 1 \le i \le t \quad$ (wlog)

Then $f(x) = \sum_{i=1}^{t} f_i(x) \cdot y_i$

where $f_i(x) = \begin{cases} 1 & \text{at } x = x_i \\ 0 & \text{for } x = x_j,\ j \neq i,\ 1 \le j \le t \end{cases}$

Furthermore:

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

This is a polynomial of degree $t-1$. So f also has degree $t-1$.

Evaluating $f(0)$ to get s simplifies to

$$s = f(0) = \sum_{i=1}^{t} y_i \cdot \frac{\prod_{j \neq i} (-x_j)}{\prod_{j \neq i} (x_i - x_j)}$$

Theorem: Secret sharing with Shamir's method is information-theoretically secure. Adversary with $< t$ shares has no information about s.

Pf: A degree $t-1$ curve can go through any point $(0, s)$ as well as any given d pts (x_i, y_i), if $d < t$. □

Refs: Reed-Solomon codes, erasure codes, error correction, information dispersal (Rabin).

Recap:

$\mathbb{Z}_p^*$ = group on $\{1, 2, \ldots, p-1\}$ with mult. mod p

$\mathbb{Z}_n^*$ = group on $\{a : 1 \le a < n \ \& \ \gcd(a,n) = 1\}$
using mult. mod n

modular exponentiation with repeated squaring
$m^e \pmod n$ e.g. for RSA
modular mpys proportional to bit length of e

LaGrange's Thm: $(\forall a \in G)\ a^{|G|} = 1$

PK crypto defns: $Gen(1^k) \to (PK, SK)$
$Enc(PK, m) \to c$
$Dec(SK, c) \to m$

CPA & CCA security

Diffie-Hellman model of PK crypto

"New Directions in Cryptography" (Nov. 1976)

- $Gen(1^\lambda) \to (PK, SK, M, C)$

  (public key, secret key, message space, ciphertext space)

  Here $|M| = |C|$

- $Enc(PK, \cdot)$ is an efficient (poly-time) computable map that is one-to-one & deterministic from M to C

  $c = Enc(PK, m)$ is (unique) ciphertext for m

- $Dec(SK, \bullet)$ is efficiently computable inverse

  $Dec(SK, c) = Dec(SK, Enc(PK, m)) = m$
  $(\forall m \in M)$

- It is hard/infeasible to decrypt with knowledge of PK but without knowledge of SK.
  SK represents "trapdoor" information that enables inversion of the (otherwise one-way) function $Enc(PK, \cdot)$.

D&H proposed model, but didn't have implementation!