Secret sharing schemes

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Cryptology 1 (2023/24)

Secret sharing schemes – introduction

- secret sharing schemes
  - distribute a secret (e.g. key) among some group of participants (users, servers)
  - rules – what group can reconstruct the secret
  - share – secret piece of information owned by individual participant
- a scheme consists of two algorithms/protocols:
  - producing and distributing the shares (usually uses a dealer)
  - reconstructing the shared secret
- motivation
  - Can you trust a single authority (admin or server)?
  - basis for other constructions – threshold cryptography, distributing computation among group of trusted servers, multi-party secure computation, electronic voting, …

Secret sharing schemes

- n participants $\mathcal{P} = \{P_1, P_2, \dots, P_n\}$
- shared secret s
- shares: $P_i \leftarrow s_i$
- access structure $\mathcal{A} \subseteq 2^{\mathcal{P}}$ (power set)
  - $A \subseteq \mathcal{P}$ can reconstruct $s \iff A \in \mathcal{A}$
  - usually monotone access structure:

$$\forall A, B \subseteq \mathcal{P} : \; A \subseteq B \;\&\; A \in \mathcal{A} \implies B \in \mathcal{A}$$

  - (t, n) threshold access structure, for $1 \leq t \leq n$:

$$\{A \mid A \subseteq \mathcal{P} \;\&\; |A| \geq t\}$$

Simple examples

- $(1, n)$ threshold
  - distribute the secret as individual shares: $s_i = s$
- (n, n) threshold – 1st attempt
  - let $s \in \{0, 1\}^l$
  - divide s into n shares $s_1, \ldots, s_n$ of length $\sim l/n$ bits
  - reconstruction: $s = s_1 \,||\, \ldots \,||\, s_n$
  - $n - 1$ participants reconstruct a large part of s, approx. $l(n-1)/n$ bits
- (n, n) threshold
  - let $s \in \{0, 1\}^l$
  - let $s_i \xleftarrow{\$} \{0, 1\}^l$ for $i = 1, \ldots, n-1$, and $s_n = s \oplus s_1 \oplus \ldots \oplus s_{n-1}$
  - reconstruction: $s = s_1 \oplus \ldots \oplus s_n$
  - security: any $n - 1$ (or less) participants learn nothing about s
  - *perfect* scheme

Simple examples

- $(1, n)$ threshold
  - distribute the secret as individual shares: $s_i = s$
- (n, n) threshold – 1st attempt
  - let $s \in \{0, 1\}^l$
  - divide s into n shares $s_1, \dots, s_n$ of length $\sim l/n$ bits
  - reconstruction: $s = s_1 \mid\mid \dots \mid\mid s_n$
  - $n - 1$ participants reconstruct a large part of s, approx. $l(n - 1)/n$ bits
- (n, n) threshold
  - let $s \in \{0, 1\}^l$
  - let $s_i \xleftarrow{\$} \{0, 1\}^l$ for $i = 1, \dots, n - 1$, and $s_n = s \oplus s_1 \oplus \dots \oplus s_{n-1}$
  - reconstruction: $s = s_1 \oplus \dots \oplus s_n$
  - security: any $n - 1$ (or less) participants learn nothing about s
  - *perfect* scheme

Shamir's secret sharing scheme

- idea: t points uniquely determine some polynomial of degree $t-1$
- finite field $\mathbb{Z}_p$, for a prime $p > n$
- shared secret $s \in \mathbb{Z}_p$; let us assume $s \xleftarrow{\$} \mathbb{Z}_p$
- computing the shares:
  - choose a random polynomial $f(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$, where $a_i \xleftarrow{\$} \mathbb{Z}_p$ for $i = 1, \ldots, t-1$
  - notice that $f(0) = s$
  - share for P_i: (i, s_i), where $s_i = f(i)$
- reconstruction; WLOG let us assume t participants $P_1, \ldots, P_t$:
  - Lagrange interpolation using (i, s_i) for $i = 1, \ldots, t$:

$$f(x) = \sum_{i=1}^{t} \underbrace{f(i)}_{s_i} \prod_{\substack{1 \le j \le t \\ j \ne i}} \frac{x - j}{i - j}$$

  - compute $s = f(0)$ (all computations are in the finite field)

Shamir's secret sharing scheme

- idea: t points uniquely determine some polynomial of degree $t-1$
- finite field $\mathbb{Z}_p$, for a prime $p > n$
- shared secret $s \in \mathbb{Z}_p$; let us assume $s \xleftarrow{\$} \mathbb{Z}_p$
- computing the shares:
  - choose a random polynomial $f(x) = s + a_1 x + \ldots + a_{t-1} x^{t-1}$, where $a_i \xleftarrow{\$} \mathbb{Z}_p$ for $i = 1, \ldots, t-1$
  - notice that $f(0) = s$
  - share for P_i: (i, s_i), where $s_i = f(i)$
- reconstruction; WLOG let us assume t participants $P_1, \ldots, P_t$:
  - Lagrange interpolation using (i, s_i) for $i = 1, \ldots, t$:

$$f(x) = \sum_{i=1}^{t} \underbrace{f(i)}_{s_i} \prod_{\substack{1 \le j \le t \\ j \ne i}} \frac{x - j}{i - j}$$

  - compute $s = f(0)$ (all computations are in the finite field)

Shamir's secret sharing scheme – security

- consider group of $t-1$ participants (WLOG $P_1, \dots, P_{t-1}$)
- the shared secret can be anything:
  - combine the shares and add point $(0, s')$ for an arbitrary $s' \in \mathbb{Z}_p$
  - t points $\Rightarrow$ unique polynomial f'
  - f' is consistent with shares of $P_1, \dots, P_{t-1}$
- $P_1, \dots, P_{t-1}$ are in the same position as someone without any share
  - probability of finding $s \sim$ is $1/p$ (guessing)
- perfect secret sharing scheme

Linear equations perspective

- unknown polynomial f (its coefficients)
- a share (i, s_i) forms a linear equation: $s_i = a_0 + a_1 i + \ldots + a_{t-1} i^{t-1}$
- t cooperating participants – the system of t equations with t variables
  - square Vandermonde matrix with distinct elements (i.e. non-zero determinant)
  - the system has a unique solution
- $t - 1$ cooperating participants – the system of $t - 1$ equations with t variables
  - add an additional equation: $s' = a_0$
  - square Vandermonde matrix with distinct elements (because any $i \neq 0$)
  - the system has a unique solution for any s' …perfect scheme

Remarks

- reconstruction is just a linear combination of shares:

$$f(0) = \sum_{i \in S} s_i \cdot r_i$$

  for coefficients $r_i = \prod_{j \in S \setminus \{i\}} -j/(i-j)$, and $S \subseteq \{1, \ldots, n\}$, $|S| = t$
- any points $(x_i, f(x_i))$ for distinct non-zero $x_1, \ldots, x_n$ can be used as shares
- homomorphic property with respect to addition:
  - two (t, n) threshold schemes defined by polynomials f and g
  - adding shares: $(i, f(i)), (i, g(i)) \mapsto (i, f(i) + g(i))$
  - polynomial (the shared secret is the addition of shared secrets $a_0 + a_0'$):

$$f(x) + g(x) = \sum_{i=1}^{t-1} a_i x^i + \sum_{i=1}^{t-1} a_i' x^i = \sum_{i=1}^{t-1} (a_i + a_i') x^i$$

Remarks (2)

- efficiency
  - polynomial time
  - long s can be divided into shorter pieces and shared by independent schemes (or we can encrypt s and share the encryption key)
- trusted dealer – generates the polynomial and distributes the shares
- one-time scheme?
  - secret revealed after reconstruction vs. black-box reconstruction
- cheating in reconstruction:
  - for example – $P_1, \dots, P_t$ try to reconstruct s
  - P_1 cheats and reveals an incorrect share $(1, s_1')$
  - the participants compute: $s' = s + s_1' r_1 - s_1 r_1$
    …and P_1 can easily compute s from s'

Information rate

- the size of share(s) vs. the size of the shared secret
- notation
  - S – set of secrets
  - $K(P_i)$ – set of all possible shares for P_i
  - random variables
- information rate for P_i: $\rho_i = H(S)/H(K(P_i))$
- information rate of the scheme: $\rho = \min_i \rho_i$
- uniform probability case: $\rho = \min_i \lg|S|/\lg|K(P_i)|$

Information rate (2)

- information rate for Shamir's scheme: $\rho = 1$
- perfect secret sharing scheme … $\rho \leq 1$
  - let us assume that $\rho > 1 \implies \forall i : \rho_i > 1$
  - for all i:

$$\begin{aligned} \lg |S| / \lg |K(P_i)| &> 1 \\ \lg |S| &> \lg |K(P_i)| \\ |S| &> |K(P_i)| \end{aligned}$$

  - there exists $A \subseteq \mathcal{P}$: $P_i \notin A$, $A \notin \mathcal{A}$, and $A \cup \{P_i\} \in \mathcal{A}$
  - take all shares from participants in A and all candidate shares from $K(P_i)$
  - compute all possible values of the shared secret … less than $|S|$
  - the scheme cannot be perfect (we can exclude some "impossible" secrets)
- a perfect secret sharing scheme with $\rho = 1$ is called ideal