Knapsack Cryptography

Jay Daigle

Occidental College

October 24, 2019

The Subset-Sum Problem

The Subset-Sum Problem

Definition (Knapsack problem)

Given a (finite) set of items x_i, each with weight w_i and value v_i, maximize $\sum_{i=1}^{n} x_i v_i$ subject to $\sum_{i=1}^{n} x_i w_i \leq W, x_i \in \{0, 1\}$.

The Subset-Sum Problem

Definition (Knapsack problem)

Given a (finite) set of items x_i, each with weight w_i and value v_i, maximize $\sum_{i=1}^{n} x_i v_i$ subject to $\sum_{i=1}^{n} x_i w_i \leq W, x_i \in \{0, 1\}$.

Definition (Subset Sum problem)

Given a list of positive integers $\mathbf{M} = (M_1, \ldots, M_n)$, and another integer S, find a subset of the integers in the list whose sum is S.

Idea

1. Alice starts with a list of positive integers $\mathbf{M} = (M_1, \ldots, M_n)$.

Idea

1. Alice starts with a list of positive integers $\mathbf{M} = (M_1, \ldots, M_n)$.
2. Writes message as an n-bit binary number with digits $x_1 x_2 \ldots x_n$

Idea

1. Alice starts with a list of positive integers $\mathbf{M} = (M_1, \ldots, M_n)$.
2. Writes message as an n-bit binary number with digits $x_1 x_2 \ldots x_n$
3. sends Bob the number $C = \sum_{i=1}^{n} x_i M_i$.

Idea

1. Alice starts with a list of positive integers $\mathbf{M} = (M_1, \ldots, M_n)$.
2. Writes message as an n-bit binary number with digits $x_1 x_2 \ldots x_n$
3. sends Bob the number $C = \sum_{i=1}^{n} x_i M_i$.

If Bob can solve the subset-sum problem, he can recover the list of integers M_i and thus the original message $M = x_1 x_2 \ldots x_n$.

Superincreasing Sequences

Superincreasing Sequences

Definition

A list of positive integers $\mathbf{r} = (r_1, \ldots, r_n)$ *is a superincreasing sequence if* $r_{i+1} \geq 2r_i$ *for all* i.

Superincreasing Sequences

Definition

A list of positive integers $\mathbf{r} = (r_1, \ldots, r_n)$ *is a superincreasing sequence if* $r_{i+1} \geq 2r_i$ *for all* i.

Lemma

If $\mathbf{r} = (r_1, \ldots, r_n)$ *is a superincreasing sequence, then* $r_k > r_{k-1} + \cdots + r_2 + r_1$ *for all* $2 \leq k \leq n$.

Subset Sum for Superincreasing Sequences

Subset Sum for Superincreasing Sequences

Proposition

Let $(\mathbf{M}, S)$ *a subset-sum problem.*
$\mathbf{M} = (M_1, \ldots, M_n)$ *a superincreasing sequence.*
Find a solution $\mathbf{x}$ *by:*

Subset Sum for Superincreasing Sequences

Proposition

Let $(\mathbf{M}, S)$ *a subset-sum problem.*
$\mathbf{M} = (M_1, \ldots, M_n)$ *a superincreasing sequence.*
Find a solution $\mathbf{x}$ *by:*

1. *Start with the largest element* M_n.

Subset Sum for Superincreasing Sequences

Proposition

Let $(\mathbf{M}, S)$ *a subset-sum problem.*
$\mathbf{M} = (M_1, \ldots, M_n)$ *a superincreasing sequence.*
Find a solution $\mathbf{x}$ *by:*

1. *Start with the largest element* M_n.
2. *If* $S \geq M_i$, *set* $x_i = 1$ *and subtract* M_i *from* S. *Otherwise, set* $x_i = 0$.

Subset Sum for Superincreasing Sequences

Proposition

Let $(\mathbf{M}, S)$ *a subset-sum problem.*
$\mathbf{M} = (M_1, \ldots, M_n)$ *a superincreasing sequence.*
Find a solution $\mathbf{x}$ *by:*

1. *Start with the largest element* M_n.
2. *If* $S \geq M_i$, *set* $x_i = 1$ *and subtract* M_i *from* S. *Otherwise, set* $x_i = 0$.
3. *Proceed to the next smallest number.*

Subset Sum for Superincreasing Sequences

Proposition

Let $(\mathbf{M}, S)$ *a subset-sum problem.*
$\mathbf{M} = (M_1, \ldots, M_n)$ *a superincreasing sequence.*
Find a solution $\mathbf{x}$ *by:*

1. *Start with the largest element* M_n.
2. *If* $S \geq M_i$, *set* $x_i = 1$ *and subtract* M_i *from* S. *Otherwise, set* $x_i = 0$.
3. *Proceed to the next smallest number.*

At the end of this process, $\mathbf{x} = (x_1, \ldots, x_n)$ *is a solution to the subset sum problem.*

Merkle-Hellman Subset-Sum Cryptography

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

1. Bob writes his plaintext $\mathbf{x}$ as a binary vector.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

1. Bob writes his plaintext $\mathbf{x}$ as a binary vector.
2. Bob computes $S = \mathbf{x} \cdot \mathbf{M} = \sum_{i=1}^{n} x_i M_i$ and sends this to Alice.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

1. Bob writes his plaintext $\mathbf{x}$ as a binary vector.
2. Bob computes $S = \mathbf{x} \cdot \mathbf{M} = \sum_{i=1}^{n} x_i M_i$ and sends this to Alice.

Decryption:

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

1. Bob writes his plaintext $\mathbf{x}$ as a binary vector.
2. Bob computes $S = \mathbf{x} \cdot \mathbf{M} = \sum_{i=1}^{n} x_i M_i$ and sends this to Alice.

Decryption:

1. Alice computes $S' \equiv A^{-1}S \mod B$ for $0 \leq S' < B$.

Merkle-Hellman Subset-Sum Cryptography

Key Generation:

1. Alice chooses a superincreasing sequence $\mathbf{r} = (r_1, \ldots, r_n)$.
2. Alice chooses A, B with $B > 2r_n$ and $\gcd(A, B) = 1$. Alice also computes the inverse of A modulo B.
3. Alice sets $M_i \equiv Ar_i \mod B$ with $0 \leq M_i < B$. Alice's public key is $\mathbf{M} = (M_1, \ldots, M_n)$.

Encryption:

1. Bob writes his plaintext $\mathbf{x}$ as a binary vector.
2. Bob computes $S = \mathbf{x} \cdot \mathbf{M} = \sum_{i=1}^{n} x_i M_i$ and sends this to Alice.

Decryption:

1. Alice computes $S' \equiv A^{-1}S \mod B$ for $0 \leq S' < B$.
2. Alice solves the subset problem for $(\mathbf{r}, S')$.

Definition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$ *be a set of linearly independent vectors. Then the lattice* L *generated by* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *is the set of integeger linear combinations of the* $\mathbf{v}_i$ *with coefficients in* $\mathbb{Z}$*:*

$$L = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n : a_i \in \mathbb{Z}\}.$$

Definition

Let $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^m$ *be a set of linearly independent vectors. Then the lattice* L *generated by* $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ *is the set of integeger linear combinations of the* $\mathbf{v}_i$ *with coefficients in* $\mathbb{Z}$*:*

$$L = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n : a_i \in \mathbb{Z}\}.$$

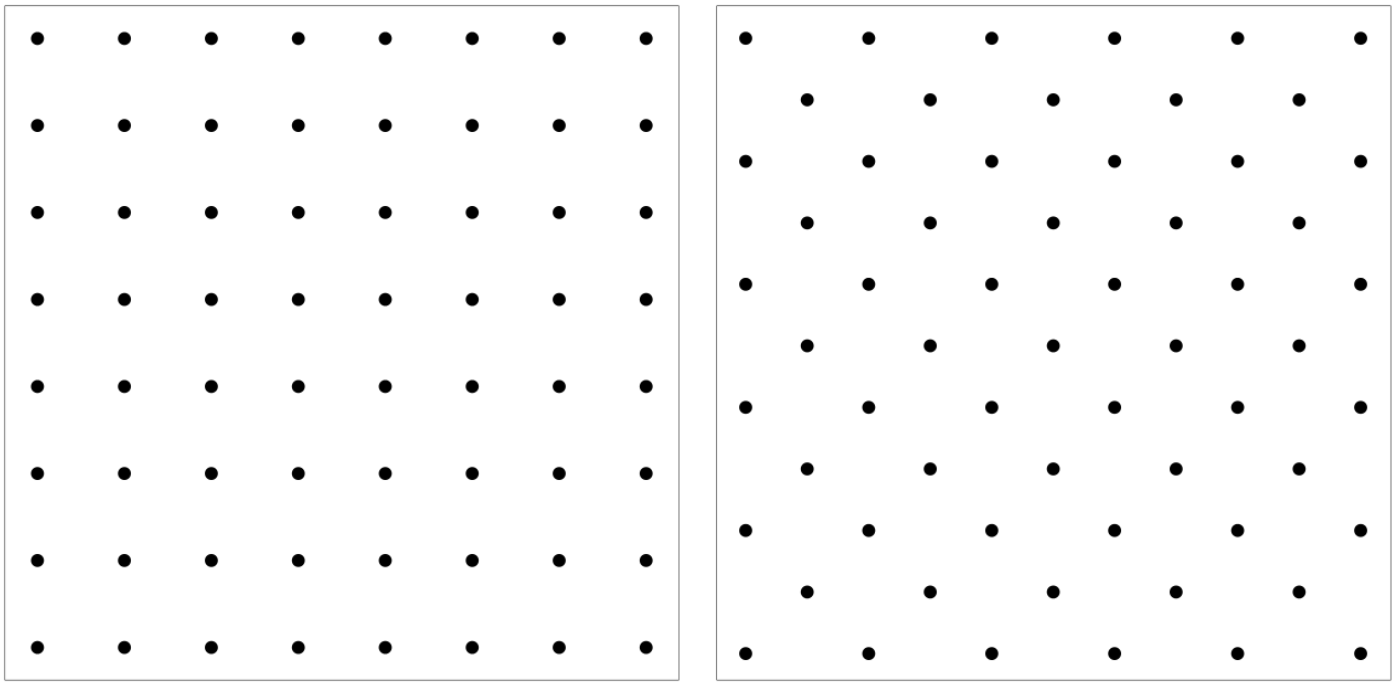

Figure: CC BY-SA 4.0 by R. A. Nonenmacher

Definition

An integral lattice is a lattice all of whose vectors have integral coordinates. We can view such a lattice as a subgroup of $\mathbb{Z}^m$.

Definition

An integral lattice is a lattice all of whose vectors have integral coordinates. We can view such a lattice as a subgroup of $\mathbb{Z}^m$.

Fact

Any two bases for a lattice L are related by an integer matrix with an integer matrix inverse. Thus the matrix must have determinant ± 1. It belongs to the General Linear Group over the integers $GL_n(\mathbb{Z})$.

Fundamental Domain

Fundamental Domain

Definition

Let L be a lattice of dimension n with basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Then the fundamental dommain for L corresponding to B is the set

$$\mathcal{F}(B) = \{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n : 0 \leq t_i < 1\}.$$

Fundamental Domain

Definition

Let L be a lattice of dimension n with basis $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$. Then the fundamental dommain for L corresponding to B is the set

$$\mathcal{F}(B) = \{t_1\mathbf{v}_1 + t_2\mathbf{v}_2 + \cdots + t_n\mathbf{v}_n : 0 \leq t_i < 1\}.$$

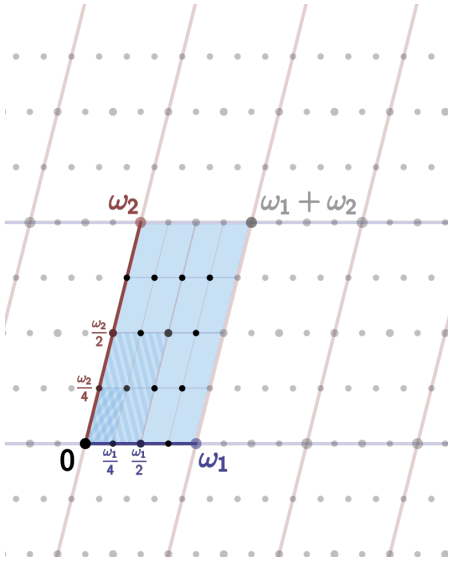

Figure: CC BY-SA 3.0 Sam Derbyshire

Fact

Let $L \subset \mathbb{R}^n$ with basis B and let $\mathcal{F}$ be the fundamental domain for L corresponding to B. Then every vector $\mathbf{w} \in \mathbb{R}^n$ can be written uniquely as $\mathbf{w} = \mathbf{t} + \mathbf{v}$ for some $\mathbf{t} \in \mathcal{F}$ and $\mathbf{v} \in L$.

Fact

Let $L \subset \mathbb{R}^n$ with basis B and let $\mathcal{F}$ be the fundamental domain for L corresponding to B. Then every vector $\mathbf{w} \in \mathbb{R}^n$ can be written uniquely as $\mathbf{w} = \mathbf{t} + \mathbf{v}$ for some $\mathbf{t} \in \mathcal{F}$ and $\mathbf{v} \in L$.

Definition

Let L be a dimension-n lattice and $\mathcal{F}$ a fundamental domain for L. Then the n-dimensional volume of $\mathcal{F}$ is called the determinant of L or $\det(L)$.

Fact

Let $L \subset \mathbb{R}^n$ with basis B and let $\mathcal{F}$ be the fundamental domain for L corresponding to B. Then every vector $\mathbf{w} \in \mathbb{R}^n$ can be written uniquely as $\mathbf{w} = \mathbf{t} + \mathbf{v}$ for some $\mathbf{t} \in \mathcal{F}$ and $\mathbf{v} \in L$.

Definition

Let L be a dimension-n lattice and $\mathcal{F}$ a fundamental domain for L. Then the n-dimensional volume of $\mathcal{F}$ is called the determinant of L or $\det(L)$.

Fact

Let L be a lattice, $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ a basis, and $\mathcal{F}$ a fundamental domain. Then

$$\det L \leq \|\mathbf{v}_1\| \cdot \cdots \cdot \|\mathbf{v}_n\|.$$

Further if we let A be the matrix whose rows are given by the $\mathbf{v}_i$, then $\det L = |\det A|$.

Definition (Shortest-Vector Problem)

Given a lattice L with a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, find a shortest non-zero vector $\mathbf{v} \in L$.

Definition (Shortest-Vector Problem)

Given a lattice L with a basis $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, find a shortest non-zero vector $\mathbf{v} \in L$.

Definition (Closest-Vector Problem)

Given a lattice L and a vector $\mathbf{w} \in \mathbb{R}^m$ that is not in L, find a vector $\mathbf{v} \in L$ that is closest to $\mathbf{w}$.
That is, minimize $\|\mathbf{w} - \mathbf{v}\|$.

Fact (Hermite's Theorem)

Every lattice L of dimension n contains a nonzero vector $\mathbf{v} \in L$ satisfying $\|\mathbf{v}\| \leq \sqrt{n}\det(L)^{1/n}$.

Fact (Hermite's Theorem)

Every lattice L of dimension n contains a nonzero vector $\mathbf{v} \in L$ satisfying $\|\mathbf{v}\| \leq \sqrt{n}\det(L)^{1/n}$.

Fact (Gaussian Heuristic)

Let L be a lattice of dimension n. The Gaussian expected shortest length is

$$\sigma(L) = \sqrt{\frac{n}{2\pi e}}(\det L)^{1/n}.$$

The Gaussian heuristic says that a shortest nonzero vector in a "random" lattice will satisfy $\|\mathbf{v}\| \approx \sigma(L)$.

$$\begin{bmatrix} 2 & 0 & 0 & \dots & 0 & m_1 \\ 0 & 2 & 0 & \dots & 0 & m_2 \\ 0 & 0 & 2 & \dots & 0 & m_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & m_n \\ 1 & 1 & 1 & \dots & 1 & S \end{bmatrix}$$

$$\begin{bmatrix} 2 & 0 & 0 & \dots & 0 & m_1 \\ 0 & 2 & 0 & \dots & 0 & m_2 \\ 0 & 0 & 2 & \dots & 0 & m_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & m_n \\ 1 & 1 & 1 & \dots & 1 & S \end{bmatrix}$$

$$\begin{aligned} \mathbf{v}_1 &= (2, 0, 0, \dots, 0, m_1) \\ \mathbf{v}_2 &= (0, 2, 0, \dots, 0, m_2) \\ &\vdots \qquad \vdots \\ \mathbf{v}_n &= (0, 0, 0, \dots, 2, m_n) \\ \mathbf{v}_{n+1} &= (1, 1, 1, \dots, 1, S). \end{aligned}$$

Consider the lattice:

$$L = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n + a_{n+1}\mathbf{v}_{n+1} : a_i \in \mathbb{Z}\}.$$

Consider the lattice:

$$L = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n + a_{n+1}\mathbf{v}_{n+1} : a_i \in \mathbb{Z}\}.$$

If $\mathbf{x} = (x_1, \ldots, x_n)$ is a solution, then L contains the vector

$$\mathbf{t} = \sum_{i=1}^{n} x_i\mathbf{v}_i - \mathbf{v}_{n+1} = (2x_1 - 1, 2x_2 - 1, \ldots, 2x_n - 1, 0).$$

Consider the lattice:

$$L = \{a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n + a_{n+1}\mathbf{v}_{n+1} : a_i \in \mathbb{Z}\}.$$

If $\mathbf{x} = (x_1, \ldots, x_n)$ is a solution, then L contains the vector

$$\mathbf{t} = \sum_{i=1}^{n} x_i\mathbf{v}_i - \mathbf{v}_{n+1} = (2x_1 - 1, 2x_2 - 1, \ldots, 2x_n - 1, 0).$$

$$\begin{aligned}
\sigma(L_{\mathbf{M},s}) &= \sqrt{\frac{n+1}{2\pi e}}\,(\det L_{\mathbf{M},s})^{1/(n+1)} \\
&= \sqrt{\frac{n+1}{2\pi e}}\,(2^n S)^{1/(n+1)} \\
&\approx \sqrt{\frac{n+1}{2\pi e}}\,8 \approx 1.936\sqrt{n}
\end{aligned}$$