Post-Quantum Encryption

Knapsack Cryptography

Subset-Sum problem

Dfn (Knapsack problem):
given finite set of items x_i;
value v_i, weight w_i

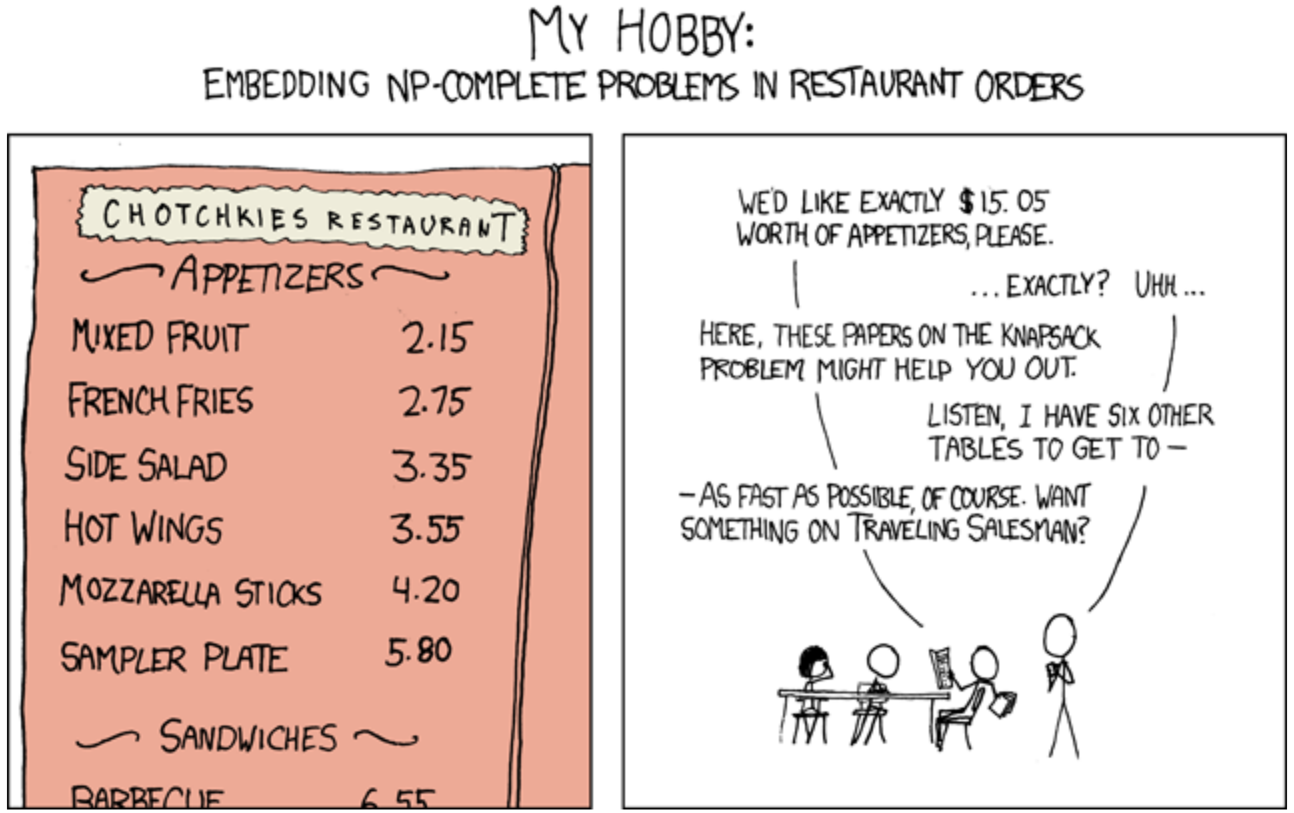
goal: maximize

$$\sum_{i=1}^{n} x_i v_i$$

subject to constraint

$$\sum_{i=1}^{n} x_i w_i \le W.$$

$x_i \in \{0,1\}$



Dfn (Subset sum): Given a list $M = (M_1, M_2, \dots, M_n)$ of positive integers, and another integer S.

Find a subset of M that sums to S.

Ex: $M = (1, 3, 5, 6, 8, 10, 11)$

$S = 24$.

$10 + 6 + 8$

$8 + 10 + 5 + 1$

$3 + 10 + 11$

---

how many subsets of M?

$\# 2^M = 2^{\# M}$

$2^7 = 128$

Brute force: try every subset $O(2^{\# M})$

Collision: what are sums of $(1, 3, 5)$? $2^3 = 8$

what are the sums of $(6, 8, 10, 11) = 2^4 = 16$

compute 24 - sums

$O(2^{n/2 + \varepsilon})$

easy to check

slow to solve

maybe a good trap-door fn.

Idea: Alice starts w/ $M = (M_1, \dots, M_n)$ wants to encipher n-bit binary $x_1 x_2 \dots x_n$.

Transmits: $S = \sum_{i=1}^{n} x_i M_i$.

If Bob can solve SS problem, he can recover the x_i, and gets the message.

Dfn: a list $\vec{r} = (r_1, \dots, r_n)$ is a <u>superincreasing sequence</u> if $r_{i+1} > 2r_i \ \forall i$.

2, 5, 11, 23, 47

2, 7, 31, 103, 519

Lemma: If $\vec{r}$ is a SI seq, then $r_K > r_{K-1} + \dots + r_1 \ \forall 2 \le K \le n$.

Pf: Induction

If $K=2$: $r_2 > 2r_1 > r_1$.

Suppose $r_K > r_{K-1} + \dots + r_1$

WTS: $r_{K+1} > r_K + \dots + r_1$

Know: $r_{K+1} > 2r_K$
$= r_K + r_K$
$> r_K + r_{K-1} + \dots + r_1$. //

Sequence grows faster than 2^n

2, 4, 8, 16, 32 $= 2^n$

this is bigger

$557 - 519 = 38 = 31 + 7$.

Prop: Let (M, S) be a SS problem, where M is an SI sequence.
If a soln $\vec{x}$ exists, can find it:

1) Start w/ M_n
2) If $S_i \geq M_i$, set $x_i = 1$
   and $S_{i-1} = S_i - M_i$
   else: set $x_i = 0$
   and $S_{i-1} = S_i$
3) Repeat for next smaller #.

And this soln is unique.

Pf/ suppose $\vec{y} \cdot \vec{M} = S$ is a soln.
downward induction
Suppose $x_i = y_i \quad \forall K < i \leq n$.
WTS $x_K = y_K$.

$$S_K = S - \sum_{i=K+1}^{n} x_i M_i$$
$$= \sum_{i=1}^{n} y_i M_i - \sum_{i=K+1}^{n} \cancel{x_i}\, y_i M_i$$
$$= \sum_{i=1}^{K} y_i M_i$$

1) if $y_K = 1$, $S_K \geq M_K$, so set $x_K = 1$
2) If $y_K = 0$, then $\Sigma \leq M_1 + \cdots M_{K-1} < M_K$
   so $x_K = 0$.

//

Ex: $M = (3, 11, 24, 50, 115)$

solve for 142

- $142 > 115$

set $x_5 = 1$

$s_4 = 142 - 115 = 27$

- $27 < 50$

$x_4 = 0$

$s_3 = s_4 = 27$

- $27 > 24$

$x_3 = 1$

$s_2 = 27 - 24 = 3$

- $3 < 11$

$x_2 = 0$

- $3 = 3$ $x_1 = 1$.

$\vec{x} = (1, 0, 1, 0, 1) \longleftrightarrow |21\rangle$

$\vec{x} \cdot M = 3 + 24 + 115 = 142$

Knapsack Cryptography

Merkle-Hellman SS cryptography

1) Alice chooses SI $\vec{r} = (r_1, \ldots, r_n)$

2) Alice chooses large A, B

$B > 2r_n$, $\gcd(A, B) = 1$

computes $A^{-1} \bmod B$.

3) sets $M_i \equiv A r_i \bmod B$

(scrambles order)

public key is $(M_1, \ldots, M_n)$

Encryption

1) Bob writes message as a binary vector $\vec{x}$

2) computes $S = \vec{x} \cdot M = \sum_{i=1}^{n} x_i M_i$

transmits.

Decryption

1) computes $S' \equiv A^{-1} S \bmod B$.

2) solves SS problem for $(\vec{r}, S')$.

$$S' \equiv A^{-1} S \equiv A^{-1} \sum_{i=1}^{n} x_i M_i$$

$$\equiv \sum_{i=1}^{n} x_i (A^{-1} M_i) \equiv \sum_{i=1}^{n} x_i \vec{r}_i \bmod B$$

Ex: Alice chooses $\vec{r} = (3, 11, 24, 50, 115)$

$A = 113$
$B = 250$

$M = (3 \cdot 113, 11 \cdot 113, 24 \cdot 113, 50 \cdot 113, 115 \cdot 113)$

$\equiv (89, 243, 212, 150, 245) \mod 250.$

$A^{-1} \equiv 177 \mod 250$

Bob wants to send $\vec{x} = (1\,0\,1\,0\,1)$

$S = \vec{x} \cdot M = 89 + 212 + 245 = 546.$

Alice computes $177 \cdot 546 \mod 250$

$\equiv 142 \mod 250$