Some slides for 20th Lecture, Algebra 1

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

24-11-2011

Knapsack crytosystem (Merkle-Hellman)

A knapsack problem:

- Consider a knapsack (or rucksack) with volume N
- Consider n objects with volume $e_1, \ldots, e_n$
- Maybe we cannot put everything in the knapsack, but we want to fill it. That is, we want to find $I \subset \{1, \ldots, n\}$ such that

$$\sum_{i \in I} e_i = N$$

Our knapsack problem

Given $e_1, \ldots, e_n \in \mathbb{N}$ and $N \in \mathbb{N}$, find a binary number k with n bits $k = (\lambda_1, \ldots, \lambda_n)$ ($\lambda_i = 0$ means object e_i is not in the knapsack) such that:

$$\sum_{i=1}^{n} \lambda_i e_i = N$$

Our knapsack problem is NP-Complete, but there is an easy case:

$$e_i > \sum_{j=1}^{i-1} e_j, \quad \forall\, i$$

Example: $(e_1, \ldots, e_5) = (2, 3, 7, 15, 31)$ and $N = 24$.
$24 - 15 = 9 \quad \rightarrow e_4$
$9 - 7 = 2 \quad \rightarrow e_3$
$2 - 2 = 0 \quad \rightarrow e_1$
Hence $N = 2 + 7 + 15$ and $k = (1, 0, 1, 1, 0) = 24$.

Message: is binary (0's and 1's). We cut it in blocks of length n. Consider that we send M, a block of length n.

1. Bob chooses an easy knapsack $(e_1, \ldots, e_n)$ and $N \in \mathbb{N}$ such that $N > \sum_{i=1}^{n} e_i$ (why?$\rightarrow$ unique encryption). He also chooses $w \in \mathbb{N}$ such that $0 < w < N$ and $\gcd(w, N) = 1$ (why?)
2. Bob computes $[w^{-1}]_N$ ($[w][w^{-1}] = [1]$) and $(a_1, \ldots a_n)$, with $0 < a_i < N$ where

$$a_i \equiv we_i (\mathrm{mod}\ N)$$

   Secret Key: $(e_1, \ldots, e_n), N, w, w^{-1}$
   Public Key: $(a_1, \ldots, a_n)$
3. Alice wants to send $M = (M_1 \ldots, M_n) \in (\mathbb{Z}/2\mathbb{Z})^n$. She computes

$$C = \sum_{i=1}^{n} M_i a_i$$

   and sends it to Bob

4. Bob gets C. He computes $[Cw^{-1}]_N$ because

$$w^{-1}C \equiv \sum_{i=1}^{n} w^{-1}a_iM_i \equiv \sum_{i=1}^{n} e_iM_i \pmod N$$

   We have $[Cw^{-1}]_N = [\sum M_ie_i]_N$. Note that $\sum M_ie_i \leq \sum e_i < N$, then $0 < \sum M_ie_i < N$ and encryption is unique.
5. Bob uses the easy knapsack to find $(M_1, \ldots, M_n)$ from $\sum M_ie_i$.
6. Eve?, she gets $C = \sum_{i=1}^{n} M_ia_i$, but it is not an easy knapsack.

Example knapsack

- $M = (1, 1, 0, 0, 1)$
- $N = 61$, $w = 17$, $\gcd(17, 61) = 1$
- $w^{-1} \equiv 18 \pmod{61}$
- $a_1 = 17 \cdot 2 \equiv 34 \pmod{61}$
  $a_2 = 17 \cdot 3 \equiv 51 \pmod{61}$
  $a_3 = 17 \cdot 7 \equiv 58 \pmod{61}$
  $a_4 = 17 \cdot 15 \equiv 11 \pmod{61}$
  $a_5 = 17 \cdot 31 \equiv 39 \pmod{61}$
- Public Key=$(34, 51, 58, 11, 39)$, so to encrypt (1,1,0,0,1) we have $34 + 51 + 39 = 124$. Alice sends 124.
- Bob receives 124 and computes $124 \cdot 18 \equiv 36 \pmod{61}$. Then he has an easy knapsack for 36:
  $36 - 31 = 5 \quad \rightarrow e_5$
  $5 - 3 = 2 \quad \rightarrow e_2$
  $2 - 2 = 0 \quad \rightarrow e_1$, and recovers $M = (1, 1, 0, 0, 1)$
- Eve could do: $124 = a_1 + a_2 + a_5 = 34 + 51 + 39$ but this is a difficult knapsack (for large numbers!)