Колесовой Ольги,
244 группа

Реферат

Мультипликативные рюкзаки

Идея мультипликативного рюкзака была предложена и опубликована в 1977 году. Так называемый мультипликативный рюкзак использует точно такую же функцию шифрования как и у аддитивной рюкзачной схемы Миркла-Хиллмана (Merkle-Hellman). Однако, имеет лазейку другой природы, основывающуюся главным образом на трансформации из задачи об аддитивном рюкзаке в задачу о мультипликативном. Это было опубликовано Мирклом и Хиллманом в их оригинальной статье. Объясним сначала схему построения открытого ключа. Выбирается n взаимно простых чисел $(p_1, p_2, \ldots, p_n)$, некоторое простое число q, такое что $q-1$ раскладывается на маленькие простые множители так что:

$$q > \prod_{i=1}^{n} p_i \tag{1}$$

и некоторый примитивный корень b по модулю q. Затем следует найти целые числа $a_i, (1 \leq a_i \leq q-1)$, такие что $p_i = b^{a_i} \ mod \ q$. a_i -– дискретный логарифм от p_i по основанию b по модулю q. Вот почему $q-1$ должен быть выбран, как произведение простых маленьких чисел, чтобы позднее при помощи алгоритма Похлиджа-Хиллмана (Pohlig-Hellman) можно было легко вычислять дискретные логарифмы в этой задаче.

Зашифрованное сообщение будет выглядеть так:

$$S = \sum_{i=1}^{n} x_i a_i$$

где x_i–n-битный вектор исходного сообщения.

Дешифрование происходит следующим образом:

$$S' = b^S \ mod \ q$$

так как $b^S = b^{\sum x_i a_i} = \prod b^{x_i a_i} = \prod p_i^{x_i} \ mod \ q$. Последнее равенство – результат условия (1). Закрытым ключом является (b, q), открытый ключ - a_i. Затем можно легко найти соответствующий x, начинающийся с S', используя тот факт, что числа p_i взаимно простые. Последнее замечание очень важно, так как в общем случае задача о произведении подмножеств NP-полная.

Эта схема может быть взломана атакой низкой плотности (low density attack). Однако неудобство заключается в необходимости отдельного запуска алгоритма редукции решетки (lattice reduction algorithm) (который занимает минимум n^4 операций) для атаки каждого n-битного сообщения. Поборол эту проблему Одлыжко, испытав другую атаку. Здесь он начал с предположения, что некоторые p_i известны. Затем он попробовал найти q и b. Он так же предполагает, что b, q и a_i состоят приблизительно из m бит. Его атака занимает полиномиальное время, если $m = O(n \log n)$.

Используемая литература:

/1/ Encyclopedia of Cryptography and Security Авторы: Henk C. A. van Tilborg Соавтор Henk C. A. van Tilborg Опубликовано издательством Springer, 2005 Всего страниц: 684

/2/ Selected Areas in Cryptography: 5th Annual International Workshop, SAC '98, Kingston, Ontario, Canada, August 17-18, 1998 : Proceedings Авторы: Stafford Tavares, Henk Meijer Соавтор Stafford Tavares Опубликовано издательством Springer, 1998 Всего страниц: 375