Un criptoanálisis del criptosistema de Chor-Rivest

Jan Alejandro Medina, Diego Fernando Ruiz
Departamento de Matemáticas
Universidad del Cauca, Popayán, Colombia
Email: janmedina14@gmail.com, dfruiz1@gmail.com

Resumen. Sean $\langle G, + \rangle$ un grupo conmutativo notado aditivamente, $h \geq 2$ un entero y $A = \{g_1, g_2, \ldots, g_k\} \subseteq G$. A es un conjunto B_h en G si todas las sumas de h elementos de A (no necesariamente distintos) son diferentes. Es decir, si todas las expresiones de la forma

$$g_{i_1} + g_{i_2} + \cdots + g_{i_h}, \quad \text{con } 1 \leq i_1 \leq i_2 \leq \cdots \leq i_h \leq k,$$

producen elementos distintos en G [1].

El criptosistema de Chor-Rivest es un criptosistema tipo mochila que utiliza la estructura y la aritmética de los campos finitos y los conjuntos B_h tipo Bose-Chowla para su implementación [2]. Una característica importante de este tipo de criptosistemas, es la densidad, la cual permite medir el tamaño de los elementos de la mochila.

La seguridad del criptosistema Chor-Rivest, por ser tipo mochila, se basa en el problema de la suma de un subconjunto pero utilizando mochilas de alta densidad, evitando así ataques como el de Lagarias y Odlyzko [5] que hace uso del algoritmo L^3. Existen varios ataques contra éste sistema, el ataque más importante es el planteado por Vaudenay, quien hace uso de la teoría de los campos finitos para romper el criptosistema en sus parámetros originales [3]. Actualmente, con la nueva definición de densidad planteada por Kunihiro [4], se demuestra que éste sistema es vulnerable al *Lattice Attack*.

En este trabajo presentaremos en forma detallada algunos ataques contra éste sistema, como el propuesto por Vaudenay que se puede considerar el ataque más completo y además mostraremos como la nueva definición de densidad afecta la seguridad de éste sistema.

Palabras claves. Campos Finitos, Criptosistema, Clave pública, Conjuntos B_h, Lattice Attack.

Referencias

[1] Gómez Ruiz, C. A. & Trujillo Solarte, C. A. (2011). Una nueva construcción de conjuntos Bh modulares. Matemáticas: Enseñanza Universitaria, XIX(1) 53-62.

[2] Chor, B. & Rivest, R. L. (1988). A knapsack-type public key cryptosystem based on arithmetic in finite fields. IEEE Transactions on Information Theory, 34, 901-909.

[3] S. Vaudenay, "Cryptanalysis of the chor-rivest cryptosystem," in *CRYPTO '98*, pp. 243–256, Springer-Verlag, 1998.

[4] N. Kunihiro, "New definition of density on knapsack cryptosystems," in *AFRICACRYPT*, pp. 156–173, 2008.

[5] J. C. Lagarias and A. M. Odlyzko, "Solving low-density subset sum problems," *J. ACM*, vol. 32, pp. 229–246, January 1985.