1056-12-1496 **Gregory V. Bard*** (bard@fordham.edu), Department of Mathematics, John Mulcahey Hall, Fordham University, Bronx, NY 10530. *Algebraic Attacks on Bivium and Trivium, Accelerated by Cutting the Variable-Sharing Graph.*

The stream ciphers Bivium and Trivium appear very simple, and intuition says that they should be therefore easily breakable. While Bivium has been the subject of many published attacks, Trivium remains notoriously difficult.

In their 2008 paper, Kenneth Wong, Gregory Bard and Robert Lewis introduced the variable-sharing graph, and showed how balanced vertex-cuts of this graph can accelerate algebraic attacks, by a wide margin.

The variable-sharing graph has a vertex for each variable in a polynomial system of equations. There is an edge between two variables if and only if those two variables ever appear together in the same equation. By searching for balanced vertex-cuts one can break the polynomial system into two smaller ones.

In that paper, such a cut was used to simulate an attack under the assumption that a few bits of the key have been leaked. A polynomial system of equations is constructed, and a balanced vertex-cut is found, which results in two easily solved systems. While other types of polynomial systems were discussed in the paper (e.g. game theory, computational geometry, molecular chemistry), Bard will focus on the Bivium and Trivium attacks for this talk. (Received September 22, 2009)