1092-68-204 **Gregory V. Bard*** (bardg@uwstout.edu), Dept. of Math., Stat., and Comp. Sci., Jarvis Hall, Science Wing, University of Wisconsin—Stout, Menomonie, WI 54751, and **Damien Koeppel**.
Reducing the Number of Variables in a System of Equations during Algebraic Cryptanalysis, by Constructing a Forest. Preliminary report.

Algebraic cryptanalysis is a two-phase process. First, one converts a cipher into a system of equations—usually polynomial and over a finite field (char 2). Second, one solves the equations to recover a secret key or plaintext. Often the polynomial system is huge, with thousands of variables. We propose an approach that introduces a middle phase.

We make use of a data structure called "a forest" which is a set of "trees." (By tree is meant a binary tree, but where each node can have any natural number of descendants, not merely 0 or 2.) Every variable in the system of equations is found exactly once in the forest; all variables in a given tree are either known to be equal to each other or known to be additive inverses, after all the original equations have been written. The entire system of equations is rewritten when the forest is complete. Every variable in the old system of equations is represented in the new, by the variable which is the unique "root" of its tree.

This results in the new system having far fewer variables than the old. In turn, that will significantly reduce the running time of solving the system. We will use the "scalable encryption algorithm" to demonstrate how this process can be applied in the case of the cryptanalysis of a block-cipher. (Received August 09, 2013)