Mathematics of Post-Quantum Cryptography

Algebraic Cryptography Center at Stevens Institute of Technology

Gregory V. Bard

(Fordham University)

Using Graph Theory to split polynomial systems of equations

Abstract:

The variable-sharing graph of a polynomial system of equations has one vertex for each variable, and an edge between two variables if and only if those variables appear together in at least one equation. If this graph is disconnected, then the system is actually two separate systems that can be solved individually. This can provide a huge speed-up, but is unlikely to occur either randomly or in applications. However, it may be the case that deleting a small number of vertices c disconnects
the variable-sharing graph in a balanced fashion, so that the ratio of the sizes of the larger and smaller components is roughly less than two.

If this is the case, then we demonstrate two techniques, one for small fields and one for large fields, to split the system. For small finite fields $\mathbb{GF}(q)$, we simply iterate through all possible q^c guesses of the c variables, and solve the separated systems. If the field is infinite or finite but large (i.e. has more than roughly five members), we separate the system with resultants. We present two methods for detecting this condition and identifying the c variables.

First, when c is small, or when $\vert V\vert$ is small, one can run a large series of depth-first searches. Alternatively, when c or $\vert V \vert$ is large, we show how to use off-the-shelf balanced
edge cut determining software to generate a “reasonable” vertex cut. Also, we state a condition for a system of equations to be immune to this approach.

We present experiments which show that this condition can occur in practice, with very sparse polynomial systems. We also present four applications. The first is to implant/detect a trapdoor in the stream cipher QUAD; the second is to show a security property of the authentication system HB/HB+; the third has to do with "the Apollonius Problem" from Euclidean Geometry; the fourth is the "cube game" from multiparty game theory.

Algebraic Cryptography Center

STEVENS Institute of Technology