MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Post-Quantum Cryptography: Unbalanced Oil and Vinegar System - Part 1

Authors: Marc Kleffmann, Enrico Thomae, Christopher Wolf
Ruhr-University Bochum
Studies in IT-Security:
http://www.hgi.rub.de/studium

March 2011

Introduction

Assume that quantum computers exist. Then the actual signing algorithms like RSA and El-Gamal are not secure anymore. Therefore we use the post-quantum system "Unbalanced Oil and Vinegar" (UOV) for secure message signing. Are you able to break it anyway?

The basic principle of UOV is as follows. Two quadratic, multivariate systems of equations are given, connected by a hidden affine map. One system is public and hard to invert. The other is secret and due to a built-in trapdoor easy to invert.
In contrast to univariate equations (e.g. in x), multivariate equations have *several*, independent variables such as x, y, z or x_1, x_2, x_3.

Introduction

An example for a multivariate system of equations in 5 variables is given on the last slide.

Let P be a quadratic system of equations in the variables $x_1, ..., x_n$. This is the public key, allowing easy verifications of any given signature $[x_1, ..., x_n]$.
Given in addition is an affine map S, mapping P to the second system of equations called F. F and S represent the secret key, allowing an easy solving of P respectively an easy message signing.

The idea of the trapdoor, placed in the secret system of equations F, is as follows. The n variables are partitioned in o oil variables and v vinegar variables.

Introduction

Whereas in the public system P all variables are completely mixed, the situation in the secret system F is comparable to a salad: There is no "real mixture" between oil and vinegar. Concretely no quadratic term in F exists, which is combined of two oil variables. There are only quadratic terms of two vinegar variables or mixed terms.

Choosing the vinegar variables by random, we derive a linear system of equations with o equations and o unknowns. This is solvable in an easy way. In the public system P a proceeding like this does not exist.

Parameter & Challenge:

Let $n = 5$, $v = 2$, $o = 3$ and let $K = \mathbb{F}_5$ be the field. (Note: In praxis $v = 2o$ is used. Here we differ from this to limit the complexity of calculations.)

Find a solution $x = [x_1, x_2, x_3, x_4, x_5]$ for the public system of equations given on the next slide, i.e. find a signature of the message $[3, 0, 2]$.

Public system of equations:

$$
\begin{aligned}
2x_1x_3 + 3x_1x_4 + 2x_1 + {x_2}^2 + 2x_2x_3 + 2x_2x_4 + x_2 + 2{x_3}^2 + \\
3x_3x_4 + 2x_3x_5 + x_3 + 4x_4 + {x_5}^2 &= 3 \\
x_1x_2 + 3x_1x_3 + x_1x_4 + 2x_1x_5 + 2x_1 + 3{x_2}^2 + 3x_2x_3 + 4x_2x_4 + \\
4x_2x_5 + x_2 + 4{x_3}^2 + x_3x_5 + {x_4}^2 + x_4x_5 + {x_5}^2 &= 0 \\
x_1x_2 + 3x_1x_3 + x_1x_4 + 2x_1x_5 + 4x_1 + x_2x_3 + 3x_2x_5 + 4x_2 + \\
4{x_3}^2 + x_3x_5 + 4x_3 + 3x_4x_5 + 4x_4 + {x_5}^2 + 4x_5 &= 2
\end{aligned}
$$