Attacking Cryptographic Schemes Based on ‘Perturbation Polynomials’

Martin Albrecht\(^1\), Craig Gentry\(^2\), Shai Halevi\(^2\), and Jonathan Katz\(^3\)
\(^1\)Royal Holloway University, \(^2\)IBM T.J. Watson Research Center, \(^3\)University of Maryland (work done while visiting IBM)

**Key Predistribution (Goal):** Pre-load keying material so that (1) all nodes in a MANET of size \(n\) can compute a shared key, yet (2) compromise of some nodes will not reveal keys used by any *uncompromised* pair of nodes.

**Trivial Solution:** Each pair of nodes share an independent key. This requires per-node storage of \(n-1\) keys, which is prohibitive for large \(n\).

**An Optimal(?) Solution:** An optimal solution for the case of *information-theoretic* (i.e., perfect) security is known. Zhang et al. (MobiHoc 2007) suggest a new, more efficient approach that they claim gives *computational* security. Their approach was adapted and extended in subsequent work at PerCom 2007 and INFOCOM 2008.

**The Scheme of Zhang et al.:** Their basic idea is to choose a (suitable) random bivariate polynomial \(F(x,y)\) and give node \(i\) the univariate polynomial \(s_i(y) = F(i, y) + noise(y)\), where \(noise\) represents a small “perturbation polynomial”. Nodes \(i\) and \(j\) can compute \(s_i(j) \approx s_j(i)\), and from this derive a key.

The claim of Zhang et al. is that the presence of the noise makes polynomial interpolation computationally infeasible, and therefore makes the scheme resilient to an unbounded number of corruptions.

**Our Results:** We show several attacks that *completely break* the scheme of Zhang et al. (as well as all subsequent generalizations). Our attacks rely on efficient list decoding algorithms for error-correcting codes, and lattice-basis reduction. Our attacks case doubt on the potential validity of the “perturbation polynomial” approach to constructing cryptosystems.