Note on Design Criteria for Rainbow-Type Multivariates

Jintai Ding[1], Bo-Yin Yang[2], Lei Hu[3], Jiun-Ming Chen[4]

[1]University of Cincinnati, Cincinnati, Ohio, USA, ding@math.uc.edu
[2]Academia Sinica, Taipei, Taiwan, by@moscito.org
[3] Graduate School of the Chinese Academy of Sciences, Beijing, China, hulei@gucas.ac.cn
[4]National Cheng-Kung University, Tainan, Taiwan, jmchen@ntu.edu.tw

April 28, 2008

Abstract

This was a short note that deals with the design of Rainbow or "stagewise unbalanced oil-and-vinegar" multivariate signature schemes. We exhibit new cryptanalysis for current schemes that relates to flawed choices of system parameters in current schemes.

These can be ameliorated according to an updated list of security design criteria.

Suspended Paper

This paper is currently under rework, and temporarily superceded by ePrint 2008/108. An update on new, actual TTS and Rainbow schemes and implementations will appear here soon.

Revision Notes

- Summer, 2005 to Winter, 2006: Discussions leading to this paper.
- March 3, 2006: First draft
- March 29, 2006: Second Draft, TWISC (Taiwan Information Security Center) tech report
- September 5, 2006: Submitted to e-Print Archive.
- September 7, 2006: Appeared, e-Print Archive.
- October 19, 2006: Third Draft.
- Mar 14, 2008: Accepted to ACNS 2008, continued as ePrint 2008/108