Cryptanalysis of Chinese S-Boxes & Japanese L-Boxes

Alexander A. Veith*

CHES '06 RUMP SESSION

a.a.veith@in-sed.com

Valid from October 11, 2006 unv.†

Abstract

This short presentation shows the different possibilities of Cryptanalysis and different side-channel attacks on Chinese S-Boxes (Sandwich boxes) and Japanese L-Boxes (Lunch Boxes). Furthermore we will show the application of the CRT (Chinese Remainder Theorem on our system) and the gohan(rice)-granularity of the solution set to the whole cryptosystem. As a last point we will tak about the snake - oil factor and how it affects S- and L- boxes and of course countermeasures to the attack presented.

1 Classification

THE FOLLOWING DOCUMENT IS A PROPOSAL THE RUMP SESSION OF CHES '06. IT HAS **DRAFT** STATUS AND IS SUBJECT TO CHANGES BY THE AUTHOR OR ANY OTHER PARTY INVOLVED WITHOUT FURTHER NOTICE. THIS DOCUMENT IS ALSO CLASSIFIED LEVEL 6 : **JET LAG INFLUENCED HUMOR**. THE AUTHOR IS NOT TO BE HELD RESPONSIBLE IF HIS JOKES ARE NOT AS GOOD AS USUAL.

*Prof. Dr. Alexander A. Veith c/o InSED RESEARCH"

†until new version