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 talk 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 docu-
ment 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