

éñŸæĂi

éĀžėõrǎĭĴrǎĭĀ āNŪāžņāȳĈæȳũæũĀāNžāȳņāĒȘșǎĭSǎNŪāZZēāŪ4āRũ
āȳņāŽĭçğŜāņēēZcēĭrǎžũčǎTçĭ'ũæĻĀ5āRũæĭĭ

GPA æŒŠǻŘŇ- 1/90

éAnăÖEäžEāRĎcgŇāRřěČjcŽDǎōđcÖřæÚzàiíííĩNārzážÖærŘcğŇǎōđcÖřæÚzàiíííĩRǎLÊáŁncz

äyŠäyŽæŁĂèČj

èrñèĹ äyñæŮĜ / èŇsèrñ (CET-6)

çĹŇăžŘèrñèĹ C, C#, Java, Verilog.

âjĹăŖŚăũěăË Microsoft Visual Studio, NetBeans IDE, Modelsim, Design Compiler

ăŖĆăyŎçndètŽ, äyŠăĹłĲŤșèrũ & èőžæŮĜăŖŚèąĹ

ăŖĆăyŎçndètŽ

2010 **ăĖĹăŽjădġăñęçŤŤșŤăñŖèőŁèőąçndètŽ (ăĹąăĹŖăőĹăĖĹćĂèrũètŽ),**
äyĹçñĹăěŮ.

2010 **ăĖĹăŽjădġăñęçŤŤșăĹąăĹŖăőĹăĖĹçndètŽ, äžŇçñĹăěŮ.**

äyŠăĹłĲŤșèrũ

2013 **ăĹĹăyĂçġŇăŖĖçăĹăłăĹŮAPIăóĹăĖĹăĜăçĂætŇăŮžæŤăŖĹçșžçžŤăĹ**
(äyŠăĹłĹăŖũjžZL 201310013010.4)

èőžæŮĜăŖŚèąĹ

2013 "Padding Oracle Attack on PKCS#1 v1.5: Can Non-standard Implementation
Act as a Shelter?", Cryptology and Network Security 2013.

ăũšăĲŤŤ "Improved fault attack on LBlock: earlier injection with no extra faults",
Chinese Journal of Electronics.

ăŖĹăĲĹèőžæŮĜ äyďçŖĜ: WISA 2013/SAC 2015