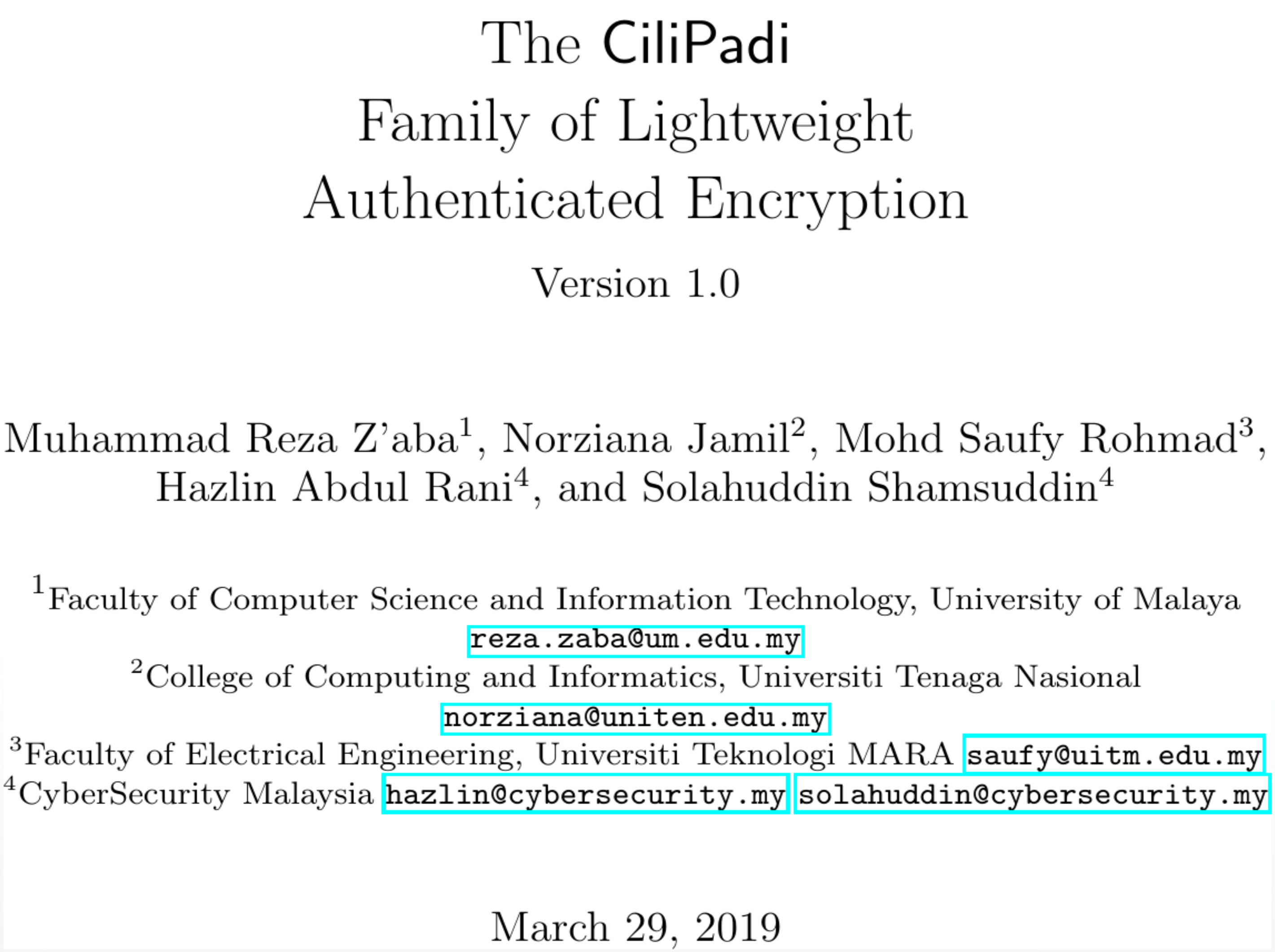
2 Days Training on IoT Architecture and Simulation using ns-3

LAB 6

Muhammad Saufy Rohmad
EE, UiTM
CompuThings

Lab 6 – Cilipadi IoT Cryptography



The CiliPadi
Family of Lightweight
Authenticated Encryption

Version 1.0

Muhammad Reza Z'aba[1], Norziana Jamil[2], Mohd Saufy Rohmad[3], Hazlin Abdul Rani[4], and Solahuddin Shamsuddin[4]

[1]Faculty of Computer Science and Information Technology, University of Malaya
reza.zaba@um.edu.my
[2]College of Computing and Informatics, Universiti Tenaga Nasional
norziana@uniten.edu.my
[3]Faculty of Electrical Engineering, Universiti Teknologi MARA saufy@uitm.edu.my
[4]CyberSecurity Malaysia hazlin@cybersecurity.my solahuddin@cybersecurity.my

March 29, 2019

Lab 6 – Cilipadi IoT Cryptography

1. #git clone https://github.com/mrzgh/cilipadi-ae.git
2. #cd cilipadi128vmild/ref
3. #gcc -o cilipadi api.h led.c led.h crypto_aead.h cilipadi.c cilipadi.h encrypt.c
4. add #define OWNMAIN in cilipadi.c
5. run #./cilipadi