Department of Computer Science

COMPUTER SCIENCE SEMINAR SERIES

Power Analysis Attack on Jamming Assisted Key Agreement

SPEAKER **Mr Qiao HU**

PhD Student
Department of Computer Science
City University of Hong Kong
Hong Kong

DATE 14 June 2017 (Wednesday)
TIME 11:30 am - 12:00 noon
VENUE CS Seminar Room, Y6405
6th Floor, Yellow Zone
Yeung Kin Man Academic Building
City University of Hong Kong
83 Tat Chee Avenue
Kowloon Tong

ABSTRACT

Physical layer key agreement which utilizing the variations of the wireless channel to generate the shared key is a trend in wireless communication. This kind of schemes has shown its effectiveness against eavesdropping. But physical layer key agreement schemes utilizing channel state to generate the key have quite low speed due to the requirement of channel changing which brings the variations of the channel. iJam is a novel scheme utilizing assisted jamming signals to generate shared key without the requirement of channel variation which increasing the key generation speed. In this paper, we propose a power analysis attack which can break iJam by analyzing the power difference of each received signal. Simulation results show that our attack breaks iJam in most time.

This paper will be presented at International Workshop on Computer Science and Engineering (WCSE 2017), June 25-27, 2017, Beijing, China.

Supervisor: Dr Gerhard Petrus HANCKE

Research Interests: Wireless Security, RFID, Smart Cards and IoT, Embedded and Mobile Systems.

All are welcome!

In case of questions, please contact Dr HANCKE Gerhard Petrus at Tel: 3442 9341, E-mail: gp.hancke@cityu.edu.hk, or visit the CS Departmental Seminar Web at http://www.cs.cityu.edu.hk/news/seminars/seminars.html.