Dr. Jiangshan Yu (B.Eng, MSc, MPhil, PhD)

Contact

Critix, SnT,
University of Luxembourg,
6, Avenue de la Fonte
L-4364, Esch-sur-Alzette,
Luxembourg.

E-mail:
j.yu.research@gmail.com

Home-page:
www.jiangshanyu.com

Employment

12.2016 – present	**Research fellow**, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg.
12.2016 – present	**Honorary research fellow**, School of Computer Science, University of Birmingham, UK.
11.2014 – present	**Director (part-time)**, CloudTomo Limited, UK. (University of Birmingham spin-out company.)
12.2014 – 05.2015	**Tech consultant (part-time)**, Jin Xin Tong Trust and Investment Corporation Ltd, UK.

Education

10.2012 – 12.2016	**Ph.D** in Cyber Security. University of Birmingham, UK.
09.2011 – 08.2012	**M.Phil** in Cryptography. University of Wollongong, Australia.
08.2010 – 07.2011	**M.Sc.** in Information Security. University of Wollongong, Australia.
09.2005 – 08.2009	**B.Eng.** in Computer Science and Technology, Northeast Agricultural University, Harbin, China.

Main research impact:

My work on ledger-based end-to-end secure messaging system has attracted news media's attention and has been covered by more than 30 international and national news media including *Science Daily*, *Phys.org*, *ACM TechNews*, *EurekAlert*, *Futurism*, and *Silicon Republic*. The news has been released in more than 7 languages by media from more than 10 countries including UK, US, Germany, Ireland, Luxembourg, Turkey, Spain, and India. I have also been invited for an interview (to explain my innovation to general listeners) by Eldoradio --- a member of RTL group which is one of the world's leading producers of television content and the leading European entertainment network.

My patent-pending ledger-based applications have been further developed by a University of Birmingham spin-off, and have attracted funding support from Innovate UK.

I've co-designed a secure booting solution for Huawei Ltd, the largest telecommunications equipment manufacturer in the world, to manage their next generation network devices securely.

Awards

2017	**Chinese Government Award for Outstanding PhD Scholar Abroad**. (Success rate: 1% worldwide, 3% in UK.)
2014	**First place award**, the Coniston poster competition, University of Birmingham, UK.
2009	**Outstanding Graduates of Heilongjiang Province**, Heilongjiang, China.
2009	**Outstanding Graduates of Northeast Agricultural University**, Harbin, Heilongjiang, China.
2009	**Best Thesis Award**, Northeast Agricultural University, Harbin, Heilongjiang, China.
2008	**Outstanding Academic Award**, The Northeast Agricultural University, China.
2007	**First National Prize** of China Contemporary Undergraduate Mathematical Contest in Modelling, China;

2006 **Second National Prize** of China Contemporary Undergraduate Mathematical Contest in Modelling, China;
2006 **Outstanding Student Award** of The Northeast Agricultural University, China;
2006 **Outstanding Student Leadership Award**, The Northeast Agricultural University, China.

Funding:

2016 Jiangshan Yu. Investigating scalable blockchains. 10,000 Euro from The University of Luxembourg, 2016.
2015 Mark Ryan and Jiangshan Yu. Public ledger based secure email and cloud storage. 33,000 GBP from Technology Strategy Board (Innovate UK), 2015.
2015 Jiangshan Yu. 1,500 GBP from Security and Privacy Group@University of Birmingham and Obillex Ltd. for organising Blockchain workship at Birmingham.

Scholarships and Travel Grant:

2015 Universitas 21 travel grant from the University of Birmingham (to visit and present his work at Shanghai Jiao Tong University, China.)
2012-2015 EPSRC project funding for PhD studies at University of Birmingham
2012-2015 Overseas top-up scholarship from the University of Birmingham for PhD studies
2008 First class scholarship, Northeast Agricultural University, China
2007 Second class scholarship, Northeast Agricultural University, China
2006 First class scholarship, Northeast Agricultural University, China

Patent application

- Jiangshan Yu and Mark Ryan. **Key usage detection.**
  - UK Patent Application GB 1416188.9
  - US Patent Application US 14/852,342

Cooperation with journals, conference programme committees and others

- **Conference Program Committee**
  2018 IEEE International Conference on Communications (ICC)
  2017 International Conf. on Information Security Practice and Experience (ISPEC).
  2016 Software Architecture for Big Data and the Cloud.

- **Workshop Organisation**
  2015 Chair. Workshop on BlockChain, Birmingham, United Kingdom.

- **Invited Reviewer (Journal):**
  2017 IEEE Transactions on Information Forensics & Security (TIFS)
  IEEE Transactions on Cloud Computing (TCC)
  Journal of Computer Science and Technology (JCST)
  International Journal of Information Security (IJIS)

  2016 IEEE Transactions on Information Forensics & Security (TIFS)
  Security and Communication Networks (SCN)
  PLOS ONE

  2015 IEEE Transactions on Information Forensics & Security (TIFS)
  The Computer Journal (Comp. J)
  Security and Communication Networks (SCN)

  2014 Security and Communication Networks (SCN)

2013 Journal of Information Security and Applications (JISA)

- **Invited Reviewer (Conference):**

2017 *European Conf. on Computer Systems* (EuroSys)
IEEE/IFIP International Conf. on Dependable Systems and Networks (DSN)
European Symposium on Research in Computer Security (ESORICS)
ACM Asia Conf. on Computer and Communications Security (ASIACCS)
ICT Systems Security and Privacy Protection (IFIP SEC)

2016 *IEEE European Symposium on Security and Privacy* (EuroS&P)
European Symposium on Research in Computer Security (ESORICS)
International Symp. on Engineering Secure Software and Systems (ESSoS)
International Conf. on Information Security Theory and Practice (WISTP)

2015 *International Conference on Principles of Security and Trust* (POST-ETAPS)
ACM Asia Conf. on Computer and Communications Security (ASIACCS)
ICT Systems Security and Privacy Protection (IFIP SEC)

2014 *International Conf. on Applied Cryptography and Network Security* (ACNS)
ICT Systems Security and Privacy Protection (IFIP SEC)
Workshop on Formal Methods for Security (FMS)
Workshop on Privacy in the Electronic Society (WPES)

2013 *European Symposium on Research in Computer Security* (ESORICS)
Australasian Conference on Information Security and Privacy (ACISP)
International Workshop on Data Privacy Management (DPM)

- **Invited presentations:**

2016 Security seminal. University of Luxembourg, Luxembourg.
Security seminal. ETH Zurich, Switzerland.
2015 CryptoForma workshop, University of Strathclyde, Glasgow, UK.
2014 Security seminar. University of Birmingham, UK, 2014.
2013 Google Certificate Transparency Hack Day. Google, London, UK.
Cloud Technologies and Trust Domains. HP Labs Bristol, UK.
Security seminar. University of Birmingham, UK.
CryptoForma Workshop at ESORICS, UK.

Participation in industrial innovation

2016.08 – 2016.12 **Co-leader** with Prof. Mark Ryan. *Huawei SoC Secure Boot Solution*, UK. Industrial partner: Huawei Ltd., Shenzhen HQ. (Funded by Huawei Ltd.)

This project designs a security solution for Huawei to securely manage its next generation network devices, even when the device might be compromised. More details of the problem and solution are under NDA.

2015.05-2015.09 **Co-leader** with Prof. Mark Ryan. *Innovate UK project on user-friendly security and privacy to increase confidence in cloud-based systems*, UK. Industrial partner: CloudTomo Ltd. (Funded by Innovate UK.)

This project investigates the feasibility of designing a small-form-factor device, which we call CT-Box, to enhance security and privacy of cloud-based systems. CT-box is a pocket-sized hardware device, provides a plug-and-play solution to

help individuals and businesses to secure their email and cloud storage. The basis of CT-box is formed by our patent-pending blockchain technologies. Located on user's premises, CT-box seamlessly encrypts files and other text before sending them to the cloud. Computations on the device will permit content search, indexing, sharing, and messaging, which are often difficult to achieve with encrypted cloud data. This will enable SMEs and individual users to use the public cloud without having to trust the cloud provider with confidentiality of the data.

Academic Research projects:

2016 **Project leader**. *Technological aspects of the Internet of Things,* UK. (Funded by Law School, University of Birmingham.)

Other activities:

2011-2012 **President**, Endless Martial Arts Association, Wollongong, Australia.

2010-2012 **Manager**, Department of Student Service, Wollongong Chinese Students & Scholars Association, Wollongong, NSW, Australia.

2007-2009 **Vice-resident**, Guild of Students, Northeast Agricultural University, China.

Publications

Since 2012, I have published 11 peer-reviewed papers, including **5** journal papers**, 5** conference papers, and **1** book chapter**. 6 out of 11** are accepted in 2017. I currently have **3** submitted papers under review.

Total IF: **17.521**
Total number of citations: **128**
H-index: **5**
i10-index: **4**

List of publications

2017

- Jiangshan Yu, Mark Ryan, and Cas Cremers. **DECIM: Detecting Endpoint Compromise In Messaging**. *IEEE Transactions on Information Forensics and Security (TIFS,* IF=4.332), 2017. [citations: 6]
- Diego Kreutz, Jiangshan Yu, Paulo Verissimo, Catia Magalhaes, Fernando Ramos. **"The KISS principle in Software-Defined Networking: a framework for secure communications"**. *IEEE Security & Privacy* (IF=1.382), 2017. (To appear).
- Jiangshan Yu and Mark Ryan. **Evaluating web PKIs.** *Software Architecture for Big Data and the Cloud*, 1st Edition, Chapter 7, June 2017.
- Kevin Milner, Cas Cremers, Jiangshan Yu, Mark Ryan. **Automatically Detecting the Misuse of Secrets: Foundations, Design Principles, and Applications.** The 30th IEEE Computer Security Foundations Symposium (*CSF),* 2017.
- Jiangshan Yu, Mark Ryan and Liqun Chen. **Authenticating compromisable storage systems**. *The 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2017.
- Marcus Völp, Francisco Rocha, Jérémie Decouchant, Jiangshan Yu and Paulo Verissimo. **Permanent Reencryption: How to Survive Generations of Cryptanalysts to Come**. *Security Protocols XXV*, 2017. (To appear)

2016

- Jiangshan Yu, Vincent Cheval, and Mark Ryan. **DTKI: a new formalized PKI with verifiable**

trusted parties. *The computer Journal* (IF=0.711), Vol. 59 No. 11, pp. 1695-1713, 2016.
[citations: 18]

2015

- Jiangshan Yu and Mark Ryan. **Device attacker models: fact and fiction"**. *Security Protocols XXIII*. pp. 158-167, 2015.
[citations: 1]

2014

- Jiangshan Yu, Guilin Wang, Yi Mu, and Wei Gao. **An Efficient and Improved Generic Framework for Three-Factor Authentication with Provably Secure Instantiation**. *IEEE Transactions on Information Forensics and Security (TIFS* IF=4.332*)*, Vol.9, No.12 , pp. 2302-2313, 2014.
[citations: 29]

2013

- Guilin Wang, Jiangshan Yu, Qi Xie. **Security Analysis of A Single Sign-On Mechanism for Distributed Computer Networks**. *IEEE Transactions on Industrial Informatics* (IF=6.764), Vol.9, No.1, pp.294-302, 2013.
[citations: 49]

2012

- Jiangshan Yu, Guilin Wang, and Yi Mu. **Provably Secure Single Sign-on Scheme in Distributed Systems and Networks**. *IEEE TrustCom*, pp. 271-278, 2012.
[citations: 23]