CS3012 Software Engineering

Biography of an influential software engineer

- Qizhi Yao

XingChen Yang

173743774

November 11,2020

Contents

1. Introduction

This document is a biographical essay about a software engineer which I found to be influential and inspiring. I think Yao Qizhi is the most influential software engineer in China. Yao Qizhi won the Turing Award in 2000 and is the only Chinese scholar to receive the award (as of 2020); he has been a full-time professor at Tsinghua University since 2004 and was elected as a foreigner of the Chinese Academy of Sciences in the same year Academician; Yao Qizhi's research directions include computing theory and its applications in cryptography and quantum computing. He first proposed the complexity of quantum communication, distributed quantum computing mode, and later became the basis of distributed quantum algorithms and quantum communication protocol security.

2. Yao Qizhi – Biography

2.1. The first stage: Algorithm theory innovation

As early as when he was studying for a Ph.D., Yao Qizhi put forward an argument for the complexity of randomization algorithms, and now it has become an important tool for researchers. In a paper in 1977, Yao Qizhi proposed Yao's min-max principle, which became the basic technique of inference random algorithm and complexity, and has also been applied to the fields of attribute testing and learning theory. In 1978, Yao Qizhi made a fundamental innovation in data structure innovation. In the "Should tables be sorted?" paper, he introduced a data structure abstract model called cell-probe model, which has been widely used to create lower bound proofs of algorithms. At this stage, Yao Qizhi's most important contribution is to put forward an important sub-field of theoretical computer science: communication complexity and pseudo-random number generation calculation theory.

2.2. The second stage: laying the foundation of cryptography

In 1982, Yao Qizhi returned to Stanford University from the Department of Computer Science at the University of California, Berkeley. His research focus gradually shifted from the original algorithm theory to the fields of cryptography, computer security and random computing. And one of the most famous problems is the problem of Yao's millionaires. How can two millionaires compare their wealth without revealing any information about their wealth? This problem was later derived from the origin of the problem of secure multi-party computing: how can users complete computing tasks collaboratively through the network in a non-innovative multi-user system, while ensuring the security of their respective data? Once the problem of secure multi-party computing was proposed, it attracted many scholars to study, and later became one of the basic problems of cryptographic protocol research. It has been widely used to solve problems in many computing fields such as data mining, database query, and scientific computing. And Yao Qizhi naturally became the founder of the foundation of modern cryptography. In 1982, Yao Qizhi gave a solution: by generating random numbers, adding public key and private key encryption and then comparing, avoiding the orderliness of the real number field and the reversibility of addition and subtraction bring redundancy Information exposure. In addition to the problem of Yao's millionaires, Yao Qizhi also made pioneering contributions in encryption and secure computing. The "Dolev-Yao model" has become the starting point for most symbolic security work, and the "Theory and applications of trapdoor Functions" and "Protocols for secure computations" have also become important works in the field of secure computing. In addition, there are XOR-lemma, a basic technology in the field of de-randomization, and a garbled circuit technology to solve secure multi-party calculations, which are also proposed by Yao Qizhi.

2.3. The Third Stage: Quantum Computing

After the 1990s, while teaching at William and Edna Macaleer Engineering and Applied Science at Princeton University, Qizhi Yao began to work on quantum computing, communication and information theory. In the 1993 paper "Quantum circuit complexity", Yao Qizhi extended the complexity of

communication envelopes to the field of quantum computing, completing the theoretical foundation of quantum computers. In the field of circuit complexity, computational geometry, data structure, and quantum computing, Professor Yao raised many open questions and developed many constructive ideas. In 1995, Yao Qizhi proposed a distributed quantum computing model, which later became the basis for the security of distributed quantum algorithms and quantum communication protocols. Relying on Yao Qizhi's basic contributions to computational theory, including the generation of pseudo-random numbers based on complexity, theories of cryptography and communication complexity, the American Computer Association ACM awarded him the Turing Award and a million-dollar prize in 2000 in recognition of Yao Qizhi's Great contribution made by the computer industry.

3. Discussion

Mr. Yao's academic contributions are undoubtedly extremely groundbreaking and far-reaching, mainly focusing on the foundations of cryptography, computational complexity and quantum computing. I personally think that Yao Qizhi is a software engineer with the greatest impact on China, and he also has a pivotal position in the world IT industry. What moved me most was that in 2016 he renounced his American citizenship and officially changed from a foreign academician of the Chinese Academy of Sciences to an academician of the Chinese Academy of Sciences. And set up a special course in Tsinghua University to improve students' computer theory foundation, and cultivate a large number of outstanding talents. After Yao Qizhi served as the dean of the School of Computer Science at Tsinghua University, the computer major of Tsinghua University ranked first in the world in the U.S. News World University Rankings.

4. Source

ANDREW CHI-CHIH YAO

https://amturing.acm.org/award_winners/yao_1611524.cfm

Andrew Yao

https://en.wikipedia.org/wiki/Andrew_Yao

Introducing 'The World's Billionaires Problem'

https://priviledge-project.eu/news/introducing-the-world-s-billionaires-problem

Berkeley in the 80s, Episode 4: Andrew Yao

https://www.youtube.com/watch?v=MGV6JaW42us

Two top Chinese-American scientists have dropped their U.S. citizenship

https://www.sciencemag.org/news/2017/02/two-top-chinese-american-scientists-have-dropped-their-us-citizenship

Yao's Principle and the Secretary Problem

https://www.mpi-inf.mpg.de/fileadmin/inf/d1/teaching/summer16/random/yaosprinciple.pdf