Fang Song

Department of Computer Science
Portland State University
fang.song@pdx.edu | fangsong.info
Google Scholar Profile

Self-Appraisal of Scholarly Agenda and Accomplishments

August 8, 2022

Table of Contents

I Scholarly Agenda and Contributions

Over the course of my employment at Portland State University (PSU), I have committed to establishing myself as a team player to promote student success, serve the university and the local community, in addition to advancing cutting-edge research and improving the greater scientific community.

These contributions are demonstrated by my publications, external funding, teaching, mentoring, professional services, and outreach activities. The concerted efforts have pushed forward the research fields, and also broadened participation and enhanced the diversity in computing. It is especially fulfilling to have initiated an expanding mass in theoretical computer science (quantum computing and quantum-safe cryptography in particular) at PSU, which had limited presence before. This will continue boosting local engagement and raising the recognition of PSU.

I provide an overlook of my major goals and contributions below in this section. They will be supported by more elaborate descriptions in the following sections. When appropriate, I will offer perspectives in both contexts – the PSU/Portland community and the academic community.

There is one special attention I would like to draw before proceeding. My appointment as an assistant professor at PSU started in Fall 2016. During 09/2018 – 02/2020, I was on leave and worked at Texas A&M University still as an tenure-track assistant professor. Then I returned to PSU since 03/2020[1]. By PSU's P&T guideline, my tenure application at this time would be considered a case that demands demonstration of "extraordinary achievements". In light of this, Section I.4 exhibits supporting evidence.

I.1 Research

My research intersects at *quantum computing* and *cryptography*, and I approach them via the perspective and tools of a *theoretical computer scientist*. The major research goals are three-fold.

1. Build a **provable-secure framework to reason about security in the presence of quantum adversaries**. This targets at the foundation of the field known as *post-quantum cryptography*.

2. Design **quantum algorithms especially for computational problems critical in post-quantum cryptography**.

3. Develop **novel cryptographic primitives using quantum information processing**, known as *quantum cryptography*, and investigate the **limits and strengths of quantum computing** via *quantum complexity* theory.

[1] More details about the internal timeline at PSU is described in the supplementary document.

I have made fundamental contributions on a number of topics, such as **quantum-secure zero-knowledge proof systems and protocols for secure computation, quantum security proofs of block ciphers and the quantum random oracle model, quantum algorithms for number-field problems, and quantum (computational) pseudorandomness**. These results have been published on top-tier conferences and journals[2], including **STOC, SODA, FOCS, SICOMP, Crypto, Eurocrypt, QIP**. These research endeavors have be supported by external grant awards in total amount of $1.5M, which includes an **NSF Career Award**, and a **SONY Faculty Innovation Award**.

Beyond the immediate scientific values, these work accompanied with other efforts, have also aimed at another broader goal of **breaking the barrier of researchers from drastically different backgrounds to expand the research boundary**.

Now turning the spotlight locally onto PSU, before I joined the Computer Science department, the presence of research in quantum computing, (post)-quantum cryptography, and theoretical computer science (TCS) at best scarce[3] I had since set the goals of building a reputable research program in quantum computing, cryptography and TCS at PSU, and gradually raising PSU as a recognizable place.

I.2 Teaching and Advising

I believe in the significant impact of STEM education. TCS in particular both possesses **profound intellectual beauty**, and also provides an effective channel to **building essential learning skills and a firm foundation** that are beneficial for the entire computer science education and future career. I have therefore striven to achieve the unique capacity made possible by the education effort in TCS.

In the academic context, I am keen to share my research findings to a broad audience via multiple avenues, and I have committed to making knowledge as accessible as possible. For instance, on my webpage I have made **publicly available my research papers, presentation slides, video recordings, lecture notes, useful resources on career developments** whenever appropriate.

At PSU, there had been a lack of TCS exposure as I mentioned earlier. My teaching efforts have hence been guided by three major objectives which lean more on the long-term payoff: **nurturing a TCS audience, developing meta skills via TCS, and training practical skills based on a solid foundation**. They also align with PSU's vision to promote **equity and socioeconomic mobility**.

I have taught 10 classes (merging two sections such as 4xx/5xx or 5xx/6xx) thus far. Besides teaching two required graduate level theory courses, I have offered regularly two theory courses close to my research area. One is on Cryptography which I have updated with exciting new developments such as post-quantum cryptography, and the other is ini-

[2]For instance, STOC, SODA, FOCS, and SICOMP are ranked the 1 - 4 TCS venues by Google Scholar.

[3]The exception is the branch of *logic and formal methods* contributed by faculty members researching on programming languages.

tiated by myself on quantum computing. These all contribute to improving and upgrading the theory curriculum at PSU. In particular, the traditional discrete math is no longer a sufficient foundation for emerging fields such as machine learning and big data analysis, and I started a new course as a means of modernizing it and better preparing students marching forward. I am proud to mention that I have devoted effort polishing my course materials and making them publicly available on my website whenever appropriate in order to increase access. Over the years, I have received warm praise from students, and got evaluations higher than the department average in all but one course. I also keep improving with constructive feedback of students as well as honing effective teaching skills from diverse channels.

Advising constitutes another fundamental component beyond the classroom setting. This is indispensable to establish a reputable research program in **an area that barely existed at PSU before**. I have four Ph.D. students, including one woman studen who has passed the candidacy exam (RPE) and another one who has successfully completed the dissertation proposal. I also have had the fortune to work with talented undergraduate and high school students, several of them have further pursed their career in industry (e.g. Google) or in top universities (e.g, Stanford).

I.3 Services and Outreach

I view returning to both the academic and local communities is not just necessary as a privilege and an invaluable opportunity to engage a broader group of people, especially those who are underrepresented and lacking of access. It is my vision via these efforts to enrich the field towards a more **diverse and equitable** future.

I have served in multiple capacities helping advance the research field, such as 18 conference program committees, journal reviewer (e.g., Journal of Cryptology, IEEE Transaction on Information Theory), NSF panelist and external reviewer under a variety of directorate and programs (CISE, MPS, ENG, SBIR/STTR), and book reviewers. At PSU, I have served at various levels, including two rounds of department faculty hiring committee and an advisory committee to the PSU President.

The power of knowledge is most meaningful when disseminated as wide as possible. Besides making my research results available (e.g., slides and video recordings of my presentations on my website), I have given invited tutorials that help attract a larger workforce in the field (e.g., at QCrypt 2019 and a summer school at IPAM, UCLA). At PSU, I provide research opportunities to students of a diverse group, sometimes via city-wide established programs (e.g., Saturday Academy), and also give public lectures to share with the general audience developments as well as **misinformation** on quantum computing and cybersecurity.

I.4 Addressing PSU's Guideline on Extraordinary Achievements

According to the PSU "POLICIES AND PROCEDURES FOR THE EVALUATION OF FACULTY FOR TENURE, PROMOTION, AND MERIT INCREASES (2018 June 25 revised)":

> "*Exceptions which result in the consideration for the promotion immediately upon eligibility should occur only on the basis of extraordinary achievement.*"

Here is a list achievements in response to this PSU guideline.

- My research has been funded by multiple external grants (total amount ~**$1.5M** as of 07/25/2022) where I am either the single PI or lead PI at PSU. According to the public data collected by the SPA at PSU on Sponsored Awards [4], which has not recorded my most recent NSF award ($300K), my sum of award amount is surpassed by a research faculty member, and is otherwise the **highest among tenure-track faculty of all ranks in the CS department** since 2016. It is **15% higher** than the next highest, and **102%** higher than another one whose early tenure case was just approved in 2022. The synthesized data is provided in the separate supplementary document.

- Among the grant awards, I received an **NSF Career Award** in 2020. I also received a **Faculty Innovation Award** by **Sony Corporation of America** in 2021, the **only one at PSU since its inception** in 2016.

- Two of my papers have been selected as **Long Plenary Talks** at the prestigious **Quantum Information Processing** conference (**QIP 2021 & 2015**). They are equivalence of **Best Paper awards** at typical computer science conferences.

- I was selected as a **Research Fellow at Simons Institute for the Theory of Computing**, a leading research institute globally located in UC Berkeley. I participated in the semester program, *Lattices: Algorithms, Complexity, and Cryptography*, in Spring 2018 as well as its subsequent summer cluster in 2022.

- I have been invited to talk at the **9th International Conference on Quantum Cryptography (QCrypt 2019)** and at the **2019 AMS Spring Joint Sectional Meeting**. In Summer 2022, I gave lectures at the **Graduate Summer School on Post-quantum and Quantum Cryptography** in the **Institute for Pure & Applied Mathematics (IPAM)** at UCLA.

[4] https://sites.google.com/pdx.edu/spa-data/home.

- I have served on program committees at flagship conferences (e.g., **QIP 2017** and **IACR Crypto 2021 & 2020**), panels at NSF, and to review submissions to top-tier journals (e.g., **Journal of Cryptology**). While it is my privileges as well as responsibilities to pay back the community via these services, they are also recognition of the research expertise in my fields.

- I have established an organic research group. Several students have presented and participated in prestigious international events, most of which have been **PSU's first occurrences**, which has generated representation of PSU among otherwise a majority of elite schools and increased the overall diversity of the community. For instance, one woman Ph.D. student, Chuhan Lu, has been selected to participate in the Women in TCS workshop, and a prestigious summer research program in the Simons Institute for the Theory of Computing at UC Berkeley (Figure 1).

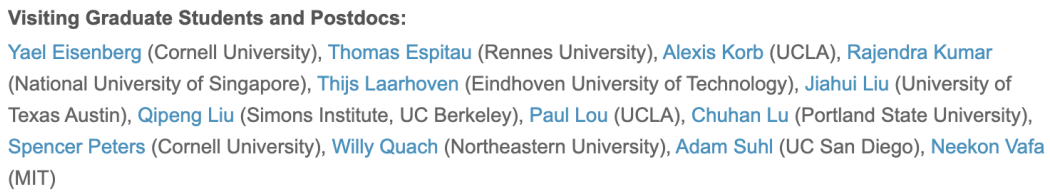
Visiting Graduate Students and Postdocs:
Yael Eisenberg (Cornell University), Thomas Espitau (Rennes University), Alexis Korb (UCLA), Rajendra Kumar (National University of Singapore), Thijs Laarhoven (Eindhoven University of Technology), Jiahui Liu (University of Texas Austin), Qipeng Liu (Simons Institute, UC Berkeley), Paul Lou (UCLA), Chuhan Lu (Portland State University), Spencer Peters (Cornell University), Willy Quach (Northeastern University), Adam Suhl (UC San Diego), Neekon Vafa (MIT)

Figure 1: Student list at the Simons Summer Cluster: Lattices and Beyond.

- Some former advisees have been accepted to prestigious schools. One undergraduate is now enrolled in a Master's program at **Stanford University**. Two high school students (one women) has been accepted to the Computer Science programs at **Stanford University** and **University of Pennsylvania** respectively.

- According to CS Rankings, an open-source and metric-based ranking system of computer science institutions, the collective CS program at PSU is ranked at **112**. Notably in the **Theory** category, contributed by myself alone, PSU's ranking sits at **59**th as of July 2022 (Figure 2).

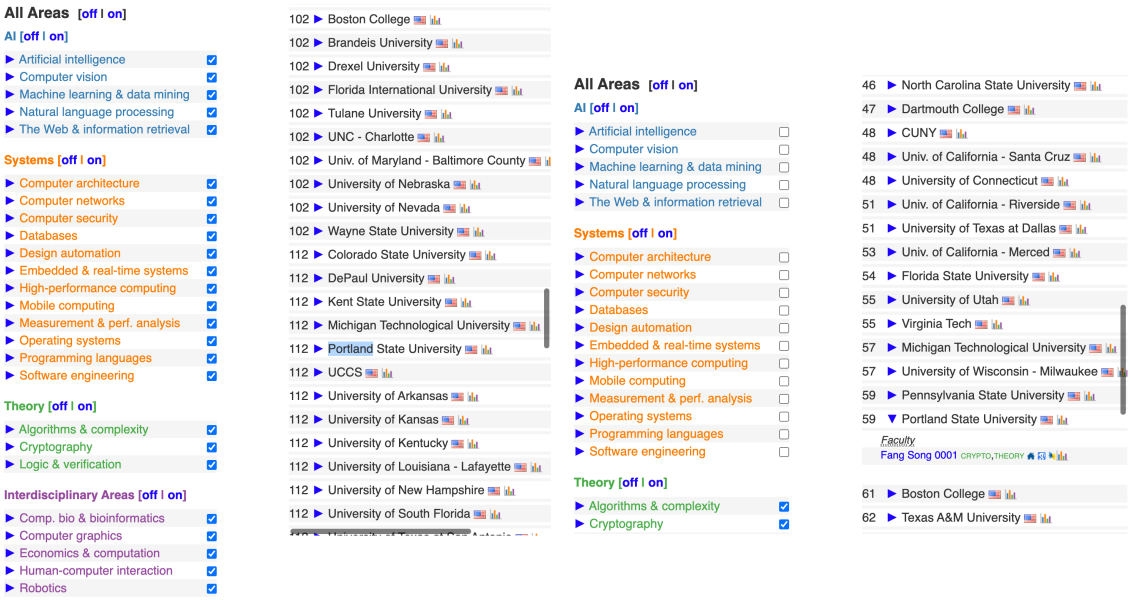

Figure 2: Left: Ranking of PSU CS program. Right: Ranking of PSU CS in Theory category.

II Research Achievements and Funded Research Program

In this section, I provide more details on three categories regarding my research: Grants Awards (Section II.1), Representative Research Results (Section II.2), and a plan for future research especially with existing Ph.D. students (Section II.3).

II.1 Grant Awards

By far, I have been awarded five external research grants in the total amount of ~**$1.5M** from both federal and industry sponsors. I am the **single PI** on two awards, including the prestigious **NSF Career Award**, and the **lead PI** at PSU on the remaining three collaborative projects with other institutes. Here is a list in reverse chronological order.

- 10/2022 – 09/30/2024. US National Science Foundation (NSF) Award #2224131, **$299,549**. *Collaborative Research: FET: Small: Minimum Quantum Circuit Size Problems, Variants, and Applications.* PI: Fang Song. Co-PI: Nai-Hui Chia, Rice University. Total award amount: $599,549.

- 03/2022 – 03/2023. Sony Corporation of America. *Sony Faculty Innovation Award: Post-Quantum Blockchains – Formal Analysis and Applications.* **$100,000**. PI: Fang Song. Co-PI (subawardee): Juan Garay, Texas A&M University.

- 04/2020 – 03/2025. US National Science Foundation (NSF) **CAREER** Award #1942706 (#2054758)[5], **$559,775**. *FET: CAREER: Algorithms, cryptography and complexity meet quantum reductions.*

- 10/2018 – 09/2022. US National Science Foundation (NSF) Award #1816869 (#2041841), **$283,852**. *AF: Small: Quantum Computational Pseudorandomness with Applications.* PI: Fang Song.

- 08/2018 – 07/2022. US National Science Foundation (NSF) Award #1764042 (#2042414), **$274,752**. *AF: Medium: Collaborative Research: Quantum-Secure Cryptography and Fine-Grained Quantum Query Complexity.* PI: Fang Song. Co-PIs: Gorjan Alagic, University of Maryland and Alexander Russell, University of Connecticut. Total award amount: $824,640.

  – 10/2021 – 07/2022, Research Experience for Undergraduate students (**REU**) supplement, $16,000.

II.2 Representative Research Results

Provable-secure post-quantum cryptography

My work [HSS15] gives the **first quantum-secure protocols** for zero-knowledge proof of knowledge systems and secure two-party computation, and proposes one of the first few **composable quantum security models**; my work [SY17] gives the first quantum security proofs of **domain-extension schemes for blockciphers such as NMAC and HMAC**, whereas similar constructions (e.g., CBC-MAC) are broken by quantum attacks; my work [HRS16; JST21] also proves **tight quantum security bounds for blockcipher key extension and hash functions** with novel techniques applicable to **quantum random oracle model and blockchain security**. This line has been funded by an **NSF (medium) grant** and a **SONY** award.

Quantum algorithms

In [EHKS14; BS16] we give efficient quantum algorithms for computing the **unit group and S-unit groups in number fields of arbitrary degree**, offering **exponential speedup** over best known classical algorithms. These algorithms solve a long-standing open question in the field and achieve exponential speedup over the best known classical algorithms. It also introduces the *continuous hidden subgroup problem* which unifies and expands the most successful framework for designing quantum algorithms with exponential speedup The quantum factoring algorithm is a notable example.

Aside from enriching the quantum algorithmic toolbox, these quantum algorithms can break several candidate post-quantum cryptosystems based on integer lattices and have

[5] Multiple award numbers exist due to transfers of grants.

enabled a series of cryptanalysis on lattice-based cryptography. This line constitutes an essential component for the project funded by **NSF Career Award**.

Quantum cryptography and complexity

In [BJSW20], we give the **first quantum zero-knowledge proof system for QMA**. This establishes the quantum analogue of the renowned classical result, which is considered revolutionary in modern cryptography. In [GLSV21] we construct **quantum protocols for secure computation based on a plain commitment scheme and hence one-way functions only**. This demonstrates the power of quantum protocols, because secure computation from one-way functions is deemed unlikely by classical constructions. In

My work [JLS18] proposes and constructs **computational quantum pseudorandom objects** (e.g., pseudorandom quantum states), which has proven fruitful in novel applications quantum cryptography as well as studying quantum complexity. For example, we show that quantum pseudorandom states give a generic construction of private-key quantum moneys, significantly simplifying prior work especially from a conceptual perspective. Some recent work makes a surprising observation that pseudorandom states suffice to realize commitment, which combined with my work [GLSV21] above, implies that secure computation is possible from pseudorandom states. Since pseudorandom states are potentially a weaker assumption than one-way functions, this further pushes the boundary of what quantum cryptography is capable of. The projects funded by **two NSF awards** including the **NSF Career award** have been or will continue exploring on these fronts.

Broader scientific impact

Beyond the immediate scientific values, these work accompanied with other efforts, have also aimed at another broader goal of **breaking the barrier of researchers from drastically different backgrounds to expand the research boundary**. This has been made particularly challenging but also rewarding for the interdisciplinary nature of the young and transformative research subject. I have collaborated with mathematicians and physicists in addition to computer scientists, and my coauthors span the globe (e.g., **US, Canada, South Korea, China, Australia, UK, Netherlands, Denmark, France**, etc.). Here is a glimpse of the impact in this context via a couple of examples.

- One recurring meta contribution of a host of my work is to pinpoint and stress basic but subtle issues concerning *modeling* and *reasoning about* quantum adversaries, which were often overlooked in the early days. They have become more and more a central topic as opposed to a decade ago at the early stage of my career, which is apparent in the **surge of submitted and accepted papers on quantum security analysis in prestigious venues, as well as researchers and students migrated to this field**.

- In another set of work (Cf. [GLSV21; JLS18]), I have brought the *computational* perspective into quantum cryptography, which had primarily targeted at information-theoretical secure constructions. The switch to computational security gives rise to new primitives (e.g., pseudorandom states) or unexpected advantages over classical cryptography. They have **inspired new lines of research**, ranging from *minimal* assumptions for cryptography to theories of black holes.

It is thrilling to witness the significant growth of the field over the past few years. I am proud to be one of many who have contributed to this (still ongoing) prosperity.

II.3 Future Research Plan

The growth of quantum computing and (post-)quantum cryptography communities is exciting. Looking ahead, I am enthusiastic to pursue many fundamental questions, which only become more pressing, and meanwhile expand the horizon of these subject that can bring about real-world impact. Existing and new Ph.D. students will play an integral role, contributing to a more diverse workforce.

One direction of effort, which is the central subject of my NSF Career Award, is to investigate quantum reductions in a systematic way. A representative questions asks: can *quantum reductions* help build a one-way function based on worst-case NP hardness? The investigation may transform the landscape of the equivalent relations of cryptographic primitives as well as complexity classes at large. My Ph.D. student Nikhil Pappu will be a main driver in this direction.

My prior work on quantum pseudorandom states opens up a world of opportunities. A general theory of quantum pseudorandomness and a will be invaluable. My Ph.D. student Chuhan Lu has been exploring *unconditional* constructions of quantum pseudorandom objects in various settings of bounded adversaries. They may shed light to the quantum counterpart of *derandomization* and generate new quantum algorithmic techniques.

Understanding the strengths and limitations of quantum computing is always intriguing. Can we demonstrate advantages on near-term quantum computers that can be verified? My Ph.D. student Mehil Agarwal is investing new domains to achieve this goal such as distributed quantum algorithm design, and a meaningful approach to the interplay of quantum computing and reinforcement learning.

Finally, my Ph.D. student Ben Hamlin, who also works full time at a local cryptographic engineering company Galois, has been investigating viable tools to reason about quantum programs, especially on the correctness and security of quantum key distribution protocols. This forms the theme of his thesis. The outcomes in this direction will be influential on the real-world deployment of new (quantum) cryptographic algorithms.

II.4 References

[BJSW20] Anne Broadbent, Zhengfeng Ji, Fang Song, and John Watrous. "Zero-Knowledge Proof Systems for QMA". In: *SIAM J. Comput.* 49.2 (2020), pp. 245–283. DOI: 10.1137/18M1193530.

[BS16] Jean-François Biasse and Fang Song. "Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields". In: *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016*. SIAM, 2016, pp. 893–902. DOI: 10.1137/1.9781611974331.ch64.

[EHKS14] Kirsten Eisenträger, Sean Hallgren, Alexei Y. Kitaev, and Fang Song. "A quantum algorithm for computing the unit group of an arbitrary degree number field". In: *Proceedings of the forty-sixth annual ACM Symposium on Theory of Computing, STOC 2014*. ACM, 2014, pp. 293–302. DOI: 10.1145/2591796.2591860.

[GLSV21] Alex B Grilo, Huijia Lin, Fang Song, and Vinod Vaikuntanathan. "Oblivious transfer is in miniqcrypt". In: *Advances in Cryptology – EUROCRYPT 2021*. Springer. 2021, pp. 531–561. DOI: 10.1007/978-3-030-77886-6_18.

[HRS16] Andreas Hülsing, Joost Rijneveld, and Fang Song. "Mitigating multi-target attacks in hash-based signatures". In: *19th IACR International Conference on Practice and Theory in Public-Key Cryptography – PKC 2016*. Springer, 2016, pp. 387–416. DOI: 10.1007/978-3-662-49384-7_15.

[HSS15] Sean Hallgren, Adam Smith, and Fang Song. "Classical cryptographic protocols in a quantum world". In: *International Journal of Quantum Information* 13.04 (2015), p. 1550028. DOI: 10.1142/S0219749915500288.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. "Pseudorandom Quantum States". In: *Advances in Cryptology – CRYPTO 2018*. Springer. 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5.

[JST21] Joseph Jaeger, Fang Song, and Stefano Tessaro. "Quantum key-length extension". In: *Theory of Cryptography Conference – TCC 2021*. Springer. 2021, pp. 209–239. DOI: 10.1007/978-3-030-90459-3_8.

[SY17] Fang Song and Aaram Yun. "Quantum Security of NMAC and Related Constructions - PRF Domain Extension Against Quantum attacks". In: *Advances in Cryptology - CRYPTO 2017*. Springer, 2017, pp. 283–309. DOI: 10.1007/978-3-319-63715-0_10.

III Effectiveness in Teaching and Advising

III.1 Teaching

Over my years at PSU, three major objectives have become more and more evident that form the guideline of my teaching in theoretical computer science (TCS).

1. nurturing a TCS audience, and challenge them to reimagine what is possible.
2. developing meta learning skills via TCS and building a firm foundation.
3. training practical skills and providing a head start for cutting edge technologies.

Despite the challenges of trailblazing a new ground, I have striven to achieve them by continuously improving course offerings and enhancing my teaching practices. So far I have offered **10 courses in six interweaving subject areas**. Each term, the Computer Science department conducts a teaching evaluation by soliciting students' feedback across 16 different questions. To get a bird-eye view, Figure 3 plots the average score (across all courses) on each of the questions expect for one non-applicable (Q14 "quality of lab") in comparison with the department average. **10 out of 15** of them are above the department average and **3 equal**. Question 10 assesses "Overall performance of instructor", which is illustrated in Figure 4. **8 out of 10** outperform the department average and **1 equal**.

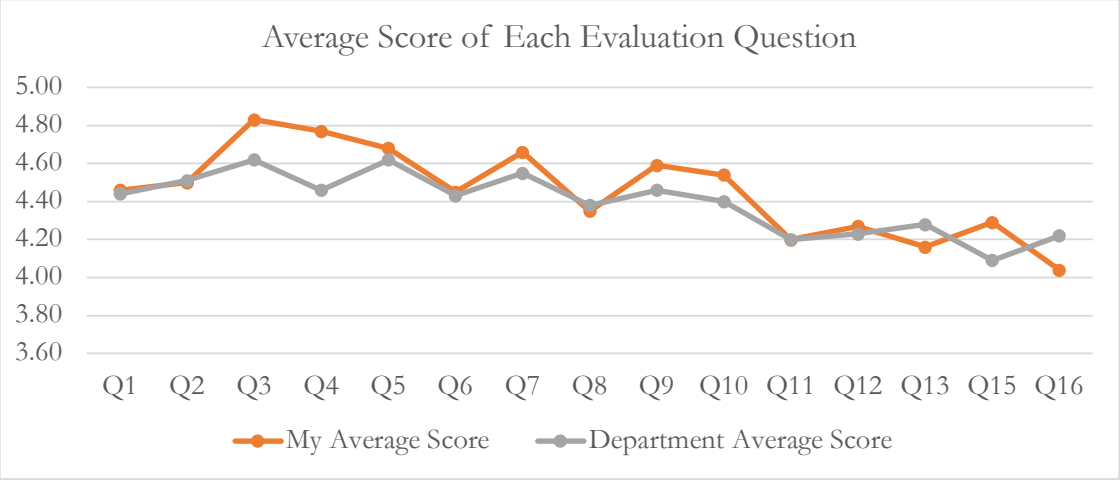

Figure 3: Scores on each of the questions on the teaching evaluation form. Question 14 about "quality of lab" is not included, because it is not applicable to my courses which do not contain lab assignments. My scores outperform or equal the department average in all questions except Q13 and Q16 regarding "homework and exams" (to be elaborated below).

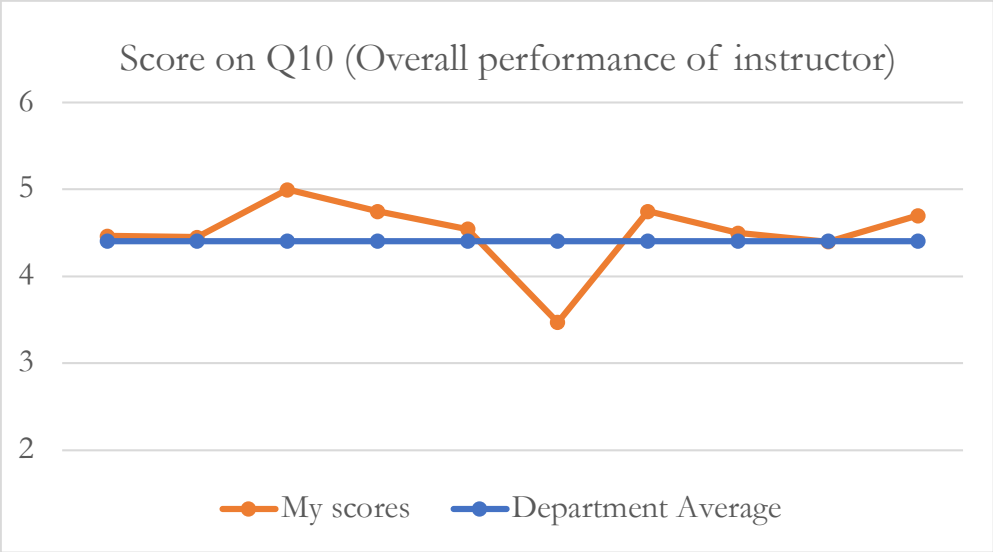

Figure 4: Scores on Question 10 "Overall performance of instructor" of my ten courses. All but one (W'21 "Algorithm designs" to be analyzed) are above or equal department average.

Over the years, I keep improving the course contents and my teaching strategies to make my classes **timely, inclusive, and suiting the students at PSU**. It is fulfilling to receive encouraging messages in my teaching evaluations such as

> *Professor Song was arguably one of the best and most understanding professors that I've had thus far at PSU. I was always able to reach him, and he made it a priority to reach out when it seemed like I was struggling.* – W'22 CS485/585 Crypto
>
> *The instructor is knowledgeable and has strong understanding of the material. Instructor is very generous with their time and is always willing to assist. One of the best educators on campus.* – F'21 CS581 ToC
>
> *An amazing course which helps with the basics of several other courses including cryptography/machine learning/ blockchain etc. I hope courses like these were offered more.* – F'21 CS410/510 FET
>
> *Fang Song is a wonderful instructor. He challenges his students but is very understanding and encouraging. He is always prepared for his lectures, and does a great job explaining challenging material.* – W'18 CS485/585 Crypto
>
> *I really enjoyed Professor Song, he's certainly my favorite professor at PSU I've had so far.* – S'17 CS410/510 Quantum

The feedback is encouraging and also reveals valuable insights on what can be improved upon, and I give a more comprehensive account below.

CS 485/585: intro to cryptography (Crypto) and CS 410/510: intro to quantum computing (Quantum). The latter is a new course I created, and the former had been in hiatus and is now considerably redesigned and updated. These two are the first courses I taught at PSU, and since then they form the primary window to advanced theory courses here at PSU. They help develop foundational as well as critical job skills (e.g., in **Cybersecurity**), and keep up with cutting-edge research and technology. In addition, the topics offer a bridge to attract students to my research area. In fact, two of my Ph.D. students were identified via these two courses.

CS 584/684: algorithm designs (Alg). This course covers core techniques for designing and analyzing computer algorithms. Many topics are considered standard including divide-and-conquer, dynamic programming, greedy algorithms, graph algorithms, and theory of NP-Completeness. On top of them, I also try to bring in **modern developments**, e.g., giving a flavor to big-data algorithms and quantum algorithms.

This course was offered in Winter 2021, on which I received the least favorable evaluation in all my courses (the only one below average on Q10: "overall performance of instructor" Figure 4). But it was also decisive for me to reflect and reshape my vision and practices on teaching, which deserves a dedicated discussion revolving three critical observations.

1. *How to take advantage of the benefits of online technology and mitigate the drawbacks of purely remote teaching?* The importance of **live interaction**, as in a white board lecture, is well accepted especially for theory courses (including math). This course was fully remote, and the fatigue (in the COVID-19 pandemic) was more than obvious. Through this experience, it reconfirms that I should provide some in-person component whenever possible. However, when that is difficulty, "baby" steps can be taken to maintain effectiveness in a remote setting, such as breaking online sessions into short ones, host informal online meetings and gatherings, and in the live sessions take turns to ask or answer questions to engage maximum participation.

2. *How does the student demography evolve and how to adapt with it?* This was my first required (graduate-level) course at PSU[6] This is in stark contrast to the Crypto and Quantum courses, where the enrolled students are generally speaking more "pro-theory" by self filtering. I did not appreciate this enough in the beginning, and this experience gave an opportunity to get a more accurate picture what the strengths and weaknesses the CS students here possess. This helped me **reassess the pace and growth curve**, which proves effective in the courses that come after.

   Besides a more representative set, another characteristic of the CS students also emerged. **They are becoming more and more diverse, including a remarkable**

[6] I did teach the same course before at Texas A&M U during my leave from PSU. This will be further discussed in the next item.

number of students switching their careers from other disciples. This is great news for the growth of CS, but the challenges are equally great. I first noticed a bit of this change in my Spring'21 Quantum course, and it was fully revealing in this class. I learned that about half of the students came from the post-bac track, where their prior Bachelor degrees were in chemistry, biology, psychology, etc. To bring success to such a diverse group, the most valuable lesson to me is to **build a common vocabulary, and use examples from multiple angles to explain the same thing**. This is also a driving factor towards a **more inclusive classroom**.

3. How to build a "**fear-no-challenge**" mindset and enable students' full potential? This experience also opened up some deeper thoughts and issues, which are not as concrete as above and consequently more challenging to address. This comes from a comparison between the offerings of essentially the same course at TAMU (Fall'19) and at PSU (Winter'21). PSU students are more likely to express that the contents are challenging, and **they do NOT believe that they are up for it**; whereas TAMU students are more willing to acknowledge the challenges and express that **I think I can figure it out**.

   This should not be simply attributed to how well-prepared they were before entering the class. More than half of the TAMU class are actually students majoring in Electrical Engineering, who had not taken a proper undergraduate algorithms class. In addition, one major improvement I made based on the feedback from the Fall'19 offering was to make the contents more accessible in the first few weeks for those who may not have sufficient prior exposure to algorithms.

   I view this as an **inadequacy on us, the faculty**. I started to reflect **whether we have helped our students achieve their true potentials**. I give a visual illustration in Figure 6. This has driven me to a new effort, which I discuss in the course "foundations of emerging technology" (FET) shortly.

CS 681: theory of computing (ToC). Similar to CS 584/684 (Alg), this is another core theory course required for most graduate students. It investigates foundational questions in computing as to what problems can be solved (Computability), and how "efficient" can we solve them (Complexity)? This course, assuming a prior introductory exposure to the theory of computation, focuses on computational complexity, including time, space, randomness complexity. I also integrate selected advanced topics such as interactive proof systems and quantum computing towards the end. One important guideline I have attempted is a **balance between useful technical skills and appreciation of rigor and elegance in TCS**.

The formal definitions and abstract reasoning often causes difficulties for students to grasp. I am glad that what I learned from the Alg experience helped make this course successful and raise the evaluation above department average. The "attend-anywhere"

teaching mode rolled out in Fall 2021 was a big advantage, where in-person attendence became possible, and in fact it was the favorable mode in this class. This offered the opportunity for me to resolve many "mini"-obstacles in their learning path instantly. I also practiced the strategies discussed above, which were welcomed by the class.

CS 410/510: foundations of emerging technology (FET). Relatively recent I have invested considerably on this new course. This is in response to a pressing challenge that the conventional **discrete math** is falling short. This course intends to providing an intensive practice on **combinatorics, probability theory, and linear algebra, driven by real-world computer-science applications**. It equips students with critical skills to succeed in advanced courses on subjects including **big data, (deep) machine learning, natural language processing, computer graphics/vision, qcryptography, and quantum computing**, where exciting research efforts and massive opportunities on the job market lie in.

Besides the practical value, this course is a starting point to address the deeper concern (item 3 under CS 584/684 Alg). I intended to come to an ealry stage to make changes. This is first to showcase some main characteristics, e.g., how to define a problem, how to approach it, and how to turn it into a formal solution or proof. This sets the norm of theory courses and equivally important I also intend to demonstrate why they need to be that way. Based on that, the more ambitious goal is to **build confidence and the courage to ake big challenges**, and to become more and more accustomed with achieving long-term payoff even if that means short-term sacrifices. Ultimately, I hope the experience should uplift students to see more clear **what their strong suits are, and be more determined and equipped to achieve what they might not have thought possible**.

CS 510/610: probabilistic graphical models. This is an advanced course to complement the popular machine learning curriculum available at PSU with a taste of **theoretical ingredient**. This was offered in the same term as CS 584/684, and received a high evaluation score (4.75 vs department average at 4.4). It is my hope to be able to offer advanced theory courses more often, once the more pressing issues discussed above get considerably improved upon.

Assessing the objectives

All the efforts contribute to the three goals set above. In terms of nurturing a theory audience, while concrete data is not easily available, there are positive indicators. There is a growth of interests in theory courses from the student body, and this partially influenced on the strategical plan of the CS department. For instance, theory was a priority area in the past two cycles of hiring, and we successfully hired two new faculty members in theory, one in complexity and the other in theory in explainable machine learning.

As to developing meta learning skills via TCS, self learning capability comes in the front row. My lectures would often be preceded by warm-up reading materials, the lectures are guided with questions, and post-lecture reading is assigned to reinforce and supplement the key points. My homework problems are usually designed for students to revisit the main topics to fully appreciate how each one works and their interconnections, and they need to put together a set of concepts or techniques to solve new problems. These problems share the same principle of examples in class, but they may not immediately resemble them (as opposed to changing a few numbers or variables in discussed examples). One skill I intend to practice, is **to distill the essence of the problems and realize the central concepts behind them**. This is to mimic **how problems may be presented in the real world**.

The reaction has been mixed, as shown in the two problems below department average evaluations (Q 13 and Q16) in Figure 3. I have generated a more detailed plot in Figure 5.

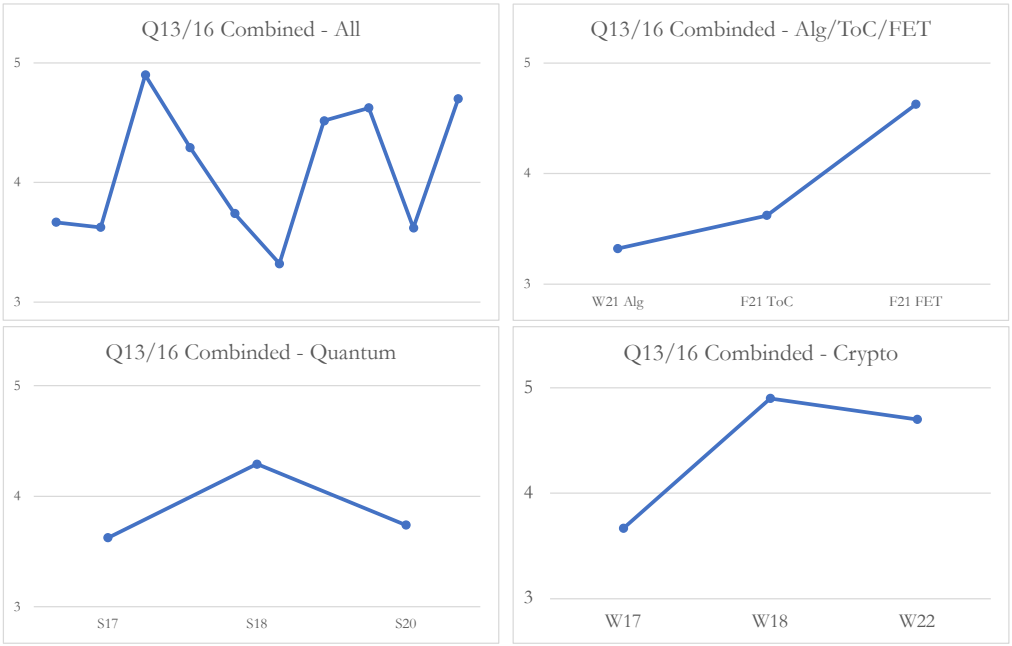

Figure 5: Top left: scores on Q13/16 of each course. Top right: trend on Alg/Toc/FET. Bottom left: trend on the Quantum course. Bottom right: trend on the Crypto course.

The summary shows fluctuation across time and subjects, and the low tide coincides with the pandemic and the deep reflection on CS 584/584 (Alg). Although I still believe in the value of my general design principle, practically I implemented changes that help **build a more smooth ramp between the content in the lectures and the homework problems**. Most of the difficulty in fact owes to jumping **out of the comfort zone**, which is undoubtedly challenging and uncomfortable, and I should and can provide all help to make this process more manageable. The upward slope is encouraging as shown in all courses in recent years as well as in individual courses.

Another meta skill is **critical thinking**. **Misinformation** is causing harms for the whole society, and the subjects I teach are not immune to it. In the most recent Quantum course, I added a new module for students to debate on public coverage of advances in quantum computing. They can help correct or debunk false statements, and also learn how to explain complex concepts to a general audience when the media did a good job. In my recent Crypto course, we also spent a couple of lectures discussing the **moral responsibilities** of cryptographers, which can help build a healthier community.

Training practical skills has been conducted via a variety of channels. Several of my courses involve a term-long course project, during which students practice **team-working, oral presentation, and written skills**. The Algorithm course helps prepare for tech interviews at major IT companies such as Google; the FET class prepares students for a wide spectrum of specializations (e.g., machine learning and big data analysis), the Crypto course helps in the cybersecurity market, and the Quantum course can give a head start in the cutting edge technologies where a job market is witnessing expansion. On a few other occasions, previous students told me that, **despite the initial struggle in class, it becomes evident how influential what they learned in my (cryptography) class becomes in advancing their career a few years later, especially the formal framework to approach challenging problems in new domains**.

III.2 Advising

Advising constitutes another fundamental component beyond the classroom setting. This is indispensable to establish a reputable research program in **an area that barely existed at PSU before**. I leave the students the **maximum degree of freedom and flexibility**, because I believe that is the basis for them to **explore, discover, and eventually grow to independent researchers with good taste**. I do my best to create an open and welcoming environment, so that they can turn to each other (myself included) at any time for advice.

- I have had the fortune to work closely with a group of research students including 4 Ph.D. students (one woman), 3 undergraduate students (one woman), and 2 high school students (one woman). I have also served on two Ph.D. dissertation committee (including one woman student) and numerous Research Proficiency Exam (RPE) committees.

- Many students have marked important milestones and achievements. Two of my Ph.D. students are in their first year, **one has completed thesis proposal** and one has **completed the RPE**. One undergraduate is now a **Master's student at Stanford** and another is now **working at Google**. Both of the high school students have been accepted into **prestigious computer science programs**, one at **Stanford** and the other at **University of Pennsylvania**.

- Several students have appeared in top-tier venues, raising the publicity of PSU and increasing the diversity of the TCS community. For example, one Ph.D. student (Ben Hamlin) and one undergraduate student (Marko Balogh) have presented at security conferences such as **CHES** and **Post-quantum Cryptography (PQCrypto)**. Another Ph.D. student (Chuhan Lu) has presented at **Asia Quantum Information Science (AQIS)**. Chuhan has also been selected to participate in the **Women in TCS workshop**, and a prestigious summer research program in the **Simons Institute for the Theory of Computing** at UC Berkeley.

Besides achieving academic excellence, equally important is to understand the **social responsibility** and act to improve. In both individual and group conversations, we discuss issues regarding **social justice, discrimination, equity, and representation** openly on a regular basis. This will continue to be an critical effort in shaping a more inclusive culture in academia and the whole society.

IV Outreach and DEI Efforts

It is an honor to get invited to speak at influential venues, and I particularly value those that expand my common audience. For instance I gave an **Invited Tutorial at the 9th International Conference on Quantum Cryptography (QCrypt 2019)** where quantum experimentalists constituted half of the audience. I was also invited to talk about quantum cryptography to a group of number theorists at the **2019 AMS Spring Joint Sectional Meeting**. I have been invited to give lectures at the **Graduate Summer School on Post-quantum and Quantum Cryptography** in the **Institute for Pure & Applied Mathematics (IPAM)** at UCLA, which is a great opportunity to inspire a future workforce in quantum information and cryptography.

I have also actively engaged local communities to share the knowledge and research opportunities.

- In Winter 2017, I organized a mini-symposium **Quantum Day** at the University Place Hotel with invited talks by international scholars (US, Australia, Netherlands, Taiwan). There were more than 60 participants from local schools and industry (e.g., Intel and Galois).

- In Summer 2017, I mentored an undergraduate student Teógenes Moura from **Brazil** participating the **Google Summer of Code** program. Teógenes successfully developed a prototype voting system based on a blockchain which achieves security features both in privacy and verifiability.

- In Summer 2018, I offered research experiences on quantum computing to two high school students via the **Apprenticeships in Science and Engineering (ASE) program** by the Portland Saturday Academy. **Sydney Von Arx**, then at Lake Oswego High School, was later accepted to the Computer Science program at **Stanford University**; and Marshal Xu, then at Lincoln High School, got in the Computer Science program at **University of Pennsylvania**.

- Quantum computing has got more press in recent years, and misinformation also exploded. I seize opportunities to explain and clarify topics in my expertise to the general public. In July 2020, I gave an online talk in the series of **Portland Quantum Computing Meetup**, where I introduced the impact of quantum computing in cybersecurity. As another example, I gave an invited lecture explaining basic principles in cryptocurrencies and blockchain technology, and clearing up some mysteries about how quantum computing might influence them.

V Governance and Professional Services

At PSU. Since my start at PSU, I have served on administrative committees at various levels in addition to these directly relevant to research and mentoring.

- Since my start at PSU, I have been on the **Graduate Admission Committee** for three academic years. One particular effort I contributed to is to update the admission criteria so to increase the diversity of graduate students.

- In the past two academic years (2020 – 2021, 2021 – 2022), I served on the **CS department faculty hiring committee**. It has been both a demanding and also rewarding experience. We have managed to hire 6 new colleagues in total. Particularly in this year, I have played a vital role in setting **Theory** (algorithms, complexity, quantum computing, etc.) as a top priority area to hire, and we have successfully recruited two talented theory faculty members. This hiring also reflects part of a comprehensive strategic vision of the department in the years to come. One position of this year's hiring was also part of a cluster hire in **Computational Science For A Sustainable Future** between MCECS (Computer Science) and College of Liberal Arts (Math and Statistics).

- During Winter and Spring in 2018, I was a member on the **President Academic Advisory Council**, which is composed of both tenure-track and non-tenure track faculty from across the university. I had represented the Computer Science department to relay voices to the President on important issues such as online courses, teaching evaluation and the promotion process.

In academia.

- I have served on more than 15 program committees on top-tier conferences, such as the prestigious **Quantum Information Processing** conference (QIP 2017) and two flagship conferences by the International Association for Cryptologic Research (IACR) – the **International Cryptology Conference** (Crypto 2021 & 2020), and **International Conference on the Theory and Application of Cryptology and Information Security** (Asiacrypt 2022 & 2017). In addition, I have also been invited to review dozens of manuscripts submitted to highly reputable journals such as **Journal of Cryptology** and **IEEE Transaction on Information Theory**.

- I have served as a panelist on multiple NSF panels. In addition, I also helped review several proposals as an ad hoc reviewer. What is most rewarding is that these tasks came from a number of directorates and programs at NSF – **CISE, MPS, SBIR/STTR**.

- I have helped review textbook proposals by academic publishers (e.g., Princeton University Press). This was an unfamiliar task to me at first, but I have become appreciative of its value as to promote timely and high-quality scholarly work that serve a larger audience than what research papers do, while correct and improve under-prepared projects.

- In 2022, I chaired the committee for Student Travel Award at the flagship conference Quantum Information Processing (QIP) held in Pasadena, CA. We managed to offer travel funds to more than forty students both in the US and from abroad. This helped make it possible to attend the conference, which was the first in-person conference for many of them.

The more I devote into outreach and services, the more I realize the deeper and grander needs for changes and improvement. For instance, when forming the student travel award committee at QIP, I experienced first-hand the lacking of representation of researchers from minority groups. And often times when I identify (a scarce number of) candidates that I believe would increase diversity, only would I find that they are already overwhelmed with numerous services. This is not acceptable, and I am committed to continue making a difference with my efforts, no matter how small they may appear at first.

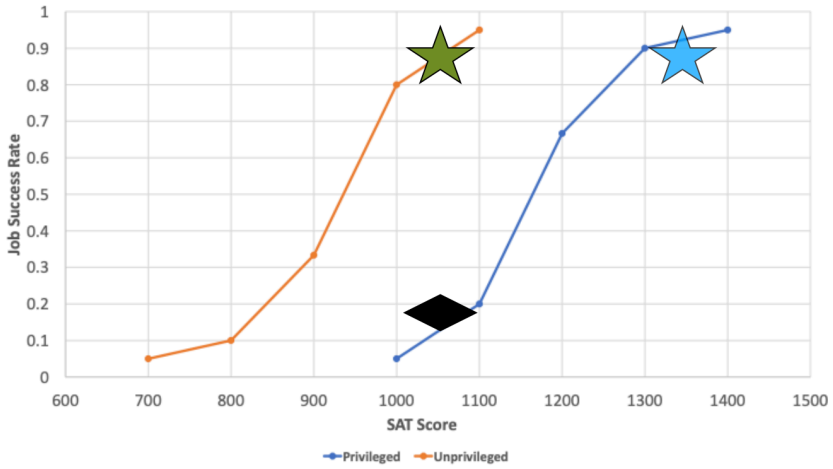

Figure 6: A mindset shift in educational goals: can we help lift students from "I did what I didn't think I can" to "I can see/achieve my real full potential"? We at PSU have excelled at providing high education to **high potential students in unprivileged groups** (marked by green star), and help them achieve what they would often not think possible. This is already remarkable. But we should not be contend with it and stop there, because these students could be as competitive as **high-potential privileged students** (marked by blue star) rather than what **average privileged students** can achieve (marked by black diamond). Data is based on a study in arXiv:2001.09784. A slide was prepared in response to the "REIMAGINE PSU" initiative in 2021, and is available at https://fangsong.info/files/talks/2021_repsu.pdf.