Establishing a Cryptography Research Lab in 2019

Brent Waters

Abstract

On July 1, 2019, NTT launched NTT Research, Inc. in Silicon Valley as part of a larger reorganization. NTT Research consists of three research labs in the areas of cryptography, quantum computing, and healthcare, where each lab is directed by a prominent researcher from Japan. I am very excited to be part of the cryptography research group. I was involved with kicking off this endeavor by recruiting several researchers. In this article, I share my thoughts on establishing a successful corporate research lab.

Keywords: reorganization, cryptography, collaboration

1. Introduction

While there is much reason for enthusiasm in starting a new research lab, it is also important to reflect on the challenges facing this endeavor. One sobering thought is that over the course of my career I have seen several vibrant cryptography research groups come and go. When I use the term "research," I mean basic research that can be published at top conferences or in journals. While some amount of change and turnover is inevitable; however, there does seem to be less permanence to corporate research labs in computer science than in university departments. One looming issue facing almost all corporate labs in basic research is the eventual pressure to produce and articulate their business value to the company. This comes with challenges. First, most good research in many fields has an impact along a longer time line, which can be at times difficult to align with the near-term goals of a company. Second, good research from any group will be publicly disseminated, will build upon research from people outside the organization, and will be used by other groups and organizations. This typically means that the returns of creating a strong research group are implicitly shared with the broader community. One path, of course, is to curtail outside publication and collaboration, but I have not seen this approach produce top quality research—at least not in my time in my field. It should be noted that by having a strong research group, a company is conversely positioned to build upon and capitalize on the innovations of outside researchers as well.

Despite these challenges, the opportunity of starting and joining a new lab can far outweigh the risks for both researchers and the organization if done the right way. Below I impart a few thoughts on how to establish a successful research lab. I emphasize that the perspective I share below is centered on creating a research lab with the primary goal of producing top-tier publications in computer science—that is, producing the *best* research—and some of these ideas might apply differently to different goals.

Be elite.

"Do it right or don't do it." It is fairly easy to start a mediocre research lab, but starting a great one is where the challenge and excitement lays.

This starts with hiring the right people. The difference between a top-tier researcher and an average hire is quite significant. It therefore makes sense to strategize on how to attract the best people. A good starting point is salary and compensation. Given the large value difference in acquiring top people, one has to do what it takes to get the right person. One comparison point is professional sports in which a team may be eager to trade several athletes to acquire a superstar. The resources for compensation will be finite. I suggest they be focused on quality over quantity.

Another way to recruit a regular stream of top talent is to begin by recruiting top talent. Top researchers will want to collaborate with each other (On the other side of the coin, not making the right hires can negatively affect future recruiting). One thing a corporate lab can do is to create an environment in which several people can work together. This also works well with recruiting interns and postdocs. If you can get a critical mass of senior researchers, the lab will become a destination that graduate students will flock to over the summer.

Let researchers do what they are good at.

If fortunate enough to hire the right people, let them do what they are best at. Top researchers have a special ability and will want to focus on basic research. The best way to manage them is really just to give them space to "do their thing." Of course, it is reasonable to have occasional requirements such as asking researchers to explain their ideas to a developer who is putting those ideas into practice. I suspect most researchers will be happy to meet such requirements. However, if the group's vision of what a researcher should be doing is much different than letting them stick to what they are good at, then I would argue that the vision wasn't compatible with basic research to begin with.

It is also important to ensure researchers have the right amount of time to do their research. Minimizing the amount of additional meetings or other activities with overhead is important. Gaining external exposure of the lab's achievements is important, although much of this will happen organically as researchers travel to present papers at conferences and invited talks. Generally, researchers will already have a good feel of where their time is best spent.

Know the competition and what is needed to compete.

Let's say we subscribe to the ideology of obtaining very strong researchers. We next need to look at the competition. Let's focus on faculty positions at research universities. As a faculty member, a researcher will have access to eager graduate students, have the opportunity to achieve lifetime job security through tenure, have a large amount of independence in pursuing his/her interests, be able to conduct research on a college campus with a nice office, and gain the prestige of being recognized as a professor.

It is important to keep this in mind when recruiting people who already have academic jobs or have just completed their Ph.D. studies and are considering university positions. There are certain things, of course, that just cannot be matched. If someone wishes to teach, be on a university campus, and be called professor, then a university job is for them. However, there are other aspects where a corporate lab can meet or exceed an academic position. Let's start with office space. Many company working environments are *open offices* where engineers work either at desks or cubicles. After speaking to many potential recruits for NTT Research, Inc. (as well as consulting my own personal feelings), I can say with great confidence that such a setup will not be popular with researchers. Researchers desire private, individual offices where they can concentrate on their ideas. This is what any computer science faculty member will be given, and if the same is not offered, it will be considered a significant minus to anyone deciding between offers. There is also a certain prestige associated with offices (and a corresponding lack of prestige associated with not having them). If you want to make a recruit feel special, this is critical.

There are other points at which a corporate lab can exceed an academic offer.

- Compensation: At universities, there are political and other pressures to keep salaries relatively uniform and lower. A corporate lab should ideally have the ability to pay more as well as have more flexibility in achieving its hiring goals.
- Number of colleagues in an area: At NTT Research we have the opportunity to hire several cryptography researchers at the same location. In a well-balanced computer science department, the hiring will be more spread out among different areas. This provides a special opportunity to researchers in a lab.
- Less overhead: At a corporate research lab, one does not have to teach, serve on committees, or search for funding. The freedom to devote more time to pure research can be a huge draw. It is important not to lessen this advantage by having too many tasks, meetings, etc.

Make collaboration and publication easy.

A surefire way to stymie the growth of an elite research lab is to put up excessive barriers to publication or collaboration. Researchers must be able to enter into collaborations with others outside the company without any barriers. Also, there should be few to no barriers to publishing or posting a research paper online. Otherwise, the best people will simply find someplace else to work. Of course, a company

should have the ability to patent research that comes out of the lab, but this should be done in a way with minimal impediment to the core research goals.

Everything above should be doable if the right resources and management style are in place. If there is a single takeaway, I would say that basic research is simply different from product development, and academically focused researchers are different from engineers. To establish a successful research lab, a company needs to develop a distinct approach.

2. Concluding remarks

I'd like to conclude by describing the many benefits of having a corporate lab that produces groundbreaking research. An obvious one is that researchers who create new ideas can help build up a company's intellectual property portfolio. In addition, having in-house expertise can be very useful for evaluating emerging technologies. However, the most important role by far is that a corporate research lab is the source for transformative and novel ideas. Embracing change and new ideas is necessary for companies to stay at the top. At NTT Research's kick-off event, I was interested to learn that less than 20% of NTT's current revenue comes from voice (including voice from mobile)—this is from a company with the words "telephone" and "telegraph" in its name. To stay relevant, a company will have to evolve over time. Big ideas in research can come from unplanned and unexpected places. For instance, one of the research contributions I am best known for is attribute-based encryption—a way of encrypting to a policy as opposed to targeting specific individuals. However, this concept sprouted out of a work (with Amit Sahai) where we were initially investigating how to encrypt biometric identities. It is precisely this ability to tap into fundamentally new ideas and technologies that make running a successful research lab a pillar to a company's future growth. I am very encouraged by the solid launch of NTT Research and excited to see where things go from here.

Brent Waters
Distinguished Scientist, Cryptography & Information Security Laboratories, NTT Research, Inc.

Dr. Brent Waters received his Ph.D. in computer science from Princeton University, NJ, USA, in 2004. From 2004–2005, he was a post-doctoral researcher at Stanford University, CA, USA, then worked at SRI International as a computer scientist. In 2008 he joined the faculty at The University of Texas at Austin. In 2019 he joined NTT Research as a distinguished scientist. Dr. Waters' research interests are in the areas of cryptography computer security. His work has focused on identity-based cryptography, functional encryption, and code obfuscation. He is noted as a founder of functional encryption and attribute-based encryption.

Dr. Waters is a recipient of the National Science Foundation CAREER award, the Presidential Early Career Award for Scientists and Engineers (PECASE), and the 2015 ACM (Association for Computing Machinery) Grace Murray Hopper award. He has been a Microsoft Faculty Fellow, Sloan Research Fellow, a Packard Science and Engineering Fellow, and a Simons Investigator.