

Dear Hiring Manager,

I am a newly minted Ph.D. graduate in computational number theory under William Stein. I am very interested in joining Galois – particularly the cryptography team.

I should begin by stating that I do not have a research-level understanding of cryptography but I do have a research-level understanding of some closely-related math topics. My thesis centered around creating and implemented algorithms for computing with modular abelian varieties which are higher-dimensional versions of elliptic curves. Consequently, I have a strong background in computing with elliptic curves.

Most of my cryptography knowledge came from when I was an undergraduate at UC Santa Barbara. I took the usual introduction to cryptography class as well as a special topics class on random number generators. But perhaps the most educational experience was attending CRYPTO 2013. I found some talks and the rump session very interesting which solidified my enthusiasm for cryptography.

Like Galois, I value contributing to open-source software. I am a regular user and developer for the Sagemath project. Sagemath is an open-source Python package, similar to numpy, but more suitable for research-level number theory computations. My contributions began with a Google Summer of Code project with Sagemath where I improved the functionality of the modular abelian variety component. The work here eventually morphed into my Ph.D. thesis. Since then I have authored 25 tickets (19 accepted) and have reviewed 10 tickets so far. My work for Sagemath has been invaluable towards my software training.

I understand that Galois uses Haskell which I find enticing. I have learned Haskell in the past as part of a computer theorem proving class but have not used it much since. If given the opportunity to join Haskell, I am more than willing to pick it up again.

I understand that my background is not the perfect fit for this position. But I hope that my thesis work and my Sagemath contributions demonstrates that I can still make valuable contributions to the team.

- Kevin Lui