UNIVERSITY OF SOUTH CAROLINA

Frank Thorne
Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, SC 29208
thorne@math.sc.edu

Friday, July 19, 2013

Kim Sacra
National Security Agency
9800 Savage Road, Suite 6844
Fort Meade, MD 20755-6844
ATTN: Mathematics Hiring Manager
kcsacra@nsa.gov

Dear Ms. Sacra (or whomever else it may concern),

I am pleased to strongly recommend **Richard Oh** for a permanent position with the National Security Agency. Richard is currently working with you on a summer internship, so you understand why I am recommending him highly. Here I describe what I've observed as his Ph.D. advisor at the University of South Carolina.

First impressions. I began at USC in Fall 2011, and I met Richard in his second year, when he took my graduate course on analytic number theory. Richard, along with one other student who was approximately his equal, was the strongest out of a class of nine.

My course was rather ambitious. I decided to use Davenport's book *Analytic Number Theory*, as opposed to gentler introductions to the subject which had been used at USC in the past. My course covered a variety of elementary and complex analytic topics in the subject (indeed, more than at least one of my colleagues seemed to think wise), and the lectures and the homeworks made full use of technical tools such as Fourier transforms and complex contour integration. I assigned weekly problem sets as well as a term project.

Richard's overall homework score was either the highest or the second highest in the class. (I regret that I have misplaced my grade sheet and don't remember more precisely.) He consistently solved difficult optional problems that were avoided by many others, and he wrote up his solutions impeccably well: indeed, I would rate his ability to write mathematics clearly at least as high as the average math professor. His term project was also, in my opinion, the best in the class. He chose to tackle the research literature and present a paper of Dorian Goldfeld, giving a simple proof that $L(1, \chi_d) \gg d^{-\epsilon}$. Goldfeld's writeup was quite short, and Richard thoroughly mastered his paper and wrote a much longer paper explaining all of the additional details in the proof. Richard also gave an excellent lecture on this paper; it was clear that he understood both the details and the big picture.

I was delighted that Richard decided to write his thesis with me. He has demonstrated not only perseverence and excellent mathematical ability, but also independence. After my analytic number theory course, I suggested a research problem related to his term project, but he has decided that he would prefer to seek out problems related to cryptography.

UNIVERSITY OF SOUTH CAROLINA

Frank Thorne
Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, SC 29208
thorne@math.sc.edu

Friday, July 19, 2013

Richard's research interests. Richard has sought out and mastered a variety of demanding reading on analytic number theory and its relation to cryptography. After he decided to work on cryptography, Richard showed me Shparlinski's book *Cryptographic Applications of Analytic Number Theory*, which he apparently found on his own, as well as a list of open problems in the subject. After skimming the book, I suggested that he learn more about exponential sums, which are a mainstay of analytic number theory and which feature prominently in the book. I asked him to read the treatment of exponential sums in Iwaniec and Kowalski's *Analytic Number Theory*, a beautiful book which nevertheless caused me severe headaches when I was a graduate student. He came back with a long list of good questions.

Based on his independent reading, he chose to investigate a cryptographic hash algorithm known as the Very Smooth Hash (VSH). This algorithm was introduced by Contini, Lenstra, and Steinfeld in 2005, and is of interest because it runs quickly and also admits proofs of security (which, to my knowledge, popular algorithms such as MD5 and SHA1 do not). Richard has been investigating the problem of proving explicit lower bounds for the security of VSH.

Such bounds translate into analytic number theory problems, and Richard has been carefully studying multiple papers which discuss VSH and some of the underlying number theory. He has paid particular attention to a paper of Pappalardi, studying the order of finitely generated subgroups of $\mathbb{Q}^\times \pmod p$, to the point of also studying one of the papers which underlie it, with an eye towards improving Pappalardi's results, and potentially leading to a lower bound on the security of VSH.

I cannot tell you whether this line of proposed research will succeed, but I certainly find it promising. In any case I have been impressed by his investigations so far – by his competence, by his thoroughness, and by his enthusiasm.

Computational ability. Richard's work has involved numerical experiments, and he has used SAGE, C++ (with libraries to handle arbitrary precision arithmetic), and shell scripting to generate data related to exponential sums occurring in the VSH algorithm, and gnuplot to graph it. Although I did not look at his code, but I did look at the graphs of his data – he found fascinating behavior in exponential sums related to VSH, demonstrating that (completely on his own) he has found a deeply interesting area of number theory to investigate.

Undergraduate research. Richard completed an undergraduate research project at Emory, which quite impressed me. He read a modern research paper in cryptography (which was apparently confusingly written) and wrote a much longer version of the same paper, explaining the method in fuller detail and also implementing the algorithm in the SAGE programming language.

UNIVERSITY OF SOUTH CAROLINA

Frank Thorne
Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, SC 29208
thorne@math.sc.edu

Friday, July 19, 2013

Oversimplifying somewhat, his project is as follows. (If I say anything inaccurate, the error is mine and not Richard's; he is much more knowledgeable about cryptography than I am.) The RSA cryptosystem relies on a private key and a public key, which can (essentially) be represented as large integers. When a user creates a keypair, he (or she) generates two large (and related) integers and broadcasts the public key. If another user somehow manages to determine the private key, then he (or she) has broken the cryptosystem and can impersonate the original user.

Richard's paper describes an attack which breaks RSA when the private key is numerically small, relative to its allowable range. RSA is based on number theory, and a method using continued fractions can be applied (when the private key is small) to determine the private key from the public key.

When Richard described this to me, it seemed interesting but unlikely to be of any practical consequence. Not so. Apparently, small private keys lead to a faster implementation, and Richard determined that the Atlanta subway system (MARTA) used RSA cryptography with this shortcut in its farecards. Exploiting this vulnerability, he used his own software (with existing hardware) to produce a physical farecard allowing him unlimited travel all over Atlanta. (He assures me that after testing his farecard with a single free ride, he resumed paying for his transportation.)

Richard's work demonstrated a shrewd understanding of the relationship between academic research and real-world practice, which I imagine would be quite valuable at the NSA.

Oral presentation skills. Richard has given two hour-long talks during our number theory seminar. This is not required of our graduate students; Richard sought me out and asked to speak. Due to travel obligations I was only able to attend one of his lectures; he gave a clear talk, demonstrating enthusiasm, mastery of his material, and an ability to put himself in the mind of an audience member.

Work with others. Richard works well with his fellow graduate students. I asked for testimonials, and one of them, Heather Smith, writes:

> Richie and I worked quite well together in studying for classes, quals [qualifying exams], and comps [comprehensive exams]. Richie listens carefully to others. He is an active listener, asking good questions and encouraging promising ideas. He is able to explain his own thoughts clearly. He has a knack at communicating on just the right level, based on your previous background. This attests to the fact that he is a good listener. I have enjoyed working with Richie these past few years, sharing knowledge and friendship.

Personality and character. Finally, I should mention that I quite admire Richard personally; he is friendly, cheerful, and takes a very positive attitude towards his work. He also takes the initiative outside of work;

UNIVERSITY OF SOUTH CAROLINA

Frank Thorne
Department of Mathematics
University of South Carolina
1523 Greene Street
Columbia, SC 29208
thorne@math.sc.edu

Friday, July 19, 2013

for example, he has organized a weekly department frisbee game (which I have cheerfully, if not always skillfully, participated in). I have always known him to be completely honest, and I have no reservations whatsoever about his character.

I have a great deal of admiration for, and confidence in, Richard, and working with him has been one of the highlights of my time at USC. If he stays in our Ph.D. program for the full five years (through 2015), then I am confident that he will write an outstanding thesis on applications of analytic number theory to cryptography – and this, despite having a thesis advisor with very limited knowledge of cryptography.

If he graduates early, in 2014, then he will be obliged to cut his thesis a bit short, but I still expect it to be very good. In any case I will be very proud to have worked with him.

I would not have nearly this level of confidence in most students in our department, but Richard's ability, motivation, and independence cause him to stand out from the crowd. He has my overwhelming recommendation for a permanent position with the NSA.

Sincerely,

Frank Thorne
Assistant Professor of Mathematics