

**Robert N. Talbert, Ph.D.**  
**Statement of Scholarship**

My overall approach to scholarship is anchored in my commitment to teaching and learning. For me, the ideal line of research is one that originates with a problem or question from a student or class, or one that ends with an application that will help a student or a class. By keeping this focus and maintaining a broad, inclusive view of what constitutes scholarship, I have enjoyed a balanced and productive record of scholarly work with promising lines of inquiry yet to be explored.

My early research made use of classical ring and module theory along with universal algebra and category theory to study constructions in geometric topology. My Ph.D. dissertation ([6]) used a category-theoretic construction called a *homotopy colimit* to establish an isomorphism between the stratified or “Quinn” homology groups  $H_*(X/G; \pi_k \mathcal{S}(p))$  and the better-understood equivariant homology groups  $H_*^G(X; M)$  in the case where  $G$  is a discrete group acting cellularly on a simplicial complex. A version of my dissertation ([5]) appeared in an international mathematics journal. My results have been useful in further work on the Isomorphism Conjecture of Farrell and Jones as well as in understanding the spectral sequence constructions of Frank Quinn.

In more recent years, I have aligned my scholarly work with the model proposed by Ernest Boyer ([1]), pursuing scholarship of *discovery, teaching, integration, and application*. Each of these four kinds of scholarship are present in the specific avenues of study I describe below. I have found this multifaceted approach to scholarship to be productive, realistic, student-centered, and conducive to a well-balanced professional life.

My primary area of mathematical research for the last several years has been *cryptology*. Cryptology is popularly known as the mathematics of codemaking and codebreaking. I was first exposed to the subject through a student whose independent study on the subject I directed. Afterwards, I attended an American Mathematical Society short course on cryptology where I studied current issues in the field and interacted with some of its most famous researchers. After this minicourse, I began to make cryptology my primary area of study through a program of self-study and through the design and teaching of a topics course in the subject.

In 2006, I published a paper ([4]) that grew out of a computer lab assignment on the *rail fence cipher*, given in my Modern Algebra class. The rail fence cipher is a columnar transposition cipher using just two columns. Since the rail fence cipher is a permutation, group theory shows that a message enciphered with the rail fence may be deciphered simply by repeated re-encipherment. My paper studies the minimum number of encipherments it takes to accomplish this, a number known as the *order* of the permutation. In the process, I discovered some interesting number-theoretic properties of the rail fence cipher. For example, the order of the rail fence cipher is a prime number  $p$  if and only if the length of the plaintext divides  $2^p - 1$ . In summer 2010, I directed two undergraduates in their research on extending some of these results for a columnar transposition cipher using three columns.

I have extended my work in cryptology beyond the scholarship of discovery in several ways. First, I designed and teach an upper-division special topics course on cryptology. The course has featured student expository research on such topics as digital steganography, quantum computing, and wi-fi encryption protocols as well as a collaborative student wiki on cryptology during World War II (<http://enigma.wikispaces.com>). Second, I have designed cryptology-flavored components for several courses, including a two-week minicourse on cryptology for students in a freshman mathematics survey course. Third, I designed an interdisciplinary liberal arts course titled “Cryptology, Privacy, and Leadership” for students with no mathematics or computing backgrounds which deals with cryptography in the context of privacy, identity theft, and civil liberties issues.

In addition to mathematical work in cryptology, I maintain an active and growing interest in the scholarship of teaching and learning. My interest in this field extends back to my work as a Master Teaching Fellow at the Vanderbilt University Center for Teaching, where I was introduced to the basic literature on the subject and then used my knowledge to help train new graduate students in the Mathematics and Economics Departments. Although my layperson’s involvement with the scholarship of teaching and learning has been ongoing, resulting in a number of publications ([2], [7], [8]) and numerous conference talks, recently I made a commitment to become fully involved in basic research in this area.

I am particularly interested in teaching and learning in the STEM (science, technology, engineering, and mathematics) disciplines and in the emerging discipline of engineering education. To this end, I received a grant from my current institution to join the American Society for Engineering Education and attend their annual conference in June 2010. At this conference, I attended a minicourse on “Getting Started in Engineering Education Research” conducted by Ruth Streveler and Karl Smith of Purdue University, two leading figures in engineering education. As a result, I am now “plugged in” to a community of both new and experienced engineering education researchers and am poised to begin my own research on teaching and learning questions related to the STEM disciplines.

My ongoing scholarly goals include the following:

- In cryptology, continue to work on extensions of the results of the *Cryptologia* paper ([4]), and become more fluent in the subject itself and allied areas. More specifically:
  - Find results pertaining the fixed points, cycle decomposition, and eventually the order of columnar transposition ciphers having three or more columns.
  - Determine the conditions under which a columnar transposition cipher will consist entirely of one cycle. In this case, the cipher has maximal order and therefore maximum security against a repeated-encryption attack. This has been a surprisingly elusive result, even in the simplest case of just two columns.
  - Improve upon the small computer program I wrote to investigate cycle decomposition of columnar transposition ciphers. The original program was a command-line Java program. In summer 2010, I ported this program to MATLAB and optimized some of the code. I would like eventually to have the program operate through a GUI and run independently on a Windows system or on the Web.
  - Continue reading, and perhaps take coursework, in cryptology and allied areas (such as number theory, probability, information theory, and programming languages) to develop my overall breadth of knowledge.
- In the scholarship of teaching and learning and in engineering education, acquire fluency with the literature and methodology of STEM education research and begin to conduct quantitative research of my own. In particular, I am interested in the following topics:
  - Develop a concept inventory for precalculus centered around students’ understanding of mathematical functions. A *concept inventory* is a quiz given to students in a subject, consisting of conceptual questions on a basic topic and no calculations. The Force Concept Inventory (FCI) from physics is the seminal example and has fomented a revolution in the teaching of introductory physics. A “function concept inventory” would be greatly helpful in studying similar issues of conceptual understanding in mathematics.
  - Use the function concept inventory to investigate the effects of peer instruction techniques and the “inverted classroom” model in introductory mathematics and computer science courses. The work of Eric Mazur (for example, [3]) describes the notion of peer instruction and the basic idea of the “inverted classroom” model of teaching. The inverted classroom moves student acquisition of basic concepts outside of the classroom (and away from lecture) and moves student assimilation of concepts into the classroom (and away from homework). I have experimented with the inverted classroom model in my introductory MATLAB course with significant success and would like to generalize to introductory mathematics classes.
  - Gather and analyze data on the effect of Mastery or Gateway Exams in calculus and precalculus courses on student learning in those subjects.
  - Study how a peer-instruction or inverted classroom approach to introductory mathematics, physics, or computing courses affects the performance of engineering students in design projects later in their college careers.
- Actively recruit undergraduates to assist me in any combination of the above research goals through collaboration or independent research projects.
- Maintain a program of reading and study in any areas that might support the above goals or lead to new avenues of scholarship.

## References

- [1] E. Boyer. *Scholarship Reconsidered: Priorities of the Professoriate*. New York: Jossey-Bass, 2000.
- [2] J. Gash and R. Talbert. Integrating spreadsheets, visualization tools, and computational knowledge engines in a liberal arts calculus course. To appear in *Proceedings of the Twenty-second International Conference on Technology in Collegiate Mathematics*.
- [3] E. Mazur. *Peer Instruction: A User's Manual*. Benjamin Cummings, 1996.
- [4] R. Talbert. The cycle structure and order of the rail fence cipher. *Cryptologia*, **30**(2):159–172, 2006.
- [5] R. Talbert. An isomorphism between Bredon and Quinn homology via homotopy colimits. *Forum Mathematicum*, **11**:591–616, 1999.
- [6] R. Talbert. *Stratified and equivariant homology via homotopy colimits*. Ph.D. dissertation, Vanderbilt University, August 1997.
- [7] R. Talbert. A tale of two wikis: Upper-level mathematics meets Web 2.0. *Proceedings of the Twentieth International Conference on Technology in Collegiate Mathematics*, <http://archives.math.utk.edu/ICTCM/i/20/C009.html>, Spring 2009.
- [8] R. Talbert. Teaching MATLAB to a Non-Canonical Audience. To appear in *Proceedings of the Twenty-second International Conference on Technology in Collegiate Mathematics*.