# Code Making and Code Breaking:
# The Innovation Behavior of Leaders and Challengers

Florenta Teodoridis

This project will be collaborative with Avi Goldfarb, University of Toronto and NBER.

The goal of this project is to provide an empirical understanding of innovation behavior in the presence of competition. Our empirical setting is academic research in cryptography (code makers) and cryptanalysis (code breakers). Because of the nature of innovation in this setting, we observe a race between code makers and code breakers and the relative advantage of each. This will enable us to investigate laggard and leader innovation as informed by Schumpeterian growth theory.

There is broad agreement that innovation is essential for economic growth. Growth theory has considered a variety of models aimed at parsing innovation behavior and its output as it contributes to economic growth. We focus on recent theoretical developments of step-by-step innovation models (e.g., Aghion et al., 2001; Aghion et al., 2005; Aghion et al., 2015) that provide a richer set of theoretical predictions relative to the innovative behavior of leaders and challengers. Implicitly, we consider both the Schumpeterian model with vertical innovations and the product variety models (e.g., Romer, 1990) with horizontal innovations (Grossman and Helpman, 1991).

A large empirical literature offers evidence informed by these theoretical models, both at the individual and firm level. A central question focuses on how different forms of competition might affect innovation behavior. However, these empirical findings remain mixed (e.g., Gilbert, 2006; Cohen, 2010). On the one hand, it is unclear if market structure plays a role in influencing innovation behavior. On the other hand, the empirical studies struggle to account for the endogenous relationship between innovation and the competitive landscape.

We propose a novel setting to further contribute to these empirical efforts. Specifically, we propose to focus on scientists' innovative behavior in cryptography (code making) and cryptanalysis (code breaking). We do so since the nature of innovation in these domains is that of a race, and thus lends itself well to the theoretical models of growth preoccupied with the relationship between innovation behavior and competition.

The goal of cryptography, a science at the intersection of mathematics, computers science and electrical engineering, is to create algorithms that hide the meaning of a message. Cryptanalysis is the science of breaking those algorithms. While the popular belief is that most code making is secretive and most code breaking is undertaken by ill-intended individuals, in reality both aspects unfold in the realm of open science. Cryptography is pervasive to our modern society. Web browsers, email programs, credit cards and cell phones, to name a few, incorporate cryptographic algorithms in order to ensure secure data transmission between parties. Academic researchers in cryptography are preoccupied with bettering these security algorithms. Cryptanalysis was formed as a result of these scientists' efforts to ensure the soundness of their cryptographic algorithms. In other words, the scientists of cryptanalysis are focused on ensuring the robustness of cryptography algorithms by launching attacks on them while still in theoretical stage (as opposed to applied and implemented).

Given the nature of these two research domains, the setting provides a rich testing bed of leader and challenger innovation behavior, with respect to both horizontal and vertical innovation,

and relative to changes in the competitive landscape as shaped by the race between code makers and code breakers. Specifically, we propose to measure changes in the differential innovative effort of code makers and code breakers relative to the perceived lag between the two groups, over time. For example, would code makers decelerate their innovation efforts when code breakers are perceived to be a large distance away from breaking their encryption algorithms, or maintain or accelerate their innovation efforts to ensure continued leadership? Furthermore, when would code makers find it optimal to abandon incremental innovation on a certain class of cryptographic algorithms and engage in developing a different class?

A concern of scholars preoccupied with the relationship between innovation and competition is the endogeneity of this connection (Cohen, 2010; Aghion et al., 2014). To this end, we propose to exploit two sets of events that provide a source of exogenous change in the innovation landscape (albeit not without limitations). The first approach focuses on changes in national encryption standards. In November 2001, the National Institute of Standards and Technology announced a new encryption standard. The winning algorithm was selected after a few years of search among the various cryptographic developments of that time. [1] The announcement generated a relative change in incentives to follow-on code making and breaking efforts between the winning algorithm and contender algorithms.

The second proposed approach exploits the events of advancements in computational technology, namely those related to quantum computers. In 1994, mathematician Peter Shor formulated a theoretical algorithm for integer factorization that computes on quantum machines. Integer factorization, the process of identifying prime factors, is believed to be infeasible on classical computers for large integers. This is important as most popular contemporaneous public cryptographic systems rely on the difficulty of factoring integers. Using Shor's algorithm, quantum computers would be capable of decrypting these security systems with significant ramifications for electronic privacy and security. This insight altered code making innovation incentives towards radical changes in cryptography employing quantum principles. For example, quantum key distribution is a result of such efforts.

In our analysis, we will focus on academic publications in cryptography and cryptanalysis as a paper trail of innovation in these domains. We will collect such data within a window of plus minus ten years around the timing of the two events mentioned above. We will not focus on very recent events for two main reasons. First, we want to ensure that we observe a telling period of innovation before and after the events. Second, we want to maintain a distance in time from very recent cryptography developments as history tells us that those are the most likely ones to be subject to secrecy, and hence incomplete public data. We collect our data from Scopus, a comprehensive bibliographic database of world-wide academic publications. We define boundaries of cryptography and cryptanalysis by a combination of citation trail and journal type. We start with the central set of journals of cryptography as identified by the International Association of Cryptographic Research (IACR). ICAR is the most prominent institution in cryptography focused on furthering research in this domain.[2] Next, we turn to identifying the various types and classes of cryptographic algorithms, the academic activity pertaining to each and the academic publications marking the move from one set of algorithms to another. We take advantage of the fact that cryptographic algorithms can be identified by name and hence innovation efforts pertaining to each can be followed through keyword searches and citation trails.

[1] http://www.nist.gov/manuscript-publication-search.cfm?pub_id=901427

[2] https://www.iacr.org/

**References**

Aghion, P., Harris, C., Howitt, P., Vickers, J. 2001. Competition, imitation and growth with step-by-step innovation" Review of Economic Studies, 68: 467-492.

Aghion,P., Bloom,N., Blundell,R., Griffith,R., and Howitt,P. 2005. "Competition and innovation: an inverted-u relationship" Quarterly Journal of Economics, 120(2):702–728.

Aghion, P., Bechtold, S., Cassar, L., Herz, H. 2014. "The causal effects of competition on innovation: Experimental evidence", NBER working paper #19987

Aghion, P., Akcigit, U., Howitt, P. 2015. "Lessons from Schumpeterian growth Theory" American Economic Review: Papers & Proceedings, 105(5): 94-99.

Cohen, W. 2010. "Fifty years of empirical studies of innovative activity and performance" In: Hall, B. H., Rosenberg, N. (Eds.), Handbook of the Economics of Innovation, vol. 1 Elsevier, pp. 129-213.

Gilbert, R. 2006. "Looking for Mr. Schumpeter: Where are we in the competition-innovation debate?" In: Jaffe, A., Lerner, S., Stern, S., (Eds.), Innovation Policy and the Economy, vol 6. MIT Press/National Bureau of Economic Research, Cambridge, MA, pp. 159-215.

Grossman, G., Helpman, E. 1991. "Quality ladders in the theory of growth" Review of Economic Studies, 58: 43-61.

Romer, P. 1990. "Endogenous technical change" Journal of Political Economy, 98: 71-102.

# Florenta Teodoridis

Marshall School of Business
University of Southern California
701 Exposition Blvd., HOH 503,
Los Angeles, CA, 90089
Office: (213) 821-0852
florenta.teodoridis@marshall.usc.edu

**Appointments:**

2014 – Present: Assistant Professor, Strategy
Marshall School of Business, University of Southern California

**Education:**

Ph.D. Strategy, Rotman School of Management, University of Toronto, 2014
MBA Strategy and International Business, Schulich School of Business, York University, Toronto, 2008
B.Sc. Mathematics and Computer Science, University of Bucharest

**Research Activity:**

Refereed Publications:

- "Understanding the Changing Structure of Scientific Inquiry" (with Ajay Agrawal and Avi Goldfarb), *American Economic Journal: Applied Economics*, 2016 8(1): 100-128

Working Papers:

- "Understanding Team Knowledge Production: Generalists and Specialists", under review at *Management Science*
- "Does Industry Collaboration Reduce Open Science in Academia? Evidence from Simultaneous Discoveries" (with Michael Bikard and Keyvan Vakili)
- "Commercialization Strategies for Disruptive Technologies: Implications for the Rate of Innovation" (with Kyle Mayer)
- "Cumulative Innovation and the Evolution of Research Trajectories" (with Jeff Furman)
- "Knowledge Diversification and Stars: Implications for the Knowledge Creation Process" (with Michael Bikard and Keyvan Vakili)

**Awards:**

- NSF Science of Science & Innovation Policy: "Collaborative Research: The Impact of Research Costs on the Rate and Direction of Scientific Discovery" (2016-2019)
  - Co-PI (with Jeff Furman) for approx. $500,000
- Grief Entrepreneurship Faculty Research Award, 2016
- Finalist, AOM TIM Dissertation Award, 2015
- Semi-finalist, ISPIM Innovation Management Dissertation Award, 2015
- Steven Klepper Award for Best Young Scholar Paper, DRUID, Copenhagen, 2014

- Research Program on the Economics of Knowledge Contribution and Distribution funded by the Sloan Foundation, Research Grant, 2014
- Best Student Paper Award, Roundtable for Engineering Entrepreneurship Research (REER), Scheller College of Business, Georgia Tech, Atlanta, 2013
- SGS Conference Grant, University of Toronto, 2013
- CCMF Doctoral Fellowship, 2009 to 2014

**Conferences and Seminars:**

Academy of Management, TIM Doctoral Dissertation Competition (2015)
Roundtable for Engineering Entrepreneurship Research (REER, 2014), Georgia Institute of Technology
Washington University in St. Louis, Olin Business School (2014)
University of California at San Diego, School of International Relations and Pacific Studies (2014)
Carnegie Mellon University, Department of Engineering and Public Policy (2014)
Georgia Institute of Technology, Scheller College of Business (2014), Atlanta
DRUID Society Conference on Entrepreneurship 2014, Organization and Innovation, Copenhagen Business School
National Bureau of Economic Research (NBER) Summer Institute 2014
Academy of Management, Symposium 2014
CCC Colloquium for Doctoral Student Research, 2013
DRUID, 35th Celebration Conference on Innovation, Strategy and Entrepreneurship 2013, ESADE, Barcelona
National Bureau of Economic Research (NBER), Productivity Seminar Series 2013
Economics of Knowledge Contribution and Distribution, Sloan Foundation in conjunction with the Roundtable for Engineering Entrepreneurship Research (REER, 2013), Georgia Institute of Technology
Bocconi University 2013, Milan
IESE Business School 2013, Barcelona
Roundtable for Engineering Entrepreneurship Research (REER, 2012), Georgia Institute of Technology, Atlanta
The Organization, Economics and Policy of Scientific Research, LEI & BRICK 2012, Turin
University of Toronto, Rotman School of Management, Strategy Seminar Series 2012

**Teaching:**

2016 – Present Research Methods in Strategy and Organization, PhD
2016 – Present Problem Solving & Decision Making: An Integrative Approach, MBA
2015 – Present Strategic Management
2009 – 2014 Teaching assistant (Strategic Management, MBA; Corporate Strategy, MBA; Venture Capital, MBA; Model-based Decision Making in Practice, MBA; International Business, MBA)

**Professional Activities:**

Ad Hoc Referee
Management Science
Organization Science
Research Policy
Academy of Management

Professional Affiliations

Academy of Management (BPS, TIM, Entrepreneurship)

Other

Fellow, Creative Destruction Lab at Rotman School of Management, University of Toronto (2013-2014)

**Non-Academic Experience:**

Identified, designed and managed the full development life-cycle of various data-driven business decision-making applications (big data, business intelligence, data warehousing)

- Consultant/Project Manager, Harlequin Enterprises – TORSTAR, Toronto, 2006-2009
- Technical Project Manager, St. Elizabeth Health Care, Toronto, 2002-2005
- Project Lead/Software Developer, IPSOS-Reid, Toronto, 2000-2002