Berkeley-Paris Conference on Cyber Risk

Joint Research Project France-Berkeley
"Modeling for cyber-risk insurance"
between ENSAE Paris CREST and Berkeley IEOR

June 12th, 2023
Berkeley University of California, Room Etcheverry 1174.

Program

9am – 9:15am: Registration

9:15am – 9:30am : Welcome address
by **Caroline HILLAIRET** ENSAE Paris and **Thibaut MASTROLIA**, UC Berkeley IEOR

9:30am – 10:10am : **Olivier LOPEZ** , ENSAE Paris, CREST
Parametric insurance for extreme claims: the case of cyber risk

10:10am – 10:50am : **Anil ASWANI**, University of California Berkeley.
Incorporating Fairness into Principal-Agent Models with Adverse Selection and Moral Hazard

10:50am – 11:10am : Coffee break

11:10am – 11:50am : **Yousra CHERKAOUI**, ENSAE Paris, CREST, and Milliman.
TBA

11:50am – 12:30pm : **Unal TATAR**, University of Albany.
TBA

12:30pm – 2pm : Lunch break

2pm – 2:40pm : **Anthony REVEILLAC**, Institut Mathématiques de Toulouse
Pseudo-chaotic expansion for Point processes and applications.

2:40pm – 3:20pm : **Sukanya KUDVA**, University of California Berkeley.
Analyzing Welfare and Privacy in specific Cyber-physical Systems

3:20pm – 4:00pm : **Wissal SABBAGH**, Le Mans Université, LMM.
TBA

4:00pm – 4:20pm : Coffee break

4.20pm – 5:00pm : **Anis MATOUSSI**, Le Mans Université, LMM.
Stochastic Algorithms for Systemic Shortfall Risk Measure: static and dynamic cases.

5:00pm – 5:40pm : **Dawn SONG**, University of California Berkeley.
TBA

5:40pm – 5:45pm : Conclusion of the day

Abstracts

Olivier LOPEZ (ENSAE Paris, CREST)

Title *Parametric insurance for extreme claims: the case of cyber risk*

Abstract Parametric (or index based) insurance is a way to indirectly cover a risk by giving to the policyholder a compensation that is based on the value of a ”parameter” and not on the true value of the claim. Compared to traditional insurance, expertise is no longer required since the parameter triggering the compensation is supposed to be available soon after the claim. This is an important advantage for the insurance company which reduces its administrative costs, and also for the policyholder provided that the parameter or index correctly reflects the risk it is designed to replace. This fastness of compensation is very appealing in the context of cyber, where the time of reaction is crucial. On the other hand, these types of products may fail to propose a sufficiently high compensation in the case of extreme claims. In this talk, we study how a combination of traditional insurance and parametric products can optimize the coverage of cyber risk, based on a specific utility function representing the expectations of the policyholder.

Anil ASWANI (University of California Berkeley.)

Title *Incorporating Fairness into Principal-Agent Models with Adverse Selection and Moral Hazard.*

Abstract Existing approaches to incentive design often overlook the important aspect of fairness, which can lead to adverse consequences for certain groups based on race, gender, or other characteristics. In this study, we address this limitation by introducing fairness into optimization problems within principal-agent models. Specifically, we focus on scenarios involving adverse selection and moral hazard. We formulate quantitative definitions of fairness and derive the policy structure for optimal fair contracts. By discussing the underlying intuition behind these contracts, we highlight the impact of fairness on incentive design. Furthermore, we present a numerical case study to illustrate the practical implications of incorporating fairness considerations in the design process. Joint work with Yoon Lee, Ilgin Dogan, Z.-J. Shen.

Yousra CHERKAOUI (ENSAE Paris, CREST, and Milliman.)

Title *Cyber risk modeling using a two-phase Hawkes process with external excitation.*

Abstract With the growing digital transformation of the worldwide economy, cyber-risk has become a major issue. As 1% of the world’s GDP (around $1,000$ billion) is allegedly lost to cyber-crime every year, IT systems continue to get increasingly interconnected, making them vulnerable to accumulation phenomena that undermine the pooling mechanism of insurance. As highlighted in the literature, Hawkes processes appear to be suitable to capture contagion phenomena and clustering features of cyber-events. This paper extends the standard Hawkes modeling of cyber-risk frequency by adding external shocks, such as the publication of cyber-vulnerabilities that are deemed to increase the likelihood of attacks in the short term. While the standard Hawkes model attributes all clustering phenomena to self-excitation, this paper introduces a model designed to capture external common factors that may explain part of the systemic pattern. This aims to provide a better quantification of contagion effects. We propose a Hawkes model with two kernels, one for the endogenous factor (the contagion from other cyber-events) and one for the exogenous component (cyber-vulnerability publications). We use parametric exponential specifications for both the internal and exogenous intensity kernels, and we compare different methods to tackle the inference problem based on public datasets containing features of cyber-attacks found in the Hackmageddon database and cyber vulnerabilities from the Known Exploited Vulnerability database and the National Vulnerability Dataset. By refining the external excitation database selection, the degree of endogeneity of the model is nearly halved. We illustrate our model with simulations and discuss the impact of taking into account the external factor driven by vulnerabilities. Once an attack has occurred, response measures may be implemented to limit the effects of an attack. These measures include patching vulnerabilities and reducing the attack's contagion. We use an augmented version of the model by adding a second phase modeling a reduction in the contagion pattern from the remediation measures. Based on this model, we explore various scenarios and quantify the effect of mitigation measures of an insurance company that aims to mitigate the effects of a cyber-pandemic in its insured portfolio. Based on a joint work with Alexandre Boumezoued et Caroline Hillairet.

Unal TATAR (University of Albany.)

Title *TBA.*

Abstract TBA

Anthony REVEILLAC (Institut Mathématiques de Toulouse.)

Title *Pseudo-chaotic expansion for Point processes and applications.*

Abstract Cyber risk modeling call for probabilistic frameworks involving counting processes with stochastic intensity. More specifically, a focus has been recently given in that line of modeling on a class of counting processes which exhibits a cluster structure such as Hawkes processes. These mathematical objects turn out to be difficult to study and very few is known for them. In this talk we introduce and make use of a new representation of Point processes at the crossroad of the so-called Poisson imbedding and Malliavin's calculus that we name pseudo-chaotic expansion. With this representation at hand we present several applications of this representation for the case of Hawkes processes. This talk is based on works with C. Hillairet and T. Peyrat.

Sukanya KUDVA (University of California Berkeley.)

Title *Analyzing Welfare and Privacy in specific Cyber-physical Systems.*

Abstract This talk explores questions around individual privacy, societal and individual welfare, and the effects of coordination among stakeholders in cyber-physical systems. It is based on two of our recent works.
Part 1: Effects of Datadividends on Individual Privacy in Online Platforms Online platforms, including social media and search platforms, have routinely used their users' data for targeted ads, to improve their services, and to sell to third-party buyers. However, an increasing awareness of the importance of users' data privacy has led to new laws regulating platform data-sharing. Further, there have been political discussions on introducing data dividends, that pay users for their data. Three interesting questions are then: When would these online platforms be incentivized to pay data dividends? How does their decision depend on whether users value their privacy more than the platform's free services? And should platforms invest in protecting users' data? We construct a principal-agent model using a Stackelberg game, calculate optimal decisions and qualitatively discuss the implications.
Part 2: Impact of Coalitions of Electric-Vehicle Charging Stations on Welfare The rapid growth of electric vehicles (EVs) is driving the expansion of charging infrastructure globally. This expansion, however, places significant charging demand on the electricity grid, impacting grid operations and electricity pricing. While coordination among all charging stations is beneficial, it may not be always feasible. However, a subset of charging stations, which could be jointly operated by a company, could coordinate to decide their charging profile. We investigate whether such coalitions between charging stations are better than

no Coordination. We model EV charging as a non-cooperative aggregative game, where each station's cost is determined by both monetary payments tied to reactive electricity prices on the grid and its sensitivity to deviations from a nominal charging profile. We consider a solution concept that we call C-Nash equilibrium, which is tied to a coalition C of charging stations coordinating to reduce their cumulative costs. We provide sufficient conditions, in terms of the demand and sensitivity of charging stations, to determine when independent (uncoordinated) operation of charging stations could result in lower overall costs to charging stations, the coalition, and charging stations outside the coalition. Somewhat counter to intuition, we demonstrate scenarios where allowing charging stations to operate independently is better than coordinating as a coalition. Jointly, these results provide operators of charging stations insights into how to coordinate their charging behavior and open several research directions.

Wissal SABBAGH **(Le Mans Université, LMM.)**

Title *Cyber risk management under optimal hacking with impulse control.*

Abstract Cyber risk is a major concern for public entities and private companies, and constitutes a systemic threat to the resilience of the financial and economic world. In fact, 1 % of the world's GDP, or 1,000 billion, goes up every year because of cyber-crime. Cyberattacks are now the biggest threat to the financial system, says Jerome Powell, Chairman of the Federal Reserve global. In this talk, we develop a first study in which a cluster owner aims to protect a computer network by regularly updating or by purchasing security software against cyber-attacks. On the one hand, not protecting the computer network induces non-negligible financial losses for the owner of the cluster. On the other hand, cyber attacks can infect the network and lead to significant cyber incidents for the cluster owner and the customers of the service provided. First, we characterize the optimal protection policy for a network against effective hacking taken as a worst-case scenario. Based on an epidemiological model, we determine the optimal (dynamic) protection strategy, as a function of the evolution of attack strategies and the network's level of infection. Then, we solve optimization problems by using deep learning methods to approximate a system of fully coupled equations. Joint work with Caroline Hillairet and Thibaut Mastrolia.

Anis MATOUSSI **(Le Mans Université, LMM.)**

Title *Stochastic Algorithms for Systemic Shortfall Risk Measure: static and dynamic cases.*

Abstract TIn this talk, we study a stochastic algorithms schemes for estimating Multivariate Shortfall Risk Measure (MSRM) and prove that the resulting estimators are consistent and asymptotically normal. We also test numerically the performance of these algorithms on several examples. We will present also a work in progress on a class of dynamic MSRM via BSDEs. The first part of the talk is based on a joint works with Sarah Kaakaï (Le Mans Université) and Achraf Tamtalini (Bank of America, London-UK), and the second one is based in a work in progress with Zakaria Bensaid (Le Mans Université), Roxana Dumitrescu (King's College of London) and Wissal Sabbagh (Le Mans Université).
References :
1. Z. Bensaid, R. Dumitrescu, A. Matoussi, W. Sabbagh. Machine learning methods for Multivariate Shortfall Risk Measures, forthcoming paper.
2. S. Kaakai, A. Matoussi, A. Tamtalini. Estimation of Systemic Shortfall Risk Measure using Stochastic Algorithms. hal-038711246 (2022), to appear in SIAM Journal on Financial Mathematics.

Dawn SONG **(University of California Berkeley.)**

Title *TBA.*

Abstract TBA