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, 2024
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.
Cyber risk modeling using a two-phase Hawkes process with external excitation.

11:50am – 12:30pm : **Unal TATAR**, University of Albany.
Bridging the Gap: Advanced Models for Cyber Insurance and Risk Analysis.

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.
Cyber risk management with impulse control.

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 – 5:10pm : 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 *Bridging the Gap: Advanced Models for Cyber Insurance and Risk Analysis.*

Abstract This presentation integrates findings from two extensive studies on cyber insurance and quantitative cyber risk analysis, aimed at bridging the gap between academic research and practical applications. The first study offers a comprehensive review of academic and grey literature on cyber insurance, highlighting the methods, datasets, challenges, and future directions that are critical for actuaries and risk managers. This interdisciplinary review is among the most extensive to date, providing a valuable resource for enhancing the development and implementation of cyber insurance policies.
The second study critiques the current cyber risk analysis methods that often isolate cyber risks as IT issues, proposing instead a holistic, enterprise-level approach. This research develops a probabilistic, quantitative model using probabilistic attack graphs and Bayesian networks to assess dynamic risks and their impacts on organizational goals. The model focuses on the loss of confidentiality, integrity, and availability (CIA) to quantify the economic consequences of cyber-attacks, offering a detailed framework for risk assessment and management. This integrated approach aims to improve decision-making processes and policy formulation in the context of cyber risk management.

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 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 In 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.

Satellite Event : Young Researchers Talks

June 13th, 2024
Berkeley University of California, Room Etcheverry 1174.

Program

9am – 9:25pm : **Tingyu ZHU** , University of California Berkeley.
Selection of the Best Policy Under Fairness and Equity Constraints.

9:25am – 9:50pm : **Alberto GENNARO**, University of California Berkeley.
Delegated optimal portfolio allocation under random horizon.

9:50am – 10:15pm : **Beatrice ONGAROTO**, University of Padova.
Optimal Cyber-Security Investment in a Dynamic Version of the Gordon-Loeb Model.

10:15am – 10:40am : **Benjamin MASSAT**, Institut Mathématiques de Toulouse.
Normal Approximation of Functionals of Point Processes: Application to Hawkes Processes.

10:45am – 11:15am : Coffee break

11:15am – 11:40am : **Thomas PEYRAT**, CREST and Exiom Partners.
A compound Hawkes process with dependencies for insurance applications.

11:40am – 12:05am : **Xinyu LI**, University of California Berkeley.
An alpha potential game framework for N-player games.

12:05am – 12:30am : **Antoine HERANVAL**, ENSAE Paris, CREST
Bayesian Credibility Model with heavy tail random variables: calibration of the prior and application to cyber insurance.

Abstracts

Tingyu ZHU (University of California Berkeley)

Title *Selection of the Best Policy Under Fairness and Equity Constraints.*

Abstract We formulate, analyze and solve the problem of Selection of the Best policy with Fairness Constraints on subpopulations (SBFC) . Standard selection of the best problem aims at selecting an arm that has the largest expected reward where the expectation is taken over the entire population. The SBFC problem requires that a selected policy must be fair to all subpopulations (e.g., different ethnic groups, age groups, or customer types) by satisfying constraints that the expected reward conditional on every subpopulation needs to be larger than some thresholds. We analyze the complexity of the SBFC problem by proving a best achievable lower bound on the sample complexity with closed-form representation. We then design an algorithm and prove that the algorithm's sample complexity matches with the lower bound in terms of order.

Alberto GENNARO (University of California Berkeley)

Title *Delegated optimal portfolio allocation under random horizon.*

Abstract In this talk, we are investing the contracting problem between an investor delegating the management of a risky portfolio to a hedge fund. The horizon of investment is assumed to be fixed but subject to a random early termination time. We illustrate our results with numerical simulations using a deep learning iterative approach.

Beatrice ONGAROTA (University of Padova)

Title *Optimal Cyber-Security Investment in a Dynamic Version of the Gordon-Loeb Model.*

Abstract We consider an entity, such as a corporation or government, that faces the threat of cyber-attacks. Inspired by the Gordon-Loeb model, we assume that the success rate of cyber-attacks depends on the vulnerability of the entity's security system. To reduce this vulnerability, the entity can invest in security measures. Our aim is to determine the optimal investment strategy. We develop a dynamic version of the Gordon-Loeb model, incorporating the attack dynamics using jump processes. The problem is framed as a stochastic control model with jumps and is addressed using Hamilton-Jacobi-Bellman (HJB) techniques. .

Benjamin MASSAT (Institut Mathématiques de Toulouse.)

Title *Normal Approximation of Functionals of Point Processes: Application to Hawkes Processes.*

Abstract In this paper, we derive an explicit upper bound for the Wasserstein distance between a functional of point processes and a Gaussian distribution. Using Stein's method in conjunction with Malliavin's calculus and the Poisson embedding representation, our result applies to a variety of point processes including discrete and continuous Hawkes processes. In particular, we establish an explicit convergence rate for stable continuous non-linear Hawkes processes and for discrete Hawkes processes. Finally, we obtain an upper bound in the context of nearly unstable Hawkes processes.

Thomas PEYRAT (CREST and Exiom Partners.)

Title *A compound Hawkes process with dependecies for insurance applications.*

Abstract In insurance, one of the processes commonly used to model risk is the compound Poisson process. Assuming independence between the counting process (Poisson Process) and the claims (independent and identically distributed random variables), the calculation of the first two cumulants is immediate. However, these assumptions limit the scope of application of this process to certain risks. In order to remove some of these assumptions, we will present a similar model in which the counting process is a Hawkes process whose intensity is impacted by claims. We will also briefly present a methodology for calculating the first two cumulants of this process.

Xinyu LI (University of California Berkeley)

Title *An alpha potential game framework for N-player games.*

Abstract Our work proposes and studies a general form of dynamic N-player non-cooperative games called α-potential games, where the change of a player's value function upon her unilateral deviation from her strategy is equal to the change of an α-potential function up to an error α. Analogous to the static potential game (which corresponds to $\alpha = 0$), the α-potential game framework is shown to reduce the challenging task of finding approximate Nash equilibria for a dynamic game to minimizing the α-potential function. Moreover, an analytical characterization of α-potential functions is established, with α represented in terms of the magnitude of the asymmetry of value functions' second-order derivatives. For stochastic differential games in which the state dynamic is a controlled diffusion, α is explicitly identified in terms of the number of players, the choice of admissible strategies, and the intensity of interactions, and the level of heterogeneity among players. This is achieved by introducing a suitable linear derivative of the value functions with respect to unilateral deviations of strategies and via analyzing the sensitivity processes of state dynamics with respect to controls. For games with mean-field type interactions, α is shown to decay to zero as the number of players goes to infinity, even with heterogeneity in state dynamics, cost functions, and admissible strategy classes. For distributed games, if a static potential function can be derived from the cost functions, then $\alpha = 0$. For crowd aversion games, α is capable of capturing the subtle difference between the choice of admissible strategies. .

Antoine HERANVAL (ENSAE Paris and CREST.)

Title *A compound Hawkes process with dependecies for insurance applications.*

Abstract The Bayesian credibility approach is a method for evaluating a certain risk of a segment of a portfolio (such as policyholder or category of policyholders) by compensating for the lack of historical data through the use of a prior distribution. This prior distribution can be thought as a preliminary expertise, that gathers information on the target distribution. This paper describes a particular Bayesian credibility model that is well-suited for situations where collective data are available to compute the prior, and when the distribution of the variables are heavy-tailed. The credibility model we consider aims to obtain a heavy tailed distribution (namely a Generalized Pareto distribution) at a collective level and provides a closed formula to compute the credibility premium at an individual level. A classical database on data leaks is used to fit a model for the volume of data exposed during a cyber incident, while the historical data on a given firm is taken into account to consider individual experience.