Hamiltonian Mechanics

Ivar Ekeland[1] and Roger Temam[2]

[1] Princeton University, Princeton NJ 08544, USA
[2] Université de Paris-Sud, Laboratoire d'Analyse Numérique, Bâtiment 425, F-91405 Orsay Cedex, France

Abstract. Cyber-insurance is a powerful economic concept that can help companies in the fight against cybercrime. From the early 80s, several researchers claimed that cyber-insurance had a bright future, were it would become a huge economical tool for handling residual cyber-risks. However, both the European and US cyber-insurance market have failed to grasp its promising potential. To fully grasp this potential they need innovative approaches to handle the unique problems of cyber-insurance. This paper find and characterize network structures with properties that make them superior as cyber-insurance. And creates several models for forming these network structures. In every model, new properties that relate the model to the real-world and real-world insurance products are added. The results show that insurers can use the insurance premium as a tool for determining the resulting formation of the network, and if set to the right level, these superior structures will evolve.
We believe our findings could help the cyber-insurance market evolve, by giving the insurers a proper tool to better analyze and control formation of cyber-insurance networks.

1 Introduction to cyber-insurance

Security breaches are increasingly prevalent in the Internet age causing huge financial losses for companies and their users. When facing security breaches and risk, there are typically four ways to act [BO1]:

1. Avoid the risk
2. Retain the risk
3. Self protect and mitigate the risk
4. Transfer the risk

The ICT industry have so far tried to prevent risks with a mixture of options two and three. This has lead to many different techniques and software trying to detect threats and anomalies, to protect the users and infrastructure. Firewalls, intrusion- detection and prevention systems, are some of the solutions. These will reduce the risk, but do not eliminate the risk completely. Although they are all good and needed actions, it is impossible to achieve perfect cyber-security, due to many reasons: Threats are continuously evolving, there will always be accidents and security flaws, attackers have different intentions, network externalities and

free-riding in security networks, the lemons-market in security products, misaligned incentives between users and product vendors, and many more. This is why we need cyber-insurance, as an fourth option, to handle the residual risk [BO2,RA1].

The paper [BS1] describes the three main problems of cyber-insurance information asymmetry, correlated risk and interdependent agents.

Information asymmetry. Information asymmetry arises when one side of a transaction or decision has more or better information than the other party. There are two different cases of information asymmetry. The first one is called adverse selection, where one party simply has less information regarding the performance of the transaction. A good example is when buying health insurance, if a person with bad health purchases insurance, and the information about her health is not available to the insurer, we have a classical adverse selection scenario, where the insurer probably charges too little. We can observe a similar situation for the cyber-industry, where an insurer has no way of confirming whether your network is "healthy", i.e. not contaminated or infected. The other information asymmetry scenario is called moral hazard. It occurs after the signing of the contract, where one party deliberately takes some action that makes the possibility of loss higher, e.g. choosing not to lock your door, since you have insurance. Or in the computer setting, deliberately visiting hostile web-pages, or not using anti-virus software, firewalls or other self-protection software, although you are required to do so.

The task of measuring the level of security is very hard, and in order to lower the premiums people will have an incentive for hiding information about their security level, hence the problem with asymmetry is highly relevant. Another problem occurs on the customer side of the market. For a customer wanting to improve his/her defense mechanisms, the software security market often becomes a lemon's market. It is difficult for the buyer to distinguish the performance of different software products, and thus the reasonable thing to do, is to buy the cheapest. Therefore, the good security products must cost the same as the bad. If the cost of producing good security software is too high, the problem can even result in abandoning the production of good software, because it would not be profitable.

Correlated risk. Another big concern regarding cyber-insurance, is the correlated risk. Among other things, the problem occurs due to the need for standards. Standardization is an important part of the business of computers and computer networks. Generally it enables computers to communicate, install and use different software. A good example is operative systems for personal computers, today we only have a small set of operative systems available, and these systems are standardized, so they can use the same communication channels. The standards generate a lot of the value in the ICT industry, but they also make many threats possible. All systems that use the same standards, create a large number of similar exposure units, i.e. they share common vulnerabilities, which could be exploited at the same time. As we see, this violates the insurance characteristic

of limited risk of catastrophically large losses. Thus create a significant difficulty for the cyber-insurance industry, because when a security breach occurs there is a high probability that it will occur to a large number of people, i.e. catastrophic and extreme events occur with a higher probability than in the regular insurance business. To compensate, the logical thing to do would be to raise the premium cost, this could however violate the characteristics of affordable premiums and large losses. If the security breach is large, it could even potentially cause so much damage, that the insurers will not be able to pay all the customers who suffered, and they could go bankrupt.

Interdependent security. Another problem in the ICT industry is interdependent security, meaning that you are not only dependent on your own investment in security, but also on everyone else's. Investment in security generates positive externalities, and as public goods, this encourages free riding. Why should I pay for security when I can just free ride on security invested by others? The problem is that the reward for a user investing in self-protection depends on the security in the rest of the network. i.e. The expected loss due to a security breach at one agent in the network, is not only dependent on this agent's level of investment in security, but also on the security investment done by adjacent agents, and their adjacent agents and so forth. A good example of this is the amount of spam sent every day, which depends on the number of compromised computers. Meaning if you have invested in security software of some kind, you still receive lots of spam because many other people have not invested. Bohme et. al argue that a model for cyber-insurance has to overcome each of these obstacles. They analyze several other papers on cyber-insurance, and show how all of them are touching upon these problems, but mostly they focus on only one or two of these, not all three.

The market for cyber-insurance emerged in the late 80's, when security software companies began collaborating with insurance companies to offer insurance policies together with their security products. From a marketing perspective, adding insurance helped highlighting the supposedly high quality of the security software. Nevertheless, this new product was a comprehensive solution, which dealt with both risk reduction and residual risk [BO3]. Continuing into the beginning of the new millennium, several companies started offering standalone cyber-insurance, which sat the frame for the current insurance product. However, as found in the papers [PO1,ST1,GN1] both the US and the european market have not managed to reach its promising potential. Companies are weekly suffering from successful attacks, but most firms still have not acquired cyber-insurance. The cyber-insurance market seem to have a huge potential, but needs some new thinking to fully take advantage of it. We will take a new approach where we focus on finding network structures that will be beneficial for cyber-insurance, and see if it i possible for insurers to force these structures to evolve.

2 Cyber-insurance network structures

Just like stock markets and airline routes, the cyber-insurance market can be described using graphs. The structure that will evolve is dependent on all the nodes and how they connect with each other. The insurer can determine the cost of establishing a link, and thus determine which nodes will connect to eachother. This is what we will try to achieve in our models. However, first we need to shed light on what kind of graph structures that would be desirable to force upon the cyber-insurance market.

To find the proper structure, many different scenarios should be covered. In a network an agent's actions are influenced by its neighborhood structure, i.e. the network connections will affect each individual agent's payoff, meaning that agents are dependent on eachother, and the probability of cascading failures are highly relevant. -If one or more fails, e.g. bankruptcy, failure to deliver at the expected time, system shut down, higher cost etc, then the whole network will be affected. In this case there are several types of networks to consider, every social and economic interaction where an agent's well-being is dependent on externalities as well as on his own actions, is a network worth considering.

We found several interesting papers from evolutionary studies and disease epidemics, which described characteristics in different graph structures. The ones we found appropriate, were those which described the benefits of star- and clique-shaped graphs. These graphs showed characteristics that could be used to make it feasible for both the insurer to offer - and the customer to acquire insurance.

The paper [**?**] is about evolutionary dynamics and how some structures can amplify or sustain evolution and drift[3]. One aspect of cyber-insurance is risk, and knowledge of how, for example, viruses spread in a network and how to use graph structures to prevent both hackers from entering and virus from spreading, is important. Evolutionary dynamics, and the research of how mutant genes spread throughout a population, as described in the paper, is analogous to this issue. If we can determine some structures where certain nodes are advantageous/disadvantageous, then these structures will have imporant properties, such as sustaining viruses from spreading, or amplify the incentive for obtaining cyber-insurance.

The paper [**?**], shows that mutants inserted into a circulation graph, will have a fixation probability equal to

$$p_1 = \frac{(1 - \frac{1}{r})}{(1 - \frac{1}{r^N})} \tag{1}$$

Where r represents the relative fitness of the mutant i.e the agents security level, if it is advantageous it will have a certain chance of fixation, and disadvantageous mutants will have a chance of extinction. A circulation graph is a graph that satisfies these two properties:

[3] Drift is the opposite of selective evolution, it is when the network/structure evolve and change at random

1. The sum of all edges leaving a vertex is equal for all vertices
2. The sum of all edges entering a vertex is equal for all vertices

A clique is a good example of a circulation graph, and the probability of fixation is as in Eq. (**??**). The fixation probability determines how probable it is that the whole network will eventually be "infected" by the mutant. Which means that it determines the rate of evolution, which relies on both the size of the network and the evolution speed. If the relative fitness of the nodes is high, then the probability of fixation will be low. A probability equal to one means that every node in the network will eventually be affected by the mutant.

An essential part of cyber-insurance is as mentioned earlier, for the insurer to be able to calculate the overall risk of the instance to be insured. Since the probability of fixation can be calculated in circulation graphs, if the insurer knows that the instance is part of a circulation graph, it is possible for the insurer to calculate the probability of fixation in that network. If we can find graphs with an fixation probability that exceeds Eq.(**??**) it is even better, because then the insurer is not only able to calculate the overall probability of fixation, but also to show that the probability of fixation is higher than the one for circulation graphs.

[**?**] shows that such graphs exist, and one example is the star topology. In this topology the fixation probability is as shown in Eq.(**??**), or more generally Eq.(**??**).

$$p_2 = \frac{(1 - \frac{1}{r^2})}{(1 - \frac{1}{r^{2N}})} \tag{2}$$

.

$$p_k = \frac{(1 - \frac{1}{r^k})}{(1 - \frac{1}{r^{kN}})} \tag{3}$$

When comparing Eq.(**??**) and Eq.(**??**), we see that the selective difference is amplified from r to r^2, i.e. a star acts as an evolutionary amplifier, favoring advantageous mutants and inhibiting disadvantageous mutants.

There are other graphs where the fixation probability is equal to **??**, examples are super-stars, such as funnels and metafunnels. These are just more complex star networks. This paper shows that as N gets large, the super-stars will have a fixation probability, for an advantageous mutant, that converges to 1, and for a disadvantageous mutant converges to 0. As exemplified earlier in this chapter, we know that there are many topologies in our society that are so called scale-free graphs. These graphs have most of their connectivity clustered in a few vertices, which are very similar to a network interconnected by multiple stars, these networks can also be considered as potent selection amplifiers.

The paper [**?**] present interesting results regarding network formation games. The authors set up a game where the nodes benefit from direct links, but these links also expose them to risk. Each node gains a payoff of a per link it establishes, but it can establish a maximum of δ links. A failure occurs at a node with probability q, and propagates on a link with probability p. If a node fails, it

will receive a negative payoff of b, no matter how many links it has established. The characteristics of this game is transferable to how we expect nodes in a cyber-insurance network to interact with eachother. Therefore, the results of the overall payoff change according to different collection of participants.

The results from the model presented by Blumen et.al. shows a situation where clustered graphs achieve a higher payoff when connected to trusted nodes, compared to when connecting with random nodes. Unlike in anonymous graphs, where nodes connect to each other at random, nodes in these graphs share some information with their neighbors, which is used when deciding whether to form a link or not. To further explain these results, they show that there exists a critical point, called *phase transition*, which occurs when nodes have a node degree of $\frac{1}{p}$. At this point a node gets a payoff of $\frac{a}{p}$, and to further increase the payoff the node needs to go into a region with significantly higher failure probability. Because once each node establishes more than $\frac{1}{p}$ links, the contagious edges will with high probability form a large cluster, which results in a rise in probability of node failure, and reduces the overall welfare. From this the paper states that when the minimum welfare exceeds $(1 + f(\delta) * \frac{a}{p})$ we have reached *super-critical payoff*. Otherwise it is called *sub-critical payoff*. Further Easley et.al, show that the only possible way of ending up with super critical payoff, is by forming clustered networks consisting of cliques with slightly more than $\frac{1}{p}$ nodes. However, if the nodes form an anonymous market, by random linking, they can only get sub-critical payoff. In other words, if the nodes can choose who they connect with, and by doing so, create trusted clustered markets, they can achieve a higher payoff by exceeding the critical node degree point.

From an insurer's point of view. If an insurance company could identify these star structures, and force them to end up in the socially optimal equilibrium, i.e. minimize the overall cost of link establishment, it would have been very beneficial for both the insurer and the customers. First of all, if the insurer could identify these structures, he could calculate the overall probability of fixation by a contagions node(virus, worm, trojan or other failures). If one could ensure that the center node is protected, one could also calculate the probability of the contagions node being extinguished from the network, and possibly being able to ensure that the network is secure, at least with high probability. One possibility of achieving this could be by offering very cheap insurance to the leaf nodes, and giving the center node an incentive to acquire security products by informing the center node about the probability of failure unless he acquires security, and offer him a decent rebate if he acquires the security product, and a very expensive insurance if not. In this way the insurer could force a rational center node into getting both insurance and a security product, and thus increase the security in the whole network.

This is a simple scenario, analyzing an exogenous network formation[4], but it shows how an insurer can force a star network to end up in the social optimal

[4] Exogenous: The network formation is given. Endogenous: The structure originates from within the network, i.e. the opposite of exogenous

cost equilibrium. Leading to overall higher security for in the network. We also showed how the insurer could calculate the probabilities of fixation in circulation, star, funnel, meta-funnel and super-star graphs. Can the insurer force cyber-insurance networks to evolve into any of these structures, and at the same time separate the nodes into trusted and untrusted environments? If so, this could contribute significantly to solving the problems of cyber-insurance. The problems of information asymmetry and interdependent risk is reduced. Because, if the insurer knows the network structure, he can calculate the probabilities of failure and catastrophic events. If the network is a star and the insurer can ensure that the center node is secure, the interdependent risk problem is limited to the security of the center node.

2.1 Research Question

Until now, our thesis has introduced cyber-insurance, presented related work on the issues regarding cyber-insurance and this chapter has presented the properties of different graph structures and briefly introduced the idea of network formation. Generally, the papers in the related work section have presented different models for solving the problems with cyber-insurance. Nevertheless, as we have seen, the cyber-insurance market still fails to evolve, despite all the solutions presented in the different papers. This is why we have chosen to take a different approach. In this chapter, we have shown some structures, especially the star and clique, which could generate benefit for both the insurer and customers in a cyber-insurance market. We will combine the knowledge of these structures and network formation games to investigate networks consisting of nodes, insured or not, wanting to increase their payoff by establishing links with eachother. Is it possible for the insurer to force these networks to evolve endogenously into these structures? We will focus on how the insurer can determine the resulting formation by adjusting the parameter he can control, i.e. the insurance cost. We know that if the insurance premium is too high, no one will buy it. On the other hand, if it is too low, everyone would benefit from having insurance, and insured nodes will make risky decisions, such as connecting to risky nodes. We will try to determine whether it is possible to find the intersections, where the desired structures will evolve, and both the insurer and their customers will benefit from this.

2.2 Autonomous Systems

In this section we will consider the case when the Hamiltonian $H(x)$ ...

The General Case: Nontriviality. We assume that H is (A_∞, B_∞)-subquadratic at infinity, for some constant ...

Notes and Comments. The first results on subharmonics were ...

Proposition 1. *Assume* $H'(0) = 0$ *and* $H(0) = 0$. *Set* ...

Proof (of proposition). Condition (8) means that, for every $\delta' > \delta$, there is some $\varepsilon > 0$ such that ... □

Example 1 (External forcing). Consider the system ...

Corollary 1. *Assume H is C^2 and (a_∞, b_∞)-subquadratic at infinity. Let ...*

Lemma 1. *Assume that H is C^2 on $\mathbb{R}^{2n}\backslash\{0\}$ and that $H''(x)$ is ...*

Theorem 1 (Ghoussoub-Preiss). *Let X be a Banach Space and $\Phi : X \to \mathbb{R}$ ...*

Definition 1. *We shall say that a C^1 function $\Phi : X \to \mathbb{R}$ satisfies ...*

3 Fine Tuning of the Text

The following should be used to improve the readability of the text:

`\,`	a thin space, e.g. between numbers or between units and numbers; a line division will not be made following this space
`--`	en dash; two strokes, without a space at either end
`␣--␣`	en dash; two strokes, with a space at either end
`-`	hyphen; one stroke, no space at either end
`$-$`	minus, in the text *only*

Input

```
21\,$^{\circ}$C etc.,
Dr h.\,c.\,Rockefellar-Smith \dots
20,000\,km and  Prof.\,Dr Mallory \dots
1950--1985 \dots
this -- written on a computer -- is now printed
$-30$\,K \dots
```

Output

21 °C etc., Dr h. c. Rockefellar-Smith ...
20,000 km and Prof. Dr Mallory ...
1950–1985 ...
this – written on a computer – is now printed
−30 K ...

4 Special Typefaces

Normal type (roman text) need not be coded. *Italic* (`{\em <text>}` better still `\emph{<text>}`) or, if necessary, **boldface** should be used for emphasis.

`{\itshape Text}`	*Italicized Text*
`{\em Text}`	*Emphasized Text – if you would like to emphasize a* definition *within an italicized text (e.g. of a* theorem*) you should code the expression to be emphasized by* `\em`.
`{\bfseries Text}`	**Important Text**
`\vec{Symbol}`	Vectors may only appear in math mode. The default LaTeX vector symbol has been adapted[5] to LLNCS conventions. `$\vec{A \times B\cdot C}` yields $\vec{A \times B\cdot C}$ `$\vec{A}^{T} \otimes \vec{B} \otimes \vec{\hat{D}}}$`yields $\vec{A}^{T} \otimes \vec{B} \otimes \vec{\hat{D}}}$

[5] If you absolutely must revive the original LaTeX design of the vector symbol (as an arrow accent), please specify the option `[orivec]` in the `documentclass` line.

5 Footnotes

Footnotes within the text should be coded:

```
\footnote{Text}
```

Sample Input

Text with a footnote`\footnote{The footnote is automatically numbered.}` and text continues ...

Sample Output

Text with a footnote[6] and text continues ...

6 Lists

Please code lists as described below:

Sample Input

```
\begin{enumerate}
  \item First item
  \item Second item
  \begin{enumerate}
    \item First nested item
    \item Second nested item
  \end{enumerate}
  \item Third item
\end{enumerate}
```

Sample Output

1. First item
2. Second item
   (a) First nested item
   (b) Second nested item
3. Third item

7 Figures

Figure environments should be inserted after (not in) the paragraph in which the figure is first mentioned. They will be numbered automatically.

Preferably the images should be enclosed as PostScript files – best as EPS data using the epsfig package.

If you cannot include them into your output this way and use other techniques for a separate production, the figures (line drawings and those containing

[6] The footnote is automatically numbered.

halftone inserts as well as halftone figures) *should not be pasted into your laser-printer output*. They should be enclosed separately in camera-ready form (original artwork, glossy prints, photographs and/or slides). The lettering should be suitable for reproduction, and after a probably necessary reduction the height of capital letters should be at least 1.8 mm and not more than 2.5 mm. Check that lines and other details are uniformly black and that the lettering on figures is clearly legible.

To leave the desired amount of space for the height of your figures, please use the coding described below. As can be seen in the output, we will automatically provide 1 cm space above and below the figure, so that you should only leave the space equivalent to the size of the figure itself. Please note that "`x`" in the following coding stands for the actual height of the figure:

```
\begin{figure}
\vspace{x cm}
\caption[ ]{...text of caption...}          (Do type [ ])
\end{figure}
```

Sample Input

```
\begin{figure}
\vspace{2.5cm}
\caption{This is the caption of the figure displaying a white
eagle and a white horse on a snow field}
\end{figure}
```

Sample Output

Fig. 1. This is the caption of the figure displaying a white eagle and a white horse on a snow field

8 Tables

Table captions should be treated in the same way as figure legends, except that the table captions appear *above* the tables. The tables will be numbered automatically.

8.1 Tables Coded with LaTeX

Please use the following coding:

Sample Input

```
\begin{table}
\caption{Critical $N$ values}
\begin{tabular}{llllll}
\hline\noalign{\smallskip}
${\mathrm M}_\odot$ & $\beta_{0}$ & $T_{\mathrm c6}$ & $\gamma$
  & $N_{\mathrm{crit}}^{\mathrm L}$
  & $N_{\mathrm{crit}}^{\mathrm{Te}}$\\
\noalign{\smallskip}
\hline
\noalign{\smallskip}
 30 & 0.82 & 38.4 & 35.7 & 154 & 320 \\
 60 & 0.67 & 42.1 & 34.7 & 138 & 340 \\
120 & 0.52 & 45.1 & 34.0 & 124 & 370 \\
\hline
\end{tabular}
\end{table}
```

Sample Output

Table 1. Critical N values

$M_\odot$	β_0	T_{c6}	γ	N_{crit}^{L}	N_{crit}^{Te}
30	0.82	38.4	35.7	154	320
60	0.67	42.1	34.7	138	340
120	0.52	45.1	34.0	124	370

Before continuing your text you need an empty line. ...

For further information you will find a complete description of the tabular environment on p. 62 ff. and p. 204 of the *LaTeX User's Guide & Reference Manual* by Leslie Lamport.

8.2 Tables Not Coded with LaTeX

If you do not wish to code your table using LaTeX but prefer to have it reproduced separately, proceed as for figures and use the following coding:

Sample Input

```
\begin{table}
\caption{text of your caption}
\vspace{x cm}     % the actual height needed for your table
\end{table}
```

8.3 Signs and Characters

Special Signs. You may need to use special signs. The available ones are listed in the *LaTeX User's Guide & Reference Manual* by Leslie Lamport, pp. 41 ff. We have created further symbols for math mode (enclosed in $):

`\grole`	yields	$\gtrless$	`\getsto`	yields	$\leftrightarrows$
`\lid`	yields	$\leqq$	`\gid`	yields	$\geqq$

Gothic (Fraktur). If gothic letters are *necessary*, please use those of the relevant $\mathcal{AMS}$-TEX alphabet which are available using the amstex package of the American Mathematical Society.

In LaTeX only the following gothic letters are available: `$\Re$` yields $\Re$ and `$\Im$` yields $\Im$. These should *not* be used when you need gothic letters for your contribution. Use $\mathcal{AMS}$-TEX gothic as explained above. For the real and the imaginary parts of a complex number within math mode you should use instead: `$\mathrm{Re}$` (which yields Re) or `$\mathrm{Im}$` (which yields Im).

Script. For script capitals use the coding

`$\mathcal{AB}$` which yields $\mathcal{AB}$

(see p. 42 of the LaTeX book).

Special Roman. If you need other symbols than those below, you could use the blackboard bold characters of $\mathcal{AMS}$-TEX, but there might arise capacity problems in loading additional $\mathcal{AMS}$-TEX fonts. Therefore we created the blackboard bold characters listed below. Some of them are not esthetically satisfactory. This need not deter you from using them: in the final printed form they will be replaced by the well-designed MT (monotype) characters of the phototypesetting machine.

`\bbbc`	(complex numbers)	yields $\mathbb{C}$	`\bbbf`	(blackboard bold F)	yields $\mathbb{F}$
`\bbbh`	(blackboard bold H)	yields $\mathbb{H}$	`\bbbk`	(blackboard bold K)	yields $\mathbb{K}$
`\bbbm`	(blackboard bold M)	yields $\mathbb{M}$	`\bbbn`	(natural numbers N)	yields $\mathbb{N}$
`\bbbp`	(blackboard bold P)	yields $\mathbb{P}$	`\bbbq`	(rational numbers)	yields $\mathbb{Q}$
`\bbbr`	(real numbers)	yields $\mathbb{R}$	`\bbbs`	(blackboard bold S)	yields $\mathbb{S}$
`\bbbt`	(blackboard bold T)	yields $\mathbb{T}$	`\bbbz`	(whole numbers)	yields $\mathbb{Z}$
`\bbbone`	(symbol one)	yields $\mathbb{1}$			

$$\mathbb{C}^{\mathbb{C}^{\mathbb{C}}} \otimes \mathbb{F}_{\mathbb{F}_{\mathbb{F}}} \otimes \mathbb{H}_{\mathbb{H}_{\mathbb{H}}} \otimes \mathbb{K}_{\mathbb{K}_{\mathbb{K}}} \otimes \mathbb{M}^{\mathbb{M}^{\mathbb{M}}} \otimes \mathbb{N}_{\mathbb{N}_{\mathbb{N}}} \otimes \mathbb{P}^{\mathbb{P}^{\mathbb{P}}}$$
$$\otimes \mathbb{Q}_{\mathbb{Q}_{\mathbb{Q}}} \otimes \mathbb{R}^{\mathbb{R}^{\mathbb{R}}} \otimes \mathbb{S}^{\mathbb{S}_{\mathbb{S}}} \otimes \mathbb{T}^{\mathbb{T}^{\mathbb{T}}} \otimes \mathbb{Z} \otimes \mathbb{1}^{\mathbb{1}_{\mathbb{1}}}$$

9 References

There are three reference systems available; only one, of course, should be used for your contribution. With each system (by number only, by letter-number or by author-year) a reference list containing all citations in the text, should be included at the end of your contribution placing the LaTeX environment `thebibliography` there. For an overall information on that environment see the *LaTeX User's Guide & Reference Manual* by Leslie Lamport, p. 71.

There is a special BibTeX style for LLNCS that works along with the class: `splncs.bst` – call for it with a line `\bibliographystyle{splncs}`. If you plan to use another BibTeX style you are customed to, please specify the option `[oribibl]` in the `documentclass` line, like:

```
\documentclass[oribibl]{llncs}
```

This will retain the original LaTeX code for the bibliographic environment and the `\cite` mechanism that many BibTeX applications rely on.

9.1 References by Letter-Number or by Number Only

References are cited in the text – using the `\cite` command of LaTeX – by number or by letter-number in square brackets, e.g. [1] or [E1, S2], [P1], according to your use of the `\bibitem` command in the `thebibliography` environment. The coding is as follows: if you choose your own label for the sources by giving an optional argument to the `\bibitem` command the citations in the text are marked with the label you supplied. Otherwise a simple numbering is done, which is preferred.

```
The results in this section are a refined version
of \cite{clar:eke}; the minimality result of Proposition~14
was the first of its kind.
```

The above input produces the citation: "... refined version of [CE1]; the minimality...". Then the `\bibitem` entry of the `thebibliography` environment should read:

The complete bibliography looks like this:[BO1]

References

[BO1] Bolot, Jean and Lelarge, Marc: Cyber insurance as an incentive for Internet security Managing information risk and the economics of security (2008) 269–290

[BO2] Lelarge, Mark, and Jean Bolot: Economic incentives to increase security in the internet: The case for insurance. INFOCOM (2009), IEEE.

[BO3] Bolot, Jean C and Lelarge, Marc A new perspective on internet security using insurance INFOCOM The 27th Conference on Computer Communications. IEEE (2008) 1948–1956

[RA1] Pal, Ranjan and Hui, Pan On Differentiating Cyber-Insurance Contracts A Topological Perspective Internet Management Conference (2013), IEEE.

[PO1] Ponemon Institute Second Annual Cost of Cyber Crime Study, Benchmark Study of U.S: Companies Ponemon Institute (2011)
[ST1] Evolving cyber cover `http://www.strategic-risk.eu/Journals/2012/02/22/i/j/w/RiskFinancing_Mar12.pdf` Accessed: 31/01/2013
[GN1] Graeme Newman Cyber liability in Europe: What insurers should knowL CFC Underwriter `http://www.cfcunderwriting.com/media/news-articles/european-cyber.aspx` Accessed: 14/02/2013
[BS1] Böhme, R. and Schwartz, G. Modeling cyber-insurance: Towards a unifying framework Proceedings of GameSec (2010)
[CE1] Clarke, F., Ekeland, I.: Nonlinear oscillations and boundary-value problems for Hamiltonian systems. Arch. Rat. Mech. Anal. **78** (1982) 315–333
[CE2] Clarke, F., Ekeland, I.: Solutions périodiques, du période donnée, des équations hamiltoniennes. Note CRAS Paris **287** (1978) 1013–1015
[MT1] Michalek, R., Tarantello, G.: Subharmonic solutions with prescribed minimal period for nonautonomous Hamiltonian systems. J. Diff. Eq. **72** (1988) 28–55
[Ta1] Tarantello, G.: Subharmonic solutions for Hamiltonian systems via a $\mathbb{Z}_p$ pseudoindex theory. Annali di Matematica Pura (to appear)
[Ra1] Rabinowitz, P.: On subharmonic solutions of a Hamiltonian system. Comm. Pure Appl. Math. **33** (1980) 609–633

Number-Only System. For this preferred system do not use the optional argument in the `\bibitem` command: then, only numbers will appear for the citations in the text (enclosed in square brackets) as well as for the marks in your bibliography (here the number is only end-punctuated without square brackets).

Subsequent citation numbers in the text are collapsed to ranges. Non-numeric and undefined labels are handled correctly but no sorting is done.

E.g., `\cite{n1,n3,n2,n3,n4,n5,foo,n1,n2,n3,?,n4,n5}` – where nx is the key of the x^{th} `\bibitem` command in sequence, `foo` is the key of a `\bibitem` with an optional argument, and `?` is an undefined reference – gives 1,3,2-5,foo,1-3,?,4,5 as the citation reference.

```
\begin{thebibliography}{1}
\bibitem {clar:eke}
Clarke, F., Ekeland, I.:
Nonlinear oscillations and boundary-value problems for
Hamiltonian systems.
Arch. Rat. Mech. Anal. {\bfseries 78} (1982) 315--333
\end{thebibliography}
```

9.2 Author-Year System

References are cited in the text by name and year in parentheses and should look as follows: (Smith 1970, 1980), (Ekeland et al. 1985, Theorem 2), (Jones and Jaffe 1986; Farrow 1988, Chap. 2). If the name is part of the sentence only the year may appear in parentheses, e.g. Ekeland et al. (1985, Sect. 2.1) The reference list should contain all citations occurring in the text, ordered alphabetically by surname (with initials following). If there are several works by the same author(s) the references should be listed in the appropriate order indicated below:

a) One author: list works chronologically;
b) Author and same co-author(s): list works chronologically;
c) Author and different co-authors: list works alphabetically according to co-authors.

If there are several works by the same author(s) and in the same year, but which are cited separately, they should be distinguished by the use of "a", "b" etc., e.g. (Smith 1982a), (Ekeland et al. 1982b).

How to Code Author-Year System. If you want to use this system you have to specify the option `[citeauthoryear]` in the `documentclass`, like:

```
\documentclass[citeauthoryear]{llncs}
```

Write your citations in the text explicitly except for the year, leaving that up to LaTeX with the `\cite` command. Then give only the appropriate year as the optional argument (i.e. the label in square brackets) with the `\bibitem` command(s).

Sample Input

```
The results in this section are a refined version
of Clarke and Ekeland (\cite{clar:eke}); the minimality result of
Proposition~14 was the first of its kind.
```

The above input produces the citation: "... refined version of Clarke and Ekeland (1982); the minimality...". Then the `\bibitem` entry of `clar:eke` in the `thebibliography` environment should read:

```
\begin{thebibliography}{}  % (do not forget {})
.
.
\bibitem[1982]{clar:eke}
Clarke, F., Ekeland, I.:
Nonlinear oscillations and boundary-value problems for
Hamiltonian systems.
Arch. Rat. Mech. Anal. {\bfseries 78} (1982) 315--333
.
.
\end{thebibliography}
```

Sample Output

References

Clarke, F., Ekeland, I.: Nonlinear oscillations and boundary-value problems for Hamiltonian systems. Arch. Rat. Mech. Anal. **78** (1982) 315–333