IHP 滞在記

渡辺　峻*

平成 28 年 4 月 11 日

昨年度末に一ヶ月ほど，パリで開催された Nexus of Information and Computation Workshop に参加してきた．このような長期型のワークショップに参加するのは初めてのことで，大変貴重な体験することができた． 今後同様なワークショップに参加する方の参考になればと思い，そこで見聞きしたことを書きとどめておくことにした．

まずはワークショップの概要について説明しておく． ワークショップは Institute of Henri Poincare (IHP) で開催された．IHP はパリ大学の数学科に属する施設で，研究者交流を目的に創られた．数学者の間では大変格式の高い場所だそうで，フィールズ賞受賞者の Cédric Villani 教授が所長を務めている．Villani 教授のご専門はボルツマン方程式や最適輸送の理論であるが，情報理論とも深く関わりのある研究をされており，IEEE IT Transaction にも論文を発表されている [1]． 普段は Lyon 大学に勤務されているため IHP にはいらっしゃらなかったが，月に何度か IHP を訪れるようで，筆者も廊下ですれちがう機会があった． 噂通り独特な雰囲気を醸し出しており，実際にお目にかかることができ大変感激した．

ワークショップのオーガナイザは，Mark Bravermen (Princeton University)， Bobak Nazer (Boston University)，Anup Rao (University of Washington)， Aslan Tchamkerten (Telecom Paristech) の四名である．聞いた話によると，2012 年頃から企画を始めていたそうで，開催日までに陳腐化してしまわないワークショップテーマを考えるのに苦慮したそうである． 最初 IHP から Tchamkerten へワークショップを企画するよう依頼があり，Tchamkerten と懇意だった Nazer が企画に加わり，コンピュータサイエンスとの交流プログラムにするために，Braverman と Rao がオーガナイザに加わったとのことである．ワークショップは２ヶ月間に渡り，４つのサブテーマ（Distributed Computation, Fundamental Inequalities, Inference Problems, Secrecy and Privacy）のワークショップが 2 週間ずつ開催された．サブテーマごとに数名のサブオーガナイザがおり，各分野の専門家が招待され講演を行った[1]．筆者は Secrecy and Privacy のサブオーガナイザである Prakash Narayan 教授の計らいで，ワークショップに招待していただいた．

筆者は後半２つの Inference Problems と Secrecy and Privacy のワークショップに参加した．Inference Problems のワークショップでは，ビッグデータ等の影響もあり，large alphabet regime に関する講演が多かったように思われる．

Secrecy and Privacy のワークショップ一日目は Iftach Haltner（Tel Aviv University）と Leo Reyzin（Boston University）による，Pseudo-entropy と Pseudo-randomness に関するチュートリアル講演から始まった．前半は leftover hashing 等，情報理論的セキュリティでも馴染みのある話が多かったが，後半の計算量的な話は大変難解であった．この週のワークショップは前の週までの雰囲気とはうってかわり，講演中に質疑が応酬される非常にアクティブなワークショップとなった．特に，最

*東京農工大学，情報工学科，shunwata@cc.tuat.ac.jp

[1] ワークショップ全期間を通して，約 230 人の参加者がおり，日本人参加者は 3 人であった．

前列に席を構えていた Venkat Anantharam 教授は非常に難しい質問を浴びせており，まるで博士論文公聴会かのようであった．セッション終了後に Anantharam 教授に会う機会があったので挨拶したところ,「君の講演を楽しみにしている」と言われた．内心嬉しかった反面恐ろしくなり，その日の晩は必死で発表準備に取り組んだ．

Secrecy and Privacy のワークショップには，日本からは筆者の他に林正人先生が参加されていた．ワークショップ二日目は量子情報に関するセッションが組まれており，林先生の他に Andreas Winter や Stephanie Wehner が講演を行った．聴衆に量子情報関係者はあまりおらず，非専門家向けに説明するのに苦労されているようであった．林先生の講演は秘匿増強に関する御自身の一連の成果を整理したもので，先に古典の成果を説明し，量子の部分は古典のアナロジーで説明することで，量子情報関係者以外にも伝わるように上手く工夫されていた．

筆者はワークショップ三日目の午前中に，共同研究者の Himanshu Tyagi と分担でチュートリアル講演を行った．３コマ（50 分× 3）で情報理論的セキュリティのチュートリアルを行うことになっていたが，あまり多くのトピックを詰め込んでも聴衆に理解してもらえないことを懸念し，基本事項の説明に加え，筆者らの secret key agreement と secure computing に関する成果 [2] を暗号コミュニティの研究者に宣伝することに焦点を絞ることにした．講演は概ね好評だったようであり，講演中にも活発な質問があった．特に secure computing は暗号コミュニティの縄張りであるため，非常に厳しい質問が多かった．また，想定していた以上に時間がなく講演は予定通りには進まなかったが，研究成果を宣伝するという目的は達成できたように思う．三日目の午後は Imre Csiszár 教授による講演があった．内容自体は既に知っている話が多かったが，皆が知っている有名な結果にこれほど多くの貢献をしていることに，改めて畏敬の念を覚えた．

翌日のワークショップ四日目の午前中にはセッションの座長を務めた．このセッションの一件目の発表は Stefan Dziembowski による side-channel attack に関するモデリングの話，二件目の発表は Sennur Ulukus によるマルチユーザ無線ネットワークにおける secure degree of freedom (DoF) の話であった．暗号コミュニティの研究者は AWGN にあまり馴染みがなく，DoF を説明するのに非常に苦労されていた．このセッションは質疑応答がヒートアップしたため，規定の時間内にセッションを切り上げることができなかった．しかしながら，それ以降のセッションでも時間を気にせずに質問を続けるという風潮になり，それはそれでよかったのではないかと考えている．

ワークショップ二週目は secure computing や privacy に関する講演が中心であった．後者の privacy は個人情報保護の必要性から近年活発に研究されている分野であり，Adam Smith による differential privacy に関するチュートリアル講演や，differential privacy の提唱者である Cynthia Dwork による講演があった．Privacy は security ほどコンセンサスのとれた評価基準が定まっておらず，物議を醸しているようであった．

IHP 滞在中には理論計算機科学の研究者と交流する機会があった．筆者は最近 communication complexity に関する研究に取り組んでいるため理論計算機科学の論文を読むことも多いが，情報理論の論文とは異なったスタイルで書かれていることから，いつも悪戦苦闘していた．特に，問題のモチベーションや問題設定の理解に苦しむことが多かった．今回分かったこととして，理論計算機科学の分野では新しい問題を作って解くというよりは，いくつかの重要かつ難しい問題（極端な例としては P-NP 問題）を解くためのステップやツールとして個々の問題に取り組むという姿勢を持っているようである．そのため，問題のモチベーションや設定等は研究者間で共通認識となっており，論文には明確な形で書かれないのかもしれない．このような研究コミュニティ間での文化の違いを知ることができたことも，今回の滞在の収穫であったと思う．

ワークショップ期間中，参加者には IHP にオフィスが割り当てられていた．参加者は講演を聞きに行ったり，オフィスに戻って仕事をしたり，いたるところにある黒板を使ってディスカッション

に勤しんだりしていた．オフィスは通常，二人でシェアされており，筆者は前述の Cynthia Dwork 博士と同室であった．話をするのは今回が初めてであったが，非常に気さくな方だった．普段は学会で顔を合わせる研究者たちと同じフロアにオフィスを構え一ヶ月過ごすうちに，彼らがまるで自分の同僚かのような錯覚を覚えた．

パリでの生活は英語がなかなか通じず困難を極めた．しかしながら，食べ物は格段に美味く，食事面では安定した生活を送ることができた．また，美術館巡りや観劇等，余暇にすることには事欠かなく，総合的には楽しい滞在であった．

今回のような長期滞在型のワークショップはそれほどメジャーではないものの，最近はいくつか開催されているようである．例えば，昨年 Bekeley の Simons Institute で同様なワークショップが開催されている[2]．このようなワークショップが研究促進にどの程度効果があるかは未知数ではあるが，通常の学会にはない多くの刺激が得られることは間違いない． 近い将来，日本でもこのようなワークショップが開催できるよう尽力したいと思う．

参考文献

[1] C. Villani, “A Short Proof of the Concavity of Entropy Power,” *IEEE Trans. Inform. Theory*, vol. 46, no. 4 July 2000.

[2] H. Tyagi and S. Watanabe, “Converses For Secret Key Agreement and Secure Computing,” *IEEE Trans. Inform. Theory*, vol. 61, no. 9, September 2015.

[3] S. Kudekar, S. Kumar, M. Mondelli, H. D. Pfister, E. Şaşoğlu, and R. Urbanke, “Reed-Muller Codes Achieve Capacity on Erasure Channels,” arXiv:1601.04689, 2016.

[2] このワークショップで Reed-Muller 符号が通信路容量を達成することの研究 [3] が始まったことは有名な話である．