**Quantum Computer:**

I studied verification of quantum computer. When the quantum devices are affected by noise, the computation outcome of quantum computer is not correct. Some of problems to be solved by the quantum computer cannot be checked by a classical computer. In this case, we need to verify the computation outcome. In the following paper, I proposed a method to guarantee the computation outcome of a quantum computer as Fig. 2. After this paper, many papers employed the method of this paper to verify quantum computers. Then, I extended my method so that it verifies the computation outcome even in the presence of noises. This method can be applied to an implementation of quantum computer.

M Hayashi, T Morimae

Verifiable measurement-only blind quantum computing with stabilizer testing

Physical review letters 115 (22), 220502 , 2015

This paper discussed the verification of measurement-based quantum computer.

K. Fujii and M. Hayashi, “Verifiable fault tolerance in measurement-based quantum computation,” Physical

Review A, Rapid Communication, Vol. 96, 030301(R) (2017).

This paper discussed the verification of fault tolerant measurement-based quantum computer. This method works even with the noise existence.

M. Hayashi and M. Hajduˇsek, “Self-guaranteed measurement-based blind quantum computation,” Physical

Review A, Vol. 97, 052308 (2018).

This paper discussed the self-testing of measurement-based quantum computer even with untrusted measurement devices.

**Quantum network coding:**

In the multiparty quantum information processing, we need a quantum network. However, a quantum network has a bottleneck. To improve the performance of the quantum network, we need to improve the bottleneck. My paper below started the analysis of quantum network coding for the first time as Fig. 3. After this paper, many researchers started to study quantum network coding. I proposed several protocols to improve the bottleneck in the quantum network. For example, in one of my protocols, I proposed an efficient use of quantum teleportation. This protocol resolves the bottleneck in the quantum butterfly network.

M Hayashi, K Iwama, H Nishimura, R Raymond, S Yamashita

Quantum network coding

Annual Symposium on Theoretical Aspects of Computer Science (STACS), 610-621 2007

This paper is the first paper of quantum network coding.

M. Hayashi, “Prior entanglement between senders enables perfect quantum network coding with modification,”

Physical Review A, Vol.76, 040301(R) (2007).

The proposed protocol in this paper has been experimentally implemented by Prof. Pan’s group in USTC.

S. Song and M. Hayashi, “Secure Quantum Network Code without Classical Communication,” IEEE Transactions on Information Theory, Volume: 66, Issue: 2, 1178 – 1192 (2020).

**Quantum statistics:**

In quantum statistics, I discussed the estimation of a quantum system and the estimation of a quantum state as Fig. 4. Usually, a quantum state is parameterized by multiple parameters. The best estimates of the respective parameters require the measurements of the respective physical quantities. However, they are non-commutative. Hence, we need to address simultaneous measurements of non-commutative physical quantities. Since their perfect simultaneous measurement is impossible, we need to optimize their approximate simultaneous measurement. In the following paper, I derived this optimization in a general way when the size of prepared quantum data is sufficiently large. This result gives the basis of the statistics of a quantum system from the side of the information science.

M Hayashi, K Matsumoto

Asymptotic performance of optimal state estimation in qubit system

Journal of Mathematical Physics 49, 102101, 2008.

This paper addresses the estimation of qubit system.

Y. Yang, G. Chiribella, and M. Hayashi, “Attaining the Ultimate Precision Limit in Quantum State Estimation,”

Communications in Mathematical Physics, vol. 368(1), 223 – 293 (2019).

This paper formalizes quantum state estimation with nuisance parameters.

J. Suzuki, Y. Yang, and M. Hayashi, “Quantum state estimation with nuisance parameters,” Journal of Physics

A: Mathematical and Theoretical, (In Press).

This is a systematic review for quantum state estimation.



**Classical statistics:**

I studied the estimation of classical Markov chains. In this study, I established information geometrical method for a Markovian chain. Based on this method, I proposed a very efficient method to estimate Markovian chains from the obtained data. Furthermore, as Fig. 5, I extended this method to the estimation of a hidden Markovian process, which has many applications in various areas, e.g., Bioinformatics, Econometrics, and Population genetics. This work has been published in the Annual of Statistics in 2016 and is considered as a representative work of information geometrical method in Markov chain. It was cited as a typical work of information geometry in Efron's paper ``Curvature and Inference for Maximum Likelihood Estimates'' and Amari's book ``Information geometry and its applications''. (Efron and Amari are the founders of information geometry.)

M Hayashi, S Watanabe

Information geometry approach to parameter estimation in Markov chains

The Annals of Statistics 44 (4), 1495-1535, 2016

This paper discusses estimation of Markovian process by using information geometry.

M. Hayashi, “Local equivalence problem in hidden Markov model,” Information Geometry, vol 2, 1 – 42

(2019).

This paper discusses the information-geometry structure of hidden Markov process.

**Finite-length Information Theory (classical):**

Traditionally, information theory has focused on the asymptotic behavior of codes with infinitely long block-length. Recently, many researchers became interested in the ultimate performance of finite-block-length code because nowadays it is possible to construct sufficiently long block length code in the channel coding. Hence, many people are interested in the second order analysis as the approximation of the finite-block length analysis. To resolve this problem, Dr. Hayashi established a systematic approach to second order analysis by combining the method of information spectrum and the central limit theorem. He applied this approach to the optimal second order coding rates for the source coding and the uniform random number generation. He also developed the second order universal coding theory for the source coding and the uniform random number generation.

Next, he tackled the second order coding rates for discrete memoryless (DMS) channel coding with energy constraint and the channel coding for additive white Gaussian noise (AWGN), which had been unsolved for 47 years. Due to the optimization of encoder, these problems cannot be solved by a simple application of the above approach. To resolve the difficulty, I revealed two notable relations between the channel coding and the binary hypothesis testing. Employing these relations, he derived the second order coding rates for these problems. Then, comparing the famous Gallager bound, he clarified the superiority of the second order analysis.

M. Hayashi, "Information Spectrum Approach to Second-Order Coding Rate in Channel Coding," IEEE Transactions on Information Theory, Vol.55, No.11, 4947 - 4966 (2009).

Using the information-spectrum method, this paper established the systematic method for second order theory for the channel coding. Then, this paper resolved the second order coding rate for AWGN channel and channel coding with energy constraint hat had been unsolved for 47 years. Although this problem was discussed by Polyanskiy, H. V. Poor, and S. Verdú (2010), this paper preceded them by one year. Due to the strength of this approach, many subsequent papers of the second order employ the proposed systematic method. Also, this paper clarifies the difference between the second order analysis and Gallager bound. Due to the above seminal contributions, this paper was awarded the 2011 IEEE Information Theory Society Paper Award.

**M. Hayashi**, “Second-order asymptotics in fixed-length source coding and intrinsic randomness,” [IEEE Transactions on Information Theory](https://ieeexplore.ieee.org/document/4626060), Vol. 54, No. 10, 4619–4637 (2008).

This paper proposes the use of the information spectrum method for a unified approach for second order asymptotics, which has been applied in many papers as a key idea.

**Finite-length Information Theory (quantum):**

I also extended this approach to the quantum setting. Firstly, he established the quantum version of the method of information spectrum for the binary hypothesis testing and the quantum data compression. Next, he extended it to the quantum channel coding, which has more serious difficulty due to the non-commutativity. To overcome it, he firstly invented a useful matrix inequality, which has often been referred to as the Hayashi-Nagaoka inequality" in many papers for quantum information theory. Using this inequality, he established the relations between the quantum channel coding and the binary quantum hypothesis testing as the quantum version of the above notable relations. Based on these relations, he established the method of the information spectrum for the quantum channel coding, and derived its error exponent, which is the best among the currently known ones. I also constructed quantum universal channel coding by using the group representation theory instead of type method.

Interestingly, this relation clarifies that the key point of second order analysis for quantum channel coding is the binary quantum hypothesis testing. The quantum difficulty for second order analysis is concentrated in the binary quantum hypothesis testing. Inventing the pinching technique, he made the second order analysis for the binary quantum hypothesis testing. Since the pinching technique is a powerful method to overcome the non-commutativity, this method has been often employed in several quantum paper recently. Applying this result, I derived the optimal second order coding rate for information reconciliation from quantum information, which derives the achievability of the optimal second order coding rate for the quantum channel coding.

M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," IEEE Transactions on Information Theory, Vol.49, No.7, pp.1753-1768 (2003).

Non-commutativity causes several kinds of difficulties in quantum information theory. To overcome this problem, this paper derived a novel matrix inequality, which has often been referred to as the Hayashi-Nagaoka inequality" in many papers for quantum information theory. This result brings us the quantum version of the information spectrum method.

As another contribution, this paper revealed two useful relations between channel coding and the binary hypothesis testing. One is the relation between existence of a good channel code and the binary hypothesis testing. The other is the relation between the optimal performance of channel code and the binary hypothesis testing. Due to their generality, both relations were used to several papers of channel coding, including the paper for the second order rate of channel coding.

M. Tomamichel and M. Hayashi, “A Hierarchy of Information Quantities for Finite Block Length Analysis of

Quantum Tasks,” IEEE Transactions on Information Theory, Vol. 59, No. 11, 7693 – 7710 (2013).

This paper established the foundation of finite-length theory of quantum system.

**Information theoretic security (classical):**

Information theoretic security is a new emerging research area of information theory. This area contains two important applied topics, one is the security analysis of the quantum key distribution, and the other is the security analysis of physical layer security, which contains the information theoretic security of wireless communication. To realize the security, we usually apply a hash function. Hence, we do not have the difficulty caused by decoding, which is the main difference from the error correcting code. Dr. Hayashi firstly pointed out that the useful relation between the wire-tap channel and the channel resolvability. Then, he derived an exponential decreasing rate of leaked information in the wire-tap channel model. Usually, we employ an auxiliary random variable as a scramble parameter for the code of wire-tap channel. All existing studies assume its perfect uniformity nevertheless it is quite difficult to guarantee it. To guarantee the security even with non-uniform auxiliary random variable, he invented a new security formula for wire-tap channel code based on the Renyi entropy of the non-uniform auxiliary random variable. Then, I succeeded in evaluating the security with such an imperfect case. Also, I proposed a practical code construction by using a linear code. These results removed several obstacles for real application of wire-tap channel model.

M. Hayashi, "General non-asymptotic and asymptotic formulas in channel resolvability and identification capacity and its application to wire-tap channel," IEEE Transactions on Information Theory, Vol. 52, No. 4, 1562-1575 (2006).

This paper pointed out the clear connection between the wire-tap channel coding and the channel resolvability. Using this connection, this paper derived an explicit exponent for leaked information by using Arimoto’s exponents. Also, combining the information spectrum approach, this paper revealed the capacity formula of general sequence of degraded wire-tap channels. Since this connection is a very powerful tool for ire-tap channel, many papers for wire-tap channel followed this idea to construct codes for wire-tap channel.

Further, this paper proved the conjecture for resolvability capacities for general sequence of channel, which had been an open problem proposed by Han-Verd´u in 1993 (13 years).

**M. Hayashi**, “Exponential decreasing rate of leaked information in universal random privacy amplification,” IEEE [Transactions on Information Theory](https://ieeexplore.ieee.org/document/5773033), Vol. 57, No. 6, 3989–4001 (2011).

This paper addresses security analysis when hash functions are applied. It applies hash function to wiretap channel, and constructs a practical code with small encoding and decoding time in finite-length setting

**Information theoretic security (quantum):**

I also discussed the secure key generation from random number partially leaked to the eavesdropper. In this model, he derived the tight exponential decreasing rate of leaked information under the application of a universal2 hash function. This bound also works for the finite-length bound for leaked information. To realize this protocol, it is enough to consider the calculation complexity of universal2 hash function. I also showed that universal2 hash function can be implemented by employing the Toeplitz matrix, whose multiplication has less calculation complexity. Therefore, his evaluation can be directly applied to the real physical layer security system. I also extended these result to the quantum setting by resolving the difficulties caused by the non-commutativity. Based on these results, I also established a security formula to guarantee the security of real quantum key distribution system that contains imperfectness in the photon source as well as in the optical communication channel.

M. Hayashi, “Practical Evaluation of Security for Quantum Key Distribution,” Physical Review A, Vol.74,

022307 (2006).

This paper discussed the second-order analysis for quantum key distribution with single-photon setting.

**M. Hayashi**, “Upper bounds of eavesdropper’s performances in finite-length code with the decoy method,” [Physical Review A](https://journals.aps.org/pra/abstract/10.1103/PhysRevA.76.012329), Vol.76, 012329 (2007); [Physical Review A](https://journals.aps.org/pra/abstract/10.1103/PhysRevA.79.019901), Vol.79, 019901(E) (2009).

This paper derives the relation between phase error probability and leaked information and provides a formula for leaked information with imperfect photon source in quantum key distribution in finite-length setting.

M. Hayashi, “Large deviation analysis for quantum security via smoothing of Renyi entropy of order 2,” IEEE

Transactions on Information Theory, Vol. 60, No. 10, 6702 – 6732 (2014).

This paper discusses the secure-random number generation in the quantum setting.