Proceedings of CONF-SPML 2026 Symposium: The 2nd Neural Computing and Applications Workshop 2025
DOI: 10.54254/2755-2721/2026.TJ30288

A Review of Quantum Key Distribution Protocols

Xiusi Yang

School of Precision Instrument and Opto-electronics Engineering, Tianjin University, Tianjin, China
yangxiusi916@icloud.com

Abstract. Against the backdrop where traditional cryptosystems are threatened by algorithms such as Shor and Grover, Quantum Key Distribution (QKD) technology serves as a next-generation security technology. However, the diversity of its protocols poses challenges to practical research, development, and application. This paper adopts a literature review approach to systematically classify the principles, characteristics, and application scenarios of mainstream protocols, including BB84, SARG04, and MDI-QKD, and also conducts a horizontal comparison of the differences between these protocols in terms of physical implementation, security, key rate, and anti-attack capability. The comparative study reveals that each type of protocol has its own advantages and disadvantages. For instance, BB84 needs to address transmission loss, SARG04 can resist Photon Number Splitting (PNS) attacks, and MDI-QKD is immune to measurement device attacks. Nevertheless, it is still necessary to select a protocol with high adaptability based on factors such as transmission distance, light source type, and environmental noise. This research lays a foundation for the practical application of QKD technology.

Keywords: QKD, BB84, SARG04, MDI-QKD

1. Introduction

In the digital era, information security has become a core pillar for critical fields such as financial transactions, government communications, and national defense. However, traditional cryptosystems are facing disruptive challenges brought by quantum computing technology. Specifically, Shor's algorithm can efficiently crack classical encryption algorithms like RSA and ECC, which are based on the problems of large number factorization and discrete logarithms. Meanwhile, Grover's algorithm can accelerate the brute-force cracking of symmetric cryptography, rendering the foundation of existing information security barriers precarious. Against this background, Quantum Key Distribution (QKD) technology has emerged. It takes the fundamental principles of quantum mechanics—rather than computational complexity—as the basis for security, and combines with the "one-time pad" encryption method. This enables information-theoretically secure data transmission and communication, making QKD a next-generation information security technology to counter future attack methods such as quantum computing [1]. Since Bennett and Brassard proposed the first practical QKD protocol (the BB84 protocol) in 1984, QKD technology has achieved significant progress in both theoretical security and experimental research. It has gradually moved from laboratory demonstrations to engineering and practical application, becoming one of the most

© 2025 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2755-2721/2026.TJ30288

promising applications for industrialization in the field of quantum information [2]. Different QKD protocols have distinct focuses in terms of principle design, technical characteristics, and application scenarios. Early Discrete-Variable QKD (DV-QKD) protocols, represented by BB84 and B92, realize basic key distribution based on the "prepare-and-measure" framework. The Entanglement-Assisted QKD (EA-QKD) protocol, initiated by the E91 protocol in 1991, enhances security through the verification of Bell's inequality. In the process of engineering advancement, Decoy-State QKD addresses the loophole of weak coherent light sources, while MDI-QKD can resist detector attacks. Continuous-Variable QKD (CV-QKD) features high key rates and compatibility with classical optical equipment, making it suitable for metropolitan area scenarios. Specialized protocols such as High-Dimensional QKD and Reference-Frame-Free QKD expand the multi-dimensional application scenarios of QKD technology to meet demands for high bandwidth and complex environments. Currently, while the diversity of QKD protocols enriches technical options, it also brings challenges in understanding and application. DV-QKD and CV-QKD exhibit significant differences in physical implementation (single-photon detection vs. coherent detection) and performance indicators (transmission distance vs. key rate). Entanglement-assisted and prepare-and-measure protocols have different emphases on security assumptions and engineering difficulty. Additionally, there is a lack of intuitive comparison regarding the optimization directions of protocols under different scenarios (e.g., long-distance with low loss vs. short-distance with high capacity). This paper employs a literature review method to briefly introduce several types of QKD protocols and explain their basic principles in a straightforward manner. Although QKD technology represents a next-generation security solution, the diversity of its protocols creates challenges for application. By systematically sorting out mainstream and specialized QKD protocols and conducting necessary horizontal comparisons, this paper clarifies the advantages, disadvantages, and scenario adaptation logic of each protocol. It provides insights for protocol selection in QKD technology practice, helps resolve key decision-making issues in its engineering implementation, and further promotes the transition of QKD technology from the laboratory to practical application. Ultimately, it offers technical application references for information security in critical fields such as finance, government affairs, and military.

2. The BB84 protocol

2.1. Principle

The BB84 protocol enables two communicating parties—Alice (the sender) and Bob (the receiver)—to share a secure key. In QKD communication, ciphertext is not transmitted; instead, keys are exchanged and negotiated between the two parties via a quantum channel [1]. Due to the indivisibility of single photons and the no-cloning theorem of quantum states, any observation conducted by an eavesdropper (Eve) on the single-photon states transmitted through the channel will introduce a bit error rate (BER) detectable by Alice and Bob. Since it is impossible to distinguish whether the BER is caused by Eve or channel noise, the BER is attributed to the presence of Eve in the channel. This compels Alice and Bob to discard the insecure shared key generated in this session, preventing Eve from obtaining the key shared by the two parties via the channel. Alice and Bob then retransmit until the BER of the sifted key falls below the error tolerance threshold. At this point, the conjugately encoded communication key can be exchanged through the quantum channel, thereby ensuring the absolute security of ciphertext communication over the classical channel [3]. On the basis of introducing the indivisibility of single photons and the no-cloning theorem of quantum states, the BB84 protocol leverages the intrinsic properties of quantum states—including

DOI: 10.54254/2755-2721/2026.TJ30288

wave nature, superposition, and instantaneous collapse upon measurement. Using single photons as information carriers, it realizes quantum teleportation-based key distribution through discussions on the BB84 protocol and Bell's inequality [4], thus guaranteeing the unconditional security of ciphertext communication over the classical channel.

2.2. Characteristics

2.2.1. System structure and two-node architecture

The two-node architecture consists of Alice (the sender) and Bob (the receiver). Alice randomly transmits single-photon states using two sets of non-orthogonal polarizers (rectilinear-basis and diagonal-basis), and Bob similarly randomly receives the single-photon states using the same two sets of non-orthogonal polarizers.

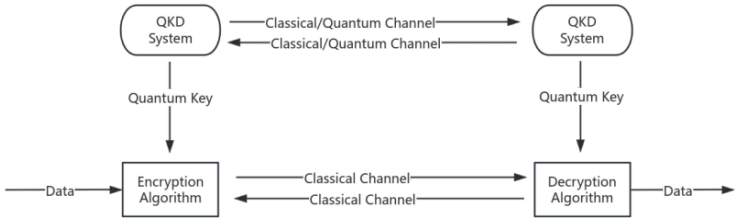

Figure 1. System structure [5]

The upper quantum channel is responsible for exchanging quantum keys, while the upper classical channel transmits information such as the bases of the two sets of non-orthogonal polarizers. The lower classical channel is used for transmitting the data ciphertext (see Figure 1). In the quantum channel segment, first, Alice randomly selects one of the two sets of polarizers to prepare single-photon states with different polarizations and sends them to Bob randomly. Bob then also randomly selects one of the two sets of polarizers to receive the single-photon states sent by Alice. In the classical channel segment, Alice and Bob compare their respective sequences of polarizer basis selections (rectilinear-basis "+" and diagonal-basis "×") via the upper classical channel. They retain data corresponding to consistent basis selections, which constitutes the sifted key. Subsequently, Alice and Bob each sample a small segment of data from the sifted key, transmit it via the classical channel, and compare the results. If the error rate exceeds the threshold, the communication is deemed insecure, and the key generated in this session is discarded. They then repeat the sampling and comparison process until the BER of the sifted key meets the error tolerance threshold. After error correction and privacy amplification, Alice and Bob share the same secure communication key via the quantum channel.

2.2.2. Summary

The BB84 protocol implements quantum key distribution using single-photon state transmission and does not require quantum entanglement. However, during fiber transmission, the extremely weak power of single-photon pulses makes them vulnerable to noise interference from the channel. Additionally, channel transmission loss limits the transmission distance of single-photon states, preventing them from being extended indefinitely. Eve can impersonate channel transmission loss to launch Photon Number Splitting (PNS) attacks. Therefore, secure communication will ultimately rely on quantum repeaters to realize quantum communication.

DOI: 10.54254/2755-2721/2026.TJ30288

3. The SARG04 protocol

3.1. Principle

In 2004, V. Scarani, A. Acin, G. Ribordy, and N. Gisin proposed the SARG04 protocol [6]. In terms of quantum processes, the SARG04 protocol is identical to the BB84 protocol. The difference between the two protocols lies in their operations on bases: In the SARG04 protocol, Alice defines four sets of non-orthogonal bases. Instead of disclosing the measurement basis used for each photon, she announces which of the four sets of non-orthogonal bases the photon's quantum state belongs to. Consequently, the probability that Bob can obtain an unambiguous result for each quantum state sent by Alice is 25%.

3.2. Characteristics

For quantum states containing two photons, since the SARG04 protocol uses non-orthogonal state encoding, even if Eve launches a PNS attack, she cannot obtain definite information when Alice announces the non-orthogonal bases—due to the inability to perfectly distinguish non-orthogonal states. This renders the attack ineffective. In contrast, in the standard BB84 protocol, Alice discloses orthogonal bases, allowing Eve to perfectly distinguish them and thus obtain all information. It is evident that even in the case of a two-photon source, the SARG04 protocol can effectively defend against PNS attacks and ensure information security. Furthermore, in a two-dimensional Hilbert space, to perform unambiguous quantum state discrimination on N linearly dependent qubits, at least N-1 copies of quantum states are required [7]. Therefore, the SARG04 protocol can generate secure keys from both single-photon and two-photon components [8].

3.3. Summary and application

3.3.1. Summary

First, the SARG04 protocol inherently possesses the property of resisting PNS attacks, which is the primary reason for its proposal. Owing to this property, when using a weak coherent light source, the SARG04 protocol exhibits significantly higher security than the traditional BB84 protocol, and its performance is comparable to that of the later proposed Decoy-State BB84 protocol. Second, the SARG04 protocol has a lower bit-sifting efficiency than the BB84 protocol, resulting in a final key generation rate that is only approximately 16.67%–50% of that of the BB84 protocol. Finally, due to the different channel noise tolerances of the SARG04 and BB84 protocols, the secure key rate and error threshold of the SARG04 protocol require independent theoretical analysis.

3.3.2. Application

The first application scenario is simple systems that use weak coherent light sources and cannot deploy decoy-state schemes. Before the maturity of decoy-state protocols, almost all QKD systems used weak coherent light sources instead of ideal single-photon sources. These weak coherent light sources emit multi-photon pulses, and if the BB84 protocol is used, the system security will decrease significantly. In this case, the SARG04 protocol can greatly improve system robustness without modifying hardware configurations. The second scenario involves extreme conditions, such as environments with extremely high detector noise or extremely high channel loss. Due to the unique exclusion logic in Bob's process of determining whether to retain qubits, the SARG04 protocol can

DOI: 10.54254/2755-2721/2026.TJ30288

exhibit stronger robustness than BB84 and still generate secure keys. The third scenario is applications requiring high security against multi-photon pulses. The design of the SARG04 protocol specifically addresses the PNS attack problem faced by multi-photon pulses, which is reflected in two aspects. First, the protocol's non-orthogonal encoding blocks the attack path of PNS. Practical QKD systems often use weak coherent light sources (which easily generate multi-photon pulses). Eve can split part of the photons from multi-photon pulses through PNS attacks and measure them to obtain keys after Alice and Bob announce their basis selections. However, the SARG04 protocol adopts four sets of non-orthogonal bases for encoding, and Alice only announces the non-orthogonal basis set to which the photon belongs (instead of the measurement basis of individual photons). Since non-orthogonal quantum states cannot be perfectly distinguished, even if Eve intercepts part of the photons in the multi-photon pulse, she cannot determine the specific quantum state of the photon or obtain complete key information, leading to the failure of the attack. Second, the source of secure keys covers multi-photon pulses. In contrast, in the BB84 protocol, only single-photon pulses can generate secure keys, while multi-photon pulses need to be discarded because they are vulnerable to PNS attacks. In the SARG04 protocol, however, both single-photon and two-photon pulses can generate secure keys. For two-photon pulses, Eve cannot obtain complete information by intercepting part of the photons. Bob can retain secure data through post-processing measures such as privacy amplification. Moreover, the proportion of pulses with more than 2 photons in weak coherent light sources is extremely low, which further ensures key security in multi-photon scenarios.

4. The MDI-QKD protocol

4.1. Overview

4.1.1. System vulnerabilities

Since Eve can control the quantum channel and send arbitrary signals to Bob, and use various dimensions related to the encoding dimension to obtain information, the measurement end of a QKD system is more vulnerable to attacks than the light source end. Take the fake state attack as an example: General QKD systems require the use of two gated-mode single-photon detectors. These devices have limited precision, and differences in Optical Path Length (OPL) can cause detector efficiency mismatch. By means of interception and retransmission, Eve can control the measurement results of the detectors [9]. In addition, there are attack methods such as double-click attacks [10], time-shift attacks [11], and detector control attacks. The defensive measures against these attacks may also be compromised, and combined with the inherent security loopholes and threats of the system, various system vulnerabilities are formed.

4.1.2. Development history

To address the vulnerabilities of all quantum devices in the system, the Device-Independent (DI) protocol was proposed [12,13]. However, this protocol imposes extremely high requirements on system efficiency (over 83%) and involves significant technical difficulties, resulting in a narrow scope of application. Researchers, including Hoi-Kwong Lo and Samuel L. Braunstein, proposed the Measurement-Device-Independent (MDI) protocol [14,15]. This protocol closes all vulnerabilities of measurement devices, is immune to various attacks on measurement devices, and solves the problem

DOI: 10.54254/2755-2721/2026.TJ30288

of low applicability of the DI protocol. It achieves a balance between security and application and has become a current research frontier and focus in the QKD field.

4.2. The decoy-state MDI-QKD protocol

The MDI-QKD protocol is an entanglement distribution protocol based on time reversal [16,17]. First, Alice and Bob act as light sources to encode four quantum states (the same as those in the BB84 protocol), which are then sent to a third party (Charlie). Charlie performs interference on the two received photons and obtains the selected Bell state through Bell-state measurement (BSM). Through this process, the originally uncorrelated qubits of Alice and Bob can become correlated. However, Charlie is completely untrusted, and Eve can manipulate Charlie. The specific process of the MDI-QKD protocol can be summarized as follows: Quantum state preparation: Alice (and Bob) uses Pol-M (Polarization Modulation) to randomly encode one of four polarization states, then uses Decoy-M (Decoy-State Modulation) to randomly modulate signal states and decoy states, and finally sends them to Charlie via their respective quantum channels. State measurement: Charlie performs BSM on the received optical pulses and announces the corresponding measurement results or invalid responses. Basis sifting: Based on the successful measurement results announced by Charlie, Alice and Bob disclose their basis selections and decoy-state selections. They retain data with consistent basis selections and discard the rest. One of Alice or Bob performs a bit-flipping operation according to the selected basis and the announced measurement results to obtain the sifted key. Parameter estimation: The decoy-state technique is used to calculate the response rate and error rate when Alice and Bob simultaneously send single-photon signals under different bases. Post-processing: Alice and Bob perform operations such as error correction and privacy amplification to obtain the final consistent secure key (the same as the post-processing steps of the BB84 protocol). The security of MDI-QKD lies in the following: Alice and Bob can judge the correlation of their bit data based on the BSM results announced by Charlie, and then generate a key through the post-processing process. Although Charlie knows the correlation of certain bit data, he still cannot obtain the specific bit values of the data. If Charlie attempts to obtain bit values by deviating from BSM methods, additional errors will be introduced, which can be detected by the two communicating parties. Theoretically, this can be explained using the virtual bit concept in GLLP analysis [18]: Assume that both the sender and receiver each have a virtual system, which is in an entangled state with the subsystem to be sent. This virtual system can determine which quantum state to prepare. The preparation process is reciprocal to Charlie’s BSM process, so the preparation process can be delayed. Therefore, the sender and receiver first send the subsystems to be transmitted to Charlie. Charlie then performs BSM on the received quantum states and announces the results. Finally, Alice and Bob measure their respective virtual systems. During this process, Charlie cannot obtain any bit of information about Alice and Bob, which proves that the MDI-QKD protocol is measurement-device-independent.

5. Discussion and outlook

5.1. Discussion

Traditional cryptosystems are threatened by Shor's and Grover's algorithms, which have led to the emergence of Quantum Key Distribution (QKD) technology. With quantum mechanics as its security foundation and combined with the "one-time pad" method, QKD achieves information-theoretic security. Since the proposal of the BB84 protocol in 1984, this technology has developed

DOI: 10.54254/2755-2721/2026.TJ30288

into a multi-protocol system. As the foundational protocol, BB84 uses single photons as carriers, and its security relies on the indivisibility of single photons and the no-cloning theorem of quantum states. However, it is vulnerable to interference, limited in transmission distance, and hard to resist Photon Number Splitting (PNS) attacks. The SARG04 protocol improves the basis announcement method, enabling it to resist PNS attacks and achieve better security when using weak coherent light sources, but it has the drawback of low bit-sifting efficiency. MDI-QKD closes measurement-side vulnerabilities by relying on a third party, making it suitable for commercial multi-node scenarios. Yet, it is plagued by issues such as limited key rates and the need for topology optimization. Currently, multiple QKD protocols coexist, but a series of challenges remain in its engineering application: it depends on immature quantum repeater technology, protocols have poor hardware compatibility, dynamic channels are prone to failure, and commercial applications face high costs and low standardization.

5.2. Outlook

To address the limitations of current protocols in long-distance transmission, the future development of QKD technology must focus on quantum repeater technology as the core breakthrough direction. The BB84 protocol suffers from limited transmission distance due to single-photon loss, and quantum repeaters can resolve this issue through entanglement swapping and quantum storage. Therefore, subsequent research should integrate the Bell inequality verification logic of Entanglement-Assisted QKD (EA-QKD) to develop high-efficiency quantum repeater nodes, reduce loss and noise during entanglement distribution, and promote the extension of QKD transmission distance. Meanwhile, the application of decoy-state technology in the MDI-QKD protocol can be further optimized to enhance the security and key rate of weak coherent light source systems in long-distance transmission, reducing reliance on ideal single-photon sources. This will provide a low-cost solution for the engineering of long-distance QKD and meet the demand for cross-domain secure transmission. As one of the core commercial technologies currently, the MDI-QKD protocol requires in-depth engineering optimization: designing modular third-party measurement nodes to improve deployment flexibility in multi-node networks, and developing miniaturized, low-power Bell-state measurement chips to adapt to the hardware requirements of commercial networks. In response to communication needs in different scenarios, it is necessary to clarify protocol selection strategies and unify the key management interfaces and hardware standards of various protocols to achieve interconnection among devices from different manufacturers. Additionally, low-cost core components should be developed to reduce the overall cost of commercial QKD systems and drive large-scale deployment. In future development, the virtual bit concept based on GLLP analysis will serve to improve the security proofs of new protocols, ensuring information-theoretic security at the theoretical level. For device vulnerabilities identified in engineering applications (such as detector time-shift attacks and side-channel attacks), it is essential to optimize the protocol's post-processing procedures, increase the frequency of dynamic bit error rate (BER) monitoring, and introduce accurate BER identification mechanisms to detect eavesdroppers' attacks in a timely manner. At the same time, strict basis-sifting strategies should be implemented to reduce security risks caused by device errors, ensuring that QKD technology can provide reliable security guarantees for critical fields.

DOI: 10.54254/2755-2721/2026.TJ30288

6. Conclusion

Since Bennett and Brassard proposed the BB84 protocol in 1984, the field of this technology has gradually developed into a multi-protocol system. It has moved from laboratory demonstrations to engineering and practical application, becoming an application with great industrialization potential in the field of quantum information. This paper systematically sorts out three types of mainstream QKD protocols. As the foundational protocol, the BB84 protocol adopts a "two-node architecture" and uses single photons as information carriers. Its security relies on the indivisibility of single photons and the no-cloning theorem of quantum states. However, it has limitations: single photons are vulnerable to channel noise interference, its transmission distance is limited, and it is difficult to resist Photon Number Splitting (PNS) attacks. Proposed in 2004, the SARG04 protocol shares the same quantum process as BB84, but its core improvement lies in announcing the non-orthogonal basis set to which a photon belongs instead of the individual measurement basis for each photon. This enables it to effectively resist PNS attacks and offers better security than the traditional BB84 protocol when using weak coherent light sources. Nevertheless, it has low bit-sifting efficiency—only about 16.67%-50% of that of BB84—and requires independent theoretical analysis of its secure key rate and error threshold. The MDI-QKD protocol was developed to address measurement-side vulnerabilities. It introduces a third party (Charlie) to perform Bell-state measurement, thereby closing all vulnerabilities of measurement devices and making itself immune to relevant attacks. However, its key generation efficiency is affected by Charlie's measurement efficiency, and the topology of multi-node networks still needs optimization. Currently, QKD technology exhibits a pattern of multi-protocol collaborative development, but the engineering application of various technologies still faces multiple challenges. In the future, the development of QKD technology needs to focus on several directions: taking quantum repeater technology as the core, integrating the logic of Entanglement-Assisted QKD (EA-QKD) to develop high-efficiency repeater nodes, and optimizing the application of decoy-state technology in MDI-QKD; advancing the engineering of MDI-QKD, designing modular measurement nodes, developing miniaturized and low-power chips, and unifying the key management interfaces and hardware standards of various protocols; relying on the virtual bit concept in GLLP analysis to improve the security proofs of new protocols, optimizing post-processing procedures, and enhancing bit error rate monitoring to address device vulnerabilities. Through these efforts, QKD technology will be promoted to provide more reliable security guarantees for critical fields such as finance and government affairs.

References

[1] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]//International Conference on Computers, Systems & Signal Processing. Bangalore, India: 1984: 175–179.
[2] Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices [J]. Reviews of Modern Physics, 2020, 92(2): 025002.
[3] MA Zhangchao, WANG Jianquan, MIAO Yajun, et al. Quantum Key Distribution Network Architecture and Its Standardization [J]. Radio Communications Technology, 2020, 46(6) : 665-666.
[4] BELL J S.On the Einstein-Podolsky-Rosen paradox [J]. Physics, 1964, 1: 195.
[5] Pu R. BB84 Protocol and Applications of QKD. Journal of Huaibei Normal University (Natural Sciences), 2022, 43(1): 69.
[6] Scarani, V. et al.: Quantum cryptography protocols Robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. 2004, 92, 057901–057904.
[7] Chefles A. Unambiguous discrimination between linearly dependent states with multiple copies. Phys. Rev. A, 2001, 64: 062305.
[8] Yao F. Some theoretical study on quantum communication. 2016, 19-20.

DOI: 10.54254/2755-2721/2026.TJ30288

[9] Ding H. Practical Security Analysis and Performance Improvement on Measurement-Device Independent Quantum Key Distribution. 2023.
[10] Beaudry N J, Moroder T, Lütkenhaus N. Squashing Models for Optical Measurements in Quantum Communication [J]. Physical Review A, 2008, 101(9): 093601.
[11] Qi B, Fung C-H F, Lo H-K, et al. Time-shift attack in practical quantum cryptosystems [J]. Quantum Information and Computation, 2007, 7(1-2): 73-82.
[12] Mayers D, Yao A. Quantum cryptography with imperfect apparatus [C]. Proceedings 39th Annual Symposium on Foundations of Computer Science, 1998: 503-509.
[13] Acín A, Brunner N, Gisin N, et al. Device-Independent Security of Quantum Cryptography against Collective Attacks [J]. Physical Review Letters, 2007, 98(23): 230501.
[14] Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2012, 108(13): 130503.
[15] Braunstein S L, Pirandola S. Side-channel-free quantum key distribution [J]. Physical Review Letters, 2012, 108(13): 130502.
[16] Biham E, Huttner B, Mor T. Quantum cryptographic network based on quantum memories, Physical Review A, 1996, 54(4): 2651.
[17] Inamori H. Security of Practical Time-Reversed EPR Quantum Key Distribution, Algorithmica, 2002, 34(4): 340.
[18] Gottesman D, Lo H K, Lütkenhaus N, et al. Security of quantum key distribution with imperfect devices [C]. International Symposium on Information Theory, 2004: 136.