On Intrinsic Information

Matthias Christandl[1]
Centre for Quantum Computation
DAMTP, University of Cambridge
Cambridge, CB3 9DQ, U.K.
e-mail: matthias.christandl@qubit.org

Renato Renner[2]
Computer Science Department
ETH Zürich
CH-8092 Zürich, Switzerland
e-mail: renner@inf.ethz.ch

Abstract — **We introduce the public Eve scenario and show that the secret key rate in this scenario is bounded by the intrinsic information. This elucidates previous results and gives new insights in the gap between formation and extraction of secret information.**

Intrinsic information, in its function as an upper bound on the secret key rate, is generalized to secret key agreement from arbitrary tripartite quantum states.

I. Public Eve Scenario

We modify the usual *secret key agreement* from a triple of random variables X, Y and Z and with secret key rate $S(X;Y||Z)$ [3], by imposing the following additional constraint on Eve: she can only publicly access her information Z. More precisely, she must choose a (probabilistic) function f which is then applied to Z^N to obtain $\bar{Z}$. The value $\bar{Z}$ together with the description of the function f is then broadcasted to Alice and Bob. We refer to this scenario as *Public Eve Scenario* with secret key rate $\tilde{S}(X;Y||Z)$.

The intrinsic information [4], similar as for the conventional secret key rate, is an upper bound for the secret key rate in the public Eve scenario.

Theorem I.1

$$S(X;Y||Z) \leq \tilde{S}(X;Y||Z) \leq I(X;Y \downarrow Z)$$

Conjecture I.2

$$\tilde{S}(X;Y||Z) = I(X;Y \downarrow Z)$$

Remark I.3 *Since secret key agreement is based on i.i.d. random variables, it is natural to pose the i.i.d. restriction on Eve's action as well. If this is done, Conjecture I.2 holds true and we obtain an operational definition of the intrinsic information as secret key rate in this scenario.*

Converse to secrecy extraction is the task of the formation of a probability distribution from secret key. We obtain the following bound for the formation rate $I_{\text{form}}(X;Y|Z)$ [5].

Theorem I.4

$$\tilde{S}(X;Y||Z) \leq I(X;Y \downarrow Z) \leq I_{form}(X;Y|Z)$$

The second inequality was proven in [5], where it was also demonstrated that strict inequality $S(X;Y||Z) < I(X;Y \downarrow Z)$ can occur. Our proof simplifies and shows that the gap between the formation of probability distributions and secrecy extraction may fall into two parts: the first one, between secret key rate and intrinsic information[5], can be removed by changing into the i.i.d public Eve scenario; a second gap may arise between intrinsic information and information of formation, its existence, however, is still unproven.

II. Secret key agreement from quantum states

Recently, secret key agreement from triples of random variables has been extended to quantum states ρ^{ABE} [1, 2]. In this setting, Alice, Bob, and Eve receive a number of identical copies of ρ^{ABE}. Alice and Bob are allowed to perform Local Operations and Classical Communication (LOCC) and may communicate via a public channel. They are then required to output an identical string that is secure against any strategy of Eve. The secret key rate is denoted by $K_D(\rho^{ABE})$. This scenario reduces to the one for random variables in the case of *classical* quantum states, i.e. $\rho^{ABE} = \sum_{xyz} P_{XYZ}(xyz)|x\rangle\langle x| \otimes |y\rangle\langle y| \otimes |z\rangle\langle z|$ for o.n. bases $\{|x\rangle\}, \{|y\rangle\}$ and $\{|z\rangle\}$ with rate $K_D(\rho^{ABE}) = S(X;Y||Z)$. The public Eve scenario, which we have introduced above, can also be generalized to the quantum case. Eve is then required to perform a joint POVM on her quantum state and to broadcast her measurement outcome. The secret key rate in this scenario is denoted by $\tilde{K}_D(\rho^{ABE})$.

Definition II.1 *The* intrinsic information *of a tripartite quantum state ρ^{ABE} is defined as*

$$I(\rho^{ABE}) := \inf_E I(A;B|Z)$$

where $I(A;B|Z) = \sum_z p_z I(A;B)_z$ with $I(A;B)_z := S(\rho_z^A) + S(\rho_z^B) - S(\rho_z^{AB})$ and $\rho_z^{AB} := \frac{1}{p_z}\mathrm{tr} E_z \rho^{ABE}$. The minimization ranges over all POVMs E with elements $\{E_z\}$.

This definition reduces to the usual definition for *classical* quantum states ρ^{ABE}.

Theorem II.2

$$K_D(\rho^{ABE}) \leq \tilde{K}_D(\rho^{ABE}) \leq I(\rho^{ABE}).$$

Both inequalities are sometimes strict.

References

[1] I. Devetak and A. Winter, Distillation of secret key from quantum states, *e-print quant-ph/0306078*, 2003.

[2] K. Horodecki, M. Horodecki, P. Horodecki and J. Oppenheim, Secure key from bound entanglement *e-print quant-ph/0309110*, 2003.

[3] U. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory, vol. 39, no. 3, pp. 733–742, 1993.

[4] U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 499–514, 1999.

[5] R. Renner and S. Wolf, New bounds in secret-key agreement: the gap between formation and secrecy extraction, In *Advances of Cryptology — EUROCRYPT 2003*, vol. 2656 of Lecture Notes in Computer Science, pp. 562–577, 2003.

[1] The author was supported by a DAAD Doktorandenstipendium and the EU project RESQ (IST-2001-37559).

[2] The author was supported by SNF No. 20-66716.01