Bound Information: The Classical Analog to Bound Quantum Entanglement

Nicolas Gisin, Renato Renner, and Stefan Wolf

Abstract. It was recently pointed out that there is a close connection between information-theoretic key agreement and quantum entanglement purification. This suggests that the concept of bound entanglement (entanglement which cannot be purified) has a classical counterpart: bound information, which cannot be used to generate a secret key by any protocol. We analyze a probability distribution which results when a specific bound entangled quantum state is measured. We show strong evidence for the fact that the corresponding mutual information is indeed bound. The probable existence of such information contrasts previous beliefs in classical information theory.

1. Information-Theoretic Key Agreement from Classical and Quantum Information

Assume that two parties Alice and Bob, who are connected by an authentic but otherwise completely insecure channel, are willing to generate a secret key (allowing them to communicate securely). More precisely, Alice and Bob want to compute, after some rounds of communication (where the random variable C summarizes the communication carried out over the public channel), strings S_A and S_B, respectively, with the property that they are most likely both equal to a uniformly distributed string S about which the adversary Eve has virtually no information. More precisely,

$$\text{Prob}\,[S_A = S_B = S] \geq 1 - \varepsilon \ , \quad H(S) = \log_2 |\mathbf{S}| \ , \quad \text{and} \quad I(S;C) < \varepsilon \qquad (1)$$

(where $\mathbf{S}$ is the range of S and $|\mathbf{S}|$ is its cardinality) should hold for some small ε. Note that the security condition in (1) is information-theoretic (sometimes also called unconditional): Even an adversary with unlimited computer power must be unable to obtain useful information. The Diffie-Hellman protocol [1] for instance achieves the goal of key agreement by insecure communication only with respect to computationally bounded adversaries.

It is a straight-forward generalization of Shannon's well-known impossibility result [13] that information-theoretic secrecy cannot be generated in this setting, i.e., from authenticity only: Public-key systems are never unconditionally secure. Hence we have to assume some additional structure in the initial setting, for instance some pieces of information given to Alice and Bob (and also Eve), respectively.

1.1. Classical Information

The general case where this information given to the three parties initially consists of the outcomes of some random experiment has been studied intensively [9], [10], [14]. Here, it is assumed that Alice, Bob, and Eve have access to realizations of random variables X, Y, and Z, respectively, jointly distributed according to P_{XYZ}. A special case is when all the parties receive noisy versions of a (binary) signal broadcast by some information source.

It was shown that if the setting is modified this way (where the secrecy condition in (1) must be replaced by $I(S;CZ) < \varepsilon$), then secret-key agreement is often possible. Shannon's pessimistic result now generalizes to the statement that the size of the resulting secret key S cannot (substantially) exceed the quantity

$$I(X;Y \downarrow Z) := \min_{XY \to Z \to \overline{Z}} I(X;Y|\overline{Z})$$

(where $XY \to Z \to \overline{Z}$ is a Markov chain) which was defined in [10] as the *intrinsic conditional information between X and Y, given Z.*

In the special case where the parties' initial information consists of the outcomes of many independent repetitions of the same random experiment given by P_{XYZ} (i.e., Alice knows $X^N := [X_1, X_2, \ldots, X_N]$, and similarly for Bob and Eve), the *secret-key rate* $S(X;Y||Z)$ was defined as the maximal key-generation rate (measured with respect to the number of required realizations of P_{XYZ}) that is asymptotically achievable (for $N \to \infty$). The above-mentioned result then implies

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

and it was conjectured that intrinsic information can always be distilled into a secret key, i.e., that $I(X;Y{\downarrow}Z) > 0$ implies $S(X;Y||Z) > 0$ [10], [14]. This conjecture was supported by some evidence given in [10]; however, it is the objective of this paper to give much stronger evidence for the opposite, i.e., that there exist types of intrinsic information *not* allowing for secret-key agreement. The motivation for the corresponding considerations comes from quantum mechanics or, more precisely, from the concept of *bound entanglement* in quantum information theory.

1.2. Quantum Information

When considering the model where certain pieces of information are given initially to the involved parties, it is a natural question where this information comes from. According to Landauer, information is always physical and hence ultimately quantum mechanical [7], [8]. Thus the random variables could come from measuring a certain quantum state $|\Psi\rangle$. In this case however it seems to be overly restrictive to force Alice and Bob to measure their quantum systems right at the beginning of the key-agreement process. It is possibly advantageous for them to carry out a protocol first (using classical communication and local quantum operations on their systems) after which they end up with a number of quantum bits in a maximally entangled state. Measuring them finally leads to a (classical) secret key. The first phase of this protocol is called *quantum (entanglement) purification.*

In order to understand what happens in a purification protocol and for which initial states such a protocol is at all possible, we recall some basic facts about quantum (information) theory[1]. In contrast to a classical bit (*Cbit* for short) which can take either of the values 0 or 1, a quantum bit (*Qbit*) can exist in a superposition of these two extremal states (with complex *probability amplitudes* a and b satisfying $|a|^2+|b|^2=1$):

$$|\psi\rangle = a|0\rangle + b|1\rangle \ .$$

When measuring this state with respect to the basis $\{|0\rangle, |1\rangle\}$, we obtain $|0\rangle$ with probability $|a|^2$ and $|1\rangle$ otherwise. All (pure) states of one Qbit can be represented as unit vectors in the Hilbert space $\mathbf{C}^2$.

A possible state of a system of two Qbits can be

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle =: |\psi_1\psi_2\rangle \ ,$$

which is simply the tensor product of the states $|\psi_1\rangle$ and $|\psi_2\rangle$ of the first and second Qbit, respectively. Such a state is called a *product state.* However, (normalized) linear combinations of quantum states lead to additional states; for instance,

$$|\psi^-\rangle := (|01\rangle - |10\rangle)/\sqrt{2}$$

is also a possible state of the two-Qbit system. This state is called *singlet state* and has the property that whenever the Qbits are measured with respect to the same basis, the outcomes are opposite bits. There is no classical explanation for this behavior which is called *(maximal) entanglement.* We conclude that two Qbits are not the same as "two times one Qbit."

As described above, the objective of Alice and Bob doing quantum purification is to generate two-Qbit systems in the state $|\psi^-\rangle$ (or in states very close to it) by classical communication and local quantum operations. The states they start with can for instance be their view of a pure state $|\Psi\rangle$ living in Alice's, Bob's, and a possible adversary Eve's (who is assumed to have total control over the entire environment) Hilbert spaces:

$$|\Psi\rangle \in H_{\text{Alice}} \otimes H_{\text{Bob}} \otimes H_{\text{Eve}} \ .$$

Then Alice and Bob's perspective

$$\rho_{AB} := \text{Tr}_{H_{\text{Eve}}}(|\Psi\rangle)$$

(the *trace* over Eve's space H_{Eve}) is generally a *mixed state.* In contrast to a pure state, which can be represented by a vector in a Hilbert space, a mixed state is described by a probability distribution over such a space[2]. A mixed state, such as ρ_{AB}, can be represented by a $(\dim H_{\text{Alice}})\cdot(\dim H_{\text{Bob}}) \times (\dim H_{\text{Alice}})\cdot(\dim H_{\text{Bob}})$

[1] For an introduction, see for example [11].

[2] Note that the notion of mixed state is actually rather information-theoretic than physical. Roughly speaking, a mixed state is a pure state that is only partially known.

matrix, namely the weighted sum (with respect to the probability distribution) of the projectors to the subspaces generated by the corresponding pure states. This matrix is called *density matrix*.

It is important to note that "purification," which transforms the mixed state ρ_{AB} into pure (singlet) states, actually means key agreement: Alice and Bob's final state is pure and hence not entangled with anything else, in particular not with anything under Eve's control. The adversary is out of the picture, whatever operations and measurements she performs.

Let us consider some properties of mixed states. A state ρ_{AB} which is *separable*, i.e., a mixture of product states, can be prepared remotely by purely classical communication. States that are not separable are called *entangled* and cannot be prepared this way. It is a natural question which states ρ_{AB} *can be purified* and which cannot. Separable states cannot be purified because of the property just described and because of the generalization of Shannon's theorem mentioned at he beginning of this paper: No information-theoretic key agreement is possible from authentic but public (classical) communication. On the other hand, if Alice's and Bob's subsystems are two-dimensional (i.e., Qbits) and entangled, then purification is always possible [4]. However, the surprising fact was recently discovered that the same is not true for higher-dimensional systems: There exist entangled states which cannot be purified [5]. (This follows from the fact that the eigenvalues of the so-called partial transposition of certain entangled density matrices ρ_{AB} are non-negative [12].) This type of entanglement is called *bound* (in contrast to *free* entanglement, which *can* be purified). From the perspective of classical information theory, the interesting point is that bound entanglement seems to have a classical counterpart with unexpected properties.

2. Linking the two Models

It was shown in [2] that there exists a close connection between the classical- and quantum-information-based secret-key-agreement scenarios, where the transition from quantum to classical information corresponds to certain measurements.

The following result was shown in [2]. Let $|\Psi\rangle$ be a pure quantum state of Alice, Bob, and Eve's systems, and let ρ_{AB} be the corresponding mixed state of Alice and Bob (obtained by tracing over Eve's space). Then the distribution P_{XYZ}, resulting from optimal measurement of $|\Psi\rangle$ by all the parties, has positive intrinsic conditional information, $I(X;Y\downarrow Z) > 0$, if and only if ρ_{AB} is an entangled state. By assuming "optimal measurement" we mean here the following statement. Whenever ρ_{AB} is entangled, but only then, there exist, for all possible measurements Eve can do (i.e., for all bases or, more generally, generating sets $\{|z\rangle\}$ she can choose to measure with respect to), measurement bases $\{|x\rangle\}$ and $\{|y\rangle\}$ for Alice and Bob, respectively, such that $I(X;Y\downarrow Z) > 0$ holds for the distribution $P_{XYZ}(x,y,z) := |\langle x,y,z|\Psi\rangle|^2$.

Given this result, it is natural to assume that the same is true also on the protocol level, i.e., that ρ_{AB} can be purified if and only if the corresponding distribution P_{XYZ} (again with respect to optimal measurements) satisfies $S(X;Y||Z) > 0$. However, this correspondence could not be generally proven so far. An interesting consequence of such a proof would be that bound entanglement has a classical counterpart, namely classical information which cannot be used for generating a secret key. We will call such information *bound*. The existence of bound information would contrast previous beliefs in classical information theory.

Although the connection between classical key agreement and quantum purification has not been proven in generality, we give, in the next section, new independent evidence that bound information does exist. The arguments are based on the analysis of a distribution coming from the "translation" of a bound entangled state described in [6].

3. Bound Information and Binarizations

We analyze a distribution that results from measuring a bound entangled quantum state, described in [6], with respect to the standard bases. Without even having a closer look at the state or the optimality of the measurements performed, we give direct evidence for the fact that this distribution yields an example of bound intrinsic information.

The distribution we consider is the following. Let $0 \leq \alpha \leq 3$.

X Y (Z)	1	2	3
1	(0) $2/21$	(1) $(5-\alpha)/21$	(2) $\alpha/21$
2	(3) $\alpha/21$	(0) $2/21$	(4) $(5-\alpha)/21$
3	(5) $(5-\alpha)/21$	(6) $\alpha/21$	(0) $2/21$

(This table reads as follows: We have for instance $P_{XYZ}(1,1,0) = 2/21$ and $P_{XYZ}(1,1,z) = 0$ for $z \neq 0$.) The corresponding quantum state $|\Psi_\alpha\rangle$ is known to be free entangled for $\alpha \in [0,1)$, bound entangled for $\alpha \in [1,2)$, and separable for $\alpha \in [2,3]$. Not surprisingly, the above distribution satisfies $I(X;Y{\downarrow}Z) > 0$ for $\alpha \in [0,2)$, but a secret-key agreement protocol is known only for $\alpha \in [0,1)$. In the following, we give evidence for the fact that there does not exist such a protocol for $\alpha \in [1,2)$. More precisely, we show the following facts for this case.

First, we prove that whenever the random variable Y is "binarized," i.e., sent through a binary-output channel $P_{\overline{Y}|Y}$ (or a ternary-output channel but where only two symbols are actually considered in the computation of the mutual information), then the intrinsic information vanishes (Proposition 1).

Proposition 2 on the other hand suggests that intrinsic information which does not resist any binarization must be bound: Whenever secret-key agreement is possible with X and Y and with respect to Z, then there exist binarizations of a certain number of repetitions of X and Y such that the intrinsic information remains positive.

These two propositions together suggest that the given distribution is indeed bound entangled. (However, note that they do not prove this.)

Proposition 1. *Assume the above distribution with* $\alpha \in [1, 2)$. *Let* $P_{\overline{Y}|Y}$ *be an arbitrary conditional distribution with* $\overline{\mathbf{Y}} = \{0, 1, \Delta\}$, *and let* E *be the event that* $\overline{Y} \in \{0, 1\}$. *Then* $I(X; \overline{Y} \downarrow Z \mid E) = 0$.

Proof. We only have to consider the case $\alpha = 1$. This implies the statement for all $\alpha \in [1, 2)$. Let the following channel $P_{\overline{Y}|Y}$ be given (where $\overline{\mathbf{Y}} = \{0, 1, \Delta\}$):

$$\begin{aligned} P_{\overline{Y}|Y}(0,1) &= x\ , \quad P_{\overline{Y}|Y}(0,2) = y\ , \quad P_{\overline{Y}|Y}(0,3) = z\ , \\ P_{\overline{Y}|Y}(1,1) &= u\ , \quad P_{\overline{Y}|Y}(1,2) = v\ , \quad P_{\overline{Y}|Y}(1,3) = w\ . \end{aligned}$$

Here, we have $x, y, z, u, v, w, x+u, y+v, z+w \in [0, 1]$. We get the following distribution $P_{X\overline{Y}Z|E}$ (to be normalized).

X / $\overline{Y}$ (Z)	1	2	3
0	(0) $2x$ (3) y (5) $4z$	(0) $2y$ (1) $4x$ (6) z	(0) $2z$ (2) x (4) $4y$
1	(0) $2u$ (3) v (5) $4w$	(0) $2v$ (1) $4u$ (6) w	(0) $2w$ (2) u (4) $4v$

The only symbol z of Z for which $I(X; \overline{Y}|Z = z, E) > 0$ holds is $z = 0$. Let us now consider a channel $P_{\overline{Z}|Z}$ with $\overline{\mathbf{Z}} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ and $P_{\overline{Z}|Z}(0, 0) = 1$. Furthermore, $P_{\overline{Z}|Z}(\overline{0}, 1) = c$ and $P_{\overline{Z}|Z}(\overline{1}, 1) = 1 - c$, and analogously for $Z = 2, 3, 4, 5$, and 6 with transition probabilities e, a, f, b, and d, respectively. Then we get for the column vectors of the $P_{X\overline{Y}|\overline{Z}=\overline{0}}$ matrix:

$$\left[2\begin{pmatrix}x\\u\end{pmatrix} + a\begin{pmatrix}y\\v\end{pmatrix} + 4b\begin{pmatrix}z\\w\end{pmatrix},\ 4c\begin{pmatrix}x\\u\end{pmatrix} + 2\begin{pmatrix}y\\v\end{pmatrix} + d\begin{pmatrix}z\\w\end{pmatrix},\ e\begin{pmatrix}x\\u\end{pmatrix} + 4f\begin{pmatrix}y\\v\end{pmatrix} + 2\begin{pmatrix}z\\w\end{pmatrix}\right].$$

Clearly, the three vectors are linearly dependent. We can assume that

$$\begin{pmatrix}x\\u\end{pmatrix} = \lambda_1\begin{pmatrix}y\\v\end{pmatrix} + \lambda_2\begin{pmatrix}z\\w\end{pmatrix}$$

holds for some $\lambda_1, \lambda_2 \in [0, \infty)$. (The other cases are analogous.)

Let $\vec{s} := \binom{y}{v}$ and $\vec{t} := \binom{z}{w}$. We then get for the above matrix

$$\left[(a + 2\lambda_1)\vec{s} + (4b + 2\lambda_2)\vec{t}, (2 + 4c\lambda_1)\vec{s} + (d + 4c\lambda_2)\vec{t}, (4f + e\lambda_1)\vec{s} + (2 + e\lambda_2)\vec{t}\right].$$

The corresponding distribution satisfies $I(X; \overline{Y}|\overline{Z} = \overline{0}, E) = 0$ if

$$\frac{a + 2\lambda_1}{4b + 2\lambda_2} = \frac{2 + 4c\lambda_1}{d + 4c\lambda_2} = \frac{4f + e\lambda_1}{2 + e\lambda_2}$$

holds. This is equivalent to

$$\begin{aligned} \lambda_1(2d - 16bc) + \lambda_2(4ac - 4) &= 8b - ad \ , \\ \lambda_1(4 - 4be) + \lambda_2(ae - 8f) &= 16bf - 2a \ . \end{aligned}$$

We show that this system is solvable, with $(a, b, c, d, e, f) \in [0, 1]^6$, for all $\lambda_1, \lambda_2 \in [0, \infty)$. For this, we prove that for all sufficiently large numbers $R > 0$, the equations are solvable for all pairs (λ_1, λ_2) on the path $(0, 0)$-$(R, 0)$-(R, R)-$(0, R)$-$(0, 0)$, and that the corresponding path in $[0, 1]^6$ is homeomorphic to S^1. Then the claim follows by a simple topological argument.

We only sketch the remainder of the proof. For $(\lambda_1, \lambda_2) = (0, 0)$, the equations are solvable by setting

$$d = f = 1 \ \text{ and } \ 8b = d \ . \tag{2}$$

For $(\lambda_1, \lambda_2) = (R, 0)$, where we assume R to be sufficiently large, a solution is given by

$$b \approx e \approx 1 \ \text{ and } \ d \approx 8c$$

(where additionally both equations of (2) should *not* be satisfied nor approximately satisfied). For $(\lambda_1, \lambda_2) = (R, R)$, the equalities are

$$\begin{aligned} R(2d - 16bc + 4ac - 4) &= 8b - ad \\ R(4 - 4be + ae - 8f) &= 16bf - 2a \end{aligned}$$

with a possible approximate solution

$$b \approx e \approx 0 \ , \quad c \approx d \approx 1 \ , \quad a \approx f \approx 1/2 \ .$$

Finally, the case $(\lambda_1, \lambda_2) = (0, R)$ can be solved by

$$a \approx c \approx 1 \ \text{ and } \ e \approx 8f \ .$$

When combining the solutions for the different cases, it is not difficult to see that there exists a path γ in $[0, 1]^6$ that, mapped to the (λ_1, λ_2) plane, exactly corresponds to the square $(0, 0)$-$(R, 0)$-(R, R)-$(0, R)$-$(0, 0)$. This is true for all sufficiently large R, and thus the argument is finished. □

Proposition 2. *Let X, Y, and Z satisfy $S(X; Y||Z) > 0$. Then there exist a number N and ternary-output channels $P_{\overline{X}|X^N}$ and $P_{\overline{Y}|Y^N}$ (with ranges $\overline{\mathbf{X}} = \overline{\mathbf{Y}} = \{0, 1, \Delta\}$ of $\overline{X}$ and $\overline{Y}$, respectively) such that the event E defined by $\overline{X} \neq \Delta \neq \overline{Y}$ has positive probability and $I(\overline{X}; \overline{Y} \downarrow Z^N \mid E) > 0$ holds.*

Proof sketch. Let $\varepsilon > 0$ to be determined later. Then, according to the definition of the secret-key rate $S(X; Y||Z)$, there exist N and a protocol that allows Alice and Bob for computing K-bit keys S_A and S_B for some $K \geq 1$ such that $S_A = S_B = S$ holds with probability at least $1 - \varepsilon$, where S is a uniformly distributed K-bit string with $H(S|CZ^N) \geq K - \varepsilon$ if C is the communication exchanged over the public channel. We construct new random variables $X' := [X^N, R_A]$ and $Y' := [Y^N, R_B]$, where R_A and R_B are random strings independent from each other and from all the rest, in such a way that we can assume the protocol to take X' and Y' as inputs and to be deterministic. Then there must exist a communication string c which occurs with positive probability and is such that $\text{Prob}\,[S_A = S_B = S \,|\, C = c] = 1$ and $H(S \,|\, Z^N, C = c) \geq K - \varepsilon/(1-\varepsilon)$ hold. Let us consider the following mappings of the ranges $\mathbf{X}'$ and $\mathbf{Y}'$ of X' and Y', respectively, to $\{0, 1, \Delta\}$. If the communication c is possible from a particular value $x' \in \mathbf{X}'$, then x' is mapped to the first bit of the resulting secret key S_A; otherwise, x' is mapped to Δ. The map from $\mathbf{Y}'$ to $\{0, 1, \Delta\}$ is defined analogously. Then the event E corresponds to the event that the communication C actually equals c, and has hence positive probability. Since R_A and R_B are independent of each other and of all the rest, these mappings are (probabilistic) binarizations $\overline{X}$ and $\overline{Y}$ of X^N and Y^N, respectively, satisfying $I(\overline{X};\overline{Y} \downarrow Z^N \,|\, E) > 0$ if ε is small enough. □

4. Concluding Remarks

We have given evidence that a certain specific probability distribution has so-called bound intrinsic information, i.e., information that cannot be used for generating a secret key by any protocol. Although the motivation for considering this particular distribution is that it results from measuring a bound entangled quantum state, our arguments are purely classical.

The existence of bound information would contrast previous beliefs in the context of unconditionally secure key agreement and be additional support for the close connection between information-theoretic key agreement and quantum purification conjectured in [2]. It should be pointed out that bound information represents one of the very few examples where quantum information theory initiates a new concept in classical information theory.

Acknowledgments

The authors thank Gilles Brassard, Nicolas Cerf, Claude Crépeau, Serge Massar, Ueli Maurer, Michele Mosca, Sandu Popescu, and Alain Tapp for interesting discussions. The first and the third author were partially supported by Switzerland's SNF, and the third author was partially supported by Canada's NSERC.

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol. 22, No. 6, pp. 644–654, 1976.

[2] N. Gisin and S. Wolf, Linking classical and quantum key agreement: is there "bound information"?, *Advances in Cryptology – Proceedings of Crypto 2000*, Lecture Notes in Computer Science, Vol. 1880, pp. 482–500, 2000.

[3] N. Gisin and S. Wolf, Quantum cryptography on noisy channels: quantum versus classical key agreement protocols, *Phys. Rev. Lett.*, Vol. 83, pp. 4200–4203, 1999.

[4] M. Horodecki, P. Horodecki, and R. Horodecki, Inseparable 2 spin 1/2 density matrices can be distilled to a singlet form, *Phys. Rev. Lett.*, Vol. 78, p. 574, 1997.

[5] P. Horodecki, Separability criterion and inseparable mixed states with positive partial transposition, *Phys. Lett. A*, Vol. 232, p. 333, 1997.

[6] P. Horodecki, M. Horodecki, and R. Horodecki, Bound entanglement can be activated, *Phys. Rev. Lett.*, Vol. 82, pp. 1056–1059, 1999. quant-ph/9806058.

[7] R. Landauer, Information is inevitably physical, *Feynman and Computation 2*, Addison Wesley, Reading, 1998.

[8] R. Landauer, The physical nature of information, *Phys. Lett. A*, Vol. 217, p. 188, 1996.

[9] U. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733–742, 1993.

[10] U. Maurer and S. Wolf, Unconditionally secure key agreement and the intrinsic conditional information, *IEEE Transactions on Information Theory*, Vol. 45, No. 2, pp. 499–514, 1999.

[11] A. Peres, *Quantum theory: concepts and methods*, Kluwer Academic Publishers, 1993.

[12] A. Peres, Separability criterion for density matrices, *Phys. Rev. Lett.*, Vol. 77, pp. 1413–1415, 1996.

[13] C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656–715, 1949.

[14] S. Wolf, *Information-theoretically and computationally secure key agreement in cryptography*, ETH dissertation No. 13138, ETH Zürich, 1999.

Nicolas Gisin
Group of Applied Physics
University of Geneva
CH-1211 Geneva, Switzerland.
`Nicolas.Gisin@physics.unige.ch`

Renato Renner
Department of Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland.
`renner@inf.ethz.ch`

Stefan Wolf
Centre for Applied Cryptographic Research
Department of Combinatorics and Optimization
University of Waterloo
Waterloo, ON N2L 3G1, Canada.
`swolf@cacr.math.uwaterloo.ca`