Towards Characterizing when Information-Theoretic Secret Key Agreement is Possible

Ueli Maurer and Stefan Wolf

Department of Computer Science
Swiss Federal Institute of Technology (ETH Zurich)
CH-8092 Zurich, Switzerland
E-mail addresses: {maurer,wolf}@inf.ethz.ch

Abstract. This paper is concerned with information-theoretically secure secret key agreement in the general scenario where three parties, Alice, Bob, and Eve, know random variables X, Y, and Z, respectively, with joint distribution P_{XYZ}, for instance resulting from receiving a sequence of random bits broadcast by a satellite. We consider the problem of determining for a given distribution P_{XYZ} whether Alice and Bob can in principle, by communicating over an insecure channel accessible to Eve, generate a secret key about which Eve's information is arbitrarily small. When X, Y, and Z are random variables that result from a binary random variable being sent through three arbitrary independent channels, it is shown that secret key agreement is possible if and only if $I(X;Y|Z) > 0$, i.e., under the sole condition that X and Y have some (arbitrarily weak) statistical dependence when given Z.

Keywords: Cryptography, Secret key agreement, Unconditional security, Information theory.

1 Introduction

Information-theoretically secure key agreement has recently attracted much attention in research in cryptography [9],[3],[7],[1],[5]. Two of the approaches that have been considered are based on quantum cryptography (e.g., see [1]) and on the exploitation of the noise in communication channels. In contrast to quantum cryptography, which is expensive to realize, noise is a natural property of every physical communication channel. This paper illustrates that noise in communication channels can be used for unconditionally secure secret key agreement and, furthermore, that it is advantageous to combine error control coding and cryptographic coding in a communication system.

We consider the classical cryptographic problem of transmitting a message M from a sender (referred to as Alice) to a receiver (Bob) over an insecure communication channel such that an enemy (Eve) with access to this channel is unable to obtain useful information about M. In the classical model of a cryptosystem (or cipher) introduced by Shannon [8], Eve has perfect access to the insecure channel; thus she is assumed to receive an identical copy of the ciphertext C received by the legitimate receiver Bob, where C is obtained by Alice as a function of the plaintext message M and a secret key K shared by Alice and Bob. Shannon defined a cipher system to be perfect if $I(M;C) = 0$, i.e., if the ciphertext gives no information about the plaintext or, equivalently, if M and C are statistically independent[1]. When a perfect cipher is used to encipher a message M, an enemy can do no better than guess M without even looking at the ciphertext C. Shannon proved the pessimistic result that perfect secrecy can be achieved only when the secret key is at least as long as the plaintext message or, more precisely, when $H(K) \geq H(M)$.

For this reason, perfect secrecy is often believed to be impractical. In [7] this pessimism has been relativized by pointing out that Shannon's apparently innocent assumption that, except for the secret key, the enemy has access to precisely the same information as the legitimate receiver, is very restrictive and that indeed in many practical scenarios, especially if one considers the fact that every transmission of data is ultimately based on the transmission of an analog signal subject to noise, the enemy has some minimal uncertainty about the signal received by the legitimate receiver(s).

Wyner [9] and subsequently Csiszár and Körner [3] considered a scenario in which the enemy Eve is assumed to receive messages transmitted by the sender Alice over a channel that is noisier than the legitimate receiver Bob's channel. The assumption that Eve's channel is worse than the main channel is unrealistic in general. It was shown in [7] that this assumption can be unnecessary if Alice and Bob can also communicate over a completely insecure (but authenticated) public channel.

For the case where Alice, Bob, and Eve know the random variables X, Y, and Z, respectively, with joint distribution P_{XYZ}, the rate at which Alice and Bob can generate a secret key by public discussion over an insecure channel is defined in [7] as follows.

Definition 1. The *secret key rate of X and Y with respect to Z*, denoted by $S(X;Y||Z)$, is the maximum rate at which Alice and Bob can agree on a secret key S such that the rate at which Eve obtains information about S is arbitrarily small. In other words, it is the maximal R such that for every $\varepsilon > 0$ and for all sufficiently large N there exists a protocol, using public discussion over an insecure but authenticated channel, such that Alice and Bob have the same key S with probability at least $1 - \varepsilon$, satisfying

$$\frac{1}{N} I(S; UZ^N) \leq \varepsilon \qquad \text{and} \qquad \frac{1}{N} H(S) \geq R - \varepsilon \ ,$$

where U denotes the collection of messages sent over the insecure channel by Alice and Bob, and $Z^N = [Z_1, \ldots, Z_N]$.

[1] We assume that the reader is familiar with the basic information-theoretic concepts. For a good introduction we refer to [2].

The following lower and upper bounds for the secret key rate are proved in [7]:

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

and

$$S(X;Y||Z) \leq \min\{I(X;Y), I(X;Y|Z)\} \; . \tag{1}$$

As already mentioned, it was shown by an example in [7] that the secret key rate $S(X;Y||Z)$ can be strictly positive even when both $I(X;Z) > I(X;Y)$ and $I(Y;Z) > I(Y;X)$. In this example a satellite broadcasts (symmetrically distributed and independent) random bits to Alice, Bob, and Eve over independent binary symmetric channels with bit error probabilities 20%, 20%, and 15%, respectively.

In this paper we consider the general scenario of three arbitrary independent memoryless discrete binary-input channels and prove that the secret key rate $S(X;Y||Z)$ is strictly positive unless Eve's channel is perfect or X and Y are independent. In other words, Alice and Bob can generate a secret key as long as they both receive an arbitrarily small but positive amount of information about the satellite signal and Eve has an arbitrarily small but positive amount of uncertainty about the satellite signal. For instance, even if Alice's and Bob's error probabilities are close to 50% and Eve's error probability is close to 0 in the case of binary symmetric channels, secret key agreement is possible. Similar to the general channel coding problem, where the existence of very good codes is known but no specific example has so far been constructed, the protocols for secret key agreement described here are not efficient in general. More efficient protocols for special cases are described in [6].

2 The Scenario and the Main Result

Let R be an arbitrary binary random variable, and let X, Y, and Z be arbitrary discrete random variables, generated from R by independent channels C_A, C_B, and C_E, respectively, i.e.,

$$P_{XYZ|R} = P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R} \; , \tag{2}$$

where $P_{X|R}$, $P_{Y|R}$, and $P_{Z|R}$ are the specifications of the channels C_A, C_B, and C_E, respectively. In other words, X, Y, and Z are statistically independent when given R. This scenario is illustrated in Figure 1. The following is a different but equivalent characterization for our scenario. There exist $0 \leq \lambda \leq 1$ and probability distributions $P_X^{(1)}$, $P_X^{(2)}$, $P_Y^{(1)}$, $P_Y^{(2)}$, $P_Z^{(1)}$, and $P_Z^{(2)}$ such that

$$P_{XYZ} = \lambda \cdot P_X^{(1)} \cdot P_Y^{(1)} \cdot P_Z^{(1)} + (1-\lambda) \cdot P_X^{(2)} \cdot P_Y^{(2)} \cdot P_Z^{(2)},$$

i.e., P_{XYZ} is the weighted sum of two "independent distributions" of XYZ. The results of this paper hold for all distributions with this property.

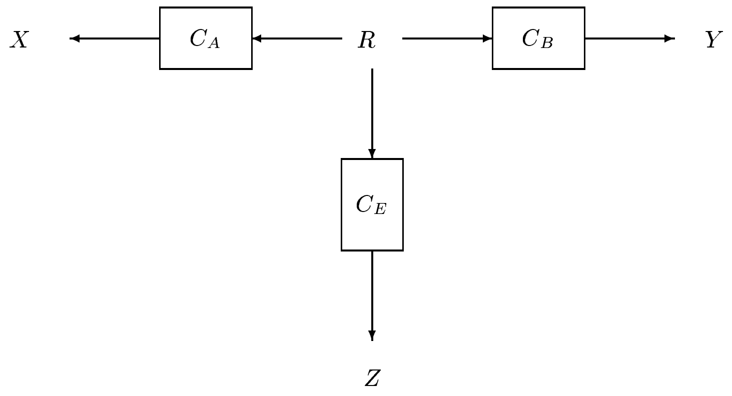

Fig. 1. The scenario of three independent channels.

We assume in the following that the distribution P_{XYZR} is publicly known. The main result of this paper is the following theorem which characterizes completely the cases for which $S(X;Y||Z) > 0$, i.e., for which secret key agreement is possible in principle.

Theorem 2. *Let R be a binary random variable, and let X, Y, and Z be discrete random variables (with ranges $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$, respectively), generated from R by independent channels, i.e., $P_{XYZ|R}(x,y,z,r) = P_{X|R}(x,r) \cdot P_{Y|R}(y,r) \cdot P_{Z|R}(z,r)$ for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$, $z \in \mathcal{Z}$, and $r \in \{0,1\}$. Then the secret key rate is strictly positive, i.e., $S(X;Y||Z) > 0$, if and only if $I(X;Y|Z) > 0$.*

Up to now it has been completely open whether this condition was sufficient. The *necessity* of the condition follows immediately from the upper bound in (1). The proof of Theorem 2 is subdivided into several steps stated below as lemmas. We begin with the special case where R is a symmetric binary random variable and all three channels are binary symmetric channels.

3 The Binary Symmetric Scenario

Let $P_R(0) = P_R(1) = 1/2$ and consider three independent binary symmetric channels C_A, C_B, and C_E with bit error probabilities α, β, and ε, respectively, i.e., we have

$$P_{X|R}(0,0) = 1 - \alpha, \quad P_{Y|R}(0,0) = 1 - \beta, \quad \text{and} \quad P_{Z|R}(0,0) = 1 - \varepsilon,$$

where $0 \leq \alpha < 1/2$, $0 \leq \beta < 1/2$, and $0 < \varepsilon \leq 1/2$.

Alice can send a randomly chosen bit C to Bob by the following protocol, which was already presented in [7]. Let N be fixed. Alice sends $[C \oplus X_1, C \oplus$

$X_2, \ldots, C \oplus X_N]$ over the public channel. Bob computes $[(C \oplus X_1) \oplus Y_1, \ldots, (C \oplus X_N) \oplus Y_N]$ and accepts if and only if this is equal to either $[0, 0, \ldots, 0]$ or $[1, 1, \ldots, 1]$. In other words, Alice and Bob make use of a repeat code of length N with the only codewords $[0, 0, \ldots, 0]$ and $[1, 1, \ldots, 1]$. Eve on the other hand can compute $[(C \oplus X_1) \oplus Z_1, \ldots, (C \oplus X_N) \oplus Z_N]$.

We show first that for all possible choices of α, β, and ε, in particular even if Eve's channel is superior to both Alice's and Bob's channel, Eve's error probability γ_N about the bit sent by Alice when using the optimal strategy for guessing this bit decreases asymptotically slower than Bob's error probability β_N for $N \longrightarrow \infty$, given that Bob accepts. (Note that γ_N is an *average* error probability, and that for a particular realization, Eve's error probability depends on the particular received string and on the message sent from Alice to Bob.)

Lemma 3. *For the above notation and assumptions, there exist b and c, $b < c$, such that $\beta_N \leq b^N$ and $\gamma_N \geq c^N$ for all sufficiently large N.*

Proof. We can assume that $\alpha = \beta$, i.e., that Alice's and Bob's channels are identical. If for example $\alpha < \beta$, Alice could (for the purpose of this proof) cascade her channel with another binary symmetric channel to obtain a situation corresponding to a binary symmetric channel with error probability β. This additional channel must be binary symmetric with error probability $(\beta - \alpha)/(1 - 2\alpha)$. (In a subsequent paper we will show that in this scenario, it is not necessary to assume $\alpha = \beta$.)

As in [7], let α_{rs} $(r, s \in \{0, 1\})$ be the probability that the single bit 0 sent by Alice is received by Bob as r and by Eve as s. Then

$$\begin{aligned}
\alpha_{00} &= (1-\alpha)^2(1-\varepsilon) + \alpha^2\varepsilon \ , \\
\alpha_{01} &= (1-\alpha)^2\varepsilon + \alpha^2(1-\varepsilon) \ , \\
\alpha_{10} &= \alpha_{11} = \alpha(1-\alpha) \ .
\end{aligned}$$

Let $p_{a,N}$ be the probability that Bob accepts the message sent by Alice. Then

$$\beta_N = \frac{1}{p_{a,N}} \cdot (\alpha_{10} + \alpha_{11})^N = \frac{1}{p_{a,N}} \cdot (2\alpha - 2\alpha^2)^N$$

and

$$\gamma_N \geq \frac{1}{2} \cdot \frac{1}{p_{a,N}} \cdot \binom{N}{N/2} \alpha_{00}^{N/2} \alpha_{01}^{N/2} \tag{3}$$

(we have assumed without loss of generality that N is even). The expression $\binom{N}{N/2} \alpha_{00}^{N/2} \alpha_{01}^{N/2} / p_{a,N}$ is the conditional probability that Bob receives the correct codeword and Eve receives the same number of 0's and 1's, given that Bob accepts. This is one of $N/2$ positive terms in γ_N, and hence clearly a lower bound on γ_N. In the case where Eve receives the same number of 0's and 1's, her error probability about the bit sent by Alice is $1/2$, independent of the guessing strategy she uses. Thus (3) gives a lower bound for Eve's average error probability for all possible strategies.

Stirling's formula (see for example [4]) states that $n!/((n/e)^n \cdot \sqrt{2\pi n}) \to 1$ for $n \to \infty$, and thus for sufficiently large even N we have

$$\binom{N}{N/2} = \frac{N!}{((N/2)!)^2} \geq \frac{1}{2} \cdot \frac{N^N \cdot \sqrt{2\pi N} \cdot e^N}{e^N \cdot (N/2)^N \cdot \pi N} = \frac{1}{\sqrt{2\pi N}} \cdot 2^N . \tag{4}$$

Hence

$$\gamma_N \geq \frac{1}{2} \cdot \frac{1}{p_{a,N}} \cdot \frac{1}{\sqrt{2\pi N}} \cdot 2^N \cdot \sqrt{\alpha_{00}\alpha_{01}}^N = \frac{C}{\sqrt{N}} \cdot \frac{(2\sqrt{\alpha_{00}\alpha_{01}})^N}{p_{a,N}}$$

for some constant C, and for sufficiently large N. For $0 < \varepsilon \leq 1/2$ we have

$$\sqrt{\alpha_{00}\alpha_{01}} = \sqrt{(1 - 2\alpha + \alpha^2 - \varepsilon + 2\alpha\varepsilon)(\alpha^2 - 2\alpha\varepsilon + \varepsilon)} > \alpha - \alpha^2 . \tag{5}$$

For $\varepsilon = 0$ equality holds in (5), and for $\varepsilon > 0$ the greater factor of the product is decreased by the same value by which the smaller factor is increased. Thus the product is greater. (For $\varepsilon = 1/2$ the factors are equal, and the left side of (5) is maximal, as expected.) From

$$(1-2\alpha+2\alpha^2)^N \leq p_{a,N} = (1-2\alpha+2\alpha^2)^N + (2\alpha-2\alpha^2)^N < 2\cdot(1-2\alpha+2\alpha^2)^N \tag{6}$$

(we have used that $1 - 2\alpha + 2\alpha^2 > 2\alpha - 2\alpha^2$ for $\alpha < 1/2$) we conclude that $\beta_N \leq b^N$ and $\gamma_N \geq c^N$, for some $c > b$, and for all sufficiently large N. □

The fact that Eve has a greater error probability than Bob when guessing C does not automatically imply that Eve has a greater uncertainty about this bit in an information theoretic sense, and that $S(X;Y||Z) > 0$. The next lemma shows that the result of Lemma 3 is sufficient for a positive secret key rate. It will also be used in the proof of Theorem 2.

Lemma 4. *Let X, Y, and Z be arbitrary random variables, and let C be a bit, randomly chosen by Alice. Assume that for all N, Alice can generate a message M from X^N (where $X^N = [X_1, \ldots, X_N]$) and C (and possibly some random bits) such that with some probability $p_N > 0$, Bob (who knows M and Y^N) publicly accepts and can compute a bit C' such that* $\text{Prob}[C \neq C'] \leq b^N$ *for some $b \geq 0$. If in addition, given that Bob accepts, for every strategy for guessing C when given M and Z^N the average error probability γ_N is at least c^N for some $c > b$ and for sufficiently large N, then $S(X;Y||Z) > 0$.*

Proof. According to the first inequality of (1) is suffices to show that Alice and Bob can, for some N, construct random variables $\hat{X}$ and $\hat{Y}$ from X^N and Y^N by exchanging messages over an insecure, but authenticated channel, such that

$$I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z}) > 0 \tag{7}$$

with $\hat{Z} = [Z^N, U]$, where U is the collection of all messages sent over the public channel.

Let $\hat{X}$ and $\hat{Y}$ be defined as follows. If Bob accepts, let $\hat{X} = C$ and $\hat{Y} = C'$, and if Bob (publicly) rejects, let $\hat{X} = \hat{Y} =$"reject". We show that (7) holds for sufficiently large N. If Bob accepts then

$$H(C|C') \leq h(b^N) \leq 2b^N \cdot \log_2(1/b^N) = 2b^N \cdot N \cdot \log_2(1/b) < c^N$$

for sufficiently large N (where $h(p) = -p\log_2 p - (1-p)\log_2(1-p)$ is the binary entropy function, the first inequality follows from Jensen's inequality, and the reason for the second inequality is that $-p\log_2 p \geq -(1-p)\log_2(1-p)$ for $p \leq 1/2$). On the other hand

$$H(C|\hat{Z}) = \sum_{\hat{z} \in \mathcal{Z}^N \times \mathcal{M}} P_{\hat{Z}}(\hat{z}) \cdot H(C|\hat{Z} = \hat{z}) = E[h(q(\hat{Z}))] \geq E[q(\hat{Z})] = \gamma_N \geq c^N,$$

where $q(\hat{z})$ is the probability of guessing C incorrectly with the optimal strategy (i.e., $q(\hat{z}) \leq 1/2$), given that $\hat{Z} = \hat{z}$. Given that Bob publicly rejects, we have $H(\hat{X}|\hat{Y}) = H(\hat{X}|\hat{Z}) = H(\hat{X}|U) = 0$. From $p_N > 0$ we conclude that $I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z}) > 0$. □

4 Generalizing the Binary Symmetric Scenario

First we show that the above results hold even when Eve knows R *precisely* with a certain probability smaller than 1. This is the case if Z is generated from R by a binary *erasure* channel instead of a binary symmetric channel, i.e., if Z is either equal to a special erasure symbol Δ, or else $Z = R$.

Lemma 5. *Consider the binary symmetric scenario of the previous section with $\alpha = \beta$ and where C_E is replaced by an erasure channel C_E^* (with erasure symbol Δ), independent of the pair (C_A,C_B), and with transition probabilities*

$$P_{Z|R}(\Delta, 0) = \delta_0,\ P_{Z|R}(0,0) = 1 - \delta_0,\ P_{Z|R}(\Delta, 1) = \delta_1,\ P_{Z|R}(1,1) = 1 - \delta_1,$$

where $\delta_0, \delta_1 > 0$. Then the statement of Lemma 3 holds also.

Proof. We show first that we can assume without loss of generality that C_E^* is symmetric. Let $\delta_0 < \delta_1$, and let an oracle be given that tells Eve the correct bit R with probability $(\delta_1 - \delta_0)/\delta_1$ if $R = 1$ and $Z = \Delta$. The additional information provided by this oracle cannot increase Eve's error probability. The random variable Z, together with the oracle, is equivalent to a random variable generated from R by a symmetric binary erasure channel with erasure probability $\delta_0 =: \delta$, and which is independent of the pair (C_A,C_B).

Let $0 < \rho < \min\{\delta, 1-\delta\}$. For sufficiently large N, the probability that the number of bits known to Eve is even and lies between $(1-\delta-\rho)N$ and $(1-\delta+\rho)N$ is at least $1/3$. Assume without loss of generality that N and $(1-\delta-\rho)N$ are even integers. We give a lower bound for Eve's average error probability γ_N about the bit sent by Alice, given that Bob accepts. As in the proof of Lemma 3, we obtain a lower bound for γ_N by taking a (small) part of all positive terms in γ_N, and again, this is a lower bound for any strategy for guessing the bit sent by Alice. We have

$$\begin{aligned}\gamma_N &\geq \frac{1}{2} \cdot \frac{(1-2\alpha+2\alpha^2)^N}{p_{a,N}} \cdot \frac{1}{3} \cdot \binom{(1-\delta-\rho)N}{(1-\delta-\rho)N/2} \cdot \cdots \\ &\qquad \cdots \cdot \left(\frac{(1-\alpha)^2}{(1-\alpha)^2+\alpha^2}\right)^{(1-\delta+\rho)N/2} \left(\frac{\alpha^2}{(1-\alpha)^2+\alpha^2}\right)^{(1-\delta+\rho)N/2} \\ &\geq \frac{1}{6 \cdot p_{a,N} \cdot \sqrt{2\pi(1-\delta-\rho)N}} \cdot \left[(1-2\alpha+2\alpha^2)^{\delta-\rho} 2^{1-\delta-\rho} (\alpha-\alpha^2)^{1-\delta+\rho}\right]^N\end{aligned}$$

for sufficiently large N. Here we have made use of (4). The first expression is $1/2$ times a lower bound for the conditional probability that Bob receives the correct codeword, that Eve knows an even number of bits which lies between $(1-\delta-\rho)N$ and $(1-\delta+\rho)N$, and that she receives the same number of 0's and 1's in her reliable bits, given that Bob accepts. The expressions $(1-\alpha)^2/((1-\alpha)^2+\alpha^2)$ and $\alpha^2/((1-\alpha)^2+\alpha^2)$ are the conditional probabilities that $R = X$ and $R \neq X$, respectively, given that $X = Y$. Bob's error probability, given that he accepts, is, like before, $\beta_N = (2\alpha - 2\alpha^2)^N / p_{a,N}$. For sufficiently small (positive) ρ we have

$$(1-2\alpha+2\alpha^2)^{\delta-\rho} 2^{1-\delta-\rho} (\alpha-\alpha^2)^{1-\delta+\rho} > 2\alpha - 2\alpha^2$$

because $\delta > 0$ and $1 - 2\alpha + 2\alpha^2 > 2\alpha - 2\alpha^2$. Considering (6), the lemma is proved. □

The next generalization step shows that it is unnecessary to assume that the random variables X, Y, and Z are symmetric. It is shown that an "appropriate" situation with *asymmetric* random variables can be transformed into a different "appropriate" situation with *symmetric* binary random variables $\tilde{X}$, $\tilde{Y}$, and $\tilde{R}$. The situation discussed in Lemma 6 is illustrated in Figure 2.

Lemma 6. *Let X, Y, and R be (possibly asymmetric) binary random variables with $0 < P_R(0) < 1$, and where X and Y are generated from R by independent channels C_A and C_B, where C_A satisfies*

$$P_{X|R}(0,0) > P_{X|R}(0,1) \tag{8}$$

$$P_{X|R}(1,1) > P_{X|R}(1,0)$$

and C_B satisfies the same conditions with X replaced by Y. Let further Z be generated from R by a binary erasure channel C_E^*, independent of the pair (C_A, C_B), with positive erasure probabilities. Then there exist binary random variables $\tilde{X}$, $\tilde{Y}$, $\tilde{Z}$, and $\tilde{R}$ such that $\tilde{X}$ and $\tilde{Y}$ can be obtained from X and Y, respectively, and such that the following statements hold:

1. $P_{\tilde{X}}(0) = P_{\tilde{Y}}(0) = P_{\tilde{R}}(0) = 1/2$.

2. $\tilde{X}$ *and* $\tilde{Y}$ *can be interpreted as being generated from* $\tilde{R}$ *by independent identical binary symmetric channels* $\tilde{C}_A$ *and* $\tilde{C}_B$ *with error probability* $\tilde{\alpha} < 1/2$.
3. *The random variable* $\tilde{Z}$ *can be interpreted as being generated from* $\tilde{R}$ *by an erasure channel* $\tilde{C}_E^*$, *independent of the pair* $(\tilde{C}_A, \tilde{C}_B)$, *with erasure probabilities* $\tilde{\delta}_0, \tilde{\delta}_1 > 0$ *such that* $\tilde{Z} = \Delta$ *only if* $Z = \Delta$, *i.e., we have* $\tilde{Z} = \tilde{R}$ *unless* Z *provides no information about* R *and* $\tilde{R}$. *(Equivalently we could say that* $\tilde{Z}$ *gives exactly the same information about* $\tilde{R}$ *as* Z *together with some additional information that can be thought as being provided by an oracle.)*

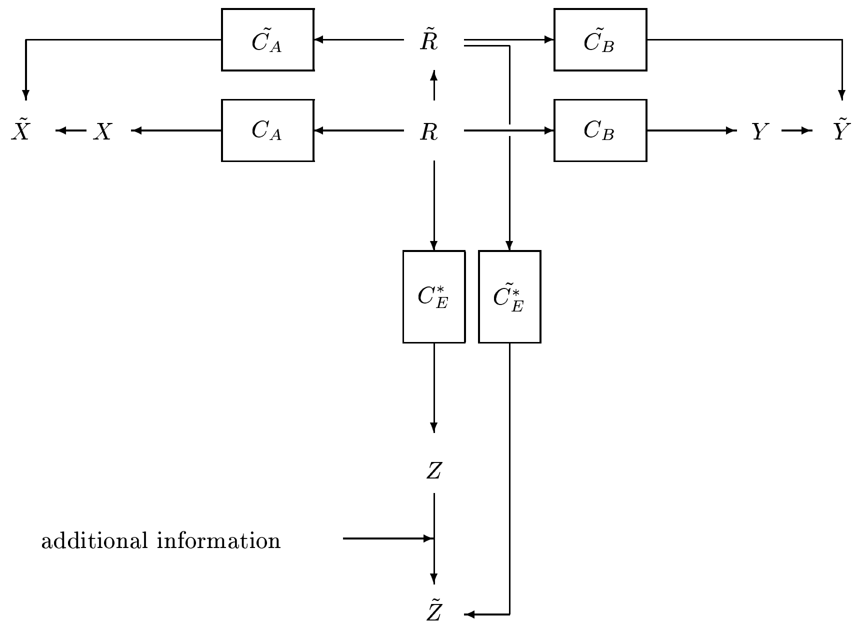

Fig. 2. The scenario described in Lemma 6.

Proof. Without loss of generality we can assume $P_R(0) \geq 1/2$. Let $\tilde{R}$ be generated from R by the following channel:

$$P_{\tilde{R}|R}(0,0) = \frac{1}{2 \cdot P_R(0)} \ , \quad P_{\tilde{R}|R}(1,0) = 1 - \frac{1}{2 \cdot P_R(0)} \ , \quad P_{\tilde{R}|R}(1,1) = 1 \ .$$

$\tilde{R}$ is obviously symmetric.

Assume first $P_X(0) \geq 1/2$. The symmetric random variable $\tilde{X}$ is generated from X as follows:

$$P_{\tilde{X}|X}(0,0) = \frac{1}{2 \cdot P_X(0)} \ , \quad P_{\tilde{X}|X}(1,0) = 1 - \frac{1}{2 \cdot P_X(0)} \ , \quad P_{\tilde{X}|X}(1,1) = 1 \ .$$

Then

$$\begin{aligned}
P_{\tilde{X}|\tilde{R}}(0,0) &= 2 \cdot P_{\tilde{X}\tilde{R}}(0,0) = 2 \cdot P_{\tilde{X}\tilde{R}XR}(0,0,0,0) \\
&= 2 \cdot P_R(0) \cdot P_{X|R}(0,0) \cdot \frac{1}{2 \cdot P_R(0)} \cdot \frac{1}{2 \cdot P_X(0)} \\
&= \frac{1}{2} \cdot \frac{P_{X|R}(0,0)}{P_{X|R}(0,0) \cdot P_R(0) + P_{X|R}(0,1) \cdot P_R(1)} > \frac{1}{2}
\end{aligned}$$

because $P_R(1) > 0$, and because of (8). Hence $\tilde{X}$ can be seen as generated from $\tilde{R}$ by a binary symmetric channel $\tilde{C}_A$ with crossover probability $\tilde{\alpha} < 1/2$. The case where $P_X(0) < 1/2$ can be treated completely analogously.

A similar cascade can be made for Y, and as in the proof of Lemma 3, we can assume without loss of generality that the channels $\tilde{C}_A$ and $\tilde{C}_B$ are identical. It is obvious that the independence of $\tilde{C}_A$ and $\tilde{C}_B$ follows from the same property of C_A and C_B.

Finally, let $\tilde{Z}$ be equal to $\tilde{R}$ unless $Z = \Delta$, in which case $\tilde{Z} = \Delta$. It is obvious that $\tilde{Z}$ has all the required properties. □

5 The General Scenario

We now consider the general scenario of random variables R, X, Y, and Z as described in Theorem 2. The following lemma states equivalent characterizations of the condition $I(X;Y|Z) > 0$.

Lemma 7. *Under the assumptions of Theorem 2 (the discrete random variables X, Y, and Z result from a binary random variable R being sent through independent channels), the following three conditions are equivalent:*

(1) $I(X;Y|Z) > 0$.
(2) $I(X;R) > 0$, $I(Y;R) > 0$, *and* $H(R|Z) > 0$.
(3) The following three conditions are satisfied:
  (i) There exist $x, x' \in \mathcal{X}$ *such that*

$$P_{X|R}(x,0) > P_{X|R}(x,1) \quad \textit{and} \quad P_{X|R}(x',0) < P_{X|R}(x',1) \ , \tag{9}$$

  (ii) there exist $y, y' \in \mathcal{Y}$ *such that*

$$P_{Y|R}(y,0) > P_{Y|R}(y,1) \quad \textit{and} \quad P_{Y|R}(y',0) < P_{Y|R}(y',1) \ , \tag{10}$$

  (iii) and there exists $z \in \mathcal{Z}$ *such that*

$$P_Z(z) > 0 \quad \textit{and} \quad 0 < P_{R|Z}(0,z) < 1 \ . \tag{11}$$

Proof. First we give an alternative characterization of the independence of the three channels, i.e., of $P_{XYZ|R} = P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R}$. (We sometimes omit all the arguments of the probability distribution functions. In this case the statements hold for all possible choices of arguments. For example, $P_{X|Y} = P_X$ stands for $P_{X|Y}(x, y) = P_X(x)$ for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.) From

$$P_{YZ|R} = \sum_{x \in \mathcal{X}} P_{XYZ|R} = \sum_{x \in \mathcal{X}} P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R} = P_{Y|R} \cdot P_{Z|R}$$

and

$$P_R \cdot P_{YZ|R} \cdot P_{X|YZR} = P_{XYZR} = P_R \cdot P_{X|R} \cdot P_{Y|R} \cdot P_{Z|R}$$

we conclude that $P_{X|YZR} = P_{X|R}$ and, analogously, that $P_{Y|XZR} = P_{Y|R}$ and $P_{Z|XYR} = P_{Z|R}$.

(1) implies (2). Let $I(X;Y|Z) > 0$. Assume $I(X;R) = 0$. Then $P_{X|YZR} = P_{X|R} = P_X$, and X is also independent of YZ (and hence of Z). Thus

$$I(X;Y|Z) = H(X|Z) - H(X|YZ) = H(X) - H(X) = 0 \ ,$$

which is a contradiction. We conclude that $I(X;R) > 0$ and by a symmetric argument that $I(Y;R) > 0$. Finally assume $H(R|Z) = 0$. Then

$$\begin{aligned} I(X;Y|Z) &= H(X|Z) + \underbrace{H(R|XZ)}_{0} - H(X|YZ) - \underbrace{H(R|XYZ)}_{0} \\ &= H(XR|Z) - H(XR|YZ) \\ &= \underbrace{H(R|Z)}_{0} + H(X|RZ) - \underbrace{H(R|YZ)}_{0} - H(X|RYZ) \\ &= H(X|R) - H(X|R) = 0 \ , \end{aligned}$$

which is a contradiction. Hence $H(R|Z) > 0$.

(2) implies (3). Let $I(X;R) > 0$, that is X and R are not statistically independent, which implies that there exist $x, x' \in \mathcal{X}$ such that (9) holds. Similarly we conclude the existence of appropriate y and y' from $I(Y;R) > 0$. Finally, $P_{R|Z}(0, z) \in \{0, 1\}$ for all $z \in \mathcal{Z}$ with $P_Z(z) > 0$ would imply that $H(R|Z) = 0$. Hence (11) holds for some $z \in \mathcal{Z}$.

(3) implies (1). It suffices to prove that $I(X;Y|Z = z) > 0$ because $P_Z(z) > 0$. This is equivalent to the fact that X and Y are not statistically independent, given $Z = z$. We show that

$$P_{X|YZ}(x, y, z) > P_{X|YZ}(x, y', z) \ . \tag{12}$$

For both $\overline{y} = y$ and $\overline{y} = y'$, we have

$$P_{X|YZ}(x, \overline{y}, z) = P_{X|R=0}(x) \cdot P_{R|YZ}(0, \overline{y}, z) + P_{X|R=1}(x) \cdot P_{R|YZ}(1, \overline{y}, z) \ .$$

Because $P_{X|R=0}(x) > P_{X|R=1}(x)$, (12) holds if

$$P_{R|YZ}(0, y, z) > P_{R|YZ}(0, y', z) \ . \tag{13}$$

Using $P_{R|YZ} = P_{Y|R} \cdot P_{RZ}/(P_{Y|Z} \cdot P_Z)$, (13) follows from

$$P_{Y|R=0}(y) \cdot [P_{Y|R=0}(y') \cdot P_{R|Z=z}(0) + P_{Y|R=1}(y') \cdot P_{R|Z=z}(1)] > \dots$$

$$\dots > P_{Y|R=0}(y) \cdot P_{Y|R=0}(y') > \dots$$

$$\dots > P_{Y|R=0}(y') \cdot [P_{Y|R=0}(y) \cdot P_{R|Z=z}(0) + P_{Y|R=1}(y) \cdot P_{R|Z=z}(1)] \ . \tag{14}$$

Both inequalities in (14) follow from the fact that $0 < P_{R|Z=z}(0) < 1$, and because of (10). □

We are now ready to prove Theorem 2.

Proof of Theorem 2. According to Lemma 7, there exist $x, x' \in \mathcal{X}$ and $y, y' \in \mathcal{Y}$ such that (9) and (10) hold. We can assume that X and Y are *binary* random variables with $\mathcal{X} = \{x, x'\}$ and $\mathcal{Y} = \{y, y'\}$: Alice and Bob publicly reject a realization if $X \notin \{x, x'\}$ or if $Y \notin \{y, y'\}$. (More precisely, Alice and Bob both receive such binary random variables $\overline{X}$ and $\overline{Y}$ from X and Y, respectively, with positive probability.)

Furthermore, there exists $z \in \mathcal{Z}$ such that (11) holds. Suppose that Eve knows the bit R unless $Z = z$ (an oracle that tells Eve the bit R if $Z \neq z$ cannot increase her error probability). This situation is equivalent to the one where Eve receives a random variable $\overline{Z}$ that is generated by an erasure channel C_E^* with some (positive) erasure probabilities δ_0 and δ_1, and such that the channels of Alice, Bob, and Eve are independent, and is illustrated in Figure 3. The probability that Alice and Bob accept N consecutive realizations of X and Y is strictly positive for every N. Lemmas 6, 5, and 4 now imply that $S(X;Y||Z) > 0$. Note that in this application of Lemma 4 the event that Bob accepts means that Alice and Bob both accept a sufficiently large number N of consecutive realizations of X and Y (if Alice does not accept, she sends $M =$"reject" over the public channel), and that Bob accepts the received message sent by Alice. □

6 Concluding Remarks

We have derived a simple characterization of whether information-theoretic secret key agreement is possible in the case of discrete random variables X, Y, and Z that are generated from a binary random variable sent over three independent noisy channels.

The condition that R is a *binary* random variable is crucial in Theorem 2. To see this, consider the following scenario: R is uniformly distributed in $\mathcal{R} := \{r_{00}, r_{01}, r_{10}, r_{11}\}$, and X, Y, and Z are binary random variables, generated from

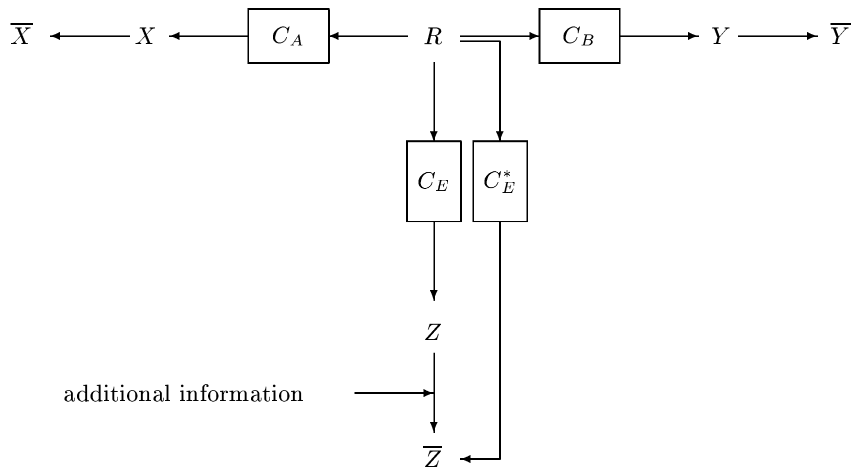

Fig. 3. The situation in the proof of Theorem 2.

R by the following independent channels (let δ be the Kronecker symbol, i.e., $\delta_{ij} = 1$ if $i = j$, and otherwise $\delta_{ij} = 0$):

$$P_{X|R}(x, r_{ij}) = \delta_{xi} \ , \quad P_{Y|R}(y, r_{ij}) = \delta_{yj} \ , \quad P_{Z|R}(z, r_{ij}) = \delta_{z,i \oplus j} \ .$$

Note that, for all $r_{ij} \in \mathcal{R}$, $Z = X \oplus Y$, that is $I(X;Y|Z) = 1$. On the other hand $I(X;Y) = 0$, and hence $S(X;Y||Z) = 0$.

The general scenario of *arbitrary* random variables is more complicated. One can state conditions for both $S(X;Y||Z) > 0$ and $S(X;Y||Z) = 0$, but an exact characterization appears to be difficult. We only mention here that in general the conditions $I(X;Y) > 0$ and $I(X;Y|Z) > 0$ together are *not* sufficient for achieving a positive secret key rate.

The presented protocols are computationally efficient, but they are not efficient in terms of the size of the generated secret key. For special cases, e.g., for the scenario of three binary symmetric channels, there exist protocols that are much more efficient with respect to the effective key generation rate (see [6]).

References

1. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, *Journal of Cryptology*, Springer Verlag, Vol. 5, No. 1, pp. 3-28, 1992.
2. T. M. Cover and J. A. Thomas, Elements of information theory, Wiley Series in Telecommunications, 1992.
3. I. Csiszár and J. Körner, Broadcast channels with confidential messages, *IEEE Transactions on Information Theory*, vol. IT-24, pp. 339-348, 1978.

4. W. Feller, An introduction to probability theory and its applications, 3rd edition, Vol. 1, Wiley International, 1968.
5. M. J. Fischer and R. N. Wright, Bounds on secret key exchange using a random deal of cards, *Journal of Cryptology*, Springer Verlag, Vol. 9, No. 2, pp. 71-99, 1996.
6. U. M. Maurer, Protocols for secret key agreement based on common information, *Advances in Cryptology - CRYPTO '92*, Lecture Notes in Computer Science, Berlin: Springer-Verlag, Vol. 740, pp. 461-470, 1993.
7. U. M. Maurer, Secret key agreement by public discussion from common information, *IEEE Transactions on Information Theory*, Vol. 39, No. 3, pp. 733-742, 1993.
8. C. E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, Vol. 28, pp. 656-715, Oct. 1949.
9. A. D. Wyner, The wire-tap channel, *Bell System Technical Journal*, Vol. 54, No. 8, pp. 1355-1387, 1975.