Lietzén, Jari; Tirkkonen, Olav; Vehkalahti, Roope

Secret Keys from Parity Bits in the Satellite Setting

Published in:
2022 IEEE International Symposium on Information Theory, ISIT 2022

DOI:
10.1109/ISIT50566.2022.9834762

Published: 01/01/2022

Document Version
Peer reviewed version

Please cite the original version:
Lietzén, J., Tirkkonen, O., & Vehkalahti, R. (2022). Secret Keys from Parity Bits in the Satellite Setting. In *2022 IEEE International Symposium on Information Theory, ISIT 2022* (pp. 2672-2677). (IEEE International Symposium on Information Theory; Vol. 2022-June). IEEE. https://doi.org/10.1109/ISIT50566.2022.9834762

Secret Keys from Parity Bits in the Satellite Setting

Jari Lietzén†, Olav Tirkkonen† and Roope Vehkalahti*
† Aalto University, Department of Communications and Networking, Maarintie 8, 02150 Espoo, Finland
* University of Jyväskylä, Department of Mathematics and Statistics, Seminaarinkatu 15, 40014 Jyväskylän yliopisto, Finland
Email: {jari.lietzen,olav.tirkkonen}@aalto.fi, roope.i.vehkalahti@jyu.fi

***Abstract*—We consider a two-way secret key distribution protocol in the satellite setting, where Alice, Bob and Eve each decode bits from noisy signals received from a source in their environment. Alice and Bob perform advantage distillation to find a secret key. We apply a Two-way Protocol with Parity bit Reconciliation (TPPR) where secret keys are collected from parity bits in course of advantage distillation, not only from the final distilled bits. We analyze the mutual information acquired by Eve from exploiting the original eavesdropped information together with the information leaked during the distillation protocol, as well as TPPR secret key rate. Comparing to the Parity-Check Protocol (PCP) known in the literature, TPPR provides complementary performance. In operation regions where PCP fare badly as compared to one-way protocols, TPPR provides gains in key rate.**

***Index Terms*—secret key agreement, source model**

I. Introduction

Information-theoretic security offers a framework in which security of information flows can be enforced by coding mechanisms [1]–[6]. In wiretap channels, where the eavesdropper Eve observes the communication from Alice to Bob, through a channel that is degraded as compared to the Alice-Bob channel, the rate of information leakage can be controlled [1]–[3]. Controlling the information leakage rate is referred to as *weak secrecy*, see [4]. In secret key agreement models [5]–[13], widely used *one-way communication* protocols [8]–[10] correct Bob's error codeword as compared to Alice's, using, e.g., state-of-the art Forward Error correction codes, such as turbo [9] or LDPC [10] codes. In the wiretap and one-way key agreement models, secure communication is possible only if Eve is at a disadvantage as compared to Alice and Bob.

Maurer [5], [6] proved that it is possible to agree on a secret key by *two-way communication* over a public channel, starting from some correlated source information. This holds even if Eve initially has a *better* channel to the source than Alice and Bob. An example source would be a satellite broadcasting random bits. Alice, Bob, and Eve receive these bits through independent binary symmetric channels (BSCs) with individual error probabilities. In order to agree on a secret key, Alice and Bob exchange messages over an authenticated public channel, overheard by Eve. Using *advantage distillation* Alice and Bob may turn Eve's initial advantage into a disadvantage by concentrating on bits that they both received reliably and discarding the rest [6]. Advantage distillation makes it possible to achieve positive secret key rates that would not be possible using only one-way communication methods; the secret key rate is improved by feedback [4]. Furthermore, compared to *weak secrecy*, *strong secrecy* is now achieved by controlling the amount of leaked information [4], [14]. Advantage distillation methods such as the parity-check protocol (PCP) [6], [12] enable Alice and Bob to collect secret key whenever Eve's error probability is non-zero, and Alice's and Bob's error probabilities are $< 1/2$.

Two-way key distillation has been widely considered in the context of Quantum Key Distribution (QKD), where Alice and Bob may assume that all errors on the channel are caused by deliberate action of Eve. In [15] we introduced a two-way key distillation protocol for QKD, where secret keys were created by correcting parity bits. We showed that the considered two-way protocol generates considerably more secret key than any one-way protocol, under the restricted individual attack model.

In this paper, we consider a similar Two-way Protocol with Parity bit Reconciliation (TPPR) in the classical communication setting of the satellite model. In TPPR, parity checking is used for advantage distillation as in PCP [6], [12], but instead of discarding parity bits after each advantage distillation round, key bits are collected from error corrected parity bits. The steps of the protocol analyzed here are the same as in the QKD case [15], but the underlying privacy amplification analysis, and accordingly the resulting key rate differs drastically between the QKD and satellite setting. We perform complete information theoretical security analysis of TPPR in the classical communication setting when Alice and Bob correct all parity bits in secret.

II. System model

The satellite model [6] is an example of the *source model* secret key agreement method [4], where a source is broadcasting a signal in the form of a sequence of uniformly distributed random bits U. Alice, Bob, and Eve receive these bits through three independent binary symmetric channels (BSCs) C_A, C_B and C_E, with corresponding error probabilities ϵ_A, ϵ_B, and ϵ_E [6]. Let X_i be Alice's bit, Y_i Bob's, and Z_i is Eve's bit received through their respective channels. Their joint probability distribution is defined as

$$P_{X_iY_iZ_i|U} = P_{X_i|U}\ P_{Y_i|U}\ P_{Z_i|U}, \tag{1}$$

where $P_{X_i|U}(x,u) = 1-\epsilon_A$ if $x = u$ and ϵ_A otherwise, and correspondingly for $P_{Y_i|U}(y,u)$ and $P_{Z_i|U}(z,u)$ [6].

This work was funded by the Academy of Finland (grant 334539).

Following [6], after N consecutive uses of the channel Alice has a length N i.i.d binary sequence with equal probabilities for 1's and 0's and Bob's sequence Y is X received through a BSC with crossover probability

$$\beta = \epsilon_A(1-\epsilon_B) + (1-\epsilon_A)\epsilon_B \ . \tag{2}$$

Eve's random variable Z is a sequence of independent identical random variables and for every x, y and z, $P(x,y,z) = \prod_{i=1}^{n} P(x_i, y_i, z_i)$. Throughout the paper X, Y and Z are i.i.d binary vectors.

III. Secret Key Agreement by Public Discussion

Alice and Bob wish to agree on a secret key using the channel of the previous section. They can use an authenticated public channel to communicate to each other. These messages are available to Eve as well, but she cannot alter them nor add new messages. The *secret-key agreement by public discussion* model proposed by Maurer proves that under these conditions it is almost always possible for Alice and Bob to agree on a secret key [5], [6], assuming they know $P(X,Y,Z)$.

A one-way key agreement protocol begins with error correction. Alice has a length L realization x of X, and Bob an erroneous version y. Alice and Bob communicate through the public channel to correct errors in Bob's vector y. This can be based on a dialogue as in the Cascade-protocol [8], or on forward error correction codes [9], [10]. After error correction, Bob's codeword is a realization of random vector Y' with $P(X \neq Y') < \epsilon$, for an ϵ characterizing the error correction scheme.

Based on the known error probabilities and the amount of information leaked during error correction, Alice and Bob can now estimate how much information Eve has of X. Using *privacy amplification* they erase this by mapping x and y' to length L_{fin} bit-vectors k and k'. These are binary i.i.d vectors with equal probabilities of 1 and 0. The probability density function after these operations is $P(K, K', Z')$. Here Z' aggregates Eve's original random variable Z and all the additional data she has managed to acquire. The constant L_{fin} is selected such that $I(K;Z') < \epsilon$.

The secret key rate of a two-way protocol is defined similarly. Instead of beginning with error correction, Alice and Bob use two-way classical communication and agree on key words k and k' so that the corresponding random variables satisfy $P(K \neq K') < \epsilon$, $I(K;Z') < \epsilon$ and $I(K';Z') < \epsilon$. General upper and lower bounds for a secret key rate are given by [12, Lemma 1] and [6, Theorem 2]. For any finite probability distribution $P(X,Y,Z)$ we have the secret key rate bounds

$$\begin{aligned} I(X;Y) - \min(I(X;Z), I(Y;Z)) &\leq S(Z;Y|Z) \\ &\leq \min(I(X;Y), I(X;Y|Z)) \ . \end{aligned} \tag{3}$$

Here the lower bound is a result of one-way communication. Not much is known about the achievable key rates for two-way protocols. For the source model with BSCs, [11], [12] represent the state of art, while the situation when Eve has an erasure channel is analyzed in [13].

A key distribution protocol achieves the *strong secrecy* key rate S if for every ϵ we can find a uniformly random K with length $L(\epsilon)$ so that for all $L > L(\epsilon)$ we have $P(K \neq K') < \epsilon$, $I(K;Z') < \epsilon$ and $L_{\text{fin}}/L \geq S - \epsilon$. Remarkably, weak and strong secrecy are equivalent under two-way communication [16].

PCP is a two-way advantage distillation protocol studied by Gander and Maurer [5], [7], [12]. At the beginning of PCP Alice and Bob divide their bit strings into pairs and compute parities for each pair. Alice and Bob compare their parities publicly over the authenticated channel and discard those pairs where the parities disagree. From each pair with parity agreement, one bit is selected for further processing, The same step may be used several times to further decrease the error probability between Alice's and Bob's key strings.

IV. Advantage Distillation with Secret Keys from Parity Bits

In contrast to PCP we do not discard parity bits, but error correct and collect distilled key material from them. We present a *key growing protocol;* Alice and Bob start with some existing secret key. A similar protocol was discussed in [15] in a QKD setting. In the source model setting, the key rate analysis, and thus the privacy amplification step changes completely.

Alice and Bob arbitrarily but jointly segment their bits to blocks of two bits, and compute a parity bit for each block. Alice sends encrypted redundancy bits to Bob so that he can correct his parity bits. The parity bits are then saved as distilled key bits. From each block where Alice and Bob agreed about the parity, they arbitrarily but jointly select one bit, which are forwarded to the next round. The protocol ends after M rounds of parity computations. The bits selected from the blocks with correct parities in round M are also error corrected and added to the distilled key. Eve's mutual information of distilled key bits is computed and the key is shortened using privacy amplification.

A. TPPR Protocol Analysis

The TPPR protocol begins after satellite communication. Alice's bits are $X \in \mathcal{X}$, Bob's bits $Y \in \mathcal{Y}$, and Eve's $Z \in \mathcal{Z}$. We run the protocol in a manner where Bob's parity bits are corrected as compared to Alice's parity bits. Bob's error probability with respect to Alice's original bits is β, given in (2). Individual bits in X are independent, while X_i, Y_i, Z_i are correlated. We define Bob's and Eve's error sequences as

$$B = Y \oplus X \ , \quad E = Z \oplus X \ . \tag{4}$$

These are correlated with the joint distribution given as $P_{E_i,B_i}(e,b) = \alpha_{be}$ with

$$\begin{aligned} \alpha_{00} &= \epsilon_A\epsilon_B\epsilon_E + (1-\epsilon_A)(1-\epsilon_B)(1-\epsilon_E) \\ \alpha_{01} &= \epsilon_A\epsilon_B(1-\epsilon_E) + (1-\epsilon_A)(1-\epsilon_B)\epsilon_E \\ \alpha_{10} &= \epsilon_A(1-\epsilon_B)\epsilon_E + (1-\epsilon_A)\epsilon_B(1-\epsilon_E) \\ \alpha_{11} &= \epsilon_A(1-\epsilon_B)(1-\epsilon_E) + (1-\epsilon_A)\epsilon_B\epsilon_E \ . \end{aligned}$$

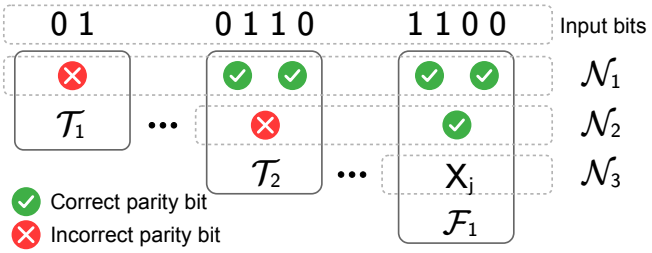

Fig. 1. Parity bit sets for two rounds, $m = 2$.

The conditional probabilities of E given B are

$$P_{E|B}(e|b) = \frac{\alpha_{be}}{\alpha_{b0} + \alpha_{b1}} \ . \tag{5}$$

The protocol will induce correlations across blocks of bits, with the blocks of correlated bits growing in each round.

The error probability of Bob's bits when round m starts is the probability that both bits were wrong in the previous round, given that the parity was correct:

$$\beta_m = \frac{\beta_{m-1}^2}{\beta_{m-1}^2 + (1-\beta_{m-1})^2} \ , \tag{6}$$

while the error probability of the parity bits in round m is

$$p_m = 2\beta_m(1-\beta_m) \ . \tag{7}$$

For completeness, we define $p_0 = 0$ and $\beta_1 = \beta$. The rate of distilled bits arising from parity bits constructed in round $m = 1, \ldots, M$ is given by

$$R_m = \frac{1}{2^m} \prod_{i=0}^{m-1} (1 - p_i) \ . \tag{8}$$

In addition, we take an arbitrary bit from each of the parity blocks of the last round M for which Bob had the correct parity. These are error corrected, and added to the set of distilled bits. We call this round $M+1$, with error probability $p_{M+1} = \beta_{M+1}$ and distilled key rate

$$R_{M+1} = (1 - p_M)\, R_M \ . \tag{9}$$

Error correction of the distilled bits collected on round m consumes $h\,(p_m)$ bits per output bit. The error correction cost has to be calculated for all the parity bits that are present at each round, as shown in Fig. 1 with sets $\mathcal{N}_\mathrm{m}$.

The mutual information leaked to Eve has to be accounted for only once, when the side information leaked to Eve related to a set of distilled bits is not growing any more. This happens whenever one of Bob's parity bits is identified to be erroneous. After that, no further correlations are created related to this bit, and all the parity bits that have previously become correlated due to the information of Bob's parity bit correctness in previous rounds. An erroneous parity bit in round m is correlated with 2^{m-i} parity bits in rounds $i = 1, \ldots m-1$. In total, an erroneous parity bit in round m represents a set $\mathcal{T}_m$ of

$$T_m = \sum_{i=1}^{m} 2^{m-i} = 2^m - 1 \tag{10}$$

correlated parity bits in rounds $i = 1, \ldots, m$. The leakage of mutual information to Eve about this set of bits is *terminated* in round m. As an example, in Fig. 1 the sets $\mathcal{T}_1$ and $\mathcal{T}_2$ are terminated at rounds 1 and 2. Irrespectively of which of the rounds $i \leq m$ a parity bit in this set is constructed in, we say that these bits are *terminated* on round m. The rate of bits terminating in round $m = 1, \ldots, M$ is

$$\tilde{R}_m = T_m\, p_m\, R_m \ . \tag{11}$$

In the final round, R_{M+1} represented the additional X_j bit, shown in Fig. 1 in set $\mathcal{F}_1$. Each of these is correlated with one correct parity bit from round M and $2^M - 2$ correct parity bits from previous rounds. Thus there is a set of $T_{M+1} = 2^M$ distilled bits correlated with each additional X_j in round $M+1$, and the rate of bits terminating in round $M+1$ is

$$\tilde{R}_{M+1} = 2^M R_{M+1} \ . \tag{12}$$

It is straight forward to verify that the total rate of distilled bits of the protocol is

$$R = \sum_{m=1}^{M+1} R_m = \sum_{m=1}^{M+1} \tilde{R}_m \ ; \tag{13}$$

all distilled bits created in rounds of correcting parity bits have been grouped to sets of correlating bits characterized by a terminating bit in one of the rounds. The probability that any given parity bit is terminated at round m is then

$$p_m^{\mathrm{term}} = \tilde{R}_m / R \ . \tag{14}$$

After each round of distillation phase, privacy amplification is performed for the bits terminating in that round. The resulting round $m = 1, \ldots, M$ of TPPR is summarized in Algorithm 1. All actions for which the actor is not mentioned, are performed by both Alice and Bob. Arbitrary segmentation in Step 1, bit selection in Step 9 are performed jointly by Alice and Bob over the public channel. The bits collected in Step 8 are, with high probability, all equal for Bob and Alice.

Algorithm 1 Round $m = 1, \ldots, M$ in TPPR

Input to Round m**:** Fraction $2R_m$ of L initial bits with error probability β_m

1. Arbitrarily segment bits to 2-bit blocks
2. Compute parity check bits for each block
3. Compute error probability p_m using (7)
4. Alice sends $LR_m\, h(p_m)$ redundancy bits to Bob using one-time pad encryption
5. Bob corrects his parity bits
6. Bob sends locations of erroneous parity bits over the public channel
7. Remove blocks with erroneous parity bits
8. Compute Eve's mutual information of blocks with terminating parity bits and perform privacy amplification
9. Select one bit arbitrarily from each kept block

Output: Fraction $R_m(1 - p_m)$ of original bits with error probability β_{m+1}

The outgoing bit-error rate β_{m+1} is used as input parameter in Step 1 as the protocol enters a new round. The bits from Step 9 are fed to the protocol and the protocol terminates after a predetermined number of rounds, after which round $M+1$ is separately treated.With $M=1$ the protocol is similar to the QKD protocol of [11]. The distinct difference to the QKD-protocols [11], [15] is in Step 8, which will be addressed next.

B. Secret Key Rate Analysis of TPPR

When computing the secret key rate, all key bits created and consumed in the protocol are taken into account. To estimate Eve's mutual information, we first state a general result.

Proposition 1: Assume that in the satellite setting with a uniformly random source Alice and Bob agree on a method to distill bits, where Alice's length-L distilled bit sequence K is constructed from a sequence X with a rank-L linear mapping as $K=\mathbf{G}X$. The linear mapping $\mathbf{G}=\mathbf{G}(B,W)$ depends on B and an external RV W. The side information $\tilde{C}$ leaked to Eve during advantage distillation consists of $\mathbf{G}$, and information about the correctness of some of Bob's distilled bits: $C=\widetilde{\mathbf{G}}(X\oplus Y)$, where $\widetilde{\mathbf{G}}$ consists of some rows from $\mathbf{G}$. Using Eve's error codeword E, define Eve's distilled error codeword $Q=\mathbf{G}E$. In the limit of infinitely long sequences, Eve's information about K is

$$I(K;\, Z,\tilde{C}) = I(K, Z\,|\,\tilde{C}) = H(K) - H(Q|\tilde{C})\ , \qquad (15)$$

where $H(Q|\tilde{C})$ is the entropy of Q conditioned on $\tilde{C}$.

Proof: The outline of the proof is as follows: As the BSCs producing X and Y are independent, X and B are independent irrespectively of ϵ_A, ϵ_B. X and W are independent by definition, thus $I(K;\tilde{C})=0$, and $I(K;\, Z,\tilde{C}) = I(K;\, Z\,|\,C)$. The proof of the second equality hinges on the fact that the linear transform $\mathbf{G}$ has a null space, which divides both $\mathcal{X}$ and $\mathcal{Z}$ to cosets. Using the fact that X is drawn i.i.d from $\mathcal{X}$ and Z i.i.d. from $\mathcal{Z}$, the statement follows. ∎

In TPPR, $\mathbf{G}$ constructs the parities and kept bits. We consider sequences in the asymptotically infinite length regime, where mutual information characterizes both Bob's and Eve's knowledge. The entropies then become entropy rates, in units of bits/channel use. Note that in TPPR, Eve acquires information about the correctness of Bob's parity bits, but not about the correctness of the additional bit of the last round.

Following Proposition 1, we next set out to compute the entropy of Eve's key error codeword, conditioned on $\tilde{C}$. The conditioning on $\mathbf{G}$ is first treated. As an RV, $\mathbf{G}$ can be described as first identifying a division of the sequence of distilled bits to sets $\mathcal{T}_{m,n}$, of correlated distilled bits, where $|\mathcal{T}_{m,n}| = T_m$. Eve's mutual information can be computed separately for each set. The RV $\mathbf{G}$ thus gives rise to a probability distribution of key bits belonging to sets (14). In addition, $\mathbf{G}$ gives rise to a permutation of Alice's bits X contributing to K, which does not affect mutual information. The conditional entropy of Eve's key errors per channel use thus becomes

$$H(Q|\tilde{C}) = R\sum_{m=1}^{M+1} p_m^{\text{term}}\ H(Q_m|C_m)/T_m\ . \qquad (16)$$

Here $H(Q_m|C_m)$ is the sum entropy of Eve's error Q_m of distilled bits in a set $\mathcal{T}_m$ of length T_m, i.e. it is not measured per channel use. $C_m=\mathbf{G}_m(X_m\oplus Y_m)$ represents the correctness of Bob's parity bits restricted to $\mathcal{T}_m$; here $\mathbf{G}_m$ is the restriction to $\mathcal{T}_m$ of the distilling matrix, and X_m and Y_m of Alice's and Bob's sequences, respectively. The expression given by the sum is the entropy in Q per distilled bit, and multiplying with R we get the entropy rate.

Now, by construction it turns out that after accounting for the permutations in $\mathbf{G}$, C_m is fixed for a set $\mathcal{T}_m$, When $m\le M$, the parity bit from round m has $C=1$, while $C=0$ for all the parity bits of previous rounds. For $m=M+1$, all Bob's parity bits have been correct, and we have $C=0$. Thus

$$H(Q|\tilde{C}) = \sum_{m=1}^{M+1} p_m R_m\ H(Q_m|c_m)\ , \qquad (17)$$

where c_m is a deterministic realization of C restricted to $\mathcal{T}_m$, and we used (14).

Considering $\mathcal{T}_m$ for $m<M$, there are $L=2^m$ of Eve's bits having information about the $L-1$ distilled bits in $\mathcal{T}_m$. In this case the side information of Bob's bits indicates that precisely half Bob's bits have been in error, and half have been correct. Thus half of Eve's bits come from the conditional distribution (5) with $b=0$, and half from the distribution with $b=1$. From the knowledge of $\mathbf{G}$ Eve knows the division to halves, but she does not know which half has $b=0$ and which $b=1$. The probability of the two alternatives of b are 1/2. The probability of Eve's error codeword of length L can thus be described in terms of two integers, w_0, w_1 which indicate the weight of E in these two halves. If w_0 were the weight of the half with $b=0$, the probability of the error codeword would be:

$$\Phi(w_0,w_1) = \frac{\alpha_{00}^{L/2-w_0}\,\alpha_{01}^{w_0}\,\alpha_{10}^{L/2-w_1}\,\alpha_{11}^{w_1}}{(\alpha_{00}+\alpha_{01})^{L/2}\,(\alpha_{10}+\alpha_{11})^{L/2}} \qquad (18)$$

As only parity bits constructed from two X_j are considered for K, the null-space of $\mathbf{G}_m$ is generated by $\mathbb{1}$, the all ones codeword. Thus the two states E and $E\oplus\mathbb{1}$ map to the same Q. Summing over the two alternatives of b, and the null space, the probability of a Q with weights w_0, w_1 is:

$$\begin{aligned}\Psi(w_0,w_1) \;=\; \frac{1}{2}\Bigg(&\Phi(w_0,w_1) + \Phi\left(\frac{L}{2}-w_0, \frac{L}{2}-w_1\right)\\ &+\Phi(w_1,w_0) + \Phi\left(\frac{L}{2}-w_1, \frac{L}{2}-w_0\right)\Bigg) \qquad (19)\end{aligned}$$

From the form of Ψ it follows that it is sufficient to consider Eve's error codewords with weights in the set

$$\mathcal{W} = \left\{(w_0,w_1)\,\middle|\, 0\le w_0\le \frac{L}{4},\ w_0\le w_1\le \frac{L}{2}-w_0\right\} \qquad (20)$$

There are multiple Q with the same probability. To compute the entropy, it is sufficient to know how many Q-states have a given probability. It turns out that there are

$$\mu(w_0,w_1) = \frac{1+(1-\delta_{w_0,w_1})(1-\delta_{w_0,L/2-w_1})}{1+\delta_{w_0,L/4}\ \delta_{w_0,L/4}} \binom{\frac{1}{2}L}{w_0}\binom{\frac{1}{2}L}{w_1} \qquad (21)$$

key error states with the same w_o, w_1. Here $\delta_{i,j}$ is the Kronecker δ-symbol. We then have

Lemma 1: The entropy of Eve's error vector for a set $\mathcal{T}_m$ of $T_m = 2^m - 1$ key bits terminating at stage $m \leq M$ is

$$H(Q_m|C_m) = -\sum_{(w_0,w_1)\in\mathcal{W}} \mu(w_0,w_1)\,\Psi(w_0,w_1)\,\log_2\Psi(w_0,w_1) \tag{22}$$

The sketch of the proof can be found above, the details are left out due to lack of space.

Next, we address Eve's key error entropy for the final round $m = M+1$. Now, Alice and Bob agree about $L = 2^M$ key bits, starting from L original bits. Constrained to a $\mathcal{T}_{M+1}$, each X maps to a different K, and each E maps to a different key error event Q. During the protocol, Bob has revealed that all the $L-1$ parities computed from the bits have been the same as Alice's. Eve thus knows that *either none, or all of Bob's bits have been in error*. The probabilities of these events are

$$P_B(b) = \frac{(\alpha_{b0}+\alpha_{b1})^L}{\sum_{b=0,1}(\alpha_{b0}+\alpha_{b1})^L}\ . \tag{23}$$

Eve thus knows that either all of her error bits E come from (5) with $b=0$, or all have $b=1$. Denoting the weight of an error codeword with w, the probability of an error event with this weight, conditioned on b, is

$$\Xi(w|b) = \frac{\alpha_{b,0}^{L-w}\alpha_{b,1}^{w}}{(\alpha_{b,0}+\alpha_{b,1})^L}\ . \tag{24}$$

As Eve does not know which event occurred, the overall probability of a key error given by a specific error keyword with weight w is

$$\Upsilon(w) = P_B(0)\ \Xi(w|0) + P_B(1)\ \Xi(w|1)\ . \tag{25}$$

The number of distinct error events with weight w is given by the binomial coefficient. We thus have

Lemma 2: The entropy of Eve's key error in the final round of TPPR-M is:

$$H(Q_{M+1}|C_{M+1}) = -\sum_{w=0}^{L}\binom{L}{w}\Upsilon(w)\,\log_2\,\Upsilon(w)\ . \tag{26}$$

Again, the sketch of the proof can be found above, and the details are left out due to lack of space.

We then have

Proposition 2: The secret key rate of TPPR-M, in the asymptotic limit of an infinitely long key sequence, is

$$S \geq \sum_{m=1}^{M+1} p_m\,R_m\,H(Q_m|C_m)\ -\ h\,(p_m)\ , \tag{27}$$

where the rate R_m of distilled bits in round m is defined in (8), the key bit error probability in round m is defined in (7), and Eve's key error entropies are in (22) for rounds $m \leq M$ and in (26) for round $m = M+1$.

Proof: From Proposition 1, Eve's mutual information rate is given by the distilled key rate minus Eve's key error entropy. Using (3), the secret key rate is lower bounded by $I(K;\hat{K}) - I(K;Z,\tilde{C})$, where $\hat{K} = \mathbf{G}Y$ is Bob's estimate of the distilled bits. With the sequence length approaching infinity, $I(K;\hat{K}) = R - \sum_{m=0}^{M+1} h(p_m)$, while $H(K) = R$. ■

The rate (27) can be computed using Lemmas 1 and 2.

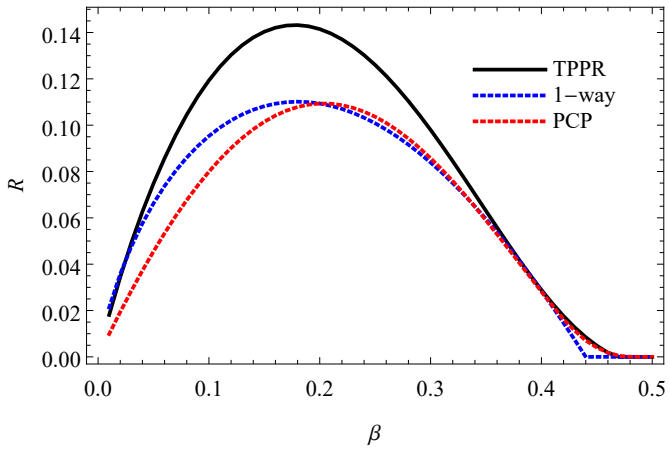

Fig. 2. Key rates when Eve's error probability is $1.5\,\epsilon_B$.

V. Performance Comparisons

It turns out that vanilla TPPR, without rounds of public parity bit correction, does not perform well in conditions where Eve has a better channel than Alice and Bob, thus resembling the one-way protocol. As an example, we have compared the secret key rates of PCP and TPPR to the upper bound of any one-way protocol of the type [8]–[10] in a situation where $\epsilon_A = \epsilon_B/2$ and when Eve's error probability is $\epsilon_E = 1.5\,\epsilon_B$. All protocols are executed in a direction where Bob's bits are corrected to correspond to Alice's. Note that if the satellite source is not collaborating with Alice and Bob, they can estimate β but cannot estimate the individual error probabilities ϵ_A and ϵ_B. Then, Alice and Bob have to blindly choose the direction of the protocol, the simulated direction being one option. The secret key rate for PCP is calculated using [12, Definition 5], rephrased from [7]. The largest rate of PCP with $M = 1,\ldots,6$ rounds is considered. TPPR rate is from (27), similarly the largest rate from $M = 1,\ldots,6$ is taken. The results are presented as functions of β in Fig. 2.

VI. Conclusions

In this paper we analyzed a two-way secret key agreement protocol TPPR that uses parity bit reconciliation to produce a secret key in a satellite setting. We demonstrated that TPPR is able to outperform the information theoretic bound limiting the performance of one-way protocols. In future work we shall analyze a complete version of TPPR protocol, where part of the parity bit error correction can be performed in public. If all the rounds are public, such a complete TPPR becomes PCP. Therefore the key rate performance of a complete TPPR is always lower bounded by that of PCP. We see this as a promising indication of TPPR being a good candidate for distilling keys from noisy environmental signals in many operational scenarios.

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[3] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," in *Advances in Cryptology*, T. Beth, N. Cot, and I. Ingemarsson, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 33–50.

[4] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE Journal on Selected Areas in Information Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[5] U. M. Maurer, "Protocols for Secret Key Agreement by Public Discussion Based on Common Information," in *Advances in Cryptology — CRYPTO' 92*, E. F. Brickell, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1993, pp. 461–470.

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

[7] M. J. Gander and U. M. Maurer, "On the secret-key rate of binary random variables," in *Proc. IEEE Int. Symp. Inform. Theory*, 1994, p. 351.

[8] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology — EUROCRYPT '93*, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[9] K. Nguyen, G. V. Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," in *Proc. Int. Symp. on Inform. Theory and its Appl.*, 2004.

[10] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information Reconciliation for Quantum Key Distribution," *Quantum Info. Comput.*, vol. 11, no. 3, p. 226–238, Mar. 2011.

[11] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," *Phys. Rev. A*, vol. 76, p. 032312, Sep 2007.

[12] D. Jost, U. Maurer, and J. L. Ribeiro, "Information-Theoretic Secret-Key Agreement: The Asymptotically Tight Relation Between the Secret-Key Rate and the Channel Quality Ratio," in *Theory of Cryptography*, A. Beimel and S. Dziembowski, Eds. Cham: Springer International Publishing, 2018, pp. 345–369.

[13] A. Gohari, O. Günlü, and G. Kramer, "Coding for positive rate in the source model key agreement problem," *IEEE Transactions on Information Theory*, vol. 66, no. 10, pp. 6303–6323, 2020.

[14] U. M. Maurer, "The strong secret key rate of discrete random triples," in *Communications and Cryptography*. Springer, 1994, pp. 271–285.

[15] J. Lietzén, R. Vehkalahti, and O. Tirkkonen, "A Two-way QKD Protocol Outperforming One-way Protocols at Low QBER," in *Proc. IEEE Int. Symp. Inform. Theory*, 2020, pp. 1106–1111.

[16] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT 2000, LNCS*, vol. 1807, 2000, pp. 351–368.