Sending-or-Not-Sending Twin-Field Quantum Key Distribution with Additional Space Multiplexing

Hai Xu¹, Xiao-Long Hu¹,², Cong Jiang¹,³, Zong-Wen Yu¹,⁴, and Xiang-Bin Wang¹,³,⁵,⁶†
¹State Key Laboratory of Low Dimensional Quantum Physics, Department of Physics, Tsinghua University, Beijing 100084, China
²School of Physics, State Key Laboratory of Optoelectronic Materials and Technologies, Sun Yat-sen University, Guangzhou 510275, China
³Jinan Institute of Quantum technology, SAICT, Jinan 250101, China
⁴Data Communication Science and Technology Research Institute, Beijing 100191, China
⁵Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People’s Republic of China
⁶Shenzhen Institute for Quantum Science and Engineering, and Physics Department, Southern University of Science and Technology, Shenzhen 518055, China

We propose to multiplex additional physical quantity such as photon polarization in Sending-or-Not-Sending (SNS) Twin-Field quantum key distribution (TF-QKD) in Fock space. Through multiplexing additional space such as photon polarization, we can post select events according to the outcome of observation to the additional quantity. This compresses the bit-flip error rate in the post selected events of SNS protocol. Calculation shows that the method using additional space multiplexing can improve the performance a lot in practical TF-QKD.

I. INTRODUCTION

Quantum Key Distribution (QKD) provides a promising approach to unconditional secure communication [1–10]. The decoy-state method [5,6] can keep the unconditional security of QKD even the imperfect single photon sources is used, and those security loopholes caused by imperfect detection devices can be closed by Measurement-Device-Independent (MDI)-QKD [9,11]. With the development in both theory and experiments on recent years [12–36], QKD is gradually mature to real world deployment over optical fiber and satellite [2,3,37,38]. Especially, the emergence of Twin-Field (TF)-QKD [19] have improved the secure distance drastically both in laboratory optical fiber experiments [39–44] and field test [45,47]. Note that, TF-QKD is also free from detection loophole.

Using fresh key is the most important application mode in practice. This requests a high efficiency with small data size. However, due to the finite-key effect [13,20–23,42,45,50], it’s not an easy job to make a satisfactory result with small data size. The SNS protocol [57] has its advantage in this scenario because it uses the traditional decoy-state analysis and hence the existing theories of finite-key effects can directly apply. However, the original SNS protocol uses small sending probability so as to control the bit-flip error rate. Applying the AOPP method [52,53,55] to the SNS protocol, we can compress bit-flip error significantly by post selection, even we use large sending probability. Theories for finite-key effects have been presented [52,53] for the AOPP method and they make it clear that the AOPP-SNS protocol can make a high key rate and long distance even with finite data size. So far the AOPP-SNS protocol has been implemented by a number of experiments [41,42,45,49,55], including the QKD experiments with the longest optical distance in field test [47]. Here we present another method, SNS protocol with additional space multiplexing (ASM). By multiplexing the additional space such as photon polarization in SNS protocol, this method can also compress the bit-flip error rate significantly and it has a better performance than all prior art methods in finite-key with small data size. This makes it a good candidate protocol for real application of QKD demanding fresh key.

This paper is arranged as follows. In Sec. II, we introduce our ASM method in detail. Then the security proof of this new method can be found in Sec. III and we give numerical simulation results in Sec. IV. An improved protocol of this method is given in Sec. V. This article is ended with concluding remarks.

II. SNS PROTOCOL WITH ADDITIONAL SPACE MULTIPLEXING

Besides the Fock space used for the SNS protocol, we consider an ASM method represented by physical quantity $\mathbf{R}$ which can be, e.g., polarization, spatial angular momentum, frequency, and so on. In each time window of the SNS protocol, Alice (Bob) randomly selects $\mathbf{R}$ value from the set $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_m (m \geq 2)$, if she (he) decides to send out a non-vacuum pulse. (Vacuum has no additional space.) In this way, they (Alice and Bob) can realize the SNS protocol with different values $\mathbf{r}_1, \mathbf{r}_2, \ldots, \mathbf{r}_m$.
FIG. 1: Schematic setup for SNS protocol with additional space multiplexing. There are two groups of detectors, left or right to the beam splitter. Charlie is supposed to announce the heralded time windows with the information of which detector has clicked. This has actually announced both the side (left or right to the beam splitter) of the clicked detector and the specific R value \( r_1, r_2 \ldots \) or \( r_m \) he has observed.

separately. By post selection with specific R, the bit-flip error is reduced and the performance of the protocol is improved. Say, at a certain time window, if Charlie’s measurement station is heralded with value \( r_1 \) of R while Alice (Bob) has sent a coherent state with a different R value, e.g., \( r_2 \), she (he) will request to discard the event of the time window. Surely, this type of post selection with ASM method can reduce wrong bits. As given in Fig. 1, \( r_i \) indicates different R value Charlie has observed.

Obviously, there are many different physical quantities as candidates of quantities for the ASM method, e.g., polarization, frequency, time bin, and so on.

For a better understanding the idea of using ASM method, here we restate our main idea using the specific R of polarization. At any specific time window, if Alice (Bob) decides to send a non-vacuum coherent state, she (he) will randomly choose its polarization from H or V. Charlie has two measurement ports after the beamsplitter, as shown in Fig 2. Each of them measures the photon polarization, H or V. Charlie announces the one-detector heralded event and the polarization he has detected, i.e., Charlie announces the information of a specific detector at a specific port that has clicked. In the case that Charlie’s announced polarization of his measurement outcome is different from the polarization of the non-vacuum coherent state sent out by Alice (Bob), she (he) requests to discard that event.

Here the complete protocol with ASM method of polarization:

**Step 1.** At any time window, Alice (Bob) randomly decides with probabilities \( p_v, p_x, p_y, p_z \) to send out a vacuum pulse of intensity \( \mu_x = 0 \), a non-vacuum pulse of intensity \( \mu_x > 0 \), a non-vacuum pulse of intensity \( \mu_y > \mu_x \), or a non-vacuum pulse of intensity \( \mu_z > \mu_x \). Each of them also chooses the polarization H or V randomly whenever she or he decides to send out a non-vacuum pulse (intensity \( \mu_x, \mu_y, \) or \( \mu_z \)).

Here we defined two time windows: heralded time window and **accepted** time window.

Heralded time window: a time window when there is one and only one detector clicks at Charlie’s measurement station. And the corresponding event is defined as a heralded event.

**Accepted** time window: a heralded time window that neither Alice nor Bob requests to discard the event happened at this time window. And the corresponding event is defined as an **accepted** event.

**Step 2.** Charlie announces those heralded time windows with the specific information of which detector has clicked. Note that in announcing which detector has clicked, Charlie has actually announced both the side (left or right to the beam splitter) of the clicked detector and the polarization (H or V) he has observed.

**Step 3.** At any heralded time window, if Alice (Bob) has decided to send out a non-vacuum pulse and the polarization she (he) has chosen for the pulse is different from the measurement outcome of polarization announced by Charlie, she (he) requests to discard the event happened at the time window.

**Step 4.** They each announces those time windows
which she (he) has chosen intensities $\mu_x$ and $\mu_y$. They also announce some time windows when Alice or Bob has decided to send out vacuum. They use the remaining survived events from the heralded time windows for code-bits. Alice assigns a bit value 1 if she has decided to send out a pulse of intensity $\mu_z$, and 0 if she has decided to send out vacuum, i.e., intensity $\mu_x = 0$. Bob’s definition of bit value is in the opposite of Alice’s. With decoy-state analysis, they can obtain the secure final key with the following key length formula:

$$N_f = n_1[1 - H(e_1^{\text{ph}})] - f n_t H(E_t) - \log_2 \frac{2}{\varepsilon_{\text{cor}}} - 2 \log_2 \frac{1}{\sqrt{2} \varepsilon_{PA} \varepsilon},$$

where $H(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary Shannon entropy function, $f$ is error correction efficiency factor. Here $\varepsilon_{\text{cor}}$ is the failure probability of error correction, $\varepsilon_{PA}$ is the failure probability of privacy amplification, $\varepsilon$ is the coefficient when using the chain rules for smooth min- and max-entropies [59]. And $n_t$ is the number of code-bits, value $E_t$ is the bit-flip error rate of those $n_t$ code-bits. In our protocol here, an event can be counted for code-bit if the following conditions are satisfied:

1. It is from a heralded time window;
2. Alice and Bob has chosen intensity $\mu_z$ or $\mu_y$;
3. Charlie’s announced polarization observed by him is the same with the polarization of the pulse of intensity $\mu_z$ sent out by Alice or Bob;
4. Each one’s choice of intensity for the sent out pulse is never announced.

$e_1^{\text{ph}}$ is the phase-flip error rate of untagged bits and $n_1$ is the number of untagged bits. Values of $n_1$ and $e_1^{\text{ph}}$ can be verified by decoy-state analysis, as shown in Refs. [49, 57, 60]. They need to announce intensities of pulses they each has used in those time windows which are not announced to be heralded time windows by Charlie. This announcement, together with those announced information in Step 4 of our protocol, enables them to take the same kind of decoy-state analysis used in Refs. [49, 57, 60]. In estimating $e_1^{\text{ph}}$, they have to set the phase slice condition [51] in post selecting events from accepted time windows when both of them have chosen intensity $\mu_x$.

Note that $n_t$ and $E_t$ can be observed directly in the experiment.

We define $t_r$ time window: a time window when Alice sends out pulse of intensity $\mu_3$ and Bob sends out pulse of intensity $\mu_r$, where $t, r$ can be $v, x, y$ or $z$.

Remark. In Step 3 above, both Alice and Bob can decide to discard events when her or his polarization of pulse of intensity $\mu_z$ is different from Charlie’s observed polarization. This post selection plays a key role in compressing the bit-flip error rate of those $n_t$ survived code-bits. Those wrong bits from heralded $zz$ time windows are for sure rejected by this step if Alice and Bob have chosen different polarization. Here the result of bit-flip error rate compressing alone is not as effective as that of AOPP [58], but the phase-flip error rate does not rise as what happens in AOPP. This makes it possible of our protocol to produce advantageous results under certain conditions, especially when the fresh key can only be distilled from a small data size.

### III. SECURITY PROOF

Here we shall show the MDI security for our protocol with ASM method as presented in the earlier section. The original SNS protocol [57] takes MDI security and it is not limited to any specific additional space. Without loss of generality, we consider the security of this new protocol with polarization multiplexing as an example. We shall start from virtual protocols.

Protocol $\mathcal{H}$, a bit-flip error free protocol using polarization $H$ for non-vacuum pulses. With secret discussion in advance, there are only time windows when both of them send intensity $\mu_x$ and time windows when one side sends out intensity $\mu_x$ and the other side sends vacuum. In a 4-intensity protocol, there are also time windows that one side sends out intensity $\mu_y$ and the other side sends out vacuum. At all time windows, the non-vacuum pulses are prepared in polarization $H$. In protocol $\mathcal{H}$, they take post selection using polarization information. In particular, after sending out quantum states, there are following steps for classical communication and post selection:

**Step-1** Charlie announces those heralded time windows and the polarization ($H$ or $V$) he has observed, and also the position (right or left to the beam splitter) of the heralded detector.

**Step-2** Given any heralded time window with a polarization $V$ announced by Charlie, any party (Alice or Bob) who has sent out the non-vacuum pulse in the time window will announce rejection and the event at that time window is discarded; given any heralded time window with a polarization $H$ announced by Charlie, they (Alice and Bob) keep silent and the event at that heralded time window is accepted and will be used in further data processing later.

**Step-3** They take post data processing based on the accepted events above and they distill the final key with key length

$$n_\mathcal{H} = n_1(\mathcal{H}) \left[1 - H(e_1^{\text{ph}}(\mathcal{H}))\right].$$

Here $n_1(\mathcal{H})$ is the number of untagged bits from Protocol $\mathcal{H}$, and $e_1^{\text{ph}}(\mathcal{H})$ is their phase-flip error rate.

As shown in the Appendix A protocol $\mathcal{H}$ is MDI secure because it is equivalent to the original SNS protocol.

Replacing all polarization $H$ by polarization $V$ in protocol $\mathcal{H}$ above, we have protocol $\mathcal{V}$, which is the bit-flip error free protocol with polarization $V$. It has the following key length formula:

$$n_\mathcal{V} = n_1(\mathcal{V}) \left[1 - H(e_1^{\text{ph}}(\mathcal{V}))\right].$$
And \( n_1(\mathcal{V}) \) is the number of untagged bits from Protocol \( \mathcal{V} \), and \( e_1^{ph}(\mathcal{V}) \) is their phase-flip error rate.

Also, mixing the two protocols above, we have protocol \( \mathcal{M} \), where in some time windows they use protocol \( \mathcal{H} \) and some time windows they use protocol \( \mathcal{V} \). They use Step 2 and Step 3 in the real protocol in Sec. II to do post selection. In particular, Charlie announces the heralded time windows with polarization \( H \) or \( V \) he has observed. Given any heralded time window announced by Charlie, any party (Alice or Bob) who has sent out a non-vacuum pulse in the time window announces rejection if the polarization of the sent out non-vacuum pulse is different from polarization announced by Charlie, otherwise, he or she keeps silent. If both Alice and Bob keep silent, the event of the corresponding heralded time window is accepted. The secure key length formula is

\[
N_f = n_H + n_V
\]

(4)

Of course they can replace phase-flip error rate of each protocol by the averaged phase-flip error rate and use the following key length formula:

\[
N'_f = n_1 \left[ 1 - H(e_1^{ph}) \right],
\]

(5)

where

\[
\begin{align*}
n_1 &= n_1(\mathcal{H}) + n_1(\mathcal{V}), \\
e_1^{ph} &= e_1^{ph}(\mathcal{H})n_1(\mathcal{H}) + e_1^{ph}(\mathcal{V})n_1(\mathcal{V}).
\end{align*}
\]

(6)

We can use this because inequality \( N_f \geq N'_f \) always hold mathematically. Using this formula, they don’t have to know which bits belong to which protocol.

Now consider the real protocol where each side takes probabilities to send different types of intensities with 50% probability choosing polarization \( H \) or \( V \). In the protocol, after Charlie’s announcement, they take post selection by Step 3 in the real protocol in Section II then they each announced those time windows she or he has sent out intensity \( \mu_c \) or \( \mu_d \) and the corresponding polarization. After post selection in the real protocol, the survived events from heralded time windows of \( vv \), \( zz \), \( vz \), \( zv \) after post selection includes 2 kinds of subsets: Subset \( C_H \oplus C_V \) which is the post selected data from the mixing of Protocol \( \mathcal{H} \) and Protocol \( \mathcal{V} \), and subset \( T \) includes all other data. In particular, \( T \) includes heralded \( vv \) events (both sides send out vacuum), and heralded events where both side have sent out non-vacuum (intensity \( \mu_x \) or \( \mu_y \) with same polarization. Subset \( C_H \oplus C_V \) contains events of \( vz \) and \( vz \) only, there is no bit-flip error. Subset \( T \) contains code-bit events of \( vv \) and \( zz \), which shall be treated as tagged bits. Note that not all \( zz \) events can survive from the post selection. The \( zz \) events from heralded time windows when Alice and Bob have chosen different polarization have been rejected in the post selection.

If they only use data of subset \( C_H \oplus C_V \), they can simply apply Eq. (5) for final key length, which is secure. Regarding data in subset \( T \) as tagged bits, they can distill the secure final key with key length formula:

\[
\hat{N}_f = n_1 \left[ 1 - H(e_1^{ph}) \right] - f n_1 H(E_f).
\]

(7)

The notation \( n_1 \) is for the total number of bits in subsets \( C_H \oplus C_V \) and \( T \), and notation \( E_f \) is for the bit-flip error rate of these \( n_1 \) bits.

Thus the security of this new protocol with polarization multiplexing has been proved. Obviously, this security proof process can be applied to the more general additional space multiplexing cases using whatever physical quantity \( R \), which completes our security proof.

### IV. NUMERICAL SIMULATION

In the following, we use linear model [49] with standard optical fiber (0.2 dB/km) to simulate the observed values in the experiment. Without loss of generality, we consider symmetrical channel, also the intensity of pulses and the corresponding channel loss are not affected by additional space. In previous works, the original SNS protocol [57] has been improved, especially by the AOPP method [59, 58], which has been adopted in several experiments [41, 42] through laboratory optical fiber, and create the record for field test [43, 44] of all types of fiber-based QKD systems. We compare this work with AOPP, with the fluctuation and finite-key effects taken into consideration. In this work, We take \( \xi = 10^{-10} \) as the failure probability of Chernoff Bound [13, 62], and we set \( \varepsilon_{	ext{cor}} = \varepsilon = \varepsilon_{PA} = \xi \).

| \( d \) | \( \eta_0 \) | \( E_d \) | \( N \) |
|---|---|---|---|
| A | \( 1 \times 10^{-8} \) | 0.50 | 0.03 | \( 1 \times 10^9 \) |
| B | \( 1 \times 10^{-8} \) | 0.50 | 0.03 | — |
| C | \( 1 \times 10^{-9} \) | 0.50 | 0.03 | \( 1 \times 10^{10} \) |
| D | \( 1 \times 10^{-8} \) | 0.50 | 0.03 | \( 1 \times 10^{12} \) |

TABLE I: Device parameters used in numerical simulations. \( d \): the dark count rate. \( \eta_0 \): the detection efficiency of all detectors. \( E_d \): the misalignment error. \( N \): total number of time windows. The fiber loss is set as 0.2 dB/km, and we set the error correction efficiency factor as \( f = 1.1 \) in this work.

In Fig. 3 we compare the secure key rate of ASM method of polarization given by Eq. (1) (the dark solid line), the original SNS protocol [57] (purple dot-dash line), and the AOPP method [55, 58] (red dash line). The simulation results show that, given a small data size \( (N \sim 10^8) \), the secure key rate of the new protocol we present here, is about 70% higher than that of the original SNS protocol [57], and the secure distance is 25 km longer compared with AOPP method [55, 58]. Parameters are given in line A of Tab. I.
FIG. 3: (Color online) The optimized key rates of ASM method of polarization by Eq. (1) (the dark solid line), the original SNS protocol [57] (purple dot-dash line), and the AOPP method [35, 58] (red dash line). Devices’ parameters are given by row A of Table I.

FIG. 4: (Color online) Asymptotic key rates of ASM method of WDM, the total number of wavelength is \( m = 20 \) (dark solid line), \( m = 6 \) (red dash line), \( m = 3 \) (blue dotted line) and \( m = 2 \) (green dot-dash line) respectively, and that given by the original SNS protocol [57] (dash-dot-dot line). Note that the result of \( m = 2 \) is also the result of ASM with photon polarization. The simulation results show that, the secure key rate of the new protocol increases obviously with the increase of total number of wavelength. PLOB-1 is repeater-less key rate bound [63] with detector efficiency \( \eta_0 = 0.5 \), i.e., the relative limit of repeater-less key rate. PLOB-2 is repeater-less key rate bound with detector efficiency \( \eta_0 = 1 \), i.e., the absolute limit of repeater-less key rate. The absolute PLOB bound and the relative PLOB bound are the bounds with whatever devices and the practical bound assuming the limited detection efficiency, respectively. At the distance of 300 km, the secure key rate of \( m = 2 \) is about 80\% higher than the secure key rate of the original SNS protocol [57], and this number for \( m = 3 \), \( m = 6 \) and \( m = 20 \) are about 150\%, 300\% and 700\% respectively. Parameters are given in line B of Tab. I.

FIG. 5: (Color online) The optimized key rates of ASM method of WDM given by Eq. (1), the total number of wavelength is \( m = 20 \) (dark solid line), \( m = 6 \) (red dot-dash line), \( m = 3 \) (brown dash-dot-dot line) and \( m = 2 \) (blue dash line) respectively, and the original SNS protocol [57] (purple short dotted line), and AOPP method [53] (green dotted line). PLOB-1 is repeater-less key rate bound [63] with detector efficiency \( \eta_0 = 0.5 \), i.e., the relative limit of repeater-less key rate. PLOB-2 is repeater-less key rate bound with detector efficiency \( \eta_0 = 1 \), i.e., the absolute limit of repeater-less key rate. Devices’ parameters are given by row C of Table I.

In Fig. 4 we compare the secure key rate of ASM method of WDM in asymptotic case (the total number of wavelength is \( m = 20 \), \( m = 6 \), \( m = 3 \) and \( m = 2 \) respectively), with that given by the original SNS protocol [57] (dash-dot-dot line). PLOB-1 is repeater-less key rate bound with detector efficiency \( \eta_0 = 0.5 \), i.e., the relative limit of repeater-less key rate. PLOB-2 is repeater-less key rate bound with detector efficiency \( \eta_0 = 1 \), i.e., the absolute limit of repeater-less key rate. The absolute PLOB bound and the relative PLOB bound are the bounds with whatever devices and the practical bound assuming the limited detection efficiency, respectively. At the distance of 300 km, the secure key rate of \( m = 2 \) is about 80\% higher than the secure key rate of the original SNS protocol [57], and this number for \( m = 3 \), \( m = 6 \) and \( m = 20 \) are about 150\%, 300\% and 700\% respectively. Parameters are given in line B of Tab. I.

In Fig. 5 we compare the secure key rate of ASM method of WDM given by Eq. (1) (total number of wavelength is \( m = 20 \), \( m = 6 \), \( m = 3 \) and \( m = 22 \) respectively), with that given by the original SNS protocol [57] and AOPP method [53]. We can see that, the secure
key rate of the new protocol increases obviously with the increase of total number of wavelength, and when this number becomes larger like $m = 20$, the secure distance becomes shorter, for the influence of dark count becomes obvious. Parameters are given in line C of Tab. [1]

In Fig. [6] we compare the secure key rate of ASM method of WDM given by Eq. (1) (total number of wavelength is $m = 6$, $m = 2$ respectively, with that given by the original SNS protocol [57] and AOPP method [53]. PLOB-1 is repeater-less key rate bound [54] with detector efficiency $\eta_0 = 0.5$, i.e., the relative limit of repeater-less key rate. PLOB-2 is repeater-less key rate bound with detector efficiency $\eta_0 = 1$, i.e., the absolute limit of repeater-less key rate. Devices’ parameters are given by row D of Table I.

V. IMPROVED PROTOCOL

In our calculations above we have used our protocol in Sec. [II] which takes the same decoy-state analysis method with the prior works [49, 53, 60] for a fair comparison. Definitely, the recently proposed improved method of SNS protocol using decoy-state analysis after error correction [64] can also apply to the ASM method in this work. In this case, the announcements in Step 4 of our protocol in Sec. [II] are not necessary and the key rate can be further improved. They can choose the code-bit option $[x, y, z] ([y, z])$, i.e., using accepted events of all those heralded $lv$ and $vr$ time windows for code-bits, with $l, r \in \{x, y, z\} (l, r \in \{y, z\})$. The key length formulas such as Eq.(4), Eq.(B2) and Eq.(B10) in Ref. [64] can all be used here.

VI. CONCLUSION

Based on SNS TF-QKD protocol [57], we propose a new protocol with additional space multiplexing. Additional space like polarization and WDM are given here as examples. Our simulation results show that, our new method can achieve better performance at all distance points over original SNS protocol. Further, when the data size is small like $10^8$, this ASM method can improve the maximum distance of AOPP method by more than 20 km, and greatly improve the key rate at long distances. Our protocol can also apply to efficient quantum digital signature by taking the post data processing method such as Ref. [65, 66]. This will be reported elsewhere.

VII. ACKNOWLEDGMENT

We acknowledge the financial support in part by Minis- tration of Science and Technology of China through National Natural Science Foundation of China Grant Nos.11974204, 12174215, 12104184, 12147107; Open Research Fund Program of the State Key Laboratory of Low-Dimensional Quantum Physics Grant No. KF202110.

Appendix A: Protocol $\mathcal{H}$ is MDI secure

Consider the post selection in Step-2 of Protocol $\mathcal{H}$ in Sec. [III]. Evidently, any independent third party can also make the same post selection result though the independent party does not know which party (Alice or Bob) has sent out a non-vacuum pulse at any time window. So we can replace Step-2 there by the following equivalent step:

Step-2’: (i) The independent party Adam announces rejecting the event from a heralded time window announced by Charlie if Charlie has announced a polarization $V$ for the measurement outcome in that time window.

(ii) If Adam announced rejection, any party from Alice and Bob will announce that he (she) has sent out a non-vacuum pulse in the time window if she/he has indeed sent out a non-vacuum pulse in the time window.

(iii) Adam announces to accept the event for further processing if Charlie has announced a polarization $H$ for
his measurement outcome in the corresponding heralded time window. 

Here the announcement of (ii) in Step-2' above does not affect the security because that’s an announcement about rejected events only. So, the security of protocol \( \mathcal{H} \) is equivalent to protocol \( \mathcal{H}_1 \) here but only takes the (i) and (iii) in its Step-2' for post selection. 

In Alice and Bob’s viewpoint, they can regard Adam’s announcement as the final form of Charlie’s announcement about the post selection, i.e., they regard Adam as Charlie’s processor and then output the final message after processing. In this viewpoint, protocol \( \mathcal{H}_1 \) is just the original SNS protocol wherever Charlie makes the post selection of events for Alice and Bob. This completes the MDI security of protocol \( \mathcal{H} \).

[1] C. H. Bennett and G. Brassard, Theor. Comput. Sci. 560, 7 (2014).
[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupu, C. Ottaviani, et al., Advances in Optics and Photonics 12, 1012 (2020).
[3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Reviews of Modern Physics 92, 025002 (2020).
[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics 74, 145 (2002).
[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Reviews of modern physics 81, 1301 (2009).
[6] W.-Y. Hwang, Physical Review Letters 91, 057901 (2003).
[7] X.-B. Wang, Physical Review Letters 94, 230503 (2005).
[8] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters 94, 230504 (2005).
[9] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters 108, 130503 (2012).
[10] S. L. Braunstein and S. Pirandola, Physical Review Letters 108, 130502 (2012).
[11] X.-B. Wang, Physical Review A 87, 012320 (2013).
[12] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Physical Review Letters 111, 130501 (2013).
[13] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature communications 5, 3732 (2014).
[14] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, Physical Review Letters 115, 160502 (2015).
[15] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nature Photonics 10, 312 (2016).
[16] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, et al., Physical Review Letters 117, 190501 (2016).
[17] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li, et al., Nature 549, 43 (2017).
[18] A. Boaron, G. Boso, D. Rusca, C. Vulăcic, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, et al., Physical Review Letters 121, 190505 (2018).
[19] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature 557, 400 (2018).
[20] J. Müller-Quade and R. Renner, New Journal of Physics 11, 085006 (2009).
[21] R. Renner, Ph.D. thesis, SWISS FEDERAL INSTITUTE OF TECHNOLOGY ZURICH (2005).
[22] R. König, R. Renner, A. Barışka, and U. Maurer, Physical Review Letters 98, 140502 (2007).
[23] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature communications 3, 634 (2012).
[24] S. Pirandola, C. Ottaviani, G. Spedaliere, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics 9, 397 (2015).
[25] C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Optica 4, 1016 (2017).
[26] H. Semenenko, P. Silber, A. Hart, M. G. Thompson, J. G. Rarity, and C. Erven, Optica 7, 238 (2020).
[27] L. Cao, W. Luo, Y. Wang, J. Zou, R. Yan, H. Cai, Y. Zhang, X. Hu, C. Jiang, W. Fan, et al., Physical Review Applied 14, 011001 (2020).
[28] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, et al., Physical Review Letters 125, 260503 (2020).
[29] F. Xu, M. Curty, B. Qi, and H.-K. Lo, New Journal of Physics 15, 113007 (2013).
[30] F. Xu, H. Xue, and H.-K. Lo, Physical Review A 89, 052333 (2014).
[31] Z.-W. Yu, Y.-H. Zhou, and X.-B. Wang, Physical Review A 93, 032318 (2015).
[32] Y.-H. Zhou, Z.-W. Yu, and X.-B. Wang, Physical Review A 94, 042324 (2016).
[33] H. Liu, J. Wang, H. Ma, and S. Sun, Physical Review Applied 12 (2019).
[34] X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, Advanced Quantum Technologies 4, 2100069 (2021).
[35] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Physical Review A 103, 012402 (2021).
[36] J. Teng, Z.-Q. Yin, G.-J. Fan-Yuan, F.-Y. Lu, R. Wang, S. Wang, W. Chen, W. Huang, B.-J. Xu, G.-C. Guo, et al., Phys. Rev. A 104, 062441 (2021), URL: https://link.aps.org/doi/10.1103/PhysRevA.104.062441.
C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, et al., Physical Review Letters 123, 100505 (2019).
[44] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, et al., Nature photonics 14, 422 (2020).
[45] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, et al., Physical Review Letters 126, 250502 (2021).
[46] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, et al., Physical Review Letters 128, 180502 (2022).
[47] C. Clivati, A. Meda, S. Donadello, S. Virzi, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, et al., Nature Communications 13, 157 (2022).
[48] C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A 89, 022307 (2014).
[49] C. Jiang, Z.-W. Yu, X.-L. Hu, and X.-B. Wang, Physical Review Applied 12, 024061 (2019).
[50] K. Maeda, T. Sasaki, and M. Koashi, Nature communications 10, 1 (2019).
[51] H.-L. Yin and Z.-B. Chen, Scientific Reports 9, 17113 (2019).
[52] C. Jiang, X.-L. Hu, H. Xu, Z.-W. Yu, and X.-B. Wang, New Journal of Physics 22, 053048 (2020).
[53] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, New Journal of Physics 23, 063038 (2021).
[54] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, npj Quantum Information 7, 1 (2021).
[55] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, et al., Physical Review Letters 128, 180502 (2022).
[56] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, et al., Nature photonics 16, 154 (2022).
[57] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Physical Review A 98, 062323 (2018).
[58] H. Xu, Z.-W. Yu, C. Jiang, X.-L. Hu, and X.-B. Wang, Physical Review A 101, 042330 (2020).
[59] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, IEEE Transactions on Information Theory 59, 2603 (2013).
[60] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Scientific Reports 9, 3080 (2019).
[61] X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, Physical Review A 100, 062337 (2019).
[62] H. Chernoff et al., The Annals of Mathematical Statistics 23, 493 (1952).
[63] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nature communications 8, 15043 (2017).
[64] X.-L. Hu, C. Jiang, Z.-W. Yu, and X.-B. Wang, arXiv preprint arXiv:2204.12890 (2022).
[65] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Physical Review A 93, 032325 (2016).
[66] J.-Q. Qin, C. Jiang, Y.-L. Yu, and X.-B. Wang, Physical Review Applied 17, 044047 (2022).