Reliability and Latency Analysis for Wireless Communication Systems with a Secret-Key Budget

Karl-Ludwig Besser, *Member, IEEE*, Rafael F. Schaefer, *Senior Member, IEEE*, and
H. Vincent Poor, *Life Fellow, IEEE*

Abstract—We consider a wireless communication system with a passive eavesdropper, in which a transmitter and legitimate receiver generate and use key bits to secure the transmission of their data. These bits are added to and used from a pool of available key bits. In this work, we analyze the reliability of the system in terms of the probability that the budget of available key bits will be exhausted. In addition, we investigate the latency before a transmission can take place. Since security, reliability, and latency are three important metrics for modern communication systems, it is of great interest to jointly analyze them in relation to the system parameters. In particular, we show under what conditions the system may remain in an active state indefinitely, i.e., never run out of available secret-key bits. The results presented in this work will allow system designers to adjust the system parameters in such a way that the requirements of the application in terms of both reliability and latency are met.

Index Terms—Physical layer security, Ruin theory, Secret-key generation, Reliability analysis, Latency analysis.

I. INTRODUCTION

The next generation of mobile communication systems 6G, is expected to bring significant advances in terms of capacity, speed, and connectivity [1]. However, with the increasing reliance on wireless networks for a variety of applications and the growing amount of sensitive information transmitted over these networks, the need for robust security measures becomes paramount [2]. While cryptography is currently the most widely used technique to protect data transmissions from potential eavesdroppers, physical layer security provides an alternative solution [3], [4]. In particular, physical layer security allows a system to achieve a degree of security that is provable from an information theoretic viewpoint, rather than relying on the presumed impracticality of computational problems. This is done by exploiting the physical properties of the communication

Karl-Ludwig Besser was with the Institute for Communications Technology, Technische Universität Braunschweig, 38106 Braunschweig, Germany, and is now with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544, USA (email: karl.besser@princeton.edu). Rafael F. Schaefer is with the Chair of Information Theory and Machine Learning, the BMBF Research Hub 6G-life, the Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop (CeTI)," and the 5G Lab Germany, Technische Universität Dresden, 01062 Dresden, Germany (e-mail: rafael.schaefer@tu-dresden.de). H. Vincent Poor is with the Department of Electrical and Computer Engineering, Princeton University, Princeton, NJ 08544, USA (email: poor@princeton.edu).

The work of K.-L. Besser is supported by the German Research Foundation (DFG) under grant BE 8098/1-1. The work of R. F. Schaefer is supported by the German Federal Ministry of Education and Research (BMBF) within the national initiative on 6G Communication Systems through the research hub 6G-life under Grant 16KISK001K as well as the 6G-ANNA project under Grant 16KISK103. The work of H. V. Poor is supported by the U.S. National Science Foundation under Grants CNS-2128448 and ECCS-2335876.

channel between the transmitter and a legitimate receiver. There are several ways to do this [5]. In particular, in addition to using wiretap codes, the characteristics of the communication channel can be used to securely generate bits that are shared only by the transmitter and the legitimate receiver. These bits can then act as a secret key in the form of a one-time pad to secure a message.

Secret-key generation (SKG) uses channel reciprocity to establish a common randomness between the transmitter and the legitimate receiver, which in turn can be used to distill the key bits [6], [7]. Due to the physical nature of wireless propagation, the channel between transmitter and legitimate receiver is difficult to predict for outside observers. Therefore, it is not possible for a potential eavesdropper to reconstruct the generated key bits, i.e., they can act as a shared key between transmitter and legitimate receiver. For the specific implementation of SKG, various schemes have been proposed in the literature [8]–[11].

In this work, we consider a wireless communication system in which the transmitter and a legitimate receiver perform SKG to secure the transmission of their data. The generated key bits are added to and used from a pool of available bits. We analyze the reliability in terms of the probability that the budget of available key bits will be exhausted. In addition, we investigate the latency before a transmission can take place. For the analysis in this work, we leverage tools from ruin theory [12].

Classical ruin theory addresses the problem of modeling the evolution of an insurance company's financial surplus and its risk of becoming insolvent [12]. In the classical ruin-theoretic model, also known as the Cramér-Lundberg model [13, Chap. IV.1], the insurance company experiences the following two cash flows. On the one hand, it receives a constant stream of income from insurance premiums. On the other hand, random claims arrive according to a Poisson process. This leads to problems such as calculating the probability of ruin, i.e., the probability that the total surplus becomes negative.

Tools from ruin theory have been applied in previous works to various problems in the broad area of wireless communications. Along the traditional lines of considering monetary quantities, the probability of financial ruin for network-sharing arrangements is considered in [14]. Other applications include resource allocation, e.g,. spectrum sharing [15], [16], user association [17], [18], and power allocation [18]. In [18], a unmanned aerial vehicle (UAV)-assisted cellular network is considered. The authors use the traditional ruin-theoretic model of constant income and random claims to describe the available

energy of the UAVs. The UAVs have only a finite amount of stored energy, which is consumed when transmitting data. The energy consumption corresponds to the claims in the ruin-theoretic model. At the same time, the battery is recharged by harvesting solar energy at a constant rate, which corresponds to the income stream in the traditional insurance model.

While we also use the basic structure of the traditional ruin-theoretic model of income and claim, we consider an adapted model in this work. In particular, the income rate is not constant but a random variable, since the quality of the wireless channels, and thus the SKG rate, varies randomly. Additionally, we assume two different scheduling schemes for generating new key bits and transmitting messages, which affects the way that claims arrive.

To the best of the authors' knowledge, this work is the first to consider a communication system with a secret-key budget and the goal of this work is to provide a framework for a theoretical analysis of such systems. Therefore, the results derived in this work are applicable to a variety of scenarios and, in particular, they are not limited to a specific underlying SKG scheme. Our main contributions and the outline of the manuscript are summarized as follows.

- We formulate a model for a communication system with a secret-key (SK) budget, in which new SK bits are generated and then used for securely transmitting messages to a legitimate receiver (Section III).
- For this model, we first consider a scheme where SKG and transmission alternate (Section IV). Reliability is analyzed in terms of both the outage probability and latency. It is shown that the system will eventually run out of key bits to securely transmit messages with probability one (Corollary 1).
- In addition, we investigate an alternative operating scheme where messages arrive randomly with probability p in each time slot and SKG is performed whenever no secure message is to be transmitted (Section V). For this setting, it may happen that the communication system can operate indefinitely. We characterize the range of p for which this is possible (Corollary 2).

The source code to reproduce all presented results and simulations is made publicly available at [19]. The provided source code can also be freely adapted to custom numerical examples.

Notation: Random variables are denoted in capital boldface letters, e.g., $\boldsymbol{X}$, and their realizations in small letters, e.g., x. We use $F_{\boldsymbol{X}}$ and $f_{\boldsymbol{X}}$ for the probability distribution and its density, respectively. The expectation is denoted by $\mathbb{E}$ and the probability of an event by $\Pr$. The relation $\boldsymbol{X} \overset{d}{=} \boldsymbol{Y}$ holds for two random variables $\boldsymbol{X}$ and $\boldsymbol{Y}$ when they are distributed according to the same probability distribution. The Bernoulli distribution with mean p is denoted as $\mathcal{B}(p)$. The indicator function is written as $\mathbb{1}$.

II. PRELIMINARIES AND BACKGROUND KNOWLEDGE

The two primary groups of themes that are touched upon in this work are secret-key generation and ruin theory. In order to improve the flow of reading, we will give a brief introduction to these areas in this section.

A. Secret-Key Generation

One way to achieve perfect information-theoretic secrecy is the use of a one-time pad [20]. This one-time pad needs to consist of key bits that are only known to the legitimate parties. Secret-key generation is a way for two legitimate communication parties to agree on such secret key bits through exploiting the physical properties of their communication channel [21]. In order to achieve this, multiple models and algorithms have been proposed and analyzed in the literature for various communication scenarios [22]–[25]. This includes static environments [26], quasi-static fading channels [27], and fast-fading channels with correlated channels [28], [29].

The concept behind secret-key agreement is that Alice and Bob have access to shared randomness, which can be used to extract identical bits to serve as key bits [30]. To correct errors when observing the randomness and protect against eavesdroppers, Alice and Bob can exchange messages across a public channel. The most notable models for secret-key agreement are the channel model (CM) and source model (SM) [31, Chap. 4], [32], each differing in the generation of the random observations. In the SM [33], both legitimate nodes and the eavesdropper have access to some source of common randomness modeled by a joint distribution. In the CM, the randomness originates from transmissions over a noisy wiretap channel [34]. In both models, the public channel is used to generate the secret key bits from the observed randomness at the legitimate nodes, leaving the eavesdropper with no information about it.

In this work, we consider a communication system with a secret-key budget. As described above, the legitimate nodes perform SKG and agree on secret key bits using any SKG scheme. They then append the newly generated bits to previously generated key bits. This way, a pool of available SK bits is built up at both legitimate communication parties. Whenever a secure transmission of a message with length n takes place, the oldest n SK bits are used as a one-time pad to encrypt the message. Since only the legitimate transmitter and receiver know the key bits, the transmission is information-theoretically secure. Due to the nature of one-time pads, the SK bits used for the transmission can only be used once and are therefore removed from the list of available key bits.

B. Ruin Theory

Ruin theory originated in economics and actuarial science, where it is used to analyze the solvency of an insurance company [13]. The basic idea is that an insurance company deals with two opposing cash flows simultaneously. On the one hand, they receive money in the form of premiums paid by customers. On the other hand, there occur claims that are paid by the insurance company.

In the traditional model, the premiums arrive at a constant (positive) rate, while the claims arrive randomly according to a Poisson process. The main quantity of interest is the probability that the insurance company will go bankrupt.

For this section, let $\tau = \inf\{t \geq 0 \mid X(t) \leq 0\}$ be the time of ruin, i.e., the first time t at which the aggregate surplus X falls to zero [35]. This defines the probability of ultimate

ruin ψ_∞ as the probability that bankruptcy will eventually occur,

$$\psi_\infty = \Pr(\tau < \infty).$$

Similarly, the probability of ruin in finite time $\psi_t = \Pr(\tau \le t)$ is given as the probability of ruin before time t.

Ruin theory has been extensively studied in the literature of mathematical finance and actuarial science, where many different problems have been discussed and explicitly solved, including expressions for finite-time ruin probability when considering specific claim distributions [36], [37] or when considering interest rates [38], [39]. For a more detailed overview of the topic, we refer the reader to [13], [35].

Due to the differences between financial systems and communication systems, we cannot simply apply all existing results from the literature. Instead, we will take some of the above ideas and definitions from the area of ruin theory as a basis and adapt them to the problem considered in this work. The system model and the exact problem formulation are discussed in the following section.

III. SYSTEM MODEL AND PROBLEM FORMULATION

Throughout this work, we consider a wiretap channel, where a transmitter (Alice) wants to securely transmit data to a legitimate receiver (Bob). The transmission is overheard by a passive eavesdropper (Eve). Both the channel between Alice and Bob and the channel between Alice and Eve are quasi-static fading channels with additive white Gaussian noise (AWGN) at the receivers and signal-to-noise ratios (SNRs) X and Y, respectively [31, Sec. 5.2]. The SNR values are assumed to be independent random variables, which also change independently over time. The achievable rates to Bob and Eve at time t are given as

$$R_{B,t} = \log_2(1 + X_t) \qquad (1)$$
$$R_{E,t} = \log_2(1 + Y_t), \qquad (2)$$

respectively, where X_t and Y_t denote the SNR values of the main channel and eavesdropper's channel at time t. According to the quasi-static model, we assume that the channels remain constant for the transmission of one codeword and the time index denotes this (discrete) time slot [31, Sec. 5.2].

To securely transmit messages to Bob, Alice uses key bits for encryption. These key bits are generated by the standard SKG procedures for wiretap channels [31, Chap. 4] and stored in a pool of available key bits. They are then used as a one-time pad to secure message bits, i.e., each SK bit can be used exactly once and is then removed from the budget of available key bits.

The SKG rate in time slot i for the considered model is given by [31, Sec. 5.1]

$$R_{SK,i} = \boldsymbol{\theta}_i = \log_2\left(\frac{1 + X_i + Y_i}{1 + Y_i}\right). \qquad (3)$$

This corresponds to the income of SK bits to the budget in time slot i. The number of key bits that are required to encrypt a transmission in time slot j is determined by the transmission

Figure 1. Exemplary illustration of the temporal progress of the number of available SK bits B_t. During the active state, both SKG and transmission are performed. Once the budget is exhausted, the system switches to a recharge state, where only new key bits are generated until a certain threshold b_0 is reached. The latency T is defined as the number of time slots between two active states. In the shown example, we have $T = 10$.

rate from Alice to Bob over the respective channel in time slot j

$$R_{B,j} = \boldsymbol{\xi}_j = \log_2\left(1 + \tilde{X}_j\right), \qquad (4)$$

where $\tilde{X}_j$ denotes the SNR during transmission. We assume that $\tilde{X}$ is distributed according to the same distribution as X, i.e., $\tilde{X} \stackrel{d}{=} X$; however, they are assumed to be independent. For simplicity, we assume that the transmit power is the same for both SKG and data transmission. However, this could further be optimized in future work.

Therefore, the total number of available SK bits at time t is given by the difference between the total number of generated key bits and the total number of used key bits up to that time slot. The total number of SK bits available at the end of time slot t is denoted as B_t. In addition to generating new key bits, we assume that the system starts with an initial budget $b_0 > 0$.

An outage is defined as the event that the SK budget is exhausted at the end of time slot t, i.e., $B_t \le 0$. Based on this, we define the *survival probability* $\bar{\psi}_t$ as the probability that the communication will last until time slot t, i.e., that $B_t > 0$ holds for all time slots $i \le t$,

$$\bar{\psi}_t(b_0) = \Pr\left(\min_{1 \le i \le t} B_i > 0\right). \qquad (5)$$

Similarly, we define the *outage probability* ψ_t as its complement

$$\psi_t(b_0) = 1 - \bar{\psi}_t(b_0). \qquad (6)$$

As long as there are still key bits available, i.e., $B_t > 0$, we say that the system is in the *active state*. Whenever the number of available SK bits drops to zero, the system enters a *recharge phase*, where no data is transmitted and only new SK bits are being generated until the initial amount b_0 is reached again. At this point, the system switches back to the active state, where both SKG and data transmission occur, as described above. An exemplary illustration of this system model can be found in Figure 1.

The duration between two active states, in which data transmission takes place, defines the latency $\boldsymbol{T}$ of the system. It is given as the first time slot within the recharge phase in which the budget reaches the specified threshold b_0, i.e.,

$$\boldsymbol{T}(b_0) = \inf \left\{ t \geq 0 \,\middle|\, \sum_{i=t_0}^{t} \boldsymbol{\theta}_i \geq b_0 \right\} - t_0 + 1, \qquad (7)$$

where t_0 denotes the first time slot of the recharge phase. Note that we can set $t_0 = 1$ without loss of generality if the distribution of $\boldsymbol{\theta}_i$ is stationary over time. Recall that during the recharge state only SKG takes place and the number of SK bits available in a specified time slot is given by the sum of the bits generated up to that time slot. Since the number of generated bits $\boldsymbol{\theta}_i$ in each time slot i is random, the latency $\boldsymbol{T}$ is also a random variable.

An overview of the most commonly used variable notation can be found in Table I.

The exact nature of the random process $\boldsymbol{B}_t$ depends on the communication scheme of the system. In this work, we will discuss two different schemes. First, we will consider a deterministic timing scheme in Section IV, where in each time slot both SKG and data transmission are performed. Second, we analyze a different model in Section V, where data transmissions occur randomly and SKG is performed when no data is to be transmitted.

A. Problem Formulation

Based on the introduction of the system model above, two immediate problems arise, which will be explicitly stated in the following.

Problem Statement 1. What is the outage probability $\psi_t(b_0)$ for given distributions of the channels and an initial budget b_0?

Problem Statement 2. What is the latency-reliability tradeoff for the described system? In particular, given an application requirement that the transmission needs to last at least τ time slots with an outage probability of at most ε, we can determine the minimum required initial budget $b_0^\tau(\varepsilon)$ by the solution of Problem 1. However, in order to generate this initial amount of SK bits, we need a certain number of time slots before any transmission can start, which defines the latency $\boldsymbol{T}$ of the system.

Both problems will be analyzed for the deterministic timing scheme and the random timing scheme in Section IV and Section V, respectively.

IV. DETERMINISTIC SCHEME

As a first scheduling scheme for the active state, we consider a deterministic scheme where SKG and transmission (TX) alternate. An illustration can be found in Figure 2. The channels are assumed to vary independently between each SKG and TX block. However, they remain constant for the entire duration of each single block. Throughout this section, we refer to the combination of one full cycle of an SKG block followed by a transmission block as one time slot, i.e., each time slot consists of one SKG block and one TX block, cf. Figure 2.

Figure 2. Illustration of the scheduling with a deterministic scheme during the active state. In each time slot, there is an SKG block followed by a TX block. While the channels are assumed to remain constant for each individual phase, they change independently between the SKG and TX blocks.

For this scheme, in each time slot i, the amount $\boldsymbol{\theta}_i$ corresponding to the SKG rate is added to the budget of available SK bits, while $\boldsymbol{\xi}_i$ bits are removed from it during the TX block. Thus, the total number of SK bits available at the end of time slot t is given as

$$\boldsymbol{B}_t = b_0 + \sum_{i=1}^{t} \boldsymbol{\theta}_i - \sum_{i=1}^{t} \boldsymbol{\xi}_i \qquad (8)$$

$$= b_0 - \sum_{i=1}^{t} \boldsymbol{Z}_i \qquad (9)$$

$$= b_0 - \boldsymbol{S}_t \qquad (10)$$

where $\boldsymbol{Z}_i = \boldsymbol{\xi}_i - \boldsymbol{\theta}_i$ describes the net usage of SK bits in time slot i and

$$\boldsymbol{S}_t = \sum_{i=1}^{t} \boldsymbol{Z}_i \qquad (11)$$

gives the accumulated net usage until time t.

A. Reliability Analysis

First, we start with a reliability analysis for the scheme described above. The first important observation is that the system loses SK bits in each time slot on average, which is formalized in the following Lemma 1.

Lemma 1 (Average Net Usage – Deterministic Scheme). *Consider the described communication system in the active state with the deterministic timing scheme. The expected value of the net usage $\boldsymbol{Z}_i = \boldsymbol{\xi}_i - \boldsymbol{\theta}_i$ is positive, i.e., $\mathbb{E}\left[\boldsymbol{Z}_i\right] > 0$. Thus, the system's SK budget reduces on average in every time slot.*

Proof. The proof can be found in Appendix A. $\square$

An important consequence that follows from Lemma 1 is stated in the following.

Corollary 1 (Probability of Ultimate Ruin – Deterministic Scheme). *The secret-key budget of the system in the active state using the deterministic timing scheme will almost surely be exhausted in finite time.*

Proof. Since $\boldsymbol{Z}_i$ has a positive expected value, cf. Lemma 1, the sum $\boldsymbol{S}_t$ forms a random walk with (positive) drift. From [40, Chap. XII.2, Thm. 1 and 2], it follows that $\boldsymbol{S}_t$ drifts to

Table I
DEFINITIONS OF THE MOST COMMONLY USED VARIABLES

X_t	SNR of the main channel (Alice to Bob) during the SKG phase in time slot t
$\tilde{X}_t$	SNR of the main channel during data transmission in time slot t
Y_t	SNR of the eavesdropper channel (Alice to Eve) during the SKG phase in time slot t
B_t	Amount of available SK bits in time slot t
θ_t	SKG rate in time slot t
ξ_t	Number of used SK bits for transmission in time slot t
Z_t	Net usage of SK bits in time slot t
$S_t = \sum_{i=1}^{t} Z_i$	Accumulated net usage of SK bits up to time slot t
b_0	Amount of initially available SK bits
$\psi_t(b_0)$	Outage probability until time t with initial budget b_0
$\bar{\psi}_t(b_0) = 1 - \psi_t(b_0)$	Survival probability until time t with initial budget b_0
$b_0^{\tau}(\varepsilon)$	Required initial budget to survive at least τ time slots with an outage probability of at most ε
T	Latency between two active system states

$+\infty$ with probability one. Thus, $B_t = b_0 - S_t$ will become negative with probability one. $\qquad\square$

Having established that the secure communication cannot last indefinitely, it is of interest to quantify the outage probability at any given time slot t. This outage probability is defined according to (6). The complementary probability is the survival probability $\bar{\psi}_t$ from (5), i.e., the probability that the system will remain in the active state until time slot t. The survival probability $\bar{\psi}_t$ can be described by the following recursive relation [41], [42]:

$$\bar{\psi}_{t+1}(b) = \int_{-\infty}^{b} \bar{\psi}_t(b - s)\mathrm{d}F_Z(s)\,, \qquad (12)$$

where F_Z describes the common distribution function of the independent and identically distributed (i.i.d.) net claims Z_i. The intuition behind this equation is that, in order to survive until time slot $t + 1$, the system needs to first survive until time t. Additionally, the net usage Z_{t+1} of the next time slot needs to be small enough to leave a positive budget remaining.

Remark. The recursive relation (12) can also be derived from the standard time-discrete ruin theoretic model without the income process [35].

Example. To illustrate (12), we solve the first steps explicitly. For the initial state of the system at time $t = 0$, the budget B_0 is equal to the initial budget b_0. The initial survival probability $\bar{\psi}_0(b_0)$ is therefore a step function, where the step from zero to one occurs at b_0. Thus, for the next time step, we obtain from (12) that

$$\bar{\psi}_1(b_0) = \int_{-\infty}^{b_0} \mathrm{d}F_Z(s) = F_Z(b_0)\,,$$

i.e., the probability of surviving the first time slot is equal to the probability that the net claim Z_1 is less than the initial available budget b_0. This relation can now be applied recursively to calculate the survival probabilities $\bar{\psi}_t$ for all time slots t.

However, the recursive equation in (12) can be difficult to solve for general distributions of the net usage F_Z. We are therefore interested in finding an efficient way to compute it numerically. It is clear that (12) is an integrodifference equation,

which can be solved numerically by several different methods. For a detailed treatise, we refer the interested reader to [43]. Throughout the following, we use the fast Fourier transform (FFT) method to calculate $\bar{\psi}_t(b_0)$ according to [43, Chap. 8]. Our implementation is made publicly available in [19].

Even though (12) can be efficiently solved numerically, it still requires a recursive calculation up to the desired time step t. Therefore, we provide an easy-to-calculate upper bound on the outage probability ψ_t in the following theorem. While this is only a (loose) worst-case bound, it can be easily computed without recursion for any given time slot t.

Theorem 1 (Worst-Case Bounds of the Ruin Probability – Deterministic Scheme). *Consider the described communication system employing the deterministic timing scheme. The outage probability $\psi_t(b_0)$ can be upper bounded by*

$$\psi_t(b_0) \leq \Psi_t(b_0) < \hat{\Psi}_t(b_0) \qquad (13)$$

with

$$\Psi_t(b_0) = \frac{\mathbb{E}\left[\max\left(S_t, 0\right)\right]}{b_0} \qquad (14)$$

and

$$\hat{\Psi}_t(b_0) = \frac{\sqrt{\mathrm{var}(S_t) + \mathbb{E}\left[S_t\right]^2}}{b_0}\,. \qquad (15)$$

Proof. The proof can be found in Appendix B. $\qquad\square$

Remark 1. Since we assume that all channel realizations are mutually independent, we can simplify (15) to

$$\hat{\Psi}_t(b_0) = \frac{\sqrt{\sum_{i=1}^{t} \mathrm{var}(Z_i) + \left(\sum_{i=1}^{t} \mathbb{E}\left[Z_i\right]\right)^2}}{b_0}\,. \qquad (16)$$

If we on top of that assume that the distribution of the channel gains does not vary over time, i.e., $Z_1 \overset{d}{=} Z_2 \overset{d}{=} \cdots \overset{d}{=} Z_i$ for all i, we can further simplify the expression to

$$\hat{\Psi}_t(b_0) = \frac{\sqrt{t\,\mathrm{var}(Z_1) + t^2\mathbb{E}\left[Z_1\right]^2}}{b_0}\,. \qquad (17)$$

Example 1 (Rayleigh Fading). We now illustrate the reliability analysis with a numerical example. For this purpose, we assume that both Bob and Eve experience Rayleigh fading,

Figure 3. Outage probability ψ_t for different initial budgets b_0 over time for a system using the deterministic scheme. The channels to both Bob and Eve are Rayleigh fading with average SNRs $\mathbb{E}\left[X_i\right] = 20\,\mathrm{dB}$ and $\mathbb{E}\left[Y_i\right] = 10\,\mathrm{dB}$, respectively. The solid lines correspond to the numerically calculated outage probabilities according to (12) while the markers indicate results from MC simulations with 10^6 samples (Example 1).

i.e., the channel gains X_i and Y_i are distributed according to an exponential distribution. The channel realizations are i.i.d. over time and independent in space. The average SNR of Bob's channel is set to $20\,\mathrm{dB}$ while Eve's average SNR is $10\,\mathrm{dB}$. With these parameters, the average net usage of SK bits per time slot is about $\mathbb{E}\left[Z_i\right] = 2.58\,\mathrm{bit}$. In Figure 3, the outage probability $\psi_t(b_0)$ is shown over time for different initial SK budgets b_0. The solid lines indicate the numerically calculated values from (12), while the markers are obtained from Monte Carlo (MC) simulations with 10^6 samples. All of the calculations and simulations can be reproduced using the source code provided in [19].

As expected from Corollary 1, all of the outage probabilities approach 1 over time. However, increasing the initially available number of SK bits b_0 decreases the outage probability, i.e., the system stays longer in the active state for a given outage probability. The upper bounds from Theorem 1 are not shown in Figure 3 because they are loose for this particular example. For $b_0 = 50$ at time $t = 15$, the bound is about $\hat{\Psi}_{15}(50) = 0.80$, while both (12) and MC simulations yield the actual outage probability of about $\psi_{15}(50) = 0.11$.

Remark 2. Throughout this work, we use the above Rayleigh fading example to numerically illustrate the theoretical results and show how they can be applied. However, it should be noted that these general results can be applied to a variety of scenarios, even including those with an active jammer. In this case, the distributions of the channel gains X_i and Y_i, and thus the resulting distributions of θ_i and ξ_i need to be adjusted accordingly. The source code for all the presented results and calculations is made freely available at [19] and can be adapted to custom numerical examples, e.g., for other types of fading like Rician fading.

B. Latency Analysis

Having analyzed the reliability of the communication system in the active state, we next investigate the latency between two active states. Recall from Section III that we assume that the system enters a recharge phase once the SK bit budget is exhausted, cf. Figure 1. In this phase, only SKG is performed until a minimum number of available key bits is reached. The number of time slots this process takes is defined to be the latency T of the system.

The minimum initial budget that needs to be reached depends on the requirements of the application. In the following, we assume that there is a constraint on the outage probability for a given time slot, i.e., the system must remain in the active state for τ time slots with an outage probability of at most ε. Equivalently, this means that the system should survive at least τ time slots with a probability of at least $1 - \varepsilon$. Thus, the minimum initial budget to achieve this is

$$b_0^\tau(\varepsilon) = \inf\left\{b \geq 0 \mid 1 - \varepsilon \leq \bar{\psi}_\tau(b)\right\},$$

which corresponds to the inverse of $\bar{\psi}_\tau$, i.e.,

$$b_0^\tau(\varepsilon) = \bar{\psi}_\tau^{-1}(1 - \varepsilon) = \psi_\tau^{-1}(\varepsilon). \qquad (18)$$

The operational meaning behind this is that we have to generate at least $b_0^\tau(\varepsilon)$ SK bits, before we can start transmitting. Once the SK bit budget is exhausted, this process needs to be repeated. Therefore, this quantity determines the latency before the communication system can securely transmit messages again.

Since the SKG rates in each time slot vary randomly, the latency T is also a random variable. The following theorem characterizes the average latency for a system with i.i.d. channel realizations.

Theorem 2 (Average Latency). *Consider the described communication system with a tolerated outage probability ε for a specified survival duration τ. The SKG rates θ_i are i.i.d. with positive and finite expectation $\mathbb{E}\left[\theta_1\right]$. The average latency between two active system states is given by*

$$\mathbb{E}\left[T\right] = \frac{b_0^\tau(\varepsilon)}{\mathbb{E}\left[\theta_1\right]}. \qquad (19)$$

Proof. The proof can be found in Appendix C. □

Remark 3. The (average) latency in (19) is defined in terms of independent channel realizations of the main channel. According to the timing model in Figure 2, two independent channel realizations form one time slot. Thus, the latency in terms of time slots is half of that in (19).

Remark 4. Up to the last step of the proof of Theorem 2, we do not require b_0 to be constant. Therefore, the result only needs to be slightly modified in the case where b_0 is a random variable. In this case, we get $\mathbb{E}\left[T\right] = \mathbb{E}\left[\mathbb{E}\left[T \mid b_0\right]\right] = \mathbb{E}\left[b_0\right]/\mathbb{E}\left[\theta_1\right]$.

Example 2 (Reliability-Latency Tradeoff). We illustrate the result of the latency analysis with the following numerical example. Similar to Example 1, we assume i.i.d. Rayleigh fading with average SNRs of $\mathbb{E}\left[X_i\right] = 20\,\mathrm{dB}$ and $\mathbb{E}\left[Y_i\right] = 10\,\mathrm{dB}$ for Bob's and Eve's channel gains, respectively. For this scenario, the minimum required initial budget $b_0^\tau(\varepsilon)$ is

Figure 4. Required initial budget b_0^τ over the outage probability ε for a system in the recharge state. The channels to both Bob and Eve are Rayleigh fading with average SNRs $\mathbb{E}[\boldsymbol{X}_i] = 20\,\text{dB}$ and $\mathbb{E}[\boldsymbol{Y}_i] = 10\,\text{dB}$, respectively. The solid lines correspond to the numerically calculated outage probabilities according to (18) while the markers indicate results from MC simulations with 10^6 samples (Example 2).

depicted in Figure 4 over the outage probability constraint ε for multiple time constraints τ. The solid lines again show the numerically calculated values by the recursive relation in (12), while the markers indicate the results of MC simulations with 10^6 samples.

The first clear observation is that the required initial budget drops to zero as the tolerated outage probability approaches one. Similarly, it increases with a stricter reliability constraint. Interestingly, for the chosen example of Rayleigh fading, the required $b_0^\tau(\varepsilon)$ increases only slowly when decreasing ε at a fixed τ. For $\tau = 5$, an initial budget of around $b_0^5(10^{-1}) = 19.9\,\text{bit}$ is required to survive with an outage probability less than 10^{-1}. For a stricter requirement of 10^{-5}, this increases to around $b_0^5(10^{-5}) = 33.3\,\text{bit}$, i.e., for a $10\,000$-times increase in reliability, the initial budget only needs to be increased by a factor of around 1.67.

In contrast, when increasing the duration τ that the system should remain in the active state, the increase in $b_0^\tau(\varepsilon)$ is more significant. In order to survive $\tau = 10$ time slots with an outage probability of at most $\varepsilon = 10^{-1}$, the required initial budget is around $b_0^{10}(10^{-1}) = 35.8\,\text{bit}$, which is an 1.8-times increase compared to $\tau = 5$ with the same outage probability constraint.

According to Theorem 2, the average latency $\mathbb{E}[\boldsymbol{T}]$ is a simple linear scaling of the required initial budget $b_0^\tau(\varepsilon)$. For this numerical example, we have an average SKG rate around $\mathbb{E}[\boldsymbol{\theta}_1] = 3.31\,\text{bit}$. Thus, we have an average latency of around $\mathbb{E}[\boldsymbol{T}] = 6$ time slots for $\tau = 5$ and $\varepsilon = 10^{-1}$. Similarly, this increases to around 10 time slots for $\varepsilon = 10^{-5}$.

V. RANDOM TRANSMISSION TIMES

After having introduced and analyzed a deterministic timing scheme in the previous section, we now consider a different scheme in which messages arrive randomly.

Figure 5. Illustration of the scheduling model with random TX blocks during the active system state. In each time slot t, there is a probability of p_t that a message is transmitted. If no message is transmitted, SKG is performed instead.

A. Random Transmission – Model Description

In each time slot t, there is a probability p_t that a message needs to be securely transmitted. An example where this timing model is applicable is a communication scenario between a sensor and a fusion center where the sensor only transmits data when an external event occurs, e.g., when the temperature rises above a threshold. Assuming that these external events occur randomly, the times at which data is transmitted are also random. By adjusting the threshold at which the sensor transmits data, the system designer could influence the transmission probability p_t.

When a message needs to be transmitted, available SK bits are used to encrypt the data. Similar to the scheme in Section IV, this removes $\boldsymbol{\xi}_t$ bits from the budget of available key bits. However, if no transmission occurs, the time slot is used for SKG, which adds $\boldsymbol{\theta}_t$ bits to the budget. An illustration can be found in Figure 5. Overall, the number of available SK bits $\boldsymbol{B}_t$ at time t is again given by

$$\boldsymbol{B}_t = b_0 - \sum_{i=1}^{t} \boldsymbol{Z}_i = b_0 - \boldsymbol{S}_t, \qquad (20)$$

where $\boldsymbol{Z}_i$ again denotes the net usage of key bits in time slot i. While this looks identical to the budget expression for the deterministic scheme in (10), the distribution of the net usage $\boldsymbol{Z}_i$ is different. In contrast to the deterministic scheme, we now express $\boldsymbol{Z}_i$ as

$$\boldsymbol{Z}_i = \boldsymbol{P}_i \boldsymbol{\xi}_i - (1 - \boldsymbol{P}_i)\boldsymbol{\theta}_i, \qquad (21)$$

where $\boldsymbol{P}_i \sim \mathcal{B}(p_i)$ is an independent Bernoulli-distributed random variable indicating whether time slot i is used to transmit a message or perform SKG. The distribution of $\boldsymbol{Z}_i$ then follows as

$$
\begin{aligned}
F_{\boldsymbol{Z}_i}(z) &= \Pr\left(\boldsymbol{P}_i \boldsymbol{\xi}_i - (1 - \boldsymbol{P}_i)\boldsymbol{\theta}_i \le z\right) \\
&= (1 - p_i)\Pr\left(-\boldsymbol{\theta}_i \le z\right) + p_i \Pr\left(\boldsymbol{\xi}_i \le z\right) \\
&= (1 - p_i)\bar{F}_{\boldsymbol{\theta}_i}(-z) + p_i F_{\boldsymbol{\xi}_i}(z), \qquad (22)
\end{aligned}
$$

where $\bar{F}_{\boldsymbol{\theta}_i} = 1 - F_{\boldsymbol{\theta}_i}$ denotes the survival function of $\boldsymbol{\theta}_i$. As before, we will assume throughout the following, that all involved random variables are mutually independent and identically distributed over time.

Remark 5. For the expression of $\boldsymbol{Z}_i$ in (21) recall that $\boldsymbol{\theta}_i$ denotes the (non-negative) SKG rate. Since the generated key bits are added to the budget, the income $\boldsymbol{\theta}_i$ is a negative usage.

Remark 6. The distribution of $\boldsymbol{Z}_i$ in (22) has the form of a mixture distribution where $\boldsymbol{P}_i$ is a mixture of $\boldsymbol{\xi}_i$ and $-\boldsymbol{\theta}_i$.

B. Reliability Analysis

Even though the distribution of $\boldsymbol{Z}_i$ is different from that in Section IV, the progress of the budget B_t over time is still given by a random walk, cf. (20). Thus, we can reuse the results on the outage probability ψ_t from Section IV-A by adjusting the distribution of $\boldsymbol{Z}_i$. However, there exists a major qualitative difference when switching to the random time scheme.

In the deterministic scheme, the average net usage of SK bits is greater than zero, i.e., $\mathbb{E}\left[\boldsymbol{Z}_i\right] > 0$, cf. Lemma 1. Therefore, on average, the system loses SK bits, which results in an eventual outage, cf. Corollary 1. In contrast, in the random scheme, it is possible for $\mathbb{E}\left[\boldsymbol{Z}_i\right]$ to be negative, as shown in the following.

Corollary 2 (Average Net Usage – Random Scheme). *Consider the described communication system in the active state where a message is transmitted with probability p_t in time slot t. The following relation between the expected value of the net usage $\boldsymbol{Z}_i$ and the transmission probability p_i holds*

$$\mathbb{E}\left[\boldsymbol{Z}_i\right] \gtreqless 0 \quad \Leftrightarrow \quad p_i \gtreqless \frac{\mathbb{E}\left[\boldsymbol{\theta}_i\right]}{\mathbb{E}\left[\boldsymbol{\theta}_i\right] + \mathbb{E}\left[\boldsymbol{\xi}_i\right]}. \quad (23)$$

Proof. The expected value of the net usage in time slot i is given as

$$\begin{aligned}\mathbb{E}\left[\boldsymbol{Z}_i\right] &= \mathbb{E}\left[\boldsymbol{P}_i\boldsymbol{\xi}_i\right] - \mathbb{E}\left[(1-\boldsymbol{P}_i)\boldsymbol{\theta}_i\right]\\ &= \mathbb{E}\left[\boldsymbol{P}_i\right]\mathbb{E}\left[\boldsymbol{\xi}_i\right] - \mathbb{E}\left[1-\boldsymbol{P}_i\right]\mathbb{E}\left[\boldsymbol{\theta}_i\right]\\ &= p_i\mathbb{E}\left[\boldsymbol{\xi}_i\right] - (1-p_i)\mathbb{E}\left[\boldsymbol{\theta}_i\right],\end{aligned}$$

where we use the assumption that $\boldsymbol{P}_i$ is independent from both $\boldsymbol{\theta}_i$ and $\boldsymbol{\xi}_i$. This yields the relation

$$\mathbb{E}\left[\boldsymbol{Z}_i\right] \gtreqless 0 \quad \Leftrightarrow \quad p_i \gtreqless \frac{\mathbb{E}\left[\boldsymbol{\theta}_i\right]}{\mathbb{E}\left[\boldsymbol{\theta}_i\right] + \mathbb{E}\left[\boldsymbol{\xi}_i\right]},$$

which concludes the proof. $\qquad\square$

The important consequence of Corollary 2 is that, depending on p_i, the average net usage of SK bits may be negative, i.e., on average more bits are generated than used in each time slot. In contrast to the result in Corollary 1 for the deterministic scheme, this implies that there is a non-zero chance for the system to remain in the active state indefinitely.

Based on the calculation of the outage probability ψ_t within a finite time horizon t in (12), we can calculate the probability of ultimate ruin $\psi = \lim_{t\to\infty} \psi_t$ according to the integral equation

$$\psi(b) = (1 - F_{\boldsymbol{Z}}(b)) + \int_0^\infty \psi(s) f_{\boldsymbol{Z}}(b-s)\mathrm{d}s \quad (24)$$

where we assume i.i.d. $\boldsymbol{Z}_i$ with density $f_{\boldsymbol{Z}}$. This is a Fredholm integral equation of the second kind, which can be solved numerically, e.g., by applying Nyström's method [44, Chap. 19.1].

For the numerical examples presented in the following, this technique is used to approximate the exact solution.

While the relation from (24) allows an exact calculation of the outage probability ψ in theory, a solution may be difficult to obtain in practice. Therefore, we provide a worst-case bound in the following theorem, which may be easier to compute in practice.

Theorem 3 (Upper Bound of Probability of Ultimate Ruin – Random Scheme). *Consider the described communication scheme in the active state with i.i.d. SKG rates $\boldsymbol{\theta}_i$ and i.i.d. rates to Bob $\boldsymbol{\xi}_i$. In time slot i, a message is transmitted with probability p_i. This probability is the same for all time slots i and fulfills*

$$p_1 = \cdots = p_i = p < \frac{\mathbb{E}\left[\boldsymbol{\theta}_1\right]}{\mathbb{E}\left[\boldsymbol{\theta}_1\right] + \mathbb{E}\left[\boldsymbol{\xi}_1\right]}. \quad (25)$$

In this case, the probability of eventually leaving the active state ψ is upper bounded by

$$\psi(b_0) \leq \exp(-r^\star b_0) \quad (26)$$

with $r^\star$ being the positive solution to

$$\mathbb{E}\left[\exp\left(r^\star \boldsymbol{Z}_1\right)\right] = 1, \quad (27)$$

assuming it exists.

Proof. The proof can be found in Appendix D. $\qquad\square$

The upper bound from (26) shows that there is a non-zero probability of staying in the active system state indefinitely if the expected net usage of SK bits $\mathbb{E}\left[\boldsymbol{Z}_i\right]$ is negative, i.e., more bits are generated than used on average.

Remark 7. The above results have direct implications for practical system design. If the system designer can influence the transmission probability p, its value should be set below the critical value $\mathbb{E}\left[\boldsymbol{\theta}_1\right]/(\mathbb{E}\left[\boldsymbol{\theta}_1\right] + \mathbb{E}\left[\boldsymbol{\xi}_1\right])$. Similar to Section IV, we can then calculate the minimum required initial budget $b_0^\infty(\varepsilon)$ for a tolerated outage probability ε. Thus, with probability ε there will be only the initial latency to generate $b_0^\infty(\varepsilon)$ key bits and no subsequent recharging phases.

Example 3 (Rayleigh Fading – Random Scheme). For this numerical example, we assume the same system parameters as in the previous Example 1 and Example 2, i.e., i.i.d. Rayleigh fading with $\mathbb{E}\left[\boldsymbol{X}_i\right] = 20\,\mathrm{dB}$ and $\mathbb{E}\left[\boldsymbol{Y}_i\right] = 10\,\mathrm{dB}$. This gives us the expected values of the SKG rates $\boldsymbol{\theta}_i$ and Bob's rates $\boldsymbol{\xi}_i$ as $\mathbb{E}\left[\boldsymbol{\theta}_i\right] = 3.31\,\mathrm{bit}$ and $\mathbb{E}\left[\boldsymbol{\xi}_i\right] = 5.889\,\mathrm{bit}$, respectively. From (23) in Corollary 2, the critical transmission probability is calculated to be $3.31/9.199 = 0.360$, i.e., for transmission probabilities $p < 0.360$ the average net usage of SK bits is negative. According to Theorem 3, this implies that the outage probability for such a scenario approaches a value less than 1 over time.

The numerical results are presented in Figure 6. First, we show the outage probability ψ_t in finite time for two values of the transmission probability $p < 0.36$ with an initial budget of $b_0 = 20\,\mathrm{bit}$ in Figure 6a. The probabilities of ultimate ruin ψ, which are indicated by the dashed lines, are numerically evaluated according to (24). Additionally, the upper bound

(a) Comparison of outage probability in finite time ψ_t with the probability of ultimate ruin ψ for an initial budget $b_0 = 20$ bit.

(b) Probability of ultimate ruin ψ over the initial budget b_0. The MC results correspond to the values after $t = 150$ time steps.

Figure 6. Probability of ultimate ruin ψ for a system with transmission probability p. The channels to both Bob and Eve are Rayleigh fading with average SNRs $\mathbb{E}[\boldsymbol{X}_i] = 20\,\mathrm{dB}$ and $\mathbb{E}[\boldsymbol{Y}_i] = 10\,\mathrm{dB}$, respectively. The dashed lines correspond to the numerically calculated outage probabilities ψ according to (24) while the markers indicate results from MC simulations with 10^6 samples. The dash-dotted lines represent the upper bound from (26). (Example 3)

from (26) in Theorem 3 is given by the dash-dotted lines. It can be seen that the outage probability ψ_t approaches the limit ψ for large t. In the case of $p = 0.1$, this limit is around $\psi = 1.45 \cdot 10^{-3}$ and the upper bound is around $3.53 \cdot 10^{-3}$. As expected, these values increase with an increasing transmission probability p, since more blocks are used for transmission which uses up more of the available SK bits. For $p = 0.35$, the probability of eventually exhausting the key-bit budget is $\psi = 0.64$, i.e., there is a 36% chance that the system will remain in the active state indefinitely.

Next, we show the behavior of the probability of ultimate ruin ψ over the initially available number of SK bits b_0 in Figure 6b. As expected, this probability decreases with an increasing initial budget and the slope is steeper for smaller transmission probabilities p.

VI. CONCLUSION

In this work, we have considered a wireless communication system with a passive eavesdropper. Alice and Bob perform SKG to generate key bits, which are added to a pool of available key bits. When transmitting a message, bits from this pool are used as a one-time pad to secure the data transmission. In this setting, we have analyzed the reliability in terms of the probability that the budget of available key bits will be exhausted. We have shown how to compute this outage probability numerically and, additionally, derive worst-case bounds. Interestingly, for randomly arriving messages, there is a positive probability that the communication system will remain active indefinitely and never run out of SK bits. In this case, there is only an initial latency to reach the initial budget of key bits before a transmission can take place.

For the cases where the system eventually runs out of available key bits, we have additionally investigated the latency between two active states, i.e., the duration during which Alice and Bob only generate new keys without performing any data transmission. It is shown that the expected latency can be computed by a simple expression that is linear in the number of SK bits that need to be initially available.

System designers can utilize the findings of this work to adjust parameters, meeting specific performance requirements, e.g., the outage probability after a specified time.

Since calculating the exact outage probability requires solving an integrodifference equation recursively, it will be interesting for future work to find approximations or tight bounds that are less computationally expensive. In addition, the assumption that the channel distributions are stationary could be removed in future work. In this way, a scenario with time-varying channel distributions could also be modeled and analyzed.

APPENDIX A
PROOF OF LEMMA 1

Based on the definitions of $\boldsymbol{Z}_i$, $\boldsymbol{\xi}_i$, and $\boldsymbol{\theta}_i$, we find that

$$
\begin{aligned}
\mathbb{E}[\boldsymbol{Z}_i] &= \mathbb{E}[\boldsymbol{\xi}_i - \boldsymbol{\theta}_i] \\
&= \mathbb{E}[\log_2(1+\boldsymbol{Y}_i)] + \mathbb{E}\left[\log_2\left(1+\tilde{\boldsymbol{X}}_i\right)\right] \\
&\qquad - \mathbb{E}[\log_2(1+\boldsymbol{X}_i+\boldsymbol{Y}_i)] \\
&= \mathbb{E}\left[\log_2\left((1+\boldsymbol{Y}_i)(1+\tilde{\boldsymbol{X}}_i)\right)\right] \\
&\qquad - \mathbb{E}[\log_2(1+\boldsymbol{X}_i+\boldsymbol{Y}_i)] \\
&= \mathbb{E}\left[\log_2\left(1+\tilde{\boldsymbol{X}}_i+\boldsymbol{Y}_i+\tilde{\boldsymbol{X}}_i\boldsymbol{Y}_i\right)\right] \\
&\qquad - \mathbb{E}[\log_2(1+\boldsymbol{X}_i+\boldsymbol{Y}_i)] \\
&= \mathbb{E}[\log_2(1+\boldsymbol{X}_i+\boldsymbol{Y}_i+\boldsymbol{X}_i\boldsymbol{Y}_i)] \\
&\qquad - \mathbb{E}[\log_2(1+\boldsymbol{X}_i+\boldsymbol{Y}_i)] \\
&> 0\,,
\end{aligned}
$$

where we require $\tilde{\boldsymbol{X}}_i \overset{d}{=} \boldsymbol{X}_i$ and $\boldsymbol{X}_i, \boldsymbol{Y}_i > 0$.

APPENDIX B
PROOF OF THEOREM 1

For the first inequality $\psi_t \leq \Psi_t$, we use Doob's martingale inequality [45, Chap. 12.6, Thm. 1]. In order to be able to

apply it, we first formulate ψ_t in terms of the probability of the maximum of $\boldsymbol{S}_i$ as follows. We start with the survival probability $\bar{\psi}_t$, which describes the probability that the SK budget $\boldsymbol{B}_t$ never falls to zero up to time t, i.e.,

$$\bar{\psi}_t(b_0) = \Pr\left(\min_{1\leq i\leq t} \boldsymbol{B}_t > 0\right).$$

This can be rewritten using the definition of $\boldsymbol{B}_t$ from (10) as

$$\bar{\psi}_t(b_0) = \Pr\left(\max_{1\leq i\leq t} \boldsymbol{S}_i < b_0\right),$$

which in turn can be expressed in terms of the outage probability ψ_t as

$$\psi_t(b_0) = \Pr\left(\max_{1\leq i\leq t} \boldsymbol{S}_i \geq b_0\right).$$

Next, we need to show that the random process $\boldsymbol{S}_t = \sum_{i=1}^t \boldsymbol{Z}_i$ forms a submartingale (together with the natural filtration), i.e., we need to show that

$$\mathbb{E}\left[\boldsymbol{S}_{t+1} \mid \boldsymbol{S}_t, \ldots, \boldsymbol{S}_1\right] \geq \boldsymbol{S}_t$$

holds. This result can be obtained as follows:

$$
\begin{aligned}
\mathbb{E}\Big[\boldsymbol{S}_{t+1} \,\Big|\, \boldsymbol{S}_t, \ldots, \boldsymbol{S}_1\Big] \\
&= \mathbb{E}\left[\boldsymbol{Z}_1 + \cdots + \boldsymbol{Z}_t + \boldsymbol{Z}_{t+1} \mid \boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_t\right] \\
&= \boldsymbol{Z}_1 + \cdots + \boldsymbol{Z}_t + \mathbb{E}\left[\boldsymbol{Z}_{t+1} \mid \boldsymbol{Z}_1, \ldots, \boldsymbol{Z}_t\right] \\
&\stackrel{(a)}{=} \boldsymbol{S}_t + \mathbb{E}\left[\boldsymbol{Z}_{t+1}\right] \\
&\stackrel{(b)}{\geq} \boldsymbol{S}_t,
\end{aligned}
$$

where (a) holds due to the assumption that all $\boldsymbol{Z}_i$ are independent from each other and (b) follows from Lemma 1. The inequality $\psi_t \leq \Psi_t$ now follows directly from Doob's martingale inequality.

For the second inequality, we use the following general observations. For a real-valued random variable $\boldsymbol{X}$ with the expected value $\mu = \mathbb{E}\left[\boldsymbol{X}\right]$ and variance $\mathrm{var}(\boldsymbol{X}) = \mathbb{E}\left[\boldsymbol{X}^2\right] - \mu^2$, it is apparent that

$$0 \leq \mathbb{E}\left[\max(\boldsymbol{X}, 0)\right] \leq \mathbb{E}\left[|\boldsymbol{X}|\right].$$

From Jensen's inequality, it follows that

$$\mathbb{E}\left[|\boldsymbol{X}|\right]^2 < \mathbb{E}\left[|\boldsymbol{X}|^2\right]$$

since x^2 is a strictly convex function. Combining the above with the fact that $\mathbb{E}\left[|\boldsymbol{X}|^2\right] = \mathbb{E}\left[\boldsymbol{X}^2\right]$ and $\mathbb{E}\left[\boldsymbol{X}^2\right] = \mathrm{var}(\boldsymbol{X}) + \mu^2$, we find that

$$
\begin{aligned}
\mathbb{E}\left[\max(\boldsymbol{X}, 0)\right]^2 &\leq \mathbb{E}\left[|\boldsymbol{X}|\right]^2 \\
&< \mathbb{E}\left[|\boldsymbol{X}|^2\right] \\
&= \mathbb{E}\left[\boldsymbol{X}^2\right] \\
&= \mathrm{var}(\boldsymbol{X}) + \mu^2,
\end{aligned}
$$

and in turn

$$\mathbb{E}\left[\max(\boldsymbol{X}, 0)\right] < \sqrt{\mathrm{var}(\boldsymbol{X}) + \mu^2}.$$

Now we can set $\boldsymbol{X} = \boldsymbol{S}_t$ to obtain the second inequality $\Psi_t < \hat{\Psi}_t$.

APPENDIX C
PROOF OF THEOREM 2

By definition of the latency $\boldsymbol{T}$ in (7), it can be seen that it is a hitting time of the random walk $\sum_{i=1}^t \boldsymbol{\theta}_i$. In [46, Thm. 4 and 8], lower and upper bounds on the expected value of such hitting times for random walks with drift are derived. In particular, it is shown that for a random walk $\{\boldsymbol{A}_t\}$, the following equality holds:

$$\mathbb{E}\left[\boldsymbol{T} \mid \boldsymbol{A}_0\right] = \frac{\boldsymbol{A}_0}{\delta},$$

with

$$\boldsymbol{T} = \inf\left\{t \geq 0 \mid \boldsymbol{A}_t \leq 0\right\},$$

if $\boldsymbol{A}_t - \mathbb{E}\left[\boldsymbol{A}_{t+1} \mid \boldsymbol{A}_0, \ldots, \boldsymbol{A}_t\right] = \delta$ holds.

In order to use this result, we use the correspondence $\boldsymbol{A}_t = b_0 - \sum_{i=1}^t \boldsymbol{\theta}_i$ with $\boldsymbol{A}_0 = b_0$. With this, we obtain

$$
\begin{aligned}
\mathbb{E}\Big[\boldsymbol{A}_{t+1} \,\Big|\, \boldsymbol{A}_0, \ldots, \boldsymbol{A}_t\Big] \\
&= \mathbb{E}\left[b_0 - \boldsymbol{\theta}_1 - \boldsymbol{\theta}_2 - \cdots - \boldsymbol{\theta}_t - \boldsymbol{\theta}_{t+1} \mid \boldsymbol{A}_0, \ldots, \boldsymbol{A}_t\right] \\
&= b_0 - \boldsymbol{\theta}_1 - \boldsymbol{\theta}_2 - \cdots - \boldsymbol{\theta}_t - \mathbb{E}\left[\boldsymbol{\theta}_{t+1}\right] \\
&= \boldsymbol{A}_t - \mathbb{E}\left[\boldsymbol{\theta}_{t+1}\right],
\end{aligned}
$$

where the steps closely follow the ones in the proof of Theorem 1. Based on the above relation, it is clear that

$$\boldsymbol{A}_t - \mathbb{E}\left[\boldsymbol{A}_{t+1} \mid \boldsymbol{A}_0, \ldots, \boldsymbol{A}_t\right] = \mathbb{E}\left[\boldsymbol{\theta}_{t+1}\right] = \delta.$$

Therefore, we have based on [46]

$$\mathbb{E}\left[\boldsymbol{T} \mid b_0\right] = \frac{b_0}{\mathbb{E}\left[\boldsymbol{\theta}_1\right]},$$

where $\mathbb{E}\left[\boldsymbol{\theta}_1\right] = \cdots = \mathbb{E}\left[\boldsymbol{\theta}_{t+1}\right]$ stems from the fact that we assume all $\boldsymbol{\theta}_i$ to be i.i.d.. Since b_0 is assumed to be a constant, it follows for the expectation of $\boldsymbol{T}$ that

$$\mathbb{E}\left[\boldsymbol{T}\right] = \mathbb{E}\left[\mathbb{E}\left[\boldsymbol{T} \mid b_0\right]\right] = \frac{b_0}{\mathbb{E}\left[\boldsymbol{\theta}_1\right]}.$$

Since we need to reach $b_0^\tau(\varepsilon)$ as an initial budget for the given system parameters, we obtain (19) as a final expression.

APPENDIX D
PROOF OF THEOREM 3

The proof closely follows the lines of the proof of Lundberg's inequality for the classical insurance risk model [47, Chap. 5].

First, recall that we aim to show

$$\psi(b_0) = \lim_{t\to\infty} \psi_t(b_0) \leq \exp\left(-r^\star b_0\right).$$

We start the proof by introducing the following functions:

$$g(r) = \log\left(\mathbb{E}\left[\exp\left(r\boldsymbol{Z}_1\right)\right]\right), \tag{28}$$
$$\boldsymbol{A}_t^r = \exp\left(r\boldsymbol{S}_t - tg(r)\right), \tag{29}$$

where $\boldsymbol{S}_t = \sum_{i=1}^{t} \boldsymbol{Z}_i$ is again the accumulated net usage. Next, we show that the stochastic process $\{\boldsymbol{A}_t^r\}_{t \geq 1}$ is a martingale,

$$
\begin{aligned}
\mathbb{E}&\left[\boldsymbol{A}_{t+1}^r \mid \boldsymbol{A}_t^r, \dots, \boldsymbol{A}_1^r\right] \\
&= \mathbb{E}\left[\exp\left(r\boldsymbol{S}_{t+1} - (t+1)g(r)\right) \mid \boldsymbol{A}_t^r, \dots, \boldsymbol{A}_1^r\right] \\
&= \mathbb{E}\left[\boldsymbol{A}_t^r \cdot \exp\left(r\boldsymbol{Z}_{t+1} - g(r)\right) \mid \boldsymbol{A}_t^r, \dots, \boldsymbol{A}_1^r\right] \\
&= \boldsymbol{A}_t^r \cdot \mathbb{E}\left[\exp\left(r\boldsymbol{Z}_{t+1} - g(r)\right) \mid \boldsymbol{A}_t^r, \dots, \boldsymbol{A}_1^r\right] \\
&\stackrel{(a)}{=} \boldsymbol{A}_t^r \cdot \mathbb{E}\left[\exp\left(r\boldsymbol{Z}_{t+1} - g(r)\right)\right] \\
&= \boldsymbol{A}_t^r \cdot \mathbb{E}\left[\exp\left(r\boldsymbol{Z}_{t+1} - \log\left(\mathbb{E}\left[\exp\left(r\boldsymbol{Z}_1\right)\right]\right)\right)\right] \\
&= \boldsymbol{A}_t^r \cdot \frac{\mathbb{E}\left[\exp\left(r\boldsymbol{Z}_{t+1}\right)\right]}{\mathbb{E}\left[\exp\left(r\boldsymbol{Z}_1\right)\right]} \\
&\stackrel{(b)}{=} \boldsymbol{A}_t^r,
\end{aligned}
$$

where we use the independence assumption in step (a) and the assumption of identical distributions in step (b). In order to take the outage condition into account, we define the following stopping time:

$$\tau_m = \inf\{t \mid \boldsymbol{S}_t \geq b_0\} \wedge m, \tag{30}$$

where $\wedge$ denotes the minimum operator. By the definition of $r^\star$ from (27), we have that

$$\mathbb{E}\left[\boldsymbol{A}_1^{r^\star}\right] = \mathbb{E}\left[\exp\left(r^\star \boldsymbol{Z}_1\right)\right] = 1.$$

It further follows

$$
\begin{aligned}
1 &= \mathbb{E}\left[\boldsymbol{A}_1^{r^\star}\right] \\
&\stackrel{(a)}{=} \mathbb{E}\left[\boldsymbol{A}_{\tau_m}^{r^\star}\right] \\
&\geq \mathbb{E}\left[\boldsymbol{A}_{\tau_m}^{r^\star} \mathbb{1}_{\tau_m < m}\right] \\
&\stackrel{(b)}{\geq} \mathbb{E}\left[\exp\left(r^\star b_0\right) \mathbb{1}_{\tau_m < m}\right] \\
&= \exp\left(r^\star b_0\right) \Pr\left(\inf\{t \mid \boldsymbol{S}_t \geq b_0\} < m\right) \\
&\stackrel{(c)}{=} \exp\left(r^\star b_0\right) \psi_m(b_0),
\end{aligned}
$$

where (a) is due to the optional stopping theorem [45, Chap. 12.5], (b) follows from the definition of the stopping time τ_m, and (c) uses the definition of the outage probability in finite time. Rearranging finally yields

$$\psi_m(b_0) \leq \exp\left(-r^\star b_0\right), \quad \text{for all} \quad m \in \mathbb{N}. \tag{31}$$

As a final step, we need to show that $r^\star$ is the positive solution to (27), assuming it exists. By Jensen's inequality, we have

$$g(r) = \log\left(\mathbb{E}\left[\exp\left(r\boldsymbol{Z}_1\right)\right]\right) \geq \mathbb{E}\left[r\boldsymbol{Z}_1\right],$$

and by the definition of $r^\star$, it follows that

$$g(r^\star) = 0 \geq r^\star \mathbb{E}\left[\boldsymbol{Z}_i\right],$$

which is a contradiction for $r^\star < 0$, since $\mathbb{E}\left[\boldsymbol{Z}_i\right] < 0$ by the assumption on p and Corollary 2.

REFERENCES

[1] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, May 2020. DOI: 10.1109/MNET.001.1900287. arXiv: 1902.10265 [cs.IT].

[2] V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and privacy for 6G: A survey on prospective technologies and challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 4, pp. 2384–2428, 2021. DOI: 10.1109/comst.2021.3108618. arXiv: 2108.11861 [cs.CR].

[3] P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1094–1122, 2021. DOI: 10.1109/ojcoms.2021.3078081.

[4] A. Chorti, A. N. Barreto, S. Köpsell, M. Zoli, M. Chafii, P. Sehier, G. Fettweis, and H. V. Poor, "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 102–108, Mar. 2022. DOI: 10.1109/mcomstd.0001.2000082.

[5] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proceedings of the National Academy of Sciences*, vol. 114, no. 1, pp. 19–26, Jan. 3, 2017. DOI: 10.1073/pnas.1618130114.

[6] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, no. 5, 497, May 2019. DOI: 10.3390/e21050497.

[7] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no. 4, pp. 6–12, Aug. 2011. DOI: 10.1109/mwc.2011.5999759.

[8] C. L. K. Ngassa, R. Molière, F. Delaveau, A. Sibille, and N. Shapira, "Secret key generation scheme from WiFi and LTE reference signals," *Analog Integrated Circuits and Signal Processing*, vol. 91, no. 2, pp. 277–292, Mar. 2017. DOI: 10.1007/s10470-017-0941-3.

[9] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Transactions on Communications*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018. DOI: 10.1109/tcomm.2018.2814607.

[10] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005. DOI: 10.1109/tap.2005.858853.

[11] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proceedings of the 2008 IEEE International Conference on Acoustics, Speech and Signal Processing*, IEEE, Mar. 2008. DOI: 10.1109/icassp.2008.4518284.

[12] S. Asmussen and H. Albrecher, *Ruin Probabilities* (Advanced Series on Statistical Science & Applied Probability 14), 2nd ed. World Scientific, Sep. 2010. DOI: 10.1142/7431.

[13] S. Asmussen and M. Steffensen, *Risk and Insurance* (Probability Theory and Stochastic Modelling 96). Springer International Publishing, 2020. DOI: 10.1007/978-3-030-35176-2.

[14] M. Egan, G. W. Peters, I. Nevat, M. Shirvanimoghaddam, and I. B. Collings, "A ruin theoretic design approach for wireless cellular network sharing with facilities," *Transactions on Emerging Telecommunications Technologies*, vol. 28, e3141, Jul. 2017. DOI: 10.1002/ett.3141. arXiv: 1409.4033 [cs.CY].

[15] A. Manzoor, N. H. Tran, W. Saad, S. M. A. Kazmi, S. R. Pandey, and C. S. Hong, "Ruin theory for dynamic spectrum allocation in LTE-U networks," *IEEE Communications Letters*, vol. 23, no. 2, pp. 366–369, Feb. 2019. DOI: 10.1109/LCOMM.2018.2890254. arXiv: 1812.04177 [cs.NI].

[16] Z. Htike and F. Kojima, "A ruin theory-inspired co-primary spectrum sharing mechanism for 5G," in *Proceedings of the 2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*, IEEE, May 2020. DOI: 10.1109/vtc2020-spring48590.2020.9128545.

[17] D. H. Kim, A. Manzoor, M. Alsenwi, Y. K. Tun, W. Saad, and C. S. Hong, "Ruin theory for user association and energy optimization in multi-access edge computing," *IEEE Transactions on Vehicular Technology*, Apr. 2023. DOI: 10.1109/TVT.2023.3269427. arXiv: 2107.00901 [cs.IT], Early Access.

[18] A. Manzoor, K. Kim, S. R. Pandey, S. M. A. Kazmi, N. H. Tran, W. Saad, and C. S. Hong, "Ruin theory for energy-efficient resource allocation in UAV-assisted cellular networks," *IEEE Transactions on Communications*, vol. 69, no. 6, pp. 3943–3956, Jun. 2021. DOI: 10.1109/TCOMM.2021.3064968. arXiv: 2006.00815 [cs.NI].

[19] K.-L. Besser. "Reliability and latency analysis for wireless communication systems with a secret-key budget, Supplementary material." (2023), [Online]. Available: https://github.com/klb2/secret-key-budget-ruin.

[20] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, Oct. 1949. DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[21] 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, Mar. 2021. DOI: 10.1109/jsait.2021.3062755.

[22] H. M. Furqan, J. M. Hamamreh, and H. Arslan, "Secret key generation using channel quantization with SVD for reciprocal MIMO channels," in *Proceedings of the 2016 International Symposium on Wireless Communication Systems (ISWCS)*, IEEE, Sep. 2016, pp. 597–602. DOI: 10.1109/iswcs.2016.7600974.

[23] M. Letafati, H. Behroozi, B. H. Khalaj, and E. A. Jorswieck, "Deep learning for hardware-impaired wireless secret key generation with man-in-the-middle attacks," in *Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM)*, IEEE, Dec. 2021. DOI: 10.1109/globecom46510.2021.9685537.

[24] H. Gao, Y. Huang, and D. Liu, "Beam-based secure physical layer key generation for mmWave massive MIMO system," in *Communications and Networking*, ser. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer International Publishing, 2021, pp. 37–51. DOI: 10.1007/978-3-030-67720-6_3.

[25] D. V. Linh and V. V. Yem, "Key generation technique based on channel characteristics for MIMO-OFDM wireless communication systems," *IEEE Access*, vol. 11, pp. 7309–7319, 2023. DOI: 10.1109/access.2023.3238573.

[26] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2692–2705, 2020. DOI: 10.1109/tifs.2020.2974621.

[27] F. Renna, M. R. Bloch, and N. Laurenti, "Semi-blind key-agreement over MIMO fading channels," *IEEE Transactions on Communications*, vol. 61, no. 2, pp. 620–627, Feb. 2013. DOI: 10.1109/tcomm.2012.102512.120084.

[28] M. Zorgui, Z. Rezki, B. Alomair, E. A. Jorswieck, and M.-S. Alouini, "On the ergodic secret-key agreement over spatially correlated multiple-antenna channels with public discussion," *IEEE Transactions on Signal Processing*, vol. 64, no. 2, pp. 495–510, Jan. 2016. DOI: 10.1109/TSP.2015.2483488.

[29] K.-L. Besser and E. A. Jorswieck, "Bounds on the ergodic secret-key capacity for dependent fading channels," in *Proceedings of the 24th International ITG Workshop on Smart Antennas (WSA 2020)*, VDE, Feb. 2020.

[30] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993. DOI: 10.1109/18.256484.

[31] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011. DOI: 10.1017/CBO9780511977985.

[32] L. Lai, Y. Liang, H. V. Poor, and W. Du, "Key generation from wireless channels," in *Physical Layer Security in Wireless Communications*, ser. Wireless Networks and Mobile Communications, X. Zhou, L. Song, and Y. Zhang, Eds., CRC Press, 2014, ch. 4, pp. 47–68. DOI: 10.1201/b15496.

[33] J. W. Wal and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010. DOI: 10.1109/tifs.2010.2052253.

[34] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography — Part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993. DOI: 10.1109/18.243431.

[35] D. C. M. Dickson, *Insurance Risk and Ruin*, 2nd ed. Cambridge University Press, 2016. DOI: 10.1017/9781316650776.

[36] W.-S. Chan and L. Zhang, "Direct derivation of finite-time ruin probabilities in the discrete risk model with exponential or geometric claims," *North American Actuarial Journal*, vol. 10, no. 4, pp. 269–279, Oct. 2006. DOI: 10.1080/10920277.2006.10597426.

[37] P. Picard and C. Lefèvre, "The probability of ruin in finite time with discrete claim size distribution," *Scandinavian Actuarial Journal*, vol. 1997, no. 1, pp. 58–69, Jan. 1997. DOI: 10.1080/03461238.1997.10413978.

[38] J. Cai, "Ruin probabilities with dependent rates of interest," *Journal of Applied Probability*, vol. 39, no. 2, pp. 312–323, Jun. 14, 2002. DOI: 10.1239/jap/1025131428.

[39] H.-x. Wang and A.-h. Wan, "Ruin probabilities with random rates of interest," *Journal of Shanghai University (English Edition)*, vol. 10, no. 3, pp. 211–214, Jun. 2006. DOI: 10.1007/s11741-006-0116-4.

[40] W. Feller, *An Introduction to Probability Theory and Its Applications* (Wiley Series in Probability and Statistics), 2nd ed. Wiley Inc., 1991, vol. 2.

[41] F. D. Vylder and M. J. Goovaerts, "Recursive calculation of finite-time ruin probabilities," *Insurance: Mathematics and Economics*, vol. 7, no. 1, pp. 1–7, Jan. 1988. DOI: 10.1016/0167-6687(88)90089-3.

[42] G. E. Willmot, "Ruin probabilities in the compound binomial model," *Insurance: Mathematics and Economics*, vol. 12, no. 2, pp. 133–142, Apr. 1993. DOI: 10.1016/0167-6687(93)90823-8.

[43] F. Lutscher, *Integrodifference Equations in Spatial Ecology* (Interdisciplinary Applied Mathematics 49). Springer International Publishing, 2019. DOI: 10.1007/978-3-030-29294-2.

[44] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes, The Art of Scientific Computing*, 3rd ed. Cambridge University Press, 2007.

[45] G. Grimmett and D. Stirzaker, *Probability and Random Processes*, 3rd ed. Oxford University Press, 2001.

[46] T. Kötzing and M. S. Krejca, "First-hitting times under drift," *Theoretical Computer Science*, vol. 796, pp. 51–69, Dec. 3, 2019. DOI: 10.1016/j.tcs.2019.08.021.

[47] H. Schmidli, *Risk Theory* (Springer Actuarial). Springer International Publishing, 2017. DOI: 10.1007/978-3-319-72005-0.