LuminaLink: Enabling Low Cost Secure Visible Light Communication with Birefringence

Ruxin Lin, Bingyan Liu, Yelin Cui, Duo Liu, Ruipeng Gao, Xiaoqiang Zhu, Jiqiang Liu, Lingkun Li*
Beijing Jiaotong University

***Abstract*—Visible Light Communication (VLC) offers a promising solution for wireless communication due to its large spectrum, interference resistance, and inherent security features. However, the broadcast nature of VLC signals poses significant security and privacy challenges, particularly in the context of the Internet of Things (IoT) where low-cost and resource-constrained devices are prevalent. In this paper, we introduce LuminaLink, a novel position-based VLC system designed to establish a secure communication link between a transmitter and a receiver located at a designated position. Leveraging the principle of birefringence, LuminaLink encodes messages using Color-Shift Keying (CSK), ensuring that only the receiver at the specified position can correctly decode the transmitted information.**

To achieve this, we design an innovative interference chip using transparent adhesive tape as a birefringence material, making LuminaLink both cost-effective and easy to deploy. Our system eliminates the need for expensive cryptographic algorithms by employing an initialization process that establishes encoding and decoding mappings, significantly reducing computational overhead. Extensive experimental results demonstrate that LuminaLink achieves an average bit-error-rate (BER) of 0.030 at the designated position, while maintaining an average BER of 0.524 at other positions, confirming its effectiveness in securing VLC communications.

I. Introduction

Visible Light Communication (VLC) has garnered significant interest in the academic community due to its distinct advantages, including a vast spectrum, resistance to interference, and inherent security features. However, similar to other wireless communication methods, VLC signals are typically broadcast over wireless channels, making them susceptible to eavesdropping. This raises significant concerns about the security and privacy of VLC systems.

In the modern Internet of Things (IoT) era, these concerns are amplified by the widespread deployment of low-cost and resource-constrained IoT devices. These devices often support only weak encryption or transmit data without any encryption [1], making their data packets susceptible to eavesdropping attacks [2]. Furthermore, even if a wireless network is encrypted, eavesdroppers can still gather privacy information by observing features of the wireless signal, such as inferring a device's location based on received signal strength [3], [4].

Several efforts have been made to enhance wireless security. For example, LiShield [5] and Kaleido [6] use flickering and rolling shutter effects to prevent unauthorized devices from capturing photos or recording videos. Patronus [7] leverages the nonlinear effects of microphones to prevent unauthorized recordings of speeches while allowing authorized devices to record. MicFrozen [8] scrambles unauthorized devices while preserving human speech to enhance acoustic transmission security. Recently, SpotSound [9] introduced a novel scheme that allows a receiver to decode a message correctly from ultrasonic signals only when positioned at a designated location.

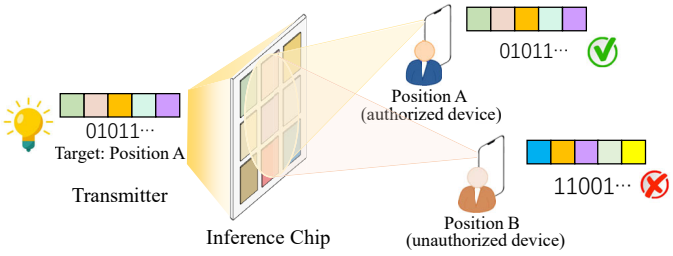


Fig. 1. Illustration of LuminaLink

However, a low-cost and resource-constrained end-to-end secure VLC system remains an unaddressed gap in the existing literature. Recent studies [10], [11] have shown that VLC signals can leak radio frequency (RF) signals, which can be exploited to intercept VLC signals even through walls, further compromising the security of VLC systems.

Our solution: In this paper, we present LuminaLink, a novel position-based VLC system designed to establish a secure link between a transmitter and a receiver at a specified position. To make LuminaLink practical, we extensively study the principle of birefringence and characterize the relationship between the output spectrum and incident spectrum as well as the receiver's position. Specifically, when a linearly polarized light beam passes through a birefringent material like quartz crystal, it splits into two refracted lights, known as ordinary and extraordinary rays. As these beams exit the material and pass through a polarizer, they produce distinct interference patterns at different positions, resulting in the receiver observing different colors based on its position. Additionally, changes in the incident beam's spectrum result in different colors being observed at the same position. As shown in Figure 1, this property enables the encoding of messages using Color-Shift Keying (CSK), which can then be transmitted securely through the LuminaLink system to a receiver at the designated position (position A) set by the transmitter. Notably, receivers at other positions (such as position B) cannot decode the message correctly, as they observe different colors than the designated receiver, ensuring the security and integrity of the transmitted

* Corresponding author, email: lkli@bjtu.edu.cn

information.

To decrease deployment costs, we built a novel interference chip utilizing transparent adhesive tape as the birefringent material. This chip is extremely cost-effective and can be easily attached to various light sources, such as multi-color LEDs or LCD displays. Additionally, the receiver can be any off-the-shelf device equipped with a camera or a photodiode, making it a highly accessible and low-cost solution.

To reduce computational overhead, we designed an initialization process utilizing our novel interference chip. After this initialization, encryption and decryption naturally occur through birefringence, eliminating the need for computationally expensive cryptographic algorithms. The initialization process establishes encoding and decoding mappings, allowing both the transmitter and receivers to use a simple lookup procedure for encoding and decoding. Consequently, the entire transmission and reception process operates at low computational costs. Additionally, this initialization can be performed at the factory and used consistently, further reducing deployment costs.

Since the encode and decode processes are fixed as a map, unauthorized devices at non-designated positions may attempt to map the observed outcome spectrum to the incident spectrum, and further map to the outcome spectrum at the designated position, ultimately decoding the message. To resolve this issue, LuminaLink conducts an in-depth study of the collision rules of birefringence and incorporates these rules into the coding table construction. Consequently, multiple incident spectra can generate the same outcome spectrum, making it challenging for receivers at non-designated positions to derive the incident spectrum from their observations. As a result, they are unable to derive the outcome spectrum at the designated position, thereby preventing illegal eavesdropping of messages.

To evaluate the performance of LuminaLink, we first implemented the system, including the interference chips, and then designed and implemented the software on both transmitter and receiver sides to achieve the encoding and decoding. We conducted extensive experiments under various settings, including different receiver positions, varying colors and intensities of ambient light, and on multiple mobile device models. The experimental results indicate that LuminaLink is capable of providing a secure and reliable VLC solution, demonstrating its effectiveness in real-world scenarios.

By utilizing LuminaLink, VLC devices can establish a secure communication link, ensuring that only the receiver at the designated position can correctly decode the message, while others cannot. LuminaLink achieves secure communication using low-cost birefringence materials on low-cost and resource-constrained devices, obviating the need for expensive cryptographic algorithms. Consequently, LuminaLink represents a significant advancement in the security of VLC systems.

Our contributions are summarized as follows:

- We introduce LuminaLink, a pioneering VLC system that leverages Color-Shift Keying (CSK) and the principles of birefringence to ensure messages are only decoded by receivers at specific designated positions, enhancing security against unauthorized access.
- LuminaLink offers a cost-effective, resource-efficient solution for secure VLC, with low deployment and computational costs, making it practical for widespread use in resource-constrained environments.
- We develop and implement LuminaLink, validating its effectiveness through extensive experiments. The experimental results indicate that LuminaLink achieves an average bit-error-rate (BER) of 0.030 at the designated position, while maintaining a BER of 0.524 at other positions, thereby demonstrating its ability to provide a secure VLC solution.

The remainder of the paper is organized as follows: Section II provides a summary of related works. Section III introduces the background of birefringence. Section IV presents the design of LuminaLink. Section V describes the implementation of LuminaLink. Section VI evaluates the performance of LuminaLink. Section VII concludes our work.

II. Related Works

Multiple VLC Schemes: The first category of existing VLC research efforts focuses on various VLC schemes, including On-Off Keying [12], Frequency-Shift Keying (FSK) [13], Color-Shift Keying (CSK) [14], and Gray-Scale Keying (GSK) [15]. These works aim to improve the throughput and bandwidth of VLC systems from different perspectives. Researchers have also explored extending the use cases of VLC systems. For example, PassiveVLC [16] enables VLC to work under the backscatter scheme. ChromaCode [17] embeds information into pixels and supports reliable screen-to-camera communication.

Applications Based on Various VLC Techniques: Many important techniques used in VLC have been deeply understood and utilized to build multiple interesting applications while researchers explore how to build reliable VLC systems [18]. For example, the rolling shutter effects of cameras equipped on mobile devices, which capture frames column by column, enable privacy protection, such as Kaleido [6] carefully modulating flickering, which, when captured by the rolling shutter camera, becomes mosaic and downgrades the quality of the screen, protecting the movie from being piracy recorded. Similarly, LiShield [5] carefully modulates flickering of multi-color LEDs, and after being captured by rolling shutter cameras, the photo is covered by color stripes, which downgrades the quality of the photo and protects the environment from being captured by hidden cameras.

Polarized Light: Polarized light is another popular phenomenon used to build interesting visible light systems. For example, POLI [19] combines the polarizer and disperser to support long-range VLC. Moreover, since humans cannot sense polarized light but devices can, CELLI [20] creates lines by polarized light beams scanning from left to right and from top to bottom, and uses a photo diode attached with a polarizer to position itself through the time-of-arrival (TOA)

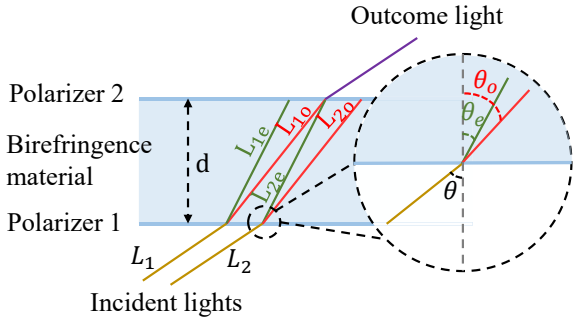


Fig. 2. Optical analysis of birefringence.

mechanism. Finally, LiCompass [21] uses polarized light to sense the direction of mobile devices.

Birefringence: Similar to LuminaLink, some systems utilize birefringence to build low-cost and reliable visible light systems. RainbowLight [22] uses birefringence to create positioning anchors, providing 3D localization. It enables 3D positioning using ambient light without any special designed electronic devices. LiTag [23] further utilizes birefringence to build a passive tag to measure the position and posture of objects attached with such a tag. ChromaLux [24] enables backscatter communication with ambient light using birefringence.

Despite these existing research efforts, enabling low-cost and secure VLC remains a significant gap in the VLC area. LuminaLink addresses this gap by providing a low-cost and reliable secure VLC solution, allowing only the receiver located at the designated position to correctly decode the message, while other receivers cannot, utilizing birefringence.

III. Preliminary

A. Birefringence Analysis

Birefringence is an optical phenomenon where an incident spectrum passing through a birefringent material between two polarizers results in a different outcome spectrum.

According to previous research [22], [23], as shown in Figure 2, every incident light beam is refracted into two light beams, namely ordinary rays (marked red) and extraordinary rays (marked green). Specifically, the incident light beams are denoted as L_1 and L_2. Since they originate from the same source, they have the same intensity I and are assumed to be parallel. L_{1o} and L_{1e} are the ordinary and extraordinary rays refracted by L_1, while L_{2o} and L_{2e} are the ordinary and extraordinary rays refracted by L_2. The ordinary rays share the same intensity I_o, and the extraordinary rays share the same intensity I_e, given that the intensities of the incident light beams are the same.

Assuming the incident angle is θ, the refractive angles of the ordinary rays and extraordinary rays are θ_o and θ_e, respectively. According to Snell's Law, we have:

$$n \sin\theta = n_e \sin\theta_e = n_o \sin\theta_o, \tag{1}$$

where n is the refractive index in the air (approximately 1), and n_e and n_o are the refractive indices of the extraordinary and ordinary rays, respectively. For a given material, n_o is usually fixed, but n_e varies with different incident angles. Typically, $n_o \neq n_e$, causing the two refracted light beams to not overlap.

Each birefringent material has an inherent direction called the optic axis. The polarized direction of the extraordinary ray aligns with the optic axis, while the polarized direction of the ordinary ray is perpendicular to the optic axis. According to Malus' Law, if the incident light is a linearly polarized single-frequency light, and the angle between its polarized direction and the optic axis is ϕ_1, then the intensities of the ordinary and extraordinary rays are given by:

$$\begin{aligned} I_o &= I \sin^2\phi_1 \\ I_e &= I \cos^2\phi_1, \end{aligned} \tag{2}$$

where I is the intensity of the incident light, and I_o and I_e are the intensities of the ordinary and extraordinary rays. Similarly, if the angle between the polarizer direction of polarizer 2 and the optic axis is ϕ_2, the intensities of the ordinary and extraordinary rays after passing through polarizer 2 are:

$$\begin{aligned} I'_o &= I_o \sin^2\phi_2 = I \sin^2\phi_1 \sin^2\phi_2 \\ I'_e &= I_e \cos^2\phi_2 = I \cos^2\phi_1 \cos^2\phi_2, \end{aligned} \tag{3}$$

where I'_o and I'_e are the intensities of the resulting ordinary and extraordinary rays.

As shown in Figure 2, when the refracted light beams exit the birefringent material and pass through polarizer 2, the outcome light is a mix of one ordinary ray and one extraordinary ray, meeting the coherent condition and exhibiting interference. Given a fixed thickness d of the birefringent material and a fixed incident angle, according to [22], the path difference can be calculated as:

$$\Delta = d(\tan\theta_o - \tan\theta_e)(\sin\theta)n + \frac{d}{\cos\theta_e} - \frac{d}{\cos\theta_o} n_o, \tag{4}$$

which, using Eq. (1) and (4), simplifies to:

$$\Delta = d(n_e \cos\theta_e - n_o \cos\theta_o). \tag{5}$$

The phase difference can then be calculated by:

$$\delta = \Delta \frac{2\pi}{\lambda} + \delta', \tag{6}$$

where δ' is 0 when the interference increases the outcome intensity and π when it decreases the outcome intensity.

Finally, the intensity of the outcome light after interference can be calculated using Eq. (3) and (6):

$$\begin{aligned} I_Q &= I'_o + I'_e + 2\sqrt{I'_o I'_e}\cos\delta \\ &= I\cos^2\phi_1\cos^2\phi_2 + I\sin^2\phi_1\sin^2\phi_2 \\ &\quad + 2I\cos\phi_1\cos\phi_2\sin\phi_1\sin\phi_2\cos\delta, \end{aligned} \tag{7}$$

where I_Q is the intensity of the outcome light after interference.

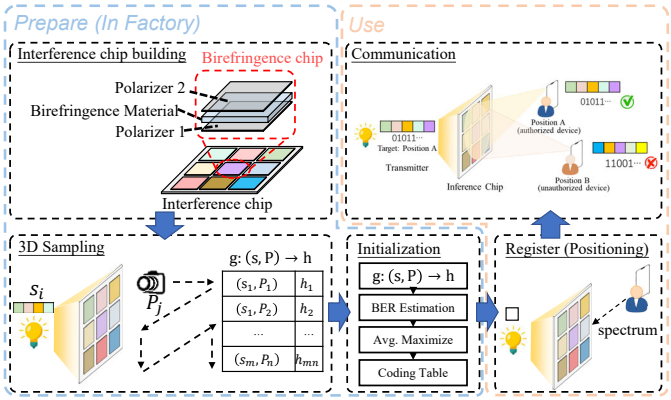


Fig. 3. LuminaLink overview

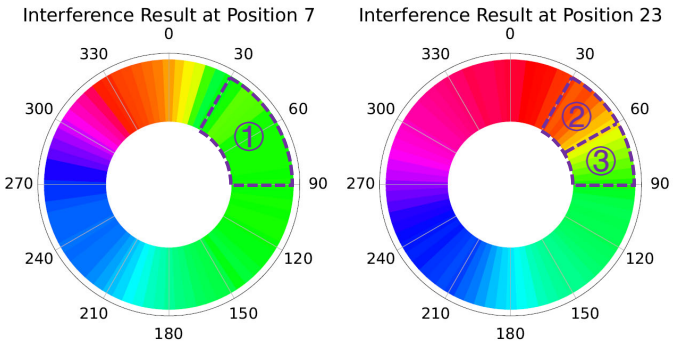


Fig. 4. Interference results of different incident spectrum with different hue values.

B. What can we learn from the analysis?

Incident light of multiple frequencies: First, when the incident light consists of multiple frequencies, we can examine the interference at each frequency component. Each component will experience different interference effects, resulting in unique intensities for each frequency. These individual intensities combine to produce an outcome spectrum that differs from the incident spectrum. Consequently, the color of the incident light will differ from the color of the outcome light.

Looking from different positions: When the receiver moves from one position to another, the incident angle θ changes accordingly if we trace the light beam from the receiver back to the source. Consequently, the refractive angles θ_e and θ_o also change, as described by Eq. (1), This variation in refractive angles alters the phase difference δ, according to Eq. (4) and (6). As a result, the receiver perceives different colors at different positions. This phenomenon can be used to determine the position of the authorized device, ensuring that receivers at non-designated positions observe a different spectrum from the one at the designated position, thereby ensuring security.

Change the incident spectrum: When the incident spectrum changes, the interference pattern changes as well. Each frequency component of the incident spectrum has a unique intensity, leading to different outcomes for each component. This results in a distinct outcome spectrum, altering the observed color of the light. This capability enables LuminaLink to encode messages using CSK.

Change the optic axis direction or thickness of the birefringence material: Altering the direction of the optic axis or the thickness of the birefringence material can also change the interference result, as the parameters ϕ_1, ϕ_2, and d are modified in Eq. (4) and (7). Although these parameters are fixed once the birefringence material and its orientation between polarizers are chosen, this adjustment allows for enhanced security. By fine-tuning these parameters in advance, we can ensure that multiple incident spectra result in the same outcome spectrum. This approach to improving security will be discussed in detail in Section IV.

IV. Design

A. Overview

The design overview is shown in Figure 3. Overall, LuminaLink comprises five stages:

1) **Interference Chip Building:** This stage involves constructing the interference chip, which is designed to display different spectra based on varying incident spectra and the receiver's positions.
2) **3D Sampling:** In this stage, the system builds a mapping between the incident spectrum, receiver's position, and the resulting outcome spectrum.
3) **Initialization:** This stage generates the encoding and decoding tables. These tables facilitate the encoding and decoding processes, enabling secure communication.
4) **Register:** When an authorized device wants to use LuminaLink, it registers with the system. This allows the transmitter to determine the device's position.
5) **Communication:** The transmitter sends the message to the receiver through the established secure link.

The first three stages are preparatory stages, which can be completed in the factory. Once completed, these stages do not need to be repeated, resulting in a low deployment cost.

This section presents these stages in detail.

B. Interference Chip Building

As discussed in Section III, the interference result is influenced by the thickness of the birefringence material, the angle between the polarizer direction and the optic axis, and the position of the receiver. Since the receiver's position cannot be determined during chip construction, we carefully adjust the other two parameters in this stage.

The goal of building the birefringence chip is to enhance security by increasing the likelihood of spectrum collision. Similar to prior works [22], [23], LuminaLink uses hue values to characterize the spectrum. By carefully adjusting the angle between the optic axis and the direction of the polarizers, as well as the thickness of the birefringence material, we perform 3D sampling to identify collision regions at each position.

For example, as shown in Figure 4, the outer labels represent the hue values of the incident light, and the colors displayed on the wheels indicate the interference results. At position 7, incident light with hue values from 20 to 90 results in the same outcome hue value, creating a collision region. In contrast, at position 23, the results show different hue values.

We can encode the incident hue between 30 and 60 (marked as (2)) to bit 1 and between 61 and 90 (marked as (3)) to bit 0 when the receiver is at position 23. This ensures that a receiver at position 7 observes the same spectrum (showing green, marked as (1)). Similarly, since position 23 has a collision region from 340 to 20, we can encode the incident hue between 340 and 0 to bit 1 and between 1 and 20 to bit 0 when the receiver is at position 7. In this scenario, a receiver at position 23 will observe the same spectrum (showing red).

This encoding scheme prevents the receiver at position 7 from illegally knowing messages sent to position 23 and prevents the receiver at position 23 from illegally knowing messages sent to position 7, since at non-designated positions, they observe no spectrum change, thereby enhancing the security of the communication system.

As shown in Figure 3, each interference chip is composed of multiple birefringence chips. Each birefringence chip has its own unique parameters and is carefully configured to ensure that its outcome spectra have at least one collision region at every position. This comprehensive setup results in an interference chip ready for the subsequent stages of the process.

C. 3D Sampling

After constructing the interference chip, it is attached to a light source and deployed. By varying the color emitted from the light source, we sample the outcome spectra at different positions in 3D space to create a mapping from the incident hue value and the receiver's position to the hue value of the outcome light. Specifically, for each incident hue value, we use a camera at various positions in the 3D space to capture the interference chip's effects and extract the hue value from each birefringence chip. This process results in the following mapping:

$$g : (s, P) \to h,$$

where s is the hue value of the incident light, P is the camera's position relative to the interference chip located at the origin, and h is the hue value of the outcome light.

Sampling every point in the 3D space would require extensive effort, so we employ a method to reduce the sampling workload by focusing on a few 2D planes. When the camera at position $A = (x, y, z)$ observes a hue value h from a birefringence chip located at position $B = (x', y', z')$, the camera will capture the same hue value h at every position along the ray $\overrightarrow{BA} = (x - x', y - y', z - z')$, because the light propagates through a straight line in the air. Thus, by sampling a selected few 2D planes, we can infer the mapping g for the entire 3D space from these results.

D. Initialization

The initialization stage utilizes the mapping g from the previous stage to construct the decoding table $c_P : h \to b$, where h is the hue value of the outcome light, $b \in \{0, 1\}$, and P is the position of the receiver. The receiver at position P uses this table to map the observed spectrum to either bit 0 or 1 for decoding the message.

Given the mapping g which correlates the incident hue s and the receiver's position P to the outcome hue value h, we can determine the outcome hue values at each position for any incident hue s. For a particular decoding table c_P for an authorized device at position P, we can compute the expected BER for an unauthorized receiver at position P' as follows:

$$E(c_P, P, P') = \frac{1}{|S|} \sum_{s \in S} |c_P(g(s, P)) - c_P(g(s, P'))|, \quad (8)$$

where S is the set of candidate incident hue values. We aim to build the decoding table c_P such that the average BER for all unauthorized positions is as close to 0.5 as possible, indicating the highest BER:

$$\hat{c_P} = \arg\min_{c_P} \frac{1}{|Q|} \sum_{P' \in Q} |E(c_P, P, P') - 0.5|, \quad (9)$$

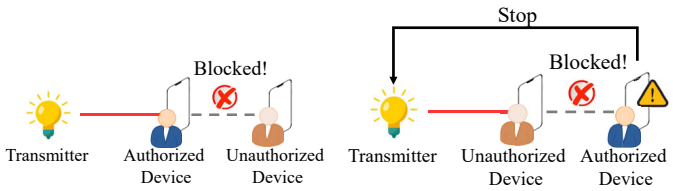
where $\hat{c_P}$ is the selected decoding table, and Q is the set of positions of unauthorized devices. We use a brute-force approach to determine the optimal decoding table, a process that can be performed in the factory and does not need to be repeated by the end user, thus keeping deployment costs low. Once the decoding table for each receiver's position is established, we can construct the encoding table by identifying the original image of the mapping g. Since multiple incident hue values can map to a particular outcome hue value, LuminaLink selects the incident hue value that resides within the most collision regions. This approach maximizes security, as it increases the difficulty for unauthorized receivers to decode the message, as discussed earlier.

E. Register

After the initialization stage, devices can use the encoding and decoding tables to communicate. However, to enable secure communication, the transmitter must know the position of the authorized device.

In the registration stage, LuminaLink lets the transmitter emit a white spectrum. The authorized receiver captures the interference chip and extracts the hue values from each birefringence chip, then sends this information to the transmitter. According to prior research [22], [23], different positions result in unique hue vectors observed by the receiver. The transmitter can then derive the relative position of the authorized device based on these hue vectors.

Once the transmitter knows the position of the authorized receiver, it will send back the decoding table of the authorized device according to its position relative to the transmitter. Finally, they can communicate securely through the established secure link.



(a) Behind the Authorized Device (b) In Front of the Authorized Device

Fig. 5. Scenarios of intercepting the transmitter.

The communication that involves the authorized device sending its hue values for positioning to the transmitter, as well as the transmitter sending back the decoding table, can occur over an insecure channel, since the decoding table is useful only when the receiver is at its corresponding position. The register stage also needs an authentication mechanism to ensure the device registered is the authorized one; however, this is beyond the scope of this paper.

F. Communication

After the registration stage, the transmitter uses the encoding table to encode the message and send it to the receiver. The receiver then uses the decoding table to decode the message. As discussed earlier, only the receiver at the designated position can correctly decode the message, ensuring secure communication.

G. Security Discussion

Enhancing the security of LuminaLink is crucial. The threat model of LuminaLink considers two primary threats:

The first one is unauthorized devices might attempt to use their observations to deduce the incident spectrum and, subsequently, the spectrum at the designated position. This threat is mitigated by the collision regions in the birefringence chip, as discussed previously. The collision regions make it difficult for unauthorized devices to accurately map their observations to the correct incident spectrum and, thus, the intended message.

Another threat is unauthorized devices may try to position themselves in such a way that they observe the same spectrum as the authorized device. Since light propagates in a straight line in the air, an unauthorized device could potentially see the same spectrum if it is located on the direct path from the birefringence chip to the authorized device.

LuminaLink addresses this issue in two ways. First, as shown in Figure 5(a), if the unauthorized device is positioned on the ray behind the authorized device, the light beam will be blocked by the authorized device due to the straight propagation of light. In this case, the unauthorized device cannot capture the birefringence chip, thus cannot derive the incident spectrum.

Conversely, as shown in Figure 5(b), if the unauthorized device is positioned between the birefringence chip and the authorized device, it could observe the same spectrum as the authorized device. However, this places the unauthorized device within the field of view (FOV) of the authorized device. The authorized device can detect the presence of an unauthorized observer and respond by stopping the transmission.

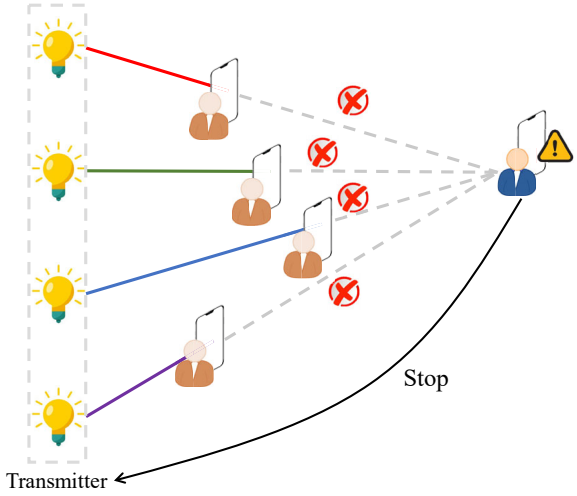


Fig. 6. The eavesdropper uses multiple devices to intercept the message.

Second, to increase the difficulty for unauthorized devices to observe the same spectrum, LuminaLink leverages multiple birefringence chips on the interference chip. Specifically, as shown in Figure 3, an interference chip consists of multiple birefringence chips. LuminaLink places a light source behind each birefringence chip to control the incident spectrum for each birefringence chip individually. This approach enables LuminaLink to transmit multiple data bits simultaneously.

With multiple birefringence chips, the eavesdropper must intercept all the birefringence chips by placing multiple devices along each ray between each birefringence chip and the authorized device to derive the entire message, as shown in Figure 6. Introducing more interceptors increases difficulty to the eavesdropper to deploy the devices, and makes it easier for the authorized receiver to detect unauthorized devices and take appropriate actions. Therefore, increasing the number of birefringence chips not only boosts data rates but also heightens the difficulty of intercepting the message while making it easier to detect unauthorized observers.

V. Implementation

We implement the prototype of LuminaLink, including both the transmitter and the receiver.

Transmitter: As shown in Figure 7(a), the interference chip is constructed using a transparent board, a piece of polarizer, and transparent adhesive tape. The transparent board serves as the base to hold the birefringence chips. The transparent adhesive tape acts as the birefringence material. By attaching different layers of the tape, we can alter its thickness, and by changing its orientation, we can create multiple birefringence chips. Figure 7(b) shows the interference chip with four birefringence chips. In Figure 7(c), the interference chip is positioned in front of a light source to construct the transmitter. Here, we use an LCD monitor as the light source, as it can vary

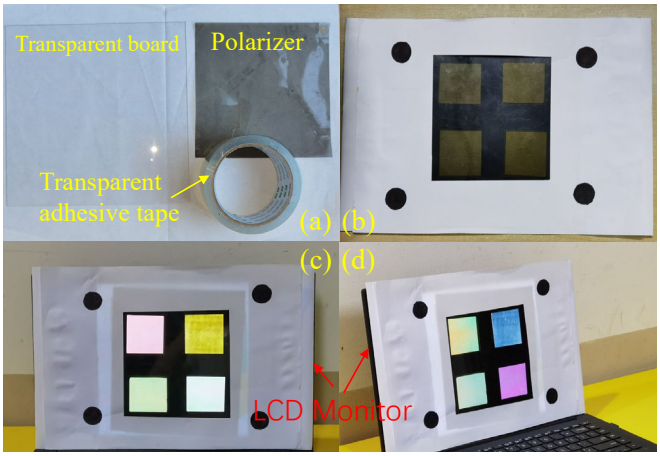


Fig. 7. Implementation of LuminaLink transmitter: (a) Materials to build the interference chip, (b) The interference chip, (c) The interference chip attached to a light source, (d) Observe the interference chip from a different position with the same incident light.

the hue value of the incident light beams for each birefringence chip. However, other light sources like RGB LEDs can also be used, keeping the system low-cost. Comparing Figures 7(c) and (d), we observe that when the incident hue value remains constant, the interference chip produces different hue values at different positions. In addition, we develop a program to modulate the message into incident hue values and display it through the LCD monitor.

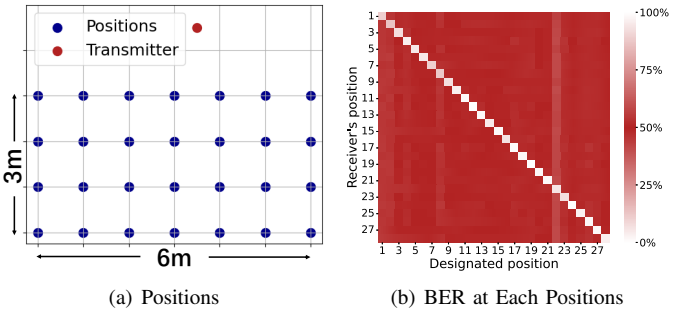
Receiver: We use a commercial off-the-shelf (COTS) smartphone as the receiver because of its convenience. However, other low-cost implementations are still feasible, such as using a CMOS camera or photodiodes with an Arduino MCU. We developed an application to capture the transmission. The app automatically detects black dots, as shown in Figure 7, to identify the interference chip within the photo. Then, the app finds each birefringence chip based on their relative positions to the black dots, extracts their hue values, and decodes the message.

VI. Evaluation

We conduct extensive experiments to evaluate the performance of LuminaLink and answer the following questions:

- **Q1 (§VI-A):** Can LuminaLink provide reliable communication to a device at the designated position while preventing devices at other positions from correctly decoding the message?
- **Q2 (§VI-B):** Is LuminaLink feasible under various practical factors, such as different ambient light intensities, color temperatures, and receiver mobile models?
- **Q3 (§VI-C):** Is LuminaLink robust when the user scenario changes?

The performance is measured by the bit-error-rate (BER), which is the ratio of incorrectly decoded bits to the total number of transmitted bits. A BER close to 0.5 indicates poor performance, as it suggests the message is being decoded randomly. Conversely, a BER near 0 or 1 is desirable, indicating reliable and accurate decoding.



(a) Positions (b) BER at Each Positions

Fig. 8. (a) Illustration of positions, (b) BER at each positions.

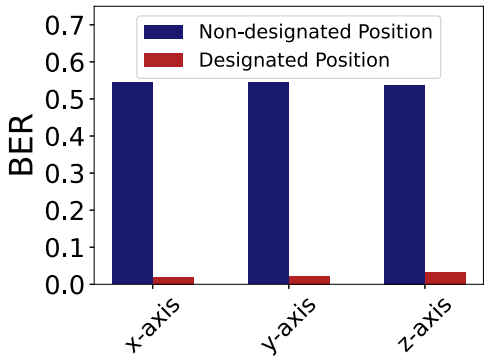


Fig. 9. BERs of devices along three axes individually.

Experiments are conducted in an area of $3m \times 6m$. We selected 28 positions within this area, evenly distributed, as depicted in Figure 8(a) (top view). The transmitter is fixed at the red dot outside the area. We placed one receiver at each position marked by blue dots. In each experiment, we selected one position as the designated position, making the device at this position the authorized device, while devices at other positions are the unauthorized devices. After the authorized device registers itself, the transmitter broadcasts the decoding table to every device, simulating the process of unauthorized devices successfully eavesdropping on the decoding table. Then, both authorized and unauthorized devices use the decoding table to decode the message. We expect that the message could be correctly decoded by the authorized device, while unauthorized devices would have a BER close to 0.5.

A. General Performance

To evaluate whether LuminaLink can provide reliable and secure communication to a device placed at the designated position while preventing unauthorized devices from correctly decoding the message, we conducted the following experiment. We randomly generated a message of 1000 bytes and transmitted it from the transmitter. Each position was designated as the authorized position in turn, and the BER was calculated at every position.

As shown in Figure 8(b), LuminaLink achieves the average BER of 0.030 at the designated positions, indicating accurate

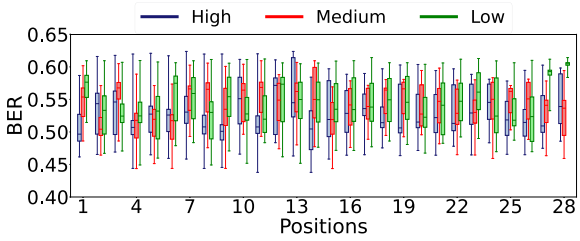


Fig. 10. BERs at every positions with different ambient light intensities.

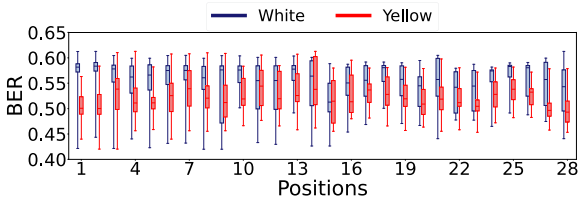


Fig. 11. BERs at every positions with different ambient light color temperatures.

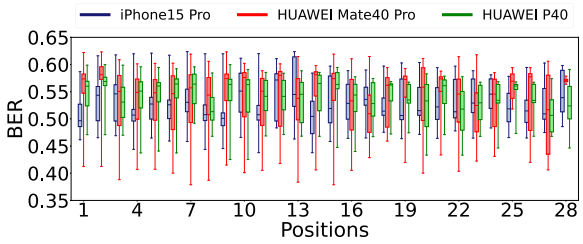


Fig. 12. BERs at every position with different receiver mobile models.

decoding. At other, non-designated positions, LuminaLink achieves BERs close to 0.5, with an average BER of around 0.524 (ranging from 0.432 to 0.622). This suggests that the decoding at non-designated positions is essentially random.

We conducted further experiments to determine which axis of positions had the most impact on BERs. In each experiment, we selected a position and placed devices along three axes: two axes sharing coordinates with the chosen position, and one axis differing. We then calculated the BERs by repeated experiment. In each turn, the device at the chosen position was designated as authorized, while the remaining devices were unauthorized.

As shown in Figure 9, the average BERs at designated positions are all below 0.03, while average BERs at non-designated positions are all around 0.5. This indicates that LuminaLink performs consistently across different axes.

These results demonstrate that LuminaLink can reliably and securely transmit messages to a device at the designated position while preventing unauthorized devices from correctly decoding the message, thus establishing a secure link from the transmitter to the designated position.

B. Impact of Practical Factors

To verify if LuminaLink is feasible under various practical factors, we conduct several experiments in this subsection. Specifically, we change the experimental settings, such as different ambient light intensities, color temperatures, and various receiver mobile models. We then perform the initialization stage and communication stage under the same setting in each of them to measure the performance of LuminaLink. In the next subsection, we conduct experiments where the initialization stage is performed under one experimental setting while the communication stage is performed under another setting.

The process of each experiment in this subsection is the same as described in Section VI-A. We repeated the experiment 10 times in each setting, each time with a randomly generated message, then calculated BERs at designated and non-designated positions, respectively.

1) Ambient Light Intensity: To determine if LuminaLink is feasible under varying ambient light intensities, we conducted experiments in environments with different light intensities: high (2046 lx), medium (1195 lx), and low (344 lx). The BER at designated positions is 0.026, while the BER at non-designated positions are shown in Figure 10. These results show that the BERs are all between 0.4 to 0.65 at all non-designated positions, regardless of ambient light intensity. This indicates that LuminaLink is feasible under different ambient light intensities.

2) Color Temperatures of Ambient Light: To determine if LuminaLink is feasible under varying color temperatures of ambient light, we conducted experiments in environments with different ambient color temperatures: white (6000 K) and yellow (3000 K). The BER at designated positions is 0.033, while the BER at non-designated positions are shown in Figure 11. These results show that the BERs are all between 0.4 and 0.65 at all non-designated positions, regardless of ambient light color temperatures. This indicates that LuminaLink is feasible under different ambient light color temperatures.

3) Mobile Models: Different mobile models have varying cameras and software engines for photo processing, which may affect the BER of LuminaLink. To determine if LuminaLink remains robust across different mobile models, we conducted experiments using three different models: iPhone 15 Pro, HUAWEI Mate40 Pro, and HUAWEI P40. The average BER at designated positions is 0.030, while the BER at non-designated positions are shown in Figure 12. These results show that the BERs are almost between 0.4 and 0.65 at all non-designated positions, regardless of the receiver mobile model. This indicates that LuminaLink maintains robustness across different mobile models.

These experiments suggest that LuminaLink is feasible under various environment settings.

C. Cross Analysis

To explore if LuminaLink is robust when the user scenario changes, we conducted experiments and performed cross analysis. Specifically, each experiment process is the same as described in Section VI-A. However, we performed the initialization stage in one environmental setting, such as white

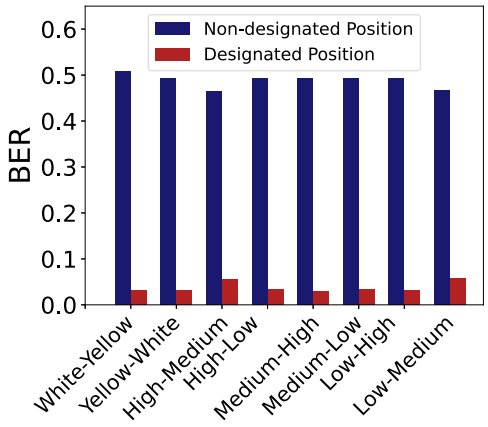


Fig. 13. Average BERs of cross analysis while changing ambient light.

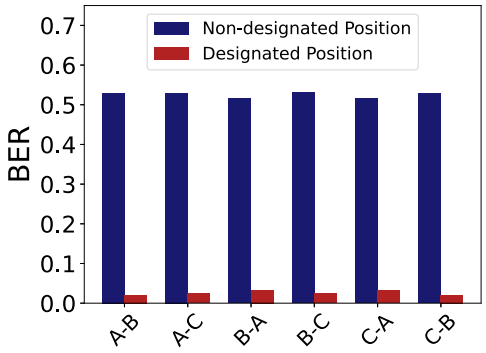


Fig. 14. Average BERs of cross analysis while changing mobile models (A: iPhone 15 Pro, B: HUAWEI Mate 40 Pro, C: HUAWEI P40).

color temperature, and the communication stage in another setting, such as yellow color temperature, and then calculated the average BER.

1) Ambient Light Changes: As shown in Figure 13, most average BERs at the designated positions are lower than 0.05, and all average BERs at non-designated positions are around 0.5, indicating that LuminaLink is robust even when the environment changes. This suggests that LuminaLink only needs one initialization at the factory under a certain ambient light condition and remains feasible under various ambient light conditions.

2) Mobile Model Changes: As shown in Figure 14, most average BERs at the designated positions are lower than 0.03, and all average BERs at non-designated positions are around 0.5, indicating that LuminaLink is robust to changes in mobile models. This suggests that LuminaLink only needs one initialization at the factory with a certain mobile model and remains feasible using various mobile models.

These experiments suggest that LuminaLink is robust to changes in user scenarios.

VII. Conclusion

In this paper, we introduced LuminaLink, a novel visible light communication system designed to provide secure and reliable data transmission. By leveraging birefringence chips, LuminaLink ensures that only devices at designated positions can accurately decode the transmitted messages, while unauthorized devices experience a high bit-error-rate (BER), close to 0.5, effectively preventing eavesdropping.

We detailed the design and implementation of LuminaLink, including the initialization, registration, and communication stages. The use of multiple birefringence chips not only enhances data rates but also increases the difficulty for unauthorized devices to intercept the message, making it easier to detect potential eavesdroppers.

Extensive experiments were conducted to evaluate LuminaLink's performance under various conditions, including different ambient light intensities, color temperatures, and mobile receiver models. The results demonstrated that LuminaLink provides robust and secure communication, with the authorized device consistently achieving a BER near 0, while unauthorized devices maintain a BER close to 0.5 across different scenarios.

Overall, LuminaLink offers a promising approach to secure visible light communication, with potential applications in areas requiring high-security data transmission. Future work will focus on enhancing the system's scalability, exploring additional security measures, and improving the ease of deployment in real-world environments.

Acknowledgement

This work is supported in part by Natural Science Foundation of China under grant No. 62402028, 62401037, 62472023, 62072029, the National Key R&D Program of China under grant No. 2023YFB2703702, Beijing Nova Program 20230484263 and 20240484607, the Talent Fund of Beijing Jiaotong University (No. 2022XKRC013), and DiDi Research Collaboration Plan.

References

[1] Xinyu Lei, Guan-Hua Tu, Chi-Yu Li, Tian Xie, and Mi Zhang. Secwir: Securing smart home iot communications via wi-fi routers with embedded intelligence. In *Proceedings of ACM MobiSys*, pages 260–272, 2020.

[2] Jingjing Ren, Daniel J Dubois, David Choffnes, Anna Maria Mandalari, Roman Kolcun, and Hamed Haddadi. Information exposure from consumer iot devices: A multidimensional, network-informed measurement approach. In *Proceedings of the Internet Measurement Conference*, pages 267–279, 2019.

[3] Yue Qiao, Ouyang Zhang, Wenjie Zhou, Kannan Srinivasan, and Anish Arora. Phycloak: Obfuscating sensing from communication signals. In *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, pages 685–699, 2016.

[4] Yanzi Zhu, Zhujun Xiao, Yuxin Chen, Zhijing Li, Max Liu, Ben Y Zhao, and Haitao Zheng. Et tu alexa? when commodity wifi devices turn into adversarial motion sensors. In *Proceedings of NDSS*, 2020.

[5] Shilin Zhu, Chi Zhang, and Xinyu Zhang. Automating visual privacy protection using a smart led. In *Proceedings of ACM MobiCom*, pages 329–342, 2017.

[6] Lan Zhang, Cheng Bo, Jiahui Hou, Xiang-Yang Li, Yu Wang, Kebin Liu, and Yunhao Liu. Kaleido: You can watch it but cannot record it. In *Proceedings of ACM MobiCom*, pages 372–385, 2015.

[7] Lingkun Li, Manni Liu, Yuguang Yao, Fan Dang, Zhichao Cao, and Yunhao Liu. Patronus: Preventing unauthorized speech recordings with support for selective unscrambling. In *Proceedings of ACM SenSys*, pages 245–257, 2020.

[8] Ming Gao, Yike Chen, Yajie Liu, Jie Xiong, Jinsong Han, and Kui Ren. Cancelling speech signals for speech privacy protection against microphone eavesdropping. In *Proceedings of ACM MobiCom*, 2023.

[9] Tingchao Fan, Huangwei Wu, Meng Jin, Tao Chen, Longfei Shangguan, Xinbing Wang, and Chenghu Zhou. Towards spatial selection transmission for low-end iot devices with spotsound. In *Proceedings of ACM MobiCom*, 2023.

[10] Muhammad Sarmad Mir, Minhao Cui, Borja Genoves Guzman, Qing Wang, Jie Xiong, and Domenico Giustiniano. Leakagescatter: Backscattering lifi-leaked rf signals. In *Proceedings of ACM MobiHoc*, pages 290–299, 2023.

[11] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. Sniffing visible light communication through walls. In *Proceedings of ACM MobiCom*, 2020.

[12] Christos Danakis, Mostafa Afgani, Gordon Povey, Ian Underwood, and Harald Haas. Using a cmos camera sensor for visible light communication. In *2012 IEEE Globecom Workshops*, pages 1244–1248. IEEE, 2012.

[13] Hui-Yu Lee, Hao-Min Lin, Yu-Lin Wei, Hsin-I Wu, Hsin-Mu Tsai, and Kate Ching-Ju Lin. Rollinglight: Enabling line-of-sight light-to-camera communications. In *Proceedings of ACM MobiSys*, pages 167–180, 2015.

[14] Pengfei Hu, Parth H Pathak, Xiaotao Feng, Hao Fu, and Prasant Mohapatra. Colorbars: Increasing data rate of led-to-camera communication using color shift keying. In *proceedings of ACM CoNEXT*, 2015.

[15] Yanbing Yang, Jiangtian Nie, and Jun Luo. Reflexcode: Coding with superposed reflection light for led-camera communication. In *Proceedings of ACM MobiCom*, pages 193–205, 2017.

[16] Xieyang Xu, Yang Shen, Junrui Yang, Chenren Xu, Guobin Shen, Guojun Chen, and Yunzhe Ni. Passivevlc: Enabling practical visible light backscatter communication for battery-free iot applications. In *Proceedings of ACM MobiCom*, pages 180–192, 2017.

[17] Kai Zhang, Chenshu Wu, Chaofan Yang, Yi Zhao, Kehong Huang, Chunyi Peng, Yunhao Liu, and Zheng Yang. Chromacode: A fully imperceptible screen-camera communication system. In *Proceedings of ACM MobiCom*, pages 575–590, 2018.

[18] Shakhrul Iman Siam, Hyunho Ahn, Li Liu, Samiul Alam, Hui Shen, Zhichao Cao, Ness Shroff, Bhaskar Krishnamachari, Mani Srivastava, and Mi Zhang. Artificial intelligence of things: A survey. *ACM Transactions on Sensor Networks*.

[19] Chun-Ling Chan, Hsin-Mu Tsai, and Kate Ching-Ju Lin. Poli: Long-range visible light communications using polarized light intensity modulation. In *Proceedings of ACM MobiSys*, pages 109–120, 2017.

[20] Yu-Lin Wei, Chang-Jung Huang, Hsin-Mu Tsai, and Kate Ching-Ju Lin. Celli: Indoor positioning using polarized sweeping light beams. In *Proceedings of ACM MobiSys*, pages 136–147, 2017.

[21] Yu-Lin Wei, Hsin-I Wu, Han-Chung Wang, Hsin-Mu Tsai, Kate Ching-Ju Lin, Rayana Boubezari, Hoa Le Minh, and Zabih Ghassemlooy. Licompass: Extracting orientation from polarized light. In *Proceedings of IEEE INFOCOM*. IEEE, 2017.

[22] Lingkun Li, Pengjin Xie, and Jiliang Wang. Rainbowlight: Towards low cost ambient light positioning with mobile phones. In *Proceedings of ACM MobiCom*, pages 445–457, 2018.

[23] Pengjin Xie, Lingkun Li, Jiliang Wang, and Yunhao Liu. Passive visible light tag system for localization and posture estimation. *IEEE Transactions on Mobile Computing*, 2024.

[24] Seyed Keyarash Ghiasi, Marco A Zúñiga Zamalloa, and Koen Langendoen. A principled design for passive light communication. In *Proceedings of ACM MobiCom*, pages 121–133, 2021.