sensors

MDPI

Article

Experimental Guesswork with Quantum Side Information Using Twisted Light

Vishal Katariya [1,*], Narayan Bhusal [2] and Chenglong You [2]

[1] Hearne Institute for Theoretical Physics, Department of Physics & Astronomy, and Center for Computation & Technology, Louisiana State University, Baton Rouge, LA 70803, USA
[2] Quantum Photonics Laboratory, Department of Physics & Astronomy, Louisiana State University, Baton Rouge, LA 70803, USA
* Correspondence: vkatariya8@gmail.com

Abstract: Guesswork is an information–theoretic quantity which can be seen as an alternate security criterion to entropy. Recent work has established the theoretical framework for guesswork in the presence of quantum side information, which we extend both theoretically and experimentally. We consider guesswork when the side information consists of the BB84 states and their higher-dimensional generalizations. With this side information, we compute the guesswork for two different scenarios for each dimension. We then performed a proof-of-principle experiment using Laguerre–Gauss modes to experimentally compute the guesswork for higher-dimensional generalizations of the BB84 states. We find that our experimental results agree closely with our theoretical predictions. This work shows that guesswork can be a viable security criterion in cryptographic tasks and is experimentally accessible in a number of optical setups.

Keywords: quantum information; quantum optics; quantum cryptography

1. Introduction

Guesswork is an information–theoretic measure of security and uncertainty of an information source [1,2], similar to entropy. In its simplest form, it can be understood as a game between two agents, Alice and Bob. Alice picks an element x from an alphabet $\mathcal{X}$ with prior probability $p_X(x)$. Bob's task then is to guess Alice's choice x while being allowed to ask questions in the form of "Is $X = x$?". The guesswork, $G(X)$, is the average number of guesses Bob needs until Alice answers with "yes". This is in contrast to entropy, where the same game is played, except that Bob is allowed to ask questions in the form of "Is $X \in \widetilde{X}$?", where $\widetilde{X}$ is a subset of the alphabet $\mathcal{X}$ [3].

Guesswork also has real-world applicability. Consider that one's account on an online portal is subjected to a brute-force hacking attack. A malicious agent is only allowed a certain number of guesses of the password before being locked out. The average number of guesses, i.e., the guesswork, would be the operational criterion of security in such a situation. Furthermore, guesswork takes on richer behavior when Bob possesses some quantum correlations with Alice, also known as side information. The theoretical framework for this problem has been laid out and studied recently [4–9]. For a general quantum ensemble, guesswork was shown to be computable by a semidefinite program [4,5]. Closed-form expressions for certain special cases of the guesswork exist, in particular, ensembles of qubit states [6–8], and the extension of guesswork to the study of classical-quantum channels has been recently initiated in Ref. [9]. However, experimental verification of the guesswork with quantum side information is yet an unexplored avenue.

Recently, spatially structured beams of light have been used extensively for multiple applications, such as 3D surface imaging, quantum cryptography, remote sensing, and correlated imaging [10–21]. Among them, the Laguerre–Gauss (LG) modes are particularly

check for updates

Citation: Katariya, V.; Bhusal, N.; You, C. Experimental Guesswork with Quantum Side Information Using Twisted Light. *Sensors* **2023**, *23*, 6570. https://doi.org/10.3390/s23146570

Academic Editor: Ettore Bernardi

Received: 30 May 2023
Revised: 17 July 2023
Accepted: 18 July 2023
Published: 21 July 2023

important, as they possess orbital angular momentum (OAM) [22,23] and allow the construction of OAM modes of light. OAM modes enable the construction of orthonormal bases of light in any arbitrary finite dimension. OAM also enables the construction of a mutually unbiased basis of azimuthal angle (ANG) [24–26]. These two properties allow for the generation of the qubit BB84 states [27], as well as their higher-dimensional generalizations, which are especially important in quantum cryptography.

In this work, we perform a proof-of-principle experiment in which we use spatial modes of light to experimentally calculate and verify the value of guesswork for several physically and cryptographically relevant examples involving the BB84 states. We extend the work of Refs. [5,6], both theoretically and experimentally, to higher-dimensional generalizations. Generalizing to higher dimensions allows for an enlarged alphabet and, thus, a more versatile and secure protocol, which is especially attractive considering that the same beams of light are used. We find excellent agreement between our experimental results and theoretical predictions. In each of the cases considered, we find that there is a "quantum" gap in the guesswork between the standard basis measurement and the optimal projective measurement. Our work shows that guesswork can be a viable security criterion in cryptographic tasks, and is experimentally accessible from optical setups.

2. Theory

First, we introduce the theoretical framework of guesswork with quantum side information. Guesswork with quantum side information can be viewed as a multi-round two-party game, as shown in Figure 1. The guesser, Bob, has a classical system or, more generally, a quantum system B, which is correlated with Alice's random variable X. In this work, we consider the latter (and more general) case where Bob possesses quantum side information. This scenario is fully characterized by a classical quantum state ρ_{XB} shared by Alice and Bob, where Alice's symbols and their associated probabilities are captured in the classical register X, and Bob's quantum side information is present in the quantum system B. In the guessing game picture of guesswork, Alice picks an element $x \in \mathcal{X}$ and sends Bob the corresponding quantum state ρ_B^x. Bob then performs quantum measurements on his side information state ρ_B^x, the results of which inform his guessing strategy. In general, Bob performs a quantum instrument before each guess. A quantum instrument yields both a classical measurement outcome and a post-measurement quantum state. This ensures that after each round, Bob has classical information used to make a guess, and also a quantum state for future rounds of the guessing game.

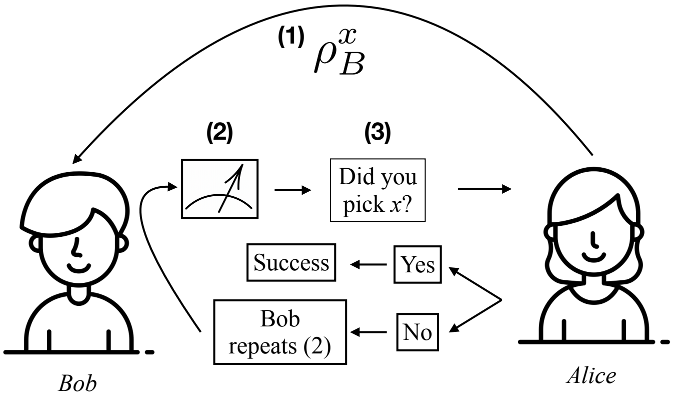

Figure 1. Guesswork can be understood via this guessing game played by Alice and Bob. Alice picks a classical symbol x and sends Bob the corresponding quantum state. Bob guesses Alice's symbol with the help of his quantum state ρ_B^x. In each round of the game, Bob performs a quantum measurement and uses the classical outcome to make a guess. He repeats this process until he guesses correctly.

However, it was shown in Ref. [5] that Bob can do just as well if he performs a single quantum measurement to decide his guessing order; that is, the typical sequential guessing strategy can be reduced to a single-round guessing strategy. This divides the guessing game into two parts: an initial step involving a quantum measurement, followed by a purely classical guessing game between Alice and Bob. Such an equivalence makes a trade-off between time and space, in the sense that Bob needs more spatial resources and fewer temporal resources than the sequential guessing game.

A simple and yet instructive example of guesswork with quantum side information is that involving the four BB84 states [27]. In this case, Alice first picks one of four classical letters x_1 through x_4 with equal probability, and then sends the corresponding BB84 states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ to Bob. Therefore, Bob's side information is hidden in his quantum state. Bob's task is to use his received quantum state to guess which classical letter Alice chose. Suppose that the projective measurement is characterized by the two orthogonal states $\{|\psi(\theta)\rangle, |\psi(\pi/2-\theta)\rangle\}$ where $|\psi(\theta)\rangle := \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$. Alice's states constitute mutually unbiased bases, and Bob's naive strategy would to be to measure in one of them. This would correspond to measuring in the $\{|0\rangle, |1\rangle\}$ basis, or the standard basis as it is known. Measuring in this basis offers the scenario most similar to a classical or digital measurement and yields the average number of guesses as 1.75 (See Appendix A). However, there exists an optimized projective measurement which leads to a smaller guesswork. This optimal measurement is characterized by $\theta = 1/2\arctan(1/3)$. This measurement can be shown to achieve a guesswork of 1.709 [5,6].

It was shown in Ref. [6] that for this case, and in general for any qubit ensemble with uniform probability distribution, a projective measurement suffices to attain the guesswork. Corollary 2 of Ref. [6] provides a closed-form expression for the guesswork applicable in this case, which evaluates the guesswork to be $\frac{5}{2} - \sqrt{\frac{5}{8}} = 1.709$, which, for the above-discussed BB84 example, is indeed the value obtained by the optimized projective measurement characterized above by $\theta = 1/2\arctan(1/3)$. Projective measurements achieve the minimum guesswork only in the $d = 2$ case, and are not sufficient in higher dimensions [6].

From the above simple example, we see a clear separation of guesswork when using the optimal projective measurement compared to a "standard" basis measurement. Such a separation can be interpreted as a quantum gap, or quantum advantage, as an optimized quantum measurement results in lesser number of guesses as compared to a standard basis measurement (resembling a classical/digital measurement). Such a "quantum" separation of the guesswork can also be obtained in higher-dimensional generalizations of the BB84 example; that is, we consider the side information system in the d-dimension BB84 generalization. Alice will pick one of the $2d$ classical symbols with equal probability, each of which is correlated with one of the $2d$ side information states. These $2d$ states are divided into two mutually unbiased bases of d states each. The states are as follows:

$$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, |\widetilde{0}\rangle, |\widetilde{1}\rangle, \ldots, |\widetilde{d-1}\rangle\} \tag{1}$$

where $|\widetilde{j}\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} e^{i2\pi kj/d}\,|k\rangle$ and $|\,\langle i|\widetilde{j}\rangle\,|^2 = 1/d\ \forall\ i,j \in \{0,1,\ldots,d-1\}$. In this case, a standard basis measurement by Bob means that he projects his state onto the basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. When outcome $|k\rangle$ is obtained, Bob can eliminate the $d-1$ standard basis states that are orthogonal to $|k\rangle$. His best strategy, in this case, is then to guess outcome k first, then $\widetilde{0}$ through $\widetilde{d-1}$, and finally the remaining labels in any order. The guesswork in this case is $(d+5)/4$. We provide more details of this calculation in Appendix A.

However, like in the two-dimensional case, Bob can do better by carefully selecting his quantum measurement. We briefly explain the strategy he can use and how it can be optimized. Consider that Bob chooses to project onto an arbitrarily chosen orthonormal basis $\{|\psi_0\rangle, \ldots, |\psi_{d-1}\rangle\}$. If he obtains the outcome corresponding to $|\psi_k\rangle$, then he guesses in decreasing order of the overlap between $|\psi_k\rangle$ and the $2d$ input states. We note again here that the post-measurement guessing strategy is purely classical, and we obtain it by invoking Massey's observation [1] to minimize the guesswork by guessing in decreasing order of the posterior probability of classical symbols.

Since the rules of the game are decided beforehand, Bob finds and decides on his optimal projective measurement via a numerical technique. We perform this optimization for dimensions $d = 3$ and 4 using MATLAB. This optimization also yields the guessing order to use with each of these measurements. Using this technique, we find that there is a significant gap between the guesswork attained by standard basis measurements and that attained by the optimized projective measurement. We summarize this gap in Table 1 and provide more details in Appendix B. We note again that the optimized projective measurement does not yield the minimum guesswork, as we are not optimizing over all POVMs, yet does provide a lower guesswork than the standard basis measurement. Simulating these projective measurements with twisted light can be done by using holograms generated by a spatial light modulator (SLM), which is what we use in our experiment, described below.

Table 1. The guesswork for each of the scenarios considered.

Dimension	Theoretical Value	Experimental Value
	Standard basis measurement	
$d = 2$	1.75	1.7505 ± 0.0017
$d = 3$	2	1.9996 ± 0.0087
$d = 4$	2.25	2.2547 ± 0.0029
	Optimized projective measurement	
$d = 2$	1.709	1.7062 ± 0.0089
$d = 3$	1.9425	1.9439 ± 0.0084
$d = 4$	2.1429	2.1411 ± 0.0025

3. Experiment

We now proceed to describe the experimental apparatus and techniques used to perform our experiment. The generalized BB84 states consist of two mutually unbiased bases. The bases we use in our experiment are the OAM basis and the ANG basis, which are mutually unbiased. Each mode of light in the OAM basis is characterized by an angular momentum quantum number ℓ. In principle, ℓ can be any integer and, therefore, the OAM basis consists of an infinite number of orthogonal modes; thus, it is simple to generate an orthonormal basis in arbitrary dimensions by selecting the appropriate values of ℓ.

For example, if Alice generates the OAM basis consisting of qunatum numbers $\ell \in \{-L, -L+1, \ldots, L-1, L\}$, then we have a $d = 2L + 1$-dimensional OAM basis, consisting of the states $\left\{\Psi^{\ell}_{\mathrm{OAM}} = e^{i\ell\varphi}\right\}_{\ell=-L}^{\ell=L}$.

The ANG basis corresponding to the OAM basis defined above also consists of $2L + 1$ orthogonal states. Each ANG state is a superposition of each of the OAM states. The basis is constituted by the following states:

$$\left\{\Psi^{n}_{\mathrm{ANG}} = \frac{1}{\sqrt{d}} \sum_{\ell=-L}^{\ell=L} e^{\frac{2i\pi n\ell}{d}} \Psi^{\ell}_{\mathrm{OAM}}\right\}_{n=-L}^{n=L}. \tag{2}$$

Simple verification shows that the two bases are indeed mutually unbiased, i.e.,

$$|\langle\Psi^{l}_{\mathrm{OAM}}|\Psi^{n}_{\mathrm{ANG}}\rangle|^2 = 1/d. \tag{3}$$

3.1. Experimental Setup

The schematic diagram of our experimental setup is depicted in Figure 2. Here, Alice prepares quantum states of light which corresponds to her choice of symbol, and then sends to Bob for further processing. In our experiment, Alice uses a spatial light modulator (SLM) and computer-generated holograms to generate the LG modes required in our experiment [28]. This technique enables us to generate spatial modes in the first-order diffraction order of the SLM. This is sufficient to generate the OAM and ANG modes that correspond to generalized BB84 states in higher dimensions. It is also a characteristic of using such spatial modes of light that the same results will hold when the input beams of light consist of single photons, similar to the results of Ref. [29]. The generated modes are filtered and sent to Bob using a 4f optical system. Bob then projects the spatial mode onto a second SLM to perform a projective measurement. The specific holograms imprinted on the SLM dictate the basis onto which the initial mode is projected. The beam reflected by the second SLM corresponds to a post-measurement state, which is propagated to a charge-coupled device (CCD). The spatial profile of the final beam is captured and analyzed. This process is repeated for each of the measurement states to be projected on, and the captured images are then used to compute the guesswork.

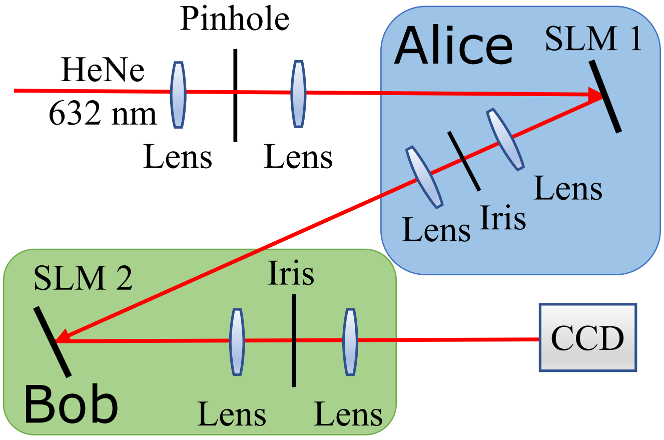

Figure 2. The schematic diagram of the setup used to demonstrate guesswork with quantum side information. The experiment utilizes a He-Ne laser whose output spatial mode is first cleaned. The higher-dimensional generalizations of the BB84 states are prepared by Alice using a spatial light modulator (SLM). The prepared states are sent to Bob through a free-space communication channel, a 4f system. Bob then performs his quantum measurement using a second SLM and a charged coupled device (CCD) camera.

3.2. Experimental Determination of Guesswork

Our goal is to compute the guesswork for the generalized BB84 states for dimensions $d = 2, 3$, and 4. For each dimension, the guesswork is computed for the standard basis measurement, as well as the optimized projective measurement, which makes for a total of six different scenarios. We remark here again that measuring in the standard basis, in this case, one of the mutually unbiased bases comprising the input states, is most akin to a classical measurement and the optimized projective measurement would represent a quantum advantage.

In each iteration of the guessing game, Bob begins with a predecided guessing order for each possible measurement outcome. For each state Alice sends, he projects onto each of the basis states that characterize his measurement. This enables him to determine the relative rate of the measurement outcomes and, hence, decide on the measurement outcome. This holds for both the standard and optimized basis measurement. Once the guessing order is decided, Bob simply sends Alice his guesses—this interaction yields the average number of guesses for each input state. Averaging over input states yields the overall guesswork. The post-processing of CCD images to compute the guesswork is performed using MATLAB.

We perform a total of six experiments corresponding to six scenarios: this comprises two sets of measurements for each of the three dimensions considered. The two measurements are the standard basis measurement and the numerically determined optimal projective measurement. In each case, we repeated the measurement ten times for each input state. Overall, this is equivalent to playing the guesswork game ten times for each of the six scenarios under consideration.

In Table 1, we present our experimental results. The results are divided into two parts: the guesswork when performing a standard basis measurement, and when performing the optimized projective measurement. The errors reported correspond to the standard deviation of our data across experimental iterations. We see that for all scenarios we consider, the guesswork is within 1% of the theoretical prediction for both the standard basis and optimal measurement.

We note here that for such a protocol to be deployed in a real-world setting, there are other considerations that are to be taken into account. These include, but are not limited to, the vulnerability of the protocol to side-channel attacks, such as fault attacks, power analysis attacks, and even combined differential fault analysis and differential power analysis. Specific countermeasures, such as fault detection architectures [30], error detection schemes [31], or fault diagnosis schemes [32], will need to be built in to a security protocol to guard against these attacks. Such a protocol could be implemented either on a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), or on an ARM processor, to name a few. The side channel attack evaluation for each of these will be slightly different, e.g., the difference between the results of Refs. [30,33]. The advent of post-quantum cryptography schemes will also need to be considered, with implementations such as those in Refs. [33,34].

Finally, we remark on the choice of specific OAM modes used for each dimension d. OAM modes are, in principle, orthogonal to each other; thus, any combination of them can be used to construct the desired orthonormal basis. However, due to the finite size of the SLM pixels, they are not perfectly orthogonal in practice. We quantify the overlap between the OAM modes under consideration using a cross-correlation matrix, shown in Figure 3. To minimize overlap errors in our experiment, we choose ℓ values that are spaced further apart from one another to generate our input states, instead of using consecutive ℓ values. For $d = 2$, we use the ℓ values $\{-3, 3\}$. Similarly, for $d = 3$ and $d = 4$, we use ℓ values $\{-3, 0, 3\}$ and $\{-3, -1, 1, 3\}$, respectively. We note that this modification does not alter any of the calculations for the guesswork itself, and is done only to reduce errors that arise from non-zero overlap between nearby OAM modes. An illustrative demonstration of the input modes used for $d = 3$, as well as some of the post-measurement states, are provided in Appendix C.

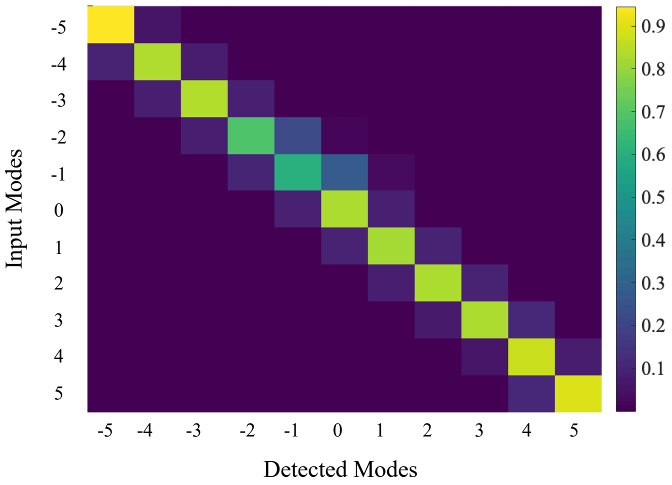

Figure 3. The cross-correlation matrix representing the conditional probabilities between sent and detected modes in the OAM basis. The off-diagonal elements in the figure indicate cross-talks between adjacent modes. The experimental overlap of two adjacent OAM modes is small, indicating a good selection of OAM modes for the experiment.

4. Conclusions

In summary, we showed how to use accessible spatial modes of light to experimentally compute the guesswork in the presence of side information. We considered the side information to be higher-dimensional generalizations of the qubit BB84 states, and showed that the experimentally calculated guesswork matches the theoretical predictions to within an error of 1%.

This proof-of-principle work lays the ground for further experimental applications of guesswork with quantum side information. Ref. [9] identifies a number of use-cases for using the guesswork as an operational quantifier of information, such as in information–disturbance relations and majorization theory. Experimental verification will be necessary for theoretical results that address these problems. The avenues of research for future experimental work also include identifying and performing the optimal measurement for each scenario outside of projective measurements, performing vulnerability analysis for various side channel attacks, and devising countermeasures to such attacks. We hope that our work will serve as a starting point for more experimental uses of the guesswork as a security criterion.

Author Contributions: Conceptualization, V.K., N.B. and C.Y.; Methodology, V.K., N.B. and C.Y.; Investigation, V.K., N.B. and C.Y.; Writing—original draft, V.K., N.B. and C.Y.; Writing—review and editing, V.K., N.B. and C.Y. All authors have read and agreed to the published version of the manuscript.

Funding: V.K. acknowledges support from the LSU Economic Development Assistantship and the US National Science Foundation via grant number 1907615. C.Y. acknowledges funding from the U.S. Department of Energy, Office of Basic Energy Sciences, Division of Materials Sciences and Engineering under Award DE-SC0021069.

Data Availability Statement: Data supporting the reported results is available on request.

Acknowledgments: The authors thank O.S.M.L. for the helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Guesswork Calculation with a Standard Basis Measurement

Appendix A.1. d = 2

In the main text, we stated that when the side information consists of the four BB84 states, the average number of guesses is 1.75 when Bob performs a standard basis $(\{|0\rangle, |1\rangle\})$ measurement.

This number can be understood as follows: if the measurement outcome is $|0\rangle$, then the posterior probabilities of states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ are $\{1/2, 0, 1/4, 1/4\}$. Likewise, for outcome $|1\rangle$, the posterior probabilities are $\{0, 1/2, 1/4, 1/4\}$. For outcome $|0\rangle$, Bob guesses in the order (x_1, x_3, x_4, x_2) and for outcome $|1\rangle$, the guessing order is (x_2, x_4, x_3, x_1). In each of these cases, the average number of guesses is $1 \cdot 1/2 + 2 \cdot 1/4 + 3 \cdot 1/4$ and, thus, the guesswork $G(X|B)_\rho = 1.75$.

Appendix A.2. General Dimension d

In the main text, we showed that for the higher-dimensional generalization of the BB84 example, the guesswork when using a standard basis measurement is $(d+5)/4$ for dimension $d \geq 2$. Here, we show how this is obtained.

We recall that, for dimension d, the $2d$ side information states are divided into two mutually unbiased bases of d states each:

$$\{|0\rangle, |1\rangle, \ldots, |d-1\rangle, |\widetilde{0}\rangle, |\widetilde{1}\rangle, \ldots, |\widetilde{d-1}\rangle\}. \tag{A1}$$

When Bob performs a standard basis measurement, it means that he projects his state onto the basis $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. We know from Massey's criterion [1] that, for optimizing the guesswork, Bob should guess in decreasing order of the posterior distribution of measurement outcomes. When outcome $|k\rangle$ is obtained, Bob can eliminate the $d-1$ computational basis states that are orthogonal to $|k\rangle$.

Given measurement outcome corresponding to $|k\rangle$, the posterior probabilities of the states

$$\{|0\rangle, |1\rangle, \ldots, |k\rangle, \ldots, |d-1\rangle, |\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |\widetilde{d-1}\rangle\} \quad \text{(A2)}$$

are $\{0, 0, \ldots, 1/2, \ldots, 0, 1/2d, 1/2d, \ldots, 1/2d\}$. This means that Bob's guessing order is $(x_k, x_{\tilde{0}}, \ldots, x_{\widetilde{d-1}}, x_0, \ldots x_{k-1}, x_{k+1}, \ldots x_{d-1})$. We note here that this guessing order is quite flexible—all that is required is that the first guess by x_k; the next d guesses correspond to $x_{\tilde{0}}$ through $x_{\widetilde{d-1}}$ in any order, and the remaining standard basis symbols follow again in any order.

The probability of Bob's first guess being right is $1/2$, which we read off the posterior distribution. In case it is incorrect, then the probability of correctness of each of his next d guesses is $1/2d$. We can use this to compute the expected value of the number of guesses:

$$\begin{aligned}
\mathbb{E}[G(X|B)] &= 1 \times \frac{1}{2} + 2 \times \frac{1}{2d} + \cdots + (d+1) \times \frac{1}{2d} + 0 + \cdots + 0 && \text{(A3)}\\
&= \frac{1}{2} + \frac{1}{2d}(2 + 3 + \cdots + (d+1)) && \text{(A4)}\\
&= \frac{1}{2} + \frac{1}{2d}\left(\frac{(d+1)(d+2)}{2} - 1\right) && \text{(A5)}\\
&= \frac{1}{4d}(2d) + \frac{1}{4d}\left(d^2 + 3d\right) && \text{(A6)}\\
&= \frac{d+5}{4}. && \text{(A7)}
\end{aligned}$$

Appendix B. Guesswork Calculation with the Optimal Projective Measurement

First, we detail how we optimize over all projective measurements for arbitrary dimension d. To do so, we consider the basis $\{|\psi_0\rangle, \ldots, |\psi_{d-1}\rangle\}$ to arise from a parameterized $d \times d$ unitary matrix [35]. The rows of the matrix correspond to the coefficients of each state of the orthonormal basis. The guessing orders for each measurement outcome are obtained by calculating the overlaps of each basis state with the generalized BB84 states and then arranging the generalized BB84 states in descending order of their overlaps, just like we described for the standard basis measurement in the preceding paragraph. The optimization procedure to determine the optimal measurement is straightforward, and is performed using the Global Optimization Toolbox in MATLAB. As an illustrative example, we describe the details of this calculation for $d = 3$ below.

Appendix B.1. Guesswork Calculation for d = 3 with the Numerically Determined Measurement

In Table 1 of the main text, we stated that the guesswork for the $d = 3$ BB84 example was 2 when using the standard basis measurement. This follows the $(d+5)/4$ formula that we derived just above in (A7). We also state that using a numerically predetermined projective measurement, we can do better and attain a value of 1.9425. Here, we show how this is achieved.

We recall that the six side information states are:

$$\{|0\rangle, |1\rangle, |2\rangle, |\tilde{0}\rangle, |\tilde{1}\rangle, |\tilde{2}\rangle\} \quad \text{(A8)}$$

whose corresponding classical symbols are $x_0, x_1, x_2, x_{\tilde{0}}, x_{\tilde{1}}$, and $x_{\tilde{2}}$.

Our numerical goal is to optimize the overall possible projective measurements with the aim of minimizing the guesswork; thus, we consider an arbitrary orthonormal basis $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$ onto which we project.

Given an arbitrary basis $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$, the first step is to calculate the overlaps of each of the six side information states (A8) with the three states given above. For each of $|\psi_0\rangle$, $|\psi_1\rangle$, and $|\psi_2\rangle$, we arrange the side information states in decreasing order of overlap. This gives us the optimal guessing order corresponding to each measurement outcome, and the overlaps for each measurement outcome yield the posterior distribution of the correct answer; thus, the average number of guesses for each measurement outcome can be calculated.

Further, Bob's state alone, before any measurement is done, is the maximally mixed state. This can be seen by considering the states in (A8) and taking a uniformly distributed mixture of them. This means that each measurement outcome, averaged over input states, is equally likely. Therefore, the overall guesswork is the average of the number of guesses for each measurement outcome.

So far, we have described how to calculate the guesswork corresponding to an arbitrarily chosen measurement basis $\{|\psi_0\rangle, |\psi_1\rangle, |\psi_2\rangle\}$. All that remains is to optimize over all such measurement bases. These states are parameterized by considering a parameterization of a $d \times d$ unitary matrix given by Hedemann [35]. A 3×3 unitary matrix is parameterized by six complex parameters, a through f, in the following manner:

$$U = \begin{pmatrix} a & bc & bd \\ b^*e & -a^*ce - d^*f^* & -a^*de + c^*f^* \\ b^*f & -a^*cf + d^*e^* & -a^*df - c^*e^* \end{pmatrix}, \tag{A9}$$

subject to the constraints $|a|^2 + |b|^2 = 1$, $|c|^2 + |d|^2 = 1$, and $|e|^2 + |f|^2 = 1$.

We, thus, have that:

$$\begin{aligned} |\psi_0\rangle &= a\,|0\rangle + bc\,|1\rangle + bd\,|2\rangle \\ |\psi_1\rangle &= b^*e\,|0\rangle + (-a^*ce - d^*f^*)\,|1\rangle + (-a^*de + c^*f^*)\,|2\rangle \\ |\psi_2\rangle &= b^*f\,|0\rangle + (-a^*cf + d^*e^*)\,|1\rangle + (-a^*df - c^*e^*)\,|2\rangle\,. \end{aligned} \tag{A10}$$

We use MATLAB's Global Optimization Toolbox to optimize over the six variables and three constraints provided above, and calculate the optimal guesswork for this example across all projective measurements. The optimal states are given by the following coefficients:

$$|\psi_0\rangle = (0.7413 - 0.6421i, \quad 0.0118 + 0.1221i, \quad -0.1085 - 0.1067i) \tag{A11}$$

$$|\psi_1\rangle = (-0.0919 + 0.1244i, \quad 0.0688 - 0.0060i, \quad -0.8069 - 0.5659i) \tag{A12}$$

$$|\psi_2\rangle = (0.0676 + 0.0985i, \quad 0.9847 + 0.1023i, \quad 0.0634 + 0.0389i). \tag{A13}$$

To calculate the guesswork from this, we construct the overlap table between the side information states and the measurement states as follows:

Table A1. This table shows the overlap between each of the input states and each of the states characterizing the measurement. Each row corresponds to an input state and each column corresponds to one of the measurement states.

	$\boldsymbol{\psi_0}$	$\boldsymbol{\psi_1}$	$\boldsymbol{\psi_2}$
$\|0\rangle$	0.4809	0.0120	0.0071
$\|1\rangle$	0.0075	0.0024	0.4901
$\|2\rangle$	0.0116	0.4857	0.0028
$\|\widetilde{0}\rangle$	0.2574	0.1170	0.1257
$\|\widetilde{1}\rangle$	0.1347	0.1482	0.2171
$\|\widetilde{2}\rangle$	0.1079	0.2348	0.1572

For each measurement outcome, the number of guesses can be calculated by arranging the corresponding column in descending order, and then taking an inner product of the column with $(1\,2\,3\,4\,5\,6)$. We then get that the average number of guesses for each of the measurement outcomes is 1.9344, 1.9423, and 1.951. Taking an average of these three numbers yields:

$$G(X|B) = 1.9425. \tag{A14}$$

Appendix B.2. Guesswork Calculation for d = 4 with the Numerically Determined Measurement

A similar procedure as above is followed for the case of $d = 4$. Just like we listed out three different states for $d = 3$ in (A10), we have for four dimensions:

$$\begin{aligned}
|\psi_0\rangle &= a\,|0\rangle + b^* g\,|1\rangle + b^* h^* j\,|2\rangle + b^* h^* k\,|3\rangle \\
|\psi_1\rangle &= bc\,|0\rangle + (-a^* cg + d^* hl)\,|1\rangle + (-a^* ch^* j - d^* g^* jl + d^* k^* m^*)\,|2\rangle \\
&\quad + (-a^* ch^* k - d^* g^* kl - d^* j^* m^*)\,|3\rangle \\
|\psi_2\rangle &= bde\,|0\rangle + (-a^* deg - c^* ehl + f^* hm)\,|1\rangle \\
&\quad + (-a^* deh^* j + c^* eg^* jl - c^* ek^* m^* - f^* g^* jm - f^* k^* l^*)\,|2\rangle \\
&\quad + (-a^* deh^* k + c^* eg^* kl + c^* ej^* m^* - f^* g^* km + f^* j^* l^*)\,|3\rangle \\
|\psi_3\rangle &= bdf\,|0\rangle + (-a^* dfg - c^* fhl - e^* hm)\,|1\rangle \\
&\quad + (-a^* dfh^* j + c^* fg^* jl - c^* fk^* m^* + e^* g^* jm + e^* k^* l^*)\,|2\rangle \\
&\quad + (-a^* dfh^* k + c^* fg^* kl + c^* fj^* m^* + e^* g^* km - e^* j^* l^*)\,|3\rangle\,.
\end{aligned} \tag{A15}$$

We use the same optimization technique used for the $d = 3$ case and obtain the final set of measurement states as follows:

$$|\psi_0\rangle = (-0.1116 - 0.04115i, \quad -0.0015 + 0.0131i, \quad 0.1336 - 0.0510i, \quad 0.0069 + 0.9824i) \tag{A16}$$

$$|\psi_1\rangle = (-0.6943 + 0.6951i, \quad 0.05941 + 0.1301i, \quad -0.081 + 0.0104i, \quad -0.1084 - 0.0490i) \tag{A17}$$

$$|\psi_2\rangle = (-0.1347 + 0.0481i, \quad 0.0138 - 0.9824i, \quad 0.1107 + 0.0435i, \quad 0.0018 - 0.0130i) \tag{A18}$$

$$|\psi_3\rangle = (-0.0104 + 0.0080i, \quad -0.0484 + 0.1086i, \quad 0.6991 + 0.6902i, \quad 0.1298 - 0.0602i). \tag{A19}$$

Following the same procedure for calculating the guesswork as we did for $d = 3$, we get the guesswork in this case to be:

$$G(X|B) = 2.1429. \tag{A20}$$

Appendix C. Alphabet of Input State Beams Used

As an illustration, we show the input beams used for one of the higher-dimensional BB84 experiments below in Figure A1. It shows the six input states that are used for the $d = 3$ case, where each row of images corresponds to one of the two mutually unbiased bases that make up the six input states.

Further, in Figure A2, we show the profiles of the beams of Figure A1 when projected onto the first basis state of the optimized projective measurement, i.e., Equation (A11).

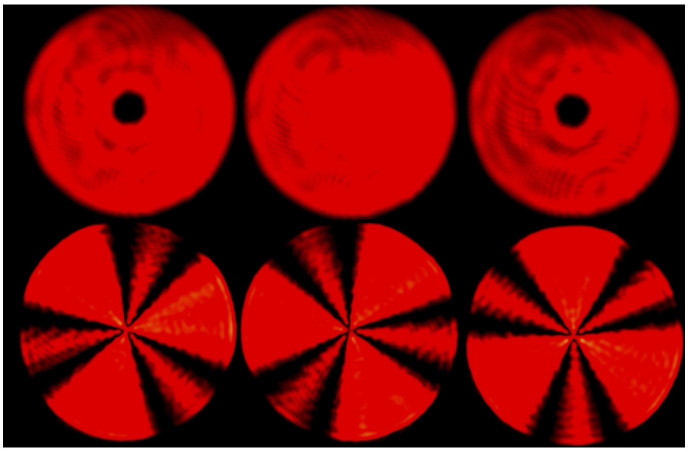

Figure A1. The alphabet of input states for the particular case of dimension $d = 3$. Each image is the CCD image of one of the six input states used. The first row corresponds to OAM modes with $l = -3$, $l = 0$, and $l = 3$. The second row corresponds to the corresponding ANG modes which are created by performing uniform superpositions of the OAM modes in the first row.

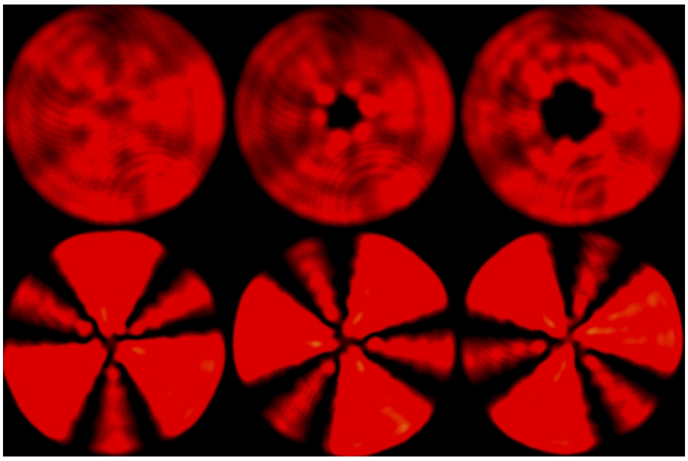

Figure A2. The figure shows the six states in Figure A1 when projected onto the first state of the optimized projective measurement basis, i.e., the state characterized by Equation (A11).

References

1. Massey, J. Guessing and entropy. In Proceedings of the 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, 27 June–1 July 1994; p. 204.
2. Arikan, E. An inequality on guessing and its application to sequential decoding. *IEEE Trans. Inf. Theory* **1996**, *42*, 99–105. [CrossRef]
3. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; Wiley-Interscience: Hoboken, NJ, USA, 2006.
4. Chen, W.; Cao, Y.; Wang, H.; Feng, Y. Minimum Guesswork Discrimination between Quantum States. *Quantum Inf. Comput.* **2015**, *15*, 737–758. [CrossRef]
5. Hanson, E.P.; Katariya, V.; Datta, N.; Wilde, M.M. Guesswork with Quantum Side Information. *IEEE Trans. Inf. Theory* **2022**, *68*, 322–338. [CrossRef]
6. Dall'Arno, M.; Buscemi, F.; Koshiba, T. Guesswork of a Quantum Ensemble. *IEEE Trans. Inf. Theory* **2022**, *68*, 3139–3143. [CrossRef]
7. Dall'Arno, M.; Buscemi, F.; Koshiba, T. Classical computation of quantum guesswork. *arXiv* **2021**, arXiv:2112.01666.
8. Dall'Arno, M. Quantum guesswork. *arXiv* **2023**, arXiv:2302.06783.
9. Avirmed, B.; Niinomi, K.; Dall'Arno, M. Adversarial guesswork with quantum side information. *arXiv* **2023**, arXiv:2306.12633.
10. Bell, T.; Li, B.; Zhang, S. Structured light techniques and applications. In *Wiley Encyclopedia of Electrical and Electronics Engineering*; Wiley-Interscience: Hoboken, NJ, USA, 1999 ; pp. 1–24.
11. Geng, J. Structured-light 3D surface imaging: A tutorial. *Adv. Opt. Photonics* **2011**, *3*, 128–160. [CrossRef]
12. Lavery, M.P.; Speirits, F.C.; Barnett, S.M.; Padgett, M.J. Detection of a spinning object using light's orbital angular momentum. *Science* **2013**, *341*, 537–540. [CrossRef]
13. Malik, M.; Boyd, R. Quantum imaging technologies. *La Rivista del Nuovo Cimento* **2014**, *37*, 273–332.

14. Chen, L.; Lei, J.; Romero, J. Quantum digital spiral imaging. *Light Sci. Appl.* **2014**, *3*, e153. [CrossRef]
15. Mirhosseini, M.; Magaña-Loaiza, O.S.; O'Sullivan, M.N.; Rodenburg, B.; Malik, M.; Lavery, M.P.; Padgett, M.J.; Gauthier, D.J.; Boyd, R.W. High-dimensional quantum cryptography with twisted light. *New J. Phys.* **2015**, *17*, 033033. [CrossRef]
16. Magaña-Loaiza, O.S.; Mirhosseini, M.; Cross, R.M.; Rafsanjani, S.M.H.; Boyd, R.W. Hanbury Brown and Twiss interferometry with twisted light. *Sci. Adv.* **2016**, *2*, e1501143. [CrossRef]
17. Rubinsztein-Dunlop, H.; Forbes, A.; Berry, M.V.; Dennis, M.R.; Andrews, D.L.; Mansuripur, M.; Denz, C.; Alpmann, C.; Banzer, P.; Bauer, T.; et al. Roadmap on structured light. *J. Opt.* **2016**, *19*, 013001. [CrossRef]
18. Yang, Z.; Magaña-Loaiza, O.S.; Mirhosseini, M.; Zhou, Y.; Gao, B.; Gao, L.; Rafsanjani, S.M.H.; Long, G.L.; Boyd, R.W. Digital spiral object identification using random light. *Light Sci. Appl.* **2017**, *6*, e17013. [CrossRef] [PubMed]
19. Milione, G.; Wang, T.; Han, J.; Bai, L. Remotely sensing an object's rotational orientation using the orbital angular momentum of light. *Chin. Opt. Lett.* **2017**, *15*, 030012. [CrossRef]
20. Magaña-Loaiza, O.S.; León-Montiel, R.d.J.; Perez-Leija, A.; U'Ren, A.B.; You, C.; Busch, K.; Lita, A.E.; Nam, S.W.; Mirin, R.P.; Gerrits, T. Multiphoton quantum-state engineering using conditional measurements. *npj Quantum Inf.* **2019**, *5*, 80. [CrossRef]
21. Jack, B.; Leach, J.; Romero, J.; Franke-Arnold, S.; Ritsch-Marte, M.; Barnett, S.; Padgett, M. Holographic ghost imaging and the violation of a Bell inequality. *Phys. Rev. Lett.* **2009**, *103*, 083602. [CrossRef]
22. Siegman, A.E. *Lasers*; University Science Books: Melville, NY, USA, 1986.
23. Allen, L.; Beijersbergen, M.W.; Spreeuw, R.; Woerdman, J. Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes. *Phys. Rev. A* **1992**, *45*, 8185. [CrossRef]
24. Giovannini, D.; Romero, J.; Leach, J.; Dudley, A.; Forbes, A.; Padgett, M.J. Characterization of High-Dimensional Entangled Systems via Mutually Unbiased Measurements. *Phys. Rev. Lett.* **2013**, *110*, 143601. [CrossRef]
25. D'Ambrosio, V.; Cardano, F.; Karimi, E.; Nagali, E.; Santamato, E.; Marrucci, L.; Sciarrino, F. Test of mutually unbiased bases for six-dimensional photonic quantum systems. *Sci. Rep.* **2013**, *3*, 2726. [CrossRef] [PubMed]
26. Malik, M.; O'Sullivan, M.; Rodenburg, B.; Mirhosseini, M.; Leach, J.; Lavery, M.P.J.; Padgett, M.J.; Boyd, R.W. Influence of atmospheric turbulence on optical communications using orbital angular momentum for encoding. *Opt. Express* **2012**, *20*, 13195–13200. [CrossRef]
27. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers Systems and Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
28. Ando, T.; Ohtake, Y.; Matsumoto, N.; Inoue, T.; Fukuchi, N. Mode purities of Laguerre–Gaussian beams generated via complex-amplitude modulation using phase-only spatial light modulators. *Opt. Lett.* **2009**, *34*, 34–36. [CrossRef] [PubMed]
29. Bhusal, N.; Lohani, S.; You, C.; Hong, M.; Fabre, J.; Zhao, P.; Knutson, E.M.; Glasser, R.T.; Magaña-Loaiza, O.S. Spatial Mode Correction of Single Photons Using Machine Learning. *Adv. Quantum Technol.* **2021**, *4*, 2000103. [CrossRef]
30. Sarker, A.; Kermani, M.M.; Azarderakhsh, R. Fault Detection Architectures for Inverted Binary Ring-LWE Construction Benchmarked on FPGA. *IEEE Trans. Circuits Syst. II Express Briefs* **2021**, *68*, 1403–1407. [CrossRef]
31. Mozaffari-Kermani, M.; Azarderakhsh, R.; Aghaie, A. Reliable and Error Detection Architectures of Pomaranch for False-Alarm-Sensitive Cryptographic Applications. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2015**, *23*, 2804–2812. [CrossRef]
32. Aghaie, A.; Mozaffari Kermani, M.; Azarderakhsh, R. Fault Diagnosis Schemes for Low-Energy Block Cipher Midori Benchmarked on FPGA. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2017**, *25*, 1528–1536. [CrossRef]
33. Seo, H.; Azarderakhsh, R. Curve448 on 32-Bit ARM Cortex-M4. In Proceedings of the Information Security and Cryptology—ICISC 2020, Seoul, Republic of Korea, 2–4 December 2020; Hong, D., Ed.; Springer: Cham, Switzerland, 2021; pp. 125–139.
34. Bisheh-Niasar, M.; Azarderakhsh, R.; Mozaffari-Kermani, M. Cryptographic Accelerators for Digital Signature Based on Ed25519. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2021**, *29*, 1297–1305. [CrossRef]
35. Hedemann, S.R. Hyperspherical Parameterization of Unitary Matrices. *arXiv* **2013**, arXiv:1303.5904.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.