DE GRUYTER OPEN Ludus

Games and Puzzles

QUANTUM DISTRIBUTION OF A SUDOKU KEY

Sian K. Jones
University of South Wales
sian-kathryn.jones@southwales.ac.uk

Abstract: *Sudoku grids are often cited as being useful in cryptography as a key for some encryption process. Historically transporting keys over an alternate channel has been very difficult. This article describes how a Sudoku grid key can be secretly transported using quantum key distribution methods whereby partial grid (or puzzle) can be received and the full key can be recreated by solving the puzzle.*

Keywords: sudoku, quantum key distribution methods.

Sudoku grids

A Sudoku grid is a 9×9 array which is further subdivided into "mini-grids" of size 3×3, with each of the 81 cells of the grid containing the values 1 to 9 such that each appears exactly once in each row, column and mini-grid. A Sudoku puzzle contains an incomplete assignment of values to a grid, with the goal of the puzzle being to complete the assignment. The values shown in the puzzle are referred to as givens or predefined cells and are unmovable. Published puzzles should contain a selection of givens chosen carefully to ensure that a solution is unique and a range of types of reasoning may be required to find the solution of a puzzle. A Sudoku puzzle, and its solution is presented in Figure 1.

Recreational Mathematics Magazine, Number 6, pp. 87–93
DOI 10.1515/rmm–2016–0009

						2		
	8				7		9	
6		2				5		
	7			6				
			9		1			
				2			4	
		5				6		3
	9		4				7	
		6						

(a) Sudoku Puzzle

9	5	7	6	1	3	2	8	4
4	8	3	2	5	7	1	9	6
6	1	2	8	4	9	5	3	7
1	7	8	3	6	4	9	5	2
5	2	4	9	7	1	3	6	8
3	6	9	5	2	8	7	4	1
8	4	5	7	9	2	6	1	3
2	9	1	4	3	6	8	7	5
7	3	6	1	8	5	4	2	9

(b) Sudoku Grid

Figure 1: An example sudoku puzzle and its solution [6].

Although published Sudoku puzzles are generally 9×9 in size, other dimensions can be used, and for every non-prime dimension n there is an $n \times n$ Sudoku grid [4]. However not every size of Sudoku has unique size mini-grids. As examples, a 6×6 Sudoku (known as Rudoku) can have mini-grids of size 3×2 or 2×3 (although these are essentially simply a rotation from one to the other), and a 12×12 Sudoku can have mini-grids of size either 3×4 or 6×2 (leading to very different puzzles).

Recently Sudoku grids have been popular for use in cryptographic systems [3, 5, 7, 10, 11] using a variety of methods. In this article we are not going to go into any detail regarding encryption methods using Sudoku grids, instead this article will detail how a key formed using a Sudoku grid can be shared using quantum key distribution using a method similar to the BB84 protocol described in [2].

Throughout this article we will refer to a sender of the message (Alice) and a receiver (Bob). Alice and Bob are two commonly used placeholder names. The names are used for convenience; for example, "Alice sends a message to Bob" is easier to follow than "Party A sends a message to Party B".

Quantum key distribution

Quantum key distribution relates to a branch of cryptography based on physics and quantum mechanics first published in [1]. Quantum cryptographic methods no longer considered to be a secure as once thought, however there are modifications to be able to cope with some attacks, for example [9]. In this section we will describe the BB84 protocol proposed by Charles H. Bennett and Gilles Brassard [2], in which a key is sent securely over a quantum channel.

For a long time physicists and scientists tried to determine if light was a wave or a particle, since it seemed to have properties relating to both. It was eventually determined that photons are the fundamental particle of light and they have the unique property in that they are both a particle and a wave. In order to simplify the explanation of quantum key distribution here we will assume that there are only four polarisation (vibrations) of photons, up-down (denoted |),

left-right ($-$), top left-bottom right ($\backslash$) and bottom left-top right ($/$). The idea is to use photons to transmit data rather than computers. Hence, to transmit a key, a message, or anything you wish to send, you could send it via a fiber optic cable as a sequence of photons.

By placing a polaroid in the path of light it is possible to ensure the emerging beam of light consists only of photons having the same polarisation (direction of vibration) by stopping those photons which are vibrating in the wrong direction (or in some cases altering the direction so that the photon leaving the polaroid is in the right polarisation even if it wasn't when it was approaching the polaroid).

The receiver of the beam of light is able to detect the polarisation of the photons only if they use the correct detector. So, for this simple example, Bob will be able to detect $|$ and $-$ photons if he uses a rectilinear detector (shaped like $+$) and able to correctly detect $\backslash$ and $/$ if he uses a diagonal filter (shaped like $\times$).

However, in some instances a photon vibrating in $\backslash$ or $/$ may travel through a rectilinear detector, randomly changing into either $|$ or $-$, and similarly in some instances a photon vibrating in $|$ or $-$ may travel through a diagonal detector, randomly changing into either $\backslash$ or $/$. A random half don't travel through but a random half do (and then these are then reoriented).

These photons can be used in quantum key distribution to send a binary key over an alternate channel:

1. Alice begins by transmitted a bit-stream of 1s and 0s represented by a polarised photon, according to either the rectilinear (horizontal/vertical) or diagonal polarisation scheme. In the rectilinear scheme 1 is represented by $|$ and 0 by $-$; in the diagonal scheme 1 is represented by $\backslash$ and 0 by $/$.
2. Bob has to measure the polarization of these photons, but since he has no idea of the scheme that Alice used he randomly swaps between his $+$ and $\times$ detectors, sometimes he gets it right sometimes wrong. If Bob uses the wrong detector he may well misinterpret Alice's photon.

   At this point Alice sent 1s and 0s and Bob has detected some correctly and some incorrectly.
3. Alice communicates with Bob on a traditional alternate channel (e.g. a telephone) and tells him the scheme for the photons, but not how she polarized them. So she might say the first was $+$ but she will not say whether it was $|$ or $-$. Bob then tells Alice of which he guessed correct.
4. Finally Alice and Bob ignore all photons for which Bob used the wrong scheme and use only those for which he used the right scheme. This generates a new short sequence of bits for which only Alice and Bob know the values.

In Figure 2 an example is given which includes Alice's original bit sequence and her polarisation schemes, Bob's detections schemes, the measurements he has

made and the final retained bit sequence corresponding to only those bits where Alice and Bob used the same scheme. These three stages have allowed Alice and Bob to share 11001001.

Alice's Bit Sequence	1	0	1	1	0	0	1	1	0	0	1	1
Alice's Polarisation Scheme	+	+	×	+	×	×	×	+	×	+	+	×
BOB's Detection Scheme	+	×	+	+	×	×	+	+	×	+	×	×
Bob's Measurement	1	0	0	1	0	0	1	1	0	0	0	1
Retained Bit Sequence	1	-	-	1	0	0	-	1	0	0	-	1

Figure 2: An example of BB84 quantum key distribution scheme [8].

The really big advantage of doing this comes via quantum mechanical properties. Heisenberg's Uncertainty Principle states that even the act of observing such photons affects them and their polarity. So, if an eavesdropper (Eve) even tries to look at (never mind even try to change!) the communication, she will destroy its configuration, and hence the fact that someone has tried to intercept or eavesdrop will be immediately obvious to the receiver.

Quantum key distribution of sudoku grids

The BB84 protocol detailed in [2] is adapted here (in a simplified version) in order to transmit a Sudoku grid over a quantum channel. In order to coincide with the method described in Section we will consider transmitting a 4×4 Sudoku grid (for example Figure 3(a)). Using two polaroid filters $+$, and $\times$ and four vibrations of photon. This time the direction of vibration will be used to represent a value between 0 and 4 where 0 is represented by $|$, 1 by $-$, 2 by $\backslash$ and 3 is represented by $/$. In order to transmit the grid over the quantum channel the following actions are performed:

1. Alice transmits the 4×4 Sudoku grid as a string of 16 photons, first representing the top left value as a photon, then working through each value of the grid in turn until she reaches the bottom right.

2. Bob has to measure the polarization of these photons, but since he has no idea of the scheme he randomly swaps between his $+$ and $\times$ detectors, sometimes he gets it right sometimes wrong. If Bob uses the wrong detector he may well misinterpret Alice's photon.

   At this point Alice sent her Sudoku grid and Bob has detected some correctly and some incorrectly.

3. Alice communicates with Bob on a traditional alternate channel (e.g. a telephone) and tells him the scheme for the photons, but not how she polarized them. So she might say the first was $+$ but she will not say whether it was $|$ or $-$. Bob then tells Alice of which he guessed correct.

4. Bob recreates the Sudoku grid with as much information as he has managed to detect using the correct filters. Since Bob will not have detected all the values then what remains is a Sudoku puzzle.

5. Bob solves the Sudoku puzzle in order to determine the Sudoku grid key which was sent by Alice.

In the event that Sudoku puzzle does not have a unique solution Bob can contact Alice on a traditional channel to request more information to help him to determine which solution Alice has. The information divulged to Bob at this point, if overhead by an eavesdropper, is not sufficient that the eavesdropper would be able to construct the Sudoku grid without the additional information that Bob has determined over the quantum channel.

Since this process is based on the BB84 protocol then this method will allow Alice and Bob to know if their communication has been eavesdropped.

Example of quantum distribution of a sudoku grid

Alice and Bob are sharing a message but first Alice needs to send her key to Bob on an alternate channel. Alice has only a small message and so has chosen to use a 4×4 Sudoku grid (Figure 3(a)). She sends this grid to Bob in the form of photons where 0 is represented by $|$, 1 by $-$, 2 by $\backslash$ and 3 is represented by $/$, this string is given in Figure 3(b) (the scheme Alice will be using - rectilinear ($+$) or diagonal ($\times$) is also given in Figure 3(b)).

0	1	2	3
3	2	1	0
2	0	3	1
1	3	0	2

(a) Sudoku Key

Value	0	1	2	3	3	2	1	0	2	0	3	1	1	3	0	2
Alice's Scheme	$+$	$+$	$\times$	$\times$	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$	$+$	$\times$
Photon Stream	$\|$	$-$	$\backslash$	$/$	$/$	$\backslash$	$-$	$\|$	$\backslash$	$\|$	$/$	$-$	$-$	$/$	$\|$	$\backslash$

(b) Photon Stream

Figure 3: Alice's sudoku key and photon stream representation.

Bob sets up his photon detector to receive the stream of photons that Alice has sent, he chooses between diagonal and rectilinear randomly (his choice is given in Figure 4(a)). He then calls Alice on an alternate channel to ask her what schemes she used to generate the photons. In those instances where Bob and Alice are using the same scheme Bob will correctly interpret the value sent by Alice. Bob can use these values to construct a Sudoku puzzle grid (Figure 4(b)), and ignore those values for which they used different schemes. He can solve the Sudoku puzzle in order to generate the Sudoku key (Figure 4(c)).

Recreational Mathematics Magazine, Number 6, pp. 87–93
DOI 10.1515/rmm–2016–0009

Photon Stream	|	−	\	/	/	\	−	|	\	|	/	−	−	/	|	\
Bob's Scheme	+	×	+	+	×	×	+	×	+	+	×	+	×	×	+	+
Alice's Scheme	+	+	×	×	×	×	+	+	×	+	×	+	+	×	+	×
Value	0				3	2	1				3	1		3		2

(a) Photon Stream

0			
3	2	1	
		3	1
	3		2

(b) Sudoku Key

0	1	2	3
3	2	1	0
2	0	3	1
1	3	0	2

(c) Sudoku Key

Figure 4: Bob's interpretation of the photon stream and sudoku puzzle/grid.

In this instance Bob does not need any extra information in order to solve the Sudoku puzzle and so Alice and Bob have shared a key over an alternate channel. Alice can now use this key to encrypt a test message and send it to Bob. If Bob can accurately decrypt the test message using the Sudoku grid then they know that Eve has not been eavesdropped in their communication. Had Eve been eavesdropping in their communication it would have altered the photon stream received by Bob and therefore his Sudoku grid would not match Alice's making accurate decryption impossible for Bob.

References

[1] C. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. "Quantum cryptography, or unforgeable subway tokens", in D. Chaum, R. Rivest, and A. Sherman, editors, *Advances in Cryptology*, 267–275, Springer US, 1983.

[2] C. H. Bennett and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing", *IEEE International Conference on Computers, Systems, and Signal Processing*, p. 175, Bangalore, 1984.

[3] C. Chang, Y. Chou, and T. D. Kieu. "An information hiding scheme using Sudoku", *ICICIC '08: Proceedings of the 2008 3rd International Conference on Innovative Computing Information and Control*, p. 17, Washington, DC, USA, 2008.

[4] S. Gupta. "Some results on Su Doku". http://theory.tifr.res.in/~sgupta/sudoku/theorems.pdf (March 2006)

[5] W. Hong, T. Chen, and C. Shiu. "Steganography using Sudoku revisited", *Intelligent Information Technology Application, 2008. IITA '08. Second International Symposium on Intelligent Information Technology Application (IITA'2008)*, 935–939, Shanghai, 2008.

[6] G. Royle. "Combinatorial concepts with Sudoku I: Symmetry". http://people.csse.uwa.edu.au/gordon/sudoku/sudoku-symmetry.pdf (March 2006)

[7] M. H. Shirali-Shahreza and M. Shirali-Shahreza. "Steganography in SMS by Sudoku puzzle", *6th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2008)*, 844–847, Doha, Qatar, March 31 - April 4, 2008.

[8] S. Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Doubleday, New York, USA, 1st edition, 1999.

[9] J. Watrous. "Zero-knowledge against quantum attacks", *Proceedings of the 38th ACM Symposium on Theory of Computing*, pages 296–305. ACM Press, New York, 2006.

[10] H. Wien, C. Tung-Shou, and S. Chih-Wei. "A minimal euclidean distance searching technique for sudoku steganography", *ISISE '08. International Symposium on Information Science and Engieering*, pages 515–518, 2008.

[11] Y. Wu, J. Noonan, and S. Agaian. *Binary data encryption using the sudoku block cipher*, 3915 –3921, 2010.

Recreational Mathematics Magazine, Number 6, pp. 87–93
DOI 10.1515/rmm–2016–0009