Hot Topics in Physical Information (HoTPI-2013)
International Journal of Modern Physics: Conference Series
Vol. 33 (2014) 1460355 (8 pages)
© The Authors
DOI: 10.1142/S201019451460355X

The double-padlock problem: Is secure classical information transmission possible without key exchange?

James M. Chappell*, Lachlan J. Gunn† and Derek Abbott‡
School of Electrical and Electronic Engineering, University of Adelaide, SA 5005, Australia
**james.chappell@adelaide.edu.au*
†*lachlan.gunn@adelaide.edu.au*
‡*derek.abbott@adelaide.edu.au*

Published 17 September 2014

The idealized Kish-Sethuraman (KS) cipher is theoretically known to offer perfect security through a classical information channel. However, realization of the protocol is hitherto an open problem, as the required mathematical operators have not been identified in the previous literature. A mechanical analogy of this protocol can be seen as sending a message in a box using two padlocks; one locked by the Sender and the other locked by the Receiver, so that theoretically the message remains secure at all times. We seek a mathematical representation of this process, considering that it would be very unusual if there was a physical process with no mathematical description. We select Clifford's geometric algebra for this task as it is a natural formalism to handle rotations in spaces of various dimension. The significance of finding a mathematical description that describes the protocol, is that it is a possible step toward a physical realization having benefits in increased security with reduced complexity.

Keywords: Kish-Sethuraman; classical communication; geometric algebra; double padlock.

PACS numbers: 02.10.−v, 02.40.Gh, 89.70.−a, 89.70.−a

Various schemes exist to maintain secure information channels that exploit physical phenomena such as quantum effects[1,2] (eg. indeterminacy, entanglement) or even classical chaos.[2–4] All existing schemes involve, one way or another, the sharing or exchange of a cryptographic key. The open question we address in this paper is: can secure transmission be achieved without any form of key exchange? And if so, which physical property of nature can be exploited to achieve this?

The *Kish-Sethuraman cipher* (KS-cipher) is an idealized protocol that achieves the goal of avoiding key exchange.[5–7] However, this protocol has not yet been realized, as the appropriate physical property, with a supporting mathematical description, has not yet been identified. We will be pursuing this idea employing higher dimensional rotation operators, and hence a natural mathematical formalism within which to explore such ideas is Clifford's geometric algebra.

First, let us briefly review how the Kish-Sethuraman cipher protocol works, using a mechanical analogy. Suppose Bob wishes to transmit a written message to Alice; Bob hides the message in a box that he securely padlocks before sending it to Alice. After receiving the box, Alice adds a second padlock and sends the box back to Bob. Then Bob unlocks his padlock, leaving the box still secured by Alice's lock, and sends it back to Alice who can then remove her lock, open the box and read the message as shown in Fig. 1.

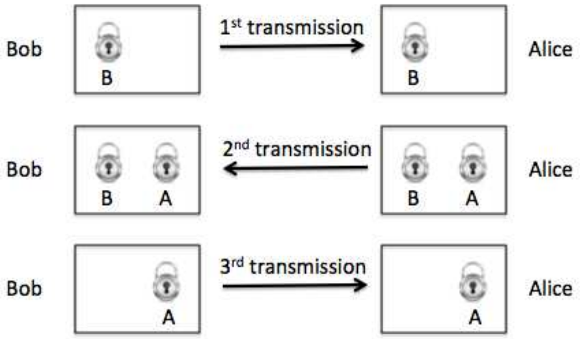

Fig. 1. The double padlock protocol of Kish and Sethuraman. Bob firstly locks the box and sends it to Alice. Then, once received, Alice also padlocks the box with a second lock and sends it back to Bob. Finally, Bob unlocks his padlock, and sends the box back to Alice who can then remove her lock, open the box, and read the message. The message appears perfectly secure because at all times it has been secured by at least one lock.

This KS-cipher protocol is perfectly secure because both Bob and Alice keep their keys undisclosed so that at all times the box is locked by at least one padlock, thus no information is leaked or shared.[6] Hence we can say that in the physical world, a completely secure classical protocol is conceptually possible. In practice, a physical box can be broken, however, what is important to our analysis is the security of the lock protocol. This physical example is clearly classical and so we would expect that there would be a mathematical model to describe this process. That is, it would seem strange if there was such a simple physical scenario for which there was no counterpart in the mathematical world and so would run counter to general trend of the success of mathematics in describing the physical world. This then underlies the motivation for expecting that a mathematical description might indeed be feasible.

The significance of a mathematical protocol simulating the double-padlock problem is that it would potentially be the underpinnings of a relatively simple method of avoiding key exchange for secure information transmission.

Firstly we note that the ordering of the padlocks commutes. That is Alice and Bob can take off or add their padlock in any order, which is the primary aspect of the protocol that permits it to work and hence we are looking to find two mathematical operations that can be applied by Alice and Bob that commute. We can immediately identify an example of this in the case of two-dimensional rotations. Two dimensional rotations can also be seen as generalization of the bit flip operation on binary strings.

For example, the message Bob wants to secretly send could be the value θ. Bob 'hides' θ by adding a random angle ϕ_1 (his 'key') to it and sends it to Alice. Then Alice adds another random angle ϕ_2 (her 'key') and sends it back to Bob. Then Bob undoes his secret rotation ϕ_1 and returns the message to Alice. Then Alice undoes her rotation ϕ_2 and recovers the original value of θ. These operations are most elegantly analyzed in two-dimensional geometric algebra, where we have a message vector $\mathbf{m} = m_1 e_1 + m_2 e_2$, using e_1 and e_2 as orthogonal basis elements and producing the bivector iota $\iota = e_1 e_2$. Acting on the message vector with a rotor $R = \mathrm{e}^{\iota\phi}$ produces a rotated vector

$$\mathbf{m}' = R\mathbf{m} = \mathrm{e}^{\iota\phi}\mathbf{m}, \tag{1}$$

where $\mathbf{m}' = m_1' e_1 + m_2' e_2$, analogous to rotations in the Argand plane. Therefore ϕ in this case represents the private key and rotates the vector $\mathbf{m}$ by a clockwise angle ϕ. Refer to the Appendix for a brief summary of these operations that utilize geometric algebra. Therefore, after the operations by Alice and Bob we find

$$\mathbf{m}_{\text{final}} = \tilde{R}_A \tilde{R}_B R_A R_B \mathbf{m} = \tilde{R}_A R_A \tilde{R}_B R_B \mathbf{m} = \mathbf{m}, \tag{2}$$

where because the rotation operators commute and $\tilde{R}_A R_A = \tilde{R}_B R_B = 1$, we recover the initial message. The message (the angle with the e_1 axis say) can be recovered from $\cos\theta = \mathbf{m} \cdot e_1 / |\mathbf{m}|$, where the vector length $|\mathbf{m}| = \sqrt{\mathbf{m}^2}$.

While this process indeed hides the message at each stage, an eavesdropper, Eve, by comparing the successive intermediate transmissions, can deduce the intermediate rotations and hence discover the two keys (ϕ_1 and ϕ_2) thereby unlocking the message. That is, intercepting two consecutive transmissions, which consist of two-dimensional vectors, Eve can easily calculate the rotation angle between them from $\mathbf{m}_2 = \mathrm{e}^{\iota\phi}\mathbf{m}_1$, which can be rearranged to give $\mathrm{e}^{\iota\phi} = \mathbf{m}_2 \mathbf{m}_1^{-1}$. The inverse of a vector being easily calculated when it is represented in geometric algebra, as shown in the Appendix.

In order to circumvent the vulnerability of two-dimensional rotations we now explore the use of rotations in three dimensions. In this case, given an initial and a final rotated vector it is not possible to simultaneously deduce the rotation axis and rotation magnitude, as only the plane of possible rotation axes can be found, and hence appears secure against an eavesdropper. In three dimensions, we have a message vector $\mathbf{m} = m_1 e_1 + m_2 e_2 + m_3 e_3$ and define the trivector $i = e_1 e_2 e_3$ that commutes with all variables with $i^2 = (e_1 e_2 e_3)^2 = -1$. Acting on the message vector with a rotor $R = \mathrm{e}^{i\hat{v}\phi/2}$ produces a rotated vector

$$\mathbf{m}' = R\mathbf{m}\tilde{R} = \mathrm{e}^{i\hat{v}\phi/2}\mathbf{m}\mathrm{e}^{-i\hat{v}\phi/2}, \tag{3}$$

where $\mathbf{m}' = m_1'e_1 + m_2'e_2 + m_3'e_3$, and $\hat{v}$ represents the unit rotation axis vector in three dimensions and ϕ a clockwise rotation magnitude in radians. We have also defined the *reversion* operation, which inverts the order of all algebraic products, that is, $\tilde{R} = \mathrm{e}^{-\iota\hat{v}\phi/2}$. Therefore ϕ and $\hat{v}$ represents a private key with three degrees of freedom. So given two rotors selected independently by Alice and Bob $R_A = \mathrm{e}^{\iota\hat{v}\phi/2}$ and $R_B = \mathrm{e}^{\iota\hat{w}\theta/2}$, we have an encryption process

$$\mathbf{m}_{\text{final}} = \tilde{R}_A\tilde{R}_B R_A R_B \mathbf{m}\tilde{R}_B\tilde{R}_A R_B R_A. \tag{4}$$

In order for this process to succeed we require R_A and R_B to commute, however

$$\begin{aligned} R_A R_B - R_B R_A &= -\sin\frac{\phi}{2}\sin\frac{\theta}{2}\left(\hat{v}\hat{w} - \hat{w}\hat{v}\right) \\ &= -\sin\frac{\phi}{2}\sin\frac{\theta}{2}\mathbf{v}\wedge\mathbf{w}. \end{aligned} \tag{5}$$

This implies $\mathbf{v}\wedge\mathbf{w} = 0$, or that $\mathbf{v}$ and $\mathbf{w}$ are parallel, or the rotation angles $\phi = 0$ or $\theta = 0$. However in order for Alice and Bob to use parallel vectors, a preferred direction would need to be communicated.

Hence, in three dimensions, while rotations are a secure form of encryption individually, in order for the rotation operators of Alice and Bob to commute they need to agree on a preferred direction, which violates the premise of the protocol. Thus, in order for rotational operators to commute it appears that we need to implement the rotations within a higher dimensional space. However, rather than proceeding immediately to a four dimensional Cartesian space, we can use instead a known result from quaternion theory,[8] that a 4D rotation can be made isomorphic to a bilinear quaternion rotation

$$q' = \mathrm{e}^{\vec{r}}q\mathrm{e}^{\vec{s}} \tag{6}$$

where we use the vector quaternions $\vec{r} = r_1\mathrm{i} + r_2\mathrm{j} + r_3\mathrm{k}$, $\vec{s} = s_1\mathrm{i} + s_2\mathrm{j} + s_3\mathrm{k}$, and where we represent a four vector with the quaternion $q = v_1 + v_2\mathrm{i} + v_3\mathrm{j} + v_4\mathrm{k}$. The quaternions defined through the usual relations $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1 = \mathrm{ijk}$ with $\mathrm{i}, \mathrm{j}, \mathrm{k}$ anticommuting. Now, using the isomorphism between quaternions and the even subalgebra of three-dimensional GA, $\mathrm{i} \to e_2e_3$, $\mathrm{j} \to e_1e_3$, $\mathrm{k} =\to e_1e_2$, we can express this result in GA as

$$\mathbf{y} + iy_4 = \mathrm{e}^{i\mathbf{v}}(\mathbf{x} + ix_4)\mathrm{e}^{i\mathbf{w}}, \tag{7}$$

where $\mathbf{v} = v_1e_1 + v_2e_2 + v_3e_3$, $\mathbf{w} = w_1e_1 + w_2e_2 + w_3e_3$ and $\mathbf{x} = x_1e_1 + x_2e_2 + x_3e_3$, $\mathbf{y} = y_1e_1 + y_2e_2 + y_3e_3$ are three vectors, and where we can define a 4D message vector as $m = \mathbf{m} + im_4$. Hence Bob (and similarly for Alice) has an operator of the form $m' = \mathrm{e}^{\mathbf{v}}m\mathrm{e}^{\mathbf{w}}$, where $\mathbf{v}, \mathbf{w}$ are three vectors. Hence the full encryption process, from Eq. (4) will be

$$m' = \mathrm{e}^{-i\mathbf{x}}\mathrm{e}^{-i\mathbf{v}}\mathrm{e}^{i\mathbf{x}}\mathrm{e}^{i\mathbf{v}}m\mathrm{e}^{i\mathbf{w}}\mathrm{e}^{i\mathbf{y}}\mathrm{e}^{-i\mathbf{w}}\mathrm{e}^{-i\mathbf{y}} \tag{8}$$

Now, referring to our previous result for 3D, from Eq. (5), these operations will only commute if the rotation axes, $\mathbf{v}, \mathbf{x}$ and $\mathbf{w}, \mathbf{y}$ are parallel. Hence, once again, this encryption process will be insecure due to having insufficient degrees of freedom. An amination has been developed to illustrate the character of 4D rotations produced in this way.

Hence we now have two choices to either proceed to five dimensional rotations, or seek a more sophisticated encryption process. An attempt at a more sophisticated encryption process is provided in the appendix.

In conclusion, in this paper, through investigating higher order rotations, we attempt to solve the double padlock problem, that would provide a set of working mathematical operators for the Kish-Sethuraman (KS) cipher that is a classically secure protocol. However, while possible conceptually, in practice it appears that we are blocked on information theoretic bounds. That is, the requirement, for example, that in order to transfer information securely we need some level of mutual information between Alice and Bob. However it would be of interest to pursue higher order solutions in higher dimensional spaces in order to discover where the limitation arises.

The encoding of these multidimensional operations onto real signals also remains an open question for further study, and it is worth noting that various multidimensional spaces are already exploited by engineers in standard communications theory, for example see Ref. 9.

Whilst it is of interest for future work to explore how to physically encode higher dimensional rotations on a wireless carrier signal, the scheme has wider implications. For example, Klappenecker has conjectured a connection between a mathematical realization of the KS-cipher protocol and the P versus NP problem in computer science.[7] Thus it may be of interest to explore implications of the KS operations developed in this paper on the P versus NP problem.

If a mathematical protocol can be encoded on a wireless carrier or fiber optic signal, a benefit would be secure communication without key exchange and the promise of a relatively simple physical realization.

Appendix A

A.1. *Geometric algebra representation of vectors*

In order to represent the three independent degrees of freedom of physical space, Clifford defined an associative algebra consisting of three elements e_1, e_2 and e_3, with the properties

$$e_1^2 = e_2^2 = e_3^2 = 1 \tag{9}$$

but with each element anticommuting, that is $e_j e_k = -e_k e_j$, for $j \neq k$. We also define the trivector $i = e_1 e_2 e_3$, which allows us to write $e_2 e_3 = i e_1$, $e_3 e_1 = i e_2$ and $e_1 e_2 = i e_3$. The highest grade element we also call the pseudoscalar.

Now, given two vectors $\mathbf{a} = a_1e_1 + a_2e_2 + a_3e_3$ and $\mathbf{b} = b_1e_1 + b_2e_2 + b_3e_3$, using the distributive law for multiplication over addition,[10] as assumed for an algebraic field, we find their product

$$\begin{aligned}\mathbf{ab} &= (a_1e_1 + a_2e_2 + a_3e_3)(b_1e_1 + b_2e_2 + b_3e_3) \\ &= a_1b_1 + a_2b_2 + a_3b_3 + (a_2b_3 - a_3b_2)e_2e_3 \\ &\quad +(a_3b_1 - a_1b_3)e_3e_1 + (a_1b_2 - a_2b_1)e_1e_2,\end{aligned} \tag{10}$$

where we have used the elementary properties of e_1, e_2, e_3 defined in Eq. (9). Recognizing the dot and wedge products, we can write

$$\mathbf{ab} = \mathbf{a}\cdot\mathbf{b} + \mathbf{a}\wedge\mathbf{b}. \tag{11}$$

We can see from Eq. (10), that the square of a vector $\mathbf{a}^2 = \mathbf{a}\cdot\mathbf{a} = a_1^2 + a_2^2 + a_3^2$, becomes a scalar quantity. Hence the Pythagorean length of a vector is simply $|\mathbf{a}| = \sqrt{\mathbf{a}^2}$, and so we can find the inverse vector

$$\mathbf{a}^{-1} = \frac{\mathbf{a}}{\mathbf{a}^2}. \tag{12}$$

These results can easily be adapted for a space of any number of dimensions. In odd dimensions the pseudoscalar is commuting, but in even dimensions it is anticommuting. In dimensions $\{2,3\},\{6,7\},\{10,11\},\ldots$ the pseudoscalar squares to minus one, while in dimensions $\{4,5\},\{8,9\},\{12,13\},\ldots$ it squares to positive one.

A.2. *Commuting multivectors in 2D*

In an attempt to circumvent the vulnerability of two-dimensional rotations, we can consider more general operators using two-dimensional multivectors

$$M = a + \mathbf{v} + \iota b, \tag{13}$$

where a and b are scalars, ι is the bivector and a planar vector $\mathbf{v} = v_1e_1 + v_2e_2$. That is $\bigwedge \Re^2$ is the exterior algebra of $\Re^2$ which produces the space of multivectors $\Re \oplus \Re^2 \oplus \bigwedge^2 \Re^2$, a four-dimensional real vector space denoted by $Cl_{2,0}(\Re)$. We now have the encryption process

$$\mathbf{m}_{\text{final}} = M_A^{1\dagger} M_B^{1\dagger} M_A^1 M_B^1 \mathbf{m} M_B^2 M_A^2 M_B^{2\dagger} M_A^{2\dagger}, \tag{14}$$

where the † operation is an *inverse* operation, such that $M_A^\dagger M_A = M_B^\dagger M_B = 1$.

Seeking commuting operators M_A and M_B, that is $M_AM_B - M_BM_A = 0$ we require

$$\begin{aligned}&(a + \mathbf{v} + \iota b)\,(c + \mathbf{w} + \iota d) - (c + \mathbf{w} + \iota d)\,(a + \mathbf{v} + \iota b) \\ &= 2\mathbf{v}\wedge\mathbf{w} - 2\iota d\mathbf{v} + 2\iota b\mathbf{w} = 0.\end{aligned} \tag{15}$$

The bivector components give $\mathbf{v}\wedge\mathbf{w} = 0$, which implies that $\mathbf{v}$ and $\mathbf{w}$ are parallel, and the vector components then give $\iota d\mathbf{v} - \iota b\mathbf{w} = 0$ that implies $\frac{|\mathbf{v}|}{b} = \frac{|\mathbf{w}|}{d} = r$, where r needs to be a preset part of the protocol along with the common direction for $\mathbf{v}$ and $\mathbf{w}$. Hence Bob can utilize multivectors

$$M_B^1 = a + ve_1 + \iota v/r\,,\; M_B^2 = b + we_2 + \iota w/r. \tag{16}$$

The message vector will be represented by a multivector with four degrees freedom, that is now acted on by encryption operators with four degrees of freedom (a, v, b, w), that will produce four equations in four unknowns and hence can be decrypted.

A.3. *Commuting multivectors in 3D*

We can write general three-dimensional multivector operators for Alice and Bob as

$$M_A = a + \mathbf{v} + i\mathbf{w} + ib\,,\; M_B = c + \mathbf{r} + i\mathbf{s} + id \tag{17}$$

where $\mathbf{v}$,$\mathbf{w}$ and $\mathbf{r}$,$\mathbf{s}$ are three-vectors. This is the space of multivectors $\Re \oplus \Re^3 \oplus \bigwedge^2 \Re^3 \oplus \bigwedge^3 \Re^3$, an eight-dimensional real vector space denoted by $Cl_{3,0}(\Re)$. We now seek M_A and M_B to be commuting in order to use the procedure in Eq. (4), requiring

$$\begin{aligned} 0 &= M_A M_B - M_B M_A \\ &= 2(\mathbf{v}\wedge\mathbf{r} - \mathbf{w}\wedge\mathbf{s}) + 2i(\mathbf{v}\wedge\mathbf{s} + \mathbf{w}\wedge\mathbf{r}), \end{aligned} \tag{18}$$

and to make this commutator vanish, while trying to avoid sharing information, we can select $\mathbf{w} = P\mathbf{v}$ and $\mathbf{s} = P\mathbf{r}$, where P anticommutes with $\mathbf{v}$ and $\mathbf{r}$, with $P^2 = -1$. In order for P to be anticommuting it is necessarily orthogonal to $\mathbf{v}$ and $\mathbf{r}$, and this orthogonal direction needs to be shared between Alice and Bob. Now, without loss of generality we can select the agreed orthogonal direction as e_3. We therefore have $\mathbf{w} = \mathbf{v}ie_3$ and $\mathbf{s} = \mathbf{r}ie_3$, with the vectors now planar in order to anticommute with e_3, so we define $\mathbf{v}_{12} = v_1e_1 + v_2e_2$. That is, we have the commuting operators

$$\begin{aligned} M_A &= (a + \mathbf{v}_{12} + e_3\mathbf{v}_{12} + ib) \\ M_B &= (c + \mathbf{w}_{12} + e_3\mathbf{w}_{12} + id)\,. \end{aligned} \tag{19}$$

We have the encrypted message for Alice, for example, given by

$$M' = (a + \mathbf{v}_{12} + e_3\mathbf{v}_{12} + ib)\, M\, (c + \mathbf{w}_{13} + e_2\mathbf{w}_{13} + id)\,. \tag{20}$$

We have eight degrees of freedom available in this encryption process $(a, v_1, v_2, b, c, w_1, w_3, d)$, acting on a eight dimensional multivector. Hence we have eight equations in eight unkowns, and the message can be decrypted by Eve.

References

1. H. Buhrman, M. Christandl, and C. Schaffner, Phys. Rev. Lett. **109**, 160501 (2012).
2. H. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
3. R. Nguimdo, P. Colet, L. Larger, and L. Pesquera, Phys. Rev. Lett. **107**, 34103 (2011).
4. I. Kanter, E. Kopelowitz, and W. Kinzel, Phys. Rev. Lett. **101**, 84102 (2008).
5. L. B. Kish and S. Sethuraman, Fluctuation and Noise Letters **4**, 1 (2004).

6. L. B. Kish, S. Sethuraman, and P. Heszler, AIP Conference Proceedings **800**, 193 (2005).
7. A. Klappenecker, Fluctuation and Noise Letters **4**, 25 (2004).
8. J. Weiner and G. R. Wilkens, Am. Math. Mon. **112**, 69 (2005).
9. M. El-Hajjar, O. Alamri, J. Wang, S. Zummo, and L. Hanzo, IEEE Trans. Wireless Comm. **8**, 3335 (2009).
10. C. J. L. Doran and A. N. Lasenby, *Geometric Algebra for Physicists* (Cambridge University Press, Cambridge, 2003).