International Journal of Modern Physics: Conference Series

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

JAMES M. CHAPPELL
School of Electrical and Electronic Engineering
THE UNIVERSITY OF ADELAIDE, SA 5005, AUSTRALIA
james.chappell@adelaide.edu.au

LACHLAN J. GUNN
School of Electrical and Electronic Engineering
THE UNIVERSITY OF ADELAIDE, SA 5005, AUSTRALIA
lachlan.gunn@adelaide.edu.au

DEREK ABBOTT
School of Electrical and Electronic Engineering
THE UNIVERSITY OF ADELAIDE, SA 5005, AUSTRALIA
derek.abbott@adelaide.edu.au

Received 8 10 2013
Revised Day Month Year

The Kish-Sethuraman (KS) cipher is a general protocol for secure communication without key exchange. 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. In this analogy the message remains secure at all times, and so we seek a mathematical representation of this process. The XOR operation can be viewed as a rotation of a bit by 180 degrees, and so we extend this idea to general rotational operators of higher dimension. We select Clifford's geometric algebra for this task as it is a natural formalism to handle rotations in spaces of any number of dimensions. A geometric interpretation of the protocol is attractive, as it may potentially provide a basis for intuitive reasoning regarding its behaviour under noise.

Keywords: Kish-Sethuraman, classical communication, geometric algebra, double padlock

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

1. Introduction

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[2,3,4,5]. 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 property can be exploited to achieve this?

The *Kish-Sethuraman cipher* (KS-cipher) is an idealized protocol that apparently achieves the goal of avoiding key exchange[6,7,8]. However, this protocol has not yet been realized, as the appropriate property, with a supporting mathematical description, has not yet been identified. Here, we pursue 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 the Kish-Sethuraman cipher protocol, 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.

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[7]. 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.

The significance of a mathematical protocol simulating the double-padlock problem is that it would potentially underpin a relatively simple method of secure information transmission without key exchange.

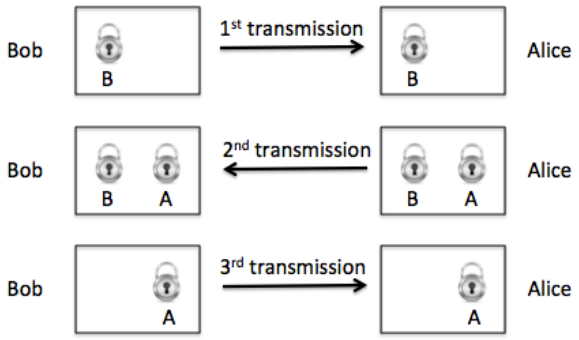

Fig. 1. The double padlock protocol of Kish and Sethuraman. Bob firstly locks the box and sends it to Alice. Then, once received, Alice also padlocks the box with a second lock and sends it back to Bob. Finally, Bob unlocks his padlock, and sends the box back to Alice who can then remove her lock, open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

2. Analysis

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. This is one of the primary aspects 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 Clifford geometric algebra (GA), 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 a plane of possible rotation axes can be found, and hence, with a single usage, secure against an eavesdropper. In three dimensions, let the message vector $\mathbf{m} = m_1 e_1 + m_2 e_2 + m_3 e_3$ and define the trivector $i = e_1 e_2 e_3$,

which commutes with all multivectors and has $i^2 = (e_1e_2e_3)^2 = -1$. 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 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

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

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

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

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, reducing this to the 2D case

Hence, in three dimensions, while rotations are a secure form of encryption, in order for the rotation operators of Alice and Bob to commute they need to agree on a preferred direction, which reduces the degrees of freedom in the keys equivalent to the 2D case. Thus, in order for rotational operators to commute it appears that we need to implement the rotations within a higher dimensional space.

2.1. *Four dimensional rotations*

Rather than proceeding immediately to a more complex four dimensional Cartesian space, we can use instead a known result from quaternion theory[9], that a 4D rotation can be made isomorphic to a bilinear quaternion operation

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

where we have 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 full 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, there is a well known isomorphism between quaternions and the even subalgebra of the three-dimensional GA. That is, in GA we can represent quaternions as $\mathrm{i} \to e_2e_3$, $\mathrm{j} \to e_1e_3, \mathrm{k} \to e_1e_2$, and hence we can now express Eq. (6) as

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

where $\mathbf{v}, \mathbf{w}, \mathbf{x}$ and $\mathbf{y}$ are three vectors, and where we can define a 4D message vector as $m = \mathbf{m} + im_4 = m_1e_1 + m_2e_2 + m_3e_3 + m_4e_1e_2e_3$. Hence Bob (and similarly for

Alice) has an encryption operator of the form $m' = \mathrm{e}^{i\mathbf{v}} m \mathrm{e}^{i\mathbf{w}}$, 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.

2.2. *Discussion*

A possible argument why further exploration in higher dimensional spaces may not yield the required result is by viewing the situation from an information-theoretic standpoint, as follows. Suppose Alice, Bob, and Eve have access to random variables X, Y, and Z, with joint distribution $P_{X,Y,Z}$. Maurer[10] provides an upper bound on the secrecy rate

$$C_s \leq I(X;Y), \tag{9}$$

where $I(X,Y)$ is the mutual information of X and Y. In the Kish-Sethuraman cipher, Alice and Bob do not have access to any shared form of randomness, merely their own random number generators. That is to say, X and Y are independent, and therefore $I(X;Y) = 0$. The secrecy rate is therefore equal to zero from Eq. (9), and the protocol thus lacks information-theoretic security. This argument is a non constructive proof of why a protocol without key exchange must fail, however a constructive proof in terms of N-dimensional rotations would still be a useful result.

2.3. *Conclusion*

In conclusion, in this paper, through investigating higher order rotations, we attempt to solve the double padlock problem, which 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, see Eq. (9). Nevertheless it would be of interest to pursue solutions in higher dimensional spaces in order to discover, if possible, a constructive proof for this result in terms of N-dimensional rotations.

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 El-Hajjar et al.[11]

Whilst KS-scheme in higher dimensional space may not offer ultimate security, it may be of benefit for providing a layer of partial security in conjunction with other schemes. Also, while 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[8]. 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 communication, with some degree of security, without key exchange and the promise of a relatively simple physical realization.

Whilst this paper indicates that moving to higher dimensional spaces apparently does not assist the KS-cipher protocol, this has motivated us to pursue a different KS implementation based on exploiting stochastic message transmission times[12]. Nonetheless, this geometric interpretation has potential value in the analysis of such protocols on noisy channels.

Appendix A. 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

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

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 $\mathbf{a} = a_1 e_1 + a_2 e_2 + a_3 e_3$ and $\mathbf{b} = b_1 e_1 + b_2 e_2 + b_3 e_3$, using the distributive law for multiplication over addition[13], as assumed for an algebraic field, we find their product

$$\begin{aligned} \mathbf{ab} &= (a_1 e_1 + a_2 e_2 + a_3 e_3)(b_1 e_1 + b_2 e_2 + b_3 e_3) \\ &= a_1 b_1 + a_2 b_2 + a_3 b_3 + (a_2 b_3 - a_3 b_2) e_2 e_3 \\ &\quad + (a_3 b_1 - a_1 b_3) e_3 e_1 + (a_1 b_2 - a_2 b_1) e_1 e_2, \end{aligned} \tag{A.2}$$

where we have used the elementary properties of e_1, e_2, e_3 defined in Eq. (A.1). Recognizing the dot and wedge products, we can write

$$\mathbf{ab} = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \wedge \mathbf{b}. \tag{A.3}$$

We can see from Eq. (A.2), 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

$$\mathbf{a}^{-1} = \frac{\mathbf{a}}{\mathbf{a}^2}. \tag{A.4}$$

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.

References

1. H. Buhrman, M. Christandl and C. Schaffner, *Phys. Rev. Lett.* **109**, p. 160501 (Oct 2012).
2. H. Lo, M. Curty and B. Qi, *Phys. Rev. Lett.* **108**, p. 130503 (2012).
3. R. Nguimdo, P. Colet, L. Larger and L. Pesquera, *Phys. Rev. Lett.* **107**, p. 34103 (2011).
4. I. Kanter, E. Kopelowitz and W. Kinzel, *Phys. Rev. Lett.* **101**, p. 84102 (2008).
5. S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe and N. Mandayam, *Wireless Communications, IEEE* **17**, 63 (2010).
6. L. B. Kish and S. Sethuraman, *Fluctuation and Noise Letters* **4**, 1 (2004).
7. L. B. Kish, S. Sethuraman and P. Heszler, *AIP Conference Proceedings* **800**, 193 (2005).
8. A. Klappenecker, *Fluctuation and Noise Letters* **4**, 25 (2004).
9. J. Weiner and G. R. Wilkens, *Am. Math. Mon.* **112**, 69 (2005).
10. U. Maurer, *IEEE Transactions on Information Theory* **39**, 733 (May 1993).
11. M. El-Hajjar, O. Alamri, J. Wang, S. Zummo and L. Hanzo, *IEEE Trans. Wireless Comm.* **8**, 3335 (July 2009).
12. L. Gunn, J. Chappell, A. Allison and D. Abbott, *International Journal of Modern Physics–in this special issue* (2013).
13. C. J. L. Doran and A. N. Lasenby, *Geometric Algebra for Physicists* (Cambridge University Press, Cambridge, 2003).