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

James M. Chappell[1,*] and Derek Abbott[1]

[1]*School of Electrical and Electronic Engineering, University of Adelaide, SA 5005, Australia*

(Dated: December 16, 2012)

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 and indeed we find a solution within a three and four dimensional Clifford algebra. 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.

PACS numbers: 03.67.Dd

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. In this paper we show that classical operations on a Clifford space remarkably possess the required mathematical properties and we develop an appropriate ansatz based on Clifford 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.

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

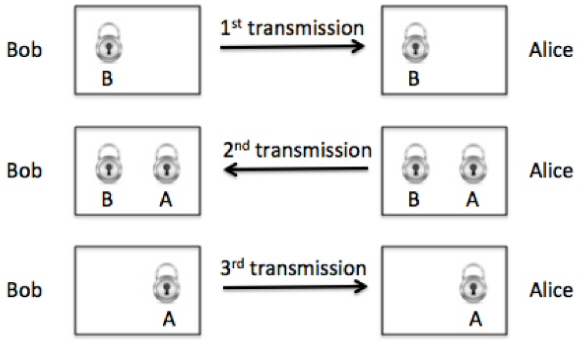

FIG. 1: The double padlock protocol of Kish and Sethuraman. Bob firstly locks the box and sends it to Alice. Then, once received, Alice also padlocks the box with a second lock and sends it back to Bob. Finally, Bob unlocks his padlock, and sends the box back to Alice who can then remove her lock, open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

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 com-

mutes. 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.

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, acted on by a rotor $R = \mathrm{e}^{\iota\phi/2}$ with $R^\dagger = \mathrm{e}^{-\iota\phi/2}$, giving a general rotation

$$\mathbf{m}' = R\mathbf{m}R^\dagger = \mathrm{e}^{\iota\phi/2}\mathbf{m}\mathrm{e}^{-\iota\phi/2} = \mathrm{e}^{\iota\phi}\mathbf{m}, \tag{1}$$

where $\mathbf{m}' = m_1' e_1 + m_2' e_2$ is the rotated vector, the bivector iota $\iota = e_1 e_2$ and where ϕ represents the private key and rotates the vector $\mathbf{m}$ by a clockwise angle ϕ in this case. We can combine the two sides of the rotation operator in this case because $\iota = e_1 e_2$ anticommutes with both e_1 and e_2 within the vector $\mathbf{m}$. 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

$$\mathbf{m}_{\text{final}} = R_A^\dagger R_B^\dagger R_A R_B \mathbf{m} = R_A^\dagger R_A R_B^\dagger R_B \mathbf{m} = \mathbf{m}, \tag{2}$$

where because the rotation operators commute 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.

However if one goes to higher dimensional rotations, might there be a subset of rotations that would still commute? If so, the double-padlock protocol may possibly work in higher dimensions, because the eavesdropper then has no way to discover both the amount of rotation and the rotation axis simultaneously. Before we explore this in the next section, we firstly consider more general operators using two-dimensional multivectors

$$M = a + \mathbf{v} + \iota b, \tag{3}$$

where a and b are scalars, ι is the bivector and $\mathbf{v} = v_1 e_1 + v_2 e_2$. 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

$$\mathbf{m}_{\text{final}} = M_A^\dagger M_B^\dagger M_A M_B \mathbf{m} M_B^\dagger M_A^\dagger M_B M_A, \tag{4}$$

however while the multivector operators now cannot be determined by an eavesdropper, we need to find multivectors that commute in order to return $\mathbf{m}_{\text{final}} = \mathbf{m}$. If we now seek M_A and M_B to commute, then we require $M_A M_B - M_B M_A = 0$ or

$$\begin{aligned}&(a + \mathbf{v} + \iota b)(c + \mathbf{w} + \iota d) - (c + \mathbf{w} + \iota d)(a + \mathbf{v} + \iota b)\\ &= 2\mathbf{v}\wedge\mathbf{w} - 2\iota d\mathbf{v} + 2\iota b\mathbf{w} = 0\end{aligned} \tag{5}$$

that allows a solution

$$M_A = 1 + v e_1 + \iota v\,,\; M_B = 1 + w e_1 + \iota w \tag{6}$$

where we have normalized the multivectors such that $M_A M_A^\dagger = M_B M_B^\dagger = 1$ with one degree of freedom after normalization. This is insufficient to ensure security of the two-dimensional message vector and so we need to seek a solution in higher dimensions.

In three dimensions, we have a message vector $\mathbf{m} = m_1 e_1 + m_2 e_2 + m_3 e_3$ and we have a general rotation

$$\mathbf{m}' = R\mathbf{m}R^\dagger = \mathrm{e}^{i\hat{\mathbf{v}}\phi/2}\mathbf{m}\mathrm{e}^{-i\hat{\mathbf{v}}\phi/2} \tag{7}$$

where $\hat{\mathbf{v}}$ is a unit vector representing a rotation axis about which a rotation of ϕ radians is applied. We also have defined the trivector $i = e_1 e_2 e_3$ that commutes with all variables with $i^2 = (e_1 e_2 e_3)^2 = -1$. Now, because the vectors $\mathbf{m}$ and $\mathbf{v}$ do not commute in general we cannot simplify this rotation operation as we did in two dimensions.

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

$$M_A = a + \mathbf{v} + i\mathbf{r} + ib\,,\; M_B = c + \mathbf{w} + i\mathbf{s} + id \tag{8}$$

where $\mathbf{v}$ and $\mathbf{r}$ 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 algorithm in Eq. (4), requiring

$$\begin{aligned}0 &= M_A M_B - M_B M_A\\ &= 2(\mathbf{v}\wedge\mathbf{w} - \mathbf{r}\wedge\mathbf{s}) + 2i(\mathbf{v}\wedge\mathbf{s} + \mathbf{r}\wedge\mathbf{w}),\end{aligned} \tag{9}$$

and to make this commutator vanish we can select $\mathbf{w} = \mathbf{v}\iota = \mathbf{v}ie_3$ and $\mathbf{s} = \mathbf{r}\iota = \mathbf{r}ie_3$, with the vectors now

planar in order to anticommute with e_3, so we define $\mathbf{v}_{12} = v_1 e_1 + v_2 e_2$. That is, we have the normalized commuting operators

$$\begin{aligned} M_A &= (a + \mathbf{v}_{12} + e_3\mathbf{v}_{12} + ib) = \mathrm{e}^{\mathbf{v}_{12}+e_3\mathbf{v}_{12}+i\phi_1} \\ M_B &= (b + \mathbf{p}_{12} + e_3\mathbf{p}_{12} + id) = \mathrm{e}^{\mathbf{p}_{12}+e_3\mathbf{p}_{12}+i\phi_2}, \end{aligned} \tag{10}$$

with the encrypted message for Alice, for example, given by

$$\mathbf{m}' = M_A \mathbf{m} M_A^\dagger. \tag{11}$$

Alice and Bob thus have private keys with three degrees of freedom available to encrypt the three component message vector.

Let us now explore if the scheme works in four dimensions. Penrose (2007) states: "In dimension higher than 3, it is not true that the composition of basic rotations about $(n-2)$-dimensional axes will always again be a rotation about an $(n-2)$-dimensional axis. In these higher dimensions, general (compositions of) rotations cannot be so simply described. Such a (generalized) rotation may have an axis (i.e. a space that is left undisturbed by the rotational motion) whose dimension can take a variety of different values. Thus, for a Clifford algebra in n dimensions, we need a hierarchy of different kinds of entity to represent such different kinds of rotation." [8]

In four dimensions we have the space of multivectors $\Re\oplus\Re^4\oplus\bigwedge^2\Re^4\oplus\bigwedge^3\Re^3\oplus\bigwedge^4\Re^4$, a sixteen-dimensional real vector space denoted by $Cl_{4,0}(\Re)$. We select a message vector $\mathbf{m} = m_1e_1 + m_2e_2 + m_3e_3 + m_4e_4$ and we define the quadvector $I = e_1e_2e_3e_4$ that anticommutes with all vectors and has a positive square, that is $I^2 = 1$. We once again now seek two four-dimensional multivectors M_A and M_B that commute in order to use the algorithm in Eq. (4). Now, requiring $M_AM_B = M_BM_A$, after some algebra detailed in the Appendix, we find several types of commuting multivectors, the simplest being

$$M_A = 1+\mathbf{v}+I\mathbf{v} = \mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\,,\; M_B = 1+\mathbf{p}+I\mathbf{p} = \mathrm{e}^{\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}, \tag{12}$$

where $\mathbf{v}, \mathbf{p}$ are four-vectors and $\hat{\mathbf{v}}, \hat{\mathbf{p}}$ are unit vectors that square to one. We thus have four degrees of freedom for the private keys for both Alice and Bob respectively. To confirm the commutativity of the first set we find

$$\begin{aligned} M_AM_B &= (1+\mathbf{v}+I\mathbf{v})(1+\mathbf{p}+I\mathbf{p}) \\ &= 1+\mathbf{p}+I\mathbf{p}+\mathbf{v}+\mathbf{vp}-I\mathbf{vp}+I\mathbf{v}+I\mathbf{vp}-\mathbf{vp} \\ &= 1+\mathbf{p}+I\mathbf{p}+\mathbf{v}+I\mathbf{v} \\ M_BM_A &= (1+\mathbf{p}+I\mathbf{p})(1+\mathbf{v}+I\mathbf{v}) \\ &= 1+\mathbf{p}+I\mathbf{p}+\mathbf{v}+I\mathbf{v}, \end{aligned} \tag{13}$$

thus confirming the commutativity. Hence following the encryption method in Eq. (4) using this set of operators we find

$$\begin{aligned} \mathbf{m}_{\text{final}} &= \mathrm{e}^{-\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{-\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathbf{m}\mathrm{e}^{-\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{-\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})} \\ &= \mathrm{e}^{-\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{-\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathbf{m}\mathrm{e}^{-\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{\phi_2(\hat{\mathbf{p}}+I\hat{\mathbf{p}})}\mathrm{e}^{-\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})}\mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})} \\ &= \mathbf{m}, \end{aligned}$$

thus accurately transmitting the message. Also $\mathbf{m}$ can become a full multivector M encrypted by the operators M_A and M_B. We have the encryption operation for Alice (and similarly for Bob)

$$M' = \mathrm{e}^{\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})} M \mathrm{e}^{-\phi_1(\hat{\mathbf{v}}+I\hat{\mathbf{v}})} \tag{14}$$

and so Eve needs to discover the private key $\mathbf{v}$ with four degrees of freedom, where M' and M are the intercepted intermediate messages, which in general is not soluble and thus intractable for Eve.

In this paper, for the first time, we provide a set of working mathematical operators for the Kish-Sethuraman (KS) cipher that is a classically secure protocol. Our solution requires the use of the space of Clifford multivectors, and we find a viable solution in three and four dimensional space.

Further exploration in higher dimensions may be of interest, though we have found a secure version in three and four dimensions.

The encoding of these multidimensional operations onto real signals 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 [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 we have developed 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 our mathematical protocol can be encoded on a wire-

less carrier or fiber optic signal, a benefit would be secure communication without key exchange and the promise of a relatively simple physical realization.

APPENDIX

Geometric algebra representation of vectors

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

$$e_1^2 = e_2^2 = e_3^2 = 1 \tag{15}$$

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 $e_1 e_2 = i e_3$.

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 [10], as assumed for an algebraic field, we find their product

$$\begin{aligned} \mathbf{ab} &= (a_1 e_1 + a_2 e_2 + a_3 e_3)(b_1 e_1 + b_2 e_2 + b_3 e_3) \\ &= a_1 b_1 + a_2 b_2 + a_3 b_3 + (a_2 b_3 - a_3 b_2) e_2 e_3 \\ &\quad + (a_3 b_1 - a_1 b_3) e_3 e_1 + (a_1 b_2 - a_2 b_1) e_1 e_2, \end{aligned} \tag{16}$$

where we have used the elementary properties of e_1, e_2, e_3 defined in Eq. (15). We recognize $a_1 b_1 + a_2 b_2 + a_3 b_3$ as the dot product and $(a_2 b_3 - a_3 b_2) e_2 e_3 + (a_3 b_1 - a_1 b_3) e_3 e_1 + (a_1 b_2 - a_2 b_1) e_1 e_2$ as the wedge product, so that we can write

$$\mathbf{ab} = \mathbf{a} \cdot \mathbf{b} + \mathbf{a} \wedge \mathbf{b}. \tag{17}$$

In three dimensions only, we can equate the wedge product to the cross product, giving $\mathbf{a} \wedge \mathbf{b} = i\mathbf{a} \times \mathbf{b}$. We can see from Eq. (16), 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

$$\mathbf{a}^{-1} = \frac{\mathbf{a}}{\mathbf{a}^2}. \tag{18}$$

These results can easily be adapted for a space of any number of dimensions.

Derivation of commuting operators in 4D

We can write a general multivector in four dimensions as

$$M = \mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y}) = x_4 + \mathbf{v} + e_4 \vec{x} - i\vec{y} + I\mathbf{w} - y_4 I \tag{19}$$

thus forming the complete set of scalar, vector, bivector, trivector and quadvector components, where $\vec{x}$ and $\vec{y}$ are three-vectors and $\mathbf{v}$, $\mathbf{w}$, $\mathbf{x}$, $\mathbf{y}$ are four vectors. The space of multivectors $\Re \oplus \Re^4 \oplus \bigwedge^2 \Re^4 \oplus \bigwedge^3 \Re^3 \oplus \bigwedge^4 \Re^4$ is a sixteen-dimensional real vector space denoted by $Cl_{4,0}(\Re)$ as shown in Eq. (19).

For two four dimensional multivector operators M_A and M_B we have the grade zero or scalar components, represented by the brackets $\langle\rangle_0$, given by

$$\begin{aligned} &\langle M_A M_B \rangle_0 \\ &= \langle (\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y}))(\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s})) \rangle_0 \\ &= \mathbf{v} \cdot \mathbf{p} - \mathbf{w} \cdot \mathbf{q} + \mathbf{x}' \cdot \mathbf{r} + \mathbf{y}' \cdot \mathbf{s} \\ &\langle M_B M_A \rangle_0 \\ &= \langle (\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s}))(\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y})) \rangle_0 \\ &= \mathbf{p} \cdot \mathbf{v} - \mathbf{q} \cdot \mathbf{w} + \mathbf{r}' \cdot \mathbf{x} + \mathbf{s}' \cdot \mathbf{y}, \end{aligned} \tag{20}$$

where $\mathbf{x}' = e_4 \mathbf{x} e_4 = -x_1 e_1 - x_2 e_2 - x_3 e_3 + x_4 e_4$ and so $\mathbf{x}' \cdot \mathbf{r} = \mathbf{x} \cdot \mathbf{r}'$. Now, because the dot product commutes, the scalar components of the product will commute as required. For the quadvector or grade four components we have

$$\begin{aligned} &\langle M_A M_B \rangle_4 \\ &= \langle (\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y}))(\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s})) \rangle_4 \\ &= -I\mathbf{v} \cdot \mathbf{q} + I\mathbf{w} \cdot \mathbf{p} - I\mathbf{x}' \cdot \mathbf{s} - I\mathbf{y}' \cdot \mathbf{r} \\ &\langle M_B M_A \rangle_4 \\ &= \langle (\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s}))(\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y})) \rangle_4 \\ &= I\mathbf{q} \cdot \mathbf{v} - I\mathbf{p} \cdot \mathbf{w} - I\mathbf{s} \cdot \mathbf{x}' - I\mathbf{r} \cdot \mathbf{y}'. \end{aligned} \tag{21}$$

In order to satisfy commutativity this requires

$$\mathbf{v} \cdot \mathbf{q} = \mathbf{w} \cdot \mathbf{p}. \tag{22}$$

For the bivector terms

$$\begin{aligned} &\langle M_A M_B \rangle_2 \\ &= \langle (\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y}))(\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s})) \rangle_2 \\ &= \mathbf{v} \wedge \mathbf{p} - I\mathbf{v} \wedge \mathbf{q} + I\mathbf{w} \wedge \mathbf{p} - \mathbf{w} \wedge \mathbf{q} \\ &+ \mathbf{x}' \wedge \mathbf{r} - I\mathbf{x}' \wedge \mathbf{s} - I\mathbf{y}' \wedge \mathbf{r} + \mathbf{y}' \wedge \mathbf{s} \\ &\langle M_B M_A \rangle_2 \\ &= \langle (\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s}))(\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y})) \rangle_2 \\ &= \mathbf{p} \wedge \mathbf{v} - I\mathbf{p} \wedge \mathbf{w} + I\mathbf{q} \wedge \mathbf{v} - \mathbf{q} \wedge \mathbf{w} \\ &+ \mathbf{r}' \wedge \mathbf{x} - I\mathbf{r}' \wedge \mathbf{y} - I\mathbf{s}' \wedge \mathbf{x} + \mathbf{s}' \wedge \mathbf{y}, \end{aligned} \tag{23}$$

which gives the condition

$$\mathbf{v} \wedge \mathbf{p} - \mathbf{w} \wedge \mathbf{q} - \vec{x} \wedge \vec{r} - \vec{y} \wedge \vec{s} + I\vec{x} \wedge \vec{s} + I\vec{y} \wedge \vec{r} = 0, \tag{24}$$

using the result that $\mathbf{x}' \wedge \mathbf{r} - \mathbf{r}' \wedge \mathbf{x} = -2\vec{x} \wedge \vec{r}$. For the vector components we find

$$\begin{aligned} &\langle M_A M_B \rangle_1 \\ &= \langle (\mathbf{v} + I\mathbf{w} + e_4 (\mathbf{x} + I\mathbf{y}))(\mathbf{p} + I\mathbf{q} + e_4 (\mathbf{r} + I\mathbf{s})) \rangle_1 \end{aligned} \tag{25}$$

$$
\begin{aligned}
&= e_4\mathbf{v}'\cdot\mathbf{r} + \langle e_4\mathbf{v}'\wedge\mathbf{r}\rangle_1 - i\vec{v}\wedge\vec{s} - i\vec{w}\wedge\vec{r} + e_4\mathbf{w}'\cdot\mathbf{s} \\
&+e_4\mathbf{x}\cdot\mathbf{p} + \langle e_4\mathbf{x}\wedge\mathbf{p}\rangle_1 + i\vec{x}\wedge\vec{q} - i\vec{y}\wedge\vec{p} - e_4\mathbf{y}\cdot\mathbf{q} \\
&\langle M_B M_A\rangle_1 \\
&= \langle(\mathbf{p} + I\mathbf{q} + e_4(\mathbf{r} + I\mathbf{s}))(\mathbf{v} + I\mathbf{w} + e_4(\mathbf{x} + I\mathbf{y}))\rangle_1 \\
&= e_4\mathbf{r}\cdot\mathbf{v} + \langle e_4\mathbf{r}\wedge\mathbf{v}\rangle_1 + i\vec{v}\wedge\vec{s} - i\vec{w}\wedge\vec{r} - e_4\mathbf{s}\cdot\mathbf{w} \\
&+e_4\mathbf{p}'\cdot\mathbf{x} + \langle e_4\mathbf{p}'\wedge\mathbf{x}\rangle_1 - i\vec{q}\wedge\vec{x} - i\vec{p}\wedge\vec{y} + e_4\mathbf{q}'\cdot\mathbf{y}.
\end{aligned}
$$

This produces the condition for commutativity $\langle M_A M_B\rangle_1 - \langle M_B M_A\rangle_1 = -e_4\vec{v}\cdot\vec{r} + v_4\vec{r} - i\vec{v}\wedge\vec{s} + e_4 w_4 s_4 + e_4\vec{x}\cdot\vec{p} - \vec{x}p_4 - i\vec{y}\wedge\vec{p} - e_4 y_4 q_4 = 0$. For the trivector terms

$$
\begin{aligned}
&\langle M_A M_B\rangle_3 \qquad (26)\\
&= \langle(\mathbf{v} + I\mathbf{w} + e_4(\mathbf{x} + I\mathbf{y}))(\mathbf{p} + I\mathbf{q} + e_4(\mathbf{r} + I\mathbf{s}))\rangle_3 \\
&= -e_4\vec{v}\wedge\vec{r} - i\mathbf{v}\cdot\mathbf{s} - \langle i\mathbf{v}\wedge\mathbf{s}\rangle_3 + i\mathbf{w}'\cdot\mathbf{r} + \langle i\mathbf{w}'\wedge\mathbf{r}\rangle_3 \\
&-e_4\vec{w}\wedge\vec{s} + e_4\vec{x}\wedge\vec{p} + i\mathbf{x}\cdot\mathbf{q} + \langle i\mathbf{x}\wedge\mathbf{q}\rangle_3 - i\mathbf{y}\cdot\mathbf{p} \\
&-\langle i\mathbf{y}\wedge\mathbf{p}\rangle_3 - e_4\vec{y}\wedge\vec{q} \\
&\langle M_B M_A\rangle_3 \\
&= \langle(\mathbf{p} + I\mathbf{q} + e_4(\mathbf{r} + I\mathbf{s}))(\mathbf{v} + I\mathbf{w} + e_4(\mathbf{x} + I\mathbf{y}))\rangle_3 \\
&= e_4\vec{r}\wedge\vec{v} - i\mathbf{s}\cdot\mathbf{v} - \langle i\mathbf{s}\wedge\mathbf{v}\rangle_3 + i\mathbf{r}\cdot\mathbf{w} + \langle i\mathbf{r}\wedge\mathbf{w}\rangle_3 \\
&-e_4\vec{s}\wedge\vec{w} - e_4\vec{p}\wedge\vec{x} + i\mathbf{q}'\cdot\mathbf{x} + \langle i\mathbf{q}'\wedge\mathbf{x}\rangle_3 - i\mathbf{p}\cdot\mathbf{y} \\
&-\langle i\mathbf{p}\wedge\mathbf{y}\rangle_3 - e_4\vec{q}\wedge\vec{y}.
\end{aligned}
$$

This produces the condition for commutativity $\langle M_A M_B\rangle_3 - \langle M_B M_A\rangle_3 = I\vec{v}s_4 - I\vec{s}v_4 - i\vec{w}\cdot\vec{r} + I\vec{r}w_4 - e_4\vec{w}\wedge\vec{s} + i\vec{x}\cdot\vec{q} - I\vec{x}q_4 + I\vec{y}p_4 - I\vec{p}y_4 - e_4\vec{y}\wedge\vec{q} = 0$.

From commutativity of the quadvector components we have the condition in Eq. (22) that firstly can have a solution $\mathbf{v} = \pm\mathbf{w}$ and $\mathbf{p} = \pm\mathbf{q}$. This then leaves the conditions for the bivectors from Eq. (24) as as $-\vec{x}\wedge\vec{r} - \vec{y}\wedge\vec{s} = 0$ and $I\vec{x}\wedge\vec{s} + I\vec{y}\wedge\vec{r} = 0$ that implies $\vec{x} = -\vec{y}$ and $\vec{r} = \vec{s}$. The vector and trivector conditions are then satisfied as well provided $\mathbf{x} = -\mathbf{v}' = -e_4\mathbf{v}e_4$ and $\mathbf{r} = \mathbf{p}$. This then gives two commuting multivectors

$$
\begin{aligned}
M_A &= a + \mathbf{v} + I\mathbf{v} - (\mathbf{v} + I\mathbf{v})e_4 = a + (\mathbf{v} + I\mathbf{v})(1 - e_4) \\
M_B &= c + \mathbf{p} + I\mathbf{p} + e_4(\mathbf{p} + I\mathbf{p}) = c + (1 + e_4)(\mathbf{p} + I\mathbf{p}).
\end{aligned}
$$

From the bivector condition, we could have selected the alternative $\mathbf{x} = \mathbf{y} = 0$, that also leads to commuting multivectors

$$
M_A = a + \mathbf{v} + I\mathbf{v}\,,\; M_B = c + \mathbf{p} + I\mathbf{p}. \qquad (27)
$$

Alternatively, beginning from Eq. (22), but selecting a solution with $\mathbf{q} = \mathbf{w} = 0$, we find the commuting operators

$$
N_A = b + e_4(\mathbf{x} - I\mathbf{x})\,,\; N_B = d + e_4(\mathbf{r} + I\mathbf{r}) \qquad (28)
$$

and we can indeed confirm the required property $M_A M_B = M_B M_A$ and $N_A N_B = N_B N_A$ through routine multiplication.

Inspecting the commuting operators in Eq. (27) we notice the use of the projection operators $P^+ = 1 + e_4$ and $P^- = 1 - e_4$, with $(P^+)^2 = 2P+$ and $P^+P^- = P^-P^+ = 0$. Hence we can identify two commuting operators

$$
M_A = a + (1+e_4)M_1(1-e_4)\,,\; M_B = b + (1+e_4)M_2(1-e_4) \qquad (29)
$$

where M_1 and M_2 are now two general four dimensional multivectors, as shown in Eq. (19) that can be used as the private keys by Alice and Bob.

* Electronic address: james.m.chappell@adelaide.edu.au

[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] R. Penrose, *The Road to Reality* (Jonathan Cape, London, 2004).

[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 Univ Pr, Cambridge, 2003).