QUANTUM ONE-WAY PERMUTATION OVER THE FINITE FIELD OF TWO ELEMENTS

ALEXANDRE DE CASTRO[1]

ABSTRACT. In quantum cryptography, a one-way permutation is a bounded unitary operator $U : \mathcal{H} \rightarrow \mathcal{H}$ on a Hilbert space $\mathcal{H}$ that is easy to compute on every input, but hard to invert given the image of a random input. Levin [Probl. Inf. Transm., vol. 39 (1): 92-103 (2003)] has conjectured that the unitary transformation $g(a,x) = (a, f(x) + ax)$, where f is any length-preserving function and $a, x \in GF_{2^{\|x\|}}$, is an information-theoretically secure operator within a polynomial factor. Here, we show that Levin's one-way permutation is provably secure because its output values are four maximally entangled two-qubit states, and whose probability of factoring them approaches zero faster than the multiplicative inverse of any positive polynomial $poly(x)$ over the Boolean ring of all subsets of x. Our results demonstrate through well-known theorems that existence of classical one-way functions implies existence of a universal quantum one-way permutation that cannot be inverted in subexponential time in the worst case. Keywords: quantum one-way permutation; CHSH inequality; controlled *NOT* gate; negligible probability; (pseudo)randomness.

1. INTRODUCTION.

One of the remarkable effects of (pseudo)randomness is breaking the symmetries inherent in many natural and artificial phenomena [1]. Because one-way permutations are quite heavily involved in the generation of (pseudo)randomness, they are seen as (pseudo)random generators themselves [2]. In the following, we will analyze Levin's construction [3] that addresses the existence of a specific one-way permutation, a one-to-one and onto mapping whose probability of security failure is negligible for a cryptographic key of arbitrary length. We will show that such a one-way permutation is a unitary operator that breaks its own symmetry, yielding a quantum cryptography protocol that is polynomially secure.

Preliminaries: Consider the Clauser-Horne-Shimony-Holt (CHSH) scenario [4], where two spatially separated parties labeled Alice and Bob can accept binary inputs $a, x \in \{0, 1\}$ and getting output bits $a', x' \in \{0, 1\}$. We can generate correlations between the output values and the input bits of a PR (Popescu-Rohrlich) box [5] from a stochastic mechanism which depends on the temporal order of the inputs [6, 7]. Suppose that the input a is the temporal parameter, a control bit so that a' occurs before x'. Then, for the group homomorphism $\{+1, -1, \times\} \mapsto \{0, 1, \oplus\}$ so that its inverse is also a group homomorphism, the condition $a' := 0$ and $x' := a \wedge x$ or $a' := 1$ and $x' := 1 \oplus a \wedge x$ produces the correlation $a' \oplus x' := a \wedge x$, where $\oplus$ is

[1]LABORATÓRIO DE MATEMÁTICA COMPUTACIONAL, CENTRO NACIONAL DE PESQUISA TECNOLÓGICA EM INFORMÁTICA PARA A AGRICULTURA (EMBRAPA INFORMÁTICA AGROPECUÁRIA), EMPRESA BRASILEIRA DE PESQUISA AGROPECUÁRIA, 13083-886 CAMPINAS-SP, BRAZIL

E-mail address: alexandre.castro@embrapa.br.

the addition modulo 2 (XOR) and the field's multiplication operation ($\times$) corresponds to the logical AND function (Eq. 1). This mapping between two isomorphic groups can be written as a 2-ary (total) function $g : (a, x) \mapsto [a':= a, x':= (f \in \{0, 1\}) \oplus a \wedge x]$ defined for all possible input values, so that the communication system yields the PR correlation characterized by the following (conditional) probability distribution:

(1)
$$\mathcal{P}r(a, x/a', x') = \begin{cases} 1/2, & a' \oplus x' := a \wedge x \\ 0, & otherwise \end{cases}$$

whence, the input state of g can only be guessed with negligible probability from its output state.

1.1. **Definition.** Let $g : \{0, 1\}^* \to \{0, 1\}^*$ be a length-preserving 2-ary total function that is easy to compute on every input but hard to invert given the image of a random input [8, 9]. The function g is called strongly one way if and only if the probability $\mathcal{P}r$ of inverting g is negligible (Eq. 2). $\mathcal{P}r$ is negligible if it approaches zero faster than the multiplicative inverse of any positive polynomial:

(2)
$$\mathcal{P}r_{\mathcal{A}(g) \in g^{-1}g} \in \mathcal{O}(1/poly),$$

where $\mathcal{A}$ is any probabilistic polynomial time algorithm [10]. In other words, a bad event that occurs with negligible probability $\mathcal{P}r_{g^{-1}g \leftarrow g} < 1/poly$ would be highly unlikely to occur even if we repeated the experiment polynomially many times. Otherwise, a function is called weakly one way if $\mathcal{P}r_{g^{-1}g \leftarrow g} > 1/poly$, i.e., if an event that occurs with noticeable probability occurs almost always when the experiment is repeated a polynomial number of times.

1.1.1. *Remark.* Inputs of $g(a, x) = (a, f(x) + ax)$ have ≤ 1 siblings on average for any length-preserving f and $a, x \in GF_{2^{\|x\|}}$ (see in [3]):

   i) The function f is length preserving if for every $x \in \{0, 1\}^*$ it holds that the length of the input is the same as the length of the output.

   ii) The output $f(x) + ax$, where a is a key bit, can be replaced by another hash function, a function that is used to map data of arbitrary sizes to data of fixed sizes.

   iii) $\|x\| = length(x)$, and GF_2 is the Galois Field of two elements.

1.1.2. *Conjecture.* The above g is one way, for any OWF (one-way function) f, and has the same (within a polynomial factor) security (see in [3]):

   i) This security scheme is provably secure if the probability of inverting g grows asymptotically no faster than the multiplicative inverse of any positive polynomial $p(x)$ for all large enough $\|x\|$.

   ii) The polynomial $p(x)$ is positive over $GF_{2^{\|x\|}}$ if $p(x) > 0$ for every $x \in GF_{2^{\|x\|}}$.

2. PROOF.

   The function $g(a, x)$ with $a, x \in GF_{2^{\|x\|}}$ is known as the universal one-way function. The question of whether one-way functions exist can be reduced to the question of whether this specific permutation is one way [11].

2.1. Definition. Given a permutation of n elements $g : \{1, ..., n\} \rightarrow \{1, ..., n\}$, its permutation matrix is a square binary (orthogonal) matrix which has exactly one entry of 1 in each row and each column and $0's$ elsewhere. Its elements are $(n = \|x\|)$-bit arrays that can be represented as polynomials over the Galois fields $GF_{2^{\|x\|}}$ [12].

2.1.1. *Remark.* For constructing a Galois extension of GF_2, e.g., the finite field $GF_{2^{length=3}}$ that represents the coordinates of the vertices defining a three-dimensional hypercube in which the sides are one unit in length, we need to choose an irreducible polynomial of degree 3 [13, 14].

Let the Table 1 below be the polynomial arithmetic modulo $x^3 \oplus x \oplus 1$. Over the finite field with characteristic 2 (1+1=0), the field's multiplication operation corresponds to the logical AND gate, and the field's addition operation corresponds to the logical XOR gate. Hence, $g(a, x) = (a, f(x) \oplus (a \wedge x))$, and:

i) For *sibling* $= 1$ (even input), $x = a$ implies that $f(x) = x[(I(x)]$; consequently, $g(a, x) = (a, x^2 \oplus x)$ because $x = x^2$ over the finite field with characteristic 2 (see Table 1).

ii) For *sibling* < 1 (odd input), $x \neq a$ implies that $f(x) = x^2 \oplus 1[NOT(x)]$; consequently, $g(a, x) = (a, x^2 \oplus x \oplus 1)$ because $x \oplus 1 = x^2 \oplus 1$ over the finite field with characteristic 2 (see Table 1).

Note that $x^2 \oplus x \oplus 1 > 0$ and $x^2 \oplus x < 1$ for $x = \{0, 1\}$.

Thus,

$$g(0,0) = (0,0) \Rightarrow \begin{bmatrix} g_{11} & g_{12} & g_{13} & g_{14} \\ g_{21} & g_{22} & g_{23} & g_{24} \\ g_{31} & g_{32} & g_{33} & g_{34} \\ g_{41} & g_{42} & g_{43} & g_{44} \end{bmatrix} \times \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \therefore \begin{bmatrix} g_{11} \\ g_{21} \\ g_{31} \\ g_{41} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

and

$$g(1,0) = (1,1) \Rightarrow \begin{bmatrix} 1 & 0 & g_{13} & g_{14} \\ 0 & 1 & g_{23} & g_{24} \\ 0 & 0 & g_{33} & g_{34} \\ 0 & 0 & g_{43} & g_{44} \end{bmatrix} \times \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \therefore \begin{bmatrix} g_{13} \\ g_{23} \\ g_{33} \\ g_{43} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}.$$

as $g_{22} = 1$ and $g_{12} = g_{32} = g_{42} = 0$ for $g(0,1) = (0,1)$. In the same way, for $g(1,1) = (1,0)$, $g_{34} = 1$ and $g_{14} = g_{24} = g_{34} = 0$.

Table 1. Logical operator precedence. For $a = NOT(x)$, $g(a, x) = (a, (x^2 \oplus 1) \oplus ((x^2 \oplus 1) \wedge x^2))$. Otherwise, $g(a, x) = (a, x \oplus (x \wedge x))$.

		000	001	010	011	100	101	110	111
	(AND)	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
011	$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	x^2+1	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+1	x^2	$x+1$

	000	001	010	011	100	101	110	111
(XOR)	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
000	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
001	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
010	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
011	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
100	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
101	x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
110	x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
111	x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Therefore, the function g is represented by the permutation matrix:

	$(a, x^2 \oplus x)$	$(a, x^2 \oplus x \oplus 1)$	$(a, x^2 \oplus x)$	$(a, x^2 \oplus x \oplus 1)$
$g_{(a<1,x=a)}$	1	0	0	0
$g_{(a<1,x>a)}$	0	1	0	0
$g_{(a>0,x<a)}$	0	0	0	1
$g_{(a>0,x=a)}$	0	0	1	0

where the four columns correspond to the orthogonal basis $|00\rangle$, $|01\rangle$, $|11\rangle$, $|10\rangle$ of the Hilbert space $\mathcal{H}_4$.

This covariance matrix form of standardized random variables denotes taht the average over the possible outcomes of all measurements may take on together according to the conditional joint probability distribution. Such a matrix form of total 2-ary unitary operator g is the controlled NOT ($CNOT$) function, a two-qubit universal quantum gate defined for all possible input values, where a is the control variable and x is the target variable.

Notice that for $a = x$, $CNOT|a\rangle\otimes|x\rangle \mapsto |a\rangle\otimes|x^2\oplus x\rangle$ and, for $a \neq x$, $CNOT|a\rangle\otimes|x\rangle \mapsto |a\rangle\otimes|x^2\oplus x\oplus 1\rangle$, where the hashing $x^2\oplus x\oplus 1 = NOT(x^2\oplus x)$, with $x = \{0,1\}$. The controlled NOT gate acts on two qubits, and applies the NOT gate $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ to the target qubit $|x\rangle$ if the first (control) qubit, $|a\rangle$, is in state $|1\rangle$. Otherwise, it applies the identity gate $= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ if the the first qubit is in state $|0\rangle$.

Considering the PR correlation given in Eq. 1, the 2-ary (total) function g can be written as $CNOT(a, x) = (a', x')$, with $x' = \begin{cases} a \wedge x & \text{, if } a = 0 \\ 1 \oplus a \wedge x & \text{, if } a = 1 \end{cases}$

Thus, $CNOT$ gate is completely specified by its truth table for $0 \sim +1$ and $1 \sim -1$:
whence, $NOT \begin{pmatrix} +1 \\ -1 \end{pmatrix} = \begin{pmatrix} -1 \\ +1 \end{pmatrix}$.

2.2. **Theorem.** Let $(\Omega, \mathcal{F}, \mathcal{P}r)$ be a Kolmogorov probability space with sample space Ω, event space $\mathcal{F}$, and probability measure $\mathcal{P}r$. Let a, x be random variables; hence, the Clauser-Horne-Shimony-Holt (CHSH) inequality for correlations $|\langle \cdot \rangle_{(0,0)} + \langle \cdot \rangle_{(0,1)} + \langle \cdot \rangle_{(1,0)} - \langle \cdot \rangle_{(1,1)}| \leq 2$ holds in the Kolmogorov axiomatization [15], where $\langle \cdot \rangle_{(a,x\in GF_2)}$ denotes the expectation values for $x^2 \oplus x$ and $x^2 \oplus x \oplus 1$.

	Input/Output	Input/Output
Target $= 0$	$\lvert 0\rangle\lvert 0\rangle \mapsto \lvert +1\rangle\lvert +1\rangle$	$\lvert 1\rangle\lvert 0\rangle \mapsto \lvert -1\rangle\lvert -1\rangle$
Target $= 1$	$\lvert 0\rangle\lvert 1\rangle \mapsto \lvert +1\rangle\lvert -1\rangle$	$\lvert 1\rangle\lvert 1\rangle \mapsto \lvert -1\rangle\lvert +1\rangle$
	Control $= 0$	Control $= 1$

Thus, $\lvert \langle x^2 \oplus x\rangle^H_{(0,0)} + \langle x^2 \oplus x \oplus 1\rangle^H_{(0,1)} + \langle x^2 \oplus x \oplus 1\rangle^H_{(1,0)} - \langle x^2 \oplus x\rangle^H_{(1,1)}\rvert \leq 2$, measured on the Hadamard basis $H = \{\lvert+\rangle, \lvert-\rangle\}$ (see Eq. 3). Therefore, the hidden (Markov) model, $\lvert \langle x^2 \oplus x \oplus 1\rangle^H_{x=\{0,1\}}\rvert \leq 1$, is the normalized upper bound to the correlation $[x \oplus NOT(x)]_{x=\{0,1\}}$ between two outcomes of the experiment (see Fig.1, below). For this symmetric function, the variable $x = \{0,1\}$ (input state) is not directly visible, since 0 and 1 are equiprobable. However, the output dependent on the input state $x = \{0,1\}$ is visible. According to reasoning assuming local hidden variable theory [16], the correlation measure cannot exceed the value 2, but there are four states of two qubits which lead to the maximal value of $2\sqrt{2}$.
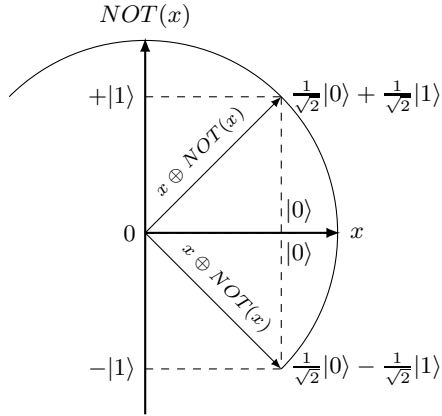

NOT(x)

$+\lvert 1\rangle$ ⟶ $\frac{1}{\sqrt{2}}\lvert 0\rangle + \frac{1}{\sqrt{2}}\lvert 1\rangle$

$x \otimes NOT(x)$

$\lvert 0\rangle$

0 ⟶ x

$\lvert 0\rangle$

$x \otimes NOT(x)$

$-\lvert 1\rangle$ ⟶ $\frac{1}{\sqrt{2}}\lvert 0\rangle - \frac{1}{\sqrt{2}}\lvert 1\rangle$

Fig.1. The absolute value of the symmetric difference $-1 \leq \langle x \oplus NOT(x)\rangle^H_{x=\{0,1\}} \leq +1$ is the normalized Euclidean metric from the point in two-dimensional rectangular space $\left[\lvert 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\right] \oplus \left[\lvert 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\right] = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ to the origin of the Cartesian coordinate system of the complex plane. In the Argand diagram, one can see that $[x \oplus NOT(x)]_{x=\{0,1\}}$ and its complex conjugate has the same absolute value. Hence, $\lvert \langle x^2 \oplus x \oplus 1\rangle^H_{x=\{0,1\}}\rvert \leq 1$, where NOT logic gate can be simulated by addition (modulo 2) operation, $NOT(x) = x^2 \oplus 1$, with $x \in GF_{2^{\lvert\lvert x\rvert\rvert}}$. Namely, one quantum bit can contain at most one classical bit of information, which is in accordance with the Holevo bound [17].

2.2.1. *Remark.* Let the controlled NOT function be $CNOT(\lvert a\rangle \otimes \lvert x\rangle) \mapsto \lvert a\rangle \otimes \lvert a \oplus x\rangle$, with the output values $\{+1,-1\}$ and its inputs, $\{0,1\}$, so that $0 \sim +1$ and $1 \sim -1$. The correlations $[x^2 \oplus x]_{x=\{0,1\}}$ and $[x^2 \oplus x \oplus 1]_{x=\{0,1\}}$ are used to realize the Bell states, and their conjugates, $\Phi^\pm$ and $\Psi^\pm$.

Consider the Hadamard basis $\{\lvert+\rangle, \lvert-\rangle\}$ of a one-qubit register given by the size-2 (discrete Fourier transform) DFT $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \lvert x\rangle_{x=\{0,1\}}$:

(3) $$\lvert x\rangle_{x=0,1} \xrightarrow{H} \frac{1}{\sqrt{2}}[(-1)^x \lvert x\rangle + \lvert 1 - x\rangle].$$

The following quantum circuits, $QXOR(x^H, I(x))$ and $QXOR(x^H, NOT(x))$, evolve the four inputs, $|a\rangle|x\rangle$ for $a, x = \{0, 1\}$, into the four entangled states of two qubits:

i) For $|x\rangle = |a\rangle$, and $x^2 = x$ over $GF_{2^{||x||}}$, we have:

$$QXOR[\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |0\rangle] = \tfrac{1}{\sqrt{2}}|0\rangle|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle|1\rangle = |\Phi^+\rangle.$$

$$QXOR[\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle), |1\rangle] = \tfrac{1}{\sqrt{2}}|0\rangle|1\rangle - \tfrac{1}{\sqrt{2}}|1\rangle|0\rangle = |\Psi^-\rangle.$$

ii) For $|x\rangle \neq |a\rangle$, and $x^2 \oplus 1 = x \oplus 1$ over $GF_{2^{||x||}}$, we have:

$$QXOR[\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle] = \tfrac{1}{\sqrt{2}}|0\rangle|1\rangle + \tfrac{1}{\sqrt{2}}|1\rangle|0\rangle = |\Psi^+\rangle.$$

$$QXOR[\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle), |0\rangle] = \tfrac{1}{\sqrt{2}}|0\rangle|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle|1\rangle = |\Phi^-\rangle.$$

This simple network applies the Hadamard gate given by Eq. 3 to the first wire and XORs the randomized first wire into the second wire yielding the maximally entangled states $|\Phi^\pm\rangle = (|0\rangle \pm |1\rangle)QXOR|0\rangle = QXOR(|0\rangle \pm |1\rangle), |0\rangle) = QXOR(|0\rangle, |0\rangle) \pm QXOR(|1\rangle, |0\rangle)$ and $|\Psi^\pm\rangle = (|0\rangle \pm |1\rangle)QXOR|1\rangle = QXOR(|0\rangle \pm |1\rangle), |1\rangle) = QXOR(|0\rangle, |1\rangle) \pm QXOR(|1\rangle, |1\rangle)$, where the normalization constant is omitted. The quantum exclusive OR operation ($QXOR$) corresponds to $CNOT$ gate that flips the second (target) qubit if the first (control) qubit is $|1\rangle$ and does nothing if the control qubit is $|0\rangle$.

Let $\Psi^+ = ||\Psi^+\rangle|$ and $\Phi^- = ||\Phi^-\rangle|$ be the expectations of the correlations $[x \oplus NOT(x)]_{x=\{0,1\}}$, after the quantum circuit to perform a Hadamard transform followed by controlled NOT gate on the input values. From the sum of Ψ^+ and Φ^-, we can write down the set of four correlations in the experiment:

$$[x \oplus NOT(x)]_{x=0} \xrightarrow{H-CNOT} \tfrac{1}{\sqrt{2}}||01\rangle + |10\rangle| \qquad\qquad (+)$$

$$\underline{[x \oplus NOT(x)]_{x=1} \xrightarrow{H-CNOT} \tfrac{1}{\sqrt{2}}||00\rangle - |11\rangle|}$$

$$2[x \oplus NOT(x)]_{x=\{0,1\}} \xrightarrow{H-CNOT} \tfrac{1}{\sqrt{2}}||01\rangle + |10\rangle| + \tfrac{1}{\sqrt{2}}||00\rangle - |11\rangle| \quad (=)$$

whence, $\langle x \oplus NOT(x)\rangle_{x=\{0,1\}}^{H-CNOT} \geq \tfrac{1}{2\sqrt{2}}||00\rangle + |10\rangle| + |10\rangle - |11\rangle|$, once by subadditivity property (triangle inequality), $||00\rangle + |10\rangle| + |10\rangle - |11\rangle| \leq ||01\rangle + |10\rangle| + ||00\rangle - |11\rangle|$. As $x \oplus NOT(x) = 1$ for $x \in GF_{2^{||x||}}$, we have that the sum of correlations is $S \leq 2\sqrt{2}$, where $S = ||00\rangle + |01\rangle + |10\rangle - |11\rangle|$ on the Hadamard basis $H = \{|+\rangle, |-\rangle\}$. Thus, the mathematical formalism shows that quantum correlations go up to Tsirelson's bound of the CHSH inequality.

Notice that the exclusive disjunction $x \oplus NOT(x) = x^2 \oplus x \oplus 1$ is the polynomial representation of the power set $\mathcal{F}^\Omega$ of the universal set $\Omega = \{x', x'', x'''\}$. Its subsets are $\{\} := 0$, $\{x'\} := x^2$, $\{x''\} := x$, $\{x'''\} := 1$, $\{x', x''\} := x^2 \oplus x$, $\{x', x'''\} := x^2 \oplus 1$, $\{x'', x'''\} := x \oplus 1$ and $\{x', x'', x'''\} := x^2 \oplus x \oplus 1$, namely the Cartesian coordinates of the Euclidean space $\mathbb{R}^3$.

The set of the subsets of the $\mathcal{F}^\Omega$ ordered by inclusion composes a poset – a partially ordered set in which binary relations as $\leq$ hold for some pairs of elements of the set, but not for all –, where the irreducible polynomial $x^2 \oplus x \oplus 1$ over $GF_{2^{||x||}}$ dependents on itself for its existence. In this ontological dependency defined on the three-dimensional space model of the physical universe[1], the basis elements of a bigger Hibert space $\mathcal{H}_0$, which is a superset of the conventional Hibert space $\mathcal{H}$, evolve into basis elements [18] in accordance with the Hasse diagram shown in Fig.2. Consequently, asymptotic behaviour is associated with $\mathcal{F}^\Omega$, once the universal set is large enough.

[1] Verify that $x^x \oplus x \oplus 1$ is the universal set (of everything) in the computational knowledge engine https://www.wolframalpha.com/input/?i=(x+and+x)+xor+x+xor+1. Verify also that $NOT(x^2 \oplus x \oplus 1) = x^2 \oplus x$ is the empty set $\{\emptyset\}$ in https://www.wolframalpha.com/input/?i=(x+and+x)+xor+x. Another interesting point about the polynomial $x^2 \oplus x \oplus 1$ can be seen in [21].
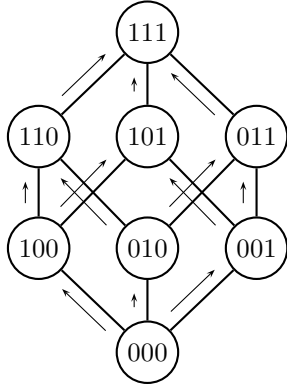
Fig.2. Ontology chart [19, 20](Hasse diagram) of the partially ordered set of all subsets of $\{x', x'', x'''\}$. The subsets $\{\} = (000)$, $\{x'\} = (100)$, $\{x''\}$, $\{x'''\} = (001)$, $\{x', x''\} = (110)$, $\{x', x'''\} = (101)$, $\{x'', x'''\} = (011)$ and $\{x', x'', x'''\} = (111)$ are basis elements that evolve into $\{x', x'', x'''\}$, and represent the coordinates of the vertices defining a 3-D hypercube. By the Cantor's first uncountability proof, such an Euclidean space has the same cardinality of the unit interval $[0, 1]$. The segment $[0, 1]$ is a subset of $\mathbb{R}$, and it has the cardinality of the continuum. Therefore, the edge of the 3-D hypercube whose side has length one unit is equal to the cube root of its volume $\sqrt[3]{1} = \begin{cases} 1 \\ -1/2 \pm i\sqrt{3}/2 \end{cases}$, where the Galois conjugates $-1/2 \pm i\sqrt{3}/2$ are zeros of the minimal polynomial $poly(x)$. Every minimal polynomial is irreducible over $GF_{2^{||x||}}$.

2.2.2. *Remark.* Measuring the first bit of the pairs $|\Psi^+\rangle$ and $|\Phi^-\rangle$ in the computational basis yields a 0 or 1 with probability $1/2$. Likewise, measuring its second bit yields the same outcome with the same probability. Therefore, measuring one bit of the maximally entangled two-qubit Bell states yields a random outcome. Hence, we can rewrite the EPR pairs $|\langle x^2 \oplus x \oplus 1\rangle^H_{x=\{0,1\}}| \leq 1$ as a Markov's inequality $poly(x)\mathcal{P}r_{poly(x)=0,1} \leq \langle x^2 \oplus x \oplus 1\rangle_{GF_{2^{||x||}}}$, where the sample space $poly(x) = |x^2 \oplus x \oplus 1|$ is the indicator random variable $1_{\mathcal{F}} : \Omega \mapsto \mathbb{R}$ defined by $1_{\mathcal{F}}(x) = 1$ if $x \in \mathcal{F}^\Omega$, otherwise, $1_{\mathcal{F}}(x) = 0$. The measure $\mathcal{P}r_{poly(x)=0,1}$ is the probability of factoring, $\mathcal{P}r_{poly(x)=0}$, or non-factoring, $\mathcal{P}r_{poly(x)=1}$, the Bell states $|\Psi^+\rangle$ and $|\Phi^-\rangle$ generated by $QXOR(x^H, NOT(x))$. Recall that the polynomial $poly(x)$ is factorable over $GF_{2^{||x||}}$ if $poly(x) = u(x)v(x)$ with both non-constant polynomials $u(x)$ and $v(x) \in GF_{2^{||x||}}$, otherwise, $poly(x)$ is irreducible. If the degree of $poly(x)$ is 2, then $poly(x)$ is a non-factorable polynomial over the finite field $GF_{2^{||x||}=3}$ if and only if $p(x)$ has no root in $GF_{2^{||x||}=3}$, i.e., $poly(x) = 1$ for $x = \{0, 1\}$.

For the sake of simplicity, from now on, we will replace $\oplus \mapsto (+)$, and will use $\oplus$ only where strictly necessary to ensure the coherence of the operation. The notation will also be simplified, once the computational basis and Hadamard basis are isomorphic.

2.3. **Theorem.** The probability of factoring $poly(x)$, $\mathcal{P}r_{poly(x)=0}$, is negligible if and only if the product $poly(x)\mathcal{P}r_{poly(x)=0}$ approaches 0 asymptotically for any positive polynomial $poly(x) > 0$. (See a proof of this theorem for negligible functions in [10]).

2.3.1. *Remark.* Any positive polynomial over $GF_{2^{||x||}}$ is reduced to the irreducible polynomial $poly(x) = x^2 \oplus x \oplus 1 > 0$. Thus, $poly(x)$ is almost surely non-factorable, since the probability of non-reducing it, $\mathcal{P}r_{poly(x)=1}$, is equal to one.

Let the factorization of $poly(x)$ be a tail event $E \in \mathcal{F}$ in the probability space $(\Omega, \mathcal{F}, \mathcal{P}r)$ that happens almost surely if $\mathcal{P}r[E] = 1$. Equivalently, E occurs almost surely if the probability of E not occurring is $\mathcal{P}r[E^c] = 0$, where E^c is the complementary event (Kolmogorov's zero–one law, see proof in [22]).

Consequently, $poly(x)\mathcal{P}r_{poly(x)=0} < 1$, because the probability of factoring $poly(x)$ vanishes for $x = \{0, 1\}$. As a result, $\mathcal{P}r_{poly(x)=0}$ is negligible, once it approaches

0 quickly as $\mathcal{P}r_{poly(x)=0} < \frac{1}{poly(x)}$, where $poly(x) = x^2 + x + 1 > 0$ and the field's addition operation $(+)$ corresponds to the exclusive OR logical operation $(\oplus)$ given the random input $x = \{0,1\}$. Notice that we can map the elements of the Hadamard basis to the computational basis using the group homomorphism $\{+1, -1, \times\} \mapsto \{0, 1, \oplus\}$ so that its inverse is also a group homomorphism. Then, the exclusive disjunction $x \oplus NOT(x) = x^2 \oplus x \oplus 1$ can be rewritten as $x^2 \oplus x \oplus 1 := l' \wedge \neg l''$, once the field's multiplication operation corresponds to the logical AND operation over the field of two elements. It is not difficult to see that for $l' = l'' = l'''$, $l' \wedge \neg l' = (l' \vee l'' \vee l''') \wedge (\neg l' \vee \neg l'' \vee \neg l''')$ can be written as 3CNF (conjunctive normal form) clauses, $(l' \vee l'' \vee l''') \wedge (l' \vee l'' \vee \neg l''') \wedge (l' \vee \neg l'' \vee l''') \wedge (l' \vee \neg l'' \vee \neg l''') \wedge (\neg l' \vee l'' \vee l''') \wedge (\neg l' \vee l'' \vee \neg l''') \wedge (\neg l' \vee \neg l'' \vee l''') \wedge (\neg l' \vee \neg l'' \vee \neg l''')$, which is unsatisfiable. As a result, factoring the polynomial $poly(x)$ over $GF_{2^{||x||=3}}$ is as hard as solving the Boolean satisfiability problem (SAT): the variables of the Boolean formula above can be consistently replaced by the values TRUE or FALSE in such a way that the formula evaluates to TRUE?

Try this Fortran code to see:

```
PROGRAM RANDOM
        LOGICAL x,y,z
        y = .NOT. x
        z = .TRUE.
        x .neqv. y = z
WRITE(*,*) x
END
```

Is there another programming language able to solve this problem?

There is no deterministic way even if we repeat the experiment polynomially many times, since $\mathcal{P}r_{poly(x)=0}$ is negligible over the Boolean ring of all subsets of x.

2.3.2. *Remark.* The question above can directly be replaced by the problem of whether $poly(x) > 0$ with any reasonable probability distribution on its inputs can be factored in polynomial time on average. [23, 24, 25].

Time complexity analysis: Let the bigger Hilbert space $\mathcal{H}_0 \supseteq \mathcal{H}$ be the same size as the set of all subsets. $\mathcal{H}_0$ has the cardinality of the continuum; therefore, the (discrete) distribution $^1/_{poly(x)}$ over GF_2, where every element[2] $x = -x$, converges to the bell-shaped (continuous) curve of the probability density function of the Cauchy distribution (its left tail is shown in Fig.3), with integral principal value (P.V.) equal to $^1/_2$ and probability $\mathcal{P}r_{x \in \mathcal{F}^\Omega}$ given by

$$(4) \qquad \frac{1}{N} \int_{-\infty}^{+\infty} \frac{1}{poly(x)} dx = 1,$$

where the normalizing constant $N = 2\pi\sqrt{^1/_3}$.

---

[2]The unitary operator $NOT^2(x) = I(x)$: $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Thus $(x^2 + 1)^2 = x^2$, hence, $x^2 + 1 = \pm x$, and we have $poly(x) = x^2 + x + 1$ or $poly(x = -x) = x^2 - x + 1$, once every element $x = x^2$ of GF_2 satisfies the property $x \oplus x = 0$.

$PDF's$

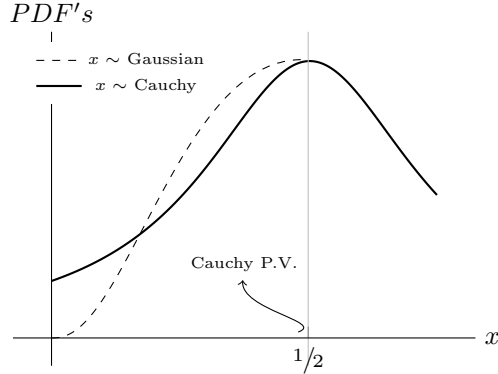- - - $x \sim$ Gaussian
—— $x \sim$ Cauchy

Cauchy P.V.

x

$1/2$

Fig.3. The probability density function of the Cauchy distribution (Eq. 4) can be written as

$$PDF_{Cauchy} = \frac{1}{\pi} \frac{\alpha}{(x - \mu)^2 + \alpha^2},$$

where α is the half width at half maximum and μ is the statistical median. PDF_{Cauchy} is similar in appearance to Gaussian curve, however, the values for away from P.V. are much more likely than they would be with a Normal distribution since its tails drop off much more slowly.

As the sample space is large enough and the input x is a Cauchy-distributed random variable, the polynomial $x^2 + x + 1 > 0$, with $x \in GF_{2^{||x||}}$, is asymptotically almost surely a hard core, once the presence of the heavy extreme values in the Cauchy distribution means that the average value does not converge to a fixed value. The Cauchy distribution is a heavy-tailed distribution belonging to the subexponential class whose probability density function decreases at a polynomial rate as $x \to -\infty$ and $x \to +\infty$, as opposed to an exponential rate. (The polynomial $x^2 + x + 1 = x + (x^2 + 1) \in GF_{2^{||x||}}$, where input x in $x^2 + 1$ is also a (standard) Cauchy-distributed random variable (Witch of Agnesi).

Consequently, the probability of factoring the predicate $poly(x) = x^2 + x + 1 > 0$ for $x = \{0, 1\}$ — which is identical to finding a way that 3CNFSAT evaluates to TRUE — is subexponentially bounded making the factorization of $poly(x)$ an NP-complete problem, which is in accordance with the exponential time hypothesis [26]. Thus, the running time $T(x)$ of any cryptanalysis algorithm to factorize $poly(x)$ on inputs of size $||x||$ grows faster than polynomial time, since 3CNFSAT cannot be decided in the subexponential class.

Considering that every exponential time algorithm takes longer than a subexponential time algorithm as $||x||$ increases, then, the running time of any algorithm to factorize $poly(x)$ is order of complexity $T(x) = 2^{\mathcal{O}(x)}$ in big $\mathcal{O}$-notation.

It is straightforward to see that the expectation of the squared deviation (variance) of the random variable x can be radically altered by the extremes of the Cauchy distribution. Hence, if the variance is unpredictable, the maximally entangled state $x^2 + x + 1 > 0 \in GF_{2^{||x||}}$ is asymptotically almost surely a hard-core predicate which is easy to compute given x, but is hard to compute x given its output of a single bit. This predicate (hidden Markov model) provides every one-way functions with a hidden bit of the same security. It yields a "perfect" random generator (PRG) with maximum entropy probability [27] from any one-way bijection, since the input x computed from the output can only be guessed with probability $1/2$. This maximum min-entropy — the smallest entropy measure in the family of Rényi's entropies — is a measure of how correlated the state $poly(x)$ is.

2.4. **Theorem.** Let one-to-one correspondence g be a function defined as $g(a, x) = (a, h(x))$, where the length of a is the same as that of x, and $h(x) = f(x) + ax$ over $GF_{2^{||x||}}$. The Boolean inner product $\langle a \oplus x \rangle_{a \neq x}$ provides a one-way function with a hidden bit of the same security. (See the proof of this theorem in [2, 10, 27, 28].

2.4.1. *Remark.* The hard-core predicate of g is the parity function of a random subset of the inputs of g. If g has a hard-core predicate $h(x)$, then it must be strongly one way. Hence, the probability of inverting g, $\mathcal{P}r_{g^{-1}g \leftarrow g}$, is the same probability of factoring the hard-core $h(x)$. Then, the probability of inverting g is negligible because the probability of factoring the maximally entangled state $h(x) = f(x) + ax = poly(x) \in GF_{2^{||x||}}$, with $x \neq a$, is less than $\frac{1}{x^2+x+1>0}$. Consequently, $\mathcal{P}r_{g^{-1}g \leftarrow g}$ approaches zero faster than $\frac{1}{poly(x)>0}$ given the random input $x = \{0,1\}$, where $poly(x) = x^2 \oplus x \oplus 1$ is the only positive polynomial[3] among the $2^3 = 8$ polynomials over $GF_{2^{||x||=3}}$.

2.5. **Theorem.** If $P \neq NP^4$, then, some strongly non-invertible functions are invertible (see proof in [29]).

2.5.1. *Corollary.* Let g be the controlled NOT gate, and its unitary (and Hermitian) matrix written in the form:

$$
(5) \qquad U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad U^2_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.
$$

The liner operator $U_{CNOT} = U^{-1}_{CNOT} = U^T_{CNOT}$ is orthogonal. Hence, g is involutory: a bijective map that is its own inverse, i.e., a mirror symmetry because when it is applied twice in succession, every state returns to its original value. A bijective function from a set to itself is a permutation [31].

2.5.2. *Remark.* It is straightforward to see that strongly non-invertible functions are invertible from the definition itself of one-way functions. (See a thermodynamic approach of one wayness [32] in input-saving machines [33, 34]).

Consider g defined on pairs of strings of the same length, so that $g(a,x) = (a, f(x) \oplus x)$ (pg. 94 in [10]).

Thus, it is self-evident that the functions

$$
(6) \qquad g = \begin{bmatrix} f(x)= I(x) & 0_2 \\ 0_2 & f(x)=NOT(x) \end{bmatrix}
$$

and $f(x)$ have information-theoretic security within the same polynomial factor.

Let the hard-core $h(x)$ in g be a permutation $f'(x) = f(x) \oplus x$, where f is any (length-preserving) one-way function. As the output of the XOR bitwise operation $f'(x) = f(x) \oplus x$ is true if and only if the inputs are not alike; otherwise, the output is false, $f(x)$ in Eq.6 can only be represented by the polynomials $f(x) = x$ $[I(x)]$ or $f(x) = x \oplus 1$ $[NOT(x)]$ over $GF_{2^{||x||}}$.

Let $GF_{2^{||x||}}$ a field and $f(x)$ a polynomial in $GF_{2^{||x||}}$. If $\deg[f(x)] = 1$, then, $f(x)$ is non-factorable over $GF_{2^{||x||}}$. This is obvious because the polynomial $f(x)$ is factorable over $GF_{2^{||x||}}$ if and only if $f(x) = u(x)v(x)$ with both non-constant polynomials $u(x)$ and $v(x)$. If $f(x) = u(x)v(x)$ for some $u(x), v(x) \in GF_{2^{||x||}}$,

---

[3]Evidently, any positive polynomial over $GF_{2^{||x||}}$ is reduced to $x^2 \oplus x \oplus 1$.

[4]The $P \overset{?}{=} NP$ problem is to determine whether every language accepted by some nondeterministic algorithm in polynomial time is also accepted by some (deterministic) algorithm in polynomial time [30]. $P \neq NP$ if and only if a total 2-ary one-way functions exists [8, 9].

then, $\deg[f(x)]=\deg[u(x)]+\deg[v(x)]$. However, $\deg[u(x)]+\deg[v(x)]$ are nonnegative integers over the integral domain $GF_{2^{||x||}}$, hence, one of the degrees must be 0. Thus, either $u(x)$ or $v(x)$ must be a constant polynomial. It follows that $f(x)$ is almost surely non-factorable[5] over $GF_{2^{||x||}}$. Hence, $f(x) = x$ or $f(x) = x \oplus 1$ are length-preserving one-way functions over $GF_{2^{||x||}}$, and any length-preserving one-way function over $GF_{2^{||x||}}$ is reduced to them. As a result, $f'(x) = x^2 \oplus x$ or $f'(x) = x^2 \oplus x \oplus 1$, where $x = x^2$ over $GF_{2^{||x||}}$.

Notice that the polynomial $x^2 \oplus x$ is factorable over $GF_{2^{||x||}}$ because it outputs 0 for $x = \{0,1\}$. Otherwise, the polynomial $x^2 \oplus x \oplus 1$ is almost surely non-factorable over $GF_{2^{||x||}}$ because the probability of factoring it is negligible. Consequently, $f'(x)$ is weakly one way for every even input and strongly one way for every input odd (see Remark 2.2.1). However, the polynomial $x^2 \oplus x \oplus 1 = (x^2 \oplus x) \oplus 1$ outputs 1 for $x = \{0,1\}$, then, by symmetry, $x^2 \oplus x = 1 \oplus 1$ yielding $x^2 \oplus x = 0$ for $x = \{0,1\}$. As a result, the exclusive disjunctions $x^2 \oplus x$ and $x^2 \oplus x \oplus 1$ are deducible from each other, since XOR operation is involutory. Therefore, every strongly one-way function is also weakly one way, once any positive polynomial over $GF_{2^{||x||}}$ and any polynomial zero over $GF_{2^{||x||}}$ is reduced to $x^2 \oplus x \oplus 1 = 1$ and $x^2 \oplus x = 0$ over $GF_{2^{||x||=3}}$, respectively. As there is a one-to-one correspondence between a complex number and its complex conjugate, the equipollence between the polynomials $x^2 \oplus x$ and $x^2 \oplus x \oplus 1$ is self-evident, since Bell states and its conjugates $|\phi^+\rangle/|\phi^-\rangle$ and $|\psi^-\rangle/|\phi^+\rangle$ are generated by $x^2 \oplus x$ and $x^2 \oplus x \oplus 1$, respectively (see detail in Remark 2.2.1).

Recall that the three-dimensional space $\{x', x'', x'''\}$ is represented by the Hasse diagram shown in Fig.2. In that ontological chart, a state is partially ordered with another state, where in every such pair of states we will label the first as *Alice* and the second as *Bob*. There are 2^3 possible combinations of such states given in the Table 2 below:

Table 2. Polynomial representation of the pairs *Alice* and *Bob*.

Alice		Bob		Probability
x'x''x'''	Polynomial	x'x''x'''	Polynomial	
111	$x^2 + x + 1$	000	0	$\mathcal{P}r^1$
110	$x^2 + x$	001	1	$\mathcal{P}r^2$
101	$x^2 + 1$	010	x	$\mathcal{P}r^3$
100	x^2	011	$x + 1$	$\mathcal{P}r^4$
011	$x + 1$	100	x^2	$\mathcal{P}r^5$
010	x	101	$x^2 + 1$	$\mathcal{P}r^6$
001	1	110	$x^2 + x$	$\mathcal{P}r^7$
000	0	111	$x^2 + x + 1$	$\mathcal{P}r^8$

where $\mathcal{P}r^i$, with $i = 1, ..., 8$, is the probability of a of a specific combination occurring in the sample space including all possible combinations. The bit arrays, *Alice* and

---

[5]The functions $I(x) = x \equiv x^2$ and $NOT(x) = x \oplus 1 \equiv x^2 \oplus 1$ hold. However, x and $x \oplus 1$ are irreducible (non-factorable), while x^2 and $x^2 \oplus 1$ are reducible (factorable) over $GF_{2^{||x||}}$. The probability density function $1/(x^2 + 1)$ is the Witch of Agnesi, a heavy-tailed distribution belonging to the subexponential class (see time complexity analysis in Remark 2.3.1), while the reciprocal random variable $1/x$ is an exponential random variable (exponential of the uniform random variable $x = \{0, 1\}$).

Bob, are polynomials $p_i(x) \in GF_{2^{||x||=3}} = \{0, 1\}$ (as shown in Table 1, Remark 2.1.1).

Taking into account the Sakurai's Bell inequality [38], we can have that $\mathcal{P}r^3 + \mathcal{P}r^4 \leq \mathcal{P}r^3 + \mathcal{P}r^4 + \mathcal{P}r^2 + \mathcal{P}r^7$ holds, where the probabilities are always nonnegative $\mathcal{P}r^i = |p_i(x)|$, with every polynomial $p_i(x) = \frac{\langle p_i(x) \rangle}{|x^2+x+1|}$. The polynomial $x^2 + x + 1$ is the powerset of all possible combinations over $GF_{2^{||x||=3}}$

Therefore, the modulo 2 arithmetic is (i) $|(x^2+1)+x^2| \leq |(x^2+1)+x^2+(x^2+1)+1|$ for *Alice*, and (ii) $|x+(x+1)| \leq |x+(x+1)+1+(x^2+x)|$ for her logical complement, *Bob*. By subadditivity, we have $|x^2+x+1| \leq |x^2+x|$ for both configurations, where $x = x^2$ over $GF_{2^{||x||}}$.

As the polynomials $x^2 + x + 1$ and $x^2 + x$ are logically deducible from each other over the finite field with characteristic 2, then, the inequality is reversed. Namely, $|x^2 + x| \leq |x^2 + x + 1|$ because $x^2 + x$ is ground set of $x^2 + x + 1$ in the partially ordered set $\{x', x'', x'''\}$.

Consider, now, the Cantor-Schröder-Bernstein theorem below:

Theorem: Given two sets $\mathcal{A}$ (*Alice*) and $\mathcal{B}$ (*Bob*). If t': $\mathcal{A} \rightarrow \mathcal{B}$ and t'': $\mathcal{B} \rightarrow \mathcal{A}$ are both injections, then, there exists a bijective function $\mathcal{A} \sim \mathcal{B}$ (see proof in [39, 40]).

Thus, $x^2 + x$ can be exchanged by $x^2 + x + 1$ so that $|x^2 + x + 1| \leq |x^2 + x + 1|$, since there is a one-to-one correspondence between the polynomials for $x = \{0, 1\}$ (they are equivalent). In fact, the powerset x^2+x+1 over $GF_{2^{||x||=3}}$ has cardinality strictly less than or equal to itself cardinality, as shown in Fig.2. Consequently, the multiplicative inverse $\frac{1}{poly(x)} \geq \frac{1}{poly(x)}$ holds, where $poly(x) = |x^2 + x + 1|$.

As $]0, 1[\subseteq \mathbb{R}$ and $[0, 1] \subseteq \mathbb{R}$ have the same cardinality, the multiplicative inverse $\frac{1}{poly(x)} < \frac{1}{poly(x)}$ for $x = \{0, 1\}$, obviously. This condition implies that the strongly one-way function $x^2+x+1 \in GF_{2^{||x||}}$ — polynomial whose (negligible) probability of factoring it approaches zero quickly — exists because the weakly one-way function $x^2 + x \in GF_{2^{||x||}}$ exists — polynomial whose (noticeable) probability of factoring it does not approach zero too quickly. The reverse is also true, since every strongly one-way function is also weakly one-way [29, 41]. Therefore, $x^2 + x$ is separable (classically correlated) because the probability of factoring it is not less than $\frac{1}{poly(x)}$. Otherwise, $x^2 + x + 1$ is entangled (or non-separable) because the probability of factoring it is not greater than $\frac{1}{poly(x)}$.

This multiplicative inverse polynomial distance between an entangled state and the separable set reduces the separability criterion in bidirectional quantum controlled schemes [35, 36, 37] to an NP-hard problem [42].

In accordance with Fig.1, the size-2 (discrete Fourier transform) DFT over the finite field with characteristic 2 generates the unit vector $|x + NOT(x)\rangle$ with coordinates $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ making a 45° angle with the axes in the plane. Hence, the probability amplitude (wave function) is equal to the reciprocal of $\sqrt{2}$ computed over $\mathbb{R}$. This number satisfies $\sin(45°)$, therefore, $[\sin(45°)]^2 = [\frac{1}{poly(x)}]^2$, where $poly(x) = |x^2 + x + 1|$. Consequently, the trigonometric inequality $\frac{1}{2}[\frac{1}{poly(x)}]^2 \leq \frac{1}{2}[\sin(22.5°)]^2 + \frac{1}{2}[\sin(22.5°)]^2$ holds. As a result, $0.2500 \leq 0.1464$, and the inequality is maximally violated for the values predicted for the "Bell test angles [43]." However, $\frac{1}{poly(x)} \geq \frac{1}{poly(x)}$ over $GF_{2^{||x||}}$, and considering that the ring of integers modulo 2 consists only of idempotent elements, we have that $[\frac{1}{poly(x)}]^2 = \frac{1}{poly(x)}$,

hence, $\frac{1}{2}[\frac{1}{poly(x)}]^2 \geq \frac{1}{2}[\sin(22.5°)]^2 + \frac{1}{2}[\sin(22.5°)]^2$. As a result, $0.2500 \geq 0.1464$, and the inequality is not violated for the values predicted for the "Bell test angles". This logical loophole [44, 45, 46, 47, 48, 49] stems directly from the existence of one-way functions, since the weak one-way function, $x^2 + x$, can be used to produce the strong one-way function, $x^2 + x + 1$ in accordance with the amplifying hardness (Yao's XOR Lemma) [11, 50].

2.6. **Conclusion.** Levin and Goldreich [2, 28] proved that the hard core of the universal one-way function g is a hidden bit (deterministic) model able to generate randomness. (See also pseudorandom generator theorems [10, 27]). Here, our one-way protocol showed that the (pseudo)randomness – necessary and sufficient condition – to buid the secure scheme g is achieved, since the Bell inequality can be reduced to polynomial inequality $|x^2 + x + 1| \leq |x^2 + x + 1|$. Whence, the asymptotic security $|x^2 + x + 1|\mathcal{P}r_{g^{-1}g} \leq 1$ for $\mathcal{P}r_{g^{-1}g} \leq 1$ is obtained from a deterministic process over the Boolean ring of all subsets of x. Conversely, there is no deterministic process that produces $|x^2 + x + 1|\mathcal{P}r_{g^{-1}g} > 1$ for $\mathcal{P}r_{g^{-1}g} \leq 1$, although both conditions are deducible from each other. Such an "equalness-of-strength" shows that the problem of determining whether a given state is entangled or separable is at least as hard as the hardest problems in NP.

REFERENCES

[1] Levin, L.A. Aperiodic Tilings: Breaking Translational Symmetry. The Computer Journal. Vol. 48 (6): 642-645 (2005).

[2] Goldreich, O., Levin, L.A. A hard-core predicate for all one-way functions. In Proceedings of the Twenty First Annual ACM Symposium on Theory of Computing, 25–32 (1989).

[3] Levin, L.A. The tale of one-way functions. Probl. Inf. Transm., Vol. 39 (1): 92-103 (2003).

[4] Clauser, J.F., Horne,M.A., Shimony, A., Holt, R.A. Proposed experiment to test local hidden-variable theories. Phys. Rev. Lett., Vol. 23 (15): 880–4 (1969).

[5] Popescu, S., Rohrlich, D. Nonlocality as an axiom. Foundations of Physics. Vol. 24 (3): 379–385 (1994).

[6] Short, A.J.,Gisin, N., Popescu, S. The Physics of No-Bit-Commitment: Generalized Quantum Non-Locality Versus Oblivious Transfer. Quantum Information Processing (2), 131–138 (2006)

[7] Bub, J. Is information the key? In: Analysis and interpretation in the exact sciences. In: Essays in honour of William Demopoulos. Eds. Franppier, M., Brown, D.H., DiSalle, R. Springer Dordrechi Heidelberg, New York (2012).

[8] Rabi, M., Sherman, A. An observation on associative one-way functions in complexity theory, Inform. Process. Lett. 64, 239–244 (1997).

[9] Hemaspaandra, L. Rothe. J. Creating strong, total, commutative, associative one-way functions from any one-way function in complexity theory, J. Comput. System Sci. 58 (3), 648–659 (1999).

[10] Goldreich, O. Foundations of Cryptography. Basic Tools. Cambridge Univ. Press (2004).

[11] Arora, S., Barak, B. Computational Complexity: A modern approach. Cambridge University Press, New York (2009).

[12] Bronshtein, I.N., Semendyayev, K.A., Musiol, G., Muehlig, H. Handbook of Mathematics, 4th ed. New York: Springer-Verlag, p. 889, (2004).

[13] Stalling, W. Cryptography and Networks Security. Principles and Practice. Prentice Hall, NY (2011).

[14] Mullen, G.L., D. Panario, D. Handbook of Finite Fields, CRC Press (2013).

[15] Khrennikov, A. Classical probability model for Bell inequality. Journal of Physics: Conference Series 012019 (2014).

[16] Sugiyama, T. Finite Sample Analysis in Quantum Estimation (Springer Theses). Springer-Verlag Berlin Heidelberg (2014).

[17] Holevo, A.S. Bounds for the quantity of information transmitted by a quantum communication channel. Problems of Information Transmission. 9: 177–183 (1973)..

[18] 't Hooft, G. The Fundamental Nature of Space and Time. In: Approaches to Quantum Gravity. Toward a New Understanding of Space, Time and Matter. Ed. Oriti, D. Cambridge University Press: 13-26 (2009).

[19] Kecheng, L. Semiotics in information systems engineering. Cambridge University Press (2000).

[20] Stamper, R.K. and Ades, Y. Semantic Normal Form and System Quality. In: Proc. IEE Conference on Requirements Engineering (2004).

[21] de Castro, A. Mental models may fail when faced with self-referential descriptors. Journal of the Association for Information Science and Technology. Vol. 67(2): 490 (2016).

[22] Jacod, J., Protter, P. Probability Essentials. Springer-Verlag Berlin Heidelberg (2004).

[23] Cook, S. The P versus NP problem,http://www.claymath.org/millennium/PvsNP/pvsnp.pdf.

[24] Levin, L.A. Average case complete problems, SIAM J. Computing 15: 285–286 (1986).

[25] Impagliazzo, R. A personal view of average-case complexity, in 10th IEEE Annual Conference on Structure in Complexity Theory, IEEE Computer Society Press. 134–147 (1995).

[26] Impagliazzo, R.; Paturi, R. The Complexity of k-SAT", Proc. 14th IEEE Conf. on Computational Complexity. 237–240 (1999).

[27] Hastad, J., Impagliazzo, R., Levin, L.A., Luby, M.A. Pseudorandom Generator from any One-way Function. SIAM Journal on Computing, Vol. 28(4): 1364-1396 (1999).

[28] Levin, L.A. Randomness and nondeterminism. J. Symb. Logic. Vol. 58(3):1102-1103 (1993).

[29] Hemaspaandra, L., Pasanen, K., Rothe, J. If $P \neq NP$ then some strongly noninvertible functions are invertible. Theoretical Computer Science. Vol; 362 (1–3): 54–62 (2006).

[30] Cook, S. The complexity of theorem proving procedures. Proceedings of the Third Annual ACM Symposium on Theory of Computing. pp. 151–158 (1971).

[31] Richter-Gebert, J. Perspectives on Projective Geometry: A Guided Tour Through Real and Complex Geometry. Springer-Verlag Berlin Heidelberg (2011).

[32] de Castro, A. One-way-ness in the input-saving (Turing) machine. Physica A: Statistical Mechanics and its Applications. Vol. 415 (1): 473–478 (2014).

[33] Bennett, C.H. Time/space trade-off for reversible computation. SIAM J. Comput., 20(4), 766-776, (1989).

[34] Ozawa, M. Conservative Quantum Computing. Phys. Rev. Lett. 89, 057902 (2002).

[35] Bayer, G.W. Quantum Computation Violates Mirror Symmetry. Quantum Information Processing. 25–30 (5) (2006).

[36] Li, Y.H., Jin, X.M.: Bidirectional controlled teleportation by using nine-qubit entangled state in noisy environments. Quantum Inf. Process. 15(2), 929–945 (2016).

[37] Li, Y.H., Li, X.L., Nie, L.P., Sang, M.H.: Quantum teleportation of three and four-qubit state using multi-qubit cluster states. Int. J. Theor. Phys. 55(3), 1820–1823 (2016).

[38] Sakurai, J.J. Modern Quantum Mechanics. Addison–Wesley, USA (1994).

[39] Halmos, P., Givant, S. Introduction to Boolean Algebras. Springer (2008).

[40] Hinkis, A. Proofs of the Cantor-Bernstein theorem. A mathematical excursion, Science Networks. Historical Studies 45, Heidelberg: Birkhäuser/Springer (2013).

[41] Zimand, M. Computational Complexity: A Quantitative Perspective. Elsevier B.V. Amsterdam (2004).

[42] Gharibian, S.Strong NP-Hardness of the Quantum Separability Problem. Quantum Information and Computation. Vol.10, 343-360 (2010).

[43] Bell. J.S. Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy 2nd ed. Cambridge Univ. Press (2004).

[44] Hess, K., Philipp, W. Breakdown of Bell's theorem for certain objective local parameter spaces. Proc. Natl. Acad. Sci. 101: 1799–1805 (2004).

[45] Hess, K., De Raedt, H., Michielsen, K. Hidden assumptions in the derivation of the theorem of Bell. Physica Scripta, 014002 (2012).

[46] Hess, K. Einstein Was Right! CRC Press, Boca Raston (2015).

[47] De Raedt, K., Michielsen, K., Hess, K. Irrelevance of Bell's Theorem for experiments involving correlations in space and time: a specific loophole-free computer-example Computer Physics Communications 209, 42-47 (2016).

[48] 't Hooft, G. The Cellular Automaton Interpretation of Quantum Mechanics. In: Fundamental Theories of Physics. Ed. van Beijeren, H. et. al. Springer (2016).

[49] Khrennikov, A. Probability and Randomness: Quantum versus Classical. Imperial College Press, London (2016).

[50] Yao, A. Probabilistic computations: Toward a unified measure of complexity, Proceedings of the 18th IEEE Symposium on Foundations of Computer Science, 222–227 (1977).