Quantum Key Distribution Without "Quantum"

Xavier Coiteux-Roy [‡] and Stefan Wolf[†‡]
School of Computation, Information and Technology, Technische Universität München, Germany.
[†]Informatics Faculty, Università della Svizzera italiana (USI), Switzerland.
[‡]Facoltà indipendente di Gandria, Switzerland.

***bstract*—Landauer's principle states that erasure of information has a thermodynamic price in the form of free energy that is dissipated as heat to the environment. We show that this manifestation of the second law of thermodynamics gives rise to a *classical* no-cloning principle based solely on a bound on the accessible free energy. Like in the quantum case, the principle allows for realizing cryptographic functionalities such as *key agreement*, as discussed in the present text. Our protocols resemble the known ones for quantum key distribution and for the bounded-storage model; however, neither quantum theory nor any bound on available memory space is required for them to work. Investigating its cryptographic possibilities sheds light on the roots of Landauer's principle.**

I. The Second Law of Thermodynamics

The history of the second law of thermodynamics started with *Carnot's* study [1] of the efficiency of heat engines operating between two reservoirs. The outcome motivated *Kelvin* to define the absolute temperature scale. Kelvin also derived his own version of the second law — "No process has as its sole effect the extraction of work from one single heat reservoir" —, whereas *Clausius'* variant reads: "Heat does not spontaneously flow from a colder to a hotter reservoir" (see [2]). *Boltzmann* was the first to give the second law a *combinatorial* twist by claiming that a closed system always transites from a smaller to a larger macrostate, not *vice versa*: *"Entropy does not decrease."* This line of reading is essentially information theoretical and has inspired researchers to find "informational second laws" (e.g., Cover [3]).

Landauer [4], along his slogan "Information is Physical," stated in his version of the second law that the erasure of information requires a compensation in the form of free energy that is then dissipated as heat to the environment. Inspired by this, *Ben Schumacher* formulated the law that *"No process has as its sole consequence the erasure of information."*

The fact that Landauer's principle asks the *logical* erasure of information to have a *thermodynamic compensation* is weirdly hybrid — when thought through, it ends up saying that:

"In a closed system, no information is erased with time."

The rationale is that when a system is closed, then no environmental compensation of information erasure is possible, so no erasure.

In a combinatorial, finite toy model, it has been shown [5] that not only the *Clausius-* and *Kelvin-* [6], but also the *Carnot-*reading of the second law follows from the no-information-erasure principle. (Note that a priori, a "no-erasure second law" is not asymmetric in time and cannot *per se* give rise to an arrow of time; if, however, fresh randomness arises in the time evolution of a closed system, then that *is* irreversible, since the reverse transformation would "undo," "forget" that randomness and so violate logical reversibility.)

The second law of thermodynamics is rarely connected to constructive consequences or applications. One of the few exceptions is perhaps the use of an entropic force such as osmotic pressure to produce work in an "osmotic power plant" (e.g., [7]). In the present article, we propose to use the law to first derive a *no-cloning principle* based on available-work limitations (Section II), and from it the security of a key-agreement protocol (Section III); the latter resembles QKD protocols [8], yet its workings and proof are purely classical. Our protocols are related to schemes in the bounded-storage model, whereas we do not require the assumption of limited memory, only energy.

II. No-Cloning from Landauer's Principle

Quantitatively, *Landauer's principle* states that the erasure — meant is here: reset the corresponding binary degree of freedom to 0 — of one bit of information requires work of at least $kT\ln 2$,[1] which is then dissipated as heat to the environment (a heat bath of temperature T); this dissipation is what compensates the entropy decrease by the resetting. In turn — that observation has been called the "converse of Landauer's principle" and brought forward by Bennett [10] — the all-zero-string 0^l of a certain length l has a *work value* of $kT\ln 2{\cdot}l$ (the work comes from the environmental heat bath of temperature T; in particular, the *first* law of thermodynamics is not violated).

Our only assumption overall the present article is that *the total free energy is (limited by an equivalent of an all-zero-string of length) of the order* n. (Note that whereas the available length of all-zero-strings is limited in our model for all parties, their total memory is not — as long as the latter is filled with randomness, that is incompressible data. In this sense, our model is only loosely related to the well-studied bounded-storage model [11].) Let

$$N := 2^n\,,$$

where n is proportional to the totally available free energy. Therefore, it is *impossible* to obtain an all-zero-string 0^N of length N. Let us observe first that such a string would allow

[1]It has been proposed to turn the principle around in the sense as using it for defining temperature as "joule per bit," getting rid of Boltzmann's constant [9].

for producing an extra identical copy of a general string of length N, say $X^{(N)}$: The reason is that the transformation

$$X^{(N)}||0^N \longleftrightarrow X^{(N)}||X^{(N)}$$

is logically reversible, in both ways in fact, even if X is "random," i.e., uniformly random, or incompressible (the Kolmogorov complexity of which is essentially equal to its length, see [6]). According to Fredkin and Toffoli [12], this transformation *can* thus be carried out in both ways thermodynamically neutrally: Redundancy, in particular identical copies, thus have the same free-energy value as an all-zero-string of corresponding length.

The following is *impossible* — and this is our *"no-cloning principle without quantum"*: The transformation

$$X^{(N)}||Y^{(N)} \not\mapsto X^{(N)}||X^{(N)}$$

is impossible if Y is incompressible and independent from X. In fact, only an amount of information of the order of $n = \mathcal{O}(\log N)$ can be copied onto a tape with initially incompressible content — due to the free-energy constraint.

This principle has several cryptographic applications. The first and most obvious one are unforgeable banknotes: If something can in principle not be copied, then we can use it for that [13].

In this note, we present a protocol for *key agreement* which resembles quantum key distribution, but where our classical no-cloning principle takes the role of quantum no-cloning: Roughly speaking, Alice sends huge data sets to potentially Eve, who then forwards them to Bob. All communication is reversible, through *swap* channels, exchanging data sets of equal size. By comparing hash values or bits at sampled positions, Alice and Bob limit the noise in their respective data; if it is too high, they abort; if it is not, they can limit Eve's information and generate secret keys. This "quantum key distribution without quantum" is developed in the remainder of this article.

We complete this section with some definitions. First, we formalize free-energy bounds.

efinition 1. A party has *free energy* F if it can produce a zero string of length $F +$ with probability at least 2 .

This definition is based on the following fact.

Lemma 1. *For any $N, M,$ $\in$, the logically reversible computation of*

$$0^N||X^{(M)} \mapsto 0^{N+}||Y^{(M)}$$

is impossible except with probability 2 when $X^{(M)}$ is uniformly chosen at random.

Proof. This proof with finite M follows from logical reversibility, by which it holds that for any $N, M,$ $\in$, there exists no reversible computation $f : \{0,1\}^{N+M} \to \{0,1\}^{N+M}$ such that for more than a fraction 2 of the $X^{(M)} \in \{0,1\}^M$, there exists $Y^{(M)} \in \{0,1\}^M$ such that $f(0^N||X^{(M)}) = 0^{N+}||Y^{(M)}$. An extended proof for unbounded M is done in [14], and a proof for the quantum analogue is sketched in [13]. □

For cryptographic purposes, it is useful to establish bounds on the conditional min-entropy of an adversary.

efinition 2. The *conditional min-entropy* $H_\infty(X|Y)$ is defined as

$$H_\infty(X|Y) \coloneqq \log \sum_y P(Y=y) \max_x P(X=x|Y=y) .$$

It has a clear operational meaning: it is the optimal probability of correctly guessing X given side information Y.

Also useful for this work is the concept of variational distance.

efinition 3. The *variational distance* between two random variables X and Y is defined as

$$(X,Y) \coloneqq \frac{1}{2} \sum_{i \in \mathcal{X} \cup \mathcal{Y}} |p(X=i) \quad p(Y=i)| . \tag{1}$$

It is operationally very useful because it characterizes the impossibility to distinguish between X and Y — using any physical experiment whatsoever. More precisely, given either X or Y with probability $1/2$, the optimal probability to correctly guess which one it is amounts to $(1 + (X,Y))/2$.

Once a bound on the conditional min-entropy of the adversary is obtained, we apply privacy amplification by hashing.

efinition 4 (2-universal hashing [15], [16])**.** Let $\mathcal{H}$ be a set of hash functions from $\{0,1\}^n \to \{0,1\}^m$. $\mathcal{H}$ is *2-universal* if, given any distinct elements $x_1, x_2 \in \{0,1\}^n$ and any (not necessarily distinct) elements $y_1, y_2 \in \{0,1\}^m$, then

$$\#\{h \in \mathcal{H} | y_1 = h(x_1) \wedge y_2 = h(x_2)\} = \frac{\#\mathcal{H}}{2^{2m}} . \tag{2}$$

Lemma 2 (Leftover hash lemma [17]–[20])**.** *Let $h : \mathcal{S} \otimes \mathcal{X} \to \{0,1\}^m$ be a 2-universal hash function. If $H_\infty(X) \geq m + 2\varepsilon$, then*

$$\Big((h(S,X),S), U \otimes S\Big) \leq 2^{\ \varepsilon} . \tag{3}$$

S is a short uniformly random seed and X is the variable whose randomness is to be amplified. U is the uniform distribution of appropriate dimension. The symbol $\otimes$ is used to represent the joint probability of independent distributions.

III. QKD Without Q

Secret-key establishment is a fundamental primitive for two-way secure communication because it allows for a perfectly secure one-time-pad encryption between Alice and Bob, about which Eve knows nothing (otherwise the protocol aborts).

efinition 5. A secret-key-establishment scheme is *sound* if, at the end the protocol, Alice and Bob possess the same key with overwhelming probability in the security parameter η:

$$P(K_A \neq K_B) \leq \frac{1}{\eta} . \tag{4}$$

efinition 6. A secret-key-establishment scheme is information-theoretically *secure* (*i.e.*, almost-perfectly secret) if the

key K_B is uniformly random even given all of the adversary's side information E, except with probability at most negligible in the security parameter ν:

$$\Big((K_B, E), U \otimes E\Big) \leq \mathbf{n}\ \mathbf{gl}(\nu)\,, \tag{5}$$

where $\mathbf{n}\ \mathbf{gl}(\nu)$ is a function that decreases faster than any inverse polynomial.

A. Protocol

Theorem 1. *The following secret-key-establishment protocol is information-theoretically sound and secure against any eavesdropper whose free energy is $\mathcal{O}(\log N)$.*[2] *Alice and Bob need a quantity of free energy that is $\mathcal{O}(\log N)$.*

Soundness is analyzed in Section III-B, and security in Section III-C.

In what follows, the variables $(A, B) \in (\mathcal{A}, \mathcal{B})$ are strings of length N, while $(X, Y) \in (\mathcal{X}, \mathcal{Y})$ denote strings of length roughly $\mathcal{O}(\log N)$. Below, $h_b(p) \coloneqq \quad p \log_2 p \quad (1 \quad p) \log_2 (1 \quad p)$ is the *binary entropy*.

Secret-key-establishment protocol:

1) Alice starts with $X \in \mathcal{X} = \{0,1\}^N$ in a uniformly random state (extracted from the thermal environment of her lab). She draws uniformly at random a subset $\subset \{1, \ldots, N\}$ of $s+t$ positions r *wkey* and copies $(r\ wkey, X_{[r\ wkey]}) \to A$ to her memory of size $O(\log N)$.
2) Alice sends $X \to Y$ to Bob using a reversible channel (*e.g.*, a SWAP channel); it is possibly intercepted by Eve.
3) Bob announces the receipt to Alice on an authenticated public channel. In case of no receipt, they abort.
4) Alice publishes the subset positions r *wkey* on the (noiseless) authenticated public channel so that Bob can select $Y_{[r\ wkey]} \to B$. Alice and Bob draw a *test* sub-subset of t bits that they sacrifice to estimate the error rate p_{error} between A and B.
5) If the estimated p_{error} is too large, they abort. Otherwise, Alice and Bob apply information reconciliation (detailed in Section III-B) on the remaining s bits $A_{\overline{[test]}}$ and $B_{\overline{[test]}}$.
6) Alice and Bob apply privacy amplification (detailed in Section III-C) and obtain a shared secret key of length $\approx ((k \quad 1)/k \quad h_b(p_{\text{error}})) \cdot s$.

The main parameters are , whose logarithm is roughly the bound in free energy of Eve; k, which determines the error tolerance between Alice and Bob; t, the number of test bits to estimate that error rate; and s, the length of the raw key (before processing).

[2]Note that the security of the protocol can in fact be strengthened against any eavesdropper with free energy N , as we show in [14].

Note that for any fixed p_{error} (as long as it is not trivially $1/2$), Alice and Bob can choose a security parameter k for which the protocol will be secure for that value of p_{error}. That is unlike, for example, the BB84 quantum-key-distribution protocol, which only tolerates error rates less than $1/4$ (any more and Eve can intercept the whole quantum state).

The intuition. — As discussed in Section II, because she is $O(\log N)$-bounded in free energy, Eve cannot copy to her memory the whole N-long string Y that she sends to Bob, on which Bob will later base the raw key. Alice circumvents this limitation by already knowing the raw-key positions at the moment she sends X (X becomes, after Eve's potential tampering, Y) and thus need not store more than an $\mathcal{O}\left((t+s)\log N\right)$-long segment of the N-long string. As in quantum key distribution, Eve can force the protocol to abort.

B. Soundness analysis

1) Parameter estimation: We first estimate (using upper bounds) between Alice and Bob the global error rate p_{error} and the non-tested *rawkey* error rate $p_{\text{error}}^{\overline{test}}$. The former quantity is important for the privacy amplification analyzed in Section III-C, while the second is needed to analyze information reconciliation.

Proposition 1. *Alice and Bob can accurately estimate the error rate p_{error} by sampling on the t test positions the error rate p_{error}^{test}:*

$$P\ \ p_{\text{error}} \leq p_{\text{error}}^{test} + \varepsilon\big) \geq 1 \quad e^{\ 2\varepsilon^2 t}\,. \tag{6}$$

Proof. p_{error}^{test} is computed from the Hamming weight $\omega(\overline{A_{[test]} \oplus B_{[test]}}) = t(1 \quad p_{\text{error}}^{test})$. Chernoff's inequality bounds p_{error}. □

Proposition 2. *Alice and Bob can accurately estimate $p_{\text{error}}^{\overline{test}}$ from p_{error}^{test}:*

$$P\left(p_{\text{error}}^{\overline{test}} \leq p_{\text{error}}^{test} + \frac{s \cdot \varepsilon}{s+t}\right) \geq 1 \quad e^{\ 2\varepsilon^2 t}\,. \tag{7}$$

Proof. We insert $p_{\text{error}} = (s \cdot p_{\text{error}}^{\overline{test}} + t \cdot p_{\text{error}}^{test})/(s+t)$ in Eq. 6 and isolate $p_{\text{error}}^{\overline{test}}$. □

2) Information reconciliation (error correction): Once they have a good estimate of $p_{\text{error}}^{\overline{test}}$, Alice and Bob achieve information reconciliation by applying error correction on that unused subset $\overline{test}$ of s bits.

Note that it is important that the established key be based on Bob's string, rather than on Alice's, because the technique using the thermodynamical no-cloning theorem of Section II bounds the mutual information between Bob and Eve, not the one between Alice and Eve (see Section III-C).

Proposition 3. *For any non-trivial constant $p_{\text{error}}^{\overline{test}} \neq 1/2$, Alice and Bob can transform the samples $A_{\overline{[test]}}, B_{\overline{[test]}}$ into the (not necessarily secret) keys K'_A, K'_B for which*

$$P\left(K'_A = K'_B\right) \geq 1 \quad \frac{1}{\eta}\,. \tag{8}$$

They can do so with $w \approx h_b(p_{\text{error}}^{\overline{test}}) \cdot s$ (the exact value is given below) bits of authenticated public communication.

We present one standard construction to correct an arbitrary error rate on the s bits of *rawkey* that were not used during the parameter-estimation phase.

a) Asymptotically optimal protocol for information reconciliation [21]::

Let $w \coloneqq \lceil s \cdot h_b(p_{\text{error}}^{\overline{test}} + \ ') + \eta \rceil$;

1) Bob picks at random a hash function $h : \{0,1\}^s \to \{0,1\}^w$ from a 2-universal family $\mathcal{H}$ and computes $h(B_{\overline{[test]}})$.
2) Bob communicates h and $h(B_{\overline{[test]}})$ to Alice, using the authenticated public channel.
3) Alice computes

$$\tilde{A}_{\overline{[test]}} \coloneqq \underset{x \in \{0,1\}^{1 \ \mathbf{n} \ s)}}{\operatorname{argmin}} \left(\omega(x, A_{\overline{[test]}}) | h(x) = h(B_{\overline{[test]}}) \right) .$$

Here, $\omega(\cdot,\cdot)$ is the Hamming distance; $'$ determines efficiency and η is the security parameter.

Proof. We first count, in the uniform distribution, the smooth number of strings with length s that contains approximately $p_{\text{error}}^{\overline{test}}$: Let $M \coloneqq \{x \in \{0,1\}^s \,|\, p_{\text{error}}^{\overline{test}} \quad ' \leq p_{\text{error}}^{\overline{test}}(x) \leq p_{\text{error}}^{test} + \ '\}$; from the asymptotic equipartition property, we have $\forall \ ' > 0$,

$$P\left(\#M \leq 2^{s \cdot h \ (p_{\text{error}}^{\overline{test}} + \ )} \right) \geq 1 \quad 2^{\ \Theta(\eta)} . \tag{9}$$

Because $\mathcal{H}$ is 2-universal, the probability of obtaining a correct hash from a non-correct candidate in M is bounded by $2^{\ w}$. By the union bound, the protocol is therefore sound except with probability at most $2^{\ w} \cdot \#M$, which is $\mathbf{n} \ \mathbf{gl}(\eta)$. □

While the above ideal information-reconciliation protocol is optimal, it offers no (known) efficient way (in the computational-complexity sense) for Alice to decode Bob's codeword. While we are in this work only concerned with thermodynamic (rather than computational) efficiency, we refer to [21], or to the theory of Shannon-optimal efficient algebraic codes, such as convoluted codes, for asymptotically ideal information-reconciliation protocols that are also computationally efficient.

C. Security analysis

If the protocol does not abort, Eve has negligible information about the key K_B at the end. This security resides on the fact that even if Eve intercepts X (which was sent from Alice to Bob) and replaces it with Y, she cannot keep roughly more than a logarithmic fraction of the information about Y. Thus, since the key is based on Y, Eve has limited knowledge about it.

Formally, our starting point is the following inequality.

Lemma 3. *If Bob has Y (which has length N) and Eve has E (with bounded free-energy $O(\log N)$), then*

$$H_\infty(Y|E) = N \quad O(\log N) . \tag{10}$$

Proof. If Eve were to guess Y with a certain probability p, she could erase it with that probability p. However, p must be less than $2^{\ N+O(\log N)}$ so as to not contradict the free-energy assumption. □

We then use a property of classical information which was evidenced by [22] and refined in [23], and to which we return in Section IV.

Proposition 4 (Vadhan [23])**.** *With very high probability, the min-entropy is approximately conserved under random sampling. Let rawkey be a random subset of s positions, we have for all $\ > 0$, that except with probability $2^{\ \Omega(s^{\ 2} \log^{2\ })} + 2^{\ \Omega(N\ )}$,*

$$H_\infty(Y_{[rawkey]}|E) \geq \frac{s \cdot H_\infty(Y|E)}{N} \quad s \cdot \tag{11}$$

$$= s \quad s \cdot \frac{O(\log N)}{N} \quad s \cdot \ . \tag{12}$$

The next step is to go from (very) *low* information to *essentially no* information. using privacy amplification. Privacy amplification turns a long string about which the adversary has potentially some knowledge into a shorter one about which the adversary has essentially none.

In secret-key establishment, Eve's partial information can come from eavesdropping (and as shown, this quantity is limited by her free energy) or from the public information leaked by the information-reconciliation protocol, which is easily characterized.

We use a straightforward sample-and-hash technique, in which privacy amplification is realized in an information-theoretically secure manner using 2-universal hashing.

Proposition 5. *After privacy amplification, K_B is approximately of length $\approx (1 \quad h_b(p_{\text{error}})) \cdot s$, and Eve has essentially no knowledge about it.*

Proof. Let w quantify the number of bits about $B_{\overline{[test]}}$ exchanged publicly during the information-reconciliation (IR) protocol. We note that $H_\infty(Y_{[rawkey]}|E^{\text{preIR}}) \leq H_\infty(K_B|E^{\text{postIR}}) \quad w$, hence we have

$$H_\infty(K_B|E^{\text{postIR}}) \geq s \quad s \cdot \frac{O(\log N)}{N} \quad s \cdot \quad w \tag{13}$$

except with probability $2^{\ \Omega(s^{\ 2} \log^{2\ })} + 2^{\ \Omega(N\ )}$. Therefore, taking $m \coloneqq s \quad s \cdot \frac{O(\log N)}{N} \quad s \cdot \quad w \quad \varepsilon$ guarantees after hashing (ε is the security parameter for the Leftover hash lemma; see Lemma 2) information-theoretic security on those remaining m bits. □

Note that for any fixed p_{error}, the number of samples s can be selected as to make m a positive quantity when the protocol does not abort (as a result of too many errors). Also note that the length N must not be too short.

IV. Cryptography as a lens for physics

In this letter, we have presented a scheme for cryptographic secret-key agreement secure under the sole assumption that the adversary is limited in available work. The security proof relies on the second law of thermodynamics; more explicitly, the nexus between the physical and informational realms is given by Landauer's principle, stating that the erasure of information has a price in terms of work that is then dissipated in the form of heat to the environment. In order to carry through the security proof, a no-cloning principle is derived from Landauer's. Specifically, this can be done in the realm of classical physics, as we have shown in the present text. Furthermore, a similar conclusion can also be made in the quantum realm. This is based on results guaranteeing the existence of condensers for min-entropy [24], [23].

It has become an established research program to attempt to base physical theories on information axioms, e.g., quantum theory on "secret-key agreement is possible" and "oblivious transfer is impossible." Let us first observe that in the classical limited-energy scenario considered here, the second statement is to be replaced by *"oblivious transfer is possible"* — as we will show in subsequent work.

The spirit of this point of view is that information processing — in this case *cryptographic* — tasks are used as a "lens" for studying and differentiating physical theories. In this sense, we ask: Is the implication from Landauer's principle to no-cloning generally possible, e.g., also in beyond-quantum worlds? We argue that the answer is *no*: It does not forbid (a weak form of) cloning, and thus these theories allow for no key agreement either.

Specifically, in analogy to the nonlocal box introduced by Popescu and Rohrlich [25], we could think of a model even *more contextual than QM*. We present such a box, the (1-out-of-n)-box; if it were to exist (for a sufficiently large n), it would break the security of our scheme. Ironically, this box is based on another cryptographic primitive: the aforementioned *oblivious transfer*.

- The (1-out-of-n)-box can "encode" n bits.
- But only 1 of those bits can be retrieved from the (1-out-of-n)-box (or alternatively, any binary predicate of those bits). Once that bit is out, the box self-destroys.
- The cost in free energy to create an (1-out-of-n)-box is $kT \ln 2 \ J/\text{bit}$.

The box is highly contextual because while any bit (out of n) can be retrieved, the act of measurement (extracting a single bit) prevents further bits from being extracted. It is straightforward to see that Landauer's erasure cost of this device is still $kT \ln 2 \ J/\text{bit}$ (as it is the cost to erase the unique bit that came out of the box before its self-destruction). Landauer's cost is, therefore, about *information actualities* rather than *information potentialities*, it corresponds to the number of bits that can be simultaneously retrieved, rather than on the number of counter-factual bits that can be encoded. In the classical and quantum worlds, these two quantities are, however, and somewhat surprisingly, virtually equal — and the security of our scheme depends on it.

An experimental test of the existence of these boxes could come in the form of Alice and Bob carrying out our key-agreement protocol — and Eve breaking it. From this, we could conclude that unless Eve has exponential amounts of free energy, these beyond-quantum boxes must exist: This would be "information-retrieval contextuality," of classical instead of quantum nature: *Quantum contextuality without quantum*, for short.

Acknowledgment

The authors thank Harry Buhrman, Gilles Brassard, Charles Bédard, and Sophie Berthelette for interesting discussions. The authors acknowledge financial support from the Swiss National Science Foundation.

References

[1] Sadi Carnot. *Réflexions sur la puissance motrice du feu et sur les machines propres développer cette puissance*. Gauthier-Villars, 1878.

[2] Jos Uffink. Bluff your way in the second law of thermodynamics. *Studies in History and Philosophy of Science Part B: Studies in History and Philosophy of Modern Physics*, 32(3):305–394, 2001.

[3] Thomas M Cover. Which processes satisfy the second law. *Physical origins of time asymmetry*, pages 98–107, 1994.

[4] Rolf Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5(3):183–191, 1961.

[5] min Baumeler, Carla Rieger, and Stefan Wolf. Thermodynamics as combinatorics: A toy theory. In *2022 IEEE Information Theory Workshop (ITW)*, pages 362–367. IEEE, 2022.

[6] min Baumeler and Stefan Wolf. Causality–complexity–consistency: Can space-time be based on logic and computation? *Time in Physics*, pages 69–101, 2017.

[7] Stein Erik Skilhagen, Jon E Dugstad, and Rolf Jarle Aaberg. Osmotic power—power production based on the osmotic pressure difference between waters with varying salt gradients. *Desalination*, 220(1-3):476–482, 2008.

[8] Charles Bennett and Gilles Brassard. Quantum crytography: Public key distribution and coin tossing. In *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India, 1984*, pages 175–179, 1984.

[9] Charles Alexandre Bédard, Sophie Berthelette, Xavier Coiteux-Roy, and Stefan Wolf. Temperature as joules per bit. *arXiv preprint arXiv:2401.12119*, 2024.

[10] Charles H Bennett. The thermodynamics of computation: a review. *International Journal of Theoretical Physics*, 21(12):905–940, 1982.

[11] Ueli M Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology*, 5(1):53–66, 1992.

[12] Edward Fredkin and Tommaso Toffoli. Conservative logic. *International Journal of theoretical physics*, 21(3):219–253, 1982.

[13] Xavier Coiteux-Roy and Stefan Wolf. Unconditional proofs-of-work and other possibilities of thermodynamic cryptography. In *2022 IEEE Information Theory Workshop (ITW)*, pages 452–457. IEEE, 2022.

[14] Xavier Coiteux-Roy and Stefan Wolf. Key agreement and oblivious transfer from free-energy limitations. *arXiv preprint arXiv:2206.01501*, 2022.

[15] J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[16] Mark N Wegman and J Lawrence Carter. New hash functions and their use in authentication and set equality. *Journal of Computer and System Sciences*, 22(3):265–279, 1981.

[17] Charles H Bennett, Gilles Brassard, and Jean-Marc Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, 1988.

[18] Russell Impagliazzo, Leonid A Levin, and Michael Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 12–24, 1989.

[19] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. Construction of a pseudo-random generator from any one-way function. In *SIAM Journal on Computing*, 1993.

[20] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[21] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 410–423. Springer, 1993.

[22] Noam Nisan and David Zuckerman. Randomness is linear in space. *Journal of Computer and System Sciences*, 52(1):43–52, 1996.

[23] Salil P Vadhan. Constructing locally computable extractors and cryptosystems in the bounded-storage model. *Journal of Cryptology*, 17(1):43–77, 2004.

[24] Robert König and Renato Renner. Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory*, 57(7):4760–4787, 2011.

[25] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24:379–385, 1994.