Cryptographic Key Exchange: An Innovation Outlook

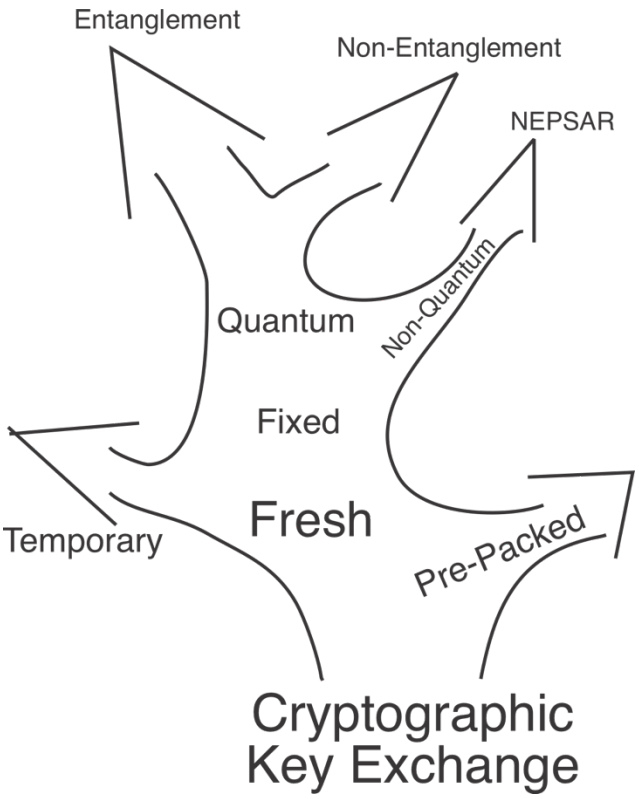
Gideon Samid

Electrical, Computer and System Engineering

Computer and Data Sciences
Case Western Reserve University, Cleveland, OH
Gideon.Samid@CASE.edu

Abstract: This article evaluates the innovation landscape facing the challenge of generating fresh shared randomness for cryptographic key exchange and various cyber security protocols. It discusses the main innovation thrust today, focused on quantum entanglement and on efficient engineering solutions to BB84, and its related alternatives. This innovation outlook highlights non-quantum solutions, and describes NEPSAR – a mechanical complexity based solution, which is applicable to any number of key sharing parties. Short-lived secret keys are also mentioned, as well as emerging innovation routes based on Richard Feynman's observation: "there is plenty of room at the bottom," extracting plenty of digital randomness from tiny amounts of matter, yielding very many measurable attributes (nanotechnology).

Life in cyberspace is powered by an ongoing fresh supply of shared randomness between cyber residents. At present two parties, strangers and non-strangers, most commonly generate shared randomness algorithmically, and use it through public key protocols, with great operational success. Alas, storm clouds gather over the cyberspace landscape, making it necessary to activate the Innovation^{SP} methodology [2, 3] to meet this challenge.



Both the generation of randomness and its sharing today is hinged on a shaky foundation: unproven mathematical complexity. None of the common protocols comes with any proof that it serves its purpose [4,5]. Faith in those protocols is hinged on the absence of publications describing a breach. In other words, life in cyberspace today is secretly resting on the

ungrounded hope that our adversaries will not be smarter than we expect them to be. For more and more thoughtful people this is way too risky. Come to think about it, cryptographic practice today is founded on the hubris of its designers, claiming intellectual superiority over any foreseeable adversary.

Math as a vector of attack has recently been supported by the emerging technology of quantum computing, which is so radically different from the Turing machines of today, [4,5] and so much more powerful, that nobody has a good handle on how profound will be their impact on peace and tranquility in cyberspace.

Add to it the cloud of artificial intelligence [6] -- another emerging unbound technology with open ended impact prospect on life in cyberspace.

We need a good umbrella, at least, to weather the coming storm. Innovation^{SP} [2,3] here we come!

First step: separation. Generating randomness and sharing randomness are two distinct issues, so we should handle them separately.

Starting with generating randomness. Von Neuman famously remarked: *"Those who use algorithms to generate randomness, understand neither algorithms, nor randomness"* . Over the years we discovered powerful randomness-generating algorithms, in as much as what they generate pass some arbitrary tests for randomness. Randomness has no objective measure only a probability statement [1]. Passing a test does not prove absence of pattern, which is the essence of randomness. The emerging technology of AI is trained to spot subtle and faint deviations from randomness, which escape any arbitrary test one devises. *In summary: we need an algorithm-replacement for randomness generation.*

Innovation^{SP} now calls for 'abstraction' to handle the challenge of algorithm replacement. Physics discovered that the microcosmos operates through perfect randomness, which good engineering can hopefully capture and harness for cryptographic purposes. Efforts were unleashed in this direction. It soon became clear that exploiting microcosmic randomness for ready protocols is rather a big challenge. The

Innovation^{SP} protocol calls then for "concentric development": achieving imperfect but non-algorithmic randomness, at least as a stop-gap measure until perfect microcosmic randomness can be put to work for the full range of its prospective use.

One readily figures out that for cryptographic terms the purpose of randomness is to achieve unpredictability. This leads one to consider generating randomness through the combined impact of a large number of factors, which themselves are rather unpredictable. A tossed dice or a flipped coin are considered random because of the multitude and resultant complexity of influences that determine the outcome. This leads one to engineer a process so fitting. This complexity approach is being Innovation^{SP} appraised to be a simpler task, and indeed, a variety of physical-complexity based randomness generators was developed and used. The most common is white noise generators which creates a non-repeat, non-algorithmic, unpredictable random series. White noise is a random signal having equal intensity at different frequencies, giving it a constant power spectral density.

A recent design creates randomness by pumping air through a bulk of a conductive fluid. The randomized bubbles change the effective electrical resistance over the bulk, yielding a randomized curve of resistance measurements over time [7]. The output randomness may be fed back into the air blowing system to generate a randomization loop which requires one to acquire knowledge of the dynamics of the air blowing, as well as the physical properties and dimensions of the contraption where it all happens. Anyway, cracking this randomness generator is not within the realm cyber hackers work in. Any party not in the possession of the contraption will see the output random stream as totally unpredictable and hence fully cryptographically useable.

While complexity-randomness is effective for most uses, for high powered industrial applications one may opt to rely on a quantum process which is backed by solid theoretical considerations. IDQ [8] in Geneva Switzerland is a pioneer on this front, constructing a gadget wherein a single photon is fired towards a 45 degree slanted half way mirror. The photon is totally unpredictable as to the process of going straight through the mirror, or bouncing off it on a perpendicular direction. Sensors on both ends record what the

photon ended up doing, and the sequence of these decisions builds up a perfect randomness. Other solutions are based on fluctuations in radiation rates of a radioactive element of long half-life. The Random Number Generator (RNG-01) from Images [9] will produce approximately one to three random numbers every minute from background radiation.

Turning now to the challenge of sharing the generated randomness. This objective has been considered for a long time the purview of quantum solutions because white noise and other complexity randomness options are unique to their source of generation, and sharing them with a remote partner would require reliance on a hackable cryptographic protocol. Quantum phenomena, by contrast, have unique features.

A quantum entity, (qbit), unlike a Maxwellian-Newtonian entity, (bit), is packing uncertainty over a given period of time. That means it can be transported between remote partners, who then figure out how to resolve this uncertainty in a coordinated way. Nature seems to be very helpful here, offering a mysterious phenomenon of entanglement -- a coordinated random behavior between two distinct quantum entities. These two quantum entities (usually photons) may be sent one to each remote party, and then rely on the 'spooky' coordination between the parties, as Einstein called it, to have the effect of shared conclusion, as to the built in uncertainty within the two coordinated (entangled) quantum entities.

Big budgets and heavy-duty engineering talent is devoted to achieve randomness generation and sharing on the basis of entanglement. The big challenge here is the instability of the shared qbits. They very easily lose their uncertainty status, and void the entanglement effect. Otherwise, entanglement is very promising: it generates perfect randomness, (as best as quantum physics can tell) and offers a very elegant sharing solution.

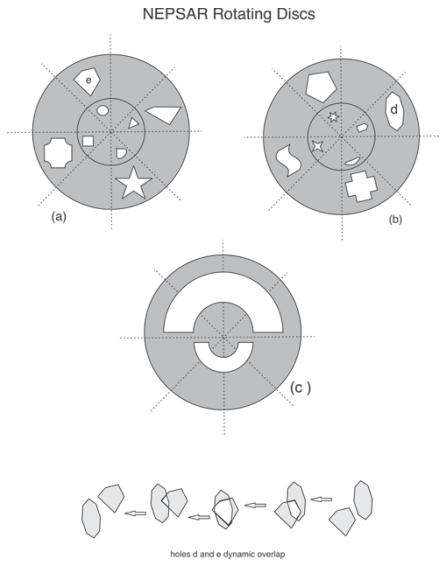
A simpler solution was proposed as early 1984, by Bennett and Brassard, known as BB84 [10]. Quantum entities are prepared randomly with one method, A, or another method B. They are sent over to a remote party who randomly inspects each quantum entity with either method A or method B. If the inspection method was the same as the preparation method, both parties hold the same result. Otherwise the

results will agree on 50% of the time. The parties eventually share which method they used for which entity and thereby know for which quantum entities they have a matching result. They discard the other quantum entities. BB84 and its variants do not require the complexity of entanglement, their theoretical foundation is solid, and the state of the art here is to come up with cost effective, industrially fitting, convenient, reliable engineering implementation. QuantLR [11] in Israel are pioneering this solution. They aim at the 'last mile' challenge where most of the randomness sharing needs are found, but the players are severely cost limited.

Other quantum exchange players are: QNu Labs, Quintessence Labs, MagiQ, SeQureNet, Quantum Optics Jena, and KEEQuant.

The difficulty and the cost of the quantum sharing solutions leads Innovation^{SP} to take a look at the challenge of sharing complexity randomness. A good innovation here might at least serve as a stop-gap solution until quantum solutions are allowed to mature. The respective innovative effort starts with *abstraction* --- asking the question of how to assemble easily duplicatable complexity. Mechanical complexity is a natural candidate because we have good means to manufacture mechanical pieces with great accuracy and tight tolerance. After all Henry Ford revolutionized the automotive industry on the idea of similar-enough parts manufacturing.

Exploring a mechanical complexity: Following Innovation^{SP}, mechanical complexity is achieved via *structure* and *motion*. A localized motion is normally circular. A rotating disc may become structure complexity via randomized holes of various shapes and sizes. This leaves one with the task of building a critical mass of complexity by combining holes-ridden rotating discs. A disc stack comes to mind, and combined complexity may be achieved through pushing a fluid through the stack comprising hole-ridden rotating discs. Such fluid at any moment will have a different passage area, if at all. To move through the stack of discs the fluid will have to go through a 'tunnel' comprised of open area in



overlapping holes. By making the construction of the holes randomized, and making the rotation speed and direction randomized, one forces the passing fluid to move as a randomized flow pattern. One may this flow rate over time -- then analog-to-digital convert it to a random bit series.

Given that discs as described can be drilled with very tight tolerance, and may be rotated with very exact angular velocity, it is fully expected that two or more such disc-based contraptions operating in faraway places but activated as to the motion of the discs with the same activation order, will all generate a sufficiently similar flow pattern from which each party will extract the same randomized binary string.

To the extent that the holes on the discs are randomized, the rotation of each disc at each moment is randomized, so must be the fluid flow, within the range of flow limits. This design is so thoroughly guided by randomness that there is no source for order and pattern to emerge, and hence to be detected. Moreover, even if the activation randomness is in the open, the flow randomness will remain obscure to any third party unaware of the construction of the discs stake. That construction can be upgraded to any desired complexity by adding more discs with fully randomized holes. It is noteworthy that a single disc can stop flow through all the other discs which may have overlapping passage flow area.

This claim of randomness is applicable to active flow situations. Flow on both ends shrinks the effect of randomness. Namely, if there are so many holes that no matter how the discs rotate, the flow is always close to maximum throughput, then activation randomness has little effect. On the other end, if the holes are so few and so small that no matter how the discs rotate the flow is negligible, then too, there is no room for flow randomness.

Randomness can be extracted in several ways. Here is one: a disc stack of a certain pattern of holes is handled with a certain pattern of rotational speeds for each disc. The parameters are fixed so that on average the fluid flow will have a capacity of $0.5F_{max}$, where F_{max} is the flow rate of the fluid through a stack with 100% holes area in all disc. This average performance implies that random deviations in the speeds of rotations will result in random deviations in the quantities of the pass-through fluid. The relationship

between the activation randomness (speeds of rotations) and the measured randomness (quantities of passing fluid) depends on the construction of the discs. To the extent that this construction is unknown to an attacker, the identity of the output randomness is equally unknown, even if the activation randomness is known. One may note that a brute force attack is not conclusive either because the attacker, is not only unaware of holes patterns, they are not in the know as to the size and number of discs that form a stack, and what is more, the passing fluid may be a result of two or more disc stacks.

This particular method, out of many, is of special interest because the output randomness depends on exact duplication of discs and their rotational speed -- factors which can be easily duplicated with great exactness for all the required duplicates.

The method chosen to measure accurately and responsively the flow of fluid through the discs can be any of a selection choices. Ref [7] points to passing the emerging fluid through a bulk of a different fluid of different electrical conductivity. The impact of the measured conductivity across the bulk is directly related to the quantity of the emerging fluid at each moment. The system in Ref [7] is Non-Entanglement Physical Shared Ad-Hoc Randomness [NEPSAR].

Each Party Generates the Shared Key from its own duplicate of the physical randomness generator.

NEPSAR's randomness generation and sharing apparatus is a solution where the number of parties in the key exchange protocol is not limited to two, as it is with the quantum solutions. But unlike the quantum solutions NEPSAR requires exchange of shared hardware (the NEPSAR apparatus). In this category of sharing hardware one may also note the Rock of Randomness [12]: a solution in which two or more parties share a lump of matter from which they decide in the open what random data to extract. Before the digital extraction, the data is kept off the digital realm, in the chemical bonding within the lump.

Key Fountain: The Rock of Randomness sits at the edge of a thick innovation forest. It was Richard Feynman who said that *"there is plenty of room at the bottom"* indicating that the material microcosmos is host to enormous amount of information. One may loosely rewrite Einstein's formula as $I = mc^2$, indicating that a small amount of matter is host to enormous amount of measurable information, (I). A group of secret sharing communicators, each holding a manufactured duplicate of a lump of matter will hold, what might be described as a "key fountain": a source of shared keys sufficient to meet any required secret generation pace. While the shared keys will not be freshly generated as with the other methods described here, they will be pulled out from a non-digital realm: captured in chemical attributes measured in agreement on each manufactured material duplicate. Today the technology for activating the Rock as key fountain is rather limited, [12]. But from an innovation analysis point of view – we identify a host of possibilities for extracting chemical data and converting it into digital data. This material key fountain as an innovation direction may compete well with the quantum based solutions that today dominate the expectations of users and investors alike.

Quantum solutions do not require a secret pre-sharing of information or items, their bit production rate is high, and their construction fits well with the equipment used by networks who are the big customers for dynamic key exchange. NEPSAR is based on desk-top size apparatus, and operates in limited bit capacity. On the other hand NEPSAR serves a party of communicators of any size, and it is not dependent on underlying electronics that must be purchased from a source with malicious intent.

It appears the quantum key exchange is destined to become the working horse for the big players in the field, while NEPSAR lays a claim on the smaller, ad-hoc, private class of users.

As networks become more regimented, more regulated and more monitored, there is expected to be a growing need for cryptographic conversation on the side. So while quantum solutions claim the lion share of use, NEPSAR assert its sizeable niche.

The solutions presented above aim at securing permanent key exchange without admitting dependence on algorithmic assumptions of complexity and intractability. One must in this swing also mention the category of short-lived secrets. If the requirement of the exchange is being relaxed to temporary status then a probability-hinged solution is a practical possibility. Ref [13] describes a simple way for two strangers to extract shared information based on the birthday problem principle. Two small enough sets of information selected randomly from a large source set have a readily calculable chance to include one shared item. Two parties, each selecting a set in a random fashion, will then engage in a dialogue that will help them flush out the shared data element within their sets. Or alternatively, the dialogue will indicate to them that they have no shared element, so they ought to try again. A persistent adversary sharing information about the source data set from where the connecting parties choose their sets, will, in due course, zero in on the shared key. The connecting parties will have to use the brief time advantage to either convert the temporary key to a permanent one, or to finish their business with the shared key before their attacker is on to them. The latter is used by BitMint and others to effect payment of digital coins. After the coin moved from the payor to the payee there is no more advantage to the shared secret. See Ref [14]

Life on cyberspace hinges on the availability of fresh shared randomness. This challenge should attract heavy-duty innovation efforts. As witnessed today the lion share of innovation activity is channeled to quantum solutions, too little attention is paid to NESPAR in the form described and in alternative variety. Long range investors are looking at emerging ground-breaking solution avenues, involving cosmological phenomena, space curvature and brain activities.

Reference

1. G. Samid “Randomness as Absence of Symmetry” The 17th International Conference On Information & Knowledge Engineering (Ike'18: July 30 - August 2, 2018, Las Vegas, Usa)

2. "Innovation Solutions Protocol" https://innovationsp.net

3. G. Samid "Artificial Intelligence Assisted Innovation" https://www.intechopen.com/chapters/75159

4. Samid, G. “The Prospect of a New Cryptography: Extensive use of non-algorithmic randomness competes with mathematical complexity” https://eprint.iacr.org/2023/383

5. Samid, G. “Pattern Devoid Cryptography” https://eprint.iacr.org/2021/1510

6. Samid, G. "AU Resistant (AIR) Cryptography" The 25th International Conference on Artificial Intelligence (ICAI'23: July 24-27, 2023; Las Vegas, USA ©2023 IEEE

7. US Patent "RandoSol: Randomness Solutions" 11,394,530

8. IDQ https://www.idquantique.com/

9. Images Scientific Instruments, https://imagesco.com/

10. Bennett[1], Charles H., and Gilles Brassard. "AN UPDATE ON QUANTUM CRYPTOGRAPHY." Advances in Cryptology. Plenum Press,., 1984.

11. QuantLR https://quantlr.com/

12. US patent "Rock of Randomnress", 10,467,522

13. US Patent "Randomized Bilateral Trust (RABiT): Trust Building Connectivity for Cyber Space" 10,798,065

14. US Patent "The Digital Cash Register: a Comprehensive Layout for Cyber Banking and Digital Coins" 11741535