Verifiable Randomness | DOI:10.1145/3416959

Why Me? Shedding Light on Random Processes via Randomness Beacons

BY ALEJANDRO HEVIA AND CAMILO GÓMEZ

WE LIVE SURROUNDED by random processes, systems whose final outcome are typically unpredictable. When drawing a raffle, playing roulette at the casino, deciding who pays the restaurant bill, or even gambling in a poker game, we take part of a random process. Indeed, their intrinsic unpredictability is often what drives us to participate in them.

There are situations, however, where the result of these random processes may have serious consequences for those involved. Being selected for a tax audit, for example, can carry significant time and legal costs, which is why the selection process must be trustworthy. We accept a tax audit if we believe the random process was not manipulated in any way, that their final outcome was not influenced in an improper manner. But, if the results are potentially unpredictable, *any* result may be likely. How do we then prove that some specific outcome was not deliberately chosen? Solving this apparent paradox is the objective of a verifiable randomness service offered by the University of Chile.

Funded by a grant from the U.S. Department of Commerce and based on a proposal by the National Institute of Standards and Technology (NIST), Random UChile[a] provides verifiable randomness through a once-a-minute online pulse, a service that generates one 512-bit value every 60 seconds. This public random value is not only generated in a robust, unpredictable, and consistent way, but also the execution of the entire process is verifiable. The system, also known as a *randomness beacon*, has been designed to be transparent and open—the most recent value can always be verified by any external observer, yet the next output value remains unpredictable. This correct randomness generation is possible thanks to a variant of a cryptographic algorithm design by NIST.[2] The pulses generated by this algorithm are then added to a signed hash chain, preventing malicious manipulation of previously posted values.

The system relies on polling random data continuously from several entropy sources, both internal (TRNG hardware) and external (online) such as the Centro Sismológico Nacional (National Seismological Center) of Chile, which indicates the characteristics of Chilean earthquakes; the University of Chile's streaming radio, which transmits live shows and music; Twitter, which supplies a stream of randomly selected tweets in real time; and the Ethereum blockchain in the form of the hashed value of its last block. One can see the beacon as turning unpredictability (earthquake, tweets, or any of the others) into a guarantee of randomness of the output values. Indeed, some key innovations and cryptographic tools are needed for this to happen.

To foster the creation of new beacons, both the technical design of the Random UChile's beacon and the cryptographic analysis that supports the claim of verifiability, are being shared with the research community.[1]

Random UChile provides verifiable randomness through a once-a-minute online pulse, a service that generates one 512-bit value every 60 seconds.

Improving Transparency in Public Organizations

One key use case of verifiable randomness is ensuring the correctness of those processes run by government agencies, particularly those that rely on randomized algorithms for their decisions. Toward this end, Random UChile has collaborated with the Comptroller General (or Contraloría General de la República, CGR) in Chile, the public agency in charge of auditing the tax expenditure in the country. The CGR must periodically select, at random, who among authorities and public servants must be subject to an audit. Without verifiable randomness, the CGR was exposed to accusations of political persecution. In response, the CGR developed a pilot program to use Random UChile's verifiable randomness, where fair selection follows from the guarantees behind the beacon design.

Random UChile can also be used to actively prevent

[a] https://random.uchile.cl/en

The Random UChile group. Top row, from left: Juan Rojas, Constanza Csori, Sergio Miranda, Alejandro Hevia, and Cristián Rojas. Bottom row, from left: Franco Pino, Alejandro González, Camilo Gómez, and María José Vilches.

conflicts of interest that otherwise may encourage litigation or, worse, increase distrust on the underlying public processes. One such example is the use of Random UChile's verifiable randomness to ensure fair selection of judges for legal disputes. A pilot of the system is being considered for domain name registration controversies at the .CL administrator.

Impact on Elections Systems

The electoral voting system in Chile relies on the work of *vocales*, poll workers that are regular citizens chosen to perform as official workers during the days of the election. Unfortunately, in every election there are well-publicized controversies about the selection of poll workers. Even though they are supposed to be selected at random among all able citizens, often poll workers complain they have been selected for three, or more, elections in a row (although the law may allow such cases to occur under limited circumstances). The opacity of this process hurts democracy as partisan selection of these roles may open the door for corruption, or at least distrust on the election outcome. With the help of verifiable randomness, we can improve the transparency of the poll worker selection process and provide a way for citizens to confirm that every nomination was indeed fair and correct.

Another use of verifiable randomness comes from auditing elections. Recent concerns about the security and trustworthiness of electronic voting systems used in the U.S. and other countries have prompted the development of post-election audits. Risk-limiting audits[5] is a well-known technique to verify an election after it has completed without doing a total recount of the votes, only counting a much smaller random sample. The use of verifiable randomness not only makes it more efficient (no need of old-fashion dice throwing) but also more transparent at a larger scale-verification results can now be inspected online by interested citizens and organizations.

Using Randomness Beacons in Complex Systems

Verifiable randomness is difficult to obtain but extremely useful in the design of fair and transparent systems. Besides allowing transparency in new applications (for example, providing fully auditable statistical sampling for verifiable scientific experiments), verifiable public randomness is likely to become a public utility, a service upon which new and more sophisticated protocols and systems will be built. Examples include faster and more secure crypto-currencies,[3] lottery systems based on verifiable yet private randomness, and privacy-preserving verifiable data management systems based on secure multiparty computation.[4] Random UChile is contributing to the effort by actively developing prototypes for some of these systems.

Similar Projects

NIST's Interoperable Randomness Beacons project[b] has become one crucial driver in the creation of new beacons. It not only maintains a beacon implementation[c] and provides the official guidelines for implementing interoperable randomness beacons, but also explicitly seeks to "promote the deployment of Beacons by multiple independent organizations." Luckily, NIST's efforts seem to be paying off. Following the Random UChile project, the Inmetro Randomness Beacon[d] in Brazil has joined the cause of reliable public randomness. Since all three beacons follow the NIST reference,[2] applications built on top of any of these services have now plenty of choices to deposit their trust.

Yet trust is hard to gain. To achieve trustworthy public randomness without trusting on a single entity, Random UChile is also contributing to a global project called The League of Entropy,[e] a large-scale effort by several organizations across the world that seeks to produce a distributed randomness beacon. In this system, the public randomness is produced by the Drand Protocol,[6] which combines the output of all participants. The result is guaranteed correct and fair as long as at least one entity follows the rules and correctly contributes to the randomness. From local trust to global trust, the journey is just starting. C

[b] https://csrc.nist.gov/projects/interoperable-randomness-beacons

[c] https://beacon.nist.gov/home

[d] https://beacon.inmetro.gov.br/

[e] https://www.cloudflare.com/leagueofentropy/

References

1. Gómez, C., Hevia, A., Miranda, S., Riveros, E., and Rojas, C. Design and Implementation of a Verifiable Public Randomness Beacon. Technical Report, submitted 2020.
2. Kelsey, J., Brandão, L. T.A.N., Peralta, R. and Booth, H. A Reference for Randomness Beacons: Format and Protocol Version 2. Draft NISTIR 8213 Publication. May 2019. https://csrc.nist.gov/publications/detail/nistir/8213/draft.
3. Kiayias, A., Russell, A., David, B. and Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In *Proceedings of the Annual Intern. Cryptology Conf.* (2017). Springer, 357–388.
4. Lindell, Y. Secure Multiparty Computation (MPC). IACR Technical report 2020/300; https://eprint.iacr.org/2020/300
5. Norden, L., Burstein, A., Hall, L.J. and Chen, M. Post-election audits: Restoring trust in elections. Technical report. Brennan Center for Justice and Samuelson Law, Technology & Public Policy Clinic, 2007.
6. Syta, E., Jovanovic, P., Kogias, E.K., Gailly, N., Gasser, L., Khoffi, I., Fischer, M.J. and Ford, B. Scalable bias-resistant distributed randomness. In *Proceedings of the 2017 IEEE Symposium on Security and Privacy* (San Jose, CA, 2017). IEEE Press, 444–460.

Alejandro Hevia is an assistant professor in the Department of Computer Science at the University of Chile, Santiago.

Camilo Gómez is Random UChile Coordinator in the Department of Computer Science at the University of Chile, Santiago.