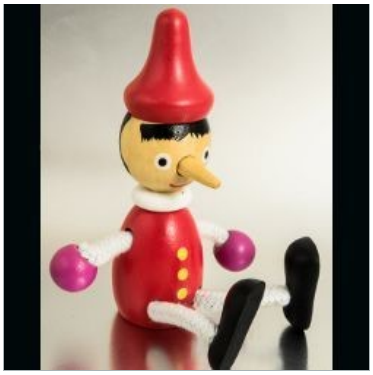
RESEARCH HIGHLIGHTS

Pinocchio: Nearly Practical Verifiable Computation

By Bryan Parno, Jon Howell, Craig Gentry, Mariana Raykova
Communications of the ACM, Vol. 59 No. 2, Pages 103-112
10.1145/2856449
Comments

PRINT

VIEW AS: SHARE: G+1



To instill greater confidence in computations outsourced to the cloud, clients should be able to *verify* the correctness of the results returned. To this end, we introduce Pinocchio, a built system for efficiently verifying general computations while relying only on cryptographic assumptions. With Pinocchio, the client creates a public evaluation key to describe her computation; this setup is proportional to evaluating the computation once. The worker then evaluates the computation on a particular input and uses the evaluation key to produce a proof of correctness. The proof is only 288 bytes, regardless of the computation performed or the size of the IO. Anyone can check the proof using a public verification key.

Crucially, our evaluation on seven applications demonstrates that Pinocchio is efficient in practice too. Pinocchio's verification time is a fixed 10 ms plus 0.4–15 µs per IO element: 5–7 orders of magnitude less than previous work[23]; indeed Pinocchio is the first general-purpose system to demonstrate verification cheaper than native execution (for some apps). The worker's proof effort is still expensive, but Pinocchio reduces it by 19×–60× relative to prior work. As an additional feature, Pinocchio allows the worker to include private inputs in the computation and prove that she performed the computation correctly without revealing any information about the private inputs to the client. Finally, to aid development, Pinocchio provides an end-to-end toolchain that compiles a subset of C into programs that implement the verifiable computation protocol.

Log in to Read the Full Article

Sign In

Sign in using your ACM Web Account username and

password to access premium content if you are an ACM member, Communications subscriber or Digital Library subscriber.

Username

Password

Forgot Password?

Need Access?

Please select one of the options below for access to premium content and features.

Create a Web Account

If you are already an ACM member, *Communications* subscriber, or Digital Library subscriber, please set up a web account to access premium content on this site.

Join the ACM

Become a member to take full advantage of ACM's outstanding computing information resources, networking opportunities, and other benefits.

Subscribe to Communications of the ACM Magazine

Get full access to 50+ years of CACM content and receive the print version of the magazine monthly.

Purchase the Article

Non-members can purchase this article or a copy of the magazine in which it appears.