Public-Key FHE: A Speculation

Andrew Poelstra

17 Jan 2014

This document assumes the existence of cryptography which has not (yet) been invented. It has some exciting conclusions. They are all vapour. Sorry.

Main. A *public-key fully homomophic encryption* (public-key FHE) scheme is a FHE scheme in which the key required to decrypt the output of a circuit is different from that required to encrypt the input. This allows the decryption key to become public, creating a circuit evaluator for which everyone can see (and verify) the output while only the holder of the encryption key knows what the input is.

Obviously the key derivation needs to depend on the circuit at hand, since otherwise the holders of the decryption key could simply swap out the circuit for one which reveals the input, defeating the whole system. Thus each keypair is tied to a single circuit.

Now, the transcript of an interaction with this system could act like a zero-knowledge argument for knowledge. But there is no reason to believe that verification would be faster than just evaluating the circuit with a replayed input (nor should we believe a succinct verifiable transcript could even be produced!) So this is not the point.

The point is: if the encryption function is surjective, or rather, the FHE circuit evaluator can act on any input, then it is possible to provide input to the FHE scheme which is (a) random and (b) unknowable except to the holder of the encryption key. If there is no holder, say, because the decryption key is some nothing-up-my-sleeve number, then we have created a system which evaluates its circuit with some random, unknowable input, and publishes the output.

This is a general solution to the "how can a coin creator provably destroy his keying material?" problem that we have for a lot of alt ideas. In particular, if the circuit under consideration is the Ben-Sasson SNARKing-key generator, then we have a way to generate zk-SNARKs for which nobody has the forging key!

(Of course, while we're assuming crypto that doesn't exist, we might as well just hypothesize a SNARK without a forging key ☺. But I think this idea is close enough to existing cryptosystems to be a viable research direction.)