Dream of iO obfuscation

Daniel J. Bernstein, Geoffroy Couteau,
Carl Ellison, Rémi Géraud, Becca Kreuter,
Tanja Lange, Kristin Lauter,
Tom Roeder, Mike Rosulek (guitar),
Eran Tromer (most of the lyrics).

Based on Californication by the Red Hot Chili Peppers.
Original music video: https://www.youtube.com/watch?v=YlUKcNNmywk

Suppose you have two circuits that
compute the same relation.
A polytime adversary
wants your implementation.
How do you transform
them to prevent discrimination?

There's a crypto primitive for any such occasion. It randomizes circuits by generic transformation. And this functionality is iO-obfuscation.

Using multilinear maps for
polytime construction.
Matrix product, circuits,
algebraic machination.

[Chorus:]
iO is born
a rare unicorn
Dream of iO-obfuscation
Dream of iO-obfuscation

Deniable encryption was a
former open question, iO
gives you most of crypto, also
DRM protection. It
gives you one way functions! (without
falsification) [KMNPR14].

A black box would be great but
we don't have the simulation [BGIRSBY01].
So we tailor puncturing
for every application.
There's no limitation
to the kinds of computation.

Finish 50 levels with a
month of computation.
But you'll have it ready just in
time for publication.

[Chorus:]
iO is born
a rare unicorn
Dream of iO-obfuscation
Dream of iO-obfuscation
Dream of iO-obfuscation
Dream of iO-obfuscation

Extractable one-way hash with auxiliary information is great for building SNARK proofs [BCCT12] but please do resist temptation. It's implausible: it contradicts the iO-obfuscation [BCPR14].

Will your protocol survive
the zero-tests combining?
Can you find an mmap that's
immune to zeroizing?

[Chorus:]
iO is born
a rare unicorn
Dream of iO-obfuscation
Dream of iO-obfuscation
Dream of iO-obfuscation
Dream of iO-obfuscation