A post-quantum fantasia

David Wakeham

June 17, 2020

The year is 2030. Neven's law — that the power of quantum computers increases *doubly exponentially* — turns out to hold, not because progress *within* a given computing paradigm is doubly exponential, but because the *paradigms shift* at an exponential rate. Expect the unexpected. This is what happens when you give the world's brightest technologists, engineers, and scientists a blank check, and say: "have fun!" It's like 50 Manhattan projects, 50 moon landings, 50 Bletchley parks, working on different ideas simultaneously, each seeing what sticks, sharing, stealing, adapting, and working it all into grand metasticky architectures. Shift happens.

But most of the shift is happening behind closed doors: in the security agencies and national labs of the creaking old world monoliths; in the snazzy facilities of Alphabet subsidiaries, IBM, Microsoft, and the umpteen bright-eyed startups they asborb for IP and talent at a doubly exponential rate; in the sprawling, military-grade subterranean compounds of the new world powers, seen only as curious geometries poking up from the desert in satellite imagery. So public perceptions lags.

It lags at a point three months old. Three months ago, quantum hardware seemed stuck, snagged on fundamental, parametrically annoying limitations which capped processors at 500 logical qubits[1] if you wanted coherence times[2] long enough to do anything interesting on them. But to break RSA-n,[3] you need $2n + 3$ logical qubits and enough coherence

[1] These are the quantum version of bits, 1s and 0s, used to perform the computation.

[2] How long a quantum computation can run before interactions with the environment destroy it.

[3] RSA is an ecnryption method which underlies a lot of internet security. The "key" tells you how strong the encryption is, with n bits, or RSA-n, corresponding to a key of size roughly 2^n.

to run n^3 gates.[4] With 500 qubits, you have no hope of cracking the 512-bit keys that a classical government cluster can break in seconds, so internet security, as well as VPNs, email servers, and public SSH, mostly continues to run on 4096 bit keys. The classical cipherpunks use 8192 bits or higher, and elliptic curves[5] for key generation. A tiny sliver of rich and suitably paranoid technocrats use the sub-performant post-quantum ciphersuites. No one else is optimistic enough to care.

But three months ago, behind closed doors, the industry got unstuck. On a little Caribbean island — purchased by Sidewalk Labs to make a "Country of the Future", climate-proofed, and quietly transformed into Google HQ — a computer scientist ate too much biryani and fell asleep on the couch. She dreamed about ostracods mating off the coast: thousands of tiny, luminescent shrimp constellated into a delicate fractal tangle, transmitting pulsed light along their coiled and counter-coiled axes... She woke up at 3 am, sketched some funny looking braids and symbols in a notebook on the coffee table, and leaned back into heavy, dreamless delta waves.

Over breakfast, she puzzled over the sketches again, and something big clicked. The AR chat with her lead started: "I had this weird dream about glowing shrimp and homotopy type theory..." Three haptic whiteboard sessions later, it became clear that, like Kekulé's hexaform dragon, an emissary of deep truth had visited her from the realm of sleep. With a few tweaks, they could make processors and coherence times as big and as long as they liked.

After a few months of Nevenian hardware breakthroughs (with Neven himself still kicking around, tickled by the progress), Project Ostracod cracked RSA-2048 and RSA-4096. Everyone at the organization knew; it was like a box that way, open and flat. But this thing needed to stay quiet. Perceptions needed to stay laggy. Keeping their goofy, overexcitable engineers from blabbing overexcitedly was an ongoing headache. There were NDAs, sure, but Google was founded on nothing if not the trust of machines, and Sidewalk discovered that controlling the interface to the outside world — via realtime, DeepFake censorship of outgoing AR, aka "DeepCensor" — was much more effective than any NDA. From the outside, you could see little slips and glitches appear-

[4] Gates are basic operations in the computer.

[5] A powerful method of encryption which is nevertheless vulnerable to large quantum computers.

ing, like ripples on the surface of a pond, but too smooth, too carefully managed, to learn the shape of the impinging pebble.

Back to the present. An autonomous, technoutopian city-state in the middle of the ocean owes no one anything, particularly if it controls half the intARnet. But military-industrial back scratching arrangements are the true axis of world power, and there is a pesky piece of legislation on the table in the US that will make business harder. Maybe, one temperate Saturday in April, a couple of athletic, middle-aged men go twitching at the North Tract in Fort Meade. Maybe, between kinglets and yellow-throated warblers, certain strategic disclosures are made. They exit at different times and take autocabs in opposite directions.

Days later, back in the Caribbean, the first man receives a VR of two hypermuscular unicorns vomiting rainbows as they jump over the moon; taste so poor it almost makes him feel nostalgic for the noughties. A string of bytes is stegged into one unicorn's left butt cheek. He retrieves the North Tract bytes, xors them and gets a message: "We can make this Alphabet anti-trust thing go away. Just give us these servers." Some 8192'ers with no NSA backdoor. A few Chinese-American hackers, would-be Jihadists, and pesky investigative journalists are exposed via "sophisticated side-channel attacks" or "social network analysis", according to the well-crafted press releases.

And that's where things should stop, just a little back-scratching before the usual round of responsible private disclosures, a grace period for updates, some deliberate leaks, then the circus of *Nature* papers and breathlessly stupid media coverage. But maybe things don't go as planned. After the disastrous Trumpire of the 20s, the economic war, the "intervention" in Belarus, and the collapse of the European alliance... these are geopolitically interesting times for the US. It's like a wounded, ravenous wolf, prowling the world stage, more dangerous than ever.

So, a few golf trips and nauseating VRs later: "We need you to sit on Ostracod for a while." Google's strategy AI (jokingly named Deep Blue) suggests obfuscatory non-compliance, not saying what you're not doing. It doesn't work. The stegs became thuggish: "So, I'm told we have some nuclear submarines on maneuver in the Gulf of Mexico. It would be a shame if somebody spoofed a Chinese sub in the Bahamas." What had they missed? Deep Blue suggests a conclusion the human has perhaps already reached: *the NSA has its own computer*. This new anti-trust legislation had been a convoluted way to check what Google was up to,

and if necessary, come down hard to maintain the strategic advantage. Say, by organizing tactical maneuvers in a nearby body of water.

Governments are like ant nests, full of bureaucrats mindlessly following the strongest pheromone trail. Maybe they read and faithfully implement the long-winded, usually unintelligible IT recommendations, for instance, the one asking them to update their TLS handshake settings. Then again, maybe they don't. The trail of custom, of legacy systems they understand and workflows than can move within, smells too strong. The NSA is now poking tiny signals intelligence holes in ant nests the world over. A Georgian oligarch or a Kazakh general sends an email on a compromised server. An older member of the Central Committee uses elliptic curves to encrypt a military communiqué.

Nothing major, perhaps, but feed enough pieces into the DARPA strategy AI, and it puts together a jigsaw puzzle of the assets and vulnerabilities of every major world power. Perhaps there is a clever way to disarm those Chinese space lasers, or rumors of ground troops in Azerbaijan, or impossible readouts from a new type of explosion at Ras Koh. And behind closed doors, the DARPA AI draws a tight window of nuclear opportunity with six targets and says: this should do the trick. The wolf smells blood. Shift happens.