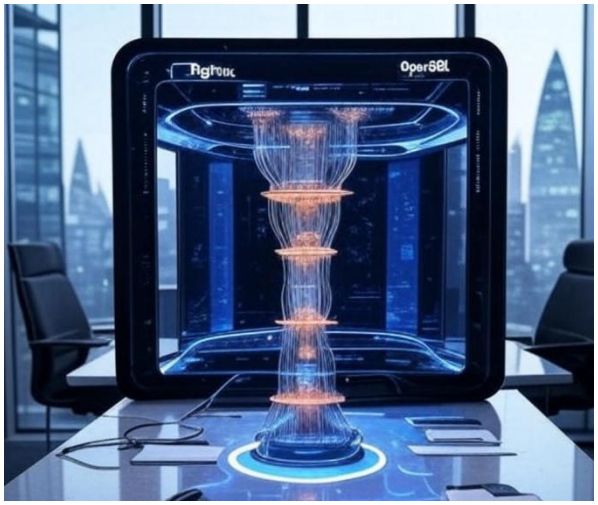
Travel in Time: Almost Free



(Not kidding. I am absolutely serious)

Important Disclaimers and Terms and Conditions
All views in this article are solely mine based on hands-on experience in my own laboratory.
My past or current employers may not necessarily agree with me or use my code.
You are free to use my code completely free – but you must not sell it.
Always test any code thoroughly in a non-production environment first.

Background

In boardrooms, conferences, and vendor meetings, you've likely heard about the so-called Quantum Threat. Some experts point to 2035, 2030, or even 2028 as deadlines to adopt Quantum-Safe algorithms. In my view, the topic is important, but some folks are turning "Post-Quantum Cryptography" into a cash grab. I don't blame them, as everyone has bills to pay and mouths to feed.

So, let's travel to the future, shall we? Imagine it's 2030. In this article, I'll show you how to make your webserver Quantum-Safe in September 2025. Tomorrow's challenge tackled today.

Proof-of-Concept: My own website

My own website at https://ztzt.dev uses nginx (pronounced Engine-X) as a webserver. So, I will take that as an example. If your business uses Apache, Caddy, IIS or something else – your IT team can do the research for you.

This **ONE LINE OF CODE** helps makes your nginx server Quantum Safe and enables Pure Post-Quantum, Hybrid, and Traditional Cryptography.

```
ssl_ecdh_curve
MLKEM1024:MLKEM768:MLKEM512:SecP384r1MLKEM1024:SecP256r1ML
KEM768:X25519MLKEM768:secp521r1:secp384r1:x448:secp256r1:x25519;
```

The first three parameters are curves for post-quantum cryptography (PQC). The next three are hybrid cryptography curves. The last five are from traditional curves.

There is a method in my madness. I have ordered the curves by PQC – hybrid – traditional sets and within each set I ordered them in decreasing order of security.

As a result, your webserver remains compatible with ultra-modern, modern, and older browsers and select the most secure option for key exchange.

Of course, it is possible to add / subtract curves to my code – depending on new algorithms that NIST may approve or drop in the future. **But this one-line code should be good enough at least for the next five years until 2030**. Once everyone starts using PQC we can drop both hybrid as well as traditional curves.

Potential Difficulties?

To make your infrastructure Quantum-Safe, you need to keep your software up to date and apply relevant patches. Here's what I use:

- **Webserver**: Nginx Version 1.29.1 released 13 August 2025.
- **Cryptographic Library**: OpenSSL Version 3.5.2 released 5 August 2025.
- **Browsers**: Chrome, Edge, Brave, and Chromium, all updated to their latest versions.

If your systems are outdated and you've accumulated technical debt, I have a friend's advice to you. Prioritise fixing those issues before spending on consultants for the Quantum Threat.

Also, ideally, you should not only reconfigure your server (which is straightforward) but also obtain Quantum-Safe SSL certificates for your website.

What's the Difference Between Reconfiguring Your Webserver and Getting a New Certificate?

The one-line code I shared focuses on "Quantum-Safe Key Exchange," which doesn't require a new certificate. Key Exchange is the biggest vulnerability to quantum computers, so this step already addresses the primary threat.

A Quantum-Safe SSL Certificate, on the other hand, is signed by the issuer using a Quantum-Safe Digital Signature. This provides extra assurance about the certificate's authenticity.

How Much Does This Cost?

There are two costs to consider for making your website Quantum-Safe:

1. **Server Configuration**: The one-line code I shared? Completely free! You're welcome.

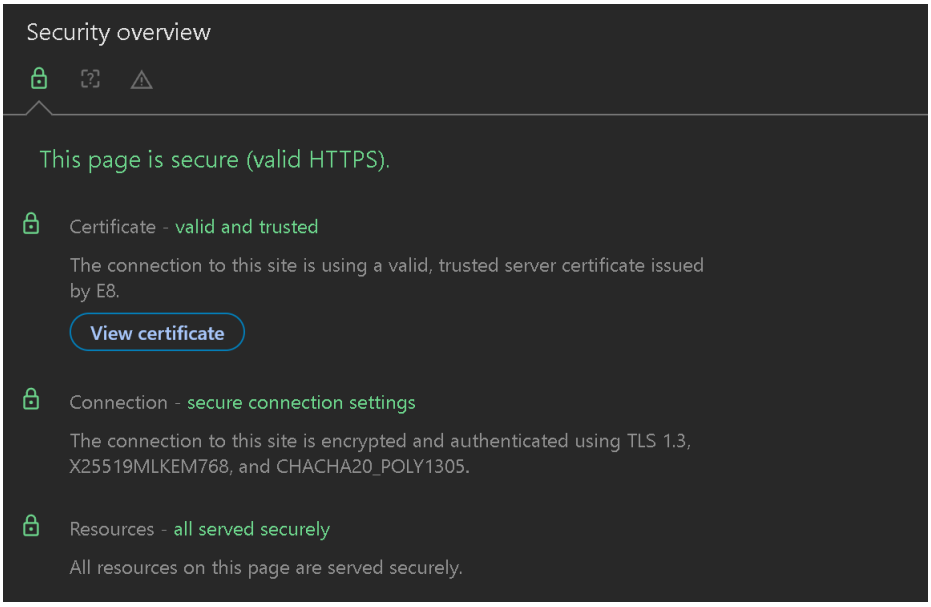
2. **TLS Certificate**: If you use Let's Encrypt certificates (like I do), they're free. However, if you opt for paid certificates, costs vary depending on the vendor. One vendor currently charges around USD 600 per domain per year, which I won't name. I wouldn't pay more than USD 100, but that's your call.

   If you can afford to spend that much, go for it. But in a few years, Let's Encrypt may offer Quantum-Safe certificates for free, so consider waiting.

Is This Too Good to Be True?

As Master Yoda would say “Snake Oil – I sell not”. 😊

I’ve implemented this code on https://ztzt.dev, and I can prove it works. The Chrome browser already uses Quantum-Safe cryptography for connections, as shown by the term “X25519MLKEM768” in my setup (see attached image). This confirms a hybrid cryptographic connection.



In short, my friends, you’ve just time-travelled to a Quantum-Safe future at almost zero cost.

About Me

As a specialised researcher and expert in Applied Cryptography, I am passionate about helping your journey to quantum safety. A few months ago, I created the world’s first online platform (https://kyber.club) to generate NIST FIPS compliant PQC key pairs. You all have benefited from over 30,000 key pairs already. Totally free.

How Can I Help Your Journey?

My DMs are always open for a discussion and collaboration in my personal capacity.

Santosh Pandit

London, 7 September 2025