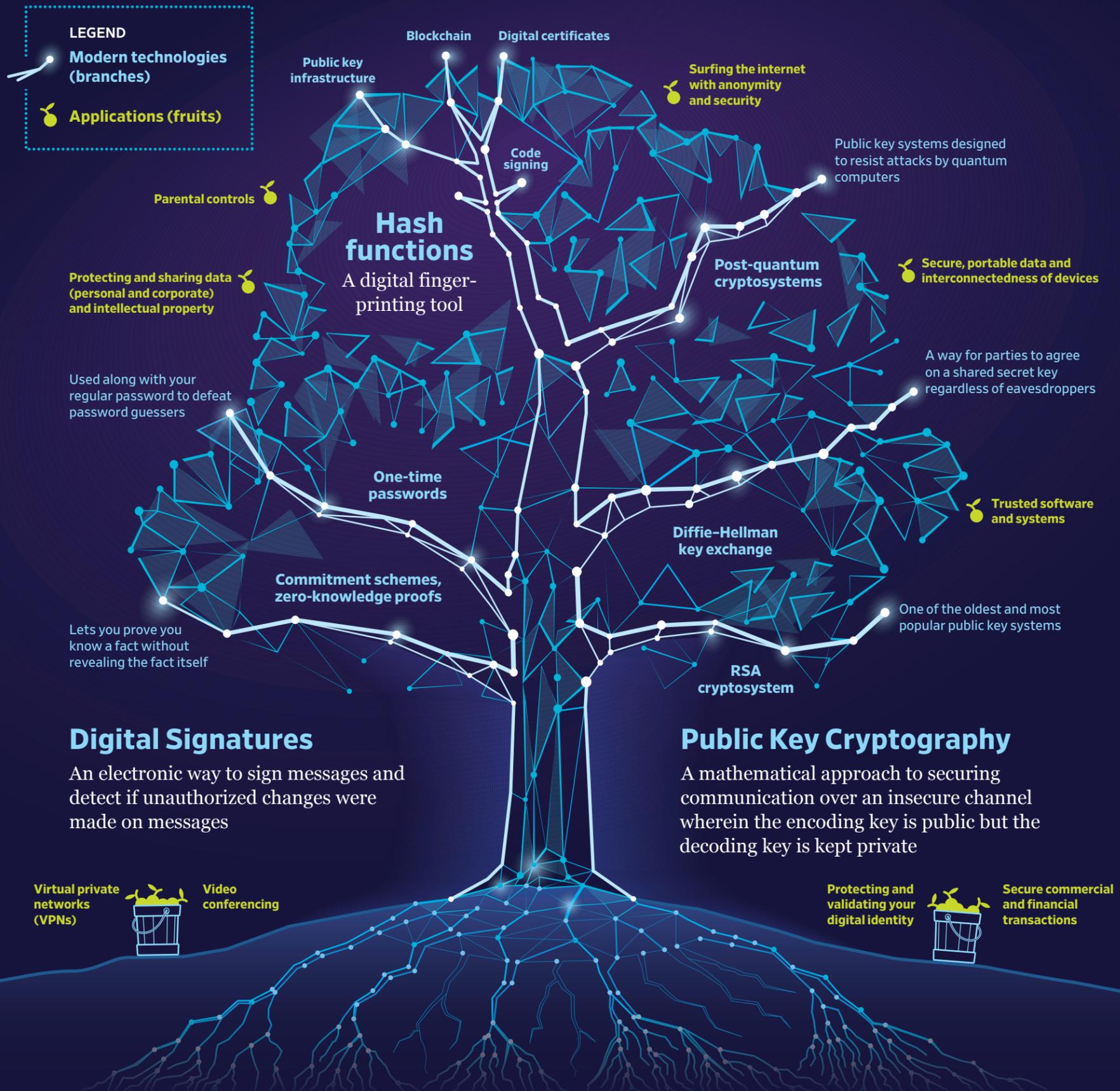


The Mathematics of Internet Security

The internet is a transformative network that is an integral part of our daily lives — but, unfortunately, its use involves many security challenges. From roots in abstract mathematics, some new and some very old, a tree of technologies (cryptosystems and authentication schemes) has grown to meet evolving threats. As users of the internet, we routinely enjoy this tree's fruits and may not appreciate their origins.

Mathematics helps protect against evolving threats

- 
Bots and fake accounts
- 
Corporate espionage
- 
Malicious websites
- 
Financial fraud and hacking
- 
Identity theft
- 
Intellectual property theft
- 
Malware or spyware
- 
Phishing, trojans and spam
- 
Stolen medical records



Intractable computations

Cryptosystems aim to force an eavesdropper to solve intractable problems that often involve large numbers while the intended users simply verify known solutions. These intractable problems include finding the shortest vector in a lattice (1998) and decoding random linear codes (1978).

Algebra on elliptic curves

An elliptic curve over a finite field is a simplified solution set to a polynomial equation. In the 1980s, it was noticed that translating cryptographic algorithms into this setting allowed the use of smaller numbers while achieving the same level of security.

Concentration inequalities

Concentration inequalities, such as Bernstein's Inequalities (c. 1930), are used to analyze the security of cryptosystems. These limit the chances that a random variable, a quantity that changes upon repeated measurements, is significantly different than what is expected.

Computational number theory

This field studies ways to use computers to solve arithmetic problems. The RSA cryptosystem uses the unique prime factorizations of numbers (c. 300 BCE) and Euler's Theorem (1763), and its security relies on the obstacle of identifying such factors for select large numbers.

High-dimensional geometry

Structured collections of points called lattices are useful settings for cryptosystems and problems in cryptology. Lattices in high dimensions were used to create the first, proof-of-concept system for homomorphic encryption (2009).

[INTERNET SECURITY IS ROOTED IN MATHEMATICS]