Summary of asymmetric attack vectors

1. “Nice” EC params

Let’s first establish a definition for the *key generator with a backdoor*. We can define this as a key generator with the following properties:

- Produces keys are looking *normal*, which means that they are indistinguishable from keys from a legitimate source by anyone else except the attacker.
- Still allows the attacker to crack the encryption (in whichever sense is plausible) faster than existing general-purpose methods.

The vector here is to design such a set of EC parameters, that keys generated for that parameters would comply to the properties established above.

This topic arises from NIST using some unexplained parameters (random seeds) when they were designing their recommended curves.

2. Space-time tradeoff

As described in the proposal, we can utilise space-time tradeoff to speed up computations required to crack the scheme. This can come as some sort of rainbow table to optimize some processes which are cyclic.

3. Biased RNG

To generate different ciphertexts and different keys every time, cryptographic schemes employ PRNGs, security of which is crucial to security of these schemes. Security of a PRNG here means that it should not be feasible to somehow work out the internal state of the PRNG given its previous outputs.

Following the Dual EC DRBG scandal, we can try to develop a random generator

with a backdoor.