for the extension degree k to be small. Essentially the only elliptic curves for which k is small are the so-called "supersingular" elliptic curves, the most familiar examples of which are curves of the form $y^2 = x^3 + ax$ when the characteristic p of $\mathbf{F}_q$ is $\equiv -1 \pmod 4$, and curves of the form $y^2 = x^3 + b$ when $p \equiv -1 \pmod 3$. The vast majority of elliptic curves, however, are nonsupersingular. For them, the reduction almost never leads to a subexponential algorithm (see my paper in *Journal of Cryptology* cited in the references).

Thus, a key advantage of elliptic curve cryptosystems is that no subexponential algorithm is known that breaks the system, provided that we avoid supersingular curves and also curves whose order has no large prime factor.

We now describe analogs of the public key systems in §IV.3 based on the discrete log problem on an elliptic curve E defined over a finite field $\mathbf{F}_q$.

Analog of the Diffie–Helman key exchange. Suppose that Aïda and Bernardo want to agree upon a key which will later be used in conjunction with a classical cryptosystem. They first publicly choose a finite field $\mathbf{F}_q$ and an elliptic curve E defined over it. Their key will be constructed from a random point P on the elliptic curve. For example, if they have a random point $P \in E$, then taking the x-coordinate of P gives a random element of $\mathbf{F}_q$, which can then be converted to a random r-digit base-p integer (where $q = p^r$) which serves as the key to their classical cryptosystem. (Here we're using the word "random" in an imprecise sense; all we mean is that its choice is arbitrary and unpredictable in a large set of admissible keys.) Their task is to choose the point P in such a way that all of their communication with one another is public and yet no one other than the two of them knows what P is.

Aïda and Bernardo first publicly choose a point $B \in E$ to serve as their "base." B plays the role of the generator g in the finite-field Diffie–Hellman system. However, we do not want to insist that B be a generator of the group of points on E. In fact, the latter group may fail to be cyclic. Even if it is cyclic, we want to avoid the effort of verifying that B is a generator (or even determining the number N of points, which we do not need to know in what follows). We would like the subgroup generated by B to be large, preferably of the same order of size as E itself. This question will be discussed later. For now, let us suppose that B is a fixed publicly known point on E whose order is very large (either N or a large divisor of N).

To generate a key, first Aïda chooses a random integer a of order of magnitude q (which is approximately the same as N), which she keeps secret. She computes $aB \in E$, which she makes public. Bernardo does the same: he chooses a random b and makes public $bB \in E$. The secret key they use is then $P = abB \in E$. Both users can compute this key. For example,