in Remark 6.20. Unfortunately, since Alice must compute the difference $C_2 - n_A C_1$, she needs the correct values of both the x-and y-coordinates of C_1 and C_2. (Note that the points $C_2 - n_A C_1$ and $C_2 + n_A C_1$ are quite different!) However, the x-coordinate of a point determines the y-coordinate up to change of sign, so Bob can send one extra bit, for example

$$\text{Extra bit} = \begin{cases} 0 & \text{if } 0 \le y < \frac{1}{2}p, \\ 1 & \text{if } \frac{1}{2}p < y < p \end{cases}$$

(See Exercise 6.16.) In this way, Bob needs to send only the x-coordinates of C_1 and C_2, plus two extra bits. This idea is sometimes referred to as *point compression*.

6.4.3 Elliptic Curve Signatures

The *Elliptic Curve Digital Signature Algorithm* (ECDSA), which is described in Table 6.7, is a straightforward analogue of the digital signature algorithm (DSA) described in Table 4.3 of Sect. 4.3. ECDSA is in widespread use, especially, but not only, in situations where signature size is important. Official specifications for implementing ECDSA are described in [6, 142]. (See also Sect. 8.8 for an amusing real-world implementation of digital cash using ECDSA.)

In order to prove that ECDSA works, i.e., that the verification step succeeds in verifying a valid signature, we compute

$$\begin{aligned} v_1 G + v_2 V &= d s_2^{-1} G + s_1 s_2^{-1}(sG) \\ &= (d + s s_1) s_2^{-1} G \\ &= (e s_2) s_2^{-1} G \\ &= eG \in E(\mathbb{F}_p). \end{aligned}$$

Hence

$$x(v_1 G + v_2 V) \bmod q = x(eG) \pmod q = s_1,$$

so the signature is accepted as valid.

6.5 The Evolution of Public Key Cryptography

The invention of RSA in the late 1970s catapulted the problem of factoring large integers into prominence, leading to improved factorization methods such as the quadratic and number field sieves described in Sect. 3.7. In 1984, Hendrik Lenstra Jr. circulated a manuscript describing a new factorization method using elliptic curves. Lenstra's algorithm [75], which we describe in Sect. 6.6, is an elliptic analogue of Pollard's $p - 1$ factorization algorithm

Public parameter creation	
A trusted party chooses a finite field $\mathbb{F}_p$, an elliptic curve $E/\mathbb{F}_p$, and a point $G \in E(\mathbb{F}_p)$ of large prime order q.	
Samantha	**Victor**
Key creation	
Choose secret signing key $1 < s < q-1$. Compute $V = sG \in E(\mathbb{F}_p)$. Publish the verification key V.	
Signing	
Choose document d mod q. Choose random element e mod q. Compute $eG \in E(\mathbb{F}_p)$ and then, $s_1 = x(eG) \bmod q$ and $s_2 \equiv (d + ss_1)e^{-1} \pmod q$. Publish the signature (s_1, s_2).	
Verification	
	Compute $v_1 \equiv ds_2^{-1} \pmod q$ and $v_2 \equiv s_1 s_2^{-1} \pmod q$. Compute $v_1G + v_2V \in E(\mathbb{F}_p)$ and verify that $x(v_1G + v_2V) \bmod q = s_1$.

Table 6.7: The elliptic curve digital signature algorithm (ECDSA)

(Sect. 3.5) and exploits the fact that the number of points in $E(\mathbb{F}_p)$ varies as one chooses different elliptic curves. Although less efficient than sieve methods for the factorization problems that occur in cryptography, Lenstra's algorithm helped introduce elliptic curves to the cryptographic community.

The importance of factorization algorithms for cryptography is that they are used to break RSA and other similar cryptosystems. In 1985, Neal Koblitz and Victor Miller independently proposed using elliptic curves to create cryptosystems. They suggested that the elliptic curve discrete logarithm problem might be more difficult than the classical discrete logarithm problem modulo p. Thus Diffie–Hellman key exchange and the Elgamal public key cryptosystem, implemented using elliptic curves as described in Sect. 6.4, might require smaller keys and run more efficiently than RSA because one could use smaller numbers.

Koblitz [67] and Miller [88] each published their ideas as academic papers, but neither of them pursued the commercial aspects of elliptic curve cryptography. Indeed, at the time, there was virtually no research on the ECDLP, so it was difficult to say with any confidence that the ECDLP was indeed significantly more difficult than the classical DLP. However, the potential of what became known as elliptic curve cryptography (ECC) was noted by Scott