

A.2.1 Generating Alternative P, Q

The curve **shall** be one of the NIST curves from FIPS 186-3 that is specified in Appendix A.1 of this Recommendation, and **shall** be appropriate for the desired *security_strength*, as specified in Table 4, Section 10.3.1.

The points P and Q **shall** be valid base points for the selected elliptic curve that are generated to be verifiably random using the procedure specified in ANS X9.62. The following input is required for each point:

An elliptic curve $E = (F_p, a, b)$, cofactor h , prime n , a bit string *domain_parameter_seed*¹, and hash function **Hash()**. The curve parameters are given in Appendix A.1 of this Recommendation. The *domain_parameter_seed* **shall** be different for each point, and the minimum length m of each *domain_parameter_seed* **shall** conform to Section 10.3.1, Table 4, under “Seed length”. The bit length of *domain_parameter_seed* may be larger than m . The hash function **shall** be SHA-512 in all cases.

The *domain_parameter_seed* **shall** be different for each point P and Q . A domain parameter seed **shall not** be the seed used to instantiate a DRBG. The domain parameter seed is an arbitrary value that may, for example, be determined from the output of a DRBG.

If the output from the ANS X9.62 generation procedure is “failure”, a different *domain_parameter_seed* **shall** be used for the point being generated.

Otherwise, the output point from the generate procedure in ANS X9.62 **shall** be used.

[EBB: Does this take care of the required relationship $Q = aP$ that is stated in Section 10.3?]]

A.2.2 Additional Self-testing Required for Alternative P, Q

To insure that the points P and Q have been generated appropriately, additional self-test procedures **shall** be performed whenever the instantiate function is invoked. Section 11.3.1 specifies that known-answer tests on the instantiate function be performed prior to creating an operational instantiation. As part of these tests, an implementation of the generation procedure in ANS X9.62 **shall** be called for each point (i.e., P and Q) with the appropriate *domain_parameter_seed* value that was used to generate that point. The point returned **shall** be compared with the corresponding stored value of the point. If the generated value does not match the stored value, the implementation **shall** halt with an error condition.

¹ Called a *SEED* in ANS X9.62.

one page
12 - 5/3/2006

E.1.4 Potential Bias Due to Modular Arithmetic for Curves Over F_p

Given an integer x in the range 0 to 2^N-1 , the r^{th} bit of x depends solely upon whether $\left\lfloor \frac{x}{2^r} \right\rfloor$ is odd or even. If all of the values in this range are sampled uniformly, the r^{th} bit will be 0 exactly $\frac{1}{2}$ of the time. But if x is restricted to F_p , i.e., to the range 0 to $p-1$, this statement is no longer true.

By excluding the $k = 2^N - p$ values $p, p+1, \dots, 2^N - 1$ from the set of all integers in Z_N , the ratio of ones and zeroes in the r^{th} bit is altered from $2^{N-1} / 2^{N-1}$ to a value that can be no smaller than $(2^{N-1} - k) / 2^{N-1}$. For all the primes p used in this Recommendation, $k/2^{N-1}$ is smaller than 2^{-31} . Thus, the ratio of ones and zeroes in any bit is within at least 2^{-31} of 1.0.

To detect this small difference from random, a sample of 2^{64} outputs is required before the observed distribution of 1's and 0's is more than one standard deviation away from flat random. This effect is dominated by the bias addressed below in section E.2.

one page

9 -

one page

10 - 5/3/2006