Lily Chen
February 14, 2006

NIST Comments on X9.82 Part 3

The ballot version of X9.82 part 3, February of 2006" is well written. It is suggested to approve. The following are minor editorial comments.

1. Page 7, section 1, replace "Part 1 should be read for a basic understanding of this Standard before reading Part 3. This part of ANSI X9.82 defines techniques for the generation of random bits using deterministic methods" with "This part, Part 3, of ANSI X9.82 defines techniques for the generation of random bits using deterministic methods. Part 1 should be read for a basic understanding of this Standard before reading Part 3"
2. Page 11, section 6, paragraph 5, replace "While a DRBG mechanism may conform to this part of the Standard (i.e., Part 3), an implementation cannot achieve the properties specified in Part 1 unless the entropy input source is included as specified in Part 4." with "While a DRBG mechanism may conform to this part of the Standard (i.e., Part 3), an implementation cannot achieve the properties specified in Part 1 unless the entropy input source, as specified in Part 4, is included."
3. Page 21, item 6, the last word "key" should be "keys".
4. Page 21, item 7, a and b, in two places, replace "*security_strength*/2" with "1/2 *security_strength*".
5. Page 25, the item 2 in the "Input from a consuming application for instantiation", the second line, in "by a the consuming application", "a" should be deleted".
6. Page 25, the item 2 in "required information …" replace "*security_strength*/2" with "1/2 *security_strength*".
7. For "prediction resistance" alternative words were used, for example, supported, provided, performed, etc. It is suggested to make a global search to make sure that they are used consistently with the scenario". For example,
    a. In page 26, it was said that "If *prediction_resistance_flag* is set, and prediction resistance is not supported, then return an **ERROR_FLAG**."
    b. In page 29, it was said that "If prediction resistance is never provided, then the *prediction_resistance_request* input parameter and step 5 of the generate process may be omitted,"
    c. In page 30, it was said that "If prediction resistence is alwasy performed, …"
8. Page 37, title of section, replace "10.2.2. HMAC_DRBG(…)" with "10.2.2. HMAC_DRBG".
9. Page 40, 3rd line from the bottom, replace "Key_old, V_old" with "Key, V".
10. Page 44, the 4th line from the bottom, replace "10.5.2" with "10.5.3".
11. Page 51, in the title of 10.3.2.2.5.1. add a space between "Bits" and "When".
12. Page 52, in the title of 10.3.2.2.5.2. add a space between "Bits" and "When".
13. Section 10.4.2.1, it is suggested to add one paragraph before introducing Dual_EC_DRBG to briefly and informally explain the concepts of finite field, elliptic curve, and a point on a curve. Especially, it shall add one sentence to explain "scalar multiplication". Then refer to Annex A for details. Otherwise, it will be quite difficult to read. NSA will consider
14. Page 59, the bottom line, GP(p) should be replaced with Fp to be consistent with other places (for example, in page 69, Annex A.1.1.).
15. Page 61, item 5, "s" and "t" are both binary strings. But in item 6 and 7, inside s = φ (x(t *P)) and r = φ (x(s *P)), s and t are both integers. Therefore, a conversion is indicated. It may need to state explicitly for this step. An also the conversion of r, from an integer in item 7 to a binary string in item 8. In page 59, the three representatives and their conversions are defined. Maybe at the same place, it shall be mentioned that in the

following of this document, we may use the same symbol for different formats without explicitly including the conversion.

16. Page 71, the last paragraph may be quoted directly from X9.62. But it needs to be said so. Otherwise, Fq shall be replaced with Fp.
17. Page 71, the last paragraph, "in Annex A" should be replaced with "in Annex A of X9.62".
18. Page 102, Annex G (Informative) Bibliography, Among the 9 references, only [8] and [9] were quoted in the context. It is suggested to delete [1] to [7]. Editor's choice
19. Page 102, Annex G (Informative) Bibliography, in [9], delete "[Sharplinski]" and ";{eelmaha, ignore}@isc.mq.edu.qu". It should provide where the paper (or book) is published at which year.