An Approach to Shorten Digital Signature Length

Nikolay A. Moldovyan

Abstract

A new method is proposed to design short signature schemes based on difficulty of factorizing a composite number $n = qr$, where q and r are two large primes. Using the method new digital signature schemes (DSS) with the 320-bit and 240-bit signature size are developed. The characteristic feature of the 240-bit signature DSS is the use of "three-level" verification equation, for example, $R = \beta^{\alpha^{kgH} \bmod n} \bmod p$, where $k = \left(R^{\alpha^{g} \bmod n} \bmod p\right) \bmod \delta$. The (k, g) signature corresponds to the H hash value and represents a pair of natural numbers having the size of 80 and 160 bits, respectively. The δ modulus is a prime number. The public key is the triple (α, β, p), where $p = 2n + 1$ is prime, β is the q order element modulo p, α is the γ order element modulo q. The private key is represented by the pair of two prime numbers (q, γ).

1 Introduction

One of important practical problems is developing digital signature schemes (DSS) with short signature length [2, 6]. In general the signature length depends on the required security level of the DSS, that can be estimated as number of group operations required to forge a signature. In this paper the signature length is compared for different DSS in the case of minimum security level that can be estimated at present as 2^{80} operations. The RSA and Rubin's DSS based on factorization problem use the 1024-bit signature length [3]. The DSA standard and Schnorr's DSS based on difficulty of finding discrete logarithm modulo

large prime number provide comparatively short signatures having the 320-bit length and providing the same security level [8]. The ECDSA standard also requires the use of the 320-bit signature size [1]. Recently a DSS with 171-bit signature length has been developed using Weil paring on elliptic curves [2].

In present paper we consider some ways to reduce the signature length in DSS based on difficulty of factorization of a composite number n calculated as production of two large primes q and r. In this investigation we propose some new designs of the DSS based on difficulty of factorization problem, which allows one to reduce the signature length up to 240 bits. In Section 2 we propose some short signature designs based on the signature formation mechanism described in [4]. The DSS with the 320-bit and 240-bit signature length and composite private modulus $\gamma = \gamma'\gamma''$, where γ' and γ'' are primes, are presented. Section 3 introduces DSS with 240-bit signature length and prime private modulus γ. Section 4 concludes the paper. We use notation $|x|$ to denote the length of the binary representation of the x value.

2   Short signatures from factorization problem

The well known cryptosystem RSA [7] is based on calculation modulo n that is a product of two randomly chosen prime numbers r and q: $n = rq$. The public key is represented by a pair of numbers (e, n), and the private key is a number d, which is calculated using the following formula: $ed \bmod \varphi(n) = 1$, where $\varphi(n) = (r - 1)(q - 1)$ is Euler phi function of n. Security of this system is based on difficulty of calculating d while $\varphi(\mathrm{n})$ is an unknown value. The $\varphi(\mathrm{n})$ value can be easily calculated after factorization of the modulus n, therefore divisors of n have to be kept in secret (or to be annihilated after the e and d keys have been generated). The signature corresponding to a plaintext M is a value S, which satisfies the following verification equation: $S^e \bmod n = H$, where H is the hash function value corresponding to the message to be signed. The signature generation equation is the following one: $S = H^d \bmod n$. In RSA the signature length is approximately equal to the n modulus length. At present in different practical appli-

cations the used n modulus has the length $|n| = 1024$ bits or more (this value corresponds to the mentioned above minimum security level).

To reduce the signature length in the case of DSS based on the factorization problem we use the novel signature formation mechanism [4] that can be applied while developing DSS with two-element signature denoted as (k, g). The mechanism is characterized in using a two-element public key with the structure (n, α), where α is the γ order element modulo n and in solving a system of two congruences (or one equation and one congruence) while generating signature. The private key is γ.

Some internal relation between the α and n values provides potentially some additional possibilities to factorize modulus n. This defines special requirements to the α element of the public key [4]. One should use composite γ, i. e. $\gamma = \gamma'\gamma''$, where $\gamma'|r - 1$, $\gamma''|q - 1$, $\gamma'' \nmid r - 1$ and $\gamma' \nmid q - 1$. To choose the size of the γ value we should take into account that the α value can be used to factorize the n modulus calculating $\gcd(\alpha^i \bmod n - 1, n)$ for $i = 1, 2, \ldots, \min\{\gamma', \gamma''\}$. Therefore we should use the 80-bit values γ' and γ''. Thus, for γ we get the following required length: $|\gamma| = 160$ bits.

A secure variant of the DSS with the 320-bit signature length is described by the following verification equation:

$$k - g = \left(\alpha^{kgH} \bmod n\right) \bmod \delta, \tag{1}$$

where $\delta \neq \gamma$ is a specified prime number and H is the hash value of the signed message. The signature generation is performed as follows: 1) generate a random number U and calculate $Z = \left(\alpha^U \bmod n\right) \bmod \delta$; 2) solve simultaneously equation $k - g = Z$ and congruence $kgh \equiv U \bmod \gamma$.

The solution gives signature elements k and g:

$$g = -\frac{Z}{2} \pm \sqrt{\frac{Z^2}{4} + \frac{U}{H}} \bmod \gamma \quad \text{and} \quad k = Z + g. \tag{2}$$

The signature elements have the size $|k| \approx |g| \approx |\gamma| \approx 160$ bits. To reduce the signature size we propose the DSS based on the following

pair of verification equations:

$$R = \alpha^{kgH} \bmod n, \quad \text{and} \quad k = (R\alpha^g \bmod n) \bmod \delta, \qquad (3)$$

where $|\delta| = 80$ bits. The signature is generated as follows:

    i) select at random U $(1 < U < \gamma)$;

    ii) calculate the first signature element $k = \left(\alpha^U \bmod n\right) \bmod \delta$;

    iii) calculate the second signature element

$$g = \frac{U}{kH + 1} \bmod \gamma. \qquad (4)$$

Thus, we have a 240-bit signature: $|k| + |g| \approx |\delta| + |\gamma| = 80 + 160 = 240$ bits. The way used in the last DSS to reduce the k element length resembles the method used earlier to reduce the signature length to the 240-bit value in the DSA standard [5]. The need to calculate $(kH+1)^{-1}$ modulo γ defines the interest in constructing DSS with prime value γ.

In the next section we consider the DSS design that provides possibility to use prime private key element γ.

3   A 240-bit signature DSS with prime γ

The design idea of the DSS with prime γ consists in hiding the modulus to which the γ order belongs. If it is so, then one can use a prime modulus q, for which the α element is a generator of the γ order group: $\alpha^\gamma \equiv 1 \bmod q$. Implementation of this idea is connected with the following contradiction. The signature should be calculated modulo q that is secret. The verification equation should allow one to check the result of such calculation without direct use of the secret modulus q. In the DSS described below the contradiction is solved using the following "three-level" verification equations:

$$R = \beta^{\alpha^{kgH} \bmod n} \bmod p \quad \text{and} \quad k = \left(R^{\alpha^g \bmod n} \bmod p\right) \bmod \delta \qquad (5)$$

where $p = 2n + 1$ is prime, n is product of two 512-bit primes q and r $(n = rq)$, β is the q order element modulo p, and α is a γ order element

modulo q. The prime modulus δ is a 80-bit value. The private key is represented by the (q, γ) pair, where γ is an 160-bit prime number ($\gamma | q - 1$). The public key is triple (α, β, p). The (k, g) signature corresponds to the H value and represents two natural numbers having the length $|k| = 80$ bits and $|g| = 160$ bits.

The signature generation procedure includes solving the system of two congruences: $t + g \equiv U \mod \delta$ (i) and $t \equiv kgH \mod \delta$ (ii), where $U < \gamma$ is selected at random, the signature element k is calculated using formula $k = \left(\beta^{\alpha^U \mod q} \mod p \right) \mod \delta$, t is an auxiliary unknown. The solution of this system gives the formula (4) for calculation of the signature element g.

The proof that signature verification works is as follows. Suppose we have a valid signature (k, g) corresponding to the H hash value. Taking into account that α is the γ order element modulo q and substituting the k and g values in the verification equation we get:

$$R = \beta^{\alpha^{kgH} \mod n} \mod p = \beta^{\alpha^{kgH} \mod q} \mod p = \beta^{\alpha^{\frac{kHU}{kH+1}} \mod q} \mod p$$

and

$$k' = \left(R^{\alpha^g \mod n} \mod p \right) \mod \delta = \left(R^{\alpha^g \mod q} \mod p \right) \mod \delta =$$

$$= \left(\left(\beta^{\alpha^{\frac{kHU}{kH+1}} \mod q} \mod p \right)^{\alpha^g \mod q} \mod p \right) \mod \delta =$$

$$= \left(\beta^{\alpha^{\frac{kHU}{kH+1} + \frac{U}{kH+1}} \mod q} \mod p \right) \mod \delta = \left(\beta^{\alpha^U \mod q} \mod p \right) \mod \delta.$$

Since $k' = k$ the signature verification result is positive, i.e. the verification equations work correctly.

A possible attack on this scheme is to find value $X = \log_\beta(R)$ (mod p) and calculate q as a divider of the value $\left(\alpha^{kgH} \mod n \right) - X$. Then the secret γ can be determined dividing $q - 1$. Due to the large value of q this attack is computationally infeasible. Another attack is to find the value $X' = \log_\alpha \left(\alpha^{kgH} \mod n \right)$ (mod n) and then to calculate γ as one of dividers of the value $kgH - X'$. The last attack defines the

following requirement to the α value: *the ϵ order of α modulo n should be large ($|\epsilon| \geq 160$ bits).* For example, we can easily generate the α value the order of which modulo n is $\epsilon = \gamma(r-1)$. If this requirement is satisfied, then the second attack is also computationally infeasible.

4 Conclusion

Using a novel mechanism of the signature generation we have proposed new short signature schemes providing the minimum security level (2^{80} group operations) with signatures having the size of 320 bits and 240 bits. We have presented two 240-bit signature DSS, one with composite private key element γ and the other one with prime γ. Using prime γ we reduce the $\Pr(\gcd(\gamma, kH+1) \neq 1)$ probability from $\gamma'^{-1} + \gamma''^{-1}$ to γ^{-1} (if $\gcd(\gamma, kH+1) \neq 1$, then the signature generation procedure should be repeated because of the necessity to calculate $(kH+1)^{-1}$). We have attained possibility to use securely the prime private key element γ due to the use of the "three-level" verification equations. Other variants of the DSS based on the "three-level" verification equations analogous to the DSS described in section 3 are also possible. Above we have considered the signature size satisfying the minimum security level. In general case for the 2^z operations security level, where $z \geq 80$, one should use $2z$-bit private key element γ and z-bit modulus δ that defines the signature length $|k| + |g| = 3z$. At present the proposed 240-bit signature schemes provide the shortest signature length among known DSS based on factorization problem. The computational efficiency of the signature generation and verification procedures in the proposed DSS is about the same as in the DSA standard.

References

[1] ANSI X9.62 and FIPS 186-2. *Elliptic curve signature algorithm*, 1998.

[2] D.Boneh, B.Lynn, and H.Shacham. *Short signatures from the Weil pairing.* J. Cryptology. 2004, vol. 17, no 4, pp. 297–319.

[3] A.J.Menezes, P.C. Van Oorschot, and S.A.Vanstone. *Handbook of Applied Cryptography.* CRC Press, Boca Raton, FL, 1997.

[4] A.A.Moldovyan, D.N.Moldovyan, L.V.Gortinskaya. *Cryptoschemes Based on New Signature Formation Mechanism.* Computer Science Journal of Moldova. 2006 (in print).

[5] D.Naccache and J.Stern. *Singing on a postcard.* In Y.Frankel, editor, Proceedings of Financial Cryptography 200, volume 1962 of LNCS, pp. 121–135, Springer-Verlag, Berlin, 2000.

[6] L.Pintsov and S.Vanstone. *Postal revenue collection in the digital age.* In Y.Frankel, editor, Proceedings of Financial Cryptography 200, volume 1962 of LNCS, pp. 105–120, Springer-Verlag, Berlin, 2000.

[7] R.L.Rivest, A.Shamir, and L.M.Adleman. *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*, Communications of the ACM, 1978, vol. 21, no 2, pp. 120–126.

[8] N.Smart. *Cryptography: an introduction.* McGraw-Hill Publication, London, 2003.

Nikolay A. Moldovyan   Received June 19, 2006

Specialized Center of Program Systems "SPECTR",
Kantemirovskaya, 10, St.Petersburg 197342, Russia;
Phone/fax: 7-812-2453743,
E–mail: *nmold@cobra.ru*