BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 62, No. 4, 2014
DOI: 10.2478/bpasts-2014-0090

Security of Nyberg-Rueppel digital signatures without message recovery

T. ADAMSKI[1*] and W. NOWAKOWSKI[2]

[1] Institute of Electronic Systems, Warsaw University of Technology, 15/19 Nowowiejska St., 00-665 Warsaw, Poland
[2] Institute of Mathematical Machines, 34 Krzywickiego St., 02-078 Warsaw, Poland

Abstract. The paper deals with Nyberg-Rueppel digital signatures without message recovery. Probability of signature forgery is analyzed and assessed. Some simple methods to minimize probability of signature forgery are proposed.

Key words: cryptography, digital signatures, Nyberg-Rueppel signatures, probability of signature forgery.

List of Symbols

N	–	set of natural numbers,
Z	–	set of integers,
Z_n	–	ring of integers modulo n,
Z_n^*	–	multiplicative group of the ring Z_n,
$< n, m >$	–	set of integer greater even to n and less even to m,
R^+	–	set of nonnegative real numbers,
φ	–	Euler's function,
$GCD(m, n)$	–	greatest common divisor of two integers m and n,
$\#A$	–	number of elements in the finite set A,
$\#G$	–	order of the finite group G,
$E(X)$	–	average of the random variable X,
$D^2(X)$	–	variance of the random variable X,
$\oplus_n$	–	addition modulo n,
$\otimes_n$	–	multiplication modulo n,
$-_n$	–	subtraction modulo n,
$B(X, Y)$	–	set of all bijections $f : X \to Y$,
$B(X)$	–	σ-field of all Borel sets of a topological space X,
2^X	–	set of all subsets of the set X,
$\lceil \cdot \rceil$	–	ceiling function.

1. Introduction

In contemporary electronics, data (like software, measurement data, transmitted data and also structure of electronic circuits) can be changed in malicious, frequently dangerous way. Digital signatures are methods preventing these malicious attacks.

Every digital signature scheme like common hand written signature under a document has three main properties:

1. the signature of a person A can be created only by the person A,
2. the signature should be unforgeable,
3. the signature should be verifiable.

Every signature scheme is composed of two algorithms: algorithm of signing (used by a document Signer) and algorithm of verification (used by a signature Verifier).

There are many different signature schemes. In general signature schemes are divided into two categories: one-time signature schemes [1, 2] and multi-use signature schemes [1, 2]. There are also two kinds of signature schemes: signature with message recovery and signature schemes with appendix (i.e. without message recovery). There are also special signatures with additional functionality like blind signatures (called also in blanco signatures), undeniable signature schemes and fail-stop signatures.

For example, one-time signature schemes are the following algorithms: one-time Rabin signatures, one-time Lamport signatures and one time Matyas-Meyer signatures.

Widely applied in practice multi use schemes are the following: RSA, ElGamal, DSA (*Digital Signature Algorithm*), ECDSA (*Elliptic Curve DSA*), Rabin, Shnore signatures, finally Nyberg-Rueppel class of signatures. Some of them are introduced to the public key cryptography standard IEEE P1363.

Nyberg-Rueppel signature schemes are wide class of digital signatures with very interesting properties. All Nyberg-Rueppel signatures are probabilistic in the sense that the signature depends on a signed document and a random variable. Security of all Nyberg-Rueppel signatures is based on DLP (*Discrete Logarithm Problem*).

We consider in the paper simple particular case of Nyberg-Rueppel scheme: so called Nyberg-Rueppel scheme without message recovery (i.e. signature scheme with appendix). In the sequel we analyze and assess probability of forgery in this signature scheme and propose simple methods to control probability of forgery.

*e-mail: t.adamski@ise.pw.edu.pl

2. Nyberg-Rueppel digital signature scheme without message recovery

Nyberg-Rueppel digital signature (in the considered in the paper version) is the signature scheme with appendix i.e. without plain text message recovery. General assumptions are the following. Assume G is a finite group of the order n i.e. $n \stackrel{df}{=} \#G$. Additionally we assume $n \geq 3$ to avoid triviality. The plaintext message m (the message which is signed) is identified with an element of the group G then $m \in G$.

Assume additionally that $f : G \rightarrow Z_n$ is an arbitrary but fixed bijection of the group G on the ring Z_n of integers modulo n. Assume also that $g \in G$, $g \neq 1$ is a generator of the group G or an element of the sufficiently large order. We assume for security reasons that the group G and the element g are chosen in this way that the discrete logarithm problem (DLP) with the basis g is practically unsolvable in the group G.

Signer chooses at random a number $x \in Z_n$ so, that $GCD(x, n) = 1$ and $x \neq 1$. The number x is a private key and is secret. Now, Signer computes $g^x \in G$ and publishes $y \stackrel{df}{=} g^x$ as a public key. Signer publishes also the order of the group G i.e. n, bijection $f : G \rightarrow Z_n$ and element g.

If $\#G = 2$ then $Z_2^* = \{1\}$ and only possible choice of $x \in Z_2^*$ is $x = 1$. Because $y = g^1 = g$ everyone knows immediately the Signer's private key. Hence the order of the group G is assumed in the sequel ≥ 3. In practice the order of the group G is a large number because DLP have to be unsolvable.

Algorithm of signing a document (a plaintext message m) i.e. signature generation is shown in Fig. 1. The signed document m is an arbitrary element of the group G. The signature is an ordered pair $(a, b) \in G \times Z_n$. The document is signed in similar way like in ElGamal signature scheme. The signed document is an ordered pair $(m, (a, b))$. Nyberg-Rueppel signature verification algorithm is shown in Fig. 2.

Algorithm Nyberg-Rueppel signature generation

Input data: the plaintext message $m \in G$, the private key $x \in Z_n^*$ and publicly known $g \in G$, $g \neq 1$, $(y \stackrel{df}{=} g^x)$, order of the group $n \stackrel{df}{=} \#G \geq 3$ and bijection $f : G \rightarrow Z_n$

Output data: $(a, b) \in G \times Z_n$

---

1. Signer computes $a \in G$. At first he chooses at random a number $k \in Z_n$ which is relatively prime to n i.e. $GCD(k, n) = 1$ and computes a in the following way:

$$a = g^{-k} \cdot m$$

2. Signer computes $b \in Z_n$ solving the equation (*) (where b is an unknown)

$$1 = f(a) \otimes_n x \ \oplus_n \ k \otimes_n b \qquad (*)$$

Solving of the equation (*) is simple. After addition $f(a) \otimes_n x$ to the left and right side of the equation (*) we have $1 -_n f(a) \otimes_n x = k \otimes_n b$. Because $GCD(k, n) = 1$, then there is an inverse k^{-1} in the ring Z_n and we finally have:

$$b = k^{-1} \otimes_n (1 -_n f(a) \otimes_n x)$$

Fig. 1. Nyberg-Rueppel signature generation algorithm

Algorithm Nyberg-Rueppel signature verification

Input data: $(m, (a, b))$, $(m \in G, (a, b) \in G \times Z_n)$ and publicly known $g \in G$, $g \neq 1$, $(y \stackrel{df}{=} g^x)$, order of the group $n \stackrel{df}{=} \#G \geq 3$ and bijection $f : G \rightarrow Z_n$

Output data: signature accepted or signature rejected

Verifier has the ordered pair $(m, (a, b))$. To verify the signature Verifier computes $f(a)$ and verifies, if the following verification formula (equation in the ring Z_n) is fulfilled.

$$y^{-f(a)} \cdot a^b = m^b \cdot g^{-1}$$

If this equation is fulfilled Verifier accepts the signature. If the equation is not fulfilled then Verifier rejects the signature.

Fig. 2. Nyberg-Rueppel signature verification algorithm

3. Solution of linear congruencies

Theorem 3.1.

Assume $a, x, y \in Z$, $m \in N$, $m \geq 2$. If $GCD(a, m) = 1$ then

$$ax \equiv ay(\mathrm{mod}m) \quad \text{if and only if} \quad x \equiv y(\mathrm{mod}m).$$

If $d \stackrel{df}{=} GCD(a, m) > 1$ then $ax \equiv ay(\mathrm{mod}m)$ if and only if $x \equiv y(\mathrm{mod}m/d)$.

Proof. 1. If $GCD(a, m) = 1$ then an inverse a^{-1} of a number $a(\mathrm{mod}\, m)$ in the ring Z_m exists. Hence, multiplying both sides of the congruence $ax \equiv ay(\mathrm{mod}m)$ by a^{-1}, we have $a^{-1}ax \equiv a^{-1}ay(\mathrm{mod}m)$. Because $a^{-1}a(\mathrm{mod}m) = 1$ then $x \equiv y(\mathrm{mod}m)$. If $x \equiv y(\mathrm{mod}m)$ then multiplying both sides of the congruence by a we obtain $ax \equiv ay(\mathrm{mod}m)$.

2. Directly from congruence definition we have, that $ax \equiv ay(\mathrm{mod}\, m)$ if and only if $\frac{a}{d}x \equiv \frac{a}{d}y \left(\mathrm{mod}\frac{m}{d}\right)$. But integers $\frac{a}{d}$ and $\frac{m}{d}$ are relatively prime because $d = NWD(a, m)$. Applying then the first part of the theorem we obtain

$$\frac{a}{d}x \equiv \frac{a}{d}y \left(\mathrm{mod}\frac{m}{d}\right) \quad \text{if and only if} \quad x \equiv y(\mathrm{mod}m/d)$$

and finally we have $ax \equiv ay(\mathrm{mod}m)$ if and only if $x \equiv y(\mathrm{mod}m/d)$.■

Corollary. Congruencies can be divided side by side (if division in Z is possible) by an integer which is relatively prime with the modulus $m \in N$, $m \geq 2$. More precisely, if $a, x, y \in Z$, $m \in N, m \geq 2$, $GCD(a, m) = 1$ and $ax \equiv ay(\mathrm{mod}m)$ then $x \equiv y(\mathrm{mod}m)$.

Example. Because $5 \cdot 2 \equiv 5 \cdot (-4)(\mathrm{mod}\, 6)$ and $GCD(5, 6) = 1$, then we have also $2 \equiv (-4)(\mathrm{mod}6)$.

Theorem 3.2. (on solutions of the linear congruence $ax \equiv b(\mathrm{mod}m)$ for $GCD(a, m) = 1$).

Assume $a, b \in Z$, $m \in N$, $m \geq 2$. If $GCD(a, m) = 1$ then the congruence $ax \equiv b(\mathrm{mod}m)$ has a solution $x \in Z$ given by the formula

$$x = ba^{-1}(\mathrm{mod}m),$$

where a^{-1} is an inverse of the number $a(\mathrm{mod}\, m)$ in the ring Z_m. Additionally every number $x' \in Z$ is the congruence solution if and only if $x' \equiv x(\mathrm{mod}m)$.

Proof. 1. We can easily verify that the integer $x = ba^{-1}(\mathrm{mod}\, m)$ (where a^{-1} is an inverse of the integer $a(\mathrm{mod}m)$ in the ring Z_m) is a solution of the congruence $ax \equiv b(\mathrm{mod}m)$. Indeed

$$(a(ba^{-1}(\mathrm{mod}m))(\mathrm{mod}m) =$$
$$= ((aa^{-1})(\mathrm{mod}m)b)(\mathrm{mod}m) = b(\mathrm{mod}m)$$

i.e. $ax \equiv b(\mathrm{mod}m)$ for $x = ba^{-1}(\mathrm{mod}m)$.

If x' is such an integer, that $ax' \equiv b(\mathrm{mod}m)$ then $ax' \equiv b(\mathrm{mod}m)$ if and only if $ax' \equiv ax(\mathrm{mod}m)$. From the proved above Theorem 3.1 "on division side by side" we obtain now, that $x' \equiv x(\mathrm{mod}m)$. On the other hand if $x' \equiv x(\mathrm{mod}m)$ then of course x' is a solution of the congruence $ax \equiv b(\mathrm{mod}m)$.■

Theorem 3.3. Assume $a, b \in Z$, $m \in N$, $m \geq 2$ and denote by $d \stackrel{df}{=} GCD(a, m)$.

1. If $d|\, b$ then the congruence $ax \equiv b(\mathrm{mod}m)$ has a solution given by the formula

$$x = \left(\left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d}\right) \left(\mathrm{mod}\frac{m}{d}\right),$$

where $\left(\frac{a}{d}\right)^{-1}$ is an inverse of the integer $\left(\frac{a}{d}\right) \left(\mathrm{mod}\frac{m}{d}\right)$ in the ring of integers modulo $\frac{m}{d}$ and an integer x' is a solution of the congruence $ax \equiv b(\mathrm{mod}m)$ if and only if $x' \equiv x(\mathrm{mod}m/d)$. Additionally in the set Z_m we have exactly d solutions of the congruence $ax \equiv b(\mathrm{mod}m)$.

2. If b is not divisible by d then the congruence $ax \equiv b(\mathrm{mod}m)$ has no solution.

Proof. Ad 1. Assume $d|\, b$ $(d = GCD(a, m))$. If $ax \equiv b(\mathrm{mod}m)$ then there is $k \in Z$ that $ax = b + k \cdot m$ and we have $\frac{a}{d}x = \frac{b}{d} + k \cdot \frac{m}{d}$. It means that $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{m}{d}\right)$. If we have $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{m}{d}\right)$ then of course $ax \equiv b(\mathrm{mod}m)$ and finally we obtain

$$ax \equiv b(\mathrm{mod}m) \quad \text{if and only if,} \quad \frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{m}{d}\right).$$

Because the integers $\frac{a}{d}$ and $\frac{m}{d}$ are relatively prime then we have from the previous Theorem 3.2 (on linear congruence solution), that the congruence $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{m}{d}\right)$ has the solution, $x = \left(\left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d}\right) \left(\mathrm{mod}\frac{m}{d}\right)$, (where $\left(\frac{a}{d}\right)^{-1}$ is an inverse of the number $\left(\frac{a}{d}\right) \left(\mathrm{mod}\frac{m}{d}\right)$ in the ring of integers modulo $\frac{m}{d}$) and an integer x' is a solution of the congruence $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\frac{m}{d}\right)$ if and only if, $x' \equiv x \left(\mathrm{mod}\frac{m}{d}\right)$.

Then the congruence $ax \equiv b(\mathrm{mod}m)$ has the solution $x = \left(\left(\frac{a}{d}\right)^{-1} \cdot \frac{b}{d}\right) \left(\mathrm{mod}\frac{m}{d}\right)$ and the integer x' is a solution of the congruence $ax \equiv b(\mathrm{mod}m)$ if and only if, $x' \equiv x \left(\mathrm{mod}\frac{m}{d}\right)$.

The last congruence is fulfilled for exactly d numbers x' from the set Z_n ($x' = x + k \cdot \frac{m}{d}$ for $k = 0, 1, ..., d-1$). Then in the set Z_m we have exactly d solutions of the congruence $ax \equiv b(\mathrm{mod}m)$.

Ad. 2. Assume inversely, that there is a solution x of the congruence $ax \equiv b(\mathrm{mod}m)$. Then there is $k \in Z$ that $ax = b + k \cdot m$ and $ax - k \cdot m = b$. The left side of the last equality is divisible by d (where $d = GCD(a, m)$) but the right side is not, which is impossible. Hence the assumption that the congruence $ax \equiv b(\mathrm{mod}m)$ has a solution leads to contradiction.■

4. Some basic theorems

The following simple fact from commutative ring theory is very useful in the sequel.

Fact 4.1

Assume Z_n is a ring of integers modulo n and $a \in Z_n$.

An element $a \in Z_n$ is invertible in the ring Z_n if and only if $GCD(n, a) = 1$.

Proof. see [3–5].

Theorem 4.2. Assume G is a finite group of the order $n \geq 3$, $m \in G$ is a signed plain text message, $x \in Z_n^*$ is a private key, $g \in G$, $g \neq 1$ is an arbitrary fixed element of the group G, $y \stackrel{df}{=} g^x$ is a public key and $f : G \to Z_n$ is a bijection. If the Nyberg-Rueppel signature is correctly computed i.e.

$$a = g^{-k} \cdot m, \tag{1}$$

$$b = k^{-1} \otimes_n (1 -_n f(a) \otimes_n x), \tag{2}$$

where $k \in Z_n^*$ is an arbitrary element chosen from Z_n^* then verification formula $y^{-f(a)} \cdot a^b = m^b \cdot g^{-1}$ is fulfilled.

Proof. From properties of raising to a power in groups we have:

$$y^{-f(a)} \cdot a^b = g^{-xf(a)} \cdot (g^{-k\cdot} \cdot m)^b =$$

$$= g^{-xf(a)} \cdot g^{-k\cdot b} \cdot m^b = g^{-xf(a)-k\cdot b} \cdot m^b.$$

It follows from the Lagrange theorem that for every element $a \in G$ we have $a^{\#G} = 1$ i.e. $a^n = 1$. Then for arbitrary $r \in Z$ we have

$$a^r = a^{r(\bmod n)}. \tag{3}$$

From (2) we obtain that the following equality is fulfilled $1 = f(a) \otimes_n x \oplus_n k \otimes_n b$. Then from (3) we have:

$$g^{-xf(a)-k\cdot b} = g^{(-xf(a)-k\cdot b)(\bmod n)} = g^{-1}$$

and finally we obtain:

$$y^{-f(a)} \cdot a^b = g^{-xf(a)-k\cdot b} \cdot m^b = g^{-1} \cdot m^b. \ \blacksquare$$

Theorem 4.3. If $f : G \to Z_n$ is a bijection and $x \in Z_n^*$ is a fixed element of the multiplicative group Z_n^* then for every $c \in Z_n$ the function $\beta : G \ni a \to g(a) = (c -_n f(a) \otimes_n x) \in Z_n$ is a bijection, in particular the function $h : G \ni a \to h(a) = (1 -_p f(a) \otimes_n x) \in Z_n$ is a bijection.

Proof. If $x \in Z_n^*$ then from the Theorem 3.2 we obtain directly that the function

$$\gamma_1 : G \ni a \to \gamma_1(a) = f(a) \otimes_n x \in Z_n$$

is a bijection. The function

$$\gamma_2 : Z_n \ni z \to \gamma_2(a) = c -_n z \in Z_n$$

is also a bijection then $\beta = \gamma_2(\gamma_1)$ as a superposition of two bijections is a bijection.■

Corollary 4.4. Under assumptions of the theorem 4.3 the number of elements $a \in G$ for which $GCD(1 -_n f(a) \otimes_n x, n) = 1$ is exactly even to $\varphi(n)$, where $\varphi : N \to N$ is the Euler's function.

Proof. A number of invertible elements in the ring Z_n is equal to $\varphi(n)$. The function $h : G \ni a \to g(a) = (1 -_p f(a) \otimes_n x) \in Z_n$ from the Theorem 4.3 is a bijection then the number of elements $a \in G$ for which $GCD(1 -_n f(a) \otimes_n x, n) = 1$ is exactly even to $\varphi(n)$.■

Theorem 4.5. Assume G is a finite group of the order $n \geq 3$, $m \in G$ is a signed plain text message, $x \in Z_n^*$ is a Signer's private key, $g \in G$, $g \neq 1$ an arbitrary fixed element of the group G, $y \stackrel{df}{=} g^x$ and $f : G \to Z_n$ is a bijection then:

1. If b is the second coordinate of the Nyberg-Rueppel signature (a, b) of the plain text message $m \in G$ (more strictly b is computed as $b = k^{-1} \otimes_n (1 -_p f(a) \otimes_n x)$ for chosen at random $k \in Z_n^*$, the fixed private key $x \in Z_n^*$ and $a = g^{-k} \cdot m$) then $b \in Z_n^*$ if and only if $GCD(1 -_n f(a) \otimes_n x, n) = 1$.

2. For every $(a, b) \in G \times Z_n$, if $GCD(1 -_n f(a) \otimes_n x, n) = 1$ (or equivalently $b \in Z_n^*$) then we can find only one ordered pair $(m, k) \in G \times Z_n^*$ that

$$a = g^{-k} \cdot m, \tag{4}$$

$$b = k^{-1} \otimes_n (1 -_n f(a) \otimes_n x). \tag{5}$$

In other words there is only one plain text message $m \in G$ and one random value $k \in Z_n^*$ that the Nyberg-Rueppel signature computed for $m \in G$ and $k \in Z_n^*$ (and for the fixed Signer's private key $x \in Z_n^*$) gives $(a, b) \in G \times Z_n$.

Then there is no plain text message $m' \in G$, $m' \neq m$, for which the Signer's signature is equal to (a, b). As a result the signature forgery is impossible.

3. If $g \in G$ is a generator of the group G then for every $(a, b) \in G \times Z_n$: if $GCD(1 -_n f(a) \otimes_n x, n) = d > 1$ then there are at least two different plain text messages $m, m' \in G, m \neq m'$ having the same signature (a, b).

Proof. Ad. 1. $\Leftarrow$ If we have $k \in Z_n^*$ and $1 -_n f(a) \otimes_n x \in Z_n^*$ then from (5) we obtain $b \in Z_n^*$.

$\Rightarrow$If we have $b \in Z_n^*$, $k \in Z_n^*$ then from (5) we obtain that $1 -_p f(a) \otimes_n x$ is invertible. Hence $GCD(1 -_n f(a) \otimes_n x, n) = 1$.

Ad. 2. If $GCD(1 -_n f(a) \otimes_n x, n) = 1$ then we can solve in unique way in Z_n Eq. (5) with an unknown k. (see the Theorem 3.2). Having $k \in Z_n^*$, we compute from Eq. (4) the unique value $m \in G$.

Ad. 3. From the Theorem 3.3 we obtain that Eq. (5) (with an unknown k) has d different solutions in Z_n and from Eq. (4) we obtain d different plain text messages which fulfill the Eq. (4).

Two possible situations (forgery impossible, forgery possible) as mentioned in the Theorem 4.5 are shown in Fig. 3.

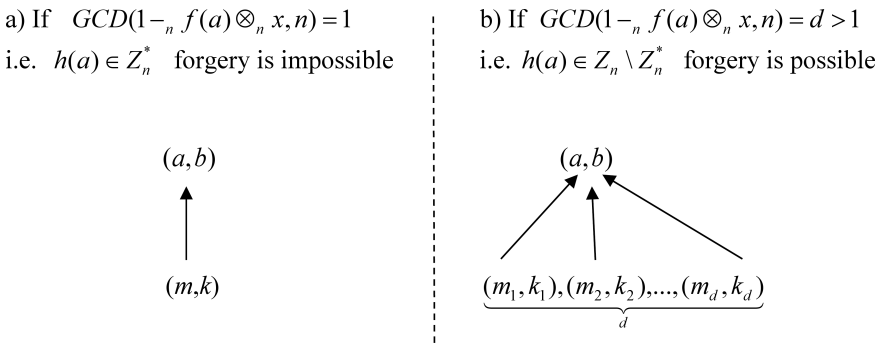

Fig. 3. Two possible situations a) and b) for a) forgery is impossible for b) forgery is possible, different messages can have the same signature, the function $h : G \to Z_n$ is given for $a \in G$ with the formula $h(a) = 1 - {}_p f(a) \otimes_n x \in Z_n$

Theorem 4.6. Assume $G$is a group of the order $n \geq 3$, $g \in G$, $g \neq 1$, $m \in G$, $k \in Z_n^*$, $f : G \to Z_n$ is a bijection, y is a public key ($y \stackrel{df}{=} g^x$, for a private key $x \in Z_n^*$) and $a \in G$, $b \in Z_n^*$ ($b \in Z_n^*$ or equivalently $GCD(1 -_n f(a) \otimes_n x, n) = 1$).

Assume additionally that $m' \in G$ is a unique plain text message which gives the signature $(a, b) \in G \times Z_n^*$ for the private key $x \in Z_n^*$, (existence and uniqueness of m' for every $(a, b) \in G \times Z_n^*$ see the Theorem 4.5). If $m \in G$ denotes the message obtained by Verifier for verification (i.e $(m, (a, b))$) then the verification formula

$$m' = m \tag{6}$$

can be in equivalent way written as

$$y^{-f(a)} \cdot a^b = m^b \cdot g^{-1}. \tag{7}$$

In other words: the problem "if $(a, b) \in G \times Z_n^*$ is a signature written (by a person with a private key x) under the plain text message m" is equivalent to fulfillment of the formula (7).

Proof. 1. From the Theorem 4.5 we obtain that for the given ordered pair $(a, b) \in G \times Z_n^*$ there is a unique ordered pair $(m', k) \in G \times Z_n^*$ for which we have

$$a = g^{-k} \cdot m', \tag{8}$$

$$b = k^{-1} \otimes_n (1 -_n f(a) \otimes_n x). \tag{9}$$

We assume that $GCD(1 -_n f(a) \otimes_n x, n) = 1$ then $1 -_n f(a) \otimes_n x \in Z_n^*$. A product of two invertible numbers from Z_n^* is invertible then b is invertible i.e. $b \in Z_n^*$.

From (9) we have

$$k = b^{-1} \otimes_n (1 -_n f(a) \otimes_n x). \tag{10}$$

On the other hand we have from (8)

$$m' = g^k \cdot a$$

and using (10) we obtain

$$m' = a \cdot g^{b^{-1} \otimes_n (1 -_n f(a) \otimes_n x)}. \tag{11}$$

2. Verification of the signature $(m, (a, b))$ is simply verification if $m' = m$.

Using (11) we can write down equivalently equation $m' = m$ as

$$a \cdot g^{b^{-1} \otimes_n (1 -_n f(a) \otimes_n x)} = m.$$

If we raise both sides of this equation to the power $b \in Z_n^*$ then we equivalently have

$$a^b \cdot g^{b \otimes_n b^{-1} \otimes_n (1 -_n f(a) \otimes_n x)} = m^b.$$

It can be written as

$$a^b \cdot g^{1 -_n f(a) \otimes_n x} = m^b.$$

Because $g^n = 1$ then equivalently we have

$$a^b \cdot g \cdot g^{-f(a)x} = m^b.$$

The above equation can be equivalently written as

$$(g^x)^{-f(a)} \cdot a^b = g^{-1} m^b.$$

But the public key $y = g^x$ then finally we have

$$y^{-f(a)} \cdot a^b = g^{-1} m^b.$$

In short, verification if $m' = m$ is equivalent to verification if $y^{-f(a)} \cdot a^b = g^{-1} m^b$.■

It is important that in the verification formula (7) we have no secret private key x.

5. Probability of forgery

From the Theorem 4.5 we obtain directly the following corollary.

Corollary 5.1. If G is a finite cyclic group of the order $n \geq 3$, $g \neq 1$, $g \in G$ is a generator of the group G, $x \in Z_n^*$ is a fixed private key of Signer and $f : G \to Z_n$ a fixed arbitrary bijection then for every $a \in G$: Nyberg-Rueppel signature (a, b) is unforgeable if and only if $GCD(1 -_n f(a) \otimes_n x, n) = 1$.

In other words if an element $1 -_n f(a) \otimes_n x$ is invertible (or equivalently $GCD(1 -_n f(a) \otimes_n x, n) = 1$) then the signature (a, b) is unforgeable.

The element $1 -_n f(a) \otimes_n x \in Z_n$ is invertible if and only if $b \in Z_n$ (the second coordinate of signature) is invertible. The random element $k \in Z_n^*$ has no influence on invertibility of the element $1 -_n f(a) \otimes_n x$.

We have only $\varphi(n)$ elements a of the group G for which the element $1 -_n f(a) \otimes_n x \in Z_n$ is invertible. Denote $A \stackrel{df}{=} \{a \in G; \quad GCD(1 -_n f(a) \otimes_n x, n) = 1\}$, of course $\#A = \varphi(n)$. For every $a \in A$ forgery is not possible.

Assume that assumptions o the Corollary 5.1 are fulfilled and we have defined two random variables X_1 and X_2 (see

the Appendix A). The random variable X_1 describes choosing at random value $k \in Z_n^*$ and the random variable X_2 describes choosing a plain text message m. From the Theorem A4 (from the Appendix A) it follows that if one of these random variables has a uniform probability distribution and X_1, X_2 are independent then the random variable $g^{-X_1} \cdot X_2$ (which describes computation of the first coordinate of the Nyberg-Rueppel signature) has a uniform probability distribution on G. Hence a probability, that the first coordinate $g^{-X_1} \cdot X_2$ of the Nyberg-Rueppel signature belongs to $G \backslash A$, is even to $1 - \varphi(n)/n$ i.e.

$$P(g^{-X_1} \cdot X_2 \in G \backslash A) = 1 - \frac{\varphi(n)}{n},$$

In other words, probability of forgery is exactly even to $1 - \varphi(n)/n$.

Because the value $1 - \varphi(n)/n$ describes probability of forgery it is important to choose the appropriate n so that $1 - \varphi(n)/n$ would be small.

Theorem 5.2. If $r \in N$ is a fixed natural number and $n = p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_r^{k_r}$, where $p_1, p_2, ..., p_r$ are primes $p_1 < p_2 < ... < p_r$ and $k_1, k_2, ..., k_r \in N$ then

$$\lim_{p_1, p_2, ..., p_r \to +\infty} \frac{\varphi(n)}{n} = 1.$$

Proof. It is a direct conclusion from basic properties of the Euler's function φ.

$$\frac{\varphi(n)}{n} = \frac{\varphi(p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_r^{k_r})}{p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_r^{k_r}} =$$

$$= \frac{\varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot ... \cdot \varphi(p_r^{k_r})}{p_1^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_r^{k_r}} =$$

$$= \frac{(p_1 - 1)p_1^{k_1 - 1} \cdot (p_2 - 1)p_2^{k_2 - 1} \cdot ... \cdot (p_r - 1)p_r^{k_r - 1}}{p_r^{k_1} \cdot p_2^{k_2} \cdot ... \cdot p_r^{k_r}} =$$

$$= \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right).$$

Then

$$\lim_{p_1, p_2, ..., p_r \to +\infty} \frac{\varphi(n)}{n}$$

$$= \lim_{p_1, p_2, ..., p_r \to +\infty} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_r}\right) = 1.$$

But in general the following well known property holds.

Theorem 5.3. If φ is the Euler function then

$$\liminf_{n \to \infty} \frac{\varphi(n)}{n} = 0 \quad \text{and} \quad \limsup_{n \to \infty} \frac{\varphi(n)}{n} = 1.$$

Proof. see [3, 4, 6].

Theorem 5.4. Assume $B(G, Z_n)$ is the set of all bijections $f : G \to Z_n$ from the group G of the order $n \geq 3$, to the ring Z_n and $(B(G, Z_n),\ 2^{B(G, Z_n)}, P)$ is a probabilistic space. If the probability distribution P is a uniform on $B(G, Z_n)$ then for every fixed $a \in G$ and every fixed $x \in Z_n^*$ we have:

$$P(\{f \in B(G, Z_n);\ \ GCD(1 -_n f(a) \otimes_n x, n) = 1\}) = \frac{\varphi(n)}{n},$$

where φ is the Euler function.

Proof. 1. The function $h : Z_n \to Z_n$ defined with the formula $h(z) = 1 -_n z \otimes x$ is a bijection. Denote $B = h^{-1}(Z_n^*)$, of course $\#B = \varphi(n)$.

2. Assume we have fixed $a \in G$ and $x \in Z_n^*$ then: a bijection $f : G \to Z_n$ fulfills the condition $GCD(1 -_n f(a) \otimes_n x, n) = 1$ if and only if $f(a) \in B$.

3. It follows from the p. 2 that the number of all bijections $f \in B(G, Z_n)$ fulfilling the condition $GCD(1 -_n f(a) \otimes_n x, n) = 1$ is equal to $\varphi(n) \cdot (n-1)!$ on the other hand $\#B(G, Z_n) = n!$ then:

$$P(\{f \in B(G, Z_n);\ \ GCD(1 -_n f(a) \otimes_n x, n) = 1\}) =$$

$$= \frac{\varphi(n) \cdot (n-1)!}{n!} = \frac{\varphi(n)}{n}.$$

6. Simple methods to improve the Nyberg-Rueppel signature scheme and control probability of forgery

We propose in the sequel two methods to control probability of forgery in the Nyberg-Rueppel signature schemes. The first is based on the Theorem 5.4 and Bernoulli process, the second is based on the Theorem 6.1 formulated below.

The first method which allows to control probability of forgery. Assume $(B(G, Z_n),\ \ 2^{B(G, Z_n)}, P)$ probabilistic space with the uniform probability distribution P on $B(G, Z_n)$. If $a \in G$ is a fixed element of the group G and $x \in Z_n^*$ is a fixed element of Z_n^* then using the Theorem 5.4 we can define a sequence of independent random variables:

$$X_1, X_2, ..., X_s, ...$$

with values in the set $\{0, 1\}$ in the following way. Assume we do a series of independent experiments. In every experiment we choose at random a bijection f from the set $B(G, Z_n)$(with the uniform distribution). For every $i \in N$: $X_i = 1$ if and only if in the i-th experiment we have chosen a bijection $f : G \to Z_n$ so that $GCD(1 -_n f(a) \otimes_n x, n) = 1$.

From the Theorem 5.4 it follows that the sequence of independent random variables $(X_i)_{i=1}^{\infty}$ is a Bernoulli stochastic process defined on the probabilistic space $(B(G, Z_n),\ \ 2^{B(G, Z_n)}, P)$ with probability of success equal to $\frac{\varphi(n)}{n}$ it means that for every $i \in N$ we have

$$P(X_i = 1) = \frac{\varphi(n)}{n}$$

and

$$P(X_i = 0) = 1 - \frac{\varphi(n)}{n}.$$

Introduce now, the random variable Y defined on the probabilistic space $(B(G, Z_n),\ 2^{B(G, Z_n)}, P)$,with values in the set $N \cup \{+\infty\}$ in the following way. We have defined above a Bernoulli process $(X_i)_{i=1}^{\infty}$ of independent experiments. For every $s \in N \cup \{+\infty\}$, $Y = s$ if and only if the condition $GCD(1 -_n f(a) \otimes_n x, n) = 1$ is true the first time in the s-th experiment, $Y = +\infty$ if and only if the condition $GCD(1 -_n f(a) \otimes_n x, n) > 1$ is true in every experiment.

Equivalently

$$Y = s$$

if and only if $X_1 = 0,\ X_2 = 0,\ ...,\ X_{s-1} = 0,\ X_s = 1$

$$Y = +\infty$$

if and only if for every $i \in N$, $X_i = 0$.

The random variable Y is a time till the first success in the Bernoulli process then it has geometrical distribution and we have (see [3]): for every $s \in N$

$$P(Y = s) = \left(1 - \frac{\varphi(n)}{n}\right)^{s-1} \cdot \frac{\varphi(n)}{n}, \tag{12}$$

$$E(Y) = \frac{n}{\varphi(n)}$$

$$\text{and} \quad D^2(Y) = \left(1 - \frac{\varphi(n)}{n}\right) \cdot \frac{n^2}{(\varphi(n))^2}. \tag{13}$$

Proposed method is based on random choosing a bijection $f : G \to Z_n$ from the set $B(G, Z_n)$ (with the uniform probability distribution on $B(G, Z_n)$) and next verifying if $GCD(1 -_n f(a) \otimes_n x, n) = 1$.

If $GCD(1 -_n f(a) \otimes_n x, n) = 1$ then we have found the appropriate bijection.

If $GCD(1 -_n f(a) \otimes_n x, n) > 1$ then we repeat the random choosing.

In short, we try at random some different independent bijections (a sequence of bijections) till the first success.

From the formulas (13) we have that the average time till the first success (i.e. the first bijection $f_i : G \to Z_n$ that $GCD(1 -_n f_i(a) \otimes_n x, n) = 1$) is equal to $\frac{n}{\varphi(n)}$.

The second method which allows to control probability of forgery

The second (deterministic) method which allows to control probability of forgery is based on the following theorem.

Theorem 6.1.

Assume G is a finite group of the order n, $n \geq 3$ and $x \in Z_n^*$ is a fixed element of the multiplicative group Z_n^*. For every $n \in N$ there is a finite sequence of r bijections $f_1, f_2, ..., f_r$, where for every $i \in < 1, r >$, $f_i : G \to Z_n$ with the following property:

$$\text{for every } a \in G \text{ there is } i \in < 1, r > \text{ that}$$
$$GCD(1 -_n f_i(a) \otimes_n x, n) = 1.$$

The smallest r from the above theorem is equal to $\left\lceil \frac{n}{\varphi(n)} \right\rceil \geq 2$.

Proof. 1. It is possible to write down the set G as a sum of r subsets $A_1, A_2, ..., A_r$

$$G = \bigcup_{i=1}^{r} A_i,$$

where $r = \left\lceil \frac{n}{\varphi(n)} \right\rceil$ and for every $i \in < 1, r >$ we have $\#A_i = \varphi(n)$ and additionally for every $i, j \in < 1, r-1 >$, $i \neq j$ we have $A_i \cap A_j = \emptyset$. It means that $A_1, A_2, ..., A_{r-1}$ are disjoint in pairs. As the the last subset A_r we can take every set which fulfils two conditions: $\#A_i = \varphi(n)$ and $G \setminus \bigcup_{i=1}^{r-1} A_i \subseteq A_r$.

2. Now, we can define r bijections $h_1, h_2, ..., h_r$, where for every $i \in < 1, r >$, $h_i : G \to Z_n$ and $h_i(A_i) = Z_n^*$.

3. For every bijection $h_i : G \to Z_n$ we can choose a bijection $f_i : G \to Z_n$ in this way that for every $a \in G$, we have $h_i(a) = 1 -_n f_i(a) \otimes_n x$. It is possible because we can take for every $a \in G$, $f_i(a) \stackrel{df}{=} (h_i(a) -_n 1) \otimes_n x^{-1}$, where x^{-1} is an inverse in the multiplicative group Z_n^*. The function $f_i : G \to Z_n$ is a bijection as superposition of 3 bijections.

4. From the point 1, we obtain now that for every $a \in G$ there is $i \in < 1, r >$ that $h_i(a) \in Z_n^*$ or equivalently $1 -_n f_i(a) \otimes_n x \in Z_n^*$. Then finally we have found a finite sequence of r bijections $f_1, f_2, ..., f_r$, that for every $a \in G$ there is $i \in < 1, r >$ that $GCD(1 -_n f_i(a) \otimes_n x, n) = 1$.

5. It is obvious that if $\widetilde{h}_1, \widetilde{h}_2, ..., \widetilde{h}_s$ is an arbitrary finite sequence of s bijections $\widetilde{h}_i : G \to Z_n$ then the smallest number s for which the following condition (14)

$$\bigcup_{i=1}^{s} \widetilde{h}_i^{-1}(Z_n^*) = G \tag{14}$$

is fulfilled is equal to $\left\lceil \frac{n}{\varphi(n)} \right\rceil$ (of course $\left\lceil \frac{n}{\varphi(n)} \right\rceil \geq 2$). Equivalently the condition (14) can be written in the following way

$$\underset{a \in G}{\forall} \underset{i \in < 1, s >}{\exists} \widetilde{h}_i(a) \in Z_n^*. \tag{15}$$

If we assume that for every $a \in G$ we have $\widetilde{h}_i(a) = h(a) = 1 -_n f_i(a) \otimes_n x$ then the condition (15) we can write in the form

$$\underset{a \in G}{\forall} \underset{i \in < 1, s >}{\exists} 1 -_n f_i(a) \otimes_n x \in Z_n^* \tag{16}$$

i.e.

$$\underset{a \in G}{\forall} \underset{i \in < 1, s >}{\exists} GCD(1 -_n f_i(a) \otimes_n x) = 1. \tag{17}$$

Then in short: for the given finite sequence $f_1, f_2, ..., f_s$ of s bijections $f_i : G \to Z_n$ the smallest number s for which the condition (16) is fulfilled is equal to $\left\lceil \frac{n}{\varphi(n)} \right\rceil$.■

That is easy to verify that for the group G of the order $n = 2$ the thesis of the above theorem is also fulfilled, but in the paper we assume for uniformity reason that $n \geq 3$.

Of course we have

$$\underset{i \in < 1, r >}{\forall} \underset{a \in A_i}{\forall} GCD(1 -_n f_i(a) \otimes_n x, n) = 1,$$

where $A_1, A_2, ..., A_r \subseteq G$ are subsets of G defined in the proof of the Theorem 6.2 or equivalently

$$\underset{i \in < 1, r >}{\forall} \underset{a \in A_i}{\forall} 1 -_n f_i(a) \otimes_n x \in Z_n^*.$$

The algorithm of the proposed method repeats the idea of the Theorem 6.1 proof.

1. Like in point 1 of the proof, we choose in arbitrary way sequence of r subsets $A_1, A_2, ..., A_r$

$$G = \bigcup_{i=1}^{r} A_i,$$

where $r = \left\lceil \frac{n}{\varphi(n)} \right\rceil$ and for every $i \in< 1, r >$ we have $\#A_i = \varphi(n)$ and additionally for every $i, j \in< 1, r-1 >$, $i \neq j$ we have $A_i \cap A_j = \emptyset$. It means that $A_1, A_2, ..., A_{r-1}$ are disjoint in pairs. As the the last subset A_r we can take every set which fulfils two conditions: $\#A_i = \varphi(n)$ and $G \setminus \bigcup_{i=1}^{r-1} A_i \subseteq A_r$.

2. Using $A_1, A_2, ..., A_r$ we find a finite sequence of r bijections $f_1, f_2, ..., f_r$, with the property, that for every $a \in G$ there is $i \in< 1, r >$ that $GCD(1 -_n f_i(a) \otimes_n x, n) = 1$.

3. Then we apply sequentially bijections $f_1, f_2, ..., f_r$ verifying for $i = 1, 2, ..., r$ if $GCD(1 -_n f_i(a) \otimes_n x, n) = 1$. The first $i \in< 1, r >$ for which $GCD(1 -_n f_i(a) \otimes_n x, n) = 1$ gives a bijection f_i used to sign a document m.

7. Conclusions

1. We can easily assess probability of possible forgery in Nyberg-Rueppel signature schemes.
2. Security of the Nyberg-Rueppel signature scheme depends on the order n of the group G. Then the order of the group G have to be carefully chosen.
3. In the paper two simple methods of fully reliable Nyberg-Rueppel like signature schemes were proposed. The first, probabilistic is based on the Bernoulli stochastic process and is reliable from probabilistic point of view. The second method is deterministic and works always correctly. The essence of the presented two methods is that we are changing the bijection f so that forgery would be impossible. As a result the bijection f is not a universal parameter for the signature scheme like in classical Nyberg-Rueppel methods and the the chosen bijection f have to be added as a third coordinate to the signature. Then a signed plain text message has the shape $(m, (a, b, f))$.

Appendix
Random variables with values in groups

Definition A.1 (topological group)

Assume $(G, \cdot)$ is a group and (G, T) is a topological space, where $T \subseteq 2^G$ is a topology. The group G is called a topological group iff the following two conditions are fulfilled:

1. the product $\cdot : G \times G \to G$ is a continuous mapping of $G \times G$ onto G,
2. the inversion $G \ni x \to x^{-1} \in G$ is a continuous mapping of G onto G.

A topological group is also in natural way a measurable space $(G, B(G))$, where $B(G)$ is a σ – field of Borel subsets of G. Hence we can define random variables with values in G.

In the paper we are interested in finite groups for which we admit that $T = 2^G$ and $B(G) = 2^G$. Then every finite group can be treated as a topological group and measurable space.

Definition A.2 (convolution of two finite measures)

Assume G is an Abelian topological group and μ_1 and μ_2 are two finite measures on the measurable space $(G, B(G))$ and $(G \times G, B(G) \times B(G), \mu_1 \times \mu_2)$ is a product of two spaces with measure: $(G, B(G), \mu_1)$ and $(G, B(G), \mu_2)$. Assume additionally that μ is an induced measure by the continuous mapping $f : G \times G(x, y) \to x \cdot y \in G$ i.e. for every $A \in B(G)$ we have $\mu(A) = \mu_1 \times \mu_2(f^{-1}(A))$. The measure μ is called a convolution of two measures: μ_1 and μ_2 and is denoted by $\mu_1 * \mu_2$ i.e. $\mu = \mu_1 * \mu_2$.

Theorem A1.

Assume G is an Abelian topological group and μ_1 and μ_2 are two finite measures on the measurable space $(G, B(G))$. If $\mu = \mu_1 * \mu_2$ then

1. The function $f : G \ni x \to \mu_1(A \cdot x^{-1}) \in R^+$ is μ_2 integrable and the function $g : Gx \to \mu_2(A \cdot x^{-1}) \in R^+$ is μ_1 integrable
2. for every $A \in B(G)$ we have

$$\mu(A) = \mu_1 * \mu_2(A) = \int_G \mu_1(A \cdot x^{-1}) \mu_2(dx) =$$

$$= \int_G \mu_2(A \cdot x^{-1}) \mu_1(dx).$$

Proof. See [7].

Theorem A2.

Assume X_1 and X_2 are independent random variables defined on a probabilistic space $(\Omega, \mathfrak{M}, P)$ and with values in an Abelian topological group G. If P_{X_i} denotes a probability distribution of the random variable X_i for $i = 1, 2$ then

1. $Y \stackrel{df}{=} X_1 \cdot X_2$ is a random variable
2. the probability distribution P_Y of the random variable Y is given by the following formula

$$P_Y = P_{X_1} * P_{X_2}.$$

Proof. See [8].

Definition A.3 (uniform probability distribution on a group G).

Assume X is a random variables defined on a probabilistic space $(\Omega, \mathfrak{M}, P)$ and with values in an Abelian topological group G. We say that the random variable X has a uniform probability distribution iff for every $A \in B(G)$ and every $x \in G$ we have

$$P_X(A) = P_X(A \cdot x),$$

where P_X denotes a probability distribution of the random variable X.

Theorem A3.

Assume X_1 and X_2 are independent random variables defined on a probabilistic space $(\Omega, \mathfrak{M}, P)$ and with values

in an Abelian topological group G. If P_{X_i} denotes a probability distribution of the random variable X_i for $i = 1, 2$ and one of the probability distributions P_{X_1},P_{X_2} is uniform then a random variable $Y \stackrel{df}{=} X_1 \cdot X_2$ has the uniform distribution.

Proof. Assume P_{X_1} is the uniform probability distribution then from theorems A1 and A2 we obtain for every $A \in B(G)$

$$P_Y(A) = P_{X_1} * P_{X_2}(A) = \int\limits_G P_{X_1}(A \cdot x^{-1}) P_{X_2}(dx) =$$

$$= \int\limits_G P_{X_1}(A) P_{X_2}(dx) = P_{X_1}(A) \int\limits_G 1 P_{X_2}(dx) = P_{X_1}(A).$$

Then the random variable $Y \stackrel{df}{=} X_1 \cdot X_2$ has the uniform distribution.■

The above theorem is frequently used in cryptography in the case when the Abelian group G is finite.

For the finite cyclic group G, the following simple fact is true. If $g \in G$ is a generator of the finite cyclic group G, the order of G is equal to n and X is a random variable with uniform probability distribution on the ring Z_n then a random variable g^X has a uniform probability distribution on G.

Theorem A4.

Assume we have two independent random variables X_1 and X_2 defined on a probabilistic space $(\Omega, \mathfrak{M}, P)$. Assume additionally that $g \in G$ is a generator of the finite cyclic group G, an order of G is equal to $n \geq 2$, X_1 is a random variable into the ring Z_n and X_2 is a random variable with values in the group G. If one of the random variables X_1, X_2 has a uniform probability distribution (X_1 on Z_n or X_2 on G) then a random variable $g^{X_1} \cdot X_2$ has a uniform probability distribution on G.

Proof. A finite cyclic group is Abelian as in the Theorem A3. Hence if the random variable X_2 has a uniform probability distribution on G then from theorem A3 we obtain that the probability distribution of the random variable $g^{X_1} \cdot X_2$ is uniform. If the random variable X_1 has the uniform probability distribution on Z_n then the random variable g^{X_1} has the uniform distribution on G and from Theorem A3 we have that the probability distribution of the random variable $g^{X_1} \cdot X_2$ has a uniform probability distribution on G.■

REFERENCES

[1] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press Inc., 1997, (http://cacr.math.uwaterloo.ca/hac).

[2] J. Pieprzyk, T. Hardjono, and J. Seberry, *Fundamentals of Computer Security*, Springer, Berlin, 2003.

[3] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, Cambridge, 2008.

[4] S. Yan, *Number Theory for Computing*, Springer, Berlin-Heidelberg, 2002.

[5] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, New York, 1994.

[6] W. Narkiewicz, *Number Theory*, PWN, Warszawa, 1990, (in Polish).

[7] K. Maurin, *Analysis*, PWN, Warszawa, 1991, (in Polish).

[8] J. Jakubowski and R. Sztencel, *Introduction to Probability Theory*, Script, Warszawa, 2004, (in Polish).

[9] C.C. Lin and C.S. Laih, "Cryptanalysis of Nyberg-Ruppel's message recovery scheme", *IEEE Communications Letters* 4 (7), 231–232 (2000), DOI: 10.1109/4234.852925.

[10] G. Ateniese and B. Medeiros, "A provably secure Nyberg-Rueppel signature variant with applications", *Cryptology ePrint Archive*, *Report* 2004/93, (http://eprint.iacr.org) (2004).

[11] 1363-2000 – *IEEE Standard Specifications for Public-Key Cryptography*. 2000. DOI:10.1109/IEEESTD.2000.92292.

[12] I. Blake, G. Seroussi, and N. Smart, *Elliptic Curves in Cryptography*, University of Cambridge, Cambridge, 2002.