2012 IX International Symposium on Telecommunications (BIHTEL)
October 25-27, 2012, Sarajevo, Bosnia and Herzegovina

FAST IMPLEMENTATION ZERO KNOWLEDGE IDENTIFICATION SCHEMES USING THE GALOIS FIELDS ARITHMETIC

Nikolaos G. Bardis[1], Oleksandr P. Markovskyi[2], Nikolaos Doukas[1] and Athanasios Drigas[3]

[1]Department of Military Sciences, Faculty of Mathematics and Engineering Science, Informatics and Computer Engineering Lab, Univ. Military Education - Hellenic Army Academy, Vari - 16673, Greece.
bardis@ieee.org, nikolaos@doukas.net.gr
[2]Department of Computer Engineering, National Technical University of Ukraine, (Polytechnic Inst. of Kiev),Peremohy pr., Kiev 252056, KPI 2003, Ukraine. markovskyy@i.ua
[3]National Centre for Scientific Research "Demokritos", Institute of Informatics & Telecommunications - Net Media Lab, Ag.Paraskevi - Athens, 15310, Greece.
dr@imm.demokritos.gr

***Abstract*—This article proposes an approach that accelerates the realization of user identification schemes that follow the principle of zero knowledge. The proposed approach is based on using finite field arithmetic to replace the usual modular arithmetic approaches. The application of this efficient method that was developed using Galois Fields, renders feasible an exponential reduction of the computation time required for classical zero knowledge authentication methods, such as FFSIS, Schnorr and Guillou & Quisquater. Modifications of the relevant schemes are presented that use Galois Field multiplication operations. It is shown, both theoretically and experimentally that the proposed procedure attains a per order acceleration of the execution time required for the user authentication by 2 – 3 orders of magnitude, via a hardware implementation.**

***Index Terms*— Galois Field, Modulo Multiplication, User Identification**

I. INTRODUCTION

THE widespread use of distributed systems for the collection, processing and management of information, both in the military and civil context, objectively underlines the importance of efficient and effective user rights access control methods. The rapid progress of information technology motivates the dynamic expansion of the use in the military field of multiple user distributed systems that perform operations of collection and processing of information, decision support and continuous control. The successful application of such systems depends to an important extent to the efficient identification of the users. The analysis of countermeasures in the context of information technology during military conflicts in recent years provides convincing evidence that the user identification subsystems in distributed command and control systems are increasingly becoming enemy targets.

Their practical use is limited by the fact that their implementation demands significant computational resources, given that they are founded on modular exponentiation operations, applied on numbers with lengths 1024 to 2048 bits, with a prospect for increase in the near future to 4096. In the application of modular exponentiation, an increase in the word length results to an exponential increase in the required calculation time. In this case, the rate of increase of the volume of calculations would demand an increase in the speed of computing equipment.

A particularly acute problem, is the problem of fast algorithms for identification schemes based on the concept of "zero – knowledge" in mobile devices and embedded microcontrollers, with limited energy consumption possibilities, that are commonly end user devices [1]. In this context, the problem of acceleration of user identification based on zero knowledge is imminent and has a wide range of practical applications.

II. IDENTIFICATION ALGORITHM BASED ON THE ZERO – KNOWLEDGE CONCEPT

According to current trends in technological development and its applications, there exist increased possibilities for unauthorized access to sensitive information resources of the integrated systems, possibilities that are enabled by interventions to the user identification procedures. It is a well understood fact that the increased use of wireless data transmission technologies makes it feasible for illegitimate users to mount attacks during the stage of user identification. Specifically in the case of wireless communications actions like the sniffing of passwords for access of legal subscriber, as well as his replacement after the session of identification are facilitated. A robust defense mechanism against imitation of legitimate users is the periodical repetition of the user identification procedures during the interaction of the system with a subscriber. For this reason the process of identification should be such that it enables fast implementations. Additional ways for illegitimate interventions during the identification

978-1-4673-4876-8/12/$31.00 ©2012 IEEE

process are the side-channel directed interactions with the system simultaneously with legitimate users, the use of viruses or via the actions of irresponsible personnel. For the broad class of commercial multi-subscriber systems the elimination of the possibility of impersonation of user access by imitation of access codes is important. On the basis of the circumstances indicated, the current means for subscriber identification must satisfy the following requirements.

1. The identifying information message (password) must change with each access to the system and the passwords used must be statistically independent;
2. The length of password should be such that it completely excludes the possibility of a brute force attack;
3. The information, which is stored in the system must not be sufficient for the reproduction of subscriber passwords;
4. identification procedures must be carried out sufficiently rapidly

In literature identification methods, which satisfy the first three of the given requirements are classified as "strict", in contrast the remaining schemes that are classified as "weak". In the class of the weak schemes belong, for example, the procedure of identification which is used in the UNIX operating system. This procedure involves the storage in the system of only the hash value of the passwords of users, that, with the use of the one way hash functions, excludes the possibility of the reproduction of password of the system; however, passwords themselves do not change, which makes it sufficient simple to intercept them. The class of strict procedures is principally composed by methods of identification that are based the concept "zero knowledge". The most commonly known of these methods are the FFSIS (Feige Fiat Shamir Identification Scheme) [2], Guillou-Quisquater [3] and Schnorr identification schemes [4].

FFSIS is a relatively simple and at the same time sufficiently effective scheme for the identification of the subscribers of multi-user systems, on the basis of which a number of more practical to use modified algorithms have been proposed. In the attempts of using this scheme in practice, the main disadvantage of FFSIS is the need for a large number of data exchanges during the user identification process, which noticeably loads the communication channels used. Other existing identification schemes, which implement the zero knowledge concept, require a substantially smaller volume of data transfers, but the procedures provided by them involve large computational complexity, since instead of the operation of squaring, they use the modular exponential operation.

The essence of the FFSIS consists of the following steps. The subscriber selects two prime numbers p and q and calculates the modulus $m=p\cdot q$. For the generation of public and private keys the subscriber selects the number v, which is been the quadratic residue on the modulus m. In other words, a v is selected for which $d^2 \bmod m=v$ and there exists v^{-1} such that $v\cdot v^{-1} \bmod m = 1$. Then the smallest s is calculated for which: $s^2 \bmod m=v^{-1}$. The number v is the public key, while the number s is the private key. During registration, the subscriber only submits their public key - the number v to the system.

In the cycle of identification the subscriber selects a random number r and calculates the value $x=r^2 \bmod m$. The calculated value x is then sent to the system. System initiates a protocol of t cycles of accreditation. In each cycle of accreditation the following actions are carried out:

The system sends a random bit b to the subscriber. If $b=0$ then the subscriber sends to the system the number r, otherwise if $b=1$ then the subscriber uses their private key s in order to calculate $y=r\cdot s \bmod m$ and sends it to the system.

If $b=0$ then the system verifies $x=r^2 \bmod m$, otherwise if $b=1$, the system verifies $x=y^2\cdot v \bmod m$, which confirms that the subscriber possesses $s=\sqrt{v^{-1}}$ since

$$y^2\cdot v\cdot \bmod m=(r^2\cdot(\sqrt{v^{-1}})^2\cdot v)\bmod m= \quad (1)$$
$$=(r^2\cdot v^{-1}\cdot v)\bmod m=r^2 \bmod m=x$$

If the intruder knows the public key ν of the legitimate subscriber, then they can select a random g and calculate $g^2\cdot v \bmod m=\xi$ and then send ξ, as if it were x. If the system sends as an answer the random bit $b=1$, then the intruder sends instead of y the code g. Hence the system calculates $g^2\cdot v \bmod m$, compares it with ξ and obtains a positive comparison result. However if $b=0$, then the intruder must send to the system the code $g^2 \bmod m\neq\xi$, which implies that they will have to attempt to use the fake code. If the intruder sends as x the code $g^2 \bmod m$, then the verification will proceed for $b=0$, but will fail for $b=1$.

It is obvious that the identification with the positive result is accessible only if the attacker selected the private key s. Solution of this problem is equivalent to finding the value v^{-1} of a known v. The most significant drawbacks in the described version of FFSIS identification scheme are the need for several cycles of accreditation and the low speed, caused by the fact that on each cycle of accreditation it is necessary to perform three operations of modular multiplication over multi-digit numbers. This deficiency becomes especially perceptible, if the terminal devices of subscribers are implemented as portable controllers (smart - cards), for which the completion of a modular multiplication operation presents a significant computational burden.

Another zero knowledge identification scheme has been proposed by C. Schnorr [4]. For the production of the keys, two prime numbers are considered, p and q, with q being a factor of p-1. A simple example is the case $q=11$ and $p=89$. Following that an a must be chosen, such that $a^q \bmod p=1$. E.g. for $a=45$: $45^{11} \bmod 89=1$. A random number is chosen $s<q$ e.g. $s=7$, and the calculation of $-s=q-s=11-7=4$ takes place. The number s is considered the private key. The public key v is calculated as $v=a^{-s} \bmod p$. For the example given $v=45^4 \bmod 89=39$.

The identification procedure based on the Schnorr schemes consists of the following steps:

1) The subscriber chooses a random $r<q$, e.g $r=5$ and calculates $x=a^r \bmod p$, e.g. $45^5 \bmod 89=64$, sending the number x to the system.

2) The system produces a random number $e<2^t$-1 and sends the calculated value to the subscriber. In the context of the previous example, consider t=6 and the corresponding e=29.

3) The subscriber calculates $y=(r+s\cdot e) \bmod q$ and sends the value y to the system. In the above example y=(5+29·7) mod 11=10.

4) The system verifies the equality $x = a^y \cdot v^e \bmod p$. For the above example, this equality is valid for $45^{10}\cdot 39^{29} \bmod 89 = 2\cdot 32 \bmod 89 = 64$.

The fundamental and most computationally expensive operation in the Schnorr schemes is the modular exponentiation $a^y \cdot v^e \bmod p$.

Another classical zero-knowledge architecture, is the Guillou-Quisquater schemes [3]. The key production is carried out in the following way. The subscriber owns a public password J, which is in practice a hash signature of the symbols of a sequence containing the subscriber's name. Consider as an example the case of J=18. The public key of the system is the number n, which is the product of two prime numbers that are kept secret, similarly to number v. The private key is the code B such that $(J\cdot B^v) \bmod n=1$. E.g. p=11 and q=19, $p\cdot q=n$ =11·19=209, B=13 and v=63 so that $J\cdot B^v \bmod n=18\cdot 151 \bmod 209=1$.

The identification sequence involves the following procedure:

1) The subscriber choses a random number r such that 1< r <n-1, calculates the value $T=r^v$ mod n and sends the value T to the system. E.g., consider r = 22, then $T=22^{63}$ mod 209=132.

2) The system produces a random number d, which must be chosen from the range 0<d<n-1, e.g d=5 and sends it to the subscriber.

3) The subscriber calculates $D=r\cdot B^d$ mod n and sends it to the system. E.g. $D = 132\cdot 13^5$ mod 209 = 176.

4) The system calculates $T' = D^v \cdot J^d$ mod n and if T =T ', then the result of the identification is considered to be positive. For the example $T' = 176^{63}\cdot 18^5$ mod 209=132.

Similarly to the Schnorr schemes, the fundamental operation in the case of the Guillou-Quisquater schemes is the modular exponentiation operation: $D^v \cdot J^d \bmod n$.

Hence the Schnorr and Guillou-Quisquater schemes demand a significantly smaller volume of data exchanges compared to the FFSIS, but their implementation involves a significantly large computational volume, as the squaring operation has been replaced by the modular exponentiation. The FFSIS is considered more economic in terms of the volume of the calculations involved, but its application demands several cycles of information exchange.

The purpose of this research is the development of a modified schemes for zero knowledge user identification, which involves significantly smaller computational complexity and increases the speed of identification with software and hardware implementations.

III. FFSIS MODIFICATION ON THE BASIS ON GALOIS FIELDS ALGEBRA

A significant simplification in the calculations, connected with the realization of the identification architectures based on the zero – knowledge concept can be achieved via their realization using algebraic formulations without the inter-bit carries and loans. This class of algebras includes the algebra on Galois fields. In recent years this algebra is widely used in coding and information security. One of its important merits is the fact that the realization of its base computational operations: multiplication, addition and modular reduction is carried out substantially more rapidly in comparison with the classical operations of multiplication, addition and the presence of remainder. This fact leads to economies in hardware complexity without increasing the algorithmic (software) complexity. In the algebra on Galois field, the addition operation corresponds to the logical addition (XOR). The multiplication operation is performed without the inter-bit carry transfers. This operation will be designated for the remainder of the paper by the symbol ⊗. The multiplication without carry transfer

$D=U\otimes V=\{d_{2\cdot r},\ldots,d_3,d_2,d_1\}=d_1+2\cdot d_2+4\cdot d_3+\ldots+2^{2\cdot r}\cdot d_{2\cdot r}, \quad \forall l\in\{1,..,2\cdot r\}: d_l\in\{0,1\}$ of two r-bit numbers $U=\{u_r,\ldots,u_2,u_1\}=u_1+2\cdot u_2+\ldots+2^r\cdot u_r$ and $V=\{v_r,\ldots,v_2,v_1\}=v_1+2\cdot v_2+\ldots+2^r\cdot v_r, \forall i\in\{1,..,r\}: v_i,u_i\in\{0,1\}$ is calculated as follows:

$$D=U\cdot v_1\oplus(U\cdot v_2)<<1\oplus\ldots\oplus(U\cdot v_r)<<(r-1), \qquad (2)$$

where '·' the operation of logical multiplication, $p<<q$- the operation of the logical shift of the number p to the left by q bits.

The operation of raising the number A to the exponent E without shift is denoted by $A|^E=A\cdot 1\otimes A\cdot 1^2\otimes\ldots\otimes A\cdot 1^E$. The operation of the calculation of the remainder of the division of the polynomial that corresponds to the number A by the polynomial corresponding to m is denoted as A rem m. Considering the above definitions, the exponentiation operations in the Galois Field may be expressed as $A|^E$ rem m, where m is the number corresponding to the formulated polynomial of the field.

The proposed realization of FFSIS identification using Galois field algebra may be outlined as follows. In the stage of registration by subscriber, the generation of the public and private keys of the selected word length - n is carried out. For this a (n+1) bits length number m which correspondents to primitive polynomial degree n on GF(2n). As an illustration, consider a low order configuration with n=4; it then is possible to select as the module 5-bit m=110012=25 which is correspondent to primitive polynomial x4+x3+1.

Further on, the arbitrarily selected integer *(n -1)* – bits number η after which the (2·n-1) - bits of the number $\eta\otimes m\oplus 1$ is factoring by the n-bit coefficients d and s so that d of $d\otimes s=\eta\otimes m\oplus 1$. For example, if η=4 and m=25, then $\eta\otimes m\oplus 1=101=9\otimes 13$. Accordingly, d=9 and s=13. After this, $v=d|^2$ rem m and $v^{-1}=s|^2$ rem m are calculated; it is trivial to prove that that $v\cdot v^{-1}$ rem m=1. On the considered example $v=(9\otimes 9)$ rem m =14 and $v^{-1}=(13\otimes 13)$ rem m=7; The number v is the public, and the number s – is the private key.

During the identification the subscriber randomly generates the r, for example r=10; the user then calculates the $d=(r|^2)$ rem m and the calculated value d is sent it to the system. For the example d=10⊗10 rem 25=11. After this, the user calculates $y=(r\otimes s)$ rem m and also sends the value y to the system – for the example y=10⊗13 rem 25=15. On obtaining of the indicated codes, the system, in accordance with the FFSIS, initiates the fulfillment the t cycles of the accreditation. In each cycle of accreditation the following actions are carried out:

1) The system sends random bit b to subscriber.
2) If b=0, then subscriber sends into the system the number r, otherwise, if b=1, then the subscriber calculates using their private key s the value y =r⊗s rem m and sends it to the system.
3) If b=0, then system checks the validity of $d=r|^2$ rem m, otherwise, if b=1, is checked, that $d=y|^2\otimes v$ rem m, convinced, that the subscriber knows $s=\sqrt{v^{-1}}$.

For example, let b=1 and the subscriber calculate value $y=(r\otimes s)$ rem m=10⊗13 rem 25=15 and the value y send it to the system. The system, after obtaining, y=15, calculates with the use of a private key v=14 z=15⊗15⊗14 rem 25=11. Since z=11=d, then the test is considered successful.

If b=0, then the subscriber sends to the system the number r=10; $z=r|^2$ rem m=10⊗10 rem 25=11 and compares it with the previously obtained value d=11.

Thus, it is shown that the FFSIS identification works with its realization in Galois field algebra.

For the modified Schnorr schemes for the production of keys, two primitive polynomials of the same degree P(x) and W(x) are chosen, to which correspond the numbers p and w. The quantity $m=p\otimes w$ is calculated. A value of q is chosen, that is a coefficient of $m\oplus 1$ and is such that $a|^q$ rem m=1. For example if the 5-bit numbers p=19 and w=25 are chosen then their modulo becomes $m=p\otimes w$=19⊗25=443, q=10, a=46.

A random number $s<q$ is chosen, e.g. s=3; then $-s=q-s$=10-3= 7. The number s is considered the private key. The public key is then calculated as v, $v = a|^{-s}$ rem m. In the example $v = a|^{-7}$ rem 443=117. The identification procedure for the modified Schnorr schemes consists of the following steps:

1) The subscriber chooses a random $r<q$, e.g. r=8 and calculates $x=a|^r$ rem m, e.g $46|^8$ rem 443=85 and sends x to the system.
2) The system produces a random $e<2^t$-1 and sends the calculated value to the subscriber. In the context of the example t=6 and consequently e=29.
3) The subscriber calculates $y=(r+s\cdot e)$ mod q and sends the calculated value y to the system. For the example y=(8+3·29) mod 11=5.
4) The system confirms the validity of the equality $x=(a|^y\otimes v|^e)$ rem m. For the above example this is satisfied as: $(46|^5\otimes 117|^{29})$ rem 443=85=x.

The modified Guillou-Quisquater scheme may be constructed as follows. The public key of the system contains the number n, which is chosen as the polynomial product of the two numbers p and q, or correspondent to primitive polynomials as well as with the number v. The private key is taken to be the code B such that $(J\otimes B|^v)$ rem n=1. E.g., p=19 and q=25, $p\otimes q=n$=11⊗19=443, if J=18, then B=39 and v=5.

The identification process involves the following actions:

1) The subscriber forms a random number r such that $1<r<n-1$, calculates $T=r|^v$ rem n and the value T is sent to the system. E.g., consider r=22, then $T=22|^5$ rem 443=159
2) The system produces a random d, that must be in the range $0<d<n$-1, e.g. d=28 and send it to the subscriber.
3) The subscriber calculates $D=r\otimes B|^d$ rem n and sends the calculated code to the system. E.g. D=22 ⊗ $39|^{28}$ rem 443=187.
4) The system calculates $T'=D|^v\otimes J|^d$ rem n and if $T=T'$, then the result of the identification exercise is considered successful. For the example $T'=187|^5\otimes 18|^{28}$ rem 443=159.

From the above given outline descriptions of the modified zero knowledge architectures, it follows that for FFSIS the operation $y^2\cdot v$ mod m that determines the speed of operation changes to $y|^2\otimes v$ rem m and for the Schnorr and Guillou & Quisquater schemes the operation $(A^v\cdot B^w)$ mod m changes to $(A|^v\otimes B|^w)$ rem m.

IV. The Organization of Effective Exponential in the Galois Algebra and Estimation of the Efficiency

For the efficient calculation of the Galois field there exists a property of the square of the number A without carry that allows increased efficiency. This property states that "*the even bits of the binary code are equal to zero and the odd bits are identical to those of the number A*". For example, if $A=\mathbf{1101}_2$, then $A|^2=\mathbf{1010001}_2$.

Taking into account the property mentioned above, the calculation of the fundamental operation of FFSIS - $y|^2\otimes v$ rem m may be organized according to the following way. Given that the public key v- is constant, then it may be pre-calculated and stored in tabular form V, with V[1]=v, V[2]= $v\cdot 4$ rem m, V[3]=$v\cdot 4^2$ rem m,..., V[k]=$v\cdot 4^{k-1}$ rem m, where *m has k*+1 bits. Defining $y_1,y_2,...,y_k$ the binary bits y: $y = y_1 + y_2\cdot 2 +...+ y_k\cdot 2^{k-1}$, then using the pre-calculated table, the operation - $y|^2\otimes v$ rem m takes the form:

$$y|^2 \otimes v \text{ rem } m = y_1\cdot V[1]\oplus y_2\cdot V[2] \oplus y_3\cdot V[3]\oplus ... \oplus y_k\cdot V[k]. \quad (3)$$

Following the software processing of the k – bit number using a w – bit processor, the number is divided into s blocks ($s=k/w$). Correspondingly the time $T_{м1}$ for the calculation of (3) involves $T_{м1} = k\cdot s\cdot t_o$ /2, where t_o – the time for completion of the XOR operations in the processor, which according to [5] is equal to - τ, $T_{m1}\approx k\cdot s/2$.

Executing the basic case of FFSIS with modular multiplication $A\cdot B$ mod M in a software implementation, requires either classical algorithms or the use of the Barrett algorithm [6]. The first of these algorithms demands for the calculation A·B s^2 processor multiplication operations, for the reduction $s^2 + 2.5\cdot s$ processor multiplication operations and s processor division operations are required. Apart from that, after each multiplication or division operation, two addition operations also need to be performed at processor level.

This way the time required for the modular multiplication using the classical algorithm, is equal to

$T_c=2\cdot(s^2+1.25\cdot s)\cdot(t_m+2\cdot t_a)+s\cdot(t_d+2\cdot t_a)$, where t_m – the time for executing multiplication operations, t_a – time for execution of addition operations, t_d – time for execution of division operations. According to [5] $t_m \approx 10\cdot\tau$; $t_a \approx \tau$; $t_d \approx 30\cdot\tau$. Taking this into account $T_c \approx 24\cdot(s^2+1.5\cdot s)\cdot\tau+s\cdot 32\cdot\tau$. Similarly, for the Barrett algorithm the time required is $T_B \approx 24\cdot(s^2+2\cdot s)\cdot\tau$. A comparison between FFSIS software implementations for k=1024 is given in Table I.

TABLE I
RELATIONSHIP OF THE IMPLEMENTATION TIME IN SOFTWARE IMPLEMENTATION OF THE ORIGINAL AND MODIFIED FFSIS FOR K=1024

Processor Word length	Algorithm using the standard FFSIS approach for modular multiplication	
	Classic: $2\cdot T_c/T_{m1}$	Barrett : $2\cdot T_B/Tm1$
8	12.3	12.3
16	6.3	6.2
32	3.3	3.2
64	1.8	1.7

TABLE II
RELATION BETWEEN THE IMPLEMENTATION TIMES FOR SOFTWARE OF THE ORIGINAL AND MODIFIED SCHNORR AND GUILLOU- QUISQUATER FOR K=1024

	Processor Bits			
T_M / T_{m2}	8	16	32	64
	29	14.5	7.4	3.8

The original schemes for zero knowledge authentication by Schnorr and Guillou – Quisquater involve modular exponentiation operations. The most efficient algorithm for their implementation is considered to be the Montgomery algorithm. The cumulative time for its calculation is [6]: $T_M \approx 36\cdot k\cdot(s^2+s)\cdot\tau$.

For the fast implementation of the exponentiation $v|^E$ rem m in Galois Fields, it is proposed that pre-calculations be used, with the results being organized in the form of four tables. Apart from the table V mentioned above, it is proposed that three more be used, namely W, U and Y, that are formed during the pre-calculation phase as: W[1]= v, W[2]= $v\cdot 16$ rem m, W[3]=$v\cdot 16^2$ rem m,..., W[k]=$v\cdot 16^{k-1}$ rem m; U[1]=1, U[2]= 256 rem m, U[3]=256^2 rem m,..., U[k]= 256^{k-1} rem m; Y[1]=1, Y[2]= 16 rem m, Y[3]= 16^2 rem m,...,Y[k]= 16^{k-1} rem m.

The exponentiation process consists of the sequential analysis of the bits of the exponent $E=\{e_1,e_2,...,e_k\}$, starting with the largest. The difference of the proposed exponentiation process from classical exponentiation is that if three consecutive bits of the exponent are equal to zero, then using the table U $R|^8$ rem m may be immediately calculated; if two consecutive bits of the exponent are zero, then using the table Y $R|^4$ rem m may be immediately calculated; if the first of two consecutive bits is is zero and the second is one then using table W $R|^4\cdot$v rem m; finally if the consecutive bits are equal to one, then using the table V then $R|^2\cdot v$ rem m may be immediately calculated:

1. j = k, R=0
2. if j =4 goto 4
3. if $e_j=e_{j+1}=e_{j+2}=0$ then $R=r_1\cdot U[1]\oplus r_2\cdot U[2]\oplus r_3 U[3]\oplus...\oplus r_k\cdot U[k]$; $j=j-3$; goto 7;
4. if $e_j=0$ and $e_{j+1}=0$ then $R=r_1\cdot Y[1]\oplus r_2\cdot Y[2]\oplus r_3\cdot Y[3]\oplus...\oplus r_k\cdot Y[k]$; $j=j-2$; goto 7;
5. if $e_j=0$ and $e_{j+1}=1$ then $R=r_1\cdot W[1]\oplus r_2\cdot W[2]\oplus r_3\cdot W[3]\oplus...\oplus r_k\cdot W[k]$; $j=j-2$; goto 7;
6. $R=r_1\cdot V[1]\oplus r_2\cdot V[2]\oplus r_3\cdot V[3]\oplus...\oplus r_k\cdot V[k]$; j=j-1;
7. If $j>0$ return to 2.

It may be easily shown that using the proposed algorithm, the average number of steps for processing the exponent is $0.3125\cdot k$, which means more than three times fewer than the Montgomery Algorithm. The total time for exponentiation in the Galois Field using the proposed method is $T_{m2} = 0.15625\cdot k^2\cdot s\cdot\tau$. The results of the comparison of the time characteristics of the implementations of the Schnorr and Guillou-Quisquater identification schemes, together with the original and modified case are shown in Table II.

The analysis of the data presented in Tables I and II, demonstrates that the use of the proposed approach is more efficient if as user terminal equipment, short word – length controllers with independent power supplies and limited computational capabilities are used. The experimental research performed gave results that are close to those presented in Tables I and II.

During the implementation at hardware level, the transfer from modular implementation to multiplication in the Galois Field gives significant benefits in terms of speed and reduction in schemes complexity. A fundamental source of these simplifications is the simplified implementation of the addition of k-bit numbers.

For the implementation of the arithmetic adder, it is possible to employ a sequential scheme or a carry accelerator. The principle criterion for the efficiency of the proposed method is: T_{ASC}/T_{XOR} (T_{APC}/T_{XOR}) – the relation between operation time of the sequential adder's operation and the sequential (parallel) transfer of carries with the time of the logical adder, S_{ASC} / S_{XOR} (S_{APC}/S_{XOR}) – the relation between the complexity of the arithmetic adder with sequential (parallel) transfer with the complexity of the logical adder.

TABLE III
RELATION BETWEEN THE TIME FOR EXECUTION AND THE COMPLEXITY OF THE SCHEME WITH HARDWARE IMPLEMENTATION OF THE ARITHMETIC AND LOGIC ADDITION (IN BRACKETS FOR K=1024)

Efficiency Criterion	Carry scheme for the arithmetic adder	
	Sequential	Parallel
Time	$T_{ASC}/T_{XOR}=4.5\cdot k$ (4608)	$T_{APC}/T_{XOR} 1.5\cdot\log_2 k$ (15)
Complexity	$S_{ASC}/S_{XOR}=6$	$S_{APC}/S_{XOR}=6\cdot k^2$ (6144)

The data of the evaluation of the proposed implementation of the two cases of adders on FPGA are presented in Table III.

V. CONCLUSIONS

Schemes were proposed that increase the efficiency of three of the most commonly used zero knowledge identification methods, have been presented and thoroughly analyzed. The proposed approach increases the efficiency of hardware and software implementations by replacing multiplication operations of modular multiplication with polynomial multiplication in the Galois field. The relevant methods for producing keys for the zero knowledge identification methods have been modified. The proposed algorithms are efficient for the implementation of the proposed schemes in software. The analysis performed showed that the practical implementation of the proposed approach guarantees a significant (per order) increase of the efficiency of the identification in hardware implementations or for systems with user terminal devices that are mobile controllers with limited power.

REFERENCES

[1] Bardis N., Doukas N. and Markovskyi O., "Fast subscriber identification based on the zero knowledge principle for multimedia content distribution", International Journal of Multimedia Intelligence and Security 2010 - Vol. 1, No.4 pp. 363 - 377, 2010.

[2] Feige U.,Fiat A.,Shamir A. "Zero knowledge proofs of identity" // Journal of Cryptology, Vol.1, No.2 1988, P.77-94.

[3] Guillou L.C., Quisquater J.-J. "A Paradoxical Identity-Based Signature Schemes Resulting from Zero Knowledge" // Advances of Cryptology - Crypto-88. Proceeding.- Springer-Verlag.-1990.- P. 216-231.

[4] Schnorr C.P. "Efficient Signature Generation for Smart Cards" // Journal of Cryptology, Vol. 4, No.3.- 1991.- pp.161-174.

[5] Brey B.B. "The Intel Microprocessors". Sixth Edition. Prentice Hall: New Jersey.-2005.- 1328 p.

[6] N.G.Bardis, A.Drigas, A.P. Markovskyy and I.Vrettaros, "Accelerated Modular Multiplication Algorithm of Large Word Length Numbers with a Fixed Module". Communications in Computer and Information Science 111, Knowledge Management, Information Systems, E-Learning, and Sustainability Research, Third World Summit on the Knowledge Society, WSKS 2010 Corfu, Greece, September 2010 Proceedings, Part I, Springer – Verlag Berlin Heidelberg, pp 573-581, 2010, DOI: 10.1007/978-3-642-16324-1_58.