A Method for Strict Remote User Identification Using non - Reversible Galois Field Transformations

Nikolaos G. Bardis[1,*], *Oleksandr P. Markovskyi*[2], and *Nikolaos Doukas*[1]

[1]Department of Mathematics and Engineering Science, Hellenic Military Academy, Vari - 16673, Greece
[2]Department of Computer Engineering, Igor Sikorsky Kyiv Polytechnic Institute | National Technical University of Ukraine, Peremohy pr., Kiev 252056, KPI 2003, Ukraine

Abstract. This article proposes an approach that accelerates the realization of strict remote user identification using non reversible Galois field transformation. The proposed approach is based on using finite field arithmetic to replace the usual modular arithmetic. 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 identification methods, such as FFSIS, Schnorr and Guillou & Quisquater. The new method for user registration and identification procedure for obtaining access to the system, are illustrated. It is shown, both theoretically and experimentally that the proposed method attains a per order acceleration of the execution time required for the user identification by 2 – 3 orders of magnitude, via a hardware implementation.

1 Introduction

Given the current conditions of 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 architectures 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] [2]. In this context, the problem of acceleration of user identification based on zero knowledge is imminent and has a wide range of practical applications.

2 Identification Algorithms 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 process are the side-channel directed interactions with the system simultaneously with

* Nikolaos G. Bardis: bardis@ieee.org.org

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 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) [3], Guillou- Quisquater [4] and Schnorr identification schemes [5].

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 module $m=p\cdot q$. For the generation of public and private keys the subscriber selects the number v, which is been the quadratic residue on the module 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

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

If the intruder knows the public key v 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 [5]. 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 architecture 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 architecture is the modular exponentiation $a^y \cdot v^e \bmod p$.

Another classical zero-knowledge architecture, is the Guillou-Quisquater architecture [4]. 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=rv mod n and sends the value T to the system. E.g., consider r = 22, then T=2263 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 $D=r\cdot B^d \bmod n$ and sends it to the system. E.g. $D = 132\cdot 13^5 \bmod 209 = 176$.
4. The system calculates $T' = D^v\cdot J^d \bmod n$ and if T =T ', then the result of the identification is considered to be positive. For the example $T' =176^{63}\cdot 18^5 \bmod 209=132$.

Similarly to the Schnorr architecture, the fundamental operation in the case of the Guillou-Quisquater architecture 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 strict remote user authentication using non reversible Galois field transformation, which involves significantly smaller computational complexity and increases the speed of identification with software and hardware implementations.

3 Mathematical Basis

In order to achieve this goal it is necessary to employ a non – reversible Galois field transformation. Using classical algebra as the basis for non – reversible transformations, the modular exponentiation operation is most commonly used: $A^E \bmod M$. Correspondingly, using Galois field algebra for constructing such transformations, the Galois field exponentiation may be utilized as: $A|^E \text{ rem } M$ [1].

This operation involves two fundamental computational procedures: polynomial multiplication or multiplication without carry – MWC hence denoted as ⊗ and the polynomial division operation that calculates the remainder of the polynomial reduction of a polynomial $U(x)$ with the base polynomial $M(x)$ of the field, with the reduction operation hence denoted as U rem M.

In conventional algebra, a significant part of cryptographic mechanisms, including RSA, have modulo M as a foundation the product of two prime numbers: $M=p\cdot q$. Similar approaches may be applied concerning the creation of cryptographic mechanisms based on Galois fields. More specifically, such an approach is proposed in the context of the present research for the purpose of zero-knowledge identification of remote users.

The foundation of the proposed method lies in the following mathematical proposals.

If $q(x)$ is a prime polynomial degree w, then for every element k of the field $GF(2^w)$ that is formulated from this polynomial, the operation executed is:

$$k|^{h-1} \text{ rem } g = 1, \quad \text{where } h=2^w. \tag{1}$$

Lemma: if the polynomial $M(x)$ formulated by the field is a polynomial product $M(x) = q(x)\otimes g(x)$, of two prime polynomials $q(x)$ of degree w and $g(x)$ of degree v then for every k such that $0<k<h$ and for every l such that $0< l< u$, where $h=2^w$, $u=2^v$ then it is true that:

$$(k \otimes g)|^h \text{ rem } M = k \otimes g \qquad (2)$$
$$(l \otimes q)|^u \text{ rem } M = l \otimes q$$

Proof:

From (1) it is true that $k|^h = \mu\otimes q \oplus 1$, where μ is an integer.

It hence follows that (2) may be transformed as follows:

$(k\otimes g)|^h \text{ rem} M=(k|^h\otimes g|^h) \text{ rem } M=((\mu\otimes q)\oplus 1)\otimes g|^h) \text{ rem} M=$ $=(\mu\otimes g^{h-1}\otimes q\otimes g) \text{ rem } M\oplus g|^h \text{ rem } M=(\mu\otimes g^{h-1}\otimes M) \text{ rem } M\oplus g|^h \text{ rem } M$.

Since $(\mu\otimes g^{h-1}\otimes M) \text{ rem } M = 0$, expression (2) may be simplified as: $(k\otimes g)|^h \text{ rem } M=g|^h \text{ rem } M$.

Taking into account (1), $g|^h$ is reformulated as: $g|^h=\lambda\otimes q\oplus 1$, where λ is an integer.

Consequently, $g|^{h+1}=\lambda\otimes q\otimes g\oplus g$, and $g|^{h+1}$ rem $M=(\lambda\otimes q\otimes g\oplus g)$ rem $M=g$.

It follows directly from the Lemma that exponentiation in the field defined using a polynomial $M(x)=q(x)\otimes g(x)$, the numbers that are a polynomial product of numbers smaller that k with the number g, have a repetition equal to 2^w-1. Since from the point of view of authentication, the number g and consequently the respective period are not known for a value M, then property (2) may be used for the creation of method for strict cryptographic identification.

4 Registration And Identification Procedures

The proposed method involves two procedures: the user registration procedure and the procedure of a user identification procedure for obtaining access.

The proposed user registration procedure involves the following steps:

1. The user randomly selects two prime polynomials of different degrees; $q(x)$ of degree w: $q(x)=x^w+q_{u-1}\cdot x^{w-1}+\ldots+ q_1\cdot x+q_0$ and $g(x)$ of degree v: $g(x)= x^v+g_{v-1}\cdot x^v+\ldots+g_1\cdot x+g_0$, where $g_0,g_1,\ldots,g_{v-1} \in\{0,1\}$, $q_0,q_1,\ldots,q_{w-1} \in\{0,1\}$ and $w > v$.
2. The user formed the base polynomial $m(x)$ in the form of a polynomial product of the selected prime polynomials $g(x)$ and $q(x)$: $M(x)=g(x)\otimes q(x)$.
3. The user selects a random number $k\in\{1,..,2^w-1\}$ and performs the calculation of f as the exponent in the Galois field with the transformation of the polynomial $M(x)$: $f = g|^k$ rem M.
4. The user encrypts the codes M and f of the public key of the system and submits them to the system. The system receives and stores the codes M and f that are subsequently used as the public key of the authentication of the given user.

The proposed registration procedure is presented in the following example using small length numbers.

According to Step 1 of the proposed user registration procedure, two prime polynomial are selected of degrees w=6 and v =4: $q(x) = x^6 + x^4 + x^2 + x + 1$ and $g(x) = x^4 + x+1$; the first polynomial $q(x)$ corresponds to the number $q=1010111_2=87$, and the second polynomial $g(x)$ – to the number $g=10011_2=19$. Subsequently, according to Step 2, the polynomial product of the selected polynomials is calculated $M(x)=g(x)\otimes q(x)=x^{10}+x^8+x^7+x^3+1$. The calculation of the polynomial corresponds to the number $M(x)=g(x)\otimes q(x)=x^{10}+x^8+x^7+x^3+1$. Following that, according to Step 3 of the procedure, the user selects the random number $k=55\in\{1,..,2^6-1\}$, and calculates $f=g|^k$ rem $M=19|^{55}$ rem 1417=465. This number, together with the number M encrypts the public key of the system and sends it to the system.

The expanded procedure of a cycle of user identification involves the following steps:

1. The system forms a random number ξ and sends it to the user.
2. The user receives the code ξ from the system and calculates η such that the expression $\xi\cdot\eta$ mod $(2^w-1) = k$ is true.
3. The user calculates the session password p for current session in the form $p = g|^\eta$ rem M and the resulting p is sent to the system.
4. The system receives from the user the session password p and calculates $r = p|^\xi$ rem M. The result obtained is compared with the fixed for the particular code f of the user. If the two codes are identical, i.e. $r=f$ then the identification cycle is considered successful.

The proposed identification cycle procedure is illustrated using the following example that continues the previously given example.

The system randomly selects the number ξ = 34 and sends it to the user.

The user receives the code ξ = 34 from the system and finds η such that $\xi\cdot\eta$ mod $(2^w-1) = k$, or equivalently $34\cdot\eta$ mod 63 = 55. This condition is satisfied for η = 22. According to Step 3, the proposed identification procedure user calculates the session password for session p in the form:

$$p = g|^\eta \text{ rem } M = 19|^{22} \text{ rem } 1417 = 641.$$

The obtained password p=641 is sent to the system.

The system according to Step 4 receives from the user session password p and calculates

$$r = p|^\xi \text{ rem } M=641|^{34} \text{ rem } 1417 = 465.$$

Since the calculated code r = 465 is identical to the stored fixed code for the particular user f= 465, the identification cycle is considered successful.

5 Estimation of the Efficiency

The principal factors used for measuring the effectiveness of the proposed method for the proposed zero – knowledge remote user identification technique are:

- the level of security against attempts to acquire unauthorized access to system resources;
- the total amount of computational resources required for the execution of a cycle of identification. In reality, critical effectiveness factor is the time required for the execution of a identification cycle by system, as such systems typically have to serve extremely large numbers of user requests.

The repeated using of already transmitted session password p is impossible, as this changes after every new identification session. In effect, for by passing the proposed identification scheme, i.e. the production of a valid session password for the user, one of the polynomials $q(x)$ or $g(x)$ is necessary to be exposed.

With external intruders that may only have available a sequence t of session passwords p_1, $p_2\ldots$ p_t, the information they possess is insufficient and does not enable the recovery of the $g(x)$. The system possesses only the fundamental polynomial $M(x)$ and by pass of the identification in this context involves analyzing it

into simple multipliers, which for high enough powers of $M(x)$ is not realistically feasible in practice.

The fundamental advantage of the proposed method is the remote user identification based on the zero – knowledge principle, using Galois field algebra and hence obtaining increased possibilities for efficiency during user authentication. Efficiency is due to the following factors:

- Operations in the Galois fields are easily executable and require less time. More specifically, the fundamental operation of exponentiation of n bit numbers both in conventional and Galois field algebra involve in general operations of calculating squares and multiplication operations. Calculating squares in a Galois field does not require computational resources in practice and involves insertions of zeros between the bits of the number [1].
- During execution of operations in Galois fields, any processing of bits is independently executed without involving the transfer of any carry bits. The simulation in software showed that exponentiation in Galois fields is significantly faster compared to exponentiation in conventional algebra. Simulation in hardware [6] demonstrated an increase in efficiency by 2 – 3 orders of magnitude and a simultaneous simplification of the circuit necessary by 3 – 4 times.
- The research conducted demonstrated that the realistic values for the magnitude of the number ξ may be significantly smaller than the order of the polynomial $M(x)$, without effecting the level of security. In reality, the level of security is maintained even for a value of ξ equal to 2. For this reason, the magnitude of ξ is determined by the actual number of possible identification cycles. The use of relatively small values for the magnitude of ξ multiply reduces the time required for exponentiation.
- The proposed method, contrary to existing techniques uses a single session for the identification of the user by system.

6 Conclusions

In this paper, zero – knowledge user identification using non – reversible transformation in Galois fields was investigated and a scheme for such identification was proposed. For this purpose a theoretical study was conducted of the properties of specific cycles that appear during exponentiation in the context of special cases of Galois fields. The theoretical results enabled the development of procedures for the registration and identification of remote users. It was theoretically determined that the level of security attained does not differ from existing zero knowledge systems. The principal advantage of the proposed method is the possibility of achieving significantly higher rates of identification. This increased rate is of vital importance in current applications with ever growing numbers of system users and the necessity for remote information processing. Maximum effectiveness of the proposed method is attained by implementation in hardware.

References

1. Bardis, Nikolaos, Nikolaos Doukas, and Oleksandr P. Markovskyi. "Fast subscriber identification based on the zero knowledge principle for multimedia content distribution." International Journal of Multimedia Intelligence and Security 1.4 363-377, (2010)
2. Stavroulakis Peter, et al. Efficient zero—Knowledge identification based on one way Boolean transformations. In: GLOBECOM Workshops (GC Wkshps), 2011 IEEE.,. p. 275-280. (2011)
3. Feige U.,Fiat A.,Shamir A. “Zero knowledge proofs of identity” // Journal of Cryptology, Vol.1, No.2, P.77-94, (1988)
4. Guillou L.C., Quisquater J.-J. A Paradoxical Identity-Based Signature Schemes Resulting from Zero Knowledge // Advances of Cryptology - Crypto-88. Proceeding.- Springer-Verlag.- P. 216-231,(1990)
5. Schnorr C.P. Efficient Signature Generation for Smart Cards // Journal of Cryptology, Vol. 4, No.3.- pp.161-174, (1991)
6. Brey B.B. The Intel Microprocessors. Sixth Edition. Prentice Hall: New Jersey.- 1328 p., (2005)