Digital Signature Schemes over the Ring of Gaussian Integers

Xuedong Dong

College of Information Engineering, Dalian University, Dalian 116622, P.R.China

dongxuedong@sina.com

Keywords: Digital signature scheme; Discrete logarithms; The ring of Gaussian integers

Abstract. In this paper, the ring of Gaussian integers instead of the integer ring is used to construct the extended ElGamal digital signature schemes with appendix and message recovery. This approach has many advantages over the classical digital signature scheme. An example is given to show the validity of the proposed extensions of digital signature schemes.

Introduction

A public-key cryptosystem and a digital signature scheme were proposed by ElGamal based on the Discrete Logarithm problem in the group of units of the ring of integers modulo a prime [1].This encryption scheme and digital signature scheme can be easily generalized to work in any finite cyclic group G. The group G should be carefully chosen so that the group operations in G would be relatively easy to apply for efficiency. The naive algorithm for computing discrete logarithms in G is to raise a generator of G to higher and higher powers until the desired element is found. This algorithm requires running time linear in the size of the group G and thus exponential in the number of digits in the size of the group. Thus, if the order of G is big enough, the Discrete Logarithm problem in G should be computationally infeasible for the security of the protocol that uses the ElGamal public-key cryptosystem and digital signature scheme. The groups of most interest in cryptography are the multiplicative groups of finite fields. The ring of Gaussian integers is a unique factorization domain and has many good properties [2, 3, 4].There are algorithms for computing the greatest common divisor of two Gaussian integers [5, 6, 7].The extension of the ElGamal public key cryptosystem to the ring of Gaussian integers is given in [8]. ELKamchouchi et al. [9, 10] proposes extensions for the RSA cryptosystem and digital signature schemes to the ring of Gaussian integers. However, it is necessary that the message integer be located in a well defined validity region in the Gauss plane which is unpractical. In this paper, the extensions of the ElGamal digital signature schemes with appendix and message recovery to the ring of Gaussian integers are given and proved. A clear algorithm is given for computing $\beta^n \left(mod \alpha\right)$, where β, α are Gaussian integers.This approach has many advantages. Firstly, due to the arithmetic of the ring of Gaussian integers the extended Euler-phi function of a prime integer p equals $p^2 - 1$, compared to $p-1$ in the ring of integers Z. The encryption exponent is chosen to be co-prime to the extended Euler-phi function, which provides more security than that of the classical case. Secondly, if the modulus is a product of two non-real Gaussian primes, the difficulty of factoring the modulus is enhanced since factorization of elements over the ring of Gaussian integers is more complex than that of elements over the integer ring. Finally, the procedures used are similar to those used in Z with the extension to include negative integers. An example is given to show the validity of the proposed extensions of the ElGamal digital signature schemes. The rest of this paper is organized as follows. In Section 2 we give some preliminaries about the ring of Gaussian integers. In Section 3 and Section 4 we give extended ElGamal digital signature schemes in the ring of Gaussian integers. Finally, concluding remarks are given in Section 5.

Preliminaries

The Gaussian integer ring is $Z[i]=\{a+bi \mid a,b\in Z\}$. The norm of a Gaussian integer $a+bi$ is defined by $N(a+bi)=a^2+b^2$. There are 4 inverse elements $\pm 1, \pm i$. The elements $\pm 1(a+bi)$, $\pm i(a+bi)$ are called the associates of $a+bi$. The Gaussian primes are $1+i$ and its associates, the rational primes $p\equiv 3(\bmod 4)$ and their associates, and the factors $a+bi$ of the rational primes p with $p\equiv 1(\bmod 4)$. The first few Gaussian primes that equal a natural prime $4k+3$ are 3,7,11,19,23,31,43,47,59,67,71,83. Some non-real Gaussian primes are $1+i, 2+i, 3+2i, 4+i, 5+2i, 7+i, 5+4i, 7+2i, 6+5i, 8+3i, 8+5i, 9+4i$. The Gaussian integer ring is a unique factorization domain, that is, each non-zero Gaussian integer can be written as a unique product of Gaussian primes apart from the order of the primes, the presence of inverse elements, and ambiguities between associated primes. For $\alpha=x+yi\in Q(i)$, where x,y are rational numbers, let $a+bi=\lfloor x+1/2\rfloor+\lfloor y+1/2\rfloor i,$where the symbol $\lfloor z\rfloor$ denotes the greatest integer of less or equal to z, then $N[\alpha-(a+bi)]=(x-a)^2+(y-b)^2\le 1/4+1/4=1/2$. In the following we use $\lfloor \alpha\rfloor$ to denote $a+bi=\lfloor x+1/2\rfloor+\lfloor y+1/2\rfloor i$ for $\alpha=x+yi\in Q(i)$. A clear algorithm is given for computing $\beta(mod\gamma)$ by $\beta\text{-}\lfloor \beta/\gamma\rfloor\gamma=\beta\text{-}\lfloor \beta\bar{\gamma}/N(\gamma)\rfloor\gamma$, where $\bar{\gamma}$ is the complex conjugation of γ.We can use the Maple software to give a program to compute $\beta(mod\gamma)=\beta\text{-}\lfloor \beta\bar{\gamma}/N(\gamma)\rfloor\gamma.$ The analogue of Fermat's theorem for $Z[i]$ is as follows.

Theorem 1. [11] Let π_1,π_2 be Gaussian primes, where π_1 is not an associate of π_2, $\alpha=\pi_1\pi_2$, $\phi(\alpha)=[N(\pi_1)-1][N(\pi_2)-1]$. Then $\beta^{\phi(\alpha)}\equiv 1(\bmod\alpha)$ for any Gaussian integer β with$(\beta,\alpha)=1$ and $\beta^{\phi(\alpha)t+1}\equiv\beta(\bmod\alpha)$ for any Gaussian integer β.

Extended ElGamal Digital Signature Scheme with Appendix

The fundamental objective of cryptography is to enable two people, usually referred to as Alice and Bob, to communicate over an insecure channel in such a way that an opponent, Eve, cannot understand what is being said.

Let H is a public cryptographic hash function, which will take a message of arbitrary length and produce a message digest of a specified size. Suppose Alice wants to sign a message m which is a positive integer such that the message is not easily recovered from the signature and the message must be included in the verification procedure.She must do the following:

(1) Choose Gaussian primes π_1,π_2 such that $N(\pi_1)-1, N(\pi_2)-1$ should have at least one "large" prime factor, where π_1 is not an associate of π_2, and compute $\alpha=\pi_1\pi_2$, $\phi(\alpha)=[N(\pi_1)-1][N(\pi_2)-1]$.

(2) Choose an Gaussian integer $\beta=c+di$ such that $(N(\beta),N(\alpha))=1$ which implies that $(\beta,\alpha)=1$.

(3) Choose a random positive integer a such that $1<a<\phi(\alpha)-1$, and calculate $\beta^a(mod\alpha)=\beta^a\text{-}\lfloor \beta^a\bar{\alpha}/N(\alpha)\rfloor\alpha.$

(4) Select an encryption exponent e such that e is coprime to the extended Euler-phi function$\phi(\alpha)$,i.e.$(e,\phi(\alpha))=1$, compute $\xi=\beta^e(mod\alpha)=\beta^e\text{-}\lfloor \beta^e\bar{\alpha}/N(\alpha)\rfloor\alpha.$

(5) Use the extended Euclidean algorithm to compute a unique integer$h$,$0<h<\phi(\alpha)$, from $eh\equiv 1(\bmod\phi(\alpha))$.

(6) Compute $s\equiv h(H(m)-a)(\bmod\phi(\alpha))$. $(H ,\alpha ,\beta ,\beta\ (mod\alpha$ as public parameter is made public.

The signed message is the triple $(H(m), s, \xi)$.

Bob can verify the signature as follows.

(1) Download Alice's public key $(\alpha, \beta, \beta^a(mod\alpha))$.

(2) Compute $\beta^a\xi^s(\bmod\alpha)$.

(3) The signature is declared valid if and only if $\beta^a\xi^s \equiv \beta^{H(m)}(\bmod\alpha)$.

We now show that the verification procedure works.

Assume the signature is valid. Since $s \equiv h(H(m)-a)(\bmod\phi(\alpha))$, we have $s = h(H(m)-a) + \phi(\alpha)t$ and $\beta^a\xi^s \equiv \beta^a\beta^{es} \equiv \beta^a\beta^{eh(H(m)-a)} \equiv \beta^{H(m)}\beta^{\phi(\alpha)l} \equiv \beta^{H(m)}(\bmod\alpha)$ by Theorem 1.

The security of the system will be in the fact that a, π_1 and π_2 are kept private. It is difficult for an adversary to determine a from $(\alpha, \beta, \beta^a(mod\alpha))$ since the Discrete Logarithm problem is considered difficult.It is very important to keep a in secret. If Eve discovers the value of a, then she can perform the signing procedure and produce Alice's signature on any desired document. If Eve has another message m , she cannot compute the corresponding s since she doesn't know a and h . Suppose she tries to bypass this step by choosing an s that satisfies the verification equation. This means she needs s to satisfy $\beta^a\xi^s \equiv \beta^{H(m)}(\bmod\alpha)$ which is a Discrete Logarithm problem.

Example 1. Alice wants to sign a message m. Suppose $H(m) = 12345$ .She does the following:

(1) Choose Gaussian primes $\pi_1 = 11, \pi_2 = 19$ and compute $\alpha = \pi_1\pi_2 = 209$ $\phi(\alpha) = [N(\pi_1)-1][N(\pi_2)-1] = 43200$

(2) Choose an Gaussian integer $\beta = 7+13i$ and a random positive integer $a = 331$, and calculate $\beta^a(mod\alpha) = \beta^a$-$\lfloor \beta^a\overline{\alpha}/N(\alpha) \rfloor\alpha = -125-53i.$

(3) Select an encryption exponent $e = 1391$ and compute $\xi = \beta^e(mod\alpha) = \beta^e$-$\lfloor \beta^e\overline{\alpha}/N(\alpha) \rfloor\alpha = -92-46i.$

(4) Use the extended Euclidean algorithm to compute a unique integer $h = 15311$ from $1391h \equiv 1(\bmod 43200)$.

(5) Compute $s \equiv h(H(m)-a) = 15311(12345-331)(\bmod 43200) = 754$.

$(\alpha, \beta, \beta^a(mod\alpha)) = (209, 7+13i, -125-53i)$ as public parameters is made public.The signed message is the triple $(H(m), s, \xi) = (12345, 754, -92-46i)$.

Bob can verify the signature as follows.

(1) Download Alice's public key $(\alpha, \beta, \beta^a(mod\alpha)) = (209, 7+13i, -125-53i)$.

(2) Compute $\beta^a\xi^s(\bmod\alpha) = (-125-53i)(-145-100i)(\bmod\alpha) = -133-88i.$

(3) Since $\beta^a\xi^s \equiv -133-88i \equiv \beta^{H(m)}(\bmod\alpha),$ the signature is declared valid.

Extended ElGamal Digital Signature Scheme with Message Recovery

Suppose Alice wants to sign a message such that the message is readily obtained from the signature. She need modify the above scheme as follows:

Choose Gaussian primes $\pi_1, \pi_2, \beta = c+di, e, h$ as before. Choose a random positive integer a so that $1 < a < \phi(\alpha)-1.$ The public-key is $(\alpha, h, \beta^a(mod\alpha)),$ the private key is $(e, a, \beta, \phi(\alpha)).$ To sign a message m , where $1 < m < \sqrt{N(\alpha)}$ (if m is larger, break it into smaller blocks), Alice computes $\vartheta = \beta^{\phi(\alpha)-a}(\bmod\alpha).$ The signature is $(m, \rho = \vartheta m^e(\bmod\alpha)).$ Bob can then verify that Alice really signed the message by doing the following:

Download Alice's $(\alpha, h, \beta^a(mod\alpha)).$ Calculate $m_1 = (\rho\beta^a)^h(\bmod\alpha).$ If $m_1 = m$, then Bob accepts the signature as valid; otherwise the signature is not valid.

This works because $(\rho\beta^{a})^{h} \equiv (\vartheta m^{e}\beta^{a})^{h} \equiv \beta^{(\phi(\alpha)h-ah)}\beta^{ah}m^{he} \equiv m(\bmod\,\alpha)$ by Theorem 1. If there is another positive integer s such that $1<s<\sqrt{N(\alpha)}$ and $s\equiv(\rho\beta^{a})^{h}(\bmod\,\alpha),$ then $s\equiv m(mod\,\alpha)$ and therefore $N(\alpha)\,|\,N(s-m)=(s-m)^{2}.$ From $|\,s-m\,|<\sqrt{N(\alpha)}$ it follows that $s=m.$

Summary

This paper proposes extensions for the ElGamal digital signature schemes with appendix and message recovery to the ring of Gaussian integers. The proposed extensions have many advantages over the classical ElGamal digital signature scheme. The security of the proposed extensions is based on the difficulty to solve the Discrete Logarithm problem over the ring of Gaussian integers. It is not necessary that the message integer be located in a well defined validity region in the Gauss plane unlike in [9, 10]. Furthermore, the proposed scheme is more efficient than existing schemes in [12] in terms of computational cost.

Acknowledgements

This research was financially supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31 (1985), 469-472.

[2] X. Dong,C.B. Soh, E. Gunawan and L. Tang,Groups of algebraic integers used for coding QAM signals,IEEE Transactions on Information Theory, 44 (1998), 1848-1860.

[3] P. Bundschuh, K. Väänänen,Linear independence of q-Logarithms over the Gaussian integers, International Journal of Mathematics and Mathematical Sciences, 2010 (2010), 1-14.

[4] G. Greaves,Cyclotomic matrices over the Eisenstein and Gaussian integers, Journal of Algebra, 372 (2012), 560-583.

[5] George E. Collins, A fast Euclidean algorithm for Gaussian integers, Journal of Symbolic Computation, 33 (2002), 385-392.

[6] H. Rolletschek,On the number of divisions of the Euclidean algorithm applied to Gaussian integers, Journal of Symbolic Computation,2 (1986) ,261-291.

[7] A. Weilert, $(1+i)-$ary GCD computation in $Z\left[i\right]$ as an analogue to the binary GCD algorithm, Journal of Symbolic Computation, 30 (2000) ,605-617.

[8] AH-Kassar, M. Rizk, N.M.Mirza, and Y.A.Awad, ElGama1 public key clyptosystem in the domain of Gaussian integers, International Journal of Applied Mathematics,7 (2001), 405-412.

[9] H.ELKamchouchi, K.ELShenawy and H.A.Shaban,Extended RSA cryptosystem and digital signature schemes in the domain of Gaussian integers, 8'International Conference on Communication Systems (ICCS 2002), 91-95, Singapore, 2002.

[10] H.ELKamchouchi, K.ELShenawy and H.A.Shaban, Two new public key techniques in the domain of Gaussian integers, Twentieth National Radio Science Conference (NRSC 2003), 17-20, Cairo,Egpt, 2003.

[11] X.Dong, A new verifiable multi-secret sharing scheme over the ring of Gaussian integers, Journal of Computational Information Systems,to be published.

[12] X. Dong,L. Hou and Y.Zhang，Public key cryptosystem and signature schemes over the ring of Eisenstein integers，2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP),210-214 ,Beijing, China, 2013.