Electronic Notes in Theoretical Computer Science 186 (2007) 67–84 

[www.elsevier.com/locate/entcs](http://www.elsevier.com/locate/entcs)

General Secret Sharing Based on the Chinese Remainder Theorem with Applications in

E-Voting

# Sorin Iftene[1](#_bookmark0)

*Faculty of Computer Science “Al.I.Cuza” University*

*Ia¸si, Romania*

Abstract

Threshold secret sharing based on the Chinese remainder theorem has been considered by Mignotte [[23](#_bookmark31)] and Asmuth and Bloom [[1](#_bookmark9)]. In this paper we demonstrate that the Chinese remainder theorem can be used for realizing more general access structures, as the compartmented or the weighted threshold ones. We also prove that there exist some non-weighted threshold access structures whose realizations require the general variant of the Chinese remainder theorem, i.e., the variant in which the modules are not necessarily pairwise coprime.

As an application of the proposed secret sharing schemes, we present a multi-authority e-voting schemes in which, as a novelty, the tallying authorities may have non-equal weights.

*Keywords:* secret sharing, Chinese remainder theorem, e-voting

# Introduction and Preliminaries

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* (or *shadows*) which are distributed to users. The secret may be recovered only by certain groups which belong to a predetermined *access structure*. In the first secret sharing schemes only the number of shares was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes. We mention here Shamir’s scheme [[29](#_bookmark37)] based on polynomial interpolation, Blakley’s geometric scheme [[5](#_bookmark13)], Mignotte’s scheme [[23](#_bookmark31)] and Asmuth-Bloom scheme [[1](#_bookmark9)], both based on the Chinese remainder theorem. Ito, Saito, and Nishizeki [[19](#_bookmark25)], Benaloh and Leichter

[[4](#_bookmark11)] have proposed constructions for more general secret sharing schemes.

In this paper we prove that the Chinese remainder theorem can be used for realizing more general access structures. We consider first the *compartmented* secret

1 Email: [siftene@infoiasi.ro](mailto:siftene@infoiasi.ro)

1571-0661 © 2007 Elsevier B.V. Open access under [CC BY-NC-ND license.](http://creativecommons.org/licenses/by-nc-nd/3.0/)

doi:10.1016/j.entcs.2007.01.065

sharing schemes, in which the set of users is partitioned into compartments and the secret can be recovered if and only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold and the total number of participants is greater than or equal to a global threshold. We extend Brickell’s construction [[6](#_bookmark14)] to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we indicate how to use the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares.

We also extend the threshold Mignotte and Asmuth-Bloom schemes in order to address more general access structures. We present how to realize any *weighted threshold* access structure (in which some positive weight is associated to each user and the secret can be reconstructed if and only if the sum of the weights of the participants is greater than or equal to a fixed threshold) but we prove that our extensions are also suitable for some non-weighted threshold access structures.

The paper is organized as follows. The rest of this section is dedicated to some preliminaries on number theory, focusing on the Chinese remainder theorem. After a short introduction to secret sharing, we survey the threshold secret sharing schemes based on the Chinese remainder theorem in Section 2. In Section 3 we extend the Brickell’s construction for compartmented secret sharing to the case that the global threshold is strictly greater than the sum of the compartment thresholds and we indicate how to use the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares. In Section 4 we extend the threshold secret sharing schemes based on the Chinese remainder theorem to more general access structures and discuss the homomorphic properties of the resulted schemes. In Section 5 we describe a multi-authority e-voting scheme based on the proposed secret sharing schemes. Our conclusions and some interesting future research directions are presented in the last section.

In the rest of this section we present some basic facts and notations from number theory. For more details, the reader is referred to [[8](#_bookmark16)].

Let *a, m* ∈ Z, *m* /= 0. The *quotient* of the integer division of *a* by *m* will be denoted by *a* div *m* and the *remainder* will be denoted by *a* mod *m*. Let *a, b, m* ∈ Z. We say that *a* and *b* are *congruent modulo m*, and we use the notation *a* ≡ *b mod m*, if *m*|(*a* — *b*). In case *m* /= 0, *a* ≡ *b mod m* is equivalent with *a* mod *m* = *b* mod *m.* The set {0*,* 1*,... ,m* — 1} will be denoted by Z*m*, for any integer *m* ≥ 1*.*

Let *a*1*,... , an* ∈ Z, *a*2 + ··· + *a*2

/= 0. The *greatest common divisor* (*gcd*)

1 *n*

of *a*1*,... , an* will be denoted by (*a*1*,... , an*). It is well-known that there exist

*α*1*,... , αn* ∈ Z that satisfy *α*1*a*1 + ··· + *αnan* = (*a*1*,... , an*) (the linear form of the

*gcd*).

Let *a*1*,... , an* ∈ Z such that *a*1 ··· *an* /= 0. The *least common multiple* (*lcm*) of

*a*1*,... , an* will be denoted by [*a*1*,... , an*].

The Chinese remainder theorem has many applications in computer science (see [[10](#_bookmark18)] for a survey on this topic). We only mention its applications to the *RSA* decryption algorithm as proposed by Quisquater and Couvreur [[27](#_bookmark35)], the discrete logarithm algorithm as proposed by Pohlig and Hellman [[26](#_bookmark34)], and the algorithm

for recovering the secret in Mignotte’s threshold secret sharing scheme [[23](#_bookmark31)] or in Asmuth-Bloom threshold secret sharing scheme [[1](#_bookmark9)].

Several versions of the Chinese remainder theorem have been proposed. The next one is called the *general* Chinese remainder theorem ([[24](#_bookmark32)]):

Theorem 1.1 *Let k* ≥ 2*, p*1*,... , pk* ≥ 2*, and b*1*,... , bk* ∈ Z*. The system of equa- tions*

⎧⎪ *x* ≡ *b*1 *mod p*1

⎪⎨ *.*

⎪⎪⎩ *x* ≡ *bk mod pk*

*has solutions in* Z *if and only if bi* ≡ *bj mod* (*pi, pj*)*, for all* 1 ≤ *i, j* ≤ *k. Moreover, if the above system of equations has solutions in* Z*, then it has a unique solution in* Z[*p*1*,...,pk*]*.*

Ore has proven that this solution can be obtained as

Σ *γiδibi* mod [*p*1*,... , pk*]*,*

*k*

*i*=1

where *δi* = [*p*1*,...,pk*] , for all 1 ≤ *i* ≤ *k,* and *γ*1*,... , γk* are arbitrary integers such that

*pi*

*γ*1*δ*1 + ··· + *γkδk* =1 (remark that (*δ*1*,... , δk*)= 1).

When (*pi, pj*) = 1, for all 1 ≤ *i < j* ≤ *k*, one gets the *standard* version of the Chinese remainder theorem. Garner [[13](#_bookmark21)] has found an efficient algorithm for this case and Fraenkel [[12](#_bookmark20)] has extended it to the general case.

# Threshold Secret Sharing Schemes Based on the Chi- nese Remainder Theorem

We present first some basic facts about secret sharing schemes. The reader is referred to [[31](#_bookmark39)] for a survey on this topic. Suppose we have *n* users labeled with the numbers 1*,... ,n* and consider a set of groups [2](#_bookmark1) A ⊆ P({1*,* 2*,... , n*}). Informally, an A*-secret sharing scheme* is a method of generating (*S,* (*I*1*,... , In*)) such that

* (*correctness*) for any *A* ∈ A, the problem of finding the element *S*, given the set

{*Ii* | *i* ∈ *A*}, is “easy”;

* (*security*) for any *A* ∈ P({1*,* 2*,... , n*}) \ A, the problem of finding the element *S*, given the set {*Ii* | *i* ∈ *A*}, is intractable.

The set A will be referred to as the *authorized access structure* or simply as the *access structure*, *S* will be referred to as the *secret* and *I*1*,... , In* will be referred to as the *shares* (or the *shadows*) of *S*. The elements of the set A will be referred to as the *authorized groups*.

2 P({1*,* 2*, ... , n*}) denotes the set of all subsets of the set {1*,* 2*,. .. , n*}.

In a *perfect* secret sharing scheme, the shares of any unauthorized group give no information (in information-theoretic sense) about the secret. Karnin, Greene, and Hellman [[20](#_bookmark26)] have proven, using the concept of entropy, that in any perfect threshold secret sharing scheme, the shares must be at least as long as the secret and, later on, Capocelli, De Santis, Gargano, and Vaccaro [[7](#_bookmark15)] have extended this result to the case of any perfect secret sharing scheme. In an *ideal* secret sharing scheme, the shares are as long as the secret.

A natural condition is that an access structure A be *monotone* ([[4](#_bookmark11)]), i.e., (∀*B* ∈ P({1*,* 2*,... , n*}))((∃*A* ∈ A)(*A* ⊆ *B*) ⇒ *B* ∈ A)*.*

Any monotone access structure A is well specified by the set of the minimal authorized groups, i.e., the set A*min* = {*A* ∈ A|(∀*B* ∈ A \ {*A*})(¬*B* ⊆ *A*)}. Also, the unauthorized access structure A, A = P({1*,* 2*,... , n*}) \ A, is well specified by the set of the maximal unauthorized groups, i.e., the set A*max* = {*A* ∈ A|(∀*B* ∈ A\ {*A*})(¬*A* ⊆ *B*)}.

In the first secret sharing schemes only the number of the participants in the reconstruction phase was important for recovering the secret. Such schemes have been referred to as *threshold* secret sharing schemes.

Definition 2.1 Let *n* ≥ 2, 2 ≤ *k* ≤ *n*. The access structure

A = {*A* ∈ P({1*,* 2*,... , n*}) | |*A*| ≥ *k*}

will be referred to as the (*k, n*)-*threshold* access structure.

In this case we also obtain that A*min* = {*A* ∈ P({1*,* 2*,... , n*}) | |*A*| = *k*},

A = {*A* ∈ P({1*,* 2*,... , n*}) | |*A*| ≤ *k* — 1}, and A*max* = {*A* ∈ P({1*,* 2*,... , n*}) |

|*A*| = *k* — 1}. Any A-secret sharing scheme will be referred to as an (*k, n*)*-threshold secret sharing scheme*.

We briefly discuss next the most important threshold secret sharing schemes based on the Chinese remainder theorem.

* 1. *Mignotte’s Threshold Secret Sharing Scheme*

Mignotte’s threshold secret sharing scheme [[23](#_bookmark31)] uses some special sequences of in- tegers, referred to as the *Mignotte sequences*.

Definition 2.2 Let *n* be a positive integer, *n* ≥ 2, and 2 ≤ *k* ≤ *n*. An (*k, n*)-

*Mignotte sequence* is a sequence of pairwise coprime positive integers *p*1 *< p*2 *<*

··· *< pn* such that

*k*−2 *k*

*pn*−*i <* *pi.*

*i*=0 *i*=1

The above inequality is equivalent with

*max*1≤*i*1*<*···*<ik*−1≤*n*(*pi*1 ··· *pik*−1 ) *< min*1≤*i*1*<*···*<ik*≤*n*(*pi*1 ··· *pik* )*.*

Given a publicly known (*k, n*)-Mignotte sequence, the scheme works as follows:

* The secret *S* is chosen as a random integer such that *β < S < α*, where *α* =

*k i*=1

*pi* and *β* = *k*−2 *pn*−*i*;

* The shares *Ii* are chosen as *Ii* = *S* mod *pi*, for all 1 ≤ *i* ≤ *n*;

*i*=0

* Given *k* distinct shares *Ii*1 *,... , Iik* , the secret *S* is recovered, using the stan- dard variant of the Chinese remainder theorem, as the unique solution modulo *pi*1 ··· *pik* of the system

⎪⎨ . *.*

⎧⎪ *x* ≡ *Ii*1 *mod pi*1

⎪⎪⎩ *x* ≡ *Iik mod pik*

Indeed, the secret *S* is an integer solution of the above system by the choice

of the shadows and, moreover, *S* lies in Z*pi* ···*pi*

because *S < α*. On the other

1 *k*

hand, having only *k* — 1 distinct shares *Ii*1 *,... , Iik*−1 , we obtain only that *S* ≡

*x*0 mod *pi*1 ··· *pik*−1 , where *x*0 is the unique solution modulo *pi*1 ··· *pik*−1 of the resulted system (in this case, *S > β* ≥ *pi*1 ··· *pik*−1 *> x*0). Therefore, in order to assure a reasonable level of security, (*k, n*)-Mignotte sequences with a large factor

*α*−*β*

*β*

must be chosen (a method of generating such sequences is presented in [[21](#_bookmark27),

page 9]).

Obviously, Mignotte’s scheme is not perfect, but it can lead to small shares and, thus, can be used in applications in which the compactness of the shares is the deciding factor.

We have extended Mignotte’s scheme in [[17](#_bookmark28)], by introducing the generalized threshold Mignotte sequences whose elements are not necessarily pairwise coprime.

Definition 2.3 Let *n* be an integer, *n* ≥ 2, and 2 ≤ *k* ≤ *n*. A *generalized* (*k, n*)*-*

*Mignotte sequence* is a sequence *p*1*,... , pn* of positive integers such that

*max*1≤*i*1*<*···*<ik*−1≤*n*([*pi*1 *,... , pik*−1 ]) *< min*1≤*i*1*<*···*<ik* ≤*n*([*pi*1 *,... , pik* ])*.*

It is easy to see that every (*k, n*)-Mignotte sequence is a generalized (*k, n*)- Mignotte sequence. Moreover, if we multiply every element of a (generalized) (*k, n*)- Mignotte sequence *p*1*,... , pn* by a fixed element *δ* ∈ Z, (*δ, p*1 ··· *pn*) = 1, we also obtain a generalized (*k, n*)-Mignotte sequence.

The extended Mignotte scheme works like Mignotte’s scheme, where *α* = *min*1≤*i*1 *<*···*<ik* ≤*n*([*pi*1 *,... , pik* ]) and *β* = *max*1≤*i*1 *<*···*<ik*−1≤*n*([*pi*1 *,... , pik*−1 ]). In this case, the general variant of the Chinese remainder theorem must be used for recov- ering the secret.

* 1. *Asmuth-Bloom Threshold Secret Sharing Scheme*

This scheme, proposed by Asmuth and Bloom in [[1](#_bookmark9)], also uses some special sequences of integers. More exactly, a sequence of pairwise coprime positive integers *p*0*, p*1 *<*

··· *< pn* is chosen such that

*k*−2 *k*

*p*0 · *pn*−*i <* *pi.*

*i*=0 *i*=1

Given a publicly known Asmuth-Bloom sequence, the scheme works as follows:

* The secret *S* is chosen as a random element of the set Z*p*0 ;
* The shares *Ii* are chosen as *Ii* = (*S* + *γ* · *p*0) mod *pi*, for all 1 ≤ *i* ≤ *n*, where *γ* is an arbitrary integer such that *S* + *γ* · *p*0 ∈ Z*p*1···*pk* ;
* Given *k* distinct shares *Ii*1 *,... , Iik* , the secret *S* can be reconstructed as *S* = *x*0 mod *p*0, where *x*0 is obtained, using the standard variant of the Chinese re- mainder theorem, as the unique solution modulo *pi*1 ··· *pik* of the system

⎪⎨ . *.*

⎧⎪ *x* ≡ *Ii*1 *mod pi*1

⎪⎪⎩ *x* ≡ *Iik mod pik*

Goldreich, Ron, and Sudan [[15](#_bookmark23)] have proposed choosing *p*0*, p*1*,... , pn* as prime numbers of the same size. Quisquater, Preneel, and Vandewalle [[28](#_bookmark36)] have proven that, by choosing *p*0*, p*1*,... , pn* as consecutive primes, the resulted schemes are asymptotically perfect and asymptotically ideal (for technical details, the reader is referred to [[28](#_bookmark36)]).

The sequences used in Asmuth-Bloom scheme can be also generalized by allowing modules that are not necessarily pairwise coprime in an obvious manner. We can use any sequence *p*0*, p*1*,* ··· *, pn* such that

*p*0 · *max*1≤*i*1 *<*···*<ik*−1 ≤*n*([*pi*1 *,... , pik*−1 ]) *< min*1≤*i*1*<*···*<ik* ≤*n*([*pi*1 *,... , pik* ])*.*

It is easy to see that if we multiply the elements, excepting the first one, of a (generalized) Asmuth-Bloom sequence *p*0*, p*1*,* ··· *, pn* with a fixed element *δ* ∈ Z, (*δ, p*0 ··· *pn*) = 1, we also obtain a generalized Asmuth-Bloom sequence.

# Compartmented Secret Sharing Based on the Chi- nese Remainder Theorem

In case of compartmented secret sharing, the set of users is partitioned into com- partments and the secret can be recovered only if the number of participants from any compartment is greater than or equal to a fixed compartment threshold, and the total number of participants is greater than or equal to a global threshold. The compartmented secret sharing has been discussed for the first time by Simmons in [[30](#_bookmark38)]. Simmons has presented the example of an official action that requires that at least two U.S. members and at least two U.S.S.R. members be simultaneously present for its initiation.

The compartmented access structures can be introduced as follows.

Definition 3.1 Let C = {*C*1*, C*2*,... , Cm*} be a partition of *C*0 = {1*,* 2*,... , n*} and consider a sequence K = (*k*0*, k*1*, k*2*,... , km*), where *kj* ≤ |*Cj*|, for all 0 ≤ *j* ≤ *m*,

and Σ*m kj* ≤ *k*0. The (C*,* K)-*compartmented access structure* is given by

*j*=1

A = {*A* ∈ P({1*,* 2*,... , n*}) |(∀*j* = 0*, m*)(|*A* ∩ *Cj*| ≥ *kj*)}*.*

In this case, any A-secret sharing scheme will be referred to as a (C*,* K)*- compartmented secret sharing scheme*. The sets *C*1*, C*2*,... , Cm* will be referred to as the *compartments* of the scheme, the values *k*1*, k*2*,... , km* as the *compartment thresholds* and *k*0 as the *global threshold* of the scheme.

An (*k, n*)-threshold secret sharing scheme is nothing else than a (C*,* K)- compartmented secret sharing scheme with C = {{1*,* 2*,... , n*}} (*m* = 1) and

K = (*k, k*).

Brickell [[6](#_bookmark14)] has proposed an elegant solution for the case *k*0 = Σ*m kj* by ex-

*j*=1

pressing the secret *S* as a combination of some compartment secrets *s*1*,... , sm*

and using an (*kj,* |*Cj*|)-threshold secret sharing scheme for obtaining the shares

{*Ii*|*i* ∈ *Cj*} corresponding to the compartment secret *sj*, for all 1 ≤ *j* ≤ *m*. In the reconstruction phase, if the number of participants from the *jth* com- partment is greater than or equal to *kj*, for all 1 ≤ *j* ≤ *m*, then all com- partment secrets can be recovered and, thus, the secret *S* can be obtained (re- mark that in this case the compartmented access structure can be simplified to

{*A* ∈ P({1*,* 2*,... , n*}) | (∀*j* = 1*, m*)(|*A* ∩ *Cj*| ≥ *kj*)}).

Ghodosi, Pieprzyk, and Safavi-Naini proposed an efficient scheme for the general case in [[14](#_bookmark22)].

We extend Brickell’s construction to the case Σ*m kj < k*0 as follows.

*j*=1

* The secret is chosen as *S* = *s*0 + *s*1 + ··· + *sm*, where *s*0*, s*1*,... , sm* are positive integers;
* The shares are chosen as *Ii* = (*gi, ci*), for any 1 ≤ *i* ≤ *n*, where
  + *g*1*,... , gn* are the shares corresponding to the secret *s*0 with respect to an ar- bitrary (*k*0*, n*)-threshold secret sharing scheme - these elements will be referred to as the *global* components of the shares;
  + for every 1 ≤ *j* ≤ *m*, {*ci*|*i* ∈ *Cj*} are the shares corresponding to the secret *sj* with respect to an arbitrary (*kj,* |*Cj*|)-threshold secret sharing scheme - these elements will be referred to as the *compartment* components of the shares.

Remark 3.2 (Correctness)

Let *A* be an authorized access group. Thus, |*A*|≥ *k*0 and, for all *j* = 1*, m*, |*A*∩*Cj*|≥ *kj*. Having at least *k*0 of the shares *g*1*,... , gn*, the value *s*0 can be obtained. Then, for any *j* = 1*, m*, having at least *kj* of the shares {*ci*|*i* ∈ *Cj*}, the value *sj* can be obtained, and finally, the secret *S* can be reconstructed as *S* = *s*0 + *s*1 + ··· + *sm*.

Remark 3.3 (Security)

Let *A* be an unauthorized access group. There are two possibilities:

* + - |*A*| *< k*0 - in this case, the value *s*0 can not be determined;
    - There is an compartment *j* such that |*A* ∩ *Cj*| *< kj* - in this case the value *sj* can not be determined.

In both cases, the secret *S* can not be reconstructed.

Using perfect threshold secret sharing schemes as building blocks can lead to large shares. We propose using the threshold secret sharing schemes based on the Chinese remainder theorem in order to decrease the size of shares, maintaining, at the same time, a reasonable level of security. For simplicity, we shall use only Mignotte’s scheme, but we have to mention that this technique can be also applied using Asmuth-Bloom scheme.

For any 0 ≤ *j* ≤ *m*, we will generate and broadcast a generalized (*kj,* |*Cj*|)- Mignotte sequence (*pj,i*|*i* ∈ *Cj*). Let *βj* = *maxi*1 *,...,ikj* −1 ∈*Cj* ([*pj,i*1 *,... , pj,ikj* −1 ]) and *αj* = *mini*1*,...,ik* ∈*Cj* ([*pj,i*1 *,... , pj,ik* ])*,* for 0 ≤ *j* ≤ *m*. We may use a generalized

*j j*

Mignotte sequence twice in case that *kj* = *kl* and |*Cj*| = |*Cl*|, for some 1 ≤ *j < l* ≤

*m*. The secret *S* is chosen as *S* = Σ*m sj*, where *βj < sj < αj*. The components

*j*=0

of the shares will be chosen as

*gi* = *s*0 mod *p*0*,i, ci* = *sc*(*i*) mod *pc*(*i*)*,i,*

where *c*(*i*) is the unique element *j*, 1 ≤ *j* ≤ *m*, such that *i* ∈ *Cj*, for all 1 ≤ *i* ≤ *n*.

Example [3.4](#_bookmark3) illustrates this scheme.

Example 3.4 (with artificially small parameters)

Let us consider *n* = 6, C = {{1*,* 2*,* 3}*,* {4*,* 5*,* 6}}, the compartment thresholds *k*1 = 2,

*k*2 = 2 and the global threshold *k*0 = 5. The sequence 5, 7, 11, 13, 17, 19 is a (5*,* 6)-Mignotte sequence, with *α*0 = 85085 and *β*0 = 46189*,* and the sequence 7, 11, 13 is a (2*,* 3)-Mignotte sequence with *α*1 = *α*2 = 77 and *β*1 = *β*2 = 13. We choose *s*0 = 50000, *s*1 = 30, and *s*2 = 40. The secret is *S* = 50070 and the corresponding shares are *I*1 = (0*,* 2), *I*2 = (6*,* 8), *I*3 = (5*,* 4), *I*4 = (2*,* 5), *I*5 = (3*,* 7),

and *I*6 = (11*,* 1).

Having the shares *I*1 = (0*,* 2), *I*2 = (6*,* 8), *I*4 = (2*,* 5), *I*5 = (3*,* 7), and *I*6 = (11*,* 1),

we solve the systems

⎧⎪ *x* ≡ 0 *mod* 5

⎪ *x* ≡ 6 *mod* 7

⎪⎨

*x* ≡ 2 *mod* 13 *,*

*x* ≡ 3 *mod* 17

⎪

⎪⎩ *x* ≡ 11 *mod* 19

⎧⎨ *x* ≡ 2 *mod* 7 *,*

⎩ *x* ≡ 8 *mod* 11

⎧⎨ *x* ≡ 7 *mod* 11 *,*

⎩ *x* ≡ 1 *mod* 13

and obtain, respectively, *s*0 = 50000, *s*1 = 30, *s*2 = 40, and finally *S* = 50070.

Let us analyze the security of the scheme. Let *B* be an unauthorized group and consider Δ*B* = {*j* ∈ {0*,* 1*,... , m*}| |*A* ∩ *Cj*| *< kj*}*.* The informations obtained from the shares corresponding to *B* lead to a set of possible vectors (*s*0*, s*1*,... , sm*)

of cardinality at least

*j*∈Δ*B*

*αj* −*βj* . The generalized Mignotte sequences can be

*j*

*β*

thus generated accordingly to the unauthorized access structure in order to obtain

a suitable security level.

Although the shares of our scheme have two components, by using Mignotte’s scheme as a building block, the sizes of shares can be smaller than the size of the secret. Further improvements can be obtained by choosing the Mignotte sequences and the values *s*0*, s*1*,... , sm* such that the global components of some shares coincide with the corresponding compartment ones, i.e., *gi* = *ci*, for some *i* ∈ {1*,* 2*,... , n*}. In this case we can define the share *Ii* as *Ii* = *gi* = *ci*. For this, we can generate first *s*1*,... , sm* and *c*1*,... , cn* and determining *s*0 by solving the system of equations

⎪⎨ . *.*

⎧⎪ *x* ≡ *c*1 *mod p*0*,*1

⎪⎪⎩ *x* ≡ *ck*0 *mod p*0*,k*0

We will choose *Ii* = *gi* = *ci*, for all 1 ≤ *i* ≤ *k*0, *gi* = *s*0 mod *p*0*,i* and *Ii* = (*gi, ci*), for all *k*0 +1 ≤ *i* ≤ *n*. Further improvements can be obtained in case that *s*0 mod *p*0*,i* = *sc*(*i*) mod *pc*(*i*)*,i*, for some *k*0 +1 ≤ *i* ≤ *n*.

Example [3.5](#_bookmark4) illustrates the reduction of the shares.

Example 3.5 (with artificially small parameters)

Let us reconsider Example [3.4](#_bookmark3). We choose *s*1 = 30 and *s*2 = 40. We obtain *c*1 = 2,

*c*2 = 8, *c*3 = 4, *c*4 = 5, *c*5 = 7, and *c*6 = 1. The system

⎧⎪ *x* ≡ 2 *mod* 5

⎪⎨ *x* ≡ 4 *mod* 11

⎪ *x* ≡ 8 *mod* 7

⎪ *x* ≡ 5 *mod* 13

⎪⎩ *x* ≡ 7 *mod* 17

has the solution *s*0 = 32817. The secret will be *S* = 32887 and the shares *I*1 = 2,

*I*2 = 8, *I*3 = 4, *I*4 = 5, *I*5 = 7, and *I*6 = (4*,* 1).

Thus, in case that *k*0 is close to *n*, real improvements related to the size of shares can be made. However, every compression of a share, i.e., any equalization of form

*g* = *c* , can affect the security with a factor of *αc*(*i*) −*βc*(*i*) . Thus, depending of the

*i i βc*(*i*)

intended application, a compromise between the size of the shares and the level of

security must be made.

# More General Secret Sharing Based on the Chinese Remainder Theorem

In this section we extend the threshold secret sharing schemes based on the Chinese remainder theorem in order to deal with more general access structures. For this, we will generalize the threshold Mignotte and Asmuth-Bloom sequences in a natural manner, the rest of these secret sharing schemes remaining unaffected.

We begin with extending Mignotte sequences.

Definition 4.1 Let *n* be a positive integer, *n* ≥ 2 and A ⊆ P({1*,* 2*,... , n*}). An

A*-Mignotte sequence* is a sequence of positive integers *p*1*,... , pn* such that

*β* = *maxB*∈A([{*pi*|*i* ∈ *B*}]) *< minA*∈A([{*pi*|*i* ∈ *A*}]) = *α.*

The above property is equivalent with

*maxB*∈A*max* ([{*pi*|*i* ∈ *B*}]) *< minA*∈A*min* ([{*pi*|*i* ∈ *A*}])*.*

If A is specified by A*min* = {*A* ∈ P({1*,* 2*,... , n*}) | |*A*| = *k*} then any A-Mignotte sequence is a generalized threshold (*k, n*)-Mignotte sequence in sense of Definition

[2.3](#_bookmark2). It is easy to see that if we multiply the elements of an A-Mignotte sequence *p*1*,* ··· *, pn* with a fixed element *δ* ∈ Z, (*δ, p*1 ··· *pn*) = 1, we also obtain an A- Mignotte sequence.

We will describe next how to construct Mignotte sequences in case of the weighted threshold access structures.

In a *weighted threshold* secret sharing scheme, a positive weight is associated to each user and the secret can be reconstructed if and only if the sum of the weights of all participants is greater than or equal to a fixed threshold. Such schemes have been considered for the first time by Shamir [[29](#_bookmark37)]. Shamir has discussed the case of sharing a secret between the executives of a company such that the secret can be recovered by any three executives, or by any executive and any vice-president, or by the president alone. The Shamir’s solution for this case is based on a threshold secret sharing scheme with the threshold 3. Thus, the president receives three shares, each vice-president receives two shares and, finally, every simple executive receives a single share.

The weighted threshold access structures can be introduced as follows.

Definition 4.2 Let *n* ≥ 2, *ω* = (*ω*1*,... , ωn*) a sequence of positive integers, and *w*

a positive integer such that 2 ≤ *w* ≤ Σ*n ωi*. The access structure

*i*=1

A = {*A* ∈ P({1*,* 2*,... , n*}) | Σ *ωi* ≥ *w*}

*i*∈*A*

will be referred to as the (*ω, w, n*)*-weighted threshold access structure*.

In this case, any A-secret sharing scheme will be referred to as an (*ω, w, n*)*- weighted threshold secret sharing scheme*. The parameters *ω*1*,... , ωn* will be referred to as the *weights* and *w* will be referred to as the *threshold* of the scheme.

An (*k, n*)-threshold secret sharing scheme is nothing else than an (*ω, w, n*)- weighted threshold secret sharing scheme with *ω*1 = ··· = *ωn* =1 and *w* = *k*.

In case that A is the (*ω, w, n*)-weighted threshold access structure, an A- Mignotte sequence will be referred to as an (*ω, w, n*)-Mignotte sequence. More exactly, an (*ω, w, n*)-Mignotte sequence is a sequence of positive integers *p*1*,... , pn* such that

*maxB*∈P({1*,*2*,...,n*}) ([{*pi*|*i* ∈ *B*}]) *< minA*∈P({1*,*2*,...,n*})([{*pi*|*i* ∈ *A*}])*.*

P

P

*i*∈*B*

*ωi*≤*w*−1

*i*∈*A*

*ωi*≥*w*

An (*ω, w, n*)-Mignotte sequence can be constructed as follows (see also [[18](#_bookmark29)]). Let

*p*' *,... , p*' be a generalized threshold (*w, N* )-Mignotte sequence, where *N* = Σ*n ωi*

1

*N*

*i*=1

and define *pi* = [{*p*' | *j* ∈ *Pi*}], for all 1 ≤ *i* ≤ *n*, where {*P*1*,... , Pn*} is an arbitrary

*j*

partition of the set {1*,* 2*,... ,N* } such that |*Pi*| = *ωi*, for all 1 ≤ *i* ≤ *n*. It is easy to prove that the sequence *p*1*,... , pn* is indeed an (*ω, w, n*)-Mignotte sequence.

Benaloh and Leichter have proven in [[4](#_bookmark11)] that there exist access structures that are not weighted threshold. We present next their example that proves this statement.

Example 4.3 (Benaloh and Leichter [[4](#_bookmark11)])

Let *n* = 4 and A*min* = {{1*,* 2}*,* {3*,* 4}}. Suppose that this access structure is a weighted threshold access structure with the weights *ω*1, *ω*2, *ω*3*, ω*4*,* and the thresh- old *w*. So, *ω*1 + *ω*2 ≥ *w* and *ω*3 + *ω*4 ≥ *w*. If we sum these inequalities we obtain *ω*1+*ω*2+*ω*3+*ω*4 ≥ 2*w*, and, thus, we obtain that 2·*max*(*ω*1*, ω*2)+2·*max*(*ω*3*, ω*4) ≥ 2*w* which leads to *max*(*ω*1*, ω*2)+ *max*(*ω*3*, ω*4) ≥ *w*. Thus, one of the sets {1*,* 3}, {1*,* 4},

{2*,* 3} or {2*,* 4} is an authorized access group!

We will present how to realize this access structure using the proposed extension of Mignotte scheme. In fact, the main problem is to find an A-Mignotte sequence. More exactly, we are interested in finding a sequence of positive integers *p*1*, p*2*, p*3*, p*4 such that

*max*([*p*1*, p*3]*,* [*p*1*, p*4]*,* [*p*2*, p*3]*,* [*p*2*, p*4]) *< min*([*p*1*, p*2]*,* [*p*3*, p*4])*.*

It is interesting to remark that this access structure can not be realized using sequences of pairwise coprime numbers. Indeed, there is no A-Mignotte sequence with pairwise coprime elements, because, otherwise, the above inequality will lead to *p*1*p*3 *< p*1*p*2 and *p*2*p*4 *< p*3*p*4 and, thus, to *p*3 *< p*2 and *p*2 *< p*3!

If *q*1*, q*2*, q*3*, q*4 are pairwise coprime, then the sequence *p*1 = *q*1*q*2*, p*2 = *q*3*q*4*, p*3 = *q*1*q*3*, p*4 = *q*2*q*4 is an A-Mignotte sequence. In this case, the general variant of the Chinese remainder theorem must be used for recovering the secret.

Asmuth-Bloom sequences can be extended as follows.

Definition 4.4 Let *n* be a positive integer, *n* ≥ 2 and A ⊆ P({1*,* 2*,... , n*}). An

A*-Asmuth-Bloom sequence* is a sequence of positive integers *p*0*, p*1*,... , pn* such that

*p*0 · *maxB*∈A([{*pi*|*i* ∈ *B*}]) *< minA*∈A([{*pi*|*i* ∈ *A*}])*.*

The above property is equivalent with

*p*0 · *maxB*∈A*max* ([{*pi*|*i* ∈ *B*}]) *< minA*∈A*min* ([{*pi*|*i* ∈ *A*}])*.*

If A is specified by A*min* = {*A* ∈ P({1*,* 2*,... , n*}) | |*A*| = *k*} then any A-Asmuth- Bloom sequence is a generalized threshold (*k, n*)-Asmuth-Bloom sequence. It is easy to see that if we multiply the elements, excepting the first one, of an A-Asmuth- Bloom sequence *p*0*, p*1*,* ··· *, pn* with a fixed element *δ* ∈ Z, (*δ, p*0 ··· *pn*) = 1, we also obtain an A-Asmuth-Bloom sequence.

We will describe next how to construct Asmuth-Bloom sequences in case of the weighted threshold access structures. Let *n* ≥ 2, *ω* = (*ω*1*,... , ωn*) a sequence of weights, and *w* a threshold. An (*ω, w, n*)*-Asmuth-Bloom sequence* is a sequence of positive integers *p*0*, p*1*,... , pn* such that

*p*0 · *maxB*∈P({1*,*2*,...,n*}) ([{*pi*|*i* ∈ *B*}]) *< minA*∈P({1*,*2*,...,n*})([{*pi*|*i* ∈ *A*}])*.*

P

P

*i*∈*B*

*ωi*≤*w*−1

*i*∈*A*

*ωi*≥*w*

An (*ω, w, n*)-Asmuth-Bloom sequence can be constructed as follows. Let

*p*' *, p*' *,... , p*'

be a generalized threshold (*w, N* )-Asmuth-Bloom sequence, where

0 1 *N*

*N* = Σ

*n i*=1

0

*j*

*ωi* and define *p*0 = *p*'

and *pi* = [{*p*'

| *j* ∈ *Pi*}], for all 1 ≤ *i* ≤ *n*, where

{*P*1*,... , Pn*} is an arbitrary partition of the set {1*,* 2*,... ,N* } such that |*Pi*| = *ωi*,

for all 1 ≤ *i* ≤ *n*. It is easy to prove that the sequence *p*0*, p*1*,... , pn* is indeed an (*ω, w, n*)-Asmuth-Bloom sequence.

Example [4.5](#_bookmark6) illustrates this construction.

Example 4.5 (with artificially small parameters)

Consider *n* = 4, the weights *ω*1 = *ω*2 = 1, *ω*3 = *ω*4 = 2, and the threshold *w* = 3. We obtain *N* = 6. The sequence 5*,* 17*,* 19*,* 23*,* 29*,* 31*,* 37 is a (3*,* 6)-Asmuth-Bloom

sequence and, if we consider the partition {{6}*,* {5}*,* {1*,* 4}*,* {2*,* 3}} of the set

{1*,* 2*,* 3*,* 4*,* 5*,* 6}, we obtain that the sequence 5, 37, 31, 17 · 29, 19 · 23 is an

((1*,* 1*,* 2*,* 2)*,* 3*,* 4)-Asmuth-Bloom sequence.

The access structure given by A*min* = {{1*,* 2}*,* {3*,* 4}} can not be realized using Asmuth-Bloom sequences of pairwise coprime numbers. Indeed, there is no A- Asmuth-Bloom sequence with pairwise coprime elements, because, otherwise, the condition *p*0 · *max*([*p*1*, p*3]*,* [*p*1*, p*4]*,* [*p*2*, p*3]*,* [*p*2*, p*4]) *< min*([*p*1*, p*2]*,* [*p*3*, p*4]) will lead

to *p*0*p*1*p*3 *< p*1*p*2 and *p*0*p*2*p*4 *< p*3*p*4 and, thus, to *p*0*p*3 *< p*2 (which implies *p*2*p*3 *<*

0

*p*0*p*2), and *p*0*p*2 *< p*3, which will finally lead to *p*2 *<* 1!

0

If *q*1*, q*2*, q*3*, q*4 are pairwise coprime, then the sequence *p*0*, p*1 = *q*1*q*2*, p*2 = *q*3*q*4*, p*3 = *q*1*q*3*, p*4 = *q*2*q*4 is an A-Asmuth-Bloom sequence, for any *p*0 *< min*(*q*1*, q*2*, q*3*, q*4). Indeed, in this case, *min*([*p*1*, p*2]*,* [*p*3*, p*4]) = *q*1*q*2*q*3*q*4 and *max*([*p*1*, p*3]*,* [*p*1*, p*4]*,* [*p*2*, p*3]*,* [*p*2*, p*4]) = *q*1*q*2*q*3*q*4 , for some *i* ∈ {1*,* 2*,* 3*,* 4}*.* In this case, the general variant of the Chinese remainder theorem must be used for recovering the secret.

*qi*

* 1. *Secret Sharing Homomorphisms*

Benaloh has introduced the notion of secret sharing homomorphisms in [[2](#_bookmark10)]. We present here a slightly different version of his definition.

Definition 4.6 Let S and S1*,... ,* S*n* be the set of possible secrets and, respectively, the set of possible shares corresponding to each user. Consider the binary operations

⊕ and ⊗1*,... ,* ⊗*n* over these sets. We say that an A-secret sharing scheme is

(⊕*,* ⊗1*,... ,* ⊗*n*) — *homomorphic* if for any *S*1*, S*2 ∈S with the corresponding shares (*I*1*,... ,I*1), and respectively, (*I*2*,... ,I*2), the shares of the secret *S*1 ⊕ *S*2 are (*I*1 ⊗1

1 *n* 1 *n* 1

*I*2*,... ,I*1 ⊗*n I*2).

1 *n n*

Intuitively, this means that the compositions of the shares are shares of the composition of the secrets.

The extended Mignotte scheme has such properties. Let ⊗ be a binary operation over Z, ⊗ ∈ {+*,* —*,* ·}, and let ⊗*m* denote the corresponding operation modulo *m*, i.e., ⊗*m* is the binary operation over Z*m* given by *a* ⊗*m b* = (*a* ⊗ *b*) mod *m*, for any *a, b* ∈ Z*m*. If *p*1*,... , pn* is an extended Mignotte sequence and ⊗ ∈ {+*,* —*,* ·}, then the corresponding secret sharing scheme is (⊗*,* ⊗*p*1 *,... ,* ⊗*pn* )-partial homomorphic, in sense that, if *S*1 and *S*2 are some secrets such that *β < S*1 ⊗ *S*2 *< α*, with

the corresponding shares (*I*1*,... ,I*1), and respectively, (*I*2*,... ,I*2), then (*I*1 ⊗*p*

1 *n* 1 *n* 1 1

*I*2*,... ,I*1 ⊗*p I*2) are the shares corresponding [3](#_bookmark7) to the secret *S*1 ⊗ *S*2.

1 *n n n*

The extended Asmuth-Bloom scheme has homomorphic properties in case that

the extended Asmuth-Bloom sequence has the property *p*0|*pi*, for all 1 ≤ *i* ≤ *n*. In this case, the secret can be expressed as

*S* = (Σ*i*∈*A γiδiIi* mod [{*pi*|*i* ∈ *A*}]) mod *p*0

= Σ*i*∈*A γiδiIi* mod *p*0*,*

for some authorized group *A*, where *δi* = [{*pi*|*i*∈*A*}] , for all *i* ∈ *A*, and *γi,* for *i* ∈

Σ

*pi*

*A,* are arbitrary integers such that *i*∈*A γiδi* = 1. Thus, any extended Asmuth-

Bloom scheme based on a sequence with such properties is (⊗*p*0 *,* ⊗*p*0 *,... ,* ⊗*p*0 ) -

homomorphic, where ⊗ ∈ {+*,* —}. Unfortunately, the property *p*0|*pi* also implies

3 This property follows directly from the properties of the congruences. More exactly, if *S*1 ≡ *I*1 *mod pi*

and *S*2 ≡ *I*2 *mod pi* then *S*1 ⊗ *S*2 ≡ *I*1 ⊗*pi I*2 *mod pi.*

*i*

*i i* *i*

that

*Ii* mod *p*0 = ((*S* + *γ* · *p*0) mod *pi*) mod *p*0

= (*S* + *γ* · *p*0) mod *p*0

= *S,*

and, thus, the security of the scheme is entirely compromised. It will be interesting to find Asmuth-Bloom sequences which lead to homomorphic properties, without affecting the security of the scheme. One solution would be to find A-Asmuth-Bloom sequences *p*0*, p*1*,... , pn* such that *p*0|[{*pi*|*i* ∈ *A*}], for all *A* ∈ A*min,* but *p*0 / |*pi*, for all 1 ≤ *i* ≤ *n*.

# An E-voting Scheme

According to [[32](#_bookmark40)], “an *electronic voting* (*e-voting*) system is a voting system in which the election data is recorded, stored and processed primarily as digital information”. We present next the most important requirements for an e-voting scheme (the reader is referred to [[16](#_bookmark24)] for more details):

* *Correctness* - according to this requirement, the announced tally is identical with the real outcome of the election;
* *Privacy* - this requirement guarantees that no reasonable sized coalitions of voters or authorities may link a voter’s identity to his vote;
* *Robustness* - according to this requirement, no reasonable sized coalitions of voters or authorities may affect the election;
* *Veriﬁability* - this requirement assures the existence of some mechanisms for au- diting the election in order to verify if it has taken place properly.

We have to remark that these properties may contradict or interrelate one with another. For example, verifiability implies the existence of some proofs for the consistency of the votes but these may affect privacy. On the other hand, verifiability is a strong supporter both for the correctness and for the robustness of the scheme. We focus only on the case of *yes/no* e-voting. We follow the approach of Benaloh [[2](#_bookmark10)], [[3](#_bookmark12)] for designing a multi-authority e-voting scheme. The novelty of our scheme is that the tallying authorities may have non-equal weights. The parties involved are the voters *V*1*,... , Vm*, the tallying authorities *A*1*,... , An* and the central authority

A. We present next the steps of our e-voting scheme.

* Setup
  + The central authority A decides on an authorized access structure A for the tally- ing authorities and generates and broadcasts an A-Mignotte sequence *p*1*,... , pn* with a large factor *α*−*β* ;

*β*

* + The central authority A broadcasts the values *vyes* and *vno*, where *vyes, vno* ∈

{*β* + 1*,... ,α* — 1} are assigned to the *yes* vote and to the *no* vote;

* Ballot Construction
* For 1 ≤ *j* ≤ *m*, the voter *Vj* chooses a vote mask [4](#_bookmark8) *bj*, 0 *< bj < α* — *vj*, for his vote *vj* ∈ {*vyes, vno*} and forms the ballot *Bj* = *vj* + *bj*;
* The voter *Vj* securely sends the sub-ballot *Bj,i* = *Bj* mod *pi* to the tallying authority *Ai*, for all 1 ≤ *j* ≤ *m* and for all 1 ≤ *i* ≤ *n*;
* Ballot Tallying
  + At the end of ballot construction period, the tallying authority *Ai* computes

the partial “masked” tally *Ti* = Σ

*m j*=1

central authority A, for all 1 ≤ *i* ≤ *n*;

*Bj,i* mod *pi* and securely sends it to the

· The central authority A obtains the final “masked” tally *T* = Σ*m Bj* by solv-

*j*=1

ing, using the general variant of the Chinese remainder theorem, the system of equations

*x* ≡ *Ti mod pi, i* ∈ *A*

for some *A* ∈ A; for the correctness of this reasoning, any possible final “masked” tally *T* must satisfy *T < α* (the relation *β < T* holds by the choice of the values *vyes, vno* and of the mask values). Indeed, in this case, by the fact that the extended Mignotte secret sharing scheme is (+*,* +*p*1 *,... ,* +*pn* )-partial homomorphic, the values *T*1*,... , Tn* are the shares of the element *T* . In order to assure *T < α*, the central authority A may impose, for example, the condition

*m* · (*max*(*vyes, vno*)+ *max*(*b*1*,... , bm*)) *< α*;

· At the previous step, the central authority A can also verify the consistency of the values *Ti,i* ∈ *A*, by testing if *Ti* ≡ *Ti*' *mod* (*pi, pi*' ), for any *i, i*' ∈ *A*;

* Vote Casting
  + At the end of ballot tallying period, the voter *Vj* securely sends *bj* to the central authority A, for all 1 ≤ *j* ≤ *m*;
* Vote Counting
  + At the end of vote casting period, the central authority A computes the sum of

votes *S* = Σ*m vj* as *S* = *T* — Σ*m bj*;

*j*=1

*j*=1

* + The numbers of *yes* and *no* votes can be obtained as the solution of the equation *vyes* · *x*+ *vno* · *y* = *S*; if the values *vyes* and *vno* are chosen such that *m* · *vyes < vno*, then this solution can be determined as

*number votes no* = *S* div *vno,*

*number votes yes* = (*S* mod *vno*) div *vyes.*

* The central authority broadcasts *number votes yes, number votes no*. Our e-voting scheme has the following properties:
* *Privacy* - in order to link a voter’s identity (*Vj*) to his vote (*vj*), at least an au- thorized group of tallying authorities and the central authority must collaborate.

4 The purpose of the masks is to hide any information about the voters’ choices. Moreover, the ballot construction and ballot tallying can be performed in advance.

Indeed, the ballot *Bj* may be reconstructed only by an authorized group of tal- lying authorities and the mask *bj* is known only by the central authority. Thus, our scheme assures privacy against any coalition formed by a group *B* ∈ A of tallying authorities and the central authority A;

* *Veriﬁability* - some verifications are made in the ballot tallying phase but some proofs have to be added at the voters’ level. This includes the proof that a voter really chooses a vote in {*vyes, vno*} and the proof that the sub-ballots are properly derived. For the second part, verifiable secret sharing (see [[11](#_bookmark19)], [[25](#_bookmark33)]) may be used. A non-interactive modular verifiable secret sharing scheme was proposed in [[22](#_bookmark30)] and we may use it for our case;
* *Robustness* - assuming that the voters’ actions are performed honestly (or using verifiable secret sharing for detecting frauds), the election carries on correctly if at least a group *A* ∈ A of tallying authorities and the central authority A act honestly.

# Conclusions and Future Work

We have demonstrated that the Chinese remainder theorem can be used for realizing more general access structures than the threshold ones.

We have first extended Brickell’s construction for compartmented secret sharing to the case that the global threshold is strictly greater than the sum of the com- partment thresholds and we have proposed using threshold secret sharing schemes based on the Chinese remainder theorem as building blocks in order to decrease the size of shares, maintaining, in the same time, a reasonable level of security.

We have then extended the threshold secret sharing schemes based on the Chi- nese remainder theorem in order to deal with more general access structures. We have presented how to realize any weighted threshold access structure but we have also proven that our extensions are suitable for realizing some non-weighted thresh- old access structures. In our future work, we will investigate what other classes of access structures can be realized using our schemes and we will also study the related problem of generating Mignotte or Asmuth-Bloom sequences. It is inter- esting to remark that some access structures can not be realized using sequences of pairwise coprime numbers and, thus, the general variant of the Chinese remain- der theorem must be used for recovering the secret. The access structure given by A*min* = {{1*,* 2}*,* {3*,* 4}} is such an example (see Section [4](#_bookmark5)). It will be interesting to find other access structures with the same property or even find a general criterion for deciding if a certain access structure may be realized using the standard variant of the Chinese remainder theorem.

We have presented a multi-authority e-voting scheme based on the proposed secret sharing schemes, in which, as a novelty, the tallying authorities may have non-equal weights. The resulted e-voting scheme has some important properties as privacy and robustness. Some verifiability mechanisms are present in the ballot tallying phase but in our future work we will try to add proofs of consistency at voters’ level and at the central authority level (following, for example, the approach

described in [[9](#_bookmark17)]).

Threshold cryptography in which the implicated parties may have non-equal weights is another promising future research direction and we think that our secret sharing schemes can be used in this sense.

# Acknowledgement

Research reported here was partially supported by the National University Research Council of Romania under the grant CNCSIS 632/2006.

# References

1. Asmuth, C. A. and J. Bloom, *A modular approach to key safeguarding*, IEEE Transactions on Information Theory IT-29 (1983), pp. 208–210.
2. Benaloh, J., *Secret sharing homomorphisms: Keeping shares of a secret secret*, in: A. M. Odlyzko, editor, *Advanced in Cryptology-CRYPTO’ 86*, Lecture Notes in Computer Science 263 (1987), pp. 251–260.
3. Benaloh, J., “Verifiable Secret-Ballot Elections,” Ph.D. thesis, Yale University (1988).
4. Benaloh, J. and J. Leichter, *Generalized secret sharing and monotone functions*, in: S. Goldwasser, editor, *Advanced in Cryptology-CRYPTO’ 88*, Lecture Notes in Computer Science 403 (1989), pp. 27–35.
5. Blakley, G. R., *Safeguarding cryptographic keys*, in: *National Computer Conference, 1979*, American Federation of Information Processing Societies Proceedings 48, 1979, pp. 313–317.
6. Brickell, E. F., *Some ideal secret sharing schemes.*, in: J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology - EUROCRYPT ’89*, Lecture Notes in Computer Science 434 (1990), pp. 468–475.
7. Capocelli, R. M., A. D. Santis, L. Gargano and U. Vaccaro, *On the size of shares for secret sharing schemes*, Journal of Cryptology 6 (1993), pp. 157–167, (a preliminary version of this paper appeared in Advances in Cryptology - CRYPTO ’91).
8. Cohen, H., “A Course in Computational Algebraic Number Theory,” Graduate Texts in Mathematics, Springer-Verlag, 2000, 4th edition.
9. Cramer, R., M. K. Franklin, B. Schoenmakers and M. Yung, *Multi-authority secret-ballot elections with* *linear work*, in: U. Maurer, editor, *Advances in Cryptology - EuroCrypt ’96*, Lecture Notes in Computer Science 1070 (1996), pp. 72–83.
10. Ding, C., D. Pei and A. Salomaa, “Chinese remainder theorem: applications in computing, coding, cryptography,” World Scientific Publishing Co., Inc., 1996.
11. Feldman, P., *A practical scheme for non-interactive verifiable secret sharing*, in: *Proceedings of the* *28th IEEE Symposium on the Foundations of Computer Science, 1987* (1987), pp. 427–437.
12. Fraenkel, A. S., *New proof of the generalized Chinese remainder theorem*, Proceedings of American Mathematical Society 14 (1963), pp. 790–791.
13. Garner, H., *The residue number system*, IRE Transactions on Electronic Computers EC-8 (1959),

pp. 140–147.

1. Ghodosi, H., J. Pieprzyk and R. Safavi-Naini, *Secret sharing in multilevel and compartmented groups.*, in: C. Boyd and E. Dawson, editors, *ACISP ’98: Proceedings of the Third Australasian Conference on Information Security and Privacy*, Lecture Notes in Computer Science 1438 (1998), pp. 367–378.
2. Goldreich, O., D. Ron and M. Sudan, *Chinese remaindering with errors*, IEEE Transactions on Information Theory IT-46 (2000), pp. 1330–1338.
3. Gritzalis, D., editor, “Secure Electronic Voting,” Advances in Information Security 7, Kluwer Academic Publishers, 2003.
4. Iftene, S., *A generalization of Mignotte’s secret sharing scheme*, in: T. Jebelean, V. Negru, D. Petcu and D. Zaharie, editors, *Proceedings of the 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania, September, 2004* (2004), pp. 196–201.
5. Iftene, S. and I. Boureanu, *Weighted threshold secret sharing based on the Chinese remainder theorem*, Scientific Annals of the ”Al. I. Cuza” University of Iasi, Computer Science Section XVI (2005), pp. 161– 172.
6. Ito, M., A. Saito and T. Nishizeki, *Secret sharing scheme realizing general access structure*, in:

*Proceedings of the IEEE Global Telecommunications Conference, Globecom ’87* (1987), pp. 99–102.

1. Karnin, E. D., J. W. Greene and M. E. Hellman, *On secret sharing systems*, IEEE Transactions on Information Theory IT-29 (1983), pp. 35–41.
2. Kranakis, E., “Primality and Cryptography,” Wiley-Teubner Series in Computer Science, 1986.
3. Li, Q., Z. Wang, X. Niu and S. Sun, *A non-interactive modular verifiable secret sharing scheme*, in: *ICCCAS’05, International Conference on Communications, Circuits and Systems, 2005*, 2005, pp. 84–87.
4. Mignotte, M., *How to share a secret*, in: T. Beth, editor, *Cryptography-Proceedings of the Workshop on Cryptography, Burg Feuerstein, 1982*, Lecture Notes in Computer Science 149 (1983), pp. 371–375.
5. Ore, O., *The general Chinese remainder theorem*, American Mathematical Monthly 59 (1952), pp. 365– 370.
6. Pedersen, T. P., *Non-interactive and information-theoretic secure verifiable secret sharing*, in:

J. Feigenbaum, editor, *Advances in Cryptology - Crypto ’91*, Lecture Notes in Computer Science 576

(1992), pp. 129–140.

1. Pohlig, S. C. and M. E. Hellman, *An improved algorithm for computing logarithms over GF*(*p*) *and its* *cryptographic significance*, IEEE Transactions on Information Theory 24 (1978), pp. 106–110.
2. Quisquater, J.-J. and C. Couvreur, *Fast decipherment algorithm for the RSA public-key cryptosystem*, IEE Electronics Letters 18 (21) (1982), pp. 905–907.
3. Quisquater, M., B. Preneel and J. Vandewalle, *On the security of the threshold scheme based on the* *Chinese remainder theorem*, in: D. Naccache and P. Paillier, editors, *Public Key Cryptography, 5th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2002*, Lecture Notes in Computer Science 2274 (2002), pp. 199–210.
4. Shamir, A., *How to share a secret*, Communications of the ACM 22 (1979), pp. 612–613.
5. Simmons, G. J., *How to (really) share a secret.*, in: S. Goldwasser, editor, *Advances in Cryptology - CRYPTO ’88*, Lecture Notes in Computer Science 403 (1990), pp. 390–448.
6. Stinson, D. R., *An explication of secret sharing schemes*, Designs, Codes and Cryptography 2 (1992),

pp. 357–390.

1. VoteHere, *Network voting system standards* (April 2002).