A New Approach to Weighted Multi-Secret Sharing

Xukai Zou*, Fabio Maino†, Elisa Bertino‡, Yan Sui*, Kai Wang* and Feng Li*
*Indiana University Purdue University Indianapolis, IN 46202, USA
Email:{xzou, ysui, wangk, fengli}@iupui.edu
†Cisco System Inc. San Jose, CA 95134, USA
Email: fmaino@cisco.com
‡Purdue University, West Lafayette, IN 47907, USA
Email: bertino@cs.purdue.edu

***Abstract*—Secret sharing is important in information and network security and has broad applications in the real world. Since an elegant secret sharing mechanism was first proposed by Shamir in 1979, many schemes have appeared in literature. These schemes deal with either single or multiple secrets and their shares have either the same weight or different weights. Weighted shares mean that different shares have different capabilities in recovering the secret(s) – a more (less) weighted share needs fewer (more) other shares to recover the secret(s). In this paper, we identify a direct relation between the length (i.e., the number of bits) and the weight of shares and, based on this relation, present a new Chinese Remainder Theorem (CRT) based weighted multiple secret sharing scheme. This scheme can also be naturally applied to other cases such as sharing a single secret with same-weight shares and is remarkably simple and easy to implement. Compared to both Shamir's scheme and Mignotte's scheme – the representative of existing CRT based secret sharing schemes, the new scheme is more efficient than both schemes in share computation and more efficient than Shamir's scheme (and as efficient as Mignotte's scheme) in secret recovery. One prominent advantage of the new scheme is that the sizes of shares can vary distantly to fit different requirements and constraints of various devices such as sensors, PDAs, cell phones, iPads, hence, the new scheme is able to apply to broader applications involving wireless/sensor networks and pervasive computing.**

***Index Terms*—Secret sharing, Shamir's secret sharing scheme, Weighted secret sharing, Chinese Remainder Theorem, Polynomial interpolation, Mignotte sequence.**

I. Introduction

A secret sharing scheme starts with a *secret* and then derives from it certain *shares* which are distributed to a group of users (i.e., participants). The secret may be uniquely determined (i.e., recovered) only by certain predetermined subgroups of users which constitute the *access structure*. An important category of access structure is the (w,N)-threshold access structure in which, given N shareholders (i.e., participants), an authorized group contains any w or more participants and any group of at most $w-1$ participants is an unauthorized group (a more detail discussion later).

Secret sharing has broad applications in the real world and can be used for situations in which access to important resources has to be protected. There is an old story which is believed to have motivated the secret sharing principle [8]: a group of pirates accidentally discovered a map that would lead them to an island full of treasure. Who was going to be entrusted to keep the map? A safe solution is: the map should be divided into pieces such that all pieces are needed to recover the map and missing any piece would make the map totally unreadable. Thus, every pirate was given one such piece. Another important application of secret sharing is e-voting where the vote of every individual will be absolutely and correctly counted in the overall voting result but there is no way for other people (including candidates and authorities) to know whom the individual voted for [13]. In today's information and networking era, secret sharing is also a fundamental issue in network security and can be used in key management and multi-party secure computation [7].

Since the concept of secret sharing, along with an efficient mechanism to enforce it, was proposed by Shamir in 1979 [21] (Blakley also did the similar work at that time [5]), there have been many papers extending Shamir's scheme and investigating new secret sharing schemes [2], [7], [9], [10], [11], [13], [15], [16], [17], [18], [19], [20], [22], [23]. Secret sharing schemes can be classified into various categories according to different criteria. In terms of numbers of secrets to be shared, two classes can be identified: single secret and multiple secrets. In terms of shares' capabilities, two classes can be identified as well: same-weight shares and weighted shares. Weighted shares mean that different shares have different capabilities in recovering the secret(s)–a more weighted share needs fewer other shares and a less weighted share needs more other shares to recover the secret(s). Based on the underlying techniques used, two typical classes can be identified: polynomial based schemes and Chinese Remainder Theorem (CRT) based schemes. Shamir's scheme [21] is an elegant polynomial based scheme and Mignotte's scheme [17] is a representative among the CRT based secret sharing schemes.

Threshold secret sharing is one of the most popular classes. (w,N)-threshold secret sharing means that there are N participants (i.e., N shares), any w or more participants (i.e., shares), when pooled together, are able to recover the secret(s), however, less than w participants cannot. Both Shamir's and Mignotte's schemes belong to the (w,N)-threshold class.

In this paper, we identify a simple relation between the lengths (i.e., the number of bits) of shares and their weights and based on this relation, we propose a new CRT based (w,N)-threshold secret sharing scheme. This new CRT based scheme is very simple in principle and efficient in complexity. Compared to all existing secret sharing schemes, the new CRT

based scheme is generic and very flexible in supporting all four secret sharing scenarios: single secret (with same-weight shares), single secret with weighted shares, multiple secrets (with same-weight shares), and multiple secrets with weighted shares. Moreover, the construction of our new scheme make it efficient and flexible in supporting various devices with different computational capabilities. Thus, the new scheme is well suited for secure applications in wireless/sensor networks and pervasive computing domains. The complexity analysis and experimental results show that the new CRT based scheme is more efficient than both Shamir's scheme and Mignotte's CRT based scheme in share computation and more efficient than Shamir's scheme (and as efficient as Mignotte's scheme) in secret recovery.

The paper is organized as follows. We review typical existing schemes in Section II. Section III particularly introduces Mignotte's scheme. The new CRT based weighted multiple secret sharing scheme is presented in Section IV, including its performance and security analyses. The experimental results and the comparisons with Shamir's and Mignotte's schemes are presented in Section V. Section VI concludes the paper.

Some notations used in the paper are listed as follows:
p: a large prime, the system modulus in Shamir's scheme.
n: the bit length of the basic numbers used in the system. n should be large enough to prevent brute-force attacks, such as $n = 128$. n is called base-bit. In general, $n = \lceil log(p) \rceil$.
w: the disclosure weight and a positive integer. That is, when the total weight of a set of shares is larger than (or equal to) w, the secret(s) can be reconstructed. Otherwise, the secret(s) cannot be recovered. w is also called *threshold*.
S: the secret to be shared.
S_i: the multiple secrets to be shared. $i = 1, \cdots, k$.
N: the number of participants.
U_i: a user or participant. Note: the terms *user* and *participant* are used interchangeably in the paper.
s_i: the shares of N participants. $i = 1, \cdots, N$.
p_i: the privileges of participants (i.e., the weights of shares) and expressed as positive integers. Assume $p_i < w$.

In addition, we use $S3(w,n,N,P)$ to denote a (w,N)-threshold secret sharing scheme, where w is the disclosure weight (i.e., threshold), n is the base-bit so that the brute-force attack is infeasible in the secret space 0 to 2^n, N is the number of participants, and $P = (p_1, \cdots, p_N)$ is a list of users' privileges. There will be a dealer in schemes which generates shares and distributes them to users.

II. Related Works

In this section, we review typical existing schemes to help understand the properties of secret sharing schemes.

A secret sharing scheme could be either "perfect" or "non-perfect". A scheme is perfect if any subset in the access structure can recover the secret(s) while any unauthorized subset cannot gain *any bit* of information (in the information-theoretic sense) about the secret(s). There are typical perfect secret sharing schemes in literature, e.g., Benaloh[4], Feldman[6], Shamir[21], and typical non-perfect secret sharing schemes, e.g., Bai[2], Iftene[13], Mignotte[17], etc. Moreover, the CRT based threshold schemes including ours are not perfect schemes. To analyze the security of the threshold schemes based on CRT in a modern framework, an unitary point of view on the modern context of security was proposed by Quisquater et. al [20]. They introduced the concept of "asymptotically perfect" which is a natural relaxation of perfect schemes and proved that the threshold scheme based on CRT with *consecutive primes* is asymptotically perfect.

Secret sharing schemes can be either threshold schemes, e.g. Bai[2], Mignotte[17], Shamir[21], etc, or non-threshold schemes, e.g., Benaloh[4], Iftene[13], etc. Regarding the accommodation of changes to access structures, some schemes are "easy to add user". This means that the dealer can easily compute a new share and securely give it to the new user without affecting existing users' shares. Most of these kinds of schemes are polynomial based since a new share is just a new point evaluated on the polynomial.

In terms of shares' capabilities, two classes can be identified: same-weight shares and weighted shares. However, most schemes can be adapted to weighted secret sharing schemes. For example, in Shamir's scheme, multiple points on the polynomial can be assigned to one participant as a more weighted share.

In particular, Shamir's scheme is a perfect threshold secret sharing scheme, and it is based on polynomials and easy to add users. This scheme can deal with either single secret or multiple secrets (as in its extension by Franklin et. al. [7]) and the shares have either the same weight or different weights. However no matter how one extends Shamir's secret sharing scheme, a weighted share having weight p_i consists of, in fact, p_i independent shares of weight 1. In response, researchers have been investigating weighted secret sharing schemes based on other techniques, e.g., CRT.

Recently, Tamir Tassa et. al. investigated different secret sharing schemes such as hierarchical threshold secret sharing [25], ideal weighted threshold secret sharing [3], and multipartite secret sharing [26]. These works are all in line with Shamir's scheme in terms of ideal and perfect secrecy and involve polynomials and interpolation, particularly, Birkhoff interpolation and bivariate Lagrange interpolation.

III. Mignotte's (w,N) - Threshold Secret Sharing Schemes

Mignotte's scheme is the representative of CRT based (w,N)-threshold secret sharing schemes. We introduce it in this section.

Mignotte's threshold secret sharing scheme [17] uses some special sequences of integers, called Mignotte sequence.

- Let N be a positive integer, $N \geq 2$, and $2 \leq w \leq N$. An $(w,N) - Mignotte\ sequence$ is a sequence of pairwise co-prime positive integers $P_1 < P_2 < ... < P_N$ such that $\prod_{i=0}^{w-2} P_{N-i} < \prod_{i=1}^{w} P_i$.

Given a publicly known (w,N)-Mignotte sequence, the scheme works as follows:

- The secret S is chosen as a random integer such that $\beta < S < \alpha$, where $\alpha = \prod_{i=1}^{w} P_i$ and $\beta = \prod_{i=1}^{w-2} P_{N-i}$;
- The shares s_i are chosen as (r_i, P_i) where $r_i = S \bmod P_i$;
- Given w distinct $s_{i_1}, ..., s_{i_w}$, S can be recovered from:

$$\begin{aligned} S &\equiv r_{i_1} \pmod{P_{i_1}} \\ S &\equiv r_{i_2} \pmod{P_{i_2}} \\ &\vdots \\ S &\equiv r_{i_w} \pmod{P_{i_w}}. \end{aligned}$$

A generalized Mignotte's scheme that allows moduli to not be pairwise co-prime was proposed in [12].

The scheme can also be applied to weighted secret sharing as follows. Consider $S3(w,n,N,P)$ where $P = (p_1, \cdots, p_N)$ is users' privileges (i.e., their shares' weights). We first generate a generalized (w,W)-Mignotte sequence $P_1^{'}, ..., P_W^{'}$, where $W = \sum_{i=1}^{N} p_i$. And then we define $P_i = [\{P_j^{'} | j \in Pa_j\}]$, for all $1 \leq i \leq N$, where $\{Pa_1, ..., Pa_N\}$ is an arbitrary partition of the set $\{1, 2, ..., W\}$ such that $|Pa_i| = p_i$, for all $1 \leq i \leq N$.

IV. The CRT based weighted secret sharing scheme

As it can be observed from the above discussion, there exists a direct relation between the size and weight of a share: i.e., the bit length of weight 1 shares, a share of weight p_i will have $p_i \times n$ bits. In addition, Mignotte's threshold scheme is not simple in principle or implementation. The generation of Mignotte's sequences and weighted threshold access structure is difficult and requires additional cost. As a result, we propose a new CRT based weighted secret sharing scheme which is simple in principle and efficient in implementation and which employs (and exhibits) this direct size weight relation.

A. Principle

1) As before, we assume the disclosure weight is w, and n is the bit length of base numbers. We also assume that $w < n$. In general, w is much smaller than n.
2) The secret S will have $w \times n$ bits (if not, S can be extended, for example, by appending some random bits).
3) For a user U_i with privilege p_i, select a prime P_i having $p_i \times n$ bits and assume $p_i < w$. Note: for simplicity, here we assume P_is are primes. In fact, pairwise co-primes are enough for the scheme to work correctly.
4) Compute $r_i = S \bmod P_i$ and assign $s_i = \{(r_i, P_i)\}$ to U_i as its share.
5) In the secret reconstruction phase, for any pool of users U_{i_1}, U_{i_2},$\cdots$, U_{i_e}, as long as the sum of their weights is larger than w, i.e., $p_{i_1} + p_{i_2} + ... + p_{i_e} > w$, form the following congruence system:

$$\begin{aligned} S &\equiv r_{i_1} \bmod P_{i_1} \\ S &\equiv r_{i_2} \bmod P_{i_2} \\ &... \\ S &\equiv r_{i_e} \bmod P_{i_e} \end{aligned}$$

Then compute and recover S by CRT.

Note: because S has $w \times n$ bits and the moduli product $\hat{P} = P_{i_1} \times P_{i_2} \times \cdots \times P_{i_e}$ has at least $(p_{i_1} + p_{i_2} + \cdots + p_{i_e}) \times n - e$ bits, so $\hat{P} > S$, as long as $w < n$.

It is clear that any share s_i is just one point (r_i, P_i) since we properly utilize the relation between the weight and bit length of the corresponding share. In addition, when all p_i are equal to 1, it is a same-weight secret sharing scheme.

In the above discussion, it is assumed that $p_{i_1} + p_{i_2} + ... + p_{i_e} > w$. This guarantees that $\hat{P} > S$ as long as $w < n$, so S can always be uniquely recovered. We can reduce this condition to $p_{i_1} + p_{i_2} + \cdots + p_{i_e} \geq w$. However, in case $p_{i_1} + p_{i_2} + \cdots + p_{i_e} = w$, since $\hat{P}$ can have bit length $w \times n - w + 1$ (in the smallest cases), there needs to limit S to have $w \times n - w$ bits.

If S must have $w \times n$ bits (even may be very rare in reality), the new scheme can still work correctly by simply introducing a *helper*, whose modulus H_P is the smallest prime of w bits and whose share is $H_S = S \bmod H_P$. The *helper* will be used as one equation in the CRT congruence system. This will assure that $P_{i_1} \times P_{i_2} \times \cdots \times P_{i_e} \times H_P > S$, so S will be recovered uniquely. Note: when P_js are not primes but pairwise co-primes, the smallest number with w bits, which is co-prime to P_js, can be used as the *helper*.

If S has just n bits, we can easily extend S to $w \times n$ (or $w \times n - w$) bits by repeating S or appending random bits.

B. Multiple Secrets

Suppose there are k secrets $S_1, \cdots, S_k$ to be shared and each secret has n bits. We can easily extend the newly proposed CRT based scheme to produce a weighted multiple secret sharing scheme. We simply concatenate the secrets together to get $k \times n$ bits. There are three cases to consider:

1) $k < w$: Append random bits to get $w \times n$ bits.
2) $k = w$: Do nothing.
3) $k > w$: Introduce a *helper* with weight $(k - w)$.

C. Complexity Analysis

We analyze the complexity of our new CRT based secret sharing scheme here. Let us consider the case of the same weight shares, i.e., $p_1 = \cdots = p_N = 1$. Other cases can be analyzed in a similar way.

The classical textbook, "The Design and Analysis of Computer Algorithms" by Aho, Hopcroft and Ullman in 1974 [1], presents detailed discussions and proofs of Chinese Remainder Theorem and Polynomial Interpolation. Here we excerpt some of these results.

From **Theorem 8.21** and its **Corollary** [1], given w moduli of n bits each, the CRT computation requires time at most $O(wn(log^2(wn))loglog(wn))$.

From **Theorem 8.8** and its **Corollary** [1], given w moduli of n bits each, the w residues may be computed in at most $O(wn(log(w))(log(wn))loglog(wn))$.

When using these results here for share computation and secret reconstruction of the new CRT based scheme, we can deduce that their complexities are in the order of $O(n(log(w))(log(wn))loglog(wn))$ and $O(wn(log^2(wn))(loglog(wn)))$ respectively.

Let us consider the complexity of Shamir's scheme [21]. From Horner's rule, the evaluation of a polynomial with degree w requires $O(w)$ (in terms of number of multiplications).

From **Theorem 8.14** [1], the interpolation of a polynomial with w points requires $O(w(log^2(w)))$ (multiplications).

Suppose the numbers in Shamir's secret scheme have n bits, then each operation will be in the complexity of $O(n^2)$ (bit operations). Thus, the complexities of polynomial evaluation and polynomial interpolation in terms of bit operations are $O(wn^2)$ and $O(w(log^2(w))n^2)$ respectively.

It can be observed that the newly proposed CRT based secret sharing scheme is more efficient than Shamir's secret sharing scheme in both share computation and secret recovery. In Section V, the experimental results on Shamir's scheme and the new scheme are presented, which justifies this analysis. Section V also analyzes Mignotte's scheme and shows that the new scheme is more efficient than Mignotte's scheme in share computation and is as efficient as Mignotte's scheme in secret recovery.

D. Security Analysis

The security of the newly proposed scheme is guaranteed since the new scheme is solely based on Chinese Remainder Theorem (CRT) and CRT has been used in many other CRT based secret sharing schemes. Here we first discuss the security features shared by the new CRT based scheme and Shamir's scheme and then briefly discuss the common security features of the new scheme and Mignotte's scheme. In terms of perfect secrecy, our new scheme is same as Mignotte's scheme, i.e., being not a perfect one. However, in terms of the brute-force attack searching space, our scheme is equivalent to Shamir's scheme. Suppose the base-bit in Shamir's scheme is n, then the brute-force attack searching space is 2^n when there are less than w shares in the pool. In our scheme, when the total weight (suppose t) in the pool is less than w, the secret will have $w \times n$ bits, and the moduli product will have $t \times n$ bits. The brute-force attack searching space will be $2^{(w-t)\times n}$, which is at least 2^n. In this sense, even though our scheme is not perfect, its security strength is no less than that of Shamir's scheme. On the other hand, the shares in Shamir's scheme have n bits, same as that of the secret. In contrast, if the secret in the new scheme has n bits, the shares (with weight 1) can have n/w bits. This feature makes the new scheme more suitable to use in power-constrained devices such as sensors and cell phones.

With regard to Mignotte's scheme and our new scheme, both are based on CRT and use the same operation to recover the secret. As for share generation, they use the same operation to generate all same weight shares. For the shares of different weights p_i, the new scheme generates $p_i \times n$ bit primes (or co-primes) directly. However, Mignotte's scheme generates a Mignotte sequence of n bits each first and then gets $p_i \times n$ bit (maybe $p_i \times n - p_i + 1$ bit) primes (or co-primes) by multiplying p_i primes (or co-primes) in the Mignotte sequence. After generating primes (or co-primes), both schemes use the same modular operation to get shares. The difference in generating primes (or co-primes) affects only performance of the schemes but not security features. As a result, the new scheme and Mignotte's scheme have identical security features.

V. Experiment and Comparisons

In this section, we present our experimental results and comparisons with both Shamir's and Mignotte's schemes.

A. Comparison with Shamir's Secret Sharing Scheme

We performed an extensive set of experiments to evaluate and compare the performance of Shamir's scheme and the new CRT based scheme. We simulated the share computation time and the secret recovery time. In our experiment, we varied secret size and number of secrets to measure the computation complexity of both schemes. The code was written in java, and the experiment was performed on Dell PowerEdge 2850 running Red Hat Enterprise Linux (v. 4) with Dual Core 3.6GHz Processor and 4 GB RAM. The results were obtained based on average of 10000 runs for each case. Details of the experiments performed and experimental results are given below.

Considering the case of same weight shares, we constructed figures using the complexity analysis of Section IV-C and the obtained experimental results to compare two schemes. Specifically, Figures 1 and 2 show the theoretical and experimental results of the share computation time and the secret recovery time for single secret with sizes ranging from 64 to 256 bits. For example in Figure 1, the experimental results come from our simulation and the theoretical results are based on the complexity analysis of the share computation of Shamir's scheme and the new CRT based scheme as shown in Section IV-C. In this case, they are drawn (automatically by a software tool: gnuplot) in the formulae of wn^2 (for Shamir's scheme) and $n(log(w))(log(wn))loglog(wn)$ (for the new CRT based scheme), specifically with w being equal to 8 and n ranging from 64 to 256. As shown in the figures, the experimental results match the theoretical analysis well. As secret size increases, the average computational time increases too. And the new CRT based scheme shows an obvious advantage over Shamir's scheme in both share computation and secret recovery.

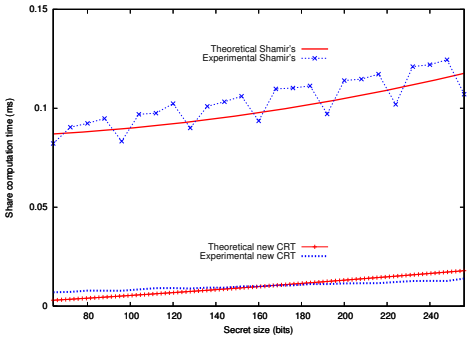

Fig. 1. Secret size VS share computation time (ms) (disclosure weight=8, number of participants = 15, number of secrets = 1)

Figure 3 and Figure 4 show similar experiments for multiple secrets. To share eight secrets with same size, the new CRT

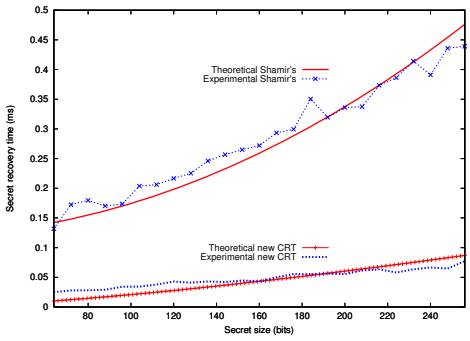

Fig. 2. Secret size VS secret recovery time (ms) (disclosure weight=8, number of participants = 15, number of secrets = 1)

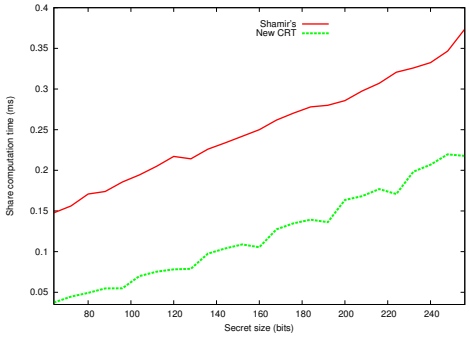

Fig. 3. Secret size VS share computation time (ms) (disclosure weight=8, number of participants = 15, number of secrets = 8)

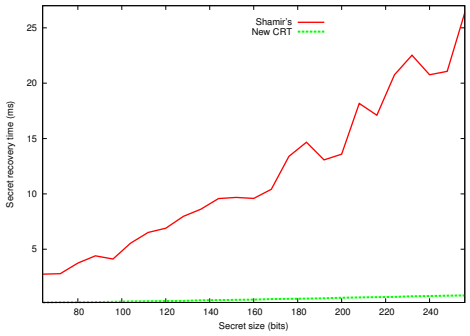

Fig. 4. Secret size VS secret recovery time (ms) (disclosure weight=8, number of participants = 15, number of secrets = 8)

based scheme needs less computation time in both share computation and secret recovery.

As shown in these figures, the new CRT based scheme takes very little time to compute shares and recover secrets. Depending on different secret sizes, disclosure weights and numbers of secrets, share computation of the new CRT based scheme can be 2 to 20 times faster than that of Shamir's scheme, while secret recovery of the new CRT based scheme can be 5 to 50 times faster than that of Shamir's scheme.

B. Comparison with Mignotte's Secret Sharing Scheme

Since Mignotte's secret sharing scheme is also based on CRT, we will make a detailed comparison between Mignotte's scheme and ours in this subsection.

The main difference between our new scheme and Mignotte's scheme is that Mignotte's scheme needs to generate Mignotte sequences first and then generate modular co-primes. Hence, we focus on the complexity analysis of these operations. Let us consider the case of shares $s_1, s_2, ..., s_N$ with weights $p_1, \cdots, p_N$ respectively. The total weight of these shares is $p_1 + p_2 + ... + p_N = W$, and the disclosure weight is w. The base-bit is n. There are several steps involved in user moduli generation of Mignotte's scheme. First, the generation of a Mignotte sequence involves generating W pairwise co-primes $P_1, ..., P_W$, sorting them and checking the condition $\prod_{i=0}^{w-2} P_{W-i} < \prod_{j=1}^{w} P_j$. The main operation involved in the generation of co-primes is the *GCD* operation, which is in $O(n^2)$ [24] (Note: *GCD* stands for Greatest Common Divisor). For each newly generated integer, we need to check if the integer is pairwise co-prime with existing integers. Therefore, the complexity of generating W pairwise co-prime integers is in $O(W^2n^2)$. We can sort the W integers in $O(Wlog(W)n)$. The computation complexity for multiplying two integers of size l bits and v bits is in $O(lv)$. When checking the condition $\prod_{i=0}^{w-2} P_{W-i} < \prod_{i=1}^{w} P_i$, the cost is $O(w^2n^2)$. Thus, the total cost of generating Mignotte sequence is in $O(W^2n^2)$. Second, there is a need to multiply p_i integers of n bits each to generate a modulus for a user with weight p_i. The complexity for generating N moduli is in $O((p_1-1)n^2 + (p_2-1)n^2 + ... + (p_N-1)n^2) = O((W-N)n^2)$. Therefore, the total cost of generating user moduli in terms of bit operation is in $O(W^2n^2)$.

Next, let us consider the newly proposed CRT based scheme. The only operation needed in the new CRT based scheme is the generation of N pairwise co-prime integers of length $p_1n, \cdots, p_Nn$. The running time of this operation mainly depends on the cost of checking whether these numbers are pairwise co-prime. Thus, the computational complexity is in $O(N^2\hat{w}^2n^2)$, where $\hat{w} = max\{p_1, \cdots, p_N\}$.

Consider the case of non-weighted secret sharing, in which $\hat{w} = 1$ and $W = N$, the complexity of our scheme is in $O(N^2n^2)$ which is equal to that of Mignotte's scheme. However, our new scheme does not involve additional operations like the generation of a Mignotte sequence, therefore, our scheme is more efficient. Consider the case of weighted secret sharing, in which it is possible that $W^2 \gg N^2$, it can be observed from our experimental results that our new scheme is still more efficient than Mignotte's scheme.

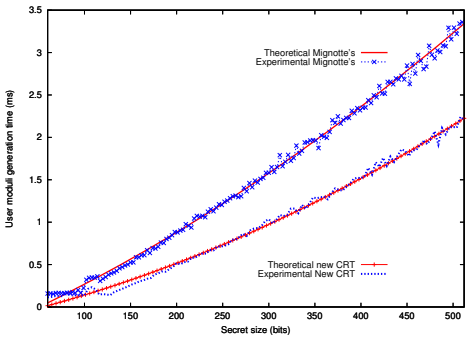

Fig. 5. Secret size VS user modulus generation Time (ms) (number of participants = 15, number of secrets = 1, disclosure weight = 4, $\hat{p} = (1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)$)

To verify the performance of Mignotte's CRT based scheme and our new CRT based scheme, we implemented and conducted experiments on Mignotte's scheme. With weights $\hat{p} =$

$(1,1,1,1,1,1,1,1,1,1,1,1,1,1,1)$ (i.e., same weighted secret sharing) as shown in Figure 5, the new CRT based scheme is more efficient in generating modulus for each user. With weights $\hat{p} = (1,2,3,1,2,3,1,2,3,1,2,3,1,2,3)$ (i.e., weighted secret sharing) as shown in Figure 6, we get the same result which indicates that the user moduli generation of our new scheme is more efficient than that of Mignotte's scheme.

It is worthy to mention that the secret recovery efficiency of our new scheme is similar to that of Mignotte's scheme since both use the identical operation. Also, computing $r_i = S \bmod P_i$ is same in both schemes.

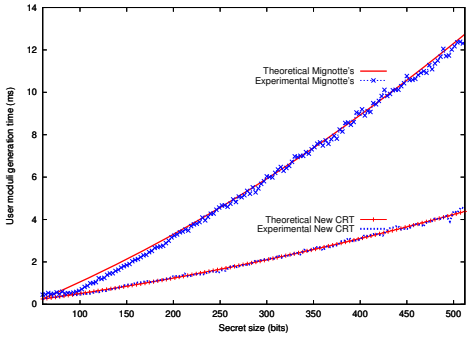

Fig. 6. Secret size VS user modulus generation Time (ms) (number of participants = 15, number of secrets = 1, disclosure weight = 4, $\hat{p} = (1,2,3,1,2,3,1,2,3,1,2,3,1,2,3)$)

In summary, our new CRT based scheme is more efficient than both Shamir's scheme and Mignotte's scheme and is much simpler than Mignotte's scheme. It is worthy to mention that even though we just compared the new CRT based scheme with original Mignotte's scheme [17], this conclusion also applies to other more recent CRT based schemes [12], [14] since they utilize the same principles and have similar efficiency as the original one.

VI. Conclusions

We proposed a clean and efficient weighted multiple secret sharing scheme based on Chinese Remainder Theorem. The new scheme is flexible in the sense that it can also be naturally applied to other cases such as sharing a single secret with same-weight shares in a uniform way. The principle of the new scheme is simple and its implementation is straightforward. Both theoretical analysis and experimental results were presented and justified that the new CRT based scheme outperforms Shamir's secret sharing scheme and Mignotte's CRT based scheme. One additional advantage of the new scheme is that the size of shares can vary distantly to fit different requirements and constraints of various devices such as sensors, PDAs, cell phones, laptops, and desktops. Hence, the new scheme is able to apply to broader applications in pervasive computing domains. This, again, justifies the flexibility and adaptivity of the new scheme.

As future work, we will extend the new scheme to deal with other desirable features such as dynamics and verifiability. We will also study the applicability of our newly proposed scheme to real world applications such as secure and efficient e-voting systems.

References

[1] Alfred V. Aho, John E. Hopcroft, and Jeffrey D. Ullman. *The design and analysis of computer algorithms*. Addison-Wesley, first edition, 1974.

[2] Li Bai and Xukai Zou. A proactive secret sharing scheme in matrix projection method. *International Journal of Security and Networks*, 4(2):15–23, 2009.

[3] Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In *Second Theory of Cryptography Conference, TCC 2005. Lecture Notes in Comput. Sci. 3378*, pages 600–619. Springer-Verlag, 2005.

[4] J. Benaloh and J. Leichter. Generalized secret sharing and monotone functions. *Lecture Notes in Computer Science*, 403:27–35, 1989.

[5] G. R. Blakley. Safeguarding cryptographic keys. *American Federation of Information Processing Societies Proceedings*, 48:313–317, 1979.

[6] P. Feldman. A practical scheme for non-interactive verifiable secret sharing. *Proceedings of the 28th IEEE Symposium on the Foundations of Computer Science*, pages 427–437, 1987.

[7] M. Franklin and M. Yung. Communication complexity of secure computation. *STOC*, pages 699–710, 1992.

[8] R. Gennaro. Theory and practice of verifiable secret sharing. *Ph.D-thesis, MIT*, 1995.

[9] H. Ghodosi, J. Pieprzyk, and R. Safavi-Naini. Secret sharing in multilevel and compartmented groups. *Lecture Notes in Computer Science*, 1438:367–378, 1998.

[10] J. He and E. Dawson. Multistage secret sharing based on one-way function. *Electronics Letters*, 30:1591–1592, 1994.

[11] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. *Lecture Notes in Computer Science*, 963:339–352, 1995.

[12] S. Iftene. A generalization of mignotte's secret sharing scheme. *Proceedings of the 6th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, pages 196–201, 2004.

[13] S. Iftene. General secret sharing based on the chinese remainder theorem with applications in e-voting. *Electronic Notes in Theoretical Computer Science*, 186:67–84, 2007.

[14] S. Iftene and I. Boureanu. Weighted threshold secret sharing based on the chinese remainder theorem. *Computer Science Section*, pages 161–172, 2005.

[15] I. Ingemarsson and G. J. Simmons. A protocol to set up shared secret schemes without the assistance of mutually trusted party. *Lecture Notes in Computer Science*, 473:266–282, 1991.

[16] K. M. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang. Changing thresholds in the absence of secure channels. *Lecture Notes in Computer Science*, 1587:177–191, 1999.

[17] M. Mignotte. How to share a secret. *Lecture Notes in Computer Science*, 149:371–375, 1983.

[18] Liaojun Pang, Huixian Li, Ye Yao, and Yumin Wang. A verifiable (t, n) multiple secret sharing scheme and its analyses. *2008 International Symposium on Electronic Commerce and Security*, pages 22–26, 2008.

[19] T. P. Pedersen. non-interactive and information theoretic secure verifiable secret sharing. *Lecture Notes in Computer Science*, 576:129–140, 1992.

[20] M. Quisquater, B. Preneel, and J. Vandewalle. On the security of the threshold scheme based on the chinese remainder theorem. *in Proc. of PKC 2002, Lecture Notes in Computer Science*, 2274:199–210, 2002.

[21] A. Shamir. How to share a secret. *Communication of ACM*, 22:612–613, November 1979.

[22] Ron Steinfelda, Josef Pieprzyka, and Huaxiong Wang. Lattice-based threshold-changeability for standard crt secret-sharing schemes. *Finite Fields and Their Applications*, 12:653–680, 2006.

[23] Ron Steinfelda, Josef Pieprzyka, and Huaxiong Wang. Lattice-based threshold changeability for standard shamir secret-sharing schemes. *IEEE Transactions on Information Theory*, 53:2542–2559, 2007.

[24] D. R. Stinson, editor. *Cryptography: Theory and Practice*. CRC Press, Inc., Boca Raton, Florida, USA, 1995.

[25] Tamir Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20(2):237–264, November 2007.

[26] Tamir Tassa, Nira Dyn, and U Ci. Multipartite secret sharing by bivariate interpolation. In *33rd International Colloquium on Automata, Languages and Programming, ICALP 2006, Lecture Notes in Comput. Sci. 4052*, pages 288–299. Springer-Verlag, 2006.