ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
СПЕЦИАЛИЗИРАНО ЖУРИ ПО
КОМУНИКАЦИОННА И КОМПЮТЪРНА
ТЕХНИКА

маг.инж.Бюлбюл Шахибова Зюлямова

МЕТОДИ ЗА РАЗПРЕДЕЛЕНИЕ НА ТАЙНАТА В СЪВРЕМЕННАТА КРИПТОГРАФИЯ

АВТОРЕФЕРАТ

НА ДИСЕРТАЦИОНЕН ТРУД
ЗА ПОЛУЧАВАНЕ НА ОБРАЗОВАТЕЛНАТА И НАУЧНА
СТЕПЕН "**ДОКТОР**"

Научна специалност: „Системно програмиране"

София, 2015 г.

ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
СПЕЦИАЛИЗИРАНО ЖУРИ ПО
КОМУНИКАЦИОННА И КОМПЮТЪРНА
ТЕХНИКА

маг.инж.Бюлбюл Шахибова Зюлямова

МЕТОДИ ЗА РАЗПРЕДЕЛЕНИЕ НА ТАЙНАТА В СЪВРЕМЕННАТА КРИПТОГРАФИЯ

АВТОРЕФЕРАТ

НА ДИСЕРТАЦИОНЕН ТРУД
ЗА ПОЛУЧАВАНЕ НА ОБРАЗОВАТЕЛНАТА И НАУЧНА
СТЕПЕН "**ДОКТОР**"

Научна специалност: „Системно програмиране"

Научни ръководители:
проф. д-р инж. Огнян Наков
проф. д-р инж. Даниела Гоцева

Рецензенти:

София, 2015 г.

Дисертационният труд се състои от пет глави. Текстът е написан на 129 страници и съдържа 8 фигури и 1 таблица. Цитирани са 177 литературни източника и Internet страници. Номерата на фигурите, таблиците и уравненията в автореферата съвпадат с тези от дисертацията.

Дисертационният труд е обсъден и насочен за защита на аседание на катедра „Компютърни системи" към Факултет по компютърни системи и управление на Технически университет – София, състояло се на 23 февруари 2015 год.

Защитата на дисертационния труд ще се състои на 19 юни 2015 г. от 12.00 часа в зала 2140 на II блок на Технически Университет– София на заседание на специализирано Научно жури по Комуникационна и Компютърна техника.

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултета по „Комютърни системи и управление", стая 1443а, I блок на Технически Университет-София.

Автор: Бюлбюл Шахибова Зюлямова
Заглавие: Методи за разпределение на тайната в съвременната криптография.

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Цел и задачи на изследването

Целта на дисертационния труд е: развитие на методите за разпределена защита на информацията срещу неправомерни действия. За изпълнение на тази цел са дефинирани следните задачи:

1. Изследване на възможностите за нарушаване достоверността на информацията, и преглед на начините и средствата за защита на данните.
2. Изследване на съществуващи вече решения за разпределена защита на информацията, от гледна точка на сигурността на данните и защитата им от неправомерен достъп.
3. Подобрение в съществуващите методи за разпределена защита на информацията, с цел увеличаване на сигурността при опит за проникване в системата .
4. Разработване на програмни решения, прилагащи предложените в точка 3 подобрения в методите за разпределена защита на информацията.
5. Анализ на получените резултати.

Структура на дисертационния труд

За да реши поставените задачи, дисертационният труд е разделен на 5 глави, справка за приносите и библиография. Всяка глава има въведение в конкретната проблематика, описание на решението на поставената задача и обобщение, в което са дадени направените изводи и препоръки за по-нататъшна работа. В края на дисертационния труд са дадени научните, научно-приложните и приложните приноси. Текстът на дисертацията е написан на 129 страници и съдържа 8 фигури и 1 таблица. Цитирани са 177 литературни източника и Internet страници. Номерата на фигурите и таблиците в автореферата съвпадат с тези от дисертацията. Ето и конкретното съдържание на всяка от главите:

1. УВОД В ПРОБЛЕМАТИКАТА

Изследвани са възможностите за нарушаване достоверността на информацията и е направен преглед на начините и средствата за защита на данните. Специално внимание е отделено на методите за споделяне на тайна.

2. КЛАСИЧЕСКО РАЗПРЕДЕЛЕНИЕ НА ТАЙНАТА

На основата на направения преглед на начините за защита на информация, е разгледан проблема за разпределената защита на информационните ресурси. Разгледани са и са описани възможностите

на различни математически подходи, посредством които се реализира разпределената защита на информацията.

3. **КВАНТОВИ КОМПЮТРИ И ОСНОВИ НА КВАНТОВАТА КРИПТОГРАФИЯ**

Представени са квантовия компютър и защитата на данните, основана на квантовата криптография. Специално внимание е отделено на по-важните квантови алгоритми , които евентуално ще бъдат използвани за криптиране и споделяне на информация.Представени са редица математически подходи за решаване на проблема със защита на информационните ресурси.

4. **СИСТЕМА ЗА РАЗПРЕДЕЛЕНИЕ НА ТАЙНАТА, ОСНОВАНА НА КИТАЙСКАТА ТЕОРЕМА ЗА ОСТАТЪЦИТЕ**

Представена е разпределената защита на основата на китайската теорема за остатъците. Направен е анализ на възможността за промяна на определени параметри при нейното използване, които позволяват подобряване защитеността на информацията.

5. **ПРОЕКТИРАНЕ И РЕАЛИЗАЦИЯ НА СИСТЕМА ЗА РАЗПРЕДЕЛЕНИЕ НА ТАЙНАТА, ОСНОВАНА НА КИТАЙСКАТА ТЕОРЕМА ЗА ОСТАТЪЦИТЕ**

Разработен е програмен продукт, с които са проведени изследвания. Посочени са резултати, получени след изследване влиянието на определени фактори свързани с използването на теоремата за остатъците като средство за разпределена защита, както и на предложеното развитие на методите за споделена отговорност при защита на информация.

Публикации

Резултатите по дисертацията са публикувани в списание “Communication and Computer Engineering”, ТУ-София, в трудовете на международните конференции “УНИТЕХ”-Габрово ”, International Conference “Challenges in High Education and Research in 21st Centuary”. Списък на публикациите по дисертацията е даден в края на автореферата.

КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава 1. Увод в проблематиката. Изследване на възможностите за нарушаване достоверността на информацията, преглед на начините и средствата за защита на данните

На този етап от повсеместно използване на компютърната техника и изградената комуникационна инфраструктура, като среда за осъществяване на различни информационни процеси, се налага използването на нови усъвършенствани и адекватни на

информационната среда, методи и средства за защита на съхраняваните, обработвани и обменяни данни.

Познаването на заплахите е от съществено значение за ефективен анализ на риска и за подходящ подбор на средствата за защита. Заплахите се променят непрекъснато заедно с развитие на информационните технологии и средствата за защита.

Източниците на заплахи за информационната сигурност могат да бъдат категоризирани по следния начин :

1. Недостатъци в политиката
   - Отсъствие на документ, описващ политиката на безопасност;
   - Отсъствие на логична система за контрол на достъпа;
   - Отсъствие на контрол при инсталиране и промени в програмното осигуряване;
   - Отсъствие на процедури за обработка на инциденти или възстановяване след атаки;
   - Неадекватно администриране, мониторинг и аудит на системната сигурност;
   - Неинформираност на потребителите;
2. Технологични недостатъци– голяма част от системите и технологиите се разработват с цел предоставяне на достъп, но не и за неговия контрол.
3. Грешки в настройките – използване по подразбиране на пароли, услуги и т.н. при настройка на оборудване.
4. Колективен достъп– колективния метод се явява основно средство за реализиране на заплахите за информационната сигурност. Той е заложен още със създаването на Интернет. Голяма част от системите биват конфигурирани за колективно ползване на информация.
5. Слаби пароли – най-често използвания метод за реализиране на заплахите за информационната сигурност са слабите пароли. Те както и в началото се ползват основно за автентификация на потребителите и се явяват съществена уязвимост за всяка система. Много често се използват къси пароли (под четири символа) или леки за отгатване, което дава възможност чрез обхождане на възможните пароли да се стигне до истинската.
6. Дефекти в програмите – при реализиране на заплахите много често се използват дефекти в програмите. Към тези дефекти се отнася оставен в програмата „черен вход” (back door), който позволява в последствие да се влиза в програмата.
7. Социален инжинеринг - получаване на несанкциониран достъп до информация или система без използване на технически средства. Залага се на човешките слабости – доверчивост, безотговорност,

липса на съответни знания. Други форми на социален ижинеринг се явява изследване на „боклуците” на организацията, използване на източници за открита информация и т.н.

8. Отказ в обслужване – DoS-атака (Denial of Service) - злонамерени действия, водещи до блокиране на системата и отказ на достъпа на потребителите до ресурсите на системата. Атаките DoS имат много форми, те биват централизирани (задействани от една система) или разпределени (задействани от няколко системи).
9. Прослушване на мрежата – прослушването, или снифинг (sniffing), се използва за събиране на системна информация. За целта мрежовия адаптер се поставя в режим на прослушване на трафика,т.е. мрежовия адаптер ще прихваща всички пакети предавани по мрежата, а не само тези които са адресирани до него.
10. Имитация на IP-адреси – правилността на IP-адресите в пакетите не се проверява. Това позволява промяна на адреса на отправителя и реализиране на заплаха.
11. Вирусите остават сериозен проблем както за голяма част от организациите, така и за домашните потребители. Най общо се различават три типа програми: компютърни вируси, програми "троянски кон", червеи.
12. Неоторизиран достъп – получаване на достъп до системните ресурси от неоторизирано лице, което действа като законен потребител на системата.
13. Несъответстващ достъп – потребител, законен или незаконен получава права за достъп до ресурс, който не е разрешено да използва. Реализира се, когато: Правата на потребителя не са определени правилно , механизмът на управление на достъпа или механизмът за определяне на привилегии не са в достатъчна степен детайлизирани.
14. Прослушване на трафика – достъп до данните, при който някой, комуто не е разрешено, чете или записва информация, когато тя се предава по мрежата. Реализира се чрез: включване към кабелната мрежа , прослушване на ефира, злоупотреба с включен към мрежата мрежов анализатор и т.н.
15. Заплаха за модифициране – опит за неправомерна промяна на информацията, обикновено реализирана чрез метода прихващане. При нея хакера прихваща трафика и има възможност да замени, добави или унищожи информация.

Механизмите за осигуряване на сигурност в информационните системи са следните:

1. Шифриране
2. Електронен цифров подпис
3. Механизми за управление на достъпа

4. Механизми за контрол на цялостта на данните
5. Механизми за автентификация
6. Механизми за запълване на трафика
7. Механизми за управление на маршрутизацията
8. Механизми за нотаризация

В условия на глобално изграждането информационно общество многообразието от криптографски средства за защита на данните, както методите за цифрово подписване при доказване автентичността на съобщенията и идентичността на участниците, се явяват единствена алтернатива и с възможности за най-широко приложение в създаваното информационно общество.

Посредством цифровото подписване могат да бъдат игнорирани редица възможности за неправомерни действия с информационните масиви като:

- отказ на източника от подадено съобщение – източника прави опит да се разграничи от информацията в съобщението, което е изпратил. Причините могат да бъдат различни, но за получателя подобен акт е опасен, тъй като може да доведе до ползване на данни, които да го компроментират в неговата по-нататъшна дейност;
- модификация на съобщението – неупълномощен потребител след успешно проведена криптоаналитична атака, внася изменения в съдържанието на документа, в резултат на което в информационната среда се разпространяват данни чиито източник остава неизвестен.
- маскиране на действителен източник – източника на съобщението се опитва да се представи чрез него под чуждо име, като използва известни за него данни за друг легитимен участник, без неговото съгласие.

В криптографията съществуват разнообразни и остроумни методи за защита на информацията, включващи размяна на ключове за използуване в криптосистеми, така че страничен наблюдател да не може да ги разбере. Този въпрос е сравнително добре изследван и съществуват редица негови решения, използувани отдавна на практика (най-известен е RSA методът на Ривест-Шамир-Аделман за криптиране с открит ключ, основан на теоремата на Ойлер за сравнения).

Остава обаче открит въпросът как да запазим в тайна самия ключ, след като вече го притежаваме. Този проблем е много сериозен, тъй като ако външно лице узнае ключа за криптиране, то ще може без проблем да чете криптираните съобщения и тогава цялата система за криптиране на информация ще бъде компрометирана. Това е първият

важен проблем, който възниква при по-детайлно изследване на съвременните системи за защита на информация.

Може да се предложи ключът да се криптира, но това всъщност не е решение, тъй като в такъв случай просто заменяме ключа с нов – този, с който криптираме нашия.

Друг проблем е как да съхраняваме ключа. Например можем да го съхраняваме в отделно тайно място или дори да го помним наизуст, но в такъв случай отделен инцидент може да доведе до безвъзвратна загуба на ключа (да забравим ключа, хард-дискът на системата да бъде изтрит, касата да бъде разбита или да изгори и т.н.) Алтернативата е да се пазят копия на ключа на няколко алтернативни места, но в такъв случай нараства рискът от откраднването му, което е друг компромис със сигурността.

Тази дисертационна работа е посветена основно на изследване проблема за запазването на тайна информация. Оказва се че този проблем е много сериозен, с много и различни приложения и е свързан с редица други проблеми – например квантовите компютри и квантовата информация.

Под запазване на тайна информация се разбира най-общо следното: информацията се съхранява на няколко различни места, достъп до които имат само оторизирани за това субекти, при това се изисква за възстановяване на първоначалната информация да се получат съхранените данни от минимален брой от тези места, така че дори определен брой хранилища (под този минимален брой) да бъдат компрометирани (т.е. информацията от тях да бъде откраднатa), първоначалната информация да не може да бъде възстановена от тях.

Как да се организира пазенето на ключ, който да бъде достъпен за група от потребители, а не за отделни такива? Например компания, използваща електронен подпис, може да желае да е невъзможно за всеки отделен неин служител да може да подписва документ по електронен път, но това да е възможно за различни групи служители.

Един от първите, който разглежда този проблем, е Ади Шамир, който през 1979 г. предлага много елегантно решение, което е разгледано накратко по-долу [168].

Първо обаче ще формализираме проблема, който дефинирахме нестрого малко по-горе:

Нека K е тайно число (което представлява ключ за криптиране или някаква друга електронна тайна) и това число трябва да се запази сигурно и надеждно. За да се осигури това,се създават „тайни части” K1, K2, ... Kn такива, че

1) знанието на кои да е t от тайните части дава възможност K да бъде изчислимо лесно

2) знанието на кои да е t-1 от тайните части не дава възможност К да бъде изчислимо, т.е. К не е определено

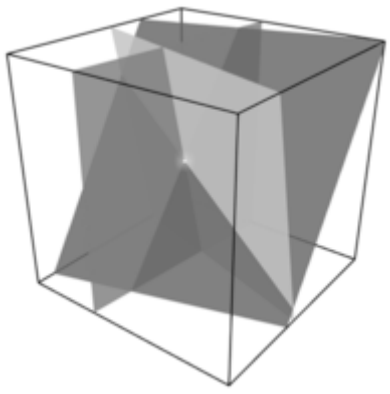
Това се нарича (t, n) – прагова схема

Нека потребителят има таен ключ и иска да го пази надеждно. Тогава той може да използва (n,2.n-1) – прагова схема. Като формира 2.n-1 тайни дяла и запази всеки от тях на различно място, потребителят си осигурява изключителна степен на надеждност, тъй като може да възстанови ключа от всеки n произволни дяла, т.е. достатъчно е да не загуби повече от половината тайни дяла, а за бъде разбит кодът, фалшификаторът трябва да открадне поне n различни дяла от n различни места.

Ако трябва да се реши проблема с компанията по-горе, то компанията трябва просто да реши колко голяма да бъде групата от служители, имаща право да подписва документите, т.е. каква да бъде стойността на n.

2 глава. Класическо разпределение на тайната

Идеятата за споделянето на тайна е представена графично на фиг.1: ако дадена информация трябва да се сподели между няколко души така, че да са необходими поне трима за да я възстановят еднозначно, тогава можем да я изобразим като точка в тримерното пространство, декартовите координати на която са численият код на тайната. Всеки от хората знае уравнението на една равнина, която минава през тази точка- това е делът, който той знае. Самата точка се възстановява като се вземе сечението на три равнини – аналитично това е решението на система от три уравнения с три неизвестни, описващи трите равнини. За да се възстанови еднозначно точката са необходими поне 3 равнини – сечението на 2 равнини е права, съдържаща освен търсената точка още безкрайно много други точки.



Фиг. 1 Споделяне на тайната

В криптографията под споделяне на тайната се разбира всеки метод, който разпределя информация между група от потребители по такъв начин, че всеки от тях притежава част от информацията. Самата

информация може да бъде възстановена само когато определен минимален брой дялове бъдат събрани и обработени съвместно по определен алгоритъм. Ако броят на дяловете е по-малък от необходимия тайната не може да бъде възстановена [123, 126, 135]

2.1. Мотивация – дефектна схема за споделяне на тайната

Една сигурна схема за споделяне на тайна трябва да разпределя дяловете по такъв начин, че всеки, който разполага с по-малко от t дяла не разполага с допълнителна информация за тайната в сравнение с друг, който разполага с 0 дяла.

Да разгледаме една наивна схема за споделяне на тайна: в нея тайната дума „парола" е разделена на дялове „па----„ , „ –ро--„ и „----ла". Ако един играч е с 0 дяла, но знае че тайната е от 6 букви, ще трябва евентуално да провери всяка от 30^6 = 729 000 000 възможни комбинации. Тази система за споделяне на тайна не е сигурна, тъй като играч с по-малко от t =3 дяла притежава съществена информация за съдържанието на тайната. Например ако притежава един дял той ще трябва да провери само 30^4 = 810 000 комбинации, а ако притежава два дяла броят на проверките намалява само до 30^2 = 900. В една сигурна схема за споделяне на тайната дори и само един липсващ дял не намалява броя на проверките – те трябва да остават 30^6 = 729 000 000.

Има ограничения, които са общи за всички такива схеми, за които няма строго доказателство за информационна сигурност:

Всеки дял от тайната трябва да бъде с големина поне равна на големината на самата тайна. Това условие се основава на теорията на информацията, но може да бъде разбрано и интуитивно: Ако имаме t-1 дяла, не трябва да можем да определим никаква допълнителна информация за тайната. Следователно липсващият дял трябва да съдържа такова количество информация, каквото съдържа и самата тайна, т.е. броят на значимите битове в тайната и в дяла трябва да бъде равен.

2.2. Тривиално споделяне на тайната

Има няколко (t, n) схеми за споделяне на тайната, когато t = n, и всички дялове са необходими за възстановяване на тайната:

- Тайната се кодира като цяло число s. Избира се за всеки играч i (без един) случайно цяло число ri. Избира се за последния играч числото (s − r1 − r2 − ... − rn − 1). Тайната се възстановява като сума от числата на всички играчи.
- Тайната се кодира като байт s. Избира се за всеки играч i (без един) случаен байт bi. Избира се за последния играч байта (s XOR b1 XOR b2 XOR ... XOR bi) където XOR е логическата

операция „изключващо или”. Тайната се възстановява като се приложи XOR за всички дялове. Ако тайната се кодира с повече байтове горната процедура се прави за всеки отделен байт.

2.3. Обновяемо споделяне на тайната

Ако играчите пазят техните дялове в незащитени компютърни сървъри, външна атака може да го кракне и да открадне тези дялове. Ако не е целесъобразно от практически съображения да се сменя тайната, тогава една безкомпромисна схема от типа на тази на Шамир може да бъде подновена. Дилърът генерира нов случаен полином със свободен член 0 и пресмята за всеки от играчите нова двойка числа, като x-координатата на старата и новата двойка са едни и същи. Всеки играч след това събира новата и старата стойност на y-координатата и така получава новата стойност на y-координатата.

2.4. Други приложения

Една схема са споделяне на тайна може да защитава дадена тайна при много сървъри и да позволява възстановяване в случай на срив на голяма част от тях.

Схема на Шамир за споделяне на тайна

Схемата на Шамир за споделяне на тайната е един алгоритъм в криптографията. Той е начин за споделяне на информация, където тайната се разделя на дялове. На всеки отделен участник се дава негов уникален дял, като точно определен минимален брой от дяловете е необходим за да се възстанови тайната.

Хомоморфна схема за споделяне на тайната

В криптографията хомоморфна схема за споделяне на тайната е начин за споделяне на тайната, използващ хомоморфизми.

В абстрактната алгебра хомоморфизмът е структурозапазващо изображение между две алгебрични структури (например групи, пръстени, векторни пространства и други. Най-общо, протоколите основани на хомоморфизъм имат ограничени възможности за мащабиране, поради което гласуването е ограничено до няколко възможности [143].

Византийска търпимост към дефектите

„Византийска търпимост към дефектите” е името, което се дава на една подобласт от изследванията за устойчивост към грешки. Тя е породена от така наречената „Задача на византийските генерали”, която е обобщение на Задачата на двамата генерали.

Обектът на изучаване на Византийската търпимост към дефектите е способността за защита срещу Византийски провал (Byzantine failure), при който някой компонент от дадена система не само се държи неправилно, но също така взаимодейства неправилно с много от останалите компоненти на системата. Коректно функциониращите компоненти при система с византийска търпимост към дефектите трябва да са в състояние да вземат същата група от решения при наличието на определен брой византийски провали, както и ако такива провали не съществуват. Разбира се, в такава система съществува горна граница на дела на предателите или ненадеждните компоненти в нея.

Тайно пресмятане с много участници

В криптографията, тайното пресмятане с много участници е задача, която първоначално е предложена от Андрю Яо (Andrew C. Yao) в негова статия от 1982 година[165]. В тази статия е предложена задачата на милионера (millionaire problem): Алис и Боб са двама милионери, които искат да проверят кой от тях е по-богат без да разкриват точната стойност на богатствата си. Яо предлага решение, позволяващо на Алис и Боб да задоволят любопитството си като спазват това ограничение.

Тази задача и нейното решение позволяват обобщение, наречено протокол за пресмятане с много участници (multi-party computation, MPC). В случая на тайно пресмятане с много участници са дадени участниците p1, p2, ..., pN, всеки от които има лични данни съответно d1, d2, ..., dN. Участниците трябва да изчислят стойността на открита функция F на N променливи в точката (d1, d2, ..., dN). Протоколът за тайно пресмятане е сигурно защитен ако никой участник не може да научи повече от описанието на откритата функция и от резултата на общото пресмятане, отколкото от собствените си входни данни.

Проверима схема за споделяне на тайната

В криптографията една схема за споделяне на тайната е проверима, ако е включена допълнителна информация, позволяваща на играчите да верифицират своите дялове съгласувано.

Формално Проверимата схема за споделяне на тайната означава, че дори дилърът да е злонамерен, съществува добре дефинирана тайна, която играчите да могат впоследствие да възстановят (в стандартното споделяне на тайната се предполага, че дилърът е честен). Концепцията за проверима схема за споделяне на тайната (verifiable secret sharing, VSS) е предложена за пръв път през 1985 от Б.Чор, С.Голдвасер, С.Микали и Б.Авербах [166].

Тайни избори с бюлетина

Проверимото споделяне на тайната може да се използва за построяване на напълно проверима система за гласуване.

Използувайки техниката на проверимото споделяне на тайната можем да решим задачата за избор, която ще опишем по-долу.

В задачата за избор всеки избирател може да гласува с 0 (против) или 1 (за), и сумата от всички вотове ще определи изборния резултат. В съответствие с изискванията за избори, трябва да бъдат изпълнени следните изисквания:

- Не се допускат компромиси с анонимността на гласуващите.
- Изборната администрация трябва да верифицира, че никой гласуващ, който да мами .

Ако се използва проверяема схема за споделяне на тайна, n преброители ще заменят изборния администратор. Всеки гласуващ ще разпредели по един дял от своя таен вот на всеки от тези n преброители. По този начин анонимността на гласуващия се гарантира и първото условие е изпълнено. Възстановяването на изборния резултат е лесно ако съществуват поне k<n преброители да открият полинома P.

Публично проверимо споделяне на тайна

В криптографията една схема за споделяне на тайната е публично проверима (publicly verifiable PVSS) ако тя е проверима схема за споделяне на тайната и ако всяка група, участваща в процеса, може да провери валидността на дяловете, които са разпределени от дилъра.

В една проверима схема за споделяне на тайната (verifiable secret sharing, VSS) целта е тя да издържи на злонамерени играчи, като:

(i) дилър, изпращащ некоректни дялове към някои или към всичките участници, и (ii) участници, изпращащи некоректни дялове в процеса на възстановяване.

3 глава. Квантови компютри и основи на квантовата криптография.

3.1. Уводни съображения

Информацията се предава, обработва и съхранява с помощта на физически средства. Следователно самата концепция за информация и изчисления може да се формулира в контекста на физическата теория, а изучаването на информационните процеси и дейности е свързано с експерименти. Това на пръв поглед тривиално наблюдение влече след

себе си далеч не тривиални следствия. Накратко ще се опитаме да опишем някои от тях по-долу.

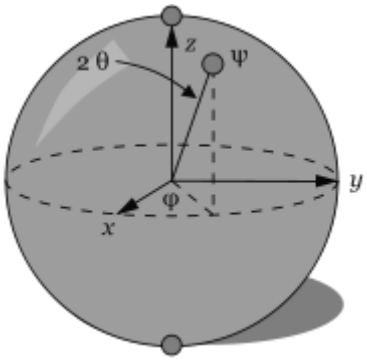
Съгласно Закона на Мур, скоростта на микропроцесорите се увеличава примерно на всеки 18 месеца. Единственият начин те да стават все по-бързи е да се намаляват физическите размери на съставните им компоненти. Ако това намаляване продължи със същите темпове, след няколко години размерите на логическите елементи, съставляващи процесорите, ще бъдат колкото няколко атома (в момента са от порядъка на 100 нанометра или 1000 ангстрьома, като технологията вече е слязла под този размер, , а типичните размери на атомите са 2-5 ангстрьома). При достигане на тези размери, освен че ще бъде достигната физическата граница за намаляването им, ще станат съществени и квантовите ефекти. Следователно ако искаме да продължим с увеличаването на бързодействието на съвременните компютри, ще трябва да бъде развита и нова технология за тяхното производство, основаваща се на квантовата механика.

Актуалността на проблема се отнася и за темата, която се разглежда в настоящата работа: ако в близко бъдеще бъде реализиран пълноценен квантов компютър, съвременните методи за криптиране и споделяне на тайна, основани на системи с открит ключ, ще се окажат неефективни. В хода на изложението ще покажем как теоретично става това, а сега ще споменем само, че ако за „разбиването" на даден ключ (например 64-битов, или разлагане на едно многоцифрено число на прости множители) са необходими години и дори векове работа на съвременен суперкомпютър, то на евентуалния квантов компютър ще са достатъчни само няколко секунди. Именно тази възможност, която засега е само теоретична – пълноценен квантов компютър все още не съществува - е основната причина всички водещи страни в света – например САЩ, Русия, Китай – да отделят значителни средства и научен потенциал, за да развият технологията, която евентуално ще позволи създаването на квантов компютър.

3.2. Предмет на квантовата информация

Науката за квантовата информация разглежда информацията като зависеща от квантовите ефекти във физиката. Тя включва теоретични публикации на изчислителни модели а също и голям брой експериментални опити в областта на квантовата физика, включващи изследвания какво може и какво не може да бъде направено с квантовата информация. Самият термин „квантова теория на информацията" се използува понякога, но той не може да обхване всички експериментални изследвания в тази област.

Квантовият бит (quantum bit, qubit, понякога qbit) е единица за квантова информация. Тази информация се описва чрез вектора на състоянието на една квантовомеханична система, която може да заема само 2 възможни състояния. Той е формално еквивалентен на двумерно векторно пространство над полето на комплексните числа Фиг.3.



Фиг. 3 Представяне на кюбит

Кюбитът има някои прилики с класическия бит, но в основата си е коренно различен. Също като бита, кюбитът може да заема две възможни състояния, нормално означавани с 0 или 1. Разликата е, че докато битът трябва да заеме еднозначно състояние 0 или 1, един кюбит може да бъде в състояние 0, 1 или тяхна суперпозиция.

Квантов регистър

Определен брой сплетени кюбитове взети заедно задават кюбитов регистър. Квантовите компютри извършват пресмятания чрез манипулации на кюбитовете в регистъра.

Всяка система с две нива може да бъде използвана като кюбит. Системи с много нива също могат да бъдат използувани ако позволяват две състояния, които да могат ефективно да бъдат разделени от останалите (например нулевото състояние и първото възбудено състояние на един нелинеен осцилатор).

3.3. Дефиниране на квантов компютър

Квантов компютър е всяко устройство за пресмятане, което използува пряко различни явления от квантовата механика, като например суперпозиция, при извършване на обработката на данни [69]. Квантовият компютър представлява изчислителна машина, работеща по законите на квантовата механика и принципно се отличава от класическите компютри, работещи по законите на класическата физика. Пълноценен квантов компютър към настоящия момент не съществува и представлява хипотетично устройство.

Ако опитите да бъде построен пълноценен квантов компютър в мащаб като сега съществуващите, такъв компютър ще бъде в

състояние да решава сега съществуващите „класически” проблеми експоненциално по-бързо в сравнение със сегашните компютри с „класическа” конструкция (например алгоритъма на Шор - Shor's algorithm) [74]. Квантовите компютри са различни от другите компютри като например традиционните компютри, основани на транзистори. Някои компютърни архитектури, като оптическите компютри например, могат да използуват класическа суперпозиция на електромагнитни вълни, но без някакви специфични квантовомеханични ресурси, те притежават по-малък потенциал за скоростни пресмятания в сравнение с квантовите компютри.

3.4. Проблеми и практически решения

Съществуват редица практически трудности, свързани с построяването на квантов компютър. Дейвид ДиВинченцо (David DiVincenzo) от IBM изброява следните изисквания, които един реален квантов компютър трябва да притежава [90]:

• физическа мащабируемост, с чиято помощ да се увеличи броят на кюбитовете

• кюбитовете да може да се инициализират с произволни стойности

• квантови гейтове по-бързи от времето за декохерентност

• универсален набор от гейтове

• кюбитовете да могат да се четат лесно

Да обобщим проблема от гледна точка на един инженер: Необходимо е да се реши проблемът за изграждане на система, която е изолирана от всичко, с изключение на механизма за измерване и манипулация. Освен това, потребителят трябва да бъде в състояние да изключи кюбитовете до момента на измерване, така че да не настъпи декохерентност на кюбитове по време на изпълнение на дейностите им.

3.5. Квантови алгоритми

Под квантов алгоритъм ще разбираме всеки физически процес, използуващ квантовите ефекти, за да извърши полезни изчисления.

Алгоритъм на Дойч-Джоса и оракул (Deutsch-Jozsa algorithm)

Алгоритъмът на Дойч-Джоса е квантов алгоритъм, предложен от Дейвид Дойч и Ричард Джоса през 1992 година [175]. Независимо от малката практическа полза от него, той е един от първите примери на квантов алгоритъм, който е по-ефективен от всеки възможен класически алгоритъм.

В алгоритъма на Дойч-Джоса имаме квантов компютър, който е „черна кутия” или оракул, и който изчислява неизвестната функция .

Известно е, че функцията е или константа (0 за всички входове или 1 за всички входове) или е балансирана (връща 1 за половината входове и 0 за другата половина от входове); задачата ни е да определим дали f е константа или е балансирана функция, т.е. какво пресмята оракулът.

Алгоритъм на Гроувър

Алгоритъмът на Гроувър е квантов алгоритъм за търсене в несортирана база данни с N състояния за време O(N1/2) и използуване на O(logN) пространство за съхранение. Той е предложен от Лов Гроувър през 1996 година [109].

Класическото търсене в една несортирана база данни изисква линейно търсене, което е със сложност O (N) във времето. Алгоритъмът на Гроувър, който изисква O(N1/2) време, е възможно най-бързият квантов алгоритъм за търсене в една несортирана база данни. Той задава "само" квадратична бързина, за разлика от другите квантови алгоритми, които могат да осигурят експоненциално ускорение в сравнение със своите класическа аналози. Въпреки това, дори и квадратичната бързина е значителна, когато базата е голяма.

Алгоритъм на Шор

Алгоритъмът на Шор е най-известният към настоящия момент квантов алгоритъм. Това е алгоритъм за факторизация (разлагане на множители) на цялото число N за време O((log N)3) и обем O(log N). Алгоритъмът е предложен от Питър Шор и носи неговото име [74].

Накратко, задачата е по зададено естествено число N да се намери естествено число k по-голямо от 1 и по-малко от N, което да дели без остатък N. По-долу ще опишем как това намиране може да се сведе до задачата за намиране на периода на някаква периодична функция f.

4 глава. Система за разпределение на тайната, основана на Китайската теорема за остатъците

4.1. Обща идея на метода

В тази глава е предложена нова схема за споделяне на информация и е показана нейната коректност. По този начин се показва, че в тази област възможностите за развитие дори на класическите методи (които не са основани на квантови компютри и квантови изчисления) далеч не са изчерпани и могат да бъдат развивани и прилагани за практически нужди.

В тази част на работата е предложена принципно различна схема, в сравнение със схемата на Шамир, осигуряваща същото ниво

на сигурност. Системата се основава на добре известната Китайска теорема за остатъците [163]:

Нека a1,a2,..., ак са естествени взаимно прости числа. Тогава за всяко цяло число с в интервала (0,a1*a2*....*ак) съществува единствена к-орка от остатъци (x1,x2,....,хк) такива, че хр е остатъкът на с при деление на ар, и с се възстановява еднозначно по к-орката (x1,x2,....,хк). Тогава схемата за споделяне на тайната, основана на Китайската теорема, е:

По зададено число с, което трябва да се скрие (сподели) се избират взаимно простите числа a1,a2,..an, намират се остатъците x1,x2,...xn, и наредените двойки (ар, хр) p=1,2,..n, се споделят между участниците. По китайската теорема от k от тези двойки може да се възстанови числото с при необходимост.

Ясно е че идеята може да се развие до степен, покриваща напълно схемата на Шамир и отговаряща на условията за споделяне на тайната.

Предимствата на новата схема са: различна от схемата на Шамир, имаща същата степен на сигурност. Ако човекът, който се опитва да разбие секрета, не знае че споделената тайна не е по схемата на Шамир, ще бъде затруднен при атаката на схемата. Тъй като атаките обикновено се основават на човешка слабост и се свеждат до кражба на отделни части от тайната, след което се пробват различни техники, ако не се знае предварително по каква схема е извършено разпределянето на тайната, това би затруднило атаката при частична информация.

4.2. Китайска теорема за остатъците

Китайската теорема за остатъците е един резултат, отнасящ се до конгруенциите (сравненията) в теорията на числата и до нейните обобщения в абстрактната алгебра.

Нека $n_1, n_2, \ldots, n_k$ са цели числа, всеки две от които са взаимно прости. Тогава за всеки набор от цели числа $a_1, a_2, \ldots, a_k$, съществува цяло число x, което е решение на системата от сравнения

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

Нещо повече: всички решения x на тази система са конгруентни по модул произведението на базите $N = n_1 n_2 \ldots n_k$.

Понякога системата от сравнения може да бъде решена дори когато n_i не са взаимно прости. Решение *x* съществува тогава и само тогава, когато

$$a_i \equiv a_j \pmod{\gcd(n_i, n_j)} \qquad \text{for all } i \text{ and } j.$$

Тогава всички решения x са конгруентни по модул най-малкото общо кратно на основите n_i.

4.3. Конструктивен алгоритъм за намиране на решението

Алгоритмът, описан по-долу, разглежда само случая, когато всички n_i са взаимно прости.

Да предположим както по-горе, че търсим решение на системата от сравнения :

$$x \equiv a_i \pmod{n_i} \quad \text{for } i = 1, \ldots, k.$$

Отново дефинираме произведението $N = n_1 n_2 \ldots n_k$. Тогава решението x може да бъде намерено по следния начин:

За всяко *i* целите числа n_i и N / n_i са взаимно прости. Използувайки разширения алгоритъм на Евклид, можем да намерим такива цели числа r_i и s_i , че $r_i n_i + s_i N / n_i = 1$. След това, използувайки означението $e_i = s_i N / n_i$, получаваме следния израз:

$$r_i n_i + e_i = 1$$

Да разгледаме e_i. Горното уравнение ни гарантира, че неговия остатък при деление на n_i трябва да бъде 1. От друга страна, тъй като това число е дефинирано като $s_i N / n_i$, а самото представяне на *N* гарантира, че то се дели без остатък на всяко от числата n_j за $j \neq i$. Накратко:

$$e_i \equiv 1 \pmod{n_i} \quad \text{and} \quad e_i \equiv 0 \pmod{n_j} \quad \text{for } i \neq j$$

Оттук, като използуваме свойствата на сравненията по отношение на операциите събиране и умножение, получаваме, че едно решение на нашата система е числото :

$$x = \sum_{i=1}^{k} a_i e_i.$$

За конкретност нека разгледаме задачата за намиране на цялото число *x* такова, че

$$x \equiv 2 \pmod{3},$$

$$x \equiv 3 \pmod{4},$$

$$x \equiv 1 \pmod{5}.$$

Използувайки разширения алгоритъм на Евклид за *3* и *4×5 = 20*, получаваме *(−13) × 3 + 2 × 20 = 1*, т.е. $e_1 = 40$. Използувайки алгоритъма на Евклид за *4* и *3×5 = 15*, получаваме *(−11) × 4 + 3 × 15*

$= 1$. Оттук $e_2 = 45$. И накрая, използувайки алгоритъма на Евклид за 5 и $3 \times 4 = 12$, получаваме $5 \times 5 + (-2) \times 12 = 1$, следователно $e_3 = -24$. Накрая решението x е равно на $2 \times 40 + 3 \times 45 + 1 \times (-24) = 191$. Всички останали решения на системата са конгруентни на $191 \bmod 60$, $(3 \times 4 \times 5 = 60)$, което означава че са конгруентни на $11 \bmod 60$.

Има многобройни реализации на разширеното евклидово алгоритъм, който ще получава различни набори от e_1, e_2, и e_3. Това обаче ще предизвика същия отговор, т.е. *11 по модул 60*.

4.4. Реализация на алгоритъма за намиране на решение

Тъй като алгоритмът за намиране на решение, описан по-горе, не е достатъчно ефективен за прилагане в конкретни пресмятания, беше направена негова модификация, която позволява достатъчно ефективна реализация на компютър.

Ето и псевдокод на модифицирания алгоритъм:

{Алгоритъм за възстановяване на число по остатъци в Китайската теорема за остатъците}

```
Input (n); {брой на базите}
For i:=1 to n do
        Begin
          Read (base[i]); {бази}
          Read  (ostatak[i]);    {остатъци на числото по базите}
        End;
For i:=1 to n-1 do {главен цикъл}
        Begin
                For j:=i to n-1 do {сорировка по възходящ ред на базите}
                        For m:=j+1 to n do if base[j]>base[m] then
                                Begin
                                        Temp1:=base[j]; Temp2:=ostatak[j];
                                        base[j]:=base[m]; ostatak[j]:=ostatak[m];
                                        base[m]:=Temp1; ostatak[m]:=Temp2;
                                End; {сортировката не е задължителна но
ускорява процеса}
                rr:=0;{нов остатък по база base[i]* base[i+1]}
                flag:=false{}
repeat {отворен цикъл за намиране на най-малкото число, даващо остатъци
ostatak[i] и ostatak[i+1] при деление на base[i] и base[i+1] съответно. По този начин
се намалява броят на базите с 1 докато остане само една: base:= base[1]*
base[2]*…* base[n]}
                        if ostatak[i]=ostatak[i+1] then
begin
 rr:=ostatak[i];
flag:=true;
end {if}
                        else if ostatak [i]<ostatak[i+1] then ostatak
[i]:=ostatak[i]+base[i]{<}
```

```
                    else ostatak[i+1]:= ostatak[i+1]+base[i+1]    {>}
        until flag=true {край на цикъла}
        base[i+1]:=base[i]*base[i+1]; {нова база }
        ostatak[i+1]:=rr; {нов остатък}
End;
Output (ostatak[n]); {търсеното число}
```

В горната схема единствената стъпка, в която има допълнителни изисквания е Изборът на модулите. Ето и условията, на които те трябва да отговарят:

За избора на модулите определящи са две съображения; големината на интервала [0,M], в който ще се намира числото c, което ще споделяме като тайна, и броят k на дяловете, които са достатъчни за възстановяване на c. Те трябва да се зададат предварително.

Ако M и k са вече известни, трябва да изберем n взаимно прости числа a1,a2,..., an, такива че произведението на кои да е k от тях да е по-голямо от M. Най-простият начин да направим това е като изберем n различни прости числа, най-малкото от които е по-голямо от $\sqrt[k]{M}$. Тогава горното условие е тривиално изпълнено.

Разбира се, от различни съображения, например изчислителни, може числата да се изберат и по други начини, но условието произведението на кои да е k от тях да е по-голямо от M трябва да е винаги изпълнено, за да се гарантират условията на Китайската теорема за остатъците.

4.5. Сигурност на предложената схема

В тази част анализираме сигурността на предложената схема. Анализът ще започне с показване на някои вероятностни характеристики на схемата

Теорема: Остатъците получавани при използване на Китайската теорема са независими.

Доказателство: Да предположим, че x е N-битово число. Нека p и q са два модула, участващи в S и нека Y, Z са случайни величини, означаващи остатъците на x mod p и x mod q съответно.

Нека y = x mod p и z = x mod q . Съгласно Китайската теорема за остатъците наредената двойка (y, z) еднозначно определя x в интервалите от стойности [0, pq -1] , [pq,2pq -1].

От това следва, че P{Y=y & Z=z}=1/p.q .

Ясно е, че P{Y=y} = 1/p, P{Z=z} = 1/q .

Резултатът от горните действия показва че P{Y=y & Z=z}= P{Y=y}. P{Z=z}, или че двете случайни величини са независими.

От горната теорема следва, че ако знаем по-малко от критичния брой k двойки (aq, xq), по никакъв начин не можем да определим

недостигащите стойности, и следователно не можем да възстановим и числото c.

4.6. Използване на системата за споделяне на тайна, основана на Китайската теорема за остатъците

Последователността от действия при използване на системата за споделяне на информация базирана на китайската теорема за остатъците е следната:

1. Имаме тайна S ,която трябва да се сподели между група от участници
2. Определя се интервал от(0-M) , в който се намира тайната
3. Задава се максималния брой участници в схемата n
4. Определя се минималния брой участници необходими за възстановяване на тайната k
5. Избират се n на брой взаимно прости числа
6. Извършва се проверка на тези числа дали отговарят на следните условия:
   - произведението на кои да е k от тях трябва да е по-голямо от горната граница на интервала M
   - произведението на кои да е k-1от тях трябва да бъде по-малко от M

   Ако избраните числа отговарят на тези условия ,то тогава се изпълнява стъпка 7.,в противен случай се избират нови числа.
7. Изчисляват се остатъците и на всеки участник в схемата му се дава част от тайната
8. Възстановяването на тайната става ,когато са налични k дяла от тайната. Самото изчисляване на тайното число се извършва по следния начин:
   - генерират се аритметични прогресии с начална стойност остатъка получен при деление на тайната S на простите числа n и стъпка на прогресията съответното число n
   - извършва се търсене на съвпадения в редиците. В примера даден по-долу се вижда ,че при наличие на по-малък брой дялове от необходимия за възстановяване на тайната няма как еднозначно да се определи кое е тайното число ,тъй като в съответните редици има и други съвпадащи стойности. При наличие на k дяла тайната се възстановява еднозначно.

Примерно използване на схема за споделяне на тайна , използваща Китайската теорема за остатъците:

- Общ брой участници: 5
- Минимален брой участници: 3
- Ключ за криптиране 649

- Интервал 0 до 1000
- Избор на взаимно прости делители: 11,13,15,17,19
- 11*13*15 = 2145 17*19 = 323
- Удовлетворява се условието на КТ
- Изчисляват се остатъците и всеки участник в схемата получава своя дял: (11,0) (13,12) (15,4) (17,3) (19,3)
- Генериране на аритметичните прогресии и възстановяване на тайната

0,11,***22***,33,44,55,66,***77***,88,99,110,121,132,143,***154***,165,176,187,198,209,220,231,242,253,264,275,286,297,308,319,330,341,352,363,374,385,396,407,418,429,440,451,462,473,484,495,506,517,528,539,550,561,572,583,594,605,616,627,638,***649***,660,671,682,693,704,715,726,737,748,759,770,781,792,803,814,825,836,847,858,869,880,891,902,913,924,***935***,946,957,968,979,990

12,25,38,51,64,***77***,90,103,116,129,142,***155***,168,181,194,207,220,233,246,259,272,285,298,311,324,337,350,363,376,389,402,415,428,441,454,467,480,493,506,519,532,545,558,571,584,597,610,623,636,***649***,662,675,688,701,714,727,740,753,766,779,792,805,818,831,844,857,870,883,896,909,922,***935***,948,961,974,987,1000

4,19,34,49,64,79,94,109,124,139,***154***,169,184,199,214,229,244,259,274,289,304,319,334,349,364,379,394,409,424,439,454,469,484,499,514,529,544,559,574,589,604,619,634,***649***,664,679,694,709,724,739,754,769,784,799,814,829,844,859,874,889,904,919,***934***,949,964,979,994

3,20,37,54,71,88,105,122,139,156,173,190,207,224,241,258,275,292,309,326,343,360,377,394,411,428,445,462,479,496,513,530,547,564,581,598,615,632,***649***,666,683,700,717,734,751,768,785,802,819,836,853,870,887,904,921,938,955,972,989

3,22,41,60,79,98,117,136,155,174,193,212,231,250,269,288,307,326,345,364,383,402,421,440,459,478,497,516,535,554,573,592,611,630,649,668,687,706,725,744,763,782,801,820,839,858,877,896,915,934,953,972,991

3,20,37,54,71,88,105,122,139,156,173,190,207,224,241,258,275,292,309,326,343,360,377,394,411,428,445,462,479,496,513,530,547,564,581,598,615,632,***649***,666,683,700,717,734,751,768,785,802,819,836,853,870,887,904,921,938,955,972,989

3,***22***,41,60,79,98,117,136,155,174,193,212,231,250,269,288,307,326,345,364,383,402,421,440,459,478,497,516,535,554,573,592,611,630,***649***,668,687,706,725,744,763,782,801,820,839,858,877,896,915,934,953,972,991

Устойчивостта на системата за споделяне на информация основана на Китайската теорема за остатъците се определя от произведението на ключовите числа M=a1*a2*…*ак, които не са известни на хакера и от средствата с които той разполага. Ако например $M>10^{50}$, а хакерът може да извърши не повече от 10^{20} проби за една секунда, ще са му необходими повече от $10^{50}/10^{20}=10^{30}$ секунди, за да успее да разбие системата. Всъщност достатъчно е това съотношение да надхвърля 10^9, тъй като в една година има $3.15*10^7$ секунди и за разбиване на системата ще са необходими над 30 години.

5 глава. Проектиране и реализация на система за разпределение на тайната, основана на Китайската теорема за остатъците

Целта на реализираната система за разпределение на тайната, основана на китайската теорема за остатъците, е да осигури контролиран достъп до файлове с конфиденциален характер в средна по размер бизнес организация. Чрез проектирането на два модула, web базиран и приложение работещо под операционна система Windows, се осигуряват следните възможности:

- Качване и криптиране на файлове на сървъра
- Контрол на достъп до файловете и тяхното сваляне
- Административни операции (промяна на лични данни, пароли и др.)
- Преглед на съдържанието на файловете (име и кратко описание)

Функционалността на разработената система трябва да бъде следната:

- Да се осигури различно ниво на достъп до файловете в системата
- Да се осигурят различни ключове в зависимост от нивото на достъп до конкретен файл
- Всеки потребител да получи свой набор от ключове, получени чрез използване на китайската теорема за остатъците
- Гарантиране на минимален брой потребители на линия за декриптиране на даден файл

Системата е разделена на два основни модула :

- WEB Crypt Приложение работещо на сървър под Linux
- Win Crypt Приложение работещо при клиента

5.1. Архитектура на реализираната система

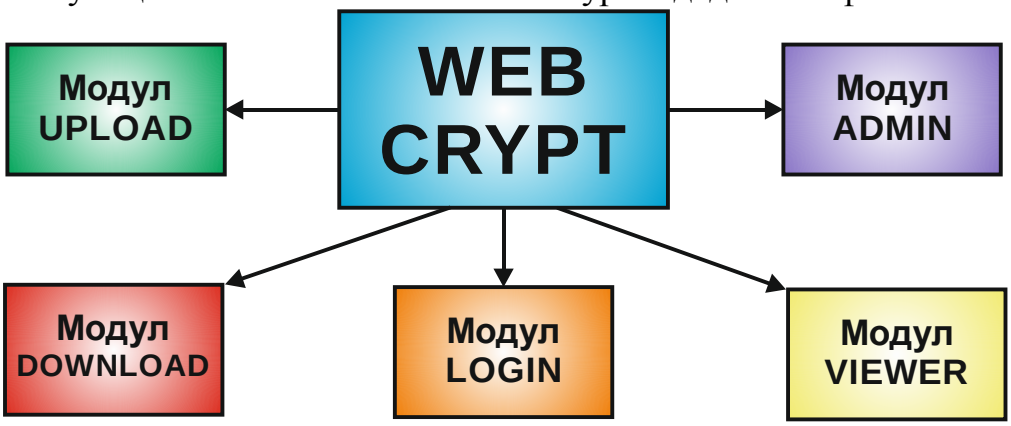
В практиката на софтуерното инженерство са се наложили множество шаблони за софтуерни архитектури, които са подходящо решение за определен клас проблеми/нужди. Всеки от тези шаблони има както предимства, така и недостатъци, и при проектирането на софтуерен продукт трябва да се прецени кой шаблон е най-подходящ за конкретния случай.

Системата за разпределение на тайната, основана на китайската теорема за остатъците е изградена с архитектура Клиент-Сървър. Това е разпределена архитектура, при която системата е разделена на един или повече сървъри и множество клиенти. Сървърът предоставя услугите на клиентите, чрез приложението WEB Crypt. Клиентите инициират връзката със сървъра използвайки приложението Windows Crypt.

5.2. Функционални схеми

Функционалната схема на Web Crypt

Функционалната схема на Web Crypt е дадена на фиг. 7



Фиг. 7 Функционална схема на WebCrypt

Първия модул WEB Crypt е WEB базиран и за използването му е необходимо единствено WEB браузър и IP свързаност със сървъра на който е инсталиран.

- Модул Login

Основната роля на този модул е авторизация на потребителя. По този начин се възпрепятства случайния достъп до системата. За по-голяма надежност на защитата на данните въведени от потребителя паролата се изпраща към сървъра в неявен вид (хеширана) чрез 128 битов MD5 алгоритъм.

- Модул Upload

След успешната авторизация, избираме файл от локалния компютър чрез браузъра. Модула се грижи за неговото физическо

качване на сървъра, както и за записването на информацията за файла в базата данни, определянето от потребителя на нивото на достъп и самото криптиране на файла.

- Модул Viewer

Този модул дава възможност на потребителя да прегледа каталога с всички файлове, които са качени на сървъра. Потребителя има достъп до информацията за файловете (тяхното описание, име, собственик на файла и др.)

- Модул Admin

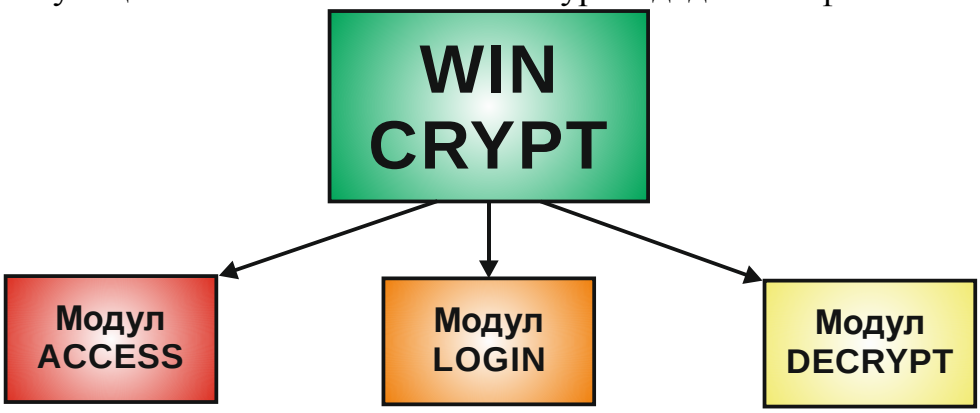
За по-голяма гъвкавост е добавена възможност за промяна на парола при забравяне на същата от страна на потребителя. Това няма да доведе до промяна на ключа с който са криптирани файловете.

- Модул Download

Този модул осигурява записа на избрания от потребителя файл, на собствения му компютър. Файла е в криптирано състояние и той е абсолютно безполезен без да бъде декриптиран с приложението Win Crypt.

Функционалната схема на Win Crypt

Функционалната схема на Win Crypt е дадена на фиг. 8.



Фиг. 8 Функционална схема на Win Crypt

Втория клиентски модул Windows Crypt е приложение, написано на езика Borland Delphi 7. Приложението работи под операционната система MS Windows XP, както и Windows Vista, Windows 7 и Windows 8.

Приложението няма нужда от предварителна инсталация и може да бъде използвано и от външен носител – USB Flash памет, CD или друг

- Модул Login

Основната роля на този модул е авторизация на потребителя и регистрацията му в базата данни. Чрез модула се следи за

минималния брой активни потребители, нужни за декриптирането на файл

- Модул ACCESS

Модула е предназначен за следене на минималния брой активни потребители, получаването на двойките числа от другите потребители, както и изчисляването на декриптиращия ключ, който ще се използва от модула Decrypt. Следенето за нужния минимален брой потребители, според изискванията за степен на сигурност на файла, е основата на приложението на китайската теорема за остатъците.

- Модул Decrypt

След обработка на ключовете от модула ACCESS, този модул получава готов ключ за декриптирането на файла. Тук се извършва същинското декриптиране и запис на готовия файл .

5.3.Тестване

Тестването е най-известният метод, чрез който се осигурява качеството на софтуерните продукти. Тестването на една софтуерна система означава откриване на несъответствия между реалното и очакваното поведение. Един начин за подобряване на тестването е използването на модели, които описват очакваното поведение според изискванията на системата. Процеса на тестване чрез модели е познат като “тестване базирано на модели”. Той обикновено се отнася до генериране на тестови случаи и оценка на резултатите въз основа на модел на поведение на системата.

Резултати от тестовете

Поради спецификата на приложението всички тестове бяха извършени ръчно.

Бяха качени 150 файла, които бяха криптирани с 4 различни нива на дъстъп.

Ниво 1 – Необходими са трима потребители за декриптиране

Ниво 2 – Необходими са четирима потребители

Ниво 3 – Необходими са пет потребители

Ниво 4 – Необходими са 7 потребители

Бяха създадени 10 потребителски акаунта. Тестовете се проведоха от 4 програмисти и 2 доброволци без компютърно образование.

Тестване на сигурността – При произволно избрани пароли, някои от тях бяка декриптирани чрез MD5 масив. Това се случи поради избора на много къси пароли като например 123, password и

др. При пароли с минимална дължина от 6 символа и задължително наличие на голяма буква и цифра, никой от програмистите не успя да прихване и разкодира MD5 паролата за вход в системата. При опитите за достъп чрез кеша на браузъра не постигнаха успех.

Издръжливост

Системата беше подложена на стрес тестове по следния начин:

- Подаване на грешен файл за декриптиране – системата връщаше отговор че не може да декриптира файла, но оставаше напълно функционална.
- Подаване на грешни данни към сървърното приложение – приложението връщаше данни към приложението работещо под windows, в които беше указана грешката. И двете приложения останаха напълно функционални.
- Тестване за SQL Injection – неуспешни опити за SQL Injection

Производителност

Файл с размер 4 Mb беше свален 100 пъти, като средното време за сваляне беше 2,21 sec.

Същия файл беше декриптиран, като времената варираха според бързината на компютрите, между 0,2 s и 0,9 sec.

Съвместимост

Системата е изтествана и работи на всички видове браузъри IE 6, 7, 8, 9, 10, 11. Chrome и FireFox.

Приложението WinCrypt работи под Windows XP, Vista, 7 и 8.1 .

Финален тест

Този тест беше проведен по метода Black Box. Всички резултати са положителни и няма проблеми при използването на програмния продукт.

АСПЕКТИ НА БЪДЕЩИ РАЗРАБОТКИ, ПРОИЗТИЧАЩИ ОТ ДИСЕРТАЦИОННИЯ ТРУД

Получените резултати стимулират за по-нататъшно развитие на изследването на криптографските методи за защита на информацията. Ето някои аспекти в тази посока:

- Добавяне на паралелно изпълняващи се конструкции в създаденото програмно приложение,с цел ускоряване на изчислителния процес;
- Създаване на модел и реализация на алгоритми, основани на квантовата криптография;
- Използване на получените резултати в учебния процес на студентите от образователна степен „магистър”.

ПРИНОСИ НА ДИСЕРТАЦИОННИЯ ТРУД

Научни приноси:

1. Проектирана и реализирана е система за разпределение на тайната на базата на Китайската теорема за остатъците

2. Предложена е модификация на метод за разпределена защита на информацията, като е реализиран алгоритъм за намиране на решение

Научно-приложни приноси:

3. Разработени са програмни модули за провеждане на изследвания, с цел установяване възможностите на предлаганото развитие на методите за разпределена защита на информацията.

Приложни:

4. Изследвани са възможностите за нарушаване достоверността на информацията, и е направен тематичен анализ на начините и средствата за защита на данните.

5. Анализирани са възможностите на вече съществуващи решения за разпределена защита на информацията по различни критерии с тематична насоченост.

6. Представено е изследване на възможностите на квантовите компютри и основните квантови алгоритми ,като най-преспективни възможности за бъдещо развитие на методите за криптиране и

ИЗПОЛЗВАНА ЛИТЕРАТУРА (ИЗВАДКА)

69. Everitt H. (ed.) Experimental aspects of quantum computing Springer, 2005.

74. Lieven M. K. Vandersypen, NMR quantum computing: Realizing Shor's algorithm, 2007.

90. David P. DiVincenzo, Patrick Hayden, Barbara M. Terhal, Hiding Quantum Data, Found. Phys. 33(11):1629-1647, 2003

109. Grover L.K.: From Schrodinger's equation to quantum search algorithm, American Journal of Physics, 69(7): 769-777, 2001.

123. R. Ahlswede and I. Csiszar, Common randomness in information theory and cryptography I: secret sharing, IEEE Transactions on Information Theory 39 , 1121-1132,1993

126. A. Beimel and B. Chor, Secret sharing with public reconstruction, in "Advances in Cryptology -- CRYPTO '95", D. Coppersmith, ed., Lecture Notes in Computer Science 963 , 353-366,1995.

135. G. R. Blakley, Safeguarding cryptographic keys, in "Proceedings of the National Computer Conference, 1979", American Federation of Information Processing Societies Proceedings 48 , 313-317,1979.

163. Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. Introduction to Algorithms, Second Edition. MIT Press and McGraw-Hill. ISBN 0-262-03293-7. Section 31.5: The Chinese remainder theorem, pp.873–876,2001.

165. Yao, Andrew C. Protocols for secure computations, 23rd Annual Symposium on Foundations of Computer Science ,pp. 160–164,1982.

166. Chor, B., S. Goldwasser, S. Micali, and B. Awerbuch, Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults, FOCS 1985, pp. 383-395, 1985.

168. A. Shamir, How to share a secret, Communications of the ACM 22, 612-613,1979.

175. David Deutsch and Richard Jozsa , "Rapid solutions of problems by quantum computation", Proceedings of the Royal Society of London A 439: 553,1992.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. O. Nakov, D. Gotseva, **B. Zyulyamova**, Protected Distant Voting With Paper Ballots, Journal of Computer & Communication Engineering, ISSN 1314-2291, за печат.

2. O. Nakov, D. Gotseva, **B. Zyulyamova**, Performance of RSA Algorithm Using Chinese Reminder Theorem, Journal of Computer & Communication Engineering, ISSN 1314-2291, за печат.

3. **Б.Зюлямова**, Повишаване на надеждността на субституционната криптографска защита чрез използване на съставни ключове на две нива , Международна научна конференция "УНИТЕХ'04"-Габрово ,I-295-I-298 , 2004.

4. **Б.Зюлямова** , Б.Александров, Ключово управляема транспозиция в блоковите криптографски шифри ,Международна научна конференция "УНИТЕХ'05"-Габрово ,III-382-III-385 , 2005.

5. **B.Zyulyamova**, O.Nakov, A.Tasheva, Secret sharing scheme using the Chinese reminder theorem, Challenges in Higher Education & Research, vol.10, 145-147, 2012.

METHODS OF ALLOCATION OF SECRECY IN CONTEMPORARY CRYPTOGRAPHY

ANOTATION

The aim of the thesis is to create methods of allocation of secrecy in contemporary cryptography. To achieve this objective the following tasks have been formulated:

- Research of the options for breaking reliability of the information and review the ways and types of data protection.
- Research of existing solutions for distributed data protection, in terms of data security and protection from unauthorized access
- Improvements in existing methods of distributed data protection to increase security in case of break-in into the system.
- Developing software solutions, implementing the proposed improvements in the methods of distributed data protection

Overview of the possibilities that could lead to improper modification of data is included in this thesis.

It's well founded the necessity of improving the security of information resources, for which responsibility is divided between a numbers of different actors.

It's described the different approaches in mathematical whit which are realized distributed data protection.

It's presented a quantum computer. It's discussed quantum algorithms that will be used for sharing information as the most perspective direction for future developments.

A new method for distributed data protection on the basis of the Chinese remainder theorem is proposed at last. It's designed and implemented a secret sharing system based on Chinese remainder theorem.