С.Сейфуллин атындағы Қазақ агротехникалық университетінің 60 жылдығына арналған «**Сейфуллин оқулары– 13: дәстүрлерді сақтай отырып, болашақты құру**» атты Республикалық ғылыми-теориялық конференциясының **материалдары** = **Материалы** Республиканской научно-теоретической конференции **«Сейфуллинские чтения – 13: сохраняя традиции, создавая будущее»**, посвященная 60-летию Казахского агротехнического университета имени С.Сейфуллина. - **2017. - Т.I, Ч.5.** - С.216-219

БАЙЛАНЫС ЖЕЛІСІ АРҚЫЛЫ БЕРУ ҮШІН ДЫБЫСТЫ ШИФРЛАУДЫҢ ЖАЛПЫ МӘСЕЛЕЛЕРІ

Алымова Б., Найманбаев С.

*Мақаланың мақсаты*байланыс желісі арқылы беру үшін дыбысты шифрлаудың жалпы мәселелерін қарастыру. Соңғы кезде дауысты компьютерлік желі арқылы беру және қабылдауды қамтамасыз ететін бағдарламалар көбейді. Бірақ, олардың ішінде желідегі дыбысты шифрлау ескерілгені өте аз. Бұл кез-келген бағдарламаны қолдану аясын тарылтады, себебі, олар заңсыз немесе құпиялықты сақтау қарастырылмаған.

Қазіргі кезде, дыбысты беру (нүктені нүктеге) деген қағидамен жүзеге асады, яғни, компьютерден компьютерге тораптар бойынша бір бағытта байланыс арқылы. Дауыспен хабарласуды құпиялығын мейлінше сақтап, шифрлау және желі арқылы дыбысты берудің жылдамдығын кешіктірмей талап етілген шашаңдықты қамтамасыз ету қойылған мақсаттың негізгі критериі болып табылады.

Желінің бір ұшында бағдарлама-клиент орнатылып, ол дыбысты ұстауға және оны шифрлауға жауап береді, ал екінші ұшында бағдарлама-сервер, ол өз кезегінде, дыбыс ағынын кері шифрлап, оны дауыстау қондырғысына шығарады. Шифрлау үшін дыбысты ұстау бірінші клиенттің дауысты микрофон арқылы ендіру барысында DirectX [1] бағдарламасы бойынша жүзеге асады. Айта кететін жағдай, осы интерфейс дыбыс картасының қондырғысымен икемді жұмыс істеуді қамтамасыз етеді.

Шифрлау блогының негізіне уақыттық және спектрлік скремблердің комбинациясы жатады. Спектрді алу үшін Фурьенің уақыт бойынша бөліктейтін дискреттік түрлендіруі қолданылады. Негізінде дыбыс – мейлінше тегіс функция, әйтпесе, сигналдардың кішкене бөліктерінің алмастырулары қарсылардың шабуылына (ортадан шабуыл) беріктілік жасай алмай қалуы мүмкін. Байланыс желісіне еніп алған қарсылас әртүрлі уақытта амплитуданың мәндерін талдап, ауқымды ауытқулардың статистикасын жүргізіп, оны өзінің құйтұрқы мақсатына пайдалануы мүмкін. Сондықтан, жеткілікті крипто қорғауды әрі уақыт және жиілік ауқымын түрлендіруді төпей қолдану іске асырады.Оның алгоритмі тек аз уақыт арасында дыбыс ақпаратын құпия беруге қолданылады. Шифр кілтін желімен берудің мағынасы жоқ, сондықтан оны генерациялау үшін, алдыңғы берілген дыбыстар ағыны мен сеанстық кілттерді саралау әдістемесімен жүзеге асады. Және ол кілттерді алмасу үшін белгілі Диффи-Хеллман алгоритмін

қолданған тиімді. Ескеретін жағдай, оны қолдану үшін желі модификациялаудан жеткілікті қорғалған болуы қажет.

Қойылған есепті ары қарай шешу жолдары байланыс желісінің толық дуплексті болып дыбыс ақпаратын қысу әдістемесіне байланысты болады [2]. Сонымен қатар, сеанстық кілттердің алмасуын мейліше қорғалған әдістемелерін ендіру арқылы жүзеге асады [3].

Дыбыстық сигналдардың негіздері. Мысалы сандық мәліметтер арқылыдыбысты алу үшін: А –гравитациялық жиіліктің эталоны (10^{18}Гц);В – атмосфералық тактілік жиілік (10^{16}Гц);С – негізгі атмосфералық тактілік жиілік(10^{15}Гц);D – адам миының тактілік жиілігі (10^{12}Гц);

– негізгі адам миының тактілік жиілігі (7.2 – 22110 Гц). Мұнда тек Е-диапазоны ғана кодталады, бірақ, кез-келген дыбыстық ақпарат С – диапазонында сақталады.Егерде, D –диапазонында дыбысты шамалы өзгертсек, онда,негізгі адам миының тактілік жиілігі өзгеріп, құлақтың естуі толығымен жоғалады немесе өзге дыбыстар шуы естіледі. Дыбысты желі арқылы берілгенде бұзылып өзгергесе, оны техникалық құрылғы арқылы қалпына келтіруге болады және ол тек, Е-диапазонына қатысты.С– диапазонындағы дыбыстар шифрлауға келмейді. Дыбысты шифрлау үшін алдымен оның қалай қалыптасуының негізін білу керек. Яғни спектр мен сигналды кодтау және спектрлік талдауға көңіл аудару қажет. Мәселен, кез-келген спектрді алу үшін эталондық (базалық) жиілік болуы қажет. Эталондық (базалық) жиілік диапазоны 10^{16}гц. Бұл диапазонда екі базалық диапазондық жиілік бар.

Дыбысты шифрлау ерекшеліктері. Дыбысты шифрлаған мен кез-келген ақпаратты шифрлау арасында аса үлкен айырмашылық жоқ, тек, келесі жағдайлар болмаса:

1. Байланыс желісінде кедергі болса, яғни бұзылған жерден ары қарай барлық тізбекке кері әсер етсе. Онда, қатені түзетуге немесе бұзылған блоктан арылтатын арнайы протокол ендіру. Мәселен, шифраторды (10-100 мс) уақыт аралығында қалпына келтіру.

2. Қабылдаушы және беруші екі желісі бар және уақыт бойынша қатал талап қойылған. Мәселен, шифратор 4096 биттік кодері болса дешифратор дер кезінде кері шифрлауға үлгермейді.

Есептің қойылуы. Байланыс желісінің екі шетінде сөйлесіп отырған абоненттер бар. Байланыс желісін абоненттер бақылай алмайды және осы қиындықты ескере отырып, кодтау арқылы ақпараттың құпиялығын сақтау.

Шешімге қойылатын талаптар:

1. Байланысты орнату жәнебайланысты құпиялық күйге келтіру ешқандай арнайы қиындықсыз болуы.

2. Шифрлау алгоритмі жіберілетін қателіктерге орнықты болуы қажет.

3. Шифрлау оны қолданытындарға қосымша шектеулер қоймауы керек.

Шешу жолдары. Есепті шешу барысында әртүрлі байланыс желілірі қолданылуы мүмкін (аналогтық және цифрлы-анологтық) .

Ақпараттар ағынының түріне қарай әртүрлі шифрлау әдістері қолданылады (мысалы, цифрлы ағындық ақпаратқа кез-келген шифрлау әдісін қолдануға болады, атап айтсақ Цезар шифры).

*Аналогтық ақпарат ағынын шифрлау жолдары.*Аналогтық ақпарат ағынына тіптен бөлек әдістеме қолданылады:

1. Дыбысқа қорғайтын шум қабаттастыру.

2. Уақыт арқылы түрлендіру (кесінді аралықты аралыстыру және уақытша инверсия жасау) .

3. Жиілік арқылы түрлендіру (спектр инверсиясы және спектр жолақтарын алмастыру).

Аналогтық ақпарат ағынын шифрлау ерекшеліктері. Дыбысты құпиялап шифрлағанда шуды қолдану. Қолданылатын шу кездейсоқ болуы қажет (негізінде, шуды туындататын мүмкіндіктер псевдо-кездейсоқ шулар арқылы іске асады және олар жеңіл түпнұсқадан бөлектенеді). Басқа әдістемелерді қолданғанда, дыбыстың қалдық бөлігінің қасиеті арқылы өте қуатты есептеу кешенінің көмегімен түпнұсқадағы дыбысты қалпына келтіруге болады. Өкінішке орай, шифрлауға шудың ағын қолдансақта, оны қабылдаушыға жіберуге тура келеді ол оны шудан тазалай алады, мұны зиянкесте жасай алады, яғни бұл әдістеменің әлсіз тұсы.

Жиілік арқылы түрлендірудің мәні дыбыс спектрін белгілі бір заңдылық бойынша өзара бір мәнді түрлендіру. Мәселен, вертикальды түзуге салыстырғанда симметриялы бейнелеу. Ескеретін жағдай, ақпаратты бұлай бейнелегенде, шифрланған мәтін адам құлағын тікелей қабылданады, ешқандай қосымша құрылғыларсыз. Бұл түрдегі қорғанысты қолданғанда екі шаманың маңыздылығы бар: қорғаныстың беріктілігі және түпнұсқадағы дыбыстың қалпына келуі. Өкінішке орай, қорғаныс күшті болған сайын, дыбысты түпнұсқаға келтіру қиындау болады [4].

Уақыт арқылы түрлендіру (скремблирлеу) Бұл әдістемені қолданғанда дыбыстың кейбір бөлігін сақтайтын блок (онда, кесінділер араластырылады) . Осыдан туындайтыны, дыбысты беру мен қабылдау уақыты кешігу мүмкін. Ескеретін жағдай, дыбыстауды шифрлауға қолданылатын уақыт бөліктерінің мейлінше кішкентай болуы, криптоқорғаныстың сенімдлігін күшейтеді. Шифрлау барысында блоктардың араласуы болғандықтан, сол түпнұсқадағы блоктарды кері қалпына келтіру барысында, бұзылу үдерісі орын алады. Егер, бөліктер мейлінше кішкентай болса, қорытынды, алынған ақпарат ағыны түсініксіз болып шығады.

Жалпы қорғанысты ұтымды күшейту үшін, аталған екі әдістемені біріктіре қолданған дұрыс.Әлбетте, жақсы нәтиженің өтемі дыбысты шифрлау құны қымбаттайды.

Цифрлық желіде дыбысты шифрлау жолдары. Айта кететін тағы бір әдістеме, аналогтық сигналды цифрлы сигналға түрлендіре отырып, соңында шифрлау жүзеге асырылады. Аналогтық ақпарат ағынын цифрлы сигналға түрлендірген соң, кез-келген шифрлық дістемелерді қолдануға болады. ифрлау барысында есептеу құралдарының қуаты нақты уақыт күйінде толық жетуі қажет және жасалған шифр мейлінше берік болғаны дұрыс.

Дыбысты мұндай шифрлауға американдық шифрлау стандартын (DES және AES) қолдануға болады. Сонымен қатар, ГОСТ 28147-89 қолдануға болады, ол 1989 жылы жасалсада әлі күнге жеткілікті беріктілікті бар.

*Қорытынды.*Мақаладажелімен дыбысты беру мен қабылдаудың құпиялығын мейлінше сақтап, шифрлау және желі арқылы дыбысты берудің жылдамдығын кешіктірмей талап етілген шашаңдықты қамтамасыз ету қарастырылған. Шифрлау үшін желіге клиенттің дауысының микрофон арқылы ендіру барысында DirectX бағдарламасын қолданған дұрыс. Дыбысты желіден беру барысында шифрлау негізінен уақыттық және спектрлік скремблердің комбинациясы арқылы іске асады. Шифрлауға қолданылатын спектрді алу Фурьенің дискреттік түрлендіруімен іске асады. Крипто қорғаудың нәтижелігі әрі уақыт және жиілік ауқымын түрлендіруді төпей (каскадты) әдістемені қолдануға байланысты. Сеанстық кілттерді алмасу үшін Диффи-Хеллман алгоритмін қолданады және желі жеткілікті қорғалған ескереміз. Көтерілген тақырыптың ары қарай зерттелу бағытының бірі ретінде, байланыс желісінің толық дуплексті болып дыбыс ақпаратын қысу әдістемесіне байланысты болатынын ескертеміз.

Әдебиеттер

1. Секунов Н.Ю. Обработка звука на PC. – СПб.: БХВ-Петербург, 2001.
2. International Telecommunication Union, “List of the ITU-T Recommendations related to the Multimedia Framework Study Areas of the Mediacom 2004 Project”. – Geneva, 12-15 March 2002, http://www.itu.int/ITU-T/worksem/ipcablecom/tlist-mediacom.html.
3. Ивонин М. В. Криптографические протоколы распределения ключей для групп с динамическим составом участников. http://kiev-security.org.ua/b/194.shtml.
4. Micciancio, DanieleОтредактировано: Gilbert, HКонференция: 29th Annual International Conference on Theory and Applications of Cryptographic TechniquesМестоположение: FRANCE публ.: MAY 30-JUN 03, 2010 Спонсоры: IntAssocCryptol Res

ADVANCES IN CRYPTOLOGY - EUROCRYPT 2010 Сериякниг: Lecture Notes in Computer Science Том:6110 Стр.: 362-380 Опубликовано: 2010