4.2. Шифр негізінде электрондық қолтаңба Эль-Гамала

Алдыңғы бөлімде электрондық қолтаңба схемасы сипатталған, қажетті қасиеттері шешімнің күрделілігімен анықталады санды көбейту есептері. Бұл бөлімде біз сипаттаймыз дискретті логарифмдеу тапсырмасына негізделген қолтаңба нұсқасы.

Жоғарыда айтылғандай, Алиса құжаттарға қол қоймақшы.

Алиса үлкен жай санды таңдайды p және G саны, сондықтан әр түрлі дәрежелер g мәні p модулі бойынша әр түрлі сандар (бөлімді қараңыз. 2.2).

Бұл сандар ашық түрде беріледі немесе сақталады және болуы мүмкін

пайдаланушылардың бүкіл тобына ортақ. Алиса кездейсоқ x, $1 < X < p - 1$ нөмірін таңдайды, ол оны құпия ұстайды. Бұл оның

құпия кілт, оны тек ол біледі. Содан кейін ол санды есептейді

$$y = g^x \bmod p.$$

Бұл сан y Алиса өзінің ашық кілті ретінде жариялайды.

Үлкен p-де y-ді біле отырып, x-ті табу мүмкін емес екенін ескеріңіз (бұл дискретті логарифм тапсырмасы).

Енді Алиса хабарламаларға қол қоя алады. Ол m = m1. . . , mn хабарламасына қол қойғысы келеді делік. Қолтаңбаны құру үшін әрекеттер тізбегін сипаттайық.

Бастапқыда Алиса H = H(m) хэш функциясының мәнін есептейді, ол $1 < h < p$ теңсіздігін қанағаттандыруы керек.

кездейсоқ k санын таңдайды ($1 < k < p-1$), p−1-мен өзара қарапайым,

және санды есептейді

$$r = g^k \bmod p. \tag{4.5}$$

Әрі қарай Алиса сандарды есептейді

$$u = (h - xr) \bmod (p - 1), \tag{4.6}$$

$$s = k^{-1}u \bmod (p - 1). \tag{4.7}$$

K^{-1} астында (4.7) теңдеуді қанағаттандыратын санды білдіреді

$$k^{-1}k \bmod (p-1) = 1 .$$

(4.8)

Мұндай k^{-1} бар, өйткені k және p-1 өзара қарапайым және мүмкін Евклидтің жалпыланған алгоритмі бойынша табылуы керек. Соңында, Алиса қол қойылған хабарламаны қалыптастырады

$$(m ; r, s).$$

(4.9)

Қол қойылған хабарламаны алушы (4.9), ең алдымен, қайта H = H(m) хэш функциясының мәнін есептейді. Содан кейін ол тексереді теңдікті қолдана отырып қол қою

$$y^{r} r^{s} = g^{h} \bmod p.$$

(4.10)

Бекіту 4.3. Егер қолтаңба дұрыс болса, онда шарт (4.10) орындалады.

Дәлел . Шынында да,

$$y^{r} r^{s} = (g^{x})^{r} (g^{k})^{s} = g^{xr} g^{k(k^{-1}(h-xr))} = g^{xr} g^{h} g^{-xr} = g^{h} \bmod p.$$

(Мұнда бірінші теңдік (4.4) және (4.5), екіншісі (4.7).)

Бекіту 4.4. Сипатталған электрондық қолтаңба қол қоюға қойылатын барлық талаптарды қанағаттандырады.

Дәлел . Қолтаңбаның бірінші қасиетін тексерейік (ешкім қолтаңбаны қолдан жасай алмайды, басқаша айтқанда, басқа ешкімmАлиса хабарламаға оның қолымен қол қоя алмайды). Шынында да, (4.6) біз қолтаңбаны қалыптастыру кезінде Құпия Сан x. сонымен қатар , xr факторы қолданылады (4.6) қолтаңбаны қалыптастыру, хабарламадан хабарламаға өзгереді (k кездейсоқ таңдалғандықтан, r кездейсоқ таңдалады).

Сол себепті Алиса өзінен бас тарта алмайды қолтаңбалар, өйткені одан басқа ешкім x білмейді, яғни. екіншісі орындалады қолтаңба сипаты

Сондай-ақ, жанжал туындаған жағдайда Алиса мен Боб, олар шындықты анықтау үшін үшінші тұлғаларға жүгіне алады. Судья барлық есептеулерді тексере алады X, m және r сандарын көрсетіңіз .

Мысал 4.2. Кейбір пайдаланушылар қауымдастығы үшін Жалпы параметрлер p = 23, g = 5 болсын. Алиса өзінің құпиясын таңдайды x = 7 кілті және ашық y кілтін есептейді (4.4)

$$y = 5^7 \bmod 23 = 17$$

Алиса m = baaaab құжатын жасасын және оған қол қойғысы келеді. Алгоритм бойынша қолтаңбаны есептеуге көшейік. Ең алдымен ол хэш функциясын есептейді, оның мәні h(m) = 3 болсын. Содан кейін Алиса кездейсоқ k санын жасайды , мысалы, k = 5. Есептеу бойынша (4.5), (4.6) беремін

$$r = 5^5 \bmod 23 = 20,$$

$$u = (3 - 7 \cdot 20) \bmod 22 = 1$$

Әрі қарай Алиса $k^{-1} \bmod 22$ табады:

$$k^{-1} \bmod 22 = 5^{-1} \bmod 22 = 9.$$

(4.7) Бойынша есептеулер (4.7) береді

$$s = 9 \cdot 17 \bmod 22 = 21.$$

Соңында, Алиса қол қойылған хабарламаны (4.9) түрінде қалыптастырады:

$$(baaaab, 20, 21)$$

Қол қойылған хабарлама жіберіледі, Боб оны алады және тексереді қолтаңбаның түпнұсқалығын. Бастапқыда ол хэш функциясының мәнін есептейді

$$h(baaaab) = 3,$$

содан кейін сол жағын есептейді (4.10)

$$17^{20} \cdot 20^{21} \bmod 23 = 16 \cdot 15 \bmod 23 = 10$$

содан кейін оң жақ бөлігі (4.10)

$$5^{3} \bmod 23 = 10$$

Боб қолтаңба дұрыс деп тұжырымдайды.

Қарастырылған электрондық қолтаңба әдісі RSA-ға қарағанда күрделірек, оның беріктігі RSA-ға қарағанда екіншісіне негізделген, бір жақты функциялар. Бұл криптография үшін өте маңызды, өйткені бір әдіс беделін түсірген жағдайда екіншісін қолдануға болады. Сонымен қатар, қосулы Эль-Гамаль қолтаңбасының негізінде тиімді алгоритм құруға болады, онда есептеу уақыты "қысқа" көрсеткіштерді қолдану арқылы айтарлықтай қысқарады. Мұндай алгоритм келесі бөлімде берілген.