Bitcoin: Efutilo lyopaungoba komuntu nomuntu.

ku Satoshi Nakamoto 2008/10/31

Engongo

Efutilo lyoshimaliwa ndyono lya tungilwa melandulathano lyoocomputer tadhi kwathathana moku tuma omatumwalaka gopaungomba, otali kwathele opo shikale oshipu omafutilo ngaka gopaungomba ga tumwe guukilila okuza komuntu gumwe guuka kumukwawo pwaahena okupitila moombaanga nenge omahangano gwalwe nga haga longo noshimaliwa. Omashaino gopaungomba nago otagakutha ombinga mokukandulapo omukundu nguka, kakele omauwanawa ogendji otaga ka kana ngele omwiinekelwa omutitatu okwa pumbiwa mokukeelela omafutilo tagii yendulula. Nomolwaasho otatu unganeke ekandulopo lyomukundu gwomafutilo tagiiyendulula mokulongitha ekwatathano lyoocomputer tadhi kwathathana. O stambe yethimbo ndyono ekwatathano lyomafutilo ganingwa otali kwashilipaleke okugamena oshimaliwa nokulongitha omukalo tagu faathanithwa nelyenge lyiinima ayihe mbyono yinasha nomafutilo ngoka, ano shino otashiithwanwa elyenge lyuumbangi wiilonga tali kalekepo ondjokonona yaashono shaningwapo mefutilo ndyono, no itali vulu nande okulundululwa ngele elyenge lyuumbangi wiilonga ina li ningululwa. Uule welyenge lyiiningomwa ita li longithwa ashike mokuulika uumbangi waashihe shono sha nyangadhalwapo ihe ota wu ulike wo uumbangi kutya efutilo ndino olyaza mudhimwe dhomoo computer dhoonkondo elela. Shampa ashike odhindji dhomoo computer ndhino dhoonkondo elela tadhi longele kumwe neehuke ndhono itadhi kambadhala okulongela omakwathano ngono uuwinayi washa, onkene kumwe otadhi etapo elyenge ele ndjono ta li nkondopaleke okuundula ondjundo yaambono taya kambadhala okulonga uuwinayi. Omakwatathano gogene oga pumbwa omutungilo omushona elela. Omatumwalaka otaga tumwa mombepo noonkambadhala oombwanawa, noohuke otadhi vulu okuthigapo omwakwatathano ngaka, oshowo okugalukilamo ngele yewete shapumbiwa, ndee tadhi taamba uumbangi wiilonga mboka uule wuvule oonkwawo, mokuulika ashihe shono sha longwapo ethimbo ndyono ohuke yali ya gwamo mombepo nenge ya thigapo omakwatathano.

Efalomo

Omalandithilo gopaungomba monena ogii kolelela unene nolundji komahangano goombanga ndhono dhililepo ngaashi omwiinekelwa omutitatu oku kwashilipaleka eineekelo momafutilo agehe gopaungomba. Nonando omulandu ngono ohagu longo nawa momiyalu dhomalandithilo ogendji, moompito dhimwe ohapu ka kala natango omashongo taga etwapo molwa uunkundi womilandu ndhono dhiikolelela meineekelo. Osha pumba lela waadhe omafutilo ngono ihaaga vulu okushunithwa monima, osho nee oombaanga nomahangano omakwawo giimaliwa itaga vulu

okukeelela nokwii dhopa mo nokuhangukununa moontamanana odho tuu ndhika. Ondilo yoku hangukununa nayo woo ohayi fala pombanda ondilo yomafutilo, naashono ohashi ngambeke uushona womalandithilo gopevi noku tetapo ompito yomafutilo omashona mpaka naa mpeyaka. Opena woo ondilo onene tayi etwapo ngele otwa kanitha ompito yokushunitha monima omafutilo shinasha niilongomwa mbono nayo ihayi vulu okushunithwa monima. Ngele pena ompito yoku shunitha omafutilo monima, ompumbwe yeineekelo nayo otayi indjipala. Aalandithi oya pumbwa oku iyageka ngele tashiya kaalandi yawo, tayeshi ningi mokuya pula pula iishiwomwa naambyo inaaya pumbwa pethimbo ndyoka. Oshipambu shimwe shomakengelelo osha taambwako onga itaashivulu okukeelelwa. Okwaaha tseya Konawa ngele tashiya kondilo, nomafutilo ohaga vulu okukeelelwa nuupu ngele tashiya kiimaliwa iikukutu, ashike kapena natango oonkambadhala dhokuninga omafutilo giikolelela muungomba pwaana omwiinekelwa omutitatu.

Shika oshapumbiwa omafutilo guunganekwa paungomba nowii kolelela muumbangi wethano lyopaungomba ndele hamei nekelo, opo kehe oombinga mbali dhahala oku tutathana ya vule oku shi ninga inaa pumbwa omwiinekelwa omutitatu. Omafutilo ngoka itaga vulu nande okushunithwa monima paungomba, molwaashoka otaga gamene aalandi komakengelelo, nomwaalu gwagwedhwapo otaguvulu okulongithwa mokugamena aalandi. Momushangwa nguka otandi etapo edhilaadhilo lyoku kandulapo omafutilo tagiiyendulula tatu longitha oo computer thadhi kwathathana moku andjakaneka ostambe yethimbo, ndjono tayi etapo uumbangi wopaungomba shiikolelela komafutilo ngono ganingwapo nogeli melandulathano. Eunganeko lyomafutilo ngano oga gamenwa, shampa ashike oohuke adhihe dhopaushili tadhi longele kumwe moku unganeka oocomputer dhoonkondo tadhi longele kumwe oshivulithe dhimwepo dhomoo huke dhililepo okulonga omauwinayi.

Uufutilo

Okoina yopaungomba ohatu yi fatulula onga eshaino-lyenge lyopaungomba. Mwene gwo koina kehe oteyi tumu komuntu omukwawo tashaina paungomba okapambu kefutilo ndyono lya ningwa nale nishapi yeegulukila kehe gumwe oyo tayi longithwa kwaangu ta tuminwa okoina, nomushangwa nguno otagu ka gwedhwa nee kehulilo lyomushangwa gwo koina. Nakufutwa ota vulu oku kwashilipaleka eshaino, opo a koleke elyenge lya mwene wokoina.

Kakele uupyakadhi owuli owala mpano kutya nakufutwa ita vulu oku kwashilipaleka kutya mwaambono ya li ooyene yokoina manga inaayi thika kuye inaye yi futilwa lwaali. Onkambadhala tayi vulu okuningwa po opo omukundu nguno gukandulwepo oku eta po oukalelipo omupokati omwiinekelwa, ngono takala noku peka peka momafutilo agehe opo a kwashilipaleke kutya kapuna omafutilo go paali ga ningwa po. Konoima yefutilo kehe lya ningwa po, okoina oya pumbwa oku shunithwa komukalelipo omupokati opo a gandje okoina ompe, nookoina ndhono dhagandjwa okuziilila komukalelipo nguka omupokati odho ashike tadhi vulu okwiinekelwa nando inadhi futwa dhiilandula. Uupyakadhi nee wekandulopo lyomukundu nguka oombuno kutya onkalo ayihe yeunganeko lyoshimaliwa shono, otayi kala yiikolelela mehangano ndyono tali ungaunga

nomukalelipo omupokati, nuufutilo auhe owa tegelelwa gapitile muyo, ongaashi naana ombaanga.

Otwa pumbwa onkambadhala yimwe opo tuvule okukwashilipaleka kutya mbono yali ooyene yokoina methimbo lyakapita inaya Shaina uufutilo uukwawo wapiti. Melalakano lyetu omafutilo ngono ganingwa tango ogo ashike taga landulwa, onkene itatu ipyakidhile nomafutilo ngono giiyendulula ngono taga elekelwa methimbo ndyono tuuka. Omukalo aguke ngono tagu vulu oku kwashilipaleka kutya kapena efutilo ogo ngono goku tseya omafutilo agehe. Momukalo gomwiinekelwa gopokati, omwiinekelwa nguno omupokati aluhe okushi omafutilo agehe ngoka ganingwapo, noha ningi omatokolo kutya efutilo lyini po lya thiki po tango. Shino otashi pondolwa pwaahena omu inekelwa nguno omutitatu ngele omafutilo agehe otaga shiwithwa mombepo yeeguluka, notwapumbwa eunganeko lyaakuthimbinga opo yatse kumwe monakuziwa yimwe yelandulathano lyomafutilo ngaashi naana gi ilemo.

Ostambe yethimbo

Ekandulopo lyomukundu ndyono twa hala oku etapo ota li tameke nostambe yethimbo. Ostambe ndjino yethimbo otayi longo moku longitha okamangwa kiimbungu wiiningomwa mbyono yapumbwa oku stambwa nethimbo ndyono ye yamo noku andjakaneka okamangwa oko tuu hoka, ngaashi moshifo nkundana nenge metumwalaka lyopaungomba. Ostambe yethimbo otayi kwashilipaleke kutya iishiomwa mbino oyi na oku kala yamonika pethimbo olyo tuu ndjoka, nkene yavulu okuyalulwa mokamangwa noku etapo elyenge, tayi longitha kehe ostambe yethimbo lyalandulako moku ngondopaleka mbyoka yeya tango.

Uumbangi wiilonga

Opo tu tule milonga ostambe yethimbo ndjono ya andjakanekwa koo computer tadhi kwathathana, otwa pumbwa oku longitha e unganeko lyuumbangi wiilonga ya faathana nokamaliwa-mpangwa ka totwa ku Adam Back[6], shivulithe oshifo nkundana nenge etumwalaka lyopaungomba. Uumbangi wiilonga otawu kwatelemo oku peka peka omwaalu ngoka gwa ndhindhilikwa nokampangwa ngashi mbyono yatseyika nawa SHA-256, endhindhiliko lyokampangwa ohali tameke noo nola, moonomola ndhono hadhi ithanwa ‘bits,’ iilonga yuupokati yapumbiwa moonomola dhoo nola odhapumbiwa , no tayi kwashilipalekwa moku tula milonga okampangwa kamwe akeke.

Mostambe yethimbo lyomakwathano getu, ohatu tula milonga uumbangi wiilonga mbyono hatu longo okugwedha konomola ndjono hayi longithwa ashike lumwe moka mpungu kehe sigo omwaalu ngono tagugandja oonola bits kokampangwa kokampungu. Shampa nee oonkambadhala dhoocomputer oonankondo dhapu mokugwanitha uumbangi wiilonga, okampungu hono itaka vulu we oku lundululwa ngele iilonga oyo nee mbyoka inayi longululwa, molwaashono methimbo tali landula uumpungu mbuno otawu ka tulwa kumwe melyenge, niilonga kehe tayi lundulula okampangwa otayi kwatelemo okulongulula uumpungu awuhe tawu ka landulako.

Uumbangi wiilonga nawo otawu kandulapo uupyakadhi woku kwashilipaleka uukalelipo mokuninga omatokolo ogendji. Ngele uuwindji owiikolelela mehogololo lyakehe ondjukithi yopainternet (IP Address), nena otayi vulu oku endwa pomunkulo kukehe gumwe ngono tavulu okugandja oondjukithi dhopainternet odhindji. Uumbangi wiilonga pampumbwe owiikolelela mehogololo lyakehe ocomputer onankondo yimwe. Opo nee omatokolo ogendji otaga kalelwapo kelyenge li ilile, ndjono lina uumbangi wiilonga wuna oonkambadhala oombwanawa dha tulwamo.

Opo tu futile po ondapo yiitopolwa yocomputer ndjono tayi yi pombanda ethimbo nethimbo, noku yoolola uuwanawa wokulongitha oowike ethimbo nethimbo, uudhigu wuumbangi wiilonga otawu hololwa keyelekanitho tali inyenge lyataalela oonomola dhiimpungu kehe mowili. Ngele otadhi longwa nondapo tayi endelele unene, uudhigu nawo otawu indjipala woo.

Ekwatathano

Omilandu dhoku tula milonga omakwatathano ongaashi tadhi landula:

1. Omafutilo omape otaga tumwa mewangadjo koowike adhihe.
2. Kehe owike otayi gongele omafutilo omape mokampungu .
3. kehe owike otayi longo noku adha uumbangi wiilonga mbyono iidhigu opo yilongithe mokampungu kayo.
4. Ngele owike oya adha uumbangi wiilonga , otayi andjakaneke nee koowike adhihe.
5. Oowike otadhi taamba uumpungu ngele omafutilo agehe gelimo oge li mondjila, no inaga futwa nale.
6. Oowike otadhi ulike etaamboko lyuumpungu, tadhi shi ningi noku etapo okampungu hono taka landulako melyenge ndika, tadhi shiningi nee nokulongitha okampangwa kokampungu hono ka taambwa, ongaashi hoka ka mangwa kethimbo lya ka pita.

Oowike aluhe ohadhi tula momadhilaadhilo elyenge ndyono ele olyo li lelepeka, ngele oohuke mbali odha andjakaneka mewangandjo oondondo dhuumpungu mbono tawu landulako dhayooloka pethimbo limwe, oohuke dhimwe otadhi kanwe nenge okakwawo tango, pompito ndjono taya longo nee naahoka ya taamba tango, ashike otaya siikilile woo okakwawo, ngele pamwe otaka ka ninga okale. Okwiihaka kwaamba ota ku tewapo nee ngele uumbangi wiilonga mboka tawu landulako owa adhika, no shitayi shimwe tashi ningi oshile : oohuke ndhono dhali tadhi longele koshitayi oshikwawo opo nee otadhi lundulukile koshitayi shika oshile.

Omafutilo omape ngono taga andjakanekwa inaga tegelelwa lela gakale gathika koohuke adhihe, shampa ashike tadhi vulu okwaadha oohuke odhindji otadhi vulu oku adha uumpungu owundji. Eandjakaneko lyuumpungu nalyo olyi na etseyo lyomatumwalaka ngono haga vulu kugwamo mombepo. Ngele ohuke inayi taamba okampungu kalandulako noya mona kutya opena kamwe kakanapo.

Uuwanawa wa gwedhwapo

Efutilo lyotango mokampungu olyo efutilo lya Shewa ndyono tali tameke okoina ompe, namwene gwayo ota kala omutotipo gwoshimpungu. Shino ohashi gwedha uuwanawa koohuke ndhono tadhi kwathele mekwatathano, noku gandja omukalo goku andjakaneka ookoina mongonga ye andjakaneko, omolwaashi kapena omupangeli gwokudhigandja.

Uuwanawa otawu vulu woo okuyambidhidhwa niishoshela yomafutilo. Ngele omwaalu ngono taguzi mefutilo omushona komwaalu ngono gwatulwamo, eyooloko ota li kala iishoshela yomafutilo mbyono yagwedhwa komwaalu guuwanawa woshimpungu shono shina efutilo olyo tuu ndjoka.Shampa nee omwaalu gwangambekwa gwa thiki peekoina ndhono dhili mongonga andjakaneko, nuuwanawa wagwedhwapo otawu vulu nee oku lunduluka, okuza kiishoshela yefutilo noku kala yaana nande egwedhelo lyasha.

Mostambe yethimbo lyomakwathano getu, ohatu tulapo uumbangi wiilonga moku gwedhapo kashona nakashona uutungipo wo miimpungu kiimpungu mbyoka, sigo omwaalu tagu adhika ngono tagu gandja o hash yoo nola mbono yapumbiwa. Shampa nee oonkambadhala dhocomputer onankondo dha longithwa oku gwanithapo shono sha pumbiwa muumbangi wiilonga, okampungu hono ita ka vulu we oku lundululwa ngele iilonga inayi longululwa, molwaashono konima yethimbo iimpungu mbino otayi ka kwatelwa kumwe , ta yi landulathana , niilonga yoku lundulula oshimpungu otayi kwatelemo oku longulula iimpungu ayihe tayi landulako.

Oku galulula ehala lyomasiikililo gopaungomba

Shampa nee omafutilo omapeepeka ga siikiliwa kohi yiimpungu yagwanaa, omafutilo ngono ga longithwa nale komeho gomafutilo ngano omape otagavulu nee oku ekelwahi, opo ga ninge ehala olindji momasiikililo ngano gopaungomba. Opo nee shininge oshipu nopwaana ku teyapo oka hash koshimpungu, omafutilo ogatulwa uu hash momukala ngaashi naana ngono gomuti gwofamili, [7][2][5], mono omudhi ogo owala gwa kwatelwamo moka hash koshimpungu. Iimpungu iikulu otayi pakelwa mumwe, naashino otashiningwa nee moku teyako iitayi yimwe yomuti ogo tuu ngoka, shaa heshi oshiningila wina. Uu hash womeni inashi pumbiwa lela wukale wa pungulwa.

Oshimpungu-palanyolo shaana mafutilo otashi tengekelwa okukala poo bytes dhili 80 lwaampo. Natutye nee iimpungu ohayi etwapo kehe mominute 10, 80 bytes * 6* 24*365 = 4.2 MB kehe momvula. O system yocomputer tayi landitha 2GB yo RAM mo 2008, nomulandu gwa Moore tagu unganeke ekoko mongaashingeyi lyili po 1.2GB kehe komumvo, ehala ita li kala oshiimbi shasha, nonando oshimpungu-palanyolo sha tulwa mo system.

Omakwashilipaleko gomafutilo ga pupalekwa

Oku kwashilipaleka omafutilo pwaana oku longitha oowike dhe andjakaneko nasho otashi vulika.

Omulongithi okwapumbwa owala akale ena okopi yoshimpungu-palanyolo yuumbangi wiilonga womethimbo ndyoka eleeleka melyenge, teyi mono okupitila moma pula pulo goowike dhe andjakaneko, sigo akwashilipaleke kutya oye ena elyenge ndyoka eleeleka, opo amone oshitayi sha Merkle shoka tashi kwatakanitha kumwe omafutilo koshimpungu hoka kuna ostambe yethimbo lyago. UUfutilo mbuka ita vulu oku wu mona kuye mwene, ashike moku wu kwatakanitha kehala lyi li melyenge, ota vulu okumona kutya uufutilo mbuka owa taambwa kuuhuke we andjakaneko, niimpungu mbyoka ya ka gwedhwamo konima yekwashilipaleko ndika kutya e andjakaneko olye wu taamba.

Ekwashilipaleko ndika otali vulu okwiinekelwa, shampa ashike uuhuke wopaushili owo tawu wilike e andjakaneko ndyoka, ka kele ngele e andjakaneko ndika olya kondwa oonkondo komuponokeli gwontumba, mpono itali vulu lela okwiigamena. Omanga uuhuke we andjakaneko tawu vulu oku kwashilipaleka uufutilo kuwo wene, omukalo ngoka gwa pupalekwa otagu vulu oku endwa miineya komafutilo ngoka gaana uushili gomuponokeli, omanga ngaa omuponokeli nguka ta tsikile noku Konda oonkondo e andjakaneko ndyoka. Omukalo gumwe goku igamena kwaashino ogo, oku taamba omalopotelo oku ziilila kuu huke we andjakaneko ngele wa ndhindhilike oshimpungu shaana oshilonga, tawu ulumike o software yomulongithi opo yi konge oshimpungu shuudha noma futilo ga lopotelwa, opo ya kwashilipaleke kutya itayi tsu kumwe shili. Oongeshefa ndhono hadhi taamba omafutilo olundji muule wethimbo eshona otashi vulika dhi kale dha hala oku longitha uuhuke wadho omolwa egameno lya manguluka nekwashilipaleko lyo meendelelo.

Oku tula kumwe noku topola ondjundo

Nonando tashi vulika opo kehe gumwe a ungaunge nookoina dhe mwene, otashi kala oshidhigu oku ninga omafutilo ga yoolokathana mu kehe osenda moma taambathano. Oku pitika ondjundo yi topolwe nokutulwa kumwe, omafutilo ogena omalombwelo ogendji ngoka haga tulwamo oshowoo oku kuthwamo. Moshito, ohapukala ongele oshitulomwa shimwe ashike okuziilila komafutilo ngoka gaka pita omanene, nenge iitulwamo oyindji yatula kumwe iipambu iishona, oshowo iikuthwamo yili nando iyali: Shimwe oshomafutilo, noshikwawo shokugalulila oshendja, ngele opena, ku nakutuma

Nashi kale nduno sha ndhindhilikwa kutya, mpono omafutilo giikolelela komafutili ogendji galwe ga gwedhwapo, kashishi oshiimbo nande nande mpaka. Ihapa kala nando ompumbwe oku kutha okopi yiithikamenapo kuyoyene monakuziwa yefutilo.

Uuholameno

Omukalo gopamu thigululwakwalo goku mbaanga otagu adha ondondo yomeholamo ngele tagu ngambeke omauyelele gaaha monike koombinga adhihe ndhoka dha kwatelwamo noshowo komu inekelwa omutitatu. Omukalo nguka inagu pitika nando ompumbwe yoku igidhila kehe gumwe

omafutilo ngaka, ashike nonando oongawo, okukala meholamo otaku vulu natango oku kalekwapo moku teyapo etaambathano lyomauyelele mehala ekwawo: Moku Kaleka iipatululo yeegulukila kehegumwe yaashiwike. Kehe gumwe ota vulu oku mona kutya oena omuntu ta tumine mukwawo ondando yontumba, ashike uuyelele itawu kwatakanitha omafutilo nado okulye. Shino otashi elekwa naana nuuyelele wagandjwa kaapinganithi yoo bond (stock exchange), mono ethimbo nuunene wepingakanitho kehe, lyatseyithilwa kehe gumwe, ashike mbono yakutha ombinga inaapopiwa kutya oyo oolye.

Mokugwedhapo, epando lyoshipatululo oshipe nali longithwe muufutilo kehe, opo ku keelelwe omafutilo ngaka gaa kwatakanithwe kumwene. Omakwatakanitho gamwe natango onga ge li itaaga vulu oku keelelwa niitulwamo moma futilo ogendji gendji, ngoka taga ka hololа kutya iitulwamo mbika yawo okwali ya mwene gumwe. Oshili sha nika oshiponga ngele mwene gwoshipatululo okwa tothwamo, ekwatakanitho otali vulu okuhololа omafutilo omakwawo ngoka gena mwene gumwe aguke.

Omayalulo

Otatu tula miilonga onkalo yomuponokeli ta kambadhala oku etapo elyenge lya yooloka meendelelo shivulithe elyenge ndyoka lyopauyuuki. Nonando elalakano lye li gwanithwepo, ihashi patululile ehwata koma shendjo gopaumwene, ngaashi oku etapo ondjundo okuziilila mombepo, nenge okukutha oshimaliwa shoka shaa heshi shomu ponokeli. Oohuke itadhi ka taamba nando omafutilo gaana uushili onga ofuto, noohuke ndhoka dhopaushili itadhi ka taamba oshimpungu shina omafutilo ngaka. Omuponokeli ota kambadhala owala oku shendja yimwe yomomafutilo ge, opo a kuthe mo oshimaliwa shoka akala noku longitha methimbo ndika.

Ethigathano pokati kelyenge lyo pauyuuki nelyenge lyomuponokeli otali iyoololelwa onga oonkatu-mwaalu dhaali melandulathano (Binomial Random Walk). Oshinyangadhalwa shono tashi ka kala sha yambukamo miikwawo osho shono shelyenge lyopauyuuki tali hedha komeho noshimpungu shimwe, tashi hedhitha pombanda uukomeho washo na +1, noshi nyangadhalwa shono tashi ka kala inaashi yambukamo osho shono shelyenge lyomuponokeli tali undulilwa komeho noshimpungu shimwe, naashino ota shi shunitha pevi ehala na -1.

Ompito yomuponokeli akale ta vulu oku endela pamwe okuziilila monkalo yoompito dha shonopala, otayi elekwa nuupyakadhi womudhani gomashina. Natu tye Omudhani gwomashina ena omwaalu goku dhana inaagu ngambekwa okwa tameke noompito dha shonopala, ta dhana sigo oonomola dhiikando mbyoka akambadhala okuzamo monkalo ndjika itadhi vulu we ku yalulwa. Otatu vulu oku yalula oompito kutya ita ka zamo we monkalo ndjoka yaashi ombwanawa, nenge oompito ndhoka omuponokeli ta ka endela pamwe nelyenge lyo pauyuuki, ngaashi tashi landula [8]:

p = probability an honest node finds the next block

q = probability the attacker finds the next block

q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & if\ p \leq q \\ (q / p)^z & if\ p > q \end{cases}$$

Given our assumption that $p > q$

, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

Etengeneko: $p > q$, Ompito otayi gu pevi meendelelo sho oonomola dhiimpungu mbyoka omuponokeli ena oku endela pamwe nayo tadhi yi pombanda. Sho oompito itaadhi longele pamwe naye, ngele ita yi komeho iikwatelela kelago manga kuyele, oompito dhe otadhi ende tadhi kanapo kashona nakashona, kehe ethimbo tagwile kokule noshimpungu.

Otatu tula nee miilonga uule thimbo mbono omutaambi gwomafutilo ngano omape apumbwa oku tegelela opo avule okukoleka lela kutya omutumi ita vulu we okushendja omafutilo ngaka. Otatu dhila dhila nee kutya omutumi nguka omuponokeli ngoka ahala omutaambi iitayela kutya okwa futwa muule thimbo wontumba, ye teshi galulako iifute mo yemwene konima shampa pwa piti ethimbo. Omutaambi ota lopotelwa shampa shoka sha ningwa, ashike omutumi ota inekele otaku ka kala kwa lata.

Omutaambi oha toto po epando epe lyiipatululo eta gandja iipatululo ya kehe gumwe komutumi, konima ashike yethimbo eshona elela manga inaa Shaina. Shino ohashi keelele nee omutumi koku longekidha elyenge lyiimpungu komeho gethimbo moku ungaunga nalyo iikando yalandulathana, sigo taningi elago moku kala aya komeho lela sha gwana, opo nee tayi komeho nomafutilo pethimbo olyo tuu ndyoka. Shampa nee omafutilo ngano ga tumwa, omutumi ngoka keeheli pauyuuki ohatameke nee talongo meholamo kelyenge ndyoka lyopomunkulo, lyina omukalo gwa yooloka kwaangoka gomafutilo ge.

Omutaambi ota tegelele naana sigo omafutilo ga gwedhwa ko shimpungu, niimpungu ya z oyakwatakanithwa konima yasho. Omutaambi nguno keshi naana omwaalu gwothaatha gwehumo komeho ndyono omuponokeli aninga, ashike natu tengeneke nee kutya iimpungu yopauyuuki oyakuthapo etengenekwa thimbo lya tegelelwa mu kehe oshimpungu, ehumo komeho lyomuponokeli otali kala oonomola dhiikando mbyono tayi yapo methimbo lya gandjwa (poisson density), no ndjundo ndyono ya tegelelwa.

$$\lambda = z \frac{q}{p}$$

Opo nee kumonike oompito ndhono omuponokeli ta vulu natango oku adha ponkatu mpano, ohatu

indjipaleke nee oonomola dhiikando mbyono tayi yapo methimbo lya gandywa (poisson density), mukehe omwaalu gwehumo komeho ndyono omuponokeli ali ena okuninga, noompito ndhono ta vulu oku adha ponkantu mpaka okuziilia po pointa ndjo.

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & if\ k \le z \\ 1 & if\ k > z \end{cases}$$

Oku ndjandjukununa opo ku keelelwe okutula kumwe omushila gwe topolo.

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Okufala komukalo gwa C

```
#include
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Mokulongitha iizemo yimwe, otatu mono kutya ompito otayigu pevi mbala na z

```
q=0.1
z=0    P=1.0000000
z=1    P=0.2045873
z=2    P=0.0509779
z=3    P=0.0131722
z=4    P=0.0034552
z=5    P=0.0009137
z=6    P=0.0002428
z=7    P=0.0000647
z=8    P=0.0000173
z=9    P=0.0000046
z=10   P=0.0000012

q=0.3
```

```
z=0    P=1.0000000
z=5    P=0.1773523
z=10   P=0.0416605
z=15   P=0.0101008
z=20   P=0.0024804
z=25   P=0.0006132
z=30   P=0.0001522
z=35   P=0.0000379
z=40   P=0.0000095
z=45   P=0.0000024
z=50   P=0.0000006
```

Oku ndjandjukununa P eli kohi ya 0.1%

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

Ehulitho

Otwa tula mo eindilo lyo system yomafutilo gopaungomba pwaana oku ikolelela keineekelo.Otwa tamekele nomutungilo gwookoina dhaningwa momashaino gopaungomba, ngono hagu etapo enkondololo lyookondo lyuumwene, ashike inashi ihwapo ngele kapena omukalo gwoku kankeka omafuto gopaali. Oku patukununa nee oshinima shino, otwa ningi nduno eindilo lye andjakaneko lyomelandulathano tatu longitha uumbangi wiilonga oku ndhindhilika onakuziwa yomafutilo ngoka ga egulukila kehe gumwe, ngoka haga keelele mbala mbala omuponokeli kaaha vule okuga shendja ngele uuhuke wopaushili owo tawu kondolola oonkondo odhindji dho CPU. E andjakaneko oha li kala noonkondo ngele lyaana omutungilo gwapupalekwa. Oohuke ohadhi longo adhihe palumwe nelongelo kumwe lya ngambekwa. Inadhi pumbwa oku tothwamo, molwaashoka omatumwalaka inaga ukililithwa kehala lyi lipo lyowina na oga pumbwa ashike okuthikithwa keitulomo lyo thaatha. Oohuke otadhi vulu okuthigapo e andjakaneko oshowo oku galukilamo kehalo lyadho yene, tadhi taamba elyenge lyuumbangi wiilonga onga uumbangi mwaashono sha ningwa po manga dha li dha zamo. Ohadhi hogolola nee noonkondo dhawo dho CPU, tadhi ulike kutya odha taamba iimpungu mbyoka yopaushili moku yi andjakaneka noku tinda iimpungu mbyoka yaali pau shili, na itadhi ka longa niimpungu mbyoka. Uuwanawa noompango ndhoka dha pumbiwa otadhi vulu oku tulwa milonga nomu kala nguka

Oonzo

1. W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.
2. H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.
3. S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.
4. D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.
5. S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.
6. A. Back, "Hashcash - a denial of service counter-measure,"]http://www.hashcash.org/papers/hashcash.pdf, 2002.
7. R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.
8. W. Feller, "An introduction to probability theory and its applications," 1957.