I-Bitcoin: Ihlelo lemali ye-elekthroni labalingani

ngo Satoshi Nakamoto 2008/10/31

Isirhunyezo

Umhlobo ocwengileko wehlelo lemali ye-elekthroni labangani uzokuvumela iimbhadelo ethunyelwe nge-inthanethi ukuthi ithunyelwe manqophana isuka komunye umuntu iye komunye ngaphandle kokuya ehlanganweni yeemali. Amasiginetjha wedijithi anikela ngengcenye yesisombululo, kodwanana inzuzo ekulu iyalahleka nakufuneka umuntu wesithathu othembekileko ukuvikela ukusetjenziswa kwemali kabili. Siphakamisa isirarululo sekinga yokuberegisa imali kabili ngokuthi kusetjenziswe ithungelelwano labalingani. Ithungelelwano lifaka iintembu zesikhathi ekuthengiselaneni ngokuzifaka eketanini eqhubekako yobufakazi bokusebenza obususelwa ku-hash, kwakha irekhodi elingeke latjhentjhwa ngaphandle kokwenza kabutjha ubufakazi bomsebenzi. Iketani ede khulu ayiberegi kuphela njengobufakazi bokulandelana kwezehlakalo eziboniweko, kodwanana bufakazi bokuthi ivela esizibeni esikhulu samandla we-CPU. Nangabe inengi lamandla we-CPU lilawulwa ma-node angaberegisaniko ukuhlasela ithungelelwano, azokukhiqiza iketani ede khulu begodu atjhiye nabahlaseli. Ithungelelwano ngokwalo lidinga ukwakheka okuncani. Imilayezo irhatjhwa ngomzamo ophuma phambili, begodu ama-node angatjhiya begodu ajoyine ithumgelelwano ngokuthanda kwawo, amukele iketani yobufakazi bomsebenzi ede khulu njengobufakazi balokho okwenzekle nakangekho.

Isingeniso

Zerhwebo ku-Intanethi sezithembele pheze eenhlaganweni zeemali ezisebenza njengabantu abathembekileko besithathu ukulungisa iimbhadelo ze-elekthroni. Ngesikhathi ihlelo lisebenza kuhle ngokwaneleko ngokuthengiselana okunengi, lisaqalane nobuthakathaka bemvelo bomhlobo owakhiwe ngokuthembana. Ukuthengiselana okungabuyeli emuva akukgonakali, ngoba iinhlangano zeemali azikgoni ukukhandela ukulamula imibango. Iindleko zokulamula zikhuphula iindleko zokuthengiselana, zinciphisa isayizi yokuthengiselana esetjenziswako begodu zinciphise amathuba wokuthengiselana okuncani okungajwayeleki, begodu kuneendleko ezibanzi ekulahlekelweni kwamandla wokwenza iimbhadelo ezingabuyiselekiko zeeinsizakalo ezingabuyiselekiko. Ngethuba lokuphendulwa, isidingo sokuthembana siyarhatjheka. Abathengisi kumele babatjheje abathengi babo, babahlukumeza ngokufuna imininingwana edlula leyo ebayidingako. Iphesenthi ethile yokukhwabanisa yamukelwa njengengagegedekiko. Lezi zindleko nembhadalo engakaqinisekiko zingagwenywa mathupha ngokuberegisa imali ebonakalako, kodwanana ayikho indlela ekhona yokubhadela esitetjhini sokuthintana ngaphandle komuntu wesithathu othembekileko.

Okufunekako lihlelo lokubhadela le-elekthroni elisuselwa kubufakazi be-cryptographic esikhundleni sokuthembana, elivumela noma ngibaphi abantu ababili abazimisele ukusebenzisana ngqo ngaphandle kokufuna umuntu wesithathu othembekileko. Ukuthengiselana ongakgoni ukukubuyisela emuva ngekhompyutha kungavikela abathengisi ekukhwabaniseni, begodu iindlela ezijwayelekile zokungena zingasetjenziswa lula ukuvikela abathengi. Kuleli phepha, siphakamisa irarululo yekinga yokusebenzisa imali kabili, sisebenzisa iseva yesitembu sesikhathi esasatjalaliswa phakathi kwabantu ababili ukukhiqiza ubufakazi bokubala ngokulandelana kokuthengiselana. Ihlelo livikelekile lokha ama-node athembekileko nakalawula ngokuhlanganyela namandla we-CPU amanengi ukudlula noma ngisiphi isiqhema esibambisana nama-node wabahlaseli.

Ukuthengiselana

Sihlathulula ihlamvu yemali ye-elekthroni njengeketani yamasiginetjha wedijithi. Umnikazi ngamunye udlulisela ihlamvu yemali komunye ngokusayina ngokwedijithi i-hash yokuthengiselana kwangaphambili nesilodlhelo esisepepeneni somnikazi olandelako bese ungezelela lokhu ekugqineni kwehlamvu yemali. Obhadelwako angaqinisekisa amasiginetjha ukuqinisekisa ubunikazi.

Ikinga ukuthi obhadelwako akakwazi ukuqinisekisa ukuthi omunye wabanikazi khange aberegise imali kabili. Isihlathululo esijwayelekileko kuthula igunya eliphakathi elithembekileko, nofana i-mint, ehlola koke ukuthengiselana okuberegisa imali kabili. Ngemuva kokuthengiselana kanye, ihlamvu yemali kufanele ibuyiselwe ku-mint ukuthi ikwazi ukukhiqiza imali etja, begodu iinhlamvu zemali ezikhutjhwe yi-mint ngizo zodwa ezithembekileko ukuthi zingasetjenziswa kabili. Ikinga ngalesi sisombululo ukuthi ikusasa lehlelo lemali lidzimelele saso soke uhlelo lwemali sincike ekhamphanini ekhambisa i-mint ngobana yoke ithengiselwano idlula kiyo, njengebhanga.

Sifuna indlela yokuthi obhadelwako azi ukuthi abanikazi bangaphambili khange basayine noma ngikuphi ukuthengiselana kwangaphambili. Ngehloso yethu, ukuthenngiselana kwangaphambili ngikho okubalulekileko, ngakho ke asikhathali ngemizamo youberegisa kabili okwenzeke emuva. Indlela eyodwa yokuqinisekisa ukungabikho kokuthengiselana kutjheja koke ukuthengiselana. Ngaphakathi komhlobo onzinze ku-mint, i-mint beyazi koke ukuthengiselana begodu yathatha isiqunto sokuthi ngiyiphi efike ekuthomeni. Ukufeza lokhu ngaphandle komuntu othembekileko, ukuthengisalana kufanele kumenyezwelwe pepenene, begodu sidinga ihlelo ukuze abahlanganyeli bavumelane ngomlando owodwa wehlelo abemukelwe ngayo. Obhadelwako kumele abe nobufakazi bokuthi ngesikhathi sokuthengiselana, inengi lama-node livumile ukuthi bekutholwa kokuthoma.

Iseva yesikhathi

Irarululo esiyiphakamisako ithoma ngeseva yesitembu sesikhathi. Iseva yesitembu sesikhathi

iberega ngokuthatha i-hash yeblogo yezinto ekumele zifakwe isitembu sesikhathi begodu ziveze i-hash kabanzi, njenge phephandabeni nofana ku-Usenet [2-5]. Lesi sitembu sesikhathi sikhomba ukuthi imininingwana beyikhona ngaleso sikhathi, ngokusebala, ukuze ungene ku-hash. Isitembu sesikhathi ngasinye sifaka isitembu sesikhathi sangaphambili ku-hash yaso, sakhe iketani, isitembu sesikhathi ngasinye esingezelelweko siqinisa lezo eziphambi kwazo.

Ubufakazi Bomsebenzi

Ukwenza iseva yesitembu sesikhathi esatjalaliswa ngokulingana, kuzokufuneka siberegise ihlelo lokuqinisekisa umsebenzi elifana ne-Adam Back's Hashcash [6], kunokuba kuthunyelwe kuphephandaba nofana ku-Usenet. Ubufakazi bomsebenzi bufaka hlangana ukuskena inani lapho iku-hash, njenge-SHA-256, i-hash ithoma ngenani lama-zero bits. Umsebenzi ojwayelekileko ofunekako enanini lama-zero bits afunekako begodu ungaqinisekiswa ngokwenza i-hash elilodwa.

Malungana nethungelwano lethu lesitembu sesikhathi, sisebenzisa ubufakazi bokusebenza ngokungezelela i-nonce ebhlogweni kuze kutholakale inani elinikela i-hash yebhlog ama-zero bits afunekako. Lapho nje umzamo we-CPU ukhukhumele ukwanelisa ubufakazi bokusebenza, ibhlogo ngeke litjhugululwe ngaphandle kokwenza umsebenzi kabutjha. Njengoba amabhlogo wamuva abotjhwe ngemuva kwayo, umsebenzi wokutjhugulula ibhlogo ungafaka hlangana ukwenza kabutjha woke amabhlogo aza ngemuva kwayo.

Ubufakazi bomsebenzi burarulula ikinga yokuthola ukujanyelwa ekuthathweni kweeinqumo ezinengi. Ngathana inengi belizinze ekhethweni elilodwa le-IP-isiphande-elilodwa, lingatjhabalaliswa noma ngubani okwazi ukwaba ama-IP amanengi. Ubufakazi bomsebenzi eqinisweni yi-CPU yinye-ivowudi. Isiqunto senengi sijanyelwe yiketani ede kunawo woke, elinomzamo omkhulu khulu wobufakazi obusetjenziswe kilo. Nangabe inengi lamandla we-CPU lilawulwa ma-node athembekileko, iketani ethembekileko lizokukhula msinya khulu begodu lidlule noma ngiziphi iinketani eziphalisana nayo. Ukutjhentjha kancani ibhlogo elidlulileko, ohlaselako kuzokufanele enze kabutjha ubufakazi bokusebenza kwebhlogo nawo woke amabhlogo angemuva kwawo bese ahlangabezana begodu adlula umsebenzi weendawo ezithembekile. Sizokukhombisa ngokukhamba kwesikhathi ukuthi amathuba wokuhlasela kancani ancipha khulu njengoba amabhlogo alandelako angezelelwa.

Ukulilisa ngokwanda kwebelo lensetjenziswa zangaphandle zekhomphyutha netjisakalo ehlukileko ekusebenzeni kwama-node ngokukhamba kwesikhathi, ubunzima bokufakazi komsebenzi butholakala ngesilinganiso esikhambako esikhombisa inani elijwayelekileko lamabhlogo nge-iri. Nangabe zikhiqizwa msinya khulu, ubunzima buyakhuphuka.

Ithungelelwano

Amagadango wokusebenzisa ithungelelwano ajame ngalendlela elandelako:

1. Ukuthengiselana okutjha kurhatjhwa kiwo woke ama-node.
2. I-node ngayinye ibuthelela ukuthengiselana okutjha ebhlogweni.
3. I-node ngayinye iberega ekutholeni ubufakazi bokusebenza obudisi bebhlogo yayo.
4. Lapho i-node ithola ubufakazi bokusebenza, irhatjha ibhlogo kuwo woke ama-node.
5. Ama-node amukela ibhlogo kwaphela lokha koke ukuthengiselana okungaphakathi kwalo kuyokusebenza begodu kungakaberegiswa.
6. Ama-node aveza ukwamukelwa kwawo kwebhlogo ngokusebenzela ukwakha ibhlogo elilandelako eketaneni ngokuberegisa i-hash yebhlogo elamukelwe njenge-hash yangaphambili.

Ama-node ngaso soke isikhathi athatha iketani ede kunawo woke njengefaneleko begodu azokuqhubeka nokulingezelela. Nangabe ama-node amabili arhatjha imihlobo ehlukahlukeneko yebhlogo elilandelaki ngesikhathi sinye, amanye ama-node angathola elilodwa nofana elinye kokuthoma. Kuleso simo, asebenza kelokuthoma abalitholileko, kodwanana agqina elinye igaja nangabe kwenzeka liba lide. Ukulingana kuzokuphulwa lapho kutholakala khoma ubufakazi bokusebenza obulandelako negaja linye liba lide; ama-node abekasebenza kelinye igaja azokutjhintjhelwa kelide.

Ukurhatjhwa okutjha kokuthengiselana akufuneki ukuthi kufike kiwo woke ama-node. Okubalulekileko kukuthi afike kuma-node amanengi, azokungena ebhlohweni ngaphandle kokumorosa isikhathi. Ukurhatjhwa kwebhlogo nakho kubekezelela imilayezo ekhutjhiweko. Nangabe i-node alitholi ibhlogo, lizolibawa lapho lithola ibhlogo elilandelako begodu libone ukuthi lilahlekelwe ngelilodwa.

Isikhuthazo

Ngehlangano, ukuthengiselana kokuthoma ebhlogweni kungukuthengiselana okukhethekileko okuthoma ihlamvu yemali etja mnikazi webhlogo. Lokhu kungezelela isikhuthazo sama-node ukusekela ithungelelwano, begodu kunikela indlela yokuthoma ukwaba iinhlamvu zemali emzombeni, ngoba umthetho ophakathi wokuwakhipha. Ukwengezelelwa okungatjhentjhiko kwenani leenhlamvu zemali ezintja kufana nokuthi abembi begolide baberegisa iinsetjenziswa zokungezelela igolide emzombeni. Esimeni sethu, sikhathi se-CPU negezi ezisetjenziswako.

Isikhuthazo singabuye sisekelwe ngemali yokuthengiselana. Nangabe inani lokukhutjhwako lokuthengiselana lingaphasi kwenani lakho lokufaka, umehluko yimali yokuthengiselana engezelelwa enanini lesikhuthazo sebhlogo eliphethe ukuthengiselana. Lapho isibalo semali esikhethwe ngaphambili sesingene emzombeni, isikhuthazo singatjhuguluka ngokupheleleko sibe yimali ebhadelwako yokuthengiselana begodu singabi nokwehla kwamandla wemali ngokupheleleko.

Isikhuthazo singarhelebha ukukhuthaza ama-node ukuthi ahlale athembekile. Uma umhlaseli

omarhamaru akwazi ukuhlanganisa amandla we-CPU amanengi kunawo woke ama-node athembekileko, kuzokufanele akhethe phakathi kokukuwaberegisa ukurobha abantu ngokweba inzuzo yakhe, nofana ukukuzisebenzisela ukukhiqiza iinhlamvu zemali ezintja. Kufanele akuthole kunenzuzo ekulu ukulandela imithetho, imithetho enjalo emvumela ngeenhlamvu zemali ezintja ngaphezulu kwabo boke abantu bahlanganisiwe, kunokuthathela phasi ihlelo nokuba semthethweni komnotho yakhe.

Ukubuyisa isikhala sediski

Lapho ukuthengiselana kwakamuva kwehlamvu yemali kungqwatjwe ngaphasi kwamabhlogo aneleko, ukuthengiselana okusetjenziswe ngaphambi kokuthi kulahlwe ukubulunga isikhala sediski. Ukwenza lokhu ngaphandle kokuphula i-hash yebhlogo, ukuthengiselana kugijinyelwa ngaphakathi kwe Merkle Tree [7] [2] [5], umrabhu ngiwo wodwa ofakwe ku-hashi yebhlogo. Amabhlogo amadala angahlanganiswa ngokugawulwa iimpande zomuthi. Asikho isidingo sokubulunga ama-hash wangaphakathi.

Ihloko yebhlogo ngaphandle kokuthengiselana ingaba mabhayidi ama-80. Nangabe sicabanga ukuthi amabhlogo akhiqizwa njalo emizuzwini eyi-10, ama-bhayidi ama-80 * 6 * 24 * 365 = 4.2MB ngonyaka. Ngamahlelo wamakhomphyutha athengisa khulu nge-2GB ye-RAM kusukela ngo-2008, noMthetho kaMorey oqagela ukukhula kwanje kwe-1.2GB ngonyaka, ukugqinwa akumele kube yikinga noma ngabe iihloko zebhlogo kufanele zigqinwe emkhumbulweni.

Ukuqinisekiswa Kwembhadelo Okulula

Kungenzeka uqinisekise imbhadelo ngaphandle kokuberegisa i-node epheleleko yethungelwano. Umberegisi udinga kuphela ukugqina ikhophi yamaheda weenhloko zebhlogo elide khulu lobufakazi bokusebenza, angalithola ngokubuza ama-node wethungelwano aze aqinisekise ukuthi uneketani ede khulu, begodu athole igatja leMerkle elihlanganisa ukuthengiselana nebhlogo eline sitembu sesikhathi. Akakwazi ukuzihlolela ukuthengiselana, kodwanana ngokukuhlanganisa nendawo eseketaneni, uyakwazi ukubona ukuthi i-node yethungelelwano iyamukele, begodu amabhlogo afakwe ngemuva kokuthi aqinisekise ukuthi ithungelelwano liyakwamukela.

Njalo, ukuqinisekisa kuyathembeka nangabe unama-node athembekileko alawulwa linethungelelwano, kodwanana kuba sengozini ekulu nangabe ithungelelwano lihlulwa mamandla womhlaseli. Ngesikhathi ama-node wethungelelwano angaqinisekisa ukuthengiselana ngokwawo, indlela eyenziwe lula ingakhohliswa kuthengiselana komhlaseli okungasikho nangabe umhlaseli aqhubeka ukuhlula ithungelelwano. Iqhinga lokuvikela lokhu kungaba kukwamukela iinyeleliso ezivela kuma-node wethungelelwano lapho athola ibhlogo elingakavumeleki, okwenza amahlelo wekhomphyutha womberegisi alande ibhlogo eliphelelekp begodu ayelelise ukuthengiselana

ukuqinisekisa ukungakhambelani. Amarhwebo athola imirholo ejwayelekileko mhlambe azobe asafuna ukwenza ama-node wawo ukuthola ukuphepha okuzijameleko nokuqinisekisa okumsinya.

Ukuhlanganisa nokuhlukanisa inani

Nanyana bekungenzeka ukuphatha iinhlamvu zemali ngazinye, bekungaba nzima ukwenza ukuthengiselana okuhlukileko ngephesenthi ngalinye ekudluliseni. Ukuvumela inani ukuthi lihlukaniswe begodu lihlanganiswe, ukuthengiselana kuphethe kokufaka nemiphumela eminengi. Ngokuvamileko kuzokuba nokufaka kunye okuvela kuthengiselwano elikhulu langaphambili nofana kokufaka okunengi okuhlanganisa amanani amancani, begodu okungenani kokukhipha okubili: yinye yokubhadela, begodu nayinye ebusela itjhentjhi, nangabe ikhona, kumthumeli.

Kumele kutjejwe ukuthi i-fan-out, lapho ukuthengiselana kudzimelele ekuthengiselaneni okunengi, begodu lokho kuthengiselana kudzimelele kokunye okunengi, akusiyo ikinga la. Asikho isidingo sokukhipha ikhophi epheleleko ezijameleko yomlando wokuthengiselana.

Ubufihlo

Imodeli yesiko yebhanga ifikelela izinga lokufihla ngokunciphisa ubungeno kulwazi kulabo abathintekako nomuntu wesithathu othembekileko. Isidingo sokumemezela koke ukuthengiselana epepeneneni kukhandela indlela le, kodwanana ubufihlo bungagqinwa ngokuphula ukukhamba kwelwazi kwenye indawo: ngokugqina iinlodlhelo zomphakathi zingaziwa. Umphakathi ungabona ukuthi umuntu othile uthumela inani komunye umuntu, kodwanana ngaphandle kwemininingwana ehlanganisa ukuthengiselana nomunye umuntu. Lokhu kufana nezinga lemininingwana ekhitjhwa ngokuhwebelana ngezabelo, lapho isikhathi nobukhulu bokurhweba ngakunye, "itheyibhu", kurhatjhwa pepenene, kodwanana ngaphandle kokuveza ukuthi bobani abathintekako.

Njenge-boda lokuvikela ikhomphyutha elingezelelweko, kufanele kusetjenziswe ipara etja yesikhiya ngokuthengiselana ngakunye ukuwavikela ukuthi angahlotjaniswa nomnikazi munye. Okunye ukuhlotjaniswa akukhandeleki ngokuthengiselana okufaka izinto ezinengi, okuveza ukuthi okufakiweko ngekomuntu munye. Ingozi kukuthi nangabe umnikazi wekhiya uyavezwa, ukumhlobanisa kungaveza okunye ukuthengiselana komnikazi loyo.

limbalo

Sitjheja isimo somhlaseli ozama ukukhiqiza enye iketani msinya ukudlula iketani elthembekileko. Nanoma lokhu kufezekile, akuvuli ihlelo ematjhugululweni angasisemthethweni, njengokwakha inani unganalutho nofana ukuthatha imali ekungasiyo yomhlaseli. Ama-node ngeke amukele ukuthengiselana okungakavumeleki njengembhadelo, begodu ama-node athembekileko ngeke

amukele ibhlogo eliwaphetheko. Umhlaseli angazama kuphela ukutjhentjha okunye kokuthengiselana kwakhe ukuze abuyise imali aqeda ukuyiberegisa.

Umjarho ophakathi kweketani eqotho noketani yomhlaseli ungabonakala njenge-Binomial Random Walk. Isehlakalo sepumelelo yiketani eqotho engezelelwe ngebhlogo linye, sikhulisa ukurhola kwalo nge +1, begodu isehlakalo sokuhluleka kungezeleleka kweketani yomhlaseli ngebhlogo linye, ukunciphisa igebhe ngo -1.

Amathuba wokuthi umhlaseli aphumelele kokushodako okunikelweko afana nekinga yeRumler's Ruin. Ake sithi umbheji onekhredithi enganamkhawulo uthoma lapho kusalela khona begodu adlale inani elinganamkhawulo weenilingo ukuzama ukufikelela lapho koke kulingana khona. Singabala amathuba wokuthi angafika yini na lapho koke kulingana khona, nofana ukuthi umhlaseli uke ahlangane neketani eqotho, ngokulandelako [8] :

p = amathuba wokuthi i-node eqotho ithole ibhlogo elilandelako
q = amathuba wokuthi umhlaseli athole ibhlogo elilandelako
q_z = amathuba wokuthi umhlaseli uzokuphumelela ngemva kokusuka ebhlogweni u- z block

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

Asithi ukuqagela kwethu kuthi $p > q$

, amathuba ehla ngebelo njengoba inani lamabhlogo umhlaseli ekufanele afikelele kilo liyanda. Ngenthjijilo aqalane nazo, nangabe akenzi ihlanhla eya phambili kusenesikhathi, amathuba wakhe ayancipha ngokutjhabalala njengoba asalela emuva.

Nje sitjheja ukuthi ummukeli wentengo entja udinga ukulinda isikhathi esingangani ngaphambi kokuthi aqinisekise ukuthi umthumeli akakgoni ukutjhentjha ukuthengiselana. Siqagel ukuthi umthumeli mhlaseli ofuna ukwenza ummukeli akholwe ukuthi umbhadele kwesikhatjhana, bese uyayitjhentjha ukuze ayibuyisele kuye ngemuva kokudlula kwesikhathi esithileko. Ummukeli uzokwaziswa nakwenzekako lokho, kodwanana umthumeli ufisa ukuthi kuzobe sekusemva kwesikhathi.

Ummukeli ukhiqiza ipara yesikhiya etja bese unikela isikhiya somphakathi kumthumeli ngaphambi nje kokusayina. Lokhu kuvimba umthumeli ekulungiseleleni iketani yamabhlogo ngaphambi kwesikhathi ngokusebenza kiwo ngokuqhubekako aze abe nehlanhla yokufika phambili ngokwaneleko, bese uyathengiselana ngaleso sikhathi. Lapho umsebenzi sewuthunyelweko, umthumeli ongakathembeki uthoma ukusebenza ngokwefihlo eketanini efanako ephethe enye indlela yokuthengiselana.

Ummukeli ulinda kuze kufike lapho ukuthengiselana kufakwe ebhlogweni begodu amabhlogo ama-z ahlotjiswane ngemuva kwako. Akalazi inani elinembako leokuqhubekela phambili elenziwe mhlaseli, kodwanana nakacabanga ukuthi amabhlogo athembekileko athathe isikhathi

esilindelekileko ngebhlogo ngayinye, ukuqhubekela phambili komhlaseli ekungaba khona kuzokuba kusatjalaliswa kwe-Poisson ngenani elilindelekileko:

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

Ukuthola amathuba wokuthi umhlaseli afikelele, siphindaphinda ukuminyana kwePoisson ngenani ngalinye lokuqhubekela phambili angalenza ngamathuba wokuthi angafikelela kusukela kuleyo ndawo:

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

Ukuhlela kabutjha ukubalekela ukuhlanganisa okungapheliko wokusabalalisa ...

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

Ukuphendulela kukhowudu u-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;
}
```

Nasitjheja imiphumela ethile, siyabona amathuba wokuthi kungenzeka ehla khulu no-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
```

Ukurarulula kwaka-P ngaphasi kuka-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
```

Isiphetho

Siphakamise ihlelo lokuthengiselana kwe elekthroni ngaphandle kokuthembela ekuthembekeni. Sithome ngephahla elijwayelekileko leenhlamvu zemali ezenziwe ngamasiginetjha wedijithi, okunikela ukulawulwa okuqinileko kobunikazi, kodwanana akukapheleli ngaphandle kwendlela yokuvimba ukusetjenziswa kwemali kabili. Ukurarulula lokhu, siphakamise ithungelelwano labalingani sisebenzisa ubufakazi bokusebenza ukurekhoda umlando osepepeneni wokuthengiselana okwenzeka msinya ukuthi umhlaseli angakgoni ukutjhentjha ngekhompuyutha nangabe ama-node athembekileko alawula inengi lamandla we-CPU. Ithungelelwano linamandla ngokulula kwalo okungakahlelwa. Ama-node asebenza ngesikhathi sinye ngokuhlangana okuncani. Akudingeki ukuthi abonwe, ngoba imilayezo ayikhambiswa kwenye nenye indawo begodu adinga ukulethwa ngomzamo ongcono khulu. Ama-node angatshiya begodu ajoyine ithungelelwano ngokuthanda kwaow, amukele iketani lobufakazi bokusebenza njengobufakazi balokho okwenzekileko lokha bekangekho. Avowuda ngamandla wawo we-CPU, Aphandlusela

ukwamukela kwawo kwamabhlogo avumelekileko ngokusebenzela ukuwangezelela nokwala amabhlogo angakavumeleki ngokwala ukuberegela phezu kwawo. Noma ngimiphi imithetho neenkhuthazo ezidingekako zingagandelelwa ngendlela le yokuvumelana.

References

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.