Sönnun án upplýsinga

Þórður Ágústsson

11. apríl 2021

Útdráttur

Ágrip hér

1 ZKP án Gagnvirkni

Umfjöllun þessa kafla er byggð á kafla 4.7 úr óútgefinni bók eftir Justin Thaler, sjá [?], sem og wikipedia-grein um Fiat-shamir, sjá [?].

Nú höfum við séð nokkrar samskiptareglur sem hægt er að nota til að sanna hinar ýmsu staðhæfingar og í þeim öllum er grundvallaratriði að sannarinn gefur sannprófaranum færi á að spyrja sig spurninga/leggja fyrir sig áskoranir. Þetta er gagnvirknin í samskiptareglunni. Gagnvirknin er sjálf samskiptin milli sannarans og sannprófarans og er, eins og við höfum drepið svo oft að áður, mikilvægasti partur sannaninnar. Það að sannprófarinn geti spurt sannarann spurninga er það sem gerir *Gagnvirkar Sannanir* traustverðugar. Þrátt fyrir það spyr maður sig samt, er hægt að komast hjá samskiptunum. Er hægt að hafa sönnun án Gagnvirkni og afhverju ætti maður að vilja það?

Þrátt fyrir að gagnvirknin sé undirstaðan í gagnvirkum sönnunum hefur hún sína ókosti eins og t.d. að sannarinn þarf að sanna staðhæfinguna sína að nýju fyrir sérhvern nýjan einstakling. Það væri kúl, og hentugra, ef sannarinn gæti bara birt sönnun sína fyrir öllum og sannprófarar farið yfir sönnunina án þess að þurfa að eiga í óþarfa samskiptum við sannarann. En einnig án þess að þurfa að gefa upp á bátinn öryggið sem gagnvirkar sannanir veita.

Svo við viljum einhvernveginn losna við samskiptin milli sannarans og sannprófarans en samt halda lögmæti sönnunarinnar. Notum samskiptareglu strjála lograns og reynum að breyta henni í sönnun án gagnvirkni.

Við þurfum fyrsta skilgreiningu á véfrétt.

Skilgreining 1.1. Við skilgreinum *Véfrétt* sem eitthvað óþekkt algrím sem tekur við inntaki og gefur úttak til baka. *Handahófskennda-Véfrétt* skilgreinum við sem óþekkt algrím sem fyrir hver tvö mismunandi inntök, gefur tvö mismunandi handahófskennd úttök, en ef inntökin 2 eru eins þá eru úttök véfréttarinnar líka eins.

Minnum okkur aftur á samskiptareglu strjála lograns

Samskiptaregla Strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r \pmod p$ og sendir h til $\mathcal{V}$.
2. $\mathcal{V}$ velur $b \in \{0, 1\}$ af handahófi og sendir til baka á $\mathcal{P}$.
3. $\mathcal{P}$ reiknar $a = r + bx \pmod p$ og sendir á $\mathcal{V}$
4. $\mathcal{V}$ athugar hvort $g^a = hv^b \pmod p$, og ef þetta gildir þá samþykkir hann staðhæfingu $\mathcal{P}$ (amk fyrir þessa umferð) en hafnar annars (og lýkur þá reglunni með höfnun)
5. Ítra skref 1-4 þar til $\mathcal{V}$ er sannfærður eða hann hafnar.

Við sjáum að til að breyta þessari samskiptareglu í sönnun án gagnvirkni þurfum við að skipta út virkni sannprófarans í samskiptunum. Þannig að við þurfum að fá valið á b einhvern veginn öðruvísi heldur en frá $\mathcal{V}$.

Fyrsta, ógáfulega, pæling til að breyta reglunni í sönnun án gagnvirkni væri að leyfa $\mathcal{P}$ að velja b-ið sjálfur af handahófi. En við áttum okkur fljótt á skyssunni þar því það mun eingöngu virka ef við treystum $\mathcal{P}$ til að velja b-ið af handahófi (því auðvitað getur $\mathcal{P}$ valið b-ið þannig að það virki alltaf fyrir hann í hverri umferð), en þar sem við viljum ekki þurfa að treysta $\mathcal{P}$ þá gengur þessi lausn ekki.

Önnur, ógáfuleg, pæling væri að nota sameiginlega véfrétt, $\mathcal{O}$, þ.a. $\mathcal{P}$ sendir h úr skrefi 1 á véfréttina og véfréttin gefur handahófskennt svar tilbaka $\{0, 1\}$ (en samt sama svar ef $\mathcal{P}$ sendir sama h-ið aftur, svo þegar $\mathcal{V}$ fer yfir sönnunina getur hann athugað hvort þetta eru réttu gildin sem véfréttin gaf). Þessi hugmynd er ekki góð því $\mathcal{P}$ getur, áður en hann býr til sönnunina, fundið mismunandi $h = g^r \pmod p$ sem gefa 0 og mismunandi $h = g^r v^{-1} \pmod p$ sem gefa 1 og notað þau í sönnuninni sinni, þá veit hann gildin sem hann mun fá og mun því geta framleitt sannfærandi sönnun. Sem er samt ósönn.

Við komumst að þeirri niðurstöðu að til að geta breytt samskiptareglunni í sönnun án gagnvirkni þurfum við að breyta henni örlítið. Þá getum við notað svipaða hugsun og að ofan með handahófskenndu véfréttina.

1.1 Fiat-Shamir Ummyndun

Við sáum í kafla 2 að gagnvirkar sannanir styðja sig heilmikið við möguleika sannprófara á að koma sannara á óvart. Pælingin í Fiat-Shamir er að nýta sér það og skipta slembileika sannprófarans út fyrir slembileika heiðarlegs þriðja aðila (sem er almennt líkt sem hass-falli (e. hash-function) í hagnýtingum) sem bæði sannari og sannprófari hafa aðgang að.

Í Fiat-Shamir ummyndun þá gerum við ráð fyrir að sannarinn og sannprófarinn hafa aðgang að sömu handahófskenndu-véfréttinni. Síðan þegar sannarinn $\mathcal{P}$ vill útbúa sönnunina þá framkvæmir hann samskiptaregluna eins og hann myndi gera við sannprófara nema í staðinn fyrir að hafa samskipti við sannprófarann hefur hann samskipti við véfréttina.

Uppfærð Samskiptaregla Strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r \pmod p$ og sendir h til $\mathcal{V}$.

2. $\mathcal{V}$ velur $0 \leq b < p$ af handahófi og sendir til baka á $\mathcal{P}$.

3. $\mathcal{P}$ reiknar $a = r + bx \pmod p$ og sendir á $\mathcal{V}$

4. $\mathcal{V}$ athugar hvort $h = g^a v^{-b}$, og ef þetta gildir þá samþykkir hann staðhæfingu $\mathcal{P}$ (amk fyrir þessa umferð) en hafnar annars (og lýkur þá reglunni með höfnun)

5. Ítra skref 1-4 þar til $\mathcal{V}$ er sannfærður eða hann hafnar.

Athugum að ef $\mathcal{P}$ er heiðarlegur þá er $g^a v^{-b} = g^{r+bx} g^{-bx} = g^r = h$ og því mun hann sannfæra $\mathcal{V}$ um staðhæfinguna. Sönnunin á því að uppfærða samskiptareglan er gagnvirk sönnun án upplýsinga fer fram á svipaðan máta og sönnunin í kaflanum á undan. Hérna getum við notað Fiat-Shamir ummyndun. Með Fiat Shamir verður sönnunin svona:

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, og reiknar $h = g^r \pmod{p}$.

2. $\mathcal{P}$ sendir h á handahófskenndu-véfréttina $\mathcal{O}$ og fær tilbaka $0 \leq b < p$.

3. $\mathcal{P}$ reiknar $a = r + bx \pmod{p}$ og geymir $(h, a)_i$ sem sönnunina á staðhæfingunni fyrir lotu i.

4. Ítra skref 1-3 þar til nógu mörg gildi $(h, a)_i$ eru tilbúin svo sönnunin sé með nægilega lága lögmætis-villu.

5. skila sönnuninni $\{(h, a)_1, (h, a)_2, ..., (h, a)_k\}$.

Athugum nú að sérhver sannprófari getur lesið sönnunina $\{(h, a)_1, (h, a)_2, ..., (h, a)_k\}$ og athugað fyrir hverja lotu hvort að $h = g^a v^{-b}$, en ekki eingöngu það heldur líka hvort $b = \mathcal{O}(h)$ þar sem $\mathcal{O}(*)$ skilar tölunni sem handahófskennda-véfréttin skilar á inntaki h. Og ef $b \neq \mathcal{O}(h)$, í einhverri lotunni, þá hafnar $\mathcal{V}$ sönnuninni.

Athugum að í þessari útfærslu af samskiptareglu strjála lograns þá þarf $\mathcal{P}$ alltaf að vita lausn á strjála logranum af v til að svara $\mathcal{V}$ á réttan máta, nema þegar $b = 0$. Þannig var það ekki í upprunalegu skilgreiningunni.

Við sjáum að lykillinn bakvið þessa sönnun án gagnvirkni er að láta töluna sem véfréttin skilar vera háða svörum $\mathcal{P}$, og að svör véfréttarinnar eru handahófskennd og mismunandi fyrir mismunandi inntök. Það veldur því að óheiðarlegur $\mathcal{P}$ mun ekki geta áætlað fyrirfram hvernig hann muni geta klekkt á væntanlegum sannprófurum.

Fiat-Shamir ummyndunin er því sú almenna aðferð að skipa út sannprófaranum fyrir handahófskennda-véfrétt, sem sannarinn og allir sannprófarar hafa aðgang að, og láta sannarann nota véfréttina þannig að svör véfréttarinnar eru háð skuldbindingu sannarans (t.d. skuldbindingu hans við töluna r og því h í skrefi 1 í strjála logranum).

Þetta svipar til Bálkakeðju-líkansins í rafmyntum þar sem sérhver bálki er háður hassinu á bálkunum á undan.

Handahófskenndar-véfréttir eru almennt útfærðar í praktís sem hass-föll, t.d. sha256 og sha3.

Þess ber að geta að Fiat-Shamir ummyndun er einungis ein aðferð til að breyta gagnvirkri sönnun í sönnun án gagnvirkni. Til eru fleiri.

1.2 Umræða um hagnýtingar á sönnunum án upplýsinga

Hagnýtingarnar eru margar. Nú þar sem sönnun án upplýsinga er gagnvirk sönnun vitum við, eins og kom fram í umræðunni um hagnýtingar á gagnvirkum sönnunum (??), að þær nýtast vel í að útrýma nauðsyn trausts á milli aðila. Eiginleikinn „án upplýsinga" er síðan hægt að nýta þar sem viðkæmar upplýsingar eru til staðar. Upplýsingar sem er nauðsynlegt að halda leyndum.

Augljós hagnýting er verndun lykilorða. Til dæmis getum við nýtt samskiptaregluna um strjála logrann (??) til að gera notanda kleyft að auðkenna sig án þess að gefa upp lykilorðið sitt. Þetta er tiltölulega lýsandi, og öflugt, dæmi. Athugum að með þessu kerfi þá er ekki nauðsynlegt fyrir notandann að senda lykilorðið sitt til (t.d.) bankans eða þess sem vill vera viss um að notandinn sé sá sem hann segist vera. Það eina sem bankinn hefur er v-ið í reglunni og þegar notandinn auðkennir sig svarar hann aðeins spurningum bankans í samræmi við samskiptaregluna. Nú er þessi samskiptaregla svo öflug að ekki er einu sinni nauðsynlegt að dulkóða skilaboðin. Því hlerari, sem reynir að stela mikilvægum upplýsingum, öðlast engar upplýsingar á því að fylgjast með samskiptunum (reglan er „án upplýsinga"). Hann getur ekki einu sinni verið viss um hvort samskiptin séu raunveruleg.

Fleiri mögulegar hagnýtingar eru í kjarnorkuafvopnun (sjá [?] og kafla 5.2 í [?]) og viðskipta-reglugerðum (sjá II-hluta ritgerðar Nihal R. Gowravaram, [?]).

ZKP-án gagnvirkni hafa einnig mikla möguleika á hagnýtingum. Mest vinna og þróun á ZKP-án gagnvirkni hefur verið gerð í rafmyntum eins og ZCash og Monero. Þar sem þær nota (meðal annars) zk-SNARKs (e. zero knowledge succint non-interactive *arguments* of knowledge, sjá [?]), sem er afbrigði af ZKP-án gagnvirkni, til að t.d. fela upphæðir í viðskiptum (e. transactions), reikningsnúmer (hver á hvaða „reikning") og hver raunverulega borgaði hvað. (fyrir Zcash sjá [?], og Monero sjá sérstaklega „Pedersen Commitment", „Stealth Address" og „Ring CT" á [?])