Sönnun án upplýsinga

Þórður Ágústsson

14. mars 2021

Útdráttur

Ágrip hér

1 Sönnun án Gagnvirkni

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, þ.e. gagnvirkni.

Það hefur sína ókosti eins og t.d. að sannarinn þarf að sanna staðhæfinguna sína að nýju fyrir sérhvern nýjan einstakling. Gott væri ef sannarinn gæti birt sönnun sína fyrir öllum og sannprófarar farið yfir sönnunina án þess að þurfa eiga í óþarfa samskiptum við sannarann.

Svo við viljum einhvernveginn losna við samskiptin við sannprófarann 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 óþekkt algrím sem tekur við inntaki og gefur úttak til baka. Handahófskennd-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.

Munum:
Samskiptaregla Strjála lograns

1. $\mathcal{P}$ velur tölu $0 \leq r < p$ af handahófi, reiknar $h = g^r (\bmod p)$ 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 $a = r + bx(\mod p)$ og sendir á $\mathcal{V}$

4. $\mathcal{V}$ athugar hvort $g^a = hv^b(\mod p)$, 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 athugum að mikilvægið sem $\mathcal{V}$ kemur með í sönnunina er slembileikinn þar sem $b \in \{0, 1\}$ er valið af handahófi. Fyrsta, ógáfulega, pæling væri því 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 $\mathcal{P}$ sem gengi gegn allri pælingunni með gagnvirkum sönnunum að sleppa því að treysta $\mathcal{P}$.

Önnur, ógáfulega, pæling væri að nota véfrétt þ.a. $\mathcal{P}$ sendir h úr skrefi 1 á véfréttina, $\mathcal{O}$, og véfréttin gefur uniformly tilbaka svar $\{0, 1\}$ (en samt sama svar ef $\mathcal{P}$ sendir sama h-ið aftur). Þessi hugmynd er ekki góð því $\mathcal{P}$ getur, áður en hann býr til sönnunina, fundið mismunandi $h = g^r(\mod p)$ sem gefa 0 og mismunandi $h = g^r v^{-1}(\mod p)$ 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 þurfum því að breyta samskiptareglunni örlítið, því við viljum nota Handahófskennda-véfrétt. Þá getum við notað svipaða hugsun og að ofan.

1.1 Fiat-Shamir Ummyndun

(ATH. eftirfarandi er veika útgáfan af Fiat-Shamir, sjá page 6 í main og wikiped heimild 8)

Við sáum í kafla 2 að gagnvirkar sannanir styðja sig heilmikið við möguleika sannprófara á að koma sannara á óvart / styðja sig við að í augum sannarans líta viðbrögð sannprófarans við svörum sannarans út eins og slembibreytur. Pælingin í Fiat-Shamir er að nýta sér það og skipta slembileika sannprófarans út fyrir slembileika þriðja aðila 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 $h = g^r(\mod p)$ 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 $a = r + bx(\mod p)$ 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. 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 $h = g^r(\mod p)$.

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

3. $\mathcal{P}$ reiknar $a = r + bx(\mod p)$ 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 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 $b \neq \mathcal{O}(h)$ þá hafnað 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.

Við sjáum að lykillinn bakvið þessa sönnun er að láta töluna sem véfréttin skilar vera háða svörum $\mathcal{P}$, og að svör véfréttarinnar eru handahófskennd og mismunandi fyrir mismunandi inntök.

Fiat-Shamir ummyndunin er því in general sú að hafa handahófskenndavéfrétt, sem sannarinn og allir sannprófarar hafa aðgang að, og láta sannarann nota véfréttina þannig að svör véfréttarinnar eru háð skuldbindingu sannaranns (t.d. skuldbindingu hans við töluna h í skrefi 1 í strjála logranum).

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

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