

Rapportens författare: Josefin Agerblad och Martin Andersen

Rapportens titel: Provably Secure Pseudo-Random Generators

Opponent: David Karlbom

Var det lätt att förstå vad kandidatjobbet gick ut på?

Ja, det var lätt att förstå vad Kandidatjobbet gick ut på. Vilket var att göra en litteraturstudie av bevisbart säkra pseudo-slumpmässiga generatorer.

Hur tycker du att titeln avspeglar rapportens innehåll?

Titel avspeglar rapporten mycket väll. Den framhäver verkligen vad som ska gå igenom i rapporten utan att titeln är för lång.

Hur beskrev författaren bakgrunden till kandidatjobbet? Finns det en introduktion till översikt av området?

Bakgrunden är mycket bra det är den stora delen utav rapporten. Det jag skulle dock vilja se lite mer av information om var tankarna om bevisbart säkra pseudo-slumpmässiga generatorer kommer ifrån. Samt bakgrunden till varför man behöver dessa.

Hur väll har författaren motiverat sitt val av metod att angripa problemet?

Det är en litteraturstudie så metoden är ganska kortfattad inte så precis men täcker in allt som behövs.

Övriga kommentarer om rapporten och dess struktur.

Figurer, Formler har ingen riktig undertext speciellt inte formlerna. Resultatet är även utelämnat. Vore bra att ha dessa med i rapporten.

Vilka är arbetes/rapportens starka sidor?

Rapportens starka sidor är bakgrunden och diskussionen. Det är där det mesta fokus har legat. Även att den är väldigt förklarande utan att man dumförklara läsaren. Samt att språket är vetenskapligt korrekt.

Vilka är arbetets/rapportens svaga sidor?

Metoden som är kort och borde kanske utvidgas eller i alla fall skrivas mer precis. Introduktionen som inte innehåller något om ämnet i sig. Problemformuleringen har ingen fråga i som ska besvaras.

Hur bedömer du arbetets nyhetsvärde?

Nyhetsvärdet är icke existerande då det bara är en litteraturstudie men det är intressant läsning. Ingenting är egentligen nytt utan istället en sammanställning av redan existerande fakta.

Sammanfatta arbetet på ett par rader.

Rapporten har en kort inledning om vilka de är och varför de gör projektet, inte egentligen något om ämnet bara problemet och en inriktning. Bakgrunden är en djupgående informativ plattform för vidare diskussioner och slutsatser. I diskussionen framhävs deras egna tankar och jämförelser görs. Genom hela rapporten finns det en stark röd tråd. Dock saknas det en resultat punkt, lite mer metod hade inte skadat samt figurtexter borde varit med.

Diskuterar författaren huruvida de förutsättningar som gäller för att metoden ska kunna använda är uppfyllda?

Nej. De diskuterar inte några förutsättningar för att metoden ska fungera.

Är metoden väl beskriven?

Metoden är kortfattat och jag kan sammanfatta det i att de har sökt efter böcker och vetenskapliga artiklar.

Har författaren presenterat sina resultat tydligt?

Resultat saknas i rapporten.

Finner du författarens slutsatser trovärdiga?

Eftersom slutsatsen är att algoritmerna inte skiljer sig så mycket i aspekter av tid samt i fråga om säkerhet. Har de dragit slutsatser utifrån vilken algoritm som används mest. Även slutsatsen angående PNP är väldigt vettig. Dock är det inte besvara deras problem formulering riktigt då de inte svar på hur de skiljer sig åt.

Vad tycker du om litteraturlista? Vilken typ av litteratur finns med? Förefaller litteraturen relevant?

Det verkar mest vara artiklar i ämnen publicerat av kunniga personer inom ämnet. Några internet sidor också men de var trovärdiga personer bakom dessa.

Vilka avsnitt i rapporten var svåra att förstå?

Ingen av avsnitten i rapporten var särskilt svåra att förstå. Eftersom den förklarade nivån är hög i stora delar av rapporten. Den enda delen som känns krånglig är 2.4 där programmet metoder presenteras.

Frågor till författaren:

1. Varför använder man sig inte av true random istället?
2. I Sidorenko:s rapport nämns även Generering genom RSA, förslagit av Goldwasser, Varför har detta inte nämnts i rapporten?
3. Dessa statistik tester som krävs för att datat ska vara säkra pseudo-slumpmässiga, vad är det för typ av test kan, man få något exempel?
4. Vad skulle hända om kvantdatorer blev verklighet?

Vilket är ditt sammanfattade omdöme om kandidatjobbet.

Kandidatjobbet har bra innehåll. Allt fakta är på plats men det är t.ex. en riktig frågeformulering som saknar. Delar av rapporten borde kanske struktureras om. Som ett helhetsintryck anses rapportens missar väggas upp av de positiva sidorna av rapporten.