Posudek vedoucího na diplomovou práci Veroniky Čadové: O DSA

Práce je napsána relativně přehledně a s malým počtem formálních chyb. Její slabinou je určitá mělkost, která se projevuje jednak tím, že podněty v zásadách pro vypracování byly využity jen omezeně, jednak tím, že autorka velmi málo překračuje horizont standardních formulací základních učebnic a přehledových pojednání.

O historii vzniku DSA, o Schnorrově soudním procesu i o interakci norem a základního algoritmu se čtenář dozví velmi málo. Chybí nástin, jak se DSA přesně používá v reálně pracujících implementacích (třeba, jak vypadá ona náhodná volba prvočísel p a q).

Po formální stránce je největší slabinou neuspokojivý formát citací.

Kladem je zprostředkování úvah o tom, že Schnorrův podpis se z určitého hlediska jeví být bezpečnější než DSA. Tato část si však zasluhovala většího rozvedení.

To platí i o dalších kladech práce, kterými je jednak poukaz na určitou drobnou neuspokojivost v matematickém základu DSA, jednak vlastní implementace (autorka například informuje o tom, že útok se zdařil, ale neříká, jaký útok, neuvádí jeho časovou náročnost ani odhad délky klíče, pro který by takový útok byl ještě výpočetně možný.) Práce se tak dostává na hranici obhajitelnosti.

Přes uvedené výhrady doporučuji, aby práce byla uznána jako práce bakalářská a hodnocena stupněm dobře.

V Praze dne 7. ledna 2012

Aleš Drápal