POSUDEK OPONENTA NA BAKALÁŘSKOU PRÁCI
DAVIDA MAŘÁKA
KORELAČNÍ ÚTOKY

Práce se zabývá korelačními útoky na proudové šifry založené na lineárních rekurencích. Zmiňuje také vztah k dekódování samoopravných kódů. Obsah práce odpovídá zadání.

Úroveň matematického vyjadřování je přijatelná. Některé důkazy jsou příliš neformální (např. důkaz Tvrzení 1), jiné zbytečně kostrbaté (není např. žádný důvod k tomu, aby důkaz Tvrzení 2 byl formulován sporem). Neobvyklé je také používání symbolu $\forall$ uvnitř věty namísto slovního „pro všechna“.

Za hlavní nedostatek práce považuji nedostatečnost některých výkladů, na kterých by student mohl prokázat porozumění absolvovaným přednáškám. Typické příklady:

- již zmíněný důkaz Tvrzení 1 (pro lineární algebru);
- nejasné (implicitní) definování rozdělení náhodných veličin (viz např. proměnné $b_{i,j}$ na str. 15);
- poznámka o kontrolní matici v oddílu 4.2 (student si zřejmě neuvědomil, že se jedná o jedno ze základních tvrzení o lineárních kódech).

Projevem nedostatečně uchopené role lineární algebry je také kolísání mezi pojmy „lineární rekurentní posloupnost“ a „lineární posuvný registr se zpětnou vazbou“.

Nepřesvědčivý je výklad vztahu k binárnímu symetrickému kanálu.

Pokud jde o základní myšlenku popisovaných útoků, totiž korelaci, není její popis zcela uspokojivý. V kapitole 2.1 se zřejmě tiše předpokládá, že proud generovaný nesprávným inicializačním vektorem nemá žádnou korelaci. Je to něčím ospravedlněno?

S uvedenými výhradami práci doporučuji k obhajobě.

Praha 28. srpna 2015 Štěpán Holub