POSUDOK OPONENTA NA BAKALÁRSKU PRÁCU:
Anna Godušová
Důkazy bezpečnosti digitálních podpisů

Predložená bakalárska práca popisuje dokázateľnú bezpečnosť podpisových schém založených na permutácii s padajúcimi dvierkami.

Práca obsahuje viacero drobných nedostatkov. Autorka napríklad používa značenie ktoré nedefinovala (strana 4, definícia 3, výraz $F^{R,Sign^R(SK,\cdot)}(PK)$), alebo uvádza kroky dôkazu v nesprávnom poradí (v dôkazoch tvrdení 2.1.1, 3.1.1 a 4.1.1 sa musí najprv vygenerovať trojica (f, f^{-1}, d) a až potom dostane algoritmus I vstup y). Za závažnejšiu chybu považujem chybnú formuláciu tvrdenia 2.1.1, ktoré je v uvedenom znení iba preformuláciou definície bezpečnosti podpisovej schémy (tvrdenie 2.1.1 by malo správne končiť bodkou za slovom *bezpečná* a naviac by namiesto $(G, Sign, Verify)$ malo obsahovať $(G, Sign^h, Verify^h)$). Taktiež v definícii 1 na strane 3 by v poslednej vete malo byť namiesto "pre všetky" uvedené "práve vtedy, keď". Ďalej by v znení tvrdenia 3.1.1 mali byť nerovnosti a nie rovnosti - v (3.1) "$t(k) \geq t'(k)\ldots$", v (3.2) "$\epsilon(k) \leq \ldots$" (v (3.2) by sme inak mohli dostať pravdepodonosť väčšiu ako 1).

Predpoklad "multiplikativity" permutácie v druhom odstavci na strane 14 by mal byť presnejšie formulovaný. Dôkaz tvrdenia 3.1.1 je z velkej časti totožný s dôkazom tvrdenia 2.1.1. Bolo by preto vhodnejšie spojiť kapitoly 2 a 3 a v dôkaze tvrdenia 3.1.1 nadviazať na dôkaz tvrdenia 2.1.1.

Napriek uvedených nedostatkov hodnotím predloženú prácu pozitívne. Za jej klady považujem zrozumiteľnosť a prehľadné rozpracovanie dôkazov.

Prosím, aby pri prezentácii boli zodpovedané nasledujúce otázky:

1. Objasnite krok 3 algoritmu na strane 16. Prečo nechceme aby $r_i = r_j$? Ak tento prípad nastane, prečo nevygenerujeme nové náhodné r_i?
2. Objasnite krok 7 algoritmu na strane 16. Prečo nechceme aby $w_i = w_j$?
3. Objasnite krok 6 algoritmu na strane 17. Prečo nechceme aby $w_i = w_j$?

Predloženú prácu doporučujem uznať ako bakalársku a hodnotiť ju známkou *velmi dobře*.

Praha, 16.1.2012 Michal Hojsík