

Tato práce se zabývá limitacemi nekomprimovatelných kódování s nepodmíněnou bezpečností. Představujeme trhliny v existujícím důkazu nemožnosti konstrukce nekomprimovatelných kódování bez výpočetních omezení na útočníka. Naším hlavním přínosem je nový kompletní důkaz tohoto negativního výsledku. V první části práce představujeme základy teorie nekomprimovatelných kódování včetně nutných definic. Dále prezentujeme nedostatky v původním důkazu a konstruujeme protipříklady. Zbývající část práce tvoří důkaz nemožnosti existence netriviálních nekomprimovatelných kódování bez výpočetních omezení kladených na útočníka. Ten budujeme v několika krocích, kde v každém kroku zahrnujeme více kódování. Na konci práce představujeme útočníka, který je schopný prolomit libovolné netriviální nekomprimovatelné kódování.