Prof. Marek Klonowski
Politechnika Wrocławska
Katedra Sztucznej Inteligencji
Marek.Klonowski@pwr.edu.pl
+48 692 842 272

Wrocław, 30.09.2024

Recenzja rozprawy doktorskiej Pana Karola Żebrowskiego

Niniejszym wnoszę o przyjęcie rozprawy doktorskiej Pana mgra Karola Żebrowskiego zatytułowanej *Analysis of the Simple Refreshing in the Noisy Leakage Model* i dopuszczenie Doktoranta do dalszych etapów procedury nadawania stopnia doktora.

1 Zawartość i struktura rozprawy

Praca dotyczy ochrony przed atakami na sprzętowe protokoły kryptograficzne, określane jako tzw. wycieki (*leakage*). Ataki tego typu mają potencjał do stworzenia faktycznego zagrożenia w rzeczywistych systemach np. jako realizacja tzw. *side-channel attacks*. Praca ma charakter teoretyczny, ewidentnie wpisując się dyscyplinę *informatyka* w ramach nauk ścisłych. Należy jednocześnie zaznaczyć, że badania zaprezentowane w pracy doktorskiej motywowane były rzeczywistymi systemami/urządzeniami kryptograficznymi. Tematyka ta jest trudna i wymaga z jednej strony silnego aparatu matematycznego. Z drugiej zaś strony prowadzenie badań w tej tematyce jest silnie ograniczone realiami technologicznymi.

Praca stanowi rozszerzoną wersję pracy z bardzo dobrej, selektywnej konferencji ASIACRYPT 2019, której poza Doktorantem współautorami byli dwaj bardzo doświadczeni naukowcy, w tym Promotor.

Rozprawa składa się z siedmiu rozdziałów. Pierwszy to wstęp zawierający bardzo zwięzły opis problematyki badawczej wraz bardzo

ogólną prezentacją najistotniejszych wyników. Drugi rozdział przedstawia nieformalnie wyniki, częściowo wprowadza używaną dalej symbolikę oraz formalizację problemu. Rozdział trzeci opisuje modele bezpieczeństwa używane w dalszej części a także wprowadza dalszą formalizację zagadnienia. Rozdział czwarty poświęcony jest bardziej detalicznemu opisowi modelu obwodu realizującego obliczenia oraz jego transformacji, które mają na celu ukrycie obliczeń dla wybranych modeli wycieku informacji. Piąty rozdział przedstawia wybrane konstrukcje w sposób bardziej formalny. Następuje tu także rozszerzenie opisanej wcześniej koncepcji *leakage diagrams*, która stanowi główny wkład merytoryczny Doktoranta. Szósty rozdział poświęcony jest na główny dowód bezpieczeństwa i efektywności protokołu ochrony przed wyciekami w modelu p-*noisy*. Siódmy rozdział to bardzo krótkie podsumowanie rozprawy.

1.1 Główne wyniki

Do głównych wyników rozprawy trzeba zaliczyć:

- Opracowanie nowej metody analizy wycieku informacji z układów reprezentujących urządzenia kryptograficzne i sprowadzenie jego analizy do problemu probabilistyczno-kombinatorycznego.
- Analizę bezpieczeństwa protokołu ochrony przed wyciekami w specyficznym, choć obecnym w literaturze modelu (p-*noisy model*) o atrakcyjnych własnościach ($O(n)$ dodatkowych bitów losowych i $O(n)$ bramek logicznych, bez użycia zaawansowanych, w praktyce nie-konstrukcyjnych struktur jak ekspendery dla parametru bezpieczeństwa n).

2 Uwagi aprobatywne

Tematyka pracy jest ciekawa i bardzo ważna dla bezpieczeństwa systemów informatycznych. Wyni są technicznie trudne. Aby uzyskać przedstawione w rozprawie rezultaty, Autor musiał wziąć pod uwagę bardzo liczne aspekty praktyczne. Dotyczy to w szczególności czas obliczeń, dodatkowego narzutu na złożoność układu logicznego, w końcu - najważniejsze - bezpieczeństwo, jakie się zapewnia.

Należy podkreślić to, że Autor wykazał się znajomością bardzo licznych technik analitycznych a sam dowód wydaje się mieć cechy oryginalne, wskazujące na pomysłowość. Innymi słowy, według

mojej wiedzy, zaproponowana konstrukcja nie jest powieleniem podobnych metod stosowanych do podobnych problemów.

W końcu docenić należy też nową (czy raczej *oryginalną*, bo wynik jest sprzed 5 lat) koncepcję *leakage diagram*, gdzie analizę protokołu sprowadza się do badania spójności pewnej grafowej struktury losowej. Metoda ta wydaje się bardzo intuicyjna i ciekawa, choć jej wykorzystanie wymaga prowadzenia żmudnej analizy związanej m.in. z uwzględnianiem probabilistycznych zależności pomiędzy zmiennymi modelującymi dostęp adwersarza do poszczególnych bitów informacji przetwarzanych przez układ.

Autor, jak się zdaje, dołożył znaczących starań, aby przystępnie wyjaśnić bardzo złożoną analizę dodając przykłady, intuicje i dzieląc rozwiązanie na odrębnie opisywane fragmenty. Opis nadal w pewnej części jest bardzo złożony i trudny w czytaniu, jednak próba jego uproszczenia (częściowo udana) zasługuje na docenienie.

3 Uwagi krytyczne

Istotnym niedostatkiem pracy jest całkowite zlekceważenie dziedziny dotyczącej rozprawy w okresie ostatnich 5 lat. Bibliografia nie zawiera prac innych niż te, które istniały w momencie składania pracy przeszło pięć lat temu. Można przyjąć jako podstawę doktoratu wyniki sprzed kilku lat, szczególnie przy tym poziomie złożoności badanych problemów przyjmując, że poprawa wyników i ich szczegółowe zaprezentowanie wymagają czasu. Niemniej całkowity brak odniesienia się do wyników późniejszych, w szczególności tych, które cytują pracę będącą podstawą rozprawy (sic!), jest trudne do przyjęcia.

Poza brakami odnośnie nowszej literatury, niedostatków można się także dopatrzeć w analizie stanu badań powiązanych z tematyką rozprawy nawet sprzed lat. Autor skromnie odnosi się do wyników innych autorów czy bezpieczeństwa systemów w kontekście wycieku informacji. Przyznać trzeba jednak, że liczba przywołanych prac nie jest aż tak mała (37 pozycji) i jest zdecydowanie większa niż literatura podana w oryginalnej pracy z ASIACRYPT 2019. Problemem jest raczej zakres skromny kwerendy i jej powierzchowność.

Przedstawione wyniki proszą się o podanie konkretnych wyliczeń poziomu bezpieczeństwa dla wybranych układów realizujących klasyczne funkcje kryptograficzne przy pewnych realistycznych założeniach dotyczących parametrów ich działania. Tej „wisienki na torcie”

w doktoracie zabrakło.

Można mieć mieszane odczucia co do samej prezentacji wyników. Jest to jednak temat na tyle złożony, że został on omówiony szerzej w dalszej części niniejszej recenzji.

Usterki pomniejsze

Praca pod względem poprawności języka, interpunkcji, jakości składu tekstu stoi na dobrym poziomie. Można wskazać jednak pewną liczbę błędów technicznych, niedociągnięć czy niespójności. Widać to w szczególności w bibliografii. Nawet podstawowa praca (pozycja [18] w bibliografii) będąca podstawą doktoratu zawiera mocno niepełne dane. Zdarzają się też sytuacje, że wprowadzenie symboli następuje po ich pierwszym użyciu.

4 Uwagi dotycząc prezentacji

Na osobny komentarz zasługuje sposób prezentacji treści w rozprawie. Zacząć trzeba od tego, że analiza protokołów tego typu jest zawsze bardzo złożona i właściwie każda mi znana analiza podobnych protokołów stanowi duże wyzwanie. W swoich badaniach opisanych w dysertacji Doktorant musiał stworzyć abstrakcyjny model układu logicznego zależnego od wielu parametrów, który następnie jest transformowany poprzez substytucję tzw. gadżetów. W efekcie powstaje pewna struktura, która podlega pewnemu procesowi losowemu, którego efektem jest reprezentacja wiedzy adwersarza. Analiza takiego systemu, dla uzyskania precyzyjnego, w pełni formalnego dowodu, wymaga bardzo drobiazgowej analizy, dużej sprawności analitycznej a także pewnej pomysłowości. A chyba przede wszystkim wytrwałości.

Autor, aby ułatwić czytelnikowi zrozumienie prezentowanych treści, stworzył wielopoziomowy opis zaczynając od wprowadzenia pewnych intuicji (rozdział 1 oraz 2), stosując przykłady i dzieląc analizę na etapy. Rzeczywiście, zabiegi te bardzo pomagają w zrozumieniu ogólnej koncepcji oraz intuicji stojących za głównymi mechanizmami wykorzystanymi w analizie formalnej. Z drugiej strony, główna część analizy jest bardzo trudna w zrozumieniu, co wynika w pierwszej kolejności z omówionej wcześniej złożoności problemu. Można jednak postawić tezę, że sama prezentacja mogłaby być lepsza i bardziej czytelna.

Daje się zauważyć, że w pracy jest obecna ogromna liczba opisywanych bytów. Analizę utrudnia to, że są one wprowadzane w różnoraki, niespójny sposób. Znajdziemy tu klasyczne, wyodrębnione definicje, opisy wprowadzone kursywą w tekście, czy nawet wewnątrz twierdzeń (np. w Lemacie 5). Zdarzają się obiekty, których opis znajdziemy w wydzielonych paragrafach (*vide „Extended leakage"*). Same definicje są często bardzo rozbudowane, odwołują się nawet do kilku innych części rozprawy (np. Definicja 10).

Podobnie wydaje się, że można by poprawić czytelność niektórych twierdzeń/lematów. Główny wynik pracy (Twierdzenie 1) byłby chyba bardziej czytelny, gdyby abstrahować tam od oczywistych uwag, że zmodyfikowany obwód liczy to co samo co obwód pierwotny. Dzięki temu „ściana teksu" byłyby nieco mniejsza a przez to zapewne bardziej zrozumiała.

Wydaje się też, że pewne fragmenty nie są zgrabnie napisane. Przykładem może być Definicja 19, w której trudno dociec, co właściwie jest definiowane. Definicja 21 z kolei to raczej fragment rozumowania ze stwierdzeniami, niż definicja. Z kolei Definicja 12, powinna być raczej lematem (?).

Dyskusyjny jest też podział treści - w szczególności podział dość spójnego fragmentu na rozdziały 4 oraz 5, co wydaje się nie być trafionym pomysłem.

Reasumując, prezentacja z pewnością nie jest idealna a czytelność rozprawy mogła być lepsza. Z drugiej strony sam problem jest bardzo złożony, a Doktorantowi zasadniczo udało się przedstawić swoje rozumowanie. Zaznaczmy, że podobne uwagi można skierować do wielu prac opublikowanych na czołowych konferencjach z tej tematyki. Zatem wskazane mankamenty nie uniemożliwiają akceptacji rozprawy w obecnej formie.

5 Inne uwagi - ani pozytywne, ani negatywne

W niniejszej części recenzji przedstawię kilka uwag, które nie mają zasadniczo charakteru wartościującego (lub odnoszą się do elementów, których nie można ocenić jednoznacznie).

Zasadnicza część pracy to wspólny wynik Autora z jedynej pracy napisanej wraz z dwoma bardzo doświadczonymi naukowcami. Trzeba jednak zaznaczyć, że praca ta była technicznie trudna a deklaracja

wkładu Doktoranta potwierdzona przez Promotora pozwala przyjąć, że bardzo znaczący wkład koncepcyjno-techniczny, który leży po stronie Doktoranta jest wystarczający. Nie dopatruję się także problemu w okoliczności, że podstawą rozprawy jest pojedyncza publikacja. Wynika to po części ze specyfiki tematyki badawczej, gdzie uzyskanie nowych, wartościowych rezultatów łączy się z niemal zawsze z trudnościami technicznymi.

Wyników oryginalnych (w sensie objętościowym) jest stosunkowo mało. Zauważmy, że wiele fragmentów jest mocno redundantnych - te same koncepcje pojawiają się nie tylko w części zasadniczej, ale też we wstępie, w licznych przykładach i przypisach. Nie ma to jednak istotnego znaczenia dla ogólnej oceny rozprawy. **Całościowy wkład Doktoranta oceniam jako wystarczający**.

Zastanawiam mnie również sama analiza protokołu. Czy Autor rozważał też inne podejścia do analizy bezpieczeństwa opartego o badanie diagramu? Dyskutowany model wyraźnie przypomina procesy perkolacyjne obrosłe już w dość bogatą literaturę i różnorodne mechanizmy analityczne dla różnych założeń.

Warto też pochylić się nad samym modelem adwersarza, który w praktyce sprowadza się do tego, że uzyskuje on dostęp do poszczególnych „rejestrów"losowo, niezależnie ze stałym prawdopodobieństwem. Model ten wydaje się nienaturalny (choć może być traktowany jako pewne górne ograniczenie na to co w praktyce adwersarz może uzyskać). Zaznaczmy jednak, że model taki jest obecny w literaturze i w pewnym stopniu stanowi kompromis pomiędzy przypadkami trywialnymi a bardziej realistycznymi modelami, które jednak byłyby zapewne jeszcze trudniejsze w analizie. Choć skupienie się na tym właśnie modelu adwersarza wydaje się właściwie ze względów metodologicznych, wartościowa byłaby szersza dyskusja na temat możliwych rozwinięć modelu oraz możliwości jego aplikacji.

6 Podsumowanie

Recenzowana praca doktorska pod licznymi względami bardzo różni się typowych typowych dysertacji przedstawianych w dyscyplinie informatyka i nie jest wolna od wad. Zawiera ona wyniki z jedynej pracy, której współautorem jest Doktorant. Mimo to, uważam że zawiera ona najistotniejszy element - rozwiązanie pewnego trudnego, dobrze umotywowanego problemu naukowego. Co więcej, przyjmując deklarację Doktoranta jak i współautorów, można przyjąć, że

Autor wykazał się solidnym warsztatem naukowym a nawet pewną pomysłowością. Praca jest w dużej części ciężka w czytaniu, trzeba jednak wziąć pod uwagę, że sam problem jest bardzo trudny do opisania, sformalizowania i przeanalizowania.

W świetle przedstawionych argumentów mogę poprzeć wniosek o dopuszczenie Pana Karola Żebrowskiego do kolejnych etapów postępowania w sprawie nadania stopnia doktora.