dr hab. Michał Wrona, prof. UJ
Wydział Matematyki i Informatyki
Uniwersytet Jagielloński

Kraków, 27.08.2024

Recenzja rozprawy doktorskiej

Analiza prostego odświeżania w zaszumionym modelu wycieku informacji

mgra Karola Żebrowskiego

Niniejsza opinia wydana zostaje w związku z uchwałą Rady Naukowej Dyscyplin Matematyka i Informatyka Uniwersytetu Warszawskiego powołującą mnie na recenzenta rozprawy doktorskiej Karola Żebrowskiego w przewodzie prowadzonym na MIM UW.

Ocena

Po przeanalizowaniu przedstawionych materiałów stwierdzam, iż przedłożona rozprawa doktorska **spełnia wymagania** *ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki*: mgr Karol Żebrowski, jak wynika z załączonych dokumentów, przedstawił oryginalne rozwiązanie problemu naukowego zaproponowanego przez prof. dr hab. Stefana Dziembowskiego oraz prof. Sebastiana Fausta — współautorów jedynego artykułu naukowego na podstawie, którego powstał oceniany doktorat. Pierwszy ze współautorów jest również promotorem ocenianej pracy doktorskiej. Wspomniany artykuł to:

Stefan Dziembowski, Sebastian Faust, Karol Żebrowski: Simple Refreshing in the Noisy Leakage Model. ASIACRYPT (3) 2019: 315–344

Problem rozwiązany w dysertacji doktorskiej dobrze wpisuje się w literaturę przedmiotu. Rozwiązanie jest nietrywialne, poprawne i przejrzyście spisane z wyjątkiem drobnych mankamentów wyszczególnionych poniżej.

Doktorant posiada również inne opublikowane prace nie związane bezpośrednio z pracą doktorską.

Uzasadnienie oceny

Główny wynik pracy

Recenzowana rozprawa doktorska dotyczy analizy niebezpieczeństwa wycieku informacji w obliczeniu wykonywanym przez *obwód arytmetyczny* C obliczającym funkcję nad dowolnym skończonym ciałem. Obwód arytmetyczny zbudowany jest z bramek wykonujących dodawanie, mnożenie, obliczanie elementu odwrotnego, kopiowanie wartości oraz generujących stałą wartość.

Jednym ze sposobów zmniejszenia prawdopodobieństwa wycieku jest zastosowanie schematu maskującego, który w wariancie *addytywnym*, rozpatrywanym w pracy, koduje wrażliwe wartości jako sumy n losowych liczb, gdzie n to parametr bezpieczeństwa. Zamiast pierwotnego obwodu arytmetycznego C rozpatruje się *przekształcony obwód* $\widehat{C}$, w którym każda wartość wrażliwa zastąpiona jest przez jej losowe kodowanie. Obwód $\widehat{C}$ zawiera poza tym n*-rundowe gadżety odświeżające* pomiędzy dowolnymi dwiema bramkami obwodu C. Realizują one *prosty schemat odświeżania*, który pojawia się w tytule. Wspomniany gadżet odświeżający nie zmienia kodowanej wartości. W każdej z n-rund zmianie ulega tylko jej kodowanie poprzez dodanie losowego kodowania zera — przewód po przewodzie. Jak pokazano w literaturze, prosty schemat maskujący nie jest bezpieczny w klasycznym modelu t-sondowania, w którym *adwersarz* ma dostęp do t wybranych przez siebie przewodów. Recenzowana rozprawa doktorska analizuje niebezpieczeństwo wycieku, w uznanym za realistyczny, *zaszumionym modelu wycieku informacji*. W zasadzie, w pracy dowód głównego twierdzenia przeprowadzony jest dla modelu losowego p-sondowania, w którym adwersarz ma dostęp do każdego z przewodów obwodu niezależnie ze stałym prawdopodobieństwem p. Znany z literatury fakt redukuje zaszumiony model wycieku do modelu losowego p-sondowania.

Przyjmuje się, że obwód jest bezpieczny, jeśli wiedza adwersarza z dostępem do każdego z przewodów z prawdopodobieństwem p, postrzegana jako zmienna losowa nie różni się znacznie od wyjścia algorytmu symulującego działanie obwodu, również postrzeganego jako zmienna losowa, który zwraca wyjście nie znając wejścia. W myśl definicji przyjętej w pracy obwód $\widehat{C}$ jest (p, ϵ)*-prywatny* jeśli *statystyczna odległość*, również zdefiniowana w pracy, pomiędzy wspomnianymi zmiennymi losowymi jest nie większa niż ϵ.

W szczególności w analizie bezpieczeństwa korzysta się ze skojarzonego z obwodem $\widehat{C}$ tzw. *diagramem wycieku*. Okazuje się, że jeśli nie zachodzi zdarzenie E tzn. odpowiednio zdefiniowane: *lewa* i *prawa strona diagramu wycieku* nie są połączone, to informacja uzyskana przez adwersarza podczas wycieku jest losowa. Ten fakt jest sformułowany jako *Claim 6*. Natomiast *Claim 7* szacuje prawdopodobieństwo tego, że *lewa* i *prawa strona diagramu wycieku* są połączone. Dowód głównego twierdzenia dysertacji doktorskiej — *Twierdzenie 1* składa się w zasadzie z dowodów *Claimów* 6 i 7. Wspomniane dowody znajdują się w rozdziale 6.

W szczególności Twierdzenie 1 aplikuje się do obwodów afinicznych (bez mnożenia), arytmetycznych (zdefiniowanych powyżej), i k-rundowych gadżetów odświeżających w rozdziale 6.1. Prawdopodobieństwo wystąpienia zdarzenia E w każdym z tych wariantów wynosi odpowiednio: $|C|\,(4p + 8\sqrt{3p})^n$ w wypadku obwodów afinicznych, $|C|\,(32np + 4n\sqrt{3p})^n$ dla obwodów arytmetycznych oraz $k(4p + 8\sqrt{3p})^n$ dla k-rundowych gadżetów odświeżających. Powyżej $|C|$ to liczba bramek w obwodzie C. Stąd wnioskuje się, że obliczenie w odpowiednich obwodach jest $(p, |C|\,(4p + 8\sqrt{3p})^n)$-prywatne, $(p, |C|\,(32np + 4n\sqrt{3p})^n)$-prywatne oraz $(p, k(4p + 8\sqrt{3p})^n)$-prywatne. Przyznaję, że brakuje mi interpretacji tych wyników tłumaczącej ich związek z bardziej abstrakcyjnym pojęciem *bezpieczeństwa obliczeń*.

Strona redakcyjna oraz bardziej szczegółowe omówienie pracy

Cała praca złożona jest z siedmiu rozdziałów, przy czym pierwszy to wstęp, a ostatni to wnioski. Rozdział drugi stanowi łagodne wprowadzenie do zagadnień dysertacji poprzez rozpatrywanie diagramu wycieku oraz zdarzenia E tylko dla gadżetów odświeżających. W szczególności omówione jest nieformalne podejście do dowodu Claimu 6 dla tego uproszczonego przypadku. Uogólnienie zdarzenia E oraz diagramu wycieku dla bardziej skomplikowanych obwodów kończy rozdział drugi. Należy pochwalić doktoranta za tego rodzaju rozdział wprowadzający, który pozwala czytelnikowi na delikatne zapoznanie się z pewnymi ważnymi pojęciami podczas gdy inne są na tym etapie tylko nieformalnie zarysowane. Przyznaję, że często wracałem do tego rozdziału, czytając pełny dowód głównego twierdzenia. Trzeci, krótki rozdział to *preliminaries*. Wprowadza kolejne ważne pojęcia, m.in. pojęcie (p, ϵ)-prywatności wspomniane wyżej.

Rozdział czwarty traktuje w szczegółach transformację z C do $\widehat{C}$. W szczególności bramki wykonujące operacje na elementach ciała w C zostają zastąpione przez gadżety wykonujące odpowiednie operacja na ich kodowaniach. Dla mnożenia w C rozpatruje się tzw. *ISW multiplication gadget*, realizujący mnożenie w $\widehat{C}$. Wspomniany gadżet jest wprowadzony w pracy [25], która poświęcona jest obwodom operującym na wartościach Boolowskich tj. realizujących operacje w ciele GF(2). Autorzy przytoczonej powyżej pracy, na której opiera się recenzowany doktorat adoptują na swoje potrzeby ten gadżet w sposób, wydaje się, dosyć nieostrożny. W rzeczy samej, w niezmienionej postaci Lemat 2, w którym dowodzi się, że gadżet ISW realizuje mnożenie w $\widehat{C}$ działa tylko dla ciała o charakterystyce 2, choć powinien dla dowolnego ciała skończonego. Lemat 2 pojawia się również w pracy konferencyjnej, na podstawie której napisany jest doktorat. W materiałach konferencyjnych ASIACRYPT nie ma dowodu tego lematu. Zainteresowany czytelnik odsyłany jest do pełnej wersji artykułu, do *Cryptology ePrint Archive*. Próżno jednak jej tam szukać. To nie jest dobra praktyka! Lemat 2 można, co prawda, łatwo naprawić, zastępując w punkcie 3 konstrukcji w ramce powyżej Lematu 2: $(z_{i,j} \oplus x_i \otimes y_j) \oplus x_j \otimes y_i$ na $(-z_{i,j} \oplus x_i \otimes y_j) \oplus x_j \otimes y_i$. Trudno jednak nie ulec wrażeniu, że to szczęśliwy, dla doktoranta, zbieg okoliczności, a nie pomyłka w konstrukcji.

W rozdziale 5 dowodzi się lematów 4-6 wykorzystywanych w dowodzie głównego twierdzenia w rozdziale 6.

Inne szczegółowe uwagi

- Strona 20, drugi akapit: "Note that in addition to" — sądzę że powinno być po prostu: "In addition to". Tutaj nie ma czego zauważać.
- W Figure 2.1 (b) na strona 21 pojawia się bramka CP, która kopiuje podaną wartość. Wytłumaczenie co to za bramka znajduje się dopiero w rozdziale 4.
- Pierwsza linijka pod Figure 2.3 na stronie 24: powinno być x_2^2 zamiast x_2^3.
- Strona 25, linijka -3: "it is easy to see that" — myślę, że nic by się stało gdyby autor wytłumaczył dlaczego jest łatwo dostrzec to, że w tym wypadku zdarzenie E powoduje poznanie wrażliwej wartości przez adwersarza. Innymi prawami rządzi się publikacja naukowa, w której nie zawsze na wszystko jest miejsce, a innymi dysertacja doktorska, która nie ma ograniczonej liczby stron. Tym bardziej warto byłoby poświęcić tej obserwacji więcej miejsca, że zdarzenie E jest kluczowe dla całej pracy. W szczególności nie jest jasne czy zdarzenie E w wypadku dowolnych obwodów wiążę się z pozyskaniem przez adwersarza wartości wrażliwej. W omawianym na stronie 25 wypadku tak jest i dlatego warto byłoby się nad tym pochylić.