prof. Damian Niwiński
Instytut Informatyki UW

Recenzja rozprawy doktorskiej pana Michała Zająca pt. *Effective cryptographic protocols with limited computational power and memory*

Rozprawa doktorska pana Michała Zająca przedstawia nową, oryginalną metodę generowania kluczy w modelu kryptografii z ograniczonym pozyskiwaniem danych (ang. *Bounded Retrieval Model*, BRM). Metoda ta generuje klucze o własnościach bliskich kluczom losowym, startując z danych o niedoskonałej losowości. Podobne zagadnienie było wcześniej rozważane w pracach Y. Dodisa i jego współautorów, którzy zaproponowali pojęcie funkcji generującej klucze (*key derivation function, kdf*). Rozważana rozprawa doktorska nawiązuje do tej koncepcji, ale pokazuje istotnie nowy algorytm uzyskujący pożądany efekt, oparty na własnościach pewnych szczególnych grafów, tzw. dysperserów (*disperser graphs*). Autor argumentuje, że nowa metoda dobrze nadaje się do zabezpieczenia kryptograficznego urządzeń o niewielkiej pamięci, jak np. tablety, gdzie klucze kryptograficzne mogłyby być generowane wprost z prywatnych materiałów użytkownika, które i tak się tam znajdują, jak np. zdjęcia. Metoda ta odpowiada na problem, jaki występował dotąd w protokołach opartych na BRM, jakim jest konieczność przechowywania wielkich kluczy. Nowy scenariusz zakłada jednak nowy postulat, nierozważany przez zespół Dodisa, a mianowicie zapewnienie prywatności – chodzi o to, żeby klucz nie ujawniał niepotrzebnie informacji o prywatnych materiałach użytkownika, z których powstał. Autor wykazuje, że zaproponowana przez niego metoda zapewnia zarówno własność bezpieczeństwa, jak i prywatności, według pewnych ściśle określonych kryteriów. Stanowi to główny wynik pracy. Autor przedstawia także dwa zastosowania nowej metody w dwóch sytuacjach kryptograficznych, w których sprawne generowanie kluczy odgrywa istotną rolę, a mianowicie w protokołach identyfikacji i podpisu elektronicznego. Autor wykazuje, że klucze generowane nową metodą zachowują się niewiele gorzej, niż klucze losowe.

Wyniki rozprawy były częściowo opublikowane w pracy *Bounded-Retrieval Model with Keys Derived from Private Data* przedstawionej na konferencji **Inscrypt** w 2016 r., autorami pracy są Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, Michał Zając i Maciej Zdanowicz.

Wyniki rozprawy

Rozprawa składa się z pięciu rozdziałów. Rozdział 1 stanowi wstęp. Autor przedstawia metodę określania bezpieczeństwa danego protokołu kryptograficznego przy pomocy gry, w której przeciwnik (*adversary*) wciela się w rolę jednego z uczestników protokołu. Bezpieczeństwo mierzy się prawdopodobieństwem zdarzenia, że przeciwnik wygra grę i tym samym osiągnie swój cel, zwodząc legalnych uczestników protokołu. Z kolei autor omawia różne typy ataków, zdarzających się lub możliwych we współczesnym świecie, nakierowanych na informację przechowywaną przez użytkowników. Klasyczna kryptografia zorientowana jest na ochronę informacji przesyłanej przez kanały komunikcyjne, przy założeniu, że informacja przechowywana przez użytkowników pozostaje tajna. Autor argumentuje, że to ostatnie założenie jest obecnie trudne do utrzymania. Sytuacja ta motywuje ważny kierunek we współczesnej kryptografii — kryptografię odporną na niekontrolowane wycieki informacji z komputerów legalnych użytkowników. Autor omawia kilka podejść do tego problemu, by dojść do tego, które rozwijane jest w rozprawie, a mianowicie wspomnianego już wyżej modelu z ograniczonym pozyskiwaniem danych przez nieprzyjaciela, *Bounded Retrieval Model*, jaki w 2006 r. zaproponował promotor pracy Stefan Dziembowski (równolegle z inną grupą autorów). W modelu tym buduje się protokoły odporne na wycieki informacji przy założeniu konkretnych ograniczeń przeciwnika – np. ograniczonego w czasie dostępu do wrażliwych danych. Autor omawia silne i słabe punkty tego modelu. Jednym z problemów w protokołach opartych na BRM jest obciążanie pamięci przez ogromne (rzędu gigabajtów) klucze – ten właśnie problem jest podjęty w rozprawie. Autor przedstawia ogólnie wyniki swojej

pracy umieszczając je w kontekście praktycznym i teoretycznym. Z jednej strony mamy oczekiwania współczesnego społeczeństwa – w szczególności rosnącą potrzebę zapewnienia prywatności. Z drugiej – ciekawe pytanie teoretyczne o możliwość efektywnego symulowania idealnej losowości, prowadzące do otwartych problemów w teorii złożoności.

W sumie rozdział wstępny stanowi dobrze przemyślany zarys sytuacji we współczesnej kryptografii. Akcenty położone są zwłaszcza na problemy praktyczne, stanowiące motywację badań teoretycznych, a także ich ostateczną weryfikację.

Rozdział 2 (*Preliminaries*) poświęcony jest ścisłemu przedstawieniu pojęć rozważanych w pracy, przede wszystkim wspomnianej wyżej gry bezpieczeństwa (*security game*) i jej różnych realizacji dostosowanych do różnych protokołów i możliwych ataków. Pojęcie to nawiązuje do koncepcji znanych z literatury, ale w obecnej ogólnej formie zostało wprowadzone we wspomnianej wyżej pracy z udziałem autora przedstawionej na konferencji Inscrypt 2016. Dyskutowane jest założenie dostępności idealnej wyroczni losowej (*random oracle*) szeroko przyjmowane w literaturze – także i w tej rozprawie. Autor uzasadnia też kryterium min-entropii (minimalne $\log \frac{1}{p}$), które w kontekście kryptograficznym lepiej przybliża losowość danych niż entropia Shannona (uśrednione $\log \frac{1}{p}$). Z kolei autor przedstawia protokoły uwierzytelnienia i podpisu przy założeniu BRM. W zakończeniu rozdziału autor wprowadza pojęcie grafów tzw. dysperserów (ang. *disperser graphs*), na jakich będzie się opierać główna konstrukcja pracy. Przypomniane są własności dysperserów znane z literatury, a w szczególności związek tych grafów z tzw. ekstraktorami, czyli funkcjami, które „powiększają losowość".

Kolejne dwa rozdziały stanowią główną techniczną część pracy. Rozdział 3 zawiera główny rezultat i jest zarazem najbardziej oryginalną częścią pracy. Autor rozpoczyna od ścisłego zdefiniowania prywatności oraz bezpieczeństwa funkcji generującej klucze (*kdf*) w modelu BRM za pomocą odpowiednich gier. Dalej przedstawiony jest algorytm realizujący taką funkcję oparty na grafach dysperserach. Główne twierdzenie rozdziału (*Theorem 9*) orzeka, że powstała w ten sposób funkcja – nazwana *Disperse* – istotnie spełnia oczekiwane warunki prywatności i bezpieczeństwa. Przypomnijmy, że zagadnienie prywatności funkcji generującej klucze (*kdf*) nie było dotąd rozważane przez innych autorów. Dowód twierdzenia jest trudny i opiera się na kilku nieoczywistych krokach pośrednich. Istotnym pojęciem jest nowa gra, tzw. *guessing game*. W ładnym teorio-informacyjnym dowodzie autor pokazuje, jak ograniczenie dolne na min-entropię danych przekłada się na ograniczenie górne prawdopodobieństwa sukcesu przeciwnika w *guessing game* (Lemat 10). Ten lemat prowadzi z kolei do własności, którą autor określa jako jednokierunkowość (*one-wayness*) funkcji *Disperse* (Lemat 11); z grubsza mówiąc chodzi tu o ograniczenie na liczbę „trafionych" pytań do wyroczni, jakie przeciwnik ma szansę wygenerować (określanych tu jako *bad queries*). Wspomniana własność leży u podstaw zarówno prywatności jak i bezpieczeństwa funkcji *Disperse*, co jest wykazane przez konstrukcję odpowiedniego symulatora i szereg subtelnych redukcji.

Rezultaty rozdziału 3 mają charakter abstrakcyjny – dotyczą prywatności i bezpieczeństwa funkcji generujących klucze (*kdf*) rozumianych jako pojęcie pierwotne (*cryptographic primitive*). W praktyce interesuje nas oczywiście zastosowanie takich funkcji w konkretnych protokołach. W rozdziale 4 autor rozważa dwa konkretne zagadnienia kryptograficzne: identyfikację i podpis, przy założeniu BRM. Rozważane tu protokoły, oparte na drzewach Merkla, były wcześniej znane. Oryginalny wkład polega na wykazaniu, że bezpieczeństwo funkcji *kdf* udowodnione w poprzednim rozdziale implikuje bezpieczeństwo rozważanych protokołów przy założeniu BRM z dobrymi parametrami – rezultaty mają postać konkretnych nierówności. Główny wysiłek nakierowany jest na protokół identyfikacji; protokół podpisu jest dalej otrzymany w standardowy sposób. Autor podejmuje też istotne w tym kontekście zagadnienie uaktualniania klucza przez uprawnionego użytkownika, kiedy dane, z których klucz jest obliczany (w praktyce będą to prywatne pliki użytkownika) ulegają zmianie. Rozumowania w tym rozdziale są nieco bardziej standardowe niż w rozdziale 3, ale także wymagały od autora znacznej biegłości technicznej.

W krótkim rozdziale 5 autor przedstawia kilka problemów otwartych, jakie w naturalny sposób wypływają z pracy, a dodatek (*Appendix A*) zawiera dowód twierdzenia z pracy innych autorów na temat redukcji protokołu podpisu do protokołu identyfikacji w modelu BRM.

Ocena i konkluzja

Wynikami rozprawy doktorskiej pana Michała Zająca są algorytmy i twierdzenia matematyczne, jakie omówiłem powyżej. Doceniając wagę praktycznych motywacji, należy jednak odróżnić perspektywiczne zastosowania od rzeczywistych wyników. I tak na przykład, opisany przez autora scenariusz generowania bezpiecznych kluczy z prywatnych plików użytkownika (jak np. zdjęcia z wakacji) stanowi w moim rozumieniu perspektywiczne zastosowanie, nie sprawdzone jeszcze w fizycznym eksperymencie, choć autor podejmuje próbę oszacowania parametrów swojej metody w rzeczywistym świecie. Nie umniejsza to jednak wartości pracy; w szczególności należy docenić podjęcie – po raz pierwszy w literaturze – zagadnienia prywatności funkcji generującej klucze w modelu BRM, właśnie z uwagi na potencjalne zastosowania.

Wyniki przedstawione w rozprawie są wartościowe i ciekawe zarówno teoretycznie, jak i ze względu na potencjalne zastosowanie. Problem „powiększania losowości" jest badany w silnych światowych ośrodkach kryptograficznych (np. przez wspomniany zespół Dodisa w New York University). Autor wykazał kompetencję w dziedzinie kryptografii, a także znaczną biegłość techniczną, a także zdolność ujmowania skomplikowanych sytuacji w ścisłe definicje matematyczne.

Pierwsza wersja pracy zawierała dość liczne usterki w zakresie prezentacji, które w obecnej wersji zostały całkowicie usunięte. Znalazłem jedynie pewne drobne niejsaności, które nie wpływają na ocenę pracy (np. w sekcji 3.3 na temat *Guessing games* typ $\mathcal{H}$ się zgadza, ale typ X wydaje się inny w Definicji 28, a inny w Lemacie 10?). W obecnej wersji pracę czyta się dobrze; definicje matematyczne, choć czasem skomplikowane, są przejrzyste, a liczne odniesienia do sytuacji z realnego świata tworzą spójną odautorską narrację.

Podsumowując, stwierdzam, że praca pana Michała Zająca spełnia ustawowe i zwyczajowe wymagania stawiane rozprawom doktorskim i wnoszę o dopuszczenie doktoranta do dalszych etapów przewodu doktorskiego.

Warszawa, 4 maja 2018 Damian Niwiński