Warszawa dn. 31-05-2016

Prof. UW Jacek Pomykała

Instytut Matematyki Wydziału

Matematyki Informatyki i Mechaniki

Uniwersytetu Warszawskiego

Recenzja rozprawy doktorskiej mgr Kamila Kluczniaka

pt. *Anonymous authentication electronic identity documents using electronic identity documents*

dla Rady Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk w Warszawie

Recenzowana rozprawa doktorska mgr Kamila Kluczniaka (o objętości 121 stron) została napisana w języku angielskim i dotyczy zasadniczo podpisów cyfrowych domenowych zarówno statycznych jak i dynamicznych. Można je podzielić na dwie klasy: podpisów ad hoc (nie wymagających istnienia właścicieli generujących klucze domenowe) i podpisów z infrastrukturą (domeny są reprezentowane przez infrastrukturę generującą odpowiednie klucze). Autor podaje w niej ścisłą definicję każdego typu podpisu oraz wymagania jakie powinien on spełniać. Pokazuje także, że jego konstrukcje spełniają zadane wymagania przy klasycznie stosowanych założeniach znanych z literatury.

Ważną częścią rozprawy jest krytyczna analiza rozwiązań rekomendowanych przez German Federal Office for Information Security (BSI) dotyczących pseudonimów domenowych, które poza wymaganiem niepowiązywalności podpisów (tzn. niemożliwości skorelowania pseudonimów tego samego użytkownika w różnych domenach) muszą być certyfikowane przez właściwy organ. Zacznijmy od podstawowych definicji i wymagań jakie mają spełniać podpisy domenowe. Występują tu podobnie jak w podpisach grupowych zasadniczo dwie strony: manager grupy (issuer) i użytkownik tworzący podpis (user). Opcjonalnie dochodzi do tego trzecia strona (infrastruktura)- właściciel domeny, odpowiedzialna za dostarczenie kluczy publicznych identyfikujących zadane domeny.

Podpisujący użytkownik dostaje (lub współtworzy) z managerem grupy odpowiedni klucz prywatny oraz odpowiedni certyfikat zaświadczający, że jest członkiem odpowiedniej grupy. Na jego podstawie oblicza unikalny i stały pseudonim dla zadanej domeny zapewniający 3 podstawowe warunki bezpieczeństwa:

Niepodrabialność(unforgeability) –nikt poza uprawnionym użytkownikiem nie jest w stanie stworzyć podpisu użytkownika bez znajomości jego klucza prywatnego

Zamkniętość (seclusiveness)-nie da się stworzyć podpisu pod pseudonimem nie odpowiadającego żadnemu użytkownikowi dodanemu przez managera grupy

Nielinkowalność (domain unlikability)- niemomożliwe jest powiązanie dwóch rożnych podpisów domenowych z jednym użytkownikiem

Autor rozprawy bada podpisy domenowe wykorzystując do tego własności znanych z literatury odwzorowań (iloczynów) dwuliniowych e: $G_1 \times G_2 \rightarrow G_T$ spełniających określone warunki (związane z „jednokierunkowością" odpowiednich funkcji indukowanych przez iloczyn e). Efektywne obliczeniowo konstrukcje takich iloczynów są wykorzystywane do projektowania protokołów kryptograficznych wykorzystujących fakt, że odpowiedni problem decyzyjny Diffie-Hellmana jest łatwy, natomiast obliczeniowy trudny. Autor rozprawy stosuje je do projektowania metod anonimowego uwierzytelniania, a konkretnie do modelowania i dowodów bezpieczeństwa odpowiednich podpisów domenowych.

Wagę proponowanych przez autora rozwiązań powyższa fakt, że stosowne, proponowane wcześniej rozwiązania w tej dziedzinie- głównie przez autorów niemieckich i francuskich zawierały pewne wady i luki w dowodach, które zostały doskonale zidentyfikowane przez mgra Kluczniaka. Autor następnie zaproponował nowe rozwiązania pozbawione zasadniczo tych słabości, związanych między innymi z kosztem obliczeniowym podpisu. Dotyczy to następujących prac:

Jens Bender, Ozgur Dagdelen, Marc Fischlin, and Dennis Kugler. *Domain-specific pseudonymous signatures for the german identity card*. In Dieter Gollmann and FelixC. Freiling, editors, Information Security, volume 7483 of Lecture Notes in Computer Science, pages 104–119. Springer Berlin Heidelberg, 2012, oraz

Julien Bringer, Herve Chabanne, Roch Lescuyer, and Alain Patey. *Efficient and strongly secure dynamic domain-specific pseudonymous signatures for id documents*. In Nicolas Christin and Reihaneh Safavi-Naini, editors, Financial Cryptography and Data Security, volume 8437 of Lecture Notes in Computer Science, pages 255–272. Springer Berlin Heidelberg, 2014,

a także

Alain Patey, *Techniques cryptographiques pour l'authentification et l'identification biometriques respectant la vie privee* (cryptographic techniques for privacy-preserving biometric authentication and identification). TELECOM ParisTech, PhD Thesis, 2014,

do których odnosi się opublikowana już praca doktoranta -Domain-specific pseudonymous signatures revisited. Cryptology ePrint Archive, Report 2016/070, 2016. http://eprint.iacr.org/.

Prezentowane w rozprawie wyniki są ułożone w sposób logiczny i przejrzysty z uwzględnieniem standardu- od ogółu do szczegółu. Bardzo obszerny spis cytowanych pozycji bibliograficznych dowodzi, że autor doskonale porusza się w omawianej problematyce kryptograficznej. Pragnę tu stwierdzić, że tematyka rozprawy jest bardzo aktualna i zajmują się nią badacze wielu ośrodków naukowych na całym świecie.

Patrząc z perspektywy podziału pracy na rozdziały to pierwsze dwa pokazują dobrze zdefiniowany stan wiedzy w tej dziedzinie oraz podstawowe pojęcia wprowadzające w tę tematykę badawczą.

W rozdziale 3 autor przedstawia formalną konstrukcję (wraz z dowodem bezpieczeństwa) podpisu domenowego ad hoc. W odróżnieniu cytowanych powyżej dwu pierwszych prac tutaj klucze domenowe nie muszą być generowane, gdyż użytkownik może obliczyć pseudonimy przy pomocy swojego klucza prywatnego i nazwy domeny. Podstawowy pomysł zastosowany przez autora rozprawy i jednocześnie punkt wyjścia do dalszych rozszerzeń i modyfikacji jest polaczeniem idei identyfikacji Fiata-Shamira oraz podpisu grupowego

Boneha, Boyena i Shachama [BBS] w wygodniejszej dla autora formie protokołu Camenischa,Chaabouni i Shelata [CCS]. Warto go zatem przybliżyć. Idea jest następująca. Kluczem prywatnym użytkownika U jest uSK={u, A=$g_1^{1/z+u}$}, gdzie zobowiązaniem dla z jest Z=g_2^z. Wartość A można traktować jako certyfikat klucza prywatnego użytkownika. Jeśli Z i u są ustalone to wartość uSK jest określona jednoznacznie.

Pseudonimem użytkownika U jest wartość D^u, gdzie D=H(dom) jest wartością funkcji haszującej na nazwie domeny. Do skonstruowania podpisu wybieramy losowe r i obliczamy odpowiednie zobowiązanie R= $g_2^{r/z+u}$. Para (Z,R) jednoznacznie określa u więc możemy przeprowadzić dowód wiedzy korzystając z idei Fiata-Shamira następująco.

Losujemy t_1 oraz t_2 z odpowiednich dziedzin i obliczamy zobowiązania $T_2=D^{t}_1$ oraz $T_1=e(A,g_2)^{-rt}_1\, e(g_1,g_2)^{t}_2$. Następnie wybieramy „losowe" wyzwanie c=H(parametry publiczne, R,T_1, T_2), gdzie H oznacza odpowiednią funkcję haszującą, natomiast w parametrach mamy klucz publiczny grupy, wiadomość, nazwę domeny i pseudonim użytkownika w danej domenie.

Podpis jest teraz trójką sig=(c, s_1, s_2), gdzie $s_1=t_1+cu$, $s_2=t_2+cr$. Przesunięcie odpowiednich wartości t_i o tą samą c-tą wielokrotność u i r odpowiednio jest kluczowe do przeprowadzenie procesu weryfikacji podpisu. Polega ona na obliczeniu

$T=e(R,Z)^{-c}\, e(R,g_2)^{-s}_1\, e(g_1,g_2)^{s}_2 = e(R,g_2)^{-cz-(t}_1{}^{+cu)\, s}_1\, e(g_1,g_2)^{t}_2{}^{+cr} = e(R,g_2)^{-c(z+u)-t}_1\, e(g_1,g_2)^{t}_2{}^{+cr}$

$=e(R,g_2)^{-cr\,-t}_1\, e(g_1,g_2)^{t}_2{}^{+cr} =e(g_1,g_2)^{-cr\,-t}_1{}^{r/z+u\,+t}_2{}^{+cr} = e(A,g_2)^{-rt}_1\, e(g_1,g_2)^{t}_2 = T_1.$

Teraz wystarczy zatem sprawdzić czy c=H(parametry publiczne, T_1, T_2) by zakończyć proces weryfikacji.

W rozdziale 4 pomysł ten jest nieco zmodyfikowany. W dalszym ciągu klucz prywatny użytkownika jest parą uSK={u, A=$g_1^{1/z+u}$}, jednak teraz autor wprowadza klucz publiczny domeny dPK. Różnica jest zasadniczo taka jak między podpisem opartym na tożsamości (ang, identity based signatures) a podpisami bazującymi na infrastrukturze klucza publicznego. Z matematycznego punktu widzenia jest to nawet prostsze, gdyż kluczową rolę odgrywa spostrzeżenie, że działanie dwuliniowe pozwala na „skolapsowany" interaktywny dowód wiedzy, polegający na sprawdzeniu czy dwa element grupy są „kodowane" tym samym sekretem. Widać to jasno w punkcie 6 fazy Setup schematu 2, rozdziału, 4.2 oraz punkcie 4 fazy Verify tegoż schematu.

Jednak kryptograficzny i obliczeniowy wymiar tego podejścia jest całkowicie różny. Po pierwsze wprowadzamy tu dodatkową infrastrukturę, ze wszystkimi jej dobrodziejstwami ale i ograniczeniami polegającymi na nieadekwatności modelu do środowiska z ograniczoną mocą obliczeniową. Ale tu mamy też miłą niespodziankę, a mianowicie dzięki takiemu podejściu autor rozprawy uzyskuje korzyść w etapie podpisywania wiadomości, gdyż jego obliczenie nie wymaga w odróżnieniu od przypadku z rozdziału 3 wykonywania działania dwuliniowego (por. punkty (a) odpowiednich faz sign). Jest to osiągnięte przez fakt, że domena D_1 nie jest dowolnym ciągiem bitów ale elementem w grupie G_2 postaci g_2^{α} i ten sam sekret α koduje wartość D_2 –patrz punkt 6 fazy Setup powyższego schematu 2. Jest to o tyle ważne, że operacje w grupie G_T są zazwyczaj bardziej czasochłonne niż operacje w G_1 i G_2. Ma to szczególne znaczenie dla kart , które nie wspierają operacji w G_T i trzeba by implementować takie operacje bez wsparcia procesora kryptograficznego, ograniczając tym samym mocno wydajność schematu. Ponadto takie podejście pozwala na częściowe odciążenie podpisującego delegując obliczenia wstępne (ang. precomputations) do obowiązków infrastruktury. Duże znaczenie może też mieć fakt możliwości zdejmowania anonimowości użytkownika przez delegowane przez managera podmioty (np. w przypadku podejrzenia o oszustwo).

W rozdziale 5 doktorant zajmuje się przypadkiem dynamicznym z ograniczonym zaufaniem do managera, który nie powinien móc wykonywać podpisu w imieniu członka grupy (ang. exculpability condition). Co więcej chodzi o to, by nie mógł on stworzyć fałszywej tożsamości, która by nie prowadziła do żadnego z członków

grupy. Dlatego ważna jest interakcja członka grupy i jej managera przy generowaniu certyfikatu jego klucza prywatnego przypominająca konstrukcję tzw. poświadczeń cyfrowych (ang. credentials). Dokładniej autor wprowadza tu dodatkową fazę protokołu zwaną Join/Issue, w której użytkownik wybiera swoją sekretną część klucza $y \in Z_p$ oraz otrzymuje na niej certyfikat postaci $A = (g_1 \cdot (g_1)^{yx})^{1/z+u}$, gdzie $z, x \in Z_p$ są sekretnymi kluczami managera grupy natomiast $u \in Z_p$ jest wybierane przez managera grupy ale przesłane podpisującemu. Wykonanie protokołu odbywa się w taki sposób, ze użytkownik nie poznaje sekretów managera grupy i vice versa. Ostatecznie podpisujący posiada trójkę (u, y, A) za pomocą której będzie mógł obliczyć pseudonim domenowy $nym=H(\text{nazwa domeny})^u g_1^y$. W ostatnim 6 rozdziale doktorant podsumowuje swoje wyniki odnosząc je do wcześniejszych prac i pokazując uzyskany w rozprawie względem nich postęp.

Wyniki naukowe rozprawy oceniam bardzo wysoko, co znajduje potwierdzenie w pracach już opublikowanych jak i tych przyjętych do publikacji: w czasopiśmie *Security and Communication Networks* (rozdział 4) oraz na konferencję *ArcticCrypt 2016* (rozdział 5).

Z uwag krytycznych miałbym jedną dotyczącą dokładniejszej analizy możliwości obliczeniowych współczesnych kart mikroprocesorowych w odniesieniu do „idealnego" systemu podpisu domenowego, dynamicznego. Dla jakiej liczby domen rozwiązanie polegające na posiadaniu przez użytkownika odrębnego klucza prywatnego i publicznego dla każdej domeny staje się niemożliwe nawet przy zastosowaniu najlepszych obecnie stosowanych technologii?

Rozprawa Pan Kamila Kluczniaka jest bardzo starannie zredagowana i dobrze napisana. Autor wprowadza odpowiednie pojęcia pierwotne określonych podpisów domenowych (ad hoc i z infrastrukturą, statycznych i dynamicznych) w sposób ścisły i pokazuje odpowiednie redukcje ich bezpieczeństwa do trudności znanych problemów obliczeniowych. Zmaga się z trudnymi zagadnieniami kryptograficznymi i obliczeniowymi uzyskując ostatecznie oryginalne, ciekawe i bardzo dobre rozwiązania. Otrzymane wyniki stanowią podstawę do rozwiązań praktycznych i implementacyjnych ważnych dla zastosowań. Problematyka rozprawy stanowi zamkniętą całość i jest przekonująca co do swej zawartości. Moim zdaniem poziom naukowy rozprawy spełnia z nawiązką wymagania stawiane pracom doktorskim.

Podsumowując uważam, że rozprawa doktorska mgr Kamila Kluczniaka dotyczy ważnych dla kryptografii zagadnień naukowych. Jego badania są dobrze umotywowane, a stosowane narzędzia badawcze ciekawe, zwłaszcza z informatycznego punktu widzenia. Praca stanowi oryginalne rozwiązanie dobrze sformułowanego problemu naukowego. Autor pokazuje w rozprawie ogólną wiedzę teoretyczną w tej dziedzinie nauki, jest dobrze zorientowany w literaturze bliskiej problematyce rozprawy i jest szczególnie kompetentny w dziedzinie badanych algorytmów i schematów kryptograficznych.

Konkludując uważam, że rozprawa Pana mgr Kamila Kluczniaka pt. *Anonymous authentication using electronic identity documents* **spełnia** wymagania artykułu 13.1 Ustawy o stopniach naukowych i tytule naukowym z dn. 14 marca 2003 roku. Może być zatem podstawą do **nadania** jej autorowi stopnia naukowego doktora nauk matematycznych w zakresie informatyki.

W związku z powyższym przedkładam Radzie Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk w Warszawie wniosek o **przyjęcie** tej rozprawy i **dopuszczenie** mgr Kamila Kluczniaka do dalszych etapów przewodu doktorskiego.

Jacek Pomykała