Prof. dr hab. Jerzy GAWINECKI
Wydział Cybernetyki
Wojskowa Akademia Techniczna

Recenzja pracy doktorskiej pt. „Anonymous Authentication Using Electronic Identity Documents" mgra Kamila KLUCZNIAKA

dla Rady Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk

Temetycznie praca odnosi się do kwestii ukrywania tożsamości w sieciach informatycznych. Bardziej szczegółowo autor, bazuje na pomyśle zaproponowanym przez niemiecką BSI, dotyczącym tzw. podpisów domenowych, który narodził się na skutek prac dotyczących rozwoju technologii dokumentów osobistych. Koncepcja podpisów domenowych została zaproponowana w celu stworzenia zarejestrowanemu użytkownikowi możliwości uwierzytelnienia wiadomości bez potrzeby ujawniania tożsamości, jednak z możliwością identyfikacji w różnych domenach. Rozważa się dwa główne rodzaje stron, mianowicie urząd rejestracyjny oraz użytkowników końcowych. Po zarejestrowaniu użytkownik końcowy otrzymuje certyfikat na swój klucz prywatny, na jego podstawie wyznacza unikalny i stały pseudonim dla każdej z domen.

Podstawowym narządziem badawczym zastosowanym przez Autora są tzw. *parowania* dwuliniowe, czyli odwzorowania przypisujące parze elementów dwóch izomorficznych grup skończonych G_1, G_2 element innej grupy skończonej tego samego rzędu. Odwzorowania te charakteryzowanie są przez własność analogiczną do dwuliniowości, ich obraz nie może być singletonem co więcej w zależności o wymaganej „*siły kryptograficznej*", dodaje się dodatkowe założenia odnośnie jednokierunkowości izomorfizmu pomiędzy G_1 oraz G_2. Ostatnie założenie, mające teoretyczny charakter, jest ważne z punktu widzenia dowodów bezpieczeństwa, gdyż wspólnie z odpowiednim założeniem o trudności obliczeniowej w grupie/pach pozwala sprowadzić problem do tej trudności. Trzeba również nadmienić, że tak zdefiniowane parowania są analogonem parowań Waila i Tate'a, znanych z teorii krzywych eliptycznych, przypisującym parom elementów odpowiednich podgrup torsyjnych element podgrupy multiplikatywnej ciała nad ktorym krzywa została zdefiniowana. Wspomniane parowania są implementowalne, zostały wykorzystane w „zerowym" pomyśle Joux odnośnie trójstronnego protokołu Diffiego-Hellmana, dalej w IBE i innych miejscach. Zwracamy uwagę na tę kwestię, gdyż aktualne zastosowania parowania, również te wykorzystane w recenzowwanej pracy, mają charakter teoretyczny bez takich możliwości implementacyjnych jak w przypadku zaprezentowanych przykładów.

Autor stara się podejść do kwestii podpisów domenowych w sposób całościowy, co prowadzi do konieczności przeanalizowania kilku przypadków i przyjęcia różnych norm klasyfikacji. Pierwszy i pojawiający się w sposób naturalny, podział odnosi się do sposobu reprezentacji domen (*ad hoc* oraz *posiadajace infrastrukturę*). Drugi odwołuje się do metody certyfikowania kluczy przez centrum autoryzacji, nazywane przez Autora „menadżerem grupy", ze znajomością odpowiednich kluczy prywatnych (*statyczny*) lub bez tej wiedzy (*dynamiczny*). Nie licząc dwóch pierwszych rozdzaiłów oraz ostatniego zawierającego wnioski, zasadnicza część pracy została zaprezentowana w trzech kolejnych rozdziałach, mianowicie trzecim, czwartym i piątym.

W Rozdziale trzecim przedstawiono model wraz z odpowiednią konstrukcją dla podpisu domenowego *ad hoc* w przypadku *statycznym*. Nowatorstwo polega na tym, że w odróżnieniu od wcześniej prezentowanego podejścia nie ma konieczności generowania kluczy domenowych, gdyż wszystkie niezbędne informacje można uzyskać za pomocą operacji matematycznych na kluczu prywatnym oraz identyfikatorze domeny. Technicznie konstrukcja opiera się na wykorzystaniu podpisu Boneh'a-Boyen'a oraz tzw. heurystyki Fiat'a-Shamira [A.Fiat, A.Shamir, How To Prove Yourself: Practical Solutions to Identification and Signature Problems, Crypto86' Lecture Notes in Computer Science no. 263, pp 186-194].

Rozdział czwarty, którego wnioski wydają się implementowane w praktyce, jest w istocie naturalnym analogonem Rozdziału trzeciego na przypadek domen posiadających infrastrukturę. Na poziomie idei nie różni on się zasadniczo od rozdziału poprzedniego. Jego realizacja wymagała jednak pokonania pewnych przeszkód natury technicznej oraz terminologicznej.

Rozdział piąty to hybryda reprezentowaności domen ad hoc, które tym razem można tworzyć na podstawie dowolnego ciągu bitów oraz przypadku dynamicznego. Wyrazem dynamiczności jest protokół `Join/Issue` pozwalający użytkownikowi zarejstrować klucz bez konieczności jego ujawnienia. Z pewnością materiał zaprezentowany w tym rozdziale wymagał głębokiej analizy problemu i przedefiniowania podejścia. Zaproponowany tam schemat podpisu znacząco różni się od dotychczasowych schematów. Wynika to przede wszystkim stąd, że jak już wspomniano encja autoryzująca nie może poznać kluczy prywatnych użytkowników oraz sekrety muszą być podzielone między tę encję oraz użytkownika który rejestruje swój klucz prywatny. Dlatego w protokole `Join/Issue` użytkownik wybiera swoją prywatną część, jako liczbę całkowitą $0 \leqslant y < p$ oraz dostaje dla niej certyfikat $A = (g_1 \cdot (g_1^y)^x)^{1/(z+u)}$, gdzie $z, x \in \mathbb{Z}_p$ są kluczami prywatnymi encji a $u \in \mathbb{Z}_p$ jest wybierane przez encję ale znane użytkownikowi. Użytkownik oraz encja autoryzująca nie znają wzajemnie swoich sekretów. Dalej, pseudonim użytkownika oblicza się jako $nym \leftarrow \mathbf{H}(\mathbf{domena})^u \cdot g_1^y$, gdzie $\mathbf{H}$ jest funkcją haszującą. Podpis konstruuje się z pomocą Σ-protokołu udowadniającego znajomość a, b, c takich, że $nym = \mathbf{H}(\mathbf{domena})^a \cdot g_1^b$ a c jest certyfikatem dla a, b.

Badawczo praca jest na wysokim poziomie, użyte metody wpisują się w ogólny tręd rozważań dotyczących zastosowania parowania dwuliniowego. Uzyskane wyniki są interesujące i z pewnością zostaną zauważone przez środowisko naukowe zainteresowane

prezentowaną tematyką. Potwierdza to fakt, że wyniki rozdziału czwartego uzyskały pozytywną recenzję i zostały przyjęte do druku w czasopiśmie Security and Communication Networks (Impact Factor 0.72) a wyniki rozdziału piątego zostały zaakceptowane na konferencję ArcticCrypt 2016.

Pomijając drobne błędy zecerskie oraz niewielkie usterki techniczne do których nie zamierzamy się odnosić, główny zarzut kierujemy w stronę podstawowego narzędzia wykorzystanego w pracy, czyli parowania. Jak wspomnieliśmy wcześniej, aplikowalne kryptograficznie parowania to parowania zadane na podgrupach torsyjnych krzywych eliptycznych. Można zatem zaryzykować stwierdzenie, że ewentualna praktyczna realizacja zaprezentowanych wyników również będzie wykorzystywać te pojęcia. W związku z tym spodziwealiśmy się bardziej pogłębionej analizy odnośnie tych kwestii. Nie udało się znaleźć żadnej wzmianki łączącej ideę parowania z podgrupami punktów krzywych eliptycznych co, jak wspomnieliśmy wcześniej, jest właściwie esencją tego pomysłu. Co więcej nie do końca jest jasne dlaczego autor ogranicza się jedynie do krzywych eliptycznych nad ciałami prostymi, wydaje się, że założenie takie nie jest konieczne. Podobnie nie jest zrozumiałe mało realistyczne założenie, że grupa punktów krzywej eliptycznej ma mieć rząd pierwszy. Prawdopodobnie chodziło Autorowi o podgrupę rzędu pierwszego.

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

DZIEKAN
WYDZIAŁU CYBERNETYKI WAT
prof. dr hab. n. mat. inż. Jerzy GAWINECKI