UNIWERSYTET
WARSZAWSKI

Wydział Matematyki,
Informatyki i Mechaniki

dr hab. Stefan Dziembowski
profesor
Instytut Informatyki
Uniwersytet Warszawski
ul. Banacha 2
02-097 Warszawa
S.Dziembowski@crypto.edu.pl
tel.: +48 22 55 44 154

Warszawa, 1 listopada 2015

Recenzja rozprawy doktorskiej mgra Lucjana Hanzlika pod tytułem „Cryptographic Protocols for Modern Identification Documents"

Omówienie zawartości pracy wraz z jej oceną

Złożona praca dotyczy problemu konstrukcji algorytmów kryptograficznych przeznaczonych dla nowoczesnych dokumentów tożsamości. Autor skupia się na niemieckim projekcie *Neuer Personalausweis* (nPA). Jest to zdecydowanie ważna i ciekawa dziedzina nauki, w której dotychczas polskie instytucje naukowe miały ograniczony udział. Fakt, że autor zdecydował się na podjecie badań w tej tematyce, oraz uzyskał wyniki na światowym poziomie zasługuje na duże uznanie. Praca zawiera następujące rezultaty:

- Rozszerzenie protokołu *Password Authenticated Connection Establishment - Generic Mapping* (PACE-GM) zaproponowanego przez niemieckie Federalne Biuro Bezpieczeństwa Informacyjnego (niem.: *Bundesamt für Sicherheit in der Informationstechnik*, BSI). Rozszerzenie to pozwala na uzyskanie autentykacji dokumentu względem czytnika, kosztem zaledwie jednego mnożenia modulo (poprzednie rozwiązania wymagały w tym celu jednego wywołania algorytmu podpisu cyfrowego). Warto zaznaczyć, że w tak praktycznej dziedzinie jaką jest konstrukcja cyfrowych dokumentów, nawet drobne z pozoru usprawnienia mają kolosalne praktyczne znaczenie, gdyż przenoszą się na znaczące oszczędności w kosztach konstrukcji sprzętu (z uwagi na efekt skali).

  Podobne rozszerzenie zostało zaproponowane równolegle (choć z innym dowodem bezpieczeństwa i w oparciu o inne założenia) przez BSI i najprawdopodobniej wejdzie do masowego użytku w najbliższych latach jako standard Organizacji Międzynarodowego Lotnictwa Cywilnego (ang.: *International Civil Aviation Organization*, ICAO) o nazwie PACE-CAM.

  Moim osobistym zdaniem fakt, że podobne wyniki zostały jednocześnie uzyskane przez kogoś innego, jest silnym argumentem na korzyść autora, bo dowodzi, że zajmuje się on ważną dziedziną i podejmuje ambitne cele, a także, że nie boi się związanego z tym ryzyka.

UNIWERSYTET
WARSZAWSKI

Wydział Matematyki,
Informatyki i Mechaniki

dr hab. Stefan Dziembowski
profesor
Instytut Informatyki
Uniwersytet Warszawski
ul. Banacha 2
02-097 Warszawa
S.Dziembowski@crypto.edu.pl
tel.: +48 22 55 44 154

- Rozszerzenie protokołu PACE kompatybilne także z protokołem *Password Authenticated Connection Establishment - Integrated Mapping* (PACE-IM). Jest to ważne, ponieważ protokół ten jest bardziej wydajny.

- Propozycja nowego mechanizmu, nazwanego w pracy *Uwierzytelnianiem Pseudonimowym* (ang. *Pseudonymous Identification*). Jest to schemat identyfikacji oparty o jeden klucz prywatny, który pozwala tworzyć wiele różnych pseudonimów, które mogą być użyte do różnych domen aktywności. Podobne idee pojawiły się już wcześniej w niemieckim nPA. Autor pokazuje, że wymagają rozwiązania z nPA wymagają silnych założeń odnośnie bezpieczeństwa używanego sprzętu oraz zaufania do organu wydającego dokument, a następnie pokazuje protokół który pozwala pozbyć się tych założeń. Uważam to za bardzo ważny wkład w stan wiedzy, zwłaszcza, że wymaganie zaufania do organu wydającego może skutecznie ograniczać praktyczne zastosowania uwierzytelniania pseudonimowego.

Praca oparta jest na współautorskich publikacjach na konferencjach *ISPEC'2013* i *TrustCom'2012*, w czasopiśmie *Journal of Universal Computer Science*, oraz dwóch nieopublikowanych manuskryptach. Według mojej osobistej oceny (a także wg. dostępnych rankingów) powyższe konferencje i czasopismo nie należą do pierwszej ligi konferencji i czasopism dotyczących kryptografii oraz praktycznego bezpieczeństwa. Mam jednak wrażenie, że w pewnym sensie jest to pochodna tematyki której dotyczy doktorat. W przypadku tak praktycznych zagadnień jak optymalizacja protokołów kryptograficznych bardziej liczy się wpływ wyników na rzeczywistość, niż konkretne miejsce opublikowania wyników. Z tego punktu widzenia praca pana Hanzlika prezentuje się znakomicie: protokoły zaproponowane w pracy weszły do standardów ICAO i najpewniej zostaną zaimplementowane na masową skalę w paszportach elektronicznych[1]

Uwagi dotyczące dowodów bezpieczeństwa oraz dowiedzionych twierdzeń

O ile sama waga naukowa otrzymanych rezultatów nie budzi moich najmniejszych wątpliwości, to jednak pewne rozczarowanie może powodować jakość techniczna złożonej rozprawy. W szczególności, cześć dowodów bezpieczeństwa wydaje się niekompletna i przekonanie się o ich poprawności wymaga od czytelnika wysiłku wykraczającego poza zwyczaje

[1] Z pewną przykrością odnotowuję, że dokument ICAO zawierający opis tych protokołów, zatytułowany *Machine Readable Travel Documents* (wersja 1.1, datowana 15.04.2014) nie zawiera odwołania do prac pana Hanzlika, a jedynie do prac naukowców z BSI. O ile dobrze rozumiem wynika to z faktu wcześniejszego opatentowania przez BSI tego protokołu. Z punktu widzenia oceny akademickiej wartości pracy pana Hanzlika nie powinno to mieć jednak znaczenia.

UNIWERSYTET
WARSZAWSKI

Wydział Matematyki,
Informatyki i Mechaniki

dr hab. Stefan Dziembowski
profesor
Instytut Informatyki
Uniwersytet Warszawski
ul. Banacha 2
02-097 Warszawa
S.Dziembowski@crypto.edu.pl
tel.: +48 22 55 44 154

przyjęte w informatyce (nawet te dotyczące prac konferencyjnych, o pracach czasopismowych i rozprawach doktorskich nie wspominając). Podkreślam, że jest to jedynie efekt pewnej niestaranności autora, a same dowody (po uzupełnieniu) wydają się być poprawne.

Przykładowo, w dowodzie Twierdzenia 3.4 w części *Impersonation execution* brakuje analizy tego co dzieje się w przypadku gdy symulator $\mathcal{R}$ otrzyma na wejściu krotkę która nie jest "invDDH". Aby dowód zadziałał konieczne jest pokazanie, że wówczas przeciwnik ma zaniedbywalne prawdopodobieństwo oszukania symulatora. Przekonanie się, że tak rzeczywiście jest wymaga od czytelnika samodzielnej analizy jakie wiadomości w symulowanej egzekucji otrzymuje przeciwnik i dokonania spostrzeżenia, że są one niezależne od zmiennej r. Niestety w pracy autor nie komentuje tego w żaden sposób, co w pierwszej chwili może wywołać u czytelnika (niesłuszne) podejrzenie, że w dowodzie jest błąd, polegający na pominięciu ważnego przypadku.

Innym przykładem może być stwierdzenie zawarte w pracy, że do dowodu bezpieczeństwa PACE i SPACE|AA wystarczy założenie, że schemat (Enc, Dec) jest bezpieczny w sensie "CPA". Niestety w ogólności tak nie jest. Aby to wykazać załóżmy, że (Enc, Dec) jest takie, że przed zaszyfrowaniem dodana jest sztucznie redundancja do wiadomości (np. dodanych jest do wiadomości 100 zer). Jeśli przeciwnik pozna $z = Enc(H(0||\pi), s)$, to może łatwo przeprowadzić atak słownikowy polegający na próbowaniu wszystkich możliwych haseł, aż do otrzymania wiadomości zaczynającej się od 100 zer, a zatem schemat PACE nie jest w tym wypadku bezpieczny. Oczywiście w praktyce nie jest to problemem, ponieważ powyższy atak nie jest możliwy jeśli użyty zostanie schemat (Enc, Dec) które nie ma tej własności. Tym niemniej brak tego założenia pokazuje na to, że od strony formalnej praca została napisana trochę niestarannie.

Drobne uwagi edytorskie

Praca zawiera też niestety sporo drobnych literówek oraz błędów edytorskich, które, choć łatwo naprawialne, w sposób znaczący utrudniają jej zrozumienie.

Przykładowo, w pracy nie określono co jest wynikiem działania niektórych protokołów. Co gorsza, czytelnik może mieć problemy z poprawnym odgadnięciem co tym wynikiem powinno być. Np. w protokole PACE nie wiadomo, czy jest to K'_{SC} (ponieważ na stronie 35 w punkcie 10 jest napisane 'use K'_{SC} as the session key"), czy raczej K_{Enc} i K_{Mac} (ponieważ w punkcie 7 na tej samej stronie to te wartości określane są one jako "session keys")? Podobnie wątpliwości nasuwają się w przypadku protokołu SPACE|AA.

Ponadto, w protokołach PACE|AA (Fig. 3.1) i SPACE|AA (Fig 3.2) niezdefiniowane są następujące zmienne: Y'_A, y'_A, Y'_B, y'_B, w zawiązku z czytelnikowi może być trudno zrozumieć te protokoły w całości. Co prawda można domyślić się, że indeksy A i B powinny być zastąpione odpowiednio przez R i C, tym niemniej od pracy doktorskiej oczekiwałbym większej staranności.

UNIWERSYTET
WARSZAWSKI

Wydział Matematyki,
Informatyki i Mechaniki

dr hab. Stefan Dziembowski
profesor
Instytut Informatyki
Uniwersytet Warszawski
ul. Banacha 2
02-097 Warszawa
S.Dziembowski@crypto.edu.pl
tel.: +48 22 55 44 154

Z innych drobnych usterek edytorskich: numeracja rozdziałów 3 i 4 w żywej paginie jest błędna (w rozdziale n-tym napisane jest "Chapter $n+1$"), co również może prowadzić do konfuzji u czytającego.

Konkluzja

Uważam, że złożona rozprawa mgra Lucjana Hanzlika bez wątpienia spełnia z nawiązką wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora w dziedzinie nauk technicznych w zakresie nauk matematycznych. Kwestią którą budzi nieco więcej moich wątpliwości jest wyróżnienie rozprawy. Z jednej strony silnym argumentem za takim wyróżnieniem jest waga wyników oraz ich związek z zastosowaniami praktycznymi. Z drugiej strony przeciw wyróżnieniu przemawia omówiona wyżej pewna niestaranność techniczna. Po rozważaniu argumentów za i przeciw wnioskuję jednak o wyróżnienie rozprawy.

Stefan Dziembowski
Instytut Informatyki UW