Warszawa dn. 20-03-2015

Prof. UW Jacek Pomykała

Instytut Matematyki Wydziału

Matematyki Informatyki i Mechaniki

Uniwersytetu Warszawskiego

Recenzja rozprawy doktorskiej **mgr Anny Lauks-Dutki**

pt. *Applied Cryptographic Schemes based on Discrete logarithm Problem*

dla Rady Naukowej Instytutu Podstaw Informatyki Polskiej Akademii Nauk w Warszawie

Recenzowana rozprawa doktorska mgr Anny Lauks-Dutki (o objętości 114 stron) została napisana w języku angielskim i dotyczy zasadniczo schematów kryptograficznych bazujących na problemie logarytmu dyskretnego. Przedmiotem badań doktorantki są formalne modele, konstrukcje i analiza bezpieczeństwa trzech schematów podpisu cyfrowego oraz protokołu trasowania cebulkowego z wykorzystaniem idei uniwersalnego re-szyfrowania. Celem rozprawy jest nie tylko stworzenie nowych propozycji dla wybranych funkcjonalności i protokołów kryptograficznych, lecz także osiągnięcie postawionych wymagań na możliwie najprostszej drodze. Dla schematów podpisu cyfrowego taką drogę wskazuje już klasyczny schemat szyfrowania oraz podpisu ElGamala. Z kolei w metodzie trasowania cebulkowego zostały zaproponowane rozwiązania bazujące na problemie logarytmu dyskretnego z uwzględnieniem idei uniwersalnego re-szyfrowania oraz idei kumulacji podpisów cyfrowych. Wyniki zawarte w rozprawie pochodzą w większości z prac współautorskich doktorantki, jednak został wyraźnie wyszczególniony jej wkład własny w podanych publikacjach. Praca składa się z 3 części. Część pierwsza jest poświęcona modelom bezpieczeństwa, trudnym problemom obliczeniowym oraz podstawowym pierwotnym pojęciom kryptograficznym. Na część drugą składają się 3 wybrane schematy podpisu cyfrowego tj. podpis warunkowy, dedykowany i modyfikowalny. Część trzecia jest poświęcona wybranym protokołom anonimizacji i ich analizie.

Prezentowane wyniki są ułożone w sposób logiczny i przejrzysty z uwzględnieniem standardu- od ogółu do szczegółu oraz od opisu do formalnej definicji. Wyjątkowo obszerny spis cytowanych pozycji bibliograficznych dowodzi, że autorka doskonale porusza się w omawianej problematyce

kryptograficznej. Pragnę też stwierdzić, że tematyka rozprawy jest bardzo aktualna i zajmują się nią uczeni z wielu ośrodków naukowych krajowych i zagranicznych.

Problematyka podpisów cyfrowych warunkowych , dedykowanych i modyfikowalnych omawianych w rozprawie zasadniczo opiera się na idei klucza wymiany Diffie-Hellmana, na którym jest oparty system szyfrujący ElGamala oraz standardzie DSS pochodzącym od podpisu ElGamala, pomijając rolę haszowania kameleona oraz idei kumulatora czy filtru Blooma w przypadku podpisów modyfikowalnych. Z matematycznego punktu widzenia zasadniczą rolę w prezentowanej rozprawie pełni pojęcie tzw. pre-podpisu (ang. presignature). Bardzo prosta i elegancka idea wykorzystana przez doktorantkę pochodzi od systemu ElGamala. Wykorzystywany jest tu fakt, że szyfrowanie zależy od elementu losowego k=k mod q oraz, że przekształcenie szyfrujące jest homomorficzne tj. $E_y(mm')= E_y(m') E_y(m')$. Przypomnijmy, że kryptogram/podpis ma postać pary (a, b), gdzie a jest zobowiązaniem losowej wartości k tj. $a=g^k$ (mod p), natomiast właściwy szyfrogram jest postaci b=b(m, x, k), gdzie x jest kluczem prywatnym, natomiast $y=g^x$ odpowiadającym mu kluczem publicznym. Wiadomość m jest elementem grupy Z_p^*. W przypadku systemu szyfrowania mamy $b=my^k$ natomiast podpisu cyfrowego $b= k^{-1}[h(m) –xa]$ mod q, gdzie q jest dużym dzielnikiem pierwszym liczby p-1. Na parametry kryptosystemu składa się więc czwórka (p, q, g , G), gdzie G jest odpowiednią podgrupą grupy Z_p^*.

Dla podpisu ElGamala pre-podpis $s_1=(a_1, b_1)$ jest postaci $(a_1, b_1S_2^z, a_2^z)$ gdzie parę $[b_1S_2^z:= b_1(a_2^{b}{}_2)^z, a_2^z]$ można traktować jako szyfrogram ElGamala dla wiadomości b_1 przy użyciu klucza (publicznego) S_2 z zastosowaniem elementu losowego $z=z$(mod q). W takim przypadku jeśli uzyskamy dostęp do wartości b_2 to rozszyfrowując go obliczymy b_1 i w konsekwencji s_1. Tak więc posiadając podpis $s_2=(a_2, b_2)$ pod pewną wiadomością m_2 można go wykorzystać do obliczenia podpisu $s_1=(a_1, b_1)$ na podstawie pre-podpisu $(a_1, b_1S_2^z, a_2^z)$. Dodajmy, że w przypadku podpisu dedykowanego a_1 jest k-tą potęgą klucza publicznego dedykowanego odbiorcy podpisu, co w oczywisty sposób powoduje, że silna weryfikacja podpisu jest możliwa przy znajomości klucza prywatnego odpowiadającego danemu kluczowi publicznemu.

Autorka rozprawy ściśle definiuje odpowiednie pojęcia pierwotne- podpisu warunkowego i dedykowanego, pokazuje korzyści z ich zastosowania i dowodzi redukcji bezpieczeństwa do problemu logarytmu dyskretnego/problemu Diffie-Hellmana. W szczególności pomysł zastosowania pre-podpisu można wykorzystać dla warunkowego deszyfrowania, o którym jest mowa w sekcji 3.4.1 rozprawy. Zasługą doktorantki jest też rozszerzenie protokołu podpisu dedykowanego na przypadek wielu odbiorców omawiany w rozdziale 4.5.

Ważnym wkładem doktorantki jest także zaproponowane użycie jednokierunkowego kumulatora zastępującego haszowanie kameleona w podpisie modyfikowalnym. Przypomnijmy, że taki kumulator bazuje na pojęciu funkcji quasi-przemiennej tj. $f: X \times Y \rightarrow X$ spełniającej warunek: $f(f(x, y_1), y_2)= f(f(x, y_2), y_1)$ dla dowolnych $x \in X$ i $y_i \in Y$, oraz $i \leq k$, która jest bezkolizyjna w tym sensie, że dla danych (x, y) trudno jest obliczyć (x',y') takie, że f(x, y)= f(x', y'). Jeśli teraz y_i będą haszami „modyfikowanych" wiadomości m_i , to taki kumulator wraz z odpowiednim świadectwem odpowiadającym k-1 –szej iteracji funkcji f pozwala potwierdzić, że odpowiednia wartość m_j pojawia

się w kumulatorze. We wcześniej zaproponowanych rozwiązaniach to właśnie haszowanie kameleona pozwalało na znalezienie odpowiednich kolizji dla modyfikowanych wiadomości częściowych i tym samym poprawnej weryfikacji podpisu całej wiadomości.

W rozprawie doktorskiej mgr Anna Lauks-Dutka stosuje kumulator polegający na (jednokierunkowym) podnoszeniu do potęgi będącej iloczynem odpowiednich haszy wiadomości modyfikowalnych modulo liczba złożona, pokazując korzyści jakie stąd wypływają. Sygnatariusz autoryzuje podpisem wartość kumulatora dokumentu M. Cenzor (modyfikujący dokument) posiadając wartości odpowiednich świadectw i kumulatora jest w stanie udowodnić w czasie weryfikacji, że wiadomość częściowa m_j należy do zbioru wiadomości dopuszczonych do modyfikacji. Z matematycznego punku widzenia kluczem do zrozumienia działania „kumulacji" jest fakt, że jeśli x^{ab} (mod n) jest „zobowiązaniem" to można łatwo udowodnić, że *a* lub *b* jest dzielnikiem wykładnika, obliczając $(x^{a})^{b}$ (mod n) lub $(x^{b})^{a}$(mod n) , ale nie udowodnimy tego o *c* różnym od *a i b o ile* nie znamy nietrywialnej faktoryzacji *a* lub *b,* ani nie znamy wielokrotności rzędu elementu x *mod n*. Warto też zauważyć korzyści z dodatkowych restrykcji jakie można narzucić na liczbę modyfikacji i nieodróżnialności przez weryfikującego wiadomości modyfikowanych od niemodyfikowanych (silna transparentność), o których mowa jest w sekcji 5.7.

Ostatnia część pracy dotycząca anonimizacji jest motywowana głównie analizą protokołu trasowania cebulkowego. Anonimowość odnosi się zasadniczo do nieodróżnialności (z punktu widzenia atakującego) kryptogramów rekodowanych, wychodzących z ustalonego węzła w tej samej rundzie protokołu. Kluczowy wkład doktorantki dotyczy metody uniwersalnego re-szyfrowania bazującej na problemie logarytmu dyskretnego. Pokazuje rozwiązanie dające odporność schematu na tzw. atak powtórzeniowy i atak przekierowujący, ale także na wybrane ataki aktywne tj. takie, w których przeciwnik całkowicie kontroluje pewną liczbę węzłów z możliwością modyfikowania danych z nich wychodzących. W zaproponowanym rozwiązaniu przeciwnik nie jest w stanie rejestrować powtórzeń w wykonaniu protokołu, a jedynie może stwierdzić, że przekierowywane wiadomości są ułożone w tej samej kolejności.

Re-szyfrowanie jest wykorzystane przez doktorantkę w rozbudowanej, wyrafinowanej formie i jest przeprowadzane kaskadowo tj. klucz publiczny w protokole jest skumulowany do iloczynu kluczy publicznych kolejnych odbiorców odsłanianych kryptogramów. Kluczową własnością rozpatrywanej kumulacji jest komutowanie odpowiednich operacji częściowego deszyfrowania i re-szyfrowania kryptogramu.

Magister Anna Lauks-Dutka umiejętnie wykorzystuje tu możliwości, jakie w tym zakresie daje krytosystem ElGamala. Przyjmując, że (*a*, b)= (g^{k}, my^{k}) jest parą (wskazówka, kryptogram wiadomości) rozważamy drugą podobną (*a'*, b')= ($g^{k'}$, $1y^{k'}$), gdzie m=1, natomiast k' jest losowym elementem mod q. Domnóżmy pierwszą wskazówkę przez losową potęgę drugiej wskazówki $(g^{k'})^{k''}$, natomiast pierwszy kryptogram przez tę samą potęgę drugiego kryptogramu. Wtedy odpowiednia para jest postaci [a $(a')^{k''}$, b $(b')^{k''}$] i jest parą kodującą tę samą wiadomość *m* przy użyciu tego samego klucza publicznego *y*. Podobnie podnosząc drugą wskazówkę do losowej potęgi l'' i drugi kryptogram do tej samej potęgi l'' otrzymamy parę [$(a')^{l''}$, $(b')^{l''}$] kodującą wiadomość *m*=1 przy użyciu klucza publicznego *y*. Wtedy czwórka: [a $(a')^{k''}$, b $(b')^{k''}$; $(a')^{l''}$, $(b')^{l''}$] jest czwórką re-szyfrującą wiadomość *m* i jak widać do jej konstrukcji wymagana była tylko znajomość losowych elementów k'' i l''. Obliczenie *m* jest tu kwestią zauważenia, że b $(b')^{k''}$= my^{k} $(y^{k'})^{k''}$=m y^{k} $y^{k'k''}$=m$y^{k+k'k''}$, natomiast *a*

$(a')^{k''} = g^{k} (g^{k'})^{k''} = g^{k+k'k''}$, więc podnosząc drugą współrzędną powyższej czwórki do potęgi *x* i wykonując dzielenie pierwszej przez drugą otrzymujemy wartość *m*.

Rozprawa doktorska jest bardzo starannie zredagowana. Zauważyłem jedynie nieliczne usterki:

Str. 24-25: jest niekonsekwencja w oznaczeniach na str. 24 alfa jest wskazówką natomiast beta szyfrogramem wiadomości, a dalej role alfa i beta zmieniają się na przeciwne

Str. 28: *g* ma chyba rząd (p-1)/2 ?

Str. 55, 10 linia od dołu: nadmiarowe jest „the"

Str. 85 linia 13 od dołu: błędny zapis „addressee"

Mam kilka uwag krytycznych dotyczących całości rozprawy.

- W sekcji 3.4.1 doktorantka nie wspomina nic o możliwości deszyfrowania wiadomości w oparciu o podpisy cyfrowe dowolnych grup uprzywilejowanych (nie tylko progowych) i tzw. szyfrowania dedykowanego politykom dostępu (ang. policy based encryptions).

- Autorka wykorzystuje pierścień Z_n (dla n złożonego) do konstrukcji kumulatora (rozdział 2.4) nie wspominając o problemie logarytmu dyskretnego w Z_n^* ?

- Naturalne wydaje się pytanie czy funkcjonalności jakie rozważa doktorantka są do osiągnięcia w innych strukturach algebraicznych niż omawiane podgrupy grupy modularnej Z_n^* i czy warto się ewentualnie nimi zajmować z praktycznego punktu widzenia? W szczególności dotyczy to tak modnej w ostatnich latach kryptografii bazującej na iloczynach dwuliniowych?

Podsumowując uważam, że rozprawa doktorska mgr Anny Lauks-Dutki dotyczy ważnych dla kryptografii zagadnień naukowych. Jej badania są dobrze umotywowane, a stosowane narzędzia badawcze ciekawe, zwłaszcza z informatycznego punktu widzenia. Praca stanowi oryginalne rozwiązanie dobrze sformułowanego problemu naukowego. Autorka pokazuje w rozprawie ogólną wiedzę teoretyczną w tej dyscyplinie nauki, jest dobrze zorientowana w literaturze bliskiej problematyce rozprawy i jest szczególnie kompetentna w dziedzinie badanych algorytmów i schematów. Otrzymane wyniki są bardzo dobrze zaprezentowane i zredagowane, a problematyka rozprawy stanowi zamkniętą całość i jest przekonująca co do swej zawartości. Moim zdaniem poziom naukowy rozprawy spełnia z nawiązką wymagania stawiane pracom doktorskim.

Konkludując uważam, że rozprawa *Applied Cryptographic Schemes based on Discrete logarithm Problem* **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 autorce 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 Anny Lauks-Dutki** do dalszych etapów przewodu doktorskiego.

Jacek Pomykała