RECENZJA ROZPRAWY DOKTORSKIEJ MGR ANNY LAUKS-DUTKI

ZBIGNIEW JELONEK

Rozprawa pani mgr Anny Lauks-Dutki wykorzystuje techniki szyfrowania asymetrycznego do zwiększenia funkcjonalności podpisu cyfrowego.

Przypomnijmy tu, że niegdyś podstawową techniką szyfrowania było szyfrowanie symetryczne za pomocą tajnego klucza, który był znany zarówno nadawcy jak i odbiorcy. Główną słabością takiego rozwiązania była metoda przekazania klucza. Stąd pojawiły się idee szyfrowania asymetrycznego, w którym pewne wiadomości o kluczu można było przesylać jawnie nie zdradzając klucza, a przekazując przy tym informacje wystarczające do rozszyfrowania wiadomości. Jedną z takich metod jest tzw. metoda El Gamala. U jej podstaw leży powszechne przekonanie, że pewne reprezentacje grupy cyklicznej $G_q = \mathbb{Z}/(q)$ posiadają tak zwaną własność Diffiego-Hellmana, tj. jeśli znamy generator g tej grupy i elementy g^x, g^y tej grupy, to niemożliwe jest efektywne (tzn. w rozsądnym czasie) obliczenie elementu g^{xy}.

Jeśli grupa G_q ma taką własność to można łatwo zaszyfrować element $m \in G$ (wiadomość). Istotnie złóżmy, że chcemy przesłać wiadomość m od Alicji do Boba. Alicja wybiera swój tajny klucz $x \in \mathbb{Z}$ (x jest tego rzędu co q) i publikuje klucz publiczny $y = g^x$. To samo robi Bob - wybiera swój klucz prywatny x' i publikuje klucz publiczny $y' = g^{x'}$. Teraz Alicja przesyła wiadomość $m' := m(y')^x$ a Bob ją dekoduje $m = m'/y^{x'}$.

Tą samą technikę można wykorzystać do stworzenia podpisu cyfrowego. W rozprawie do tego celu użyta jest (standardowa) reprezentacja G_q grupy $\mathbb{Z}/(q)$ jako podgrupy grupy multiplikatywnej ciała skończonego $\mathbb{F}_p$. Elementy tej grupy możemy traktować jako liczby naturalne - reszty z dzielenia przez p, a mnożenie to mnożenie modulo p. Załóżmy teraz, że chcemy podpisać wiadomość m którą Alicja przesłała używając klucza prywatnego x. Niech g będzie generatorem grupy G_q. Alicja wybiera nowy klucz prywatny k (tylko do podpisu). Niech $a := g^k$ będzie nowym kluczem publicznym. Weźmy $t = k^{-1} mod\ q$ i $b := t(H(m) - xa) mod\ q$, gdzie H jest pewną funkcją haszującą o wartościach całkowitych. Podpisem jest para liczb (a, b). Zauważmy, że

$$y^a a^b = g^{H(m)} mod\ p$$

i ta własność charakteryzuje podpis cyfrowy.

Praca mgr Anny Lauks-Dutki w zakresie podpisu cyfrowego wykorzystuje metodę El Gamala w dwojaki sposób:

1) został stworzony model podpisu warunkowego, w którym stosuje się szyfrowanie El Gamala do stworzenia pre-podpisu, który zawiera część zaszyfrowanego podpisu. Cechą charakterystyczną tego warunkowego podpisu cyfrowego jest to, że weryfikacja podpisu jest możliwa wyłącznie w przypadku istnienia podpisu elektronicznego dla innej wiadomości, jest on w pewnym sensie kluczem do wydobycia tego podpisu. Podano też analizę możliwych ataków na ten system.

2) W modelu podpisu dedykowanego autor wykorzystuje fakt, że podpis cyfrowy zawiera pewną nadokreśloność- w istocie mamy nieskończoną ilość równoprawnych podpisów (w zależności od wyboru losowego parametru k). Model pozwala odtworzyć podpis

cyfrowy określonej osobie, ale tylko jeden z nich powiązany z kluczem prywatnym tej osoby. Zatem ujawnienie podpisu wskazuje tą osobę. Ten trick bardzo mi się podoba, jest prosty i pomysłowy. Rozprawa zawiera również pewne rozszerzenia schematu pozwalajçe np. dedykowa podpis grupie osób. Wykorzystuje się tu metody dzielenia sekretu. Tutaj funkcja kary (ujawnienia tożsamości itd.) uruchomiona zostaje, kiedy wszyscy bądź też pewna podgrupa dedykowanych weryfikujcych ujawni podpisy pod dedykowanymi im wiadomościami.

Rozprawa zawiera też ulepszenie znanego w literaturze podpisu modyfikowalnego. Cechą charakterystyczną zaprezentowanych w rozprawie rozszerzonych podpisów modyfikowalnych jest możliwość automatycznego ograniczenia zakresu wprowadzanych przez cenzora modyfikacji. Narzędziem tutaj są akumulatory kryptograficzne oraz filtry Blooma do wprowadzenia ograniczonego zbioru modyfikacji konkretnej czci wiadomości, metodę wymuszenia ma cenzorze wprowadzania dokładnie tych samych modyfikacji wiadomości w wybranych częściach modyfikowalnych, schemat z progiem pozwalajcy cenzorowi wykonać modyfikacje na k z n potencjalnie modyfikowalnych częściach wiadomości (tu podobnie jak w podpisach dedykowanych zastosowana została funkcja kary- utraty klucz prywatnego za modyfikacje w więcej niż k częściach).

W końcu w zakresie anonimowej komunikacji głównym celem rozprawy byo opracowanie schematów odpowiednich dla środowisk rozproszonych i odpornych na pewne klasy ataków i wydaje się, że przynajmniej częściowo to się udało.

Zalety rozprawy:

Autorka używa prostych algebraicznych konstrukcji do stworzenia użytecznych w praktyce, ciekawych algorytmów. Autorka biegle opanowała metody szyfrowania oparte na metodzie El Gamala w podgrupie grupy multiplikatywnej ciała $\mathbb{F}_p$ i widać , że ma tu bardzo dobre intuicje.

Autorka prostymi środkami potrafi badać złożone problemy dotyczące np. anonimowej komunikacji.

Wady rozprawy:

1) Brakuje przykładowych implementacji podanych algorytmów, zamiast tego są opisy algorytmów w pseudokodzie.

2) Brakuje choćby słowa na temat złożoności obliczeniowej proponowanych algorytmów.

3) Autorka nie podaje zakresu stosowalności swoich metod, brakuje tu oszacowania bezpiecznych w użyciu liczb pierwszych p, q itd. Co prawda autorka wspomina o metodzie indeksu, czyli prawdopodobnie jest świadoma faktu, że stosowana przez nią metoda El Gamala może być złamana za pomocą metod o podwykładniczej złożoności, ale nie jest to należycie zaznaczone.

4) W części pracy autorka stosuje nadmierny formalizm, a tam gdzie jest on naprawdę potrzebny tego formalizmu nie ma. Niech przykładem będzie tu główna definicja podpisu cyfrowego! Tak jak jest ona zapisana na stronie 26 nie ma ona sensu. Jeśli g jest generatorem podgrupy G grupy $\mathbb{Z}/(p)^*$ to wyrażenia $g^k mod\ p$, czy też y^a formalnie nie mają sensu. Te nieprawidłowości zmusiły recenzenta do przydługawego (ale ścisłego wstępu do tej recenzji, gdzie wprowadzam ten podpis poprawnie!). Również tabelka na górze tej strony nie jest poprawna : np. powinno być $H(m) = bk + xamod\ q$ a nie $H(m) = bk + xa$, itd.

5) Rozczarowuje brak odniesień do metody El Gamala opartej na grupie punktów krzywej eliptycznej nad ciałem skończonym. Powszechnie obecnie uznaje się wyższość tej metody nad metodą zaprezentowaną w tej rozprawie. Przede wszystkim wydaje się , że metoda indeksu nie ma tutaj zastosowania (przynajmniej dla ogólnych krzywych eliptycznych), a zatem liczby pierwsze które się tu pojawią mogą być znacznie mniejsze, co ma niebagatelne znaczenie w zastosowaniach. Ponadto krzywe eliptyczne oferują pewne naturalne podpisy cyfrowe oparte na uogólnionych iloczynach Weila, wydaje się, że mogą one być z powodzeniem zastosowane przy podobnych konstrukcjach jak w rozprawie.

Podsumowując uważam że rozprawa zawiera ciekawe elementy i mimo usterek o których napisałem spełnia wszystkie wymogi Ustawy o tytule naukowym i stopniach naukowych konieczne do uzyskania stopnia doktora.

(Z. Jelonek) Instytut Matematyczny, Polska Akademia Nauk, Śniadeckich 8, 00-956 Warszawa, Poland

E-mail address: najelone@cyf-kr.edu.pl