prof. dr hab. Mirosław Kutyłowski
Instytut Matematyki i Informatyki
Politechnika Wrocławska

Wrocław, 14.9.2014

Ocena rozprawy habilitacyjnej i dorobku dra inż. Jerzego Pejasia

Niniejsza opinia sporządzona została w związku z powołaniem mnie, zgodnie z decyzją Centralnej Komisji ds Stopni i Tytułów na recenzenta w postępowaniu o nadanie dr inż. Jerzemu Pejasiowi stopnia dra hab. toczącym się na Zachodniopomorskim Uniwersytecie Technologicznym, nr pisma WI/HAB.-12/2014.

Ocena

Po przeanalizowaniu rozprawy i dorobku naukowego dra inż. Jerzego Pejasia z przykrością stwierdzam, iz moim zdaniem przedstawiona rozprawa habilitacyjna i dorobek naukowy

nie dają podstaw do nadania stopnia dr habilitowanego.

W mojej opinii przedstawiona rozprawa habilitacyjna i pozostały dorobek *stanowią wkład autora w rozwój dyscypliny naukowej* będącej przedmiotem badań Kandydata, jednak z całą pewnością nie jest to wkład **znaczny**, a tym samym nie są spełnione warunki Ustawy. Wkład ten oceniam jako bardzo ograniczony i nie przekraczający wkładu wymaganego przy ubieganiu się o stopień doktora.

Uzasadnienie

Rozprawa habilitacyjna - zawartość merytoryczna

Kandydat wskazuje monografię "Schematy podpisu cyfrowego z jawnymi i niejawnymi certyfikatami w infrastrukturze z wieloma urzędami zaufania" wydaną przez Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie jako *osiągnięcie stanowiące znaczny wkład autora w rozwój określonej dyscypliny naukowej*.

Aby odnieść się do zawartości merytorycznej rozprawy warto omówić poszczególne jej rozdziały wskazując na wkład Autora w stosunku do istniejącego stanu wiedzy:

Rozdział 1: sformułowany tu jest problem nazwany przez Autora MTA-TKMA. Warunki definiujące MTA-TKMA i motywacje dla takiego rodzaju schematu nie są jasne. Brak jest sceanriuszy użycia pokazujących konieczność budowy takiego typu podpisu i wspierającej ich infrastruktury. W szczególności warunki wydają się tak sformułowane by pasowały do rozwiązania przedstawionego w Rozdziale 4.

ellR

Rozdział 2: zgodnie z deklaracją Autora Rozdział 2.4 zawiera oryginalny wkład polegający na propozycji nowych trudnych problemów obliczeniowych: extended DCDH oraz advanced k-CCA oraz wykazania ich równoważności z innymi wcześniejszymi problemami. Trudno uważać to za istotny wkład - równoważność jest oczywista i przedstawienie dowodu jest prostym ćwiczeniem.

Kolejną częścią Rozdziału 2 są formalne modele schematów podpisów cyfrowych. Mimo, że jest to klasyka, zwraca uwagę bizantyjski styl i przerost formy nad treścią. Pojawiają się również wątpliwości: schemat podpisu opartego na certyfikacie niejawnym obejmuje utworzenie certyfikatu $Cert_{ID}$, jednak certyfikat ten w żaden sposób nie jest wykorzystany - inaczej niż w przypadku cytowanej pracy [168]. Model podpisu auto-certyfikowanego to w istocie mutacja podpisu opartego o certyfikat – do weryfikacji wykorzystuje się dane przekazane przez TA. Ich postać może się różnić od klasycznych certyfikatów, ale funkcjonalność jest taka sama[1]. Trudno jest uzasadnić nazwanie schematu auto-certyfikowanym – w istocie poświadczenie jest certyfikatem, zwłaszcza w sensie polskiego prawa.

Zaprezentowane w Tabeli 2.1 porównanie zdefiniowanych schematów z proponowanym w Rozdziale 6 jest nieco stronnicze. Dla przykładu: niejasne z tabeli są kwestie związane z kontrolowaniem statusu klucza publicznego. De facto oznacza to powrót do mechanizmu OCSP i wskazuje na brak istotnych ulepszeń w stosunku do najbardziej klasycznych rozwiązań.

Drobne wątpliwości budzi także kwestia modelu bezpieczeństwa. Przedstawiona definicja dopuszcza by adwersarz utworzył nowy podpis dla wiadomości uprzednio podpisanej.

Rozdział 3: główna część zaczyna się w rozdziale 3.4.2.2. Jest tam proponowana uogólniona wersja schematu Gentry-Silverberg. Uogólnienie jest jednak minimalne i polega na wprowadzeniu izomorfizmów zamiast operowania na tych samych grupach. Powoduje to oczywiście nieco utrudnień, ale zasadnicza idea schematu jest ta sama jak w pracy Gentry-Silverberg. Z inżynierskiego punktu widzenia cel modyfikacji jest dla mnie niejasny.

Rozdział 4: jest to niewątpliwie główna część rozprawy. Zasadniczy schemat przedstawiony jest na stronach 111-115. Konstrukcja wykorzystuje kilka trików pochodzących z poprzednich prac - zresztą rzetelnie wymienionych rozprawie. Niewątpliwą wadą konstrukcji, w sensie inżynierskim, jest jej zawikłanie, które może na przykład prowadzić do błędów w trakcie implementacji (najlepsze konstrukcje kryptograficzne - inaczej niż w przypadku teoretycznych prac matematycznych – są proste i eleganckie). Błędów takich nie uniknęła zresztą specyfikacja podana w rozprawie: podany sposób generowania Sk'_{ID_s} wymaga znajomości kluczy $s_{1_{ID_s}}$ oraz $s_{2_{ID_s}}$, które są sekretami użytkownika i nie mogą być przekazane TA[2].

[1] Krytykę schematu auto-certyfikowanego odnieść należy w przeważającej części do autora pracy [101]. Należy jednak pamiętać, że jest to jedynie praca magisterska.

[2] Problem tem można obejść korzystając z X_{ID_s} oraz s_{TA}. Jest jednak zastanawiające dlaczego tak kluczowy moment konstrukcji zawiera tego typu błąd.

MK

Konstrukcja w istocie składa się z wygenerowania klucza prywatnego użytkownika z dwóch części: jednej znanej jedynie użytkownikowi a drugiej znanej TA. Komentarz o tym, że TA zna swój składnik jedynie w momencie generowania wartości jest dyskusyjny – Autor postuluje by TA zapomniało generowanych wartości. Argument taki jest równie dobry w przypadku budowania schematów opartych o zaufany KGC - zwykle prostszych.

Dowód bezpieczeństwa schematu proponowanego w Rozdziale 4 znajduje się w Dodatku (umieszczenie podstawowego fragmentu rozprawy w Dodatku jest samo w sobie nieco dziwne). Największym problemem dowodu bezpieczeństwa są jednak ograniczenia ukryte w stosie notacji: na stronie 157 w trakcie omawiania *Sign-query* przyjmuje się, że żądania złożenia podpisu przez atakowanego użytkownika t kończą się błędem. Niestety, takie założenie w dramatyczny sposób osłabia wartość dowodu bezpieczeństwa: w praktycznych atakach adwersarz może doprowadzić do podpisywania przez użytkownika dowolnie wybranych tekstów – i wykazać należy, że żaden dodatkowy podpis nie może być wygenerowany. Ze względu na te ograniczenie trudno uznać przedstawiony schemat podpisu za dowodliwie bezpieczny.

Ostatnia część Rozdziału 4 poświęcona jest rozszerzeniu na wiele TA. Przedstawione rozwiązanie w istocie jest realizacją idei mediatora – klucz prywatny generowany przez TA w istocie składa się z sumy kluczy generowanych niezależnie przez różne TA. Konstrukcja jest standardowa.

Niewątpliwie największym wkładem rozprawy jest schemat przedstawiony w Rozdziale 4. Dowodzi on pewnej biegłości Autora i znajomości najnowszej literatury. Z drugiej strony jest to schemat dość kontrowersyjny zarówno pod względem motywacji jak i jakości rozwiązania. Wkład w rozwój dziedziny naukowej, zdaniem niżej podpisującego, nie powinien polegać na przedstawieniu zawikłanego rozwiązania (co w przypadku kryptografii jest zadaniem stosunkowo prostym i może być uzyskane w miarę automatycznie), ale schematu rozwiązującego określony problem techniczny. Opiniodawca stoi na stanowisku, że w świetle przedstawionych argumentów wkład Autora w rozwój dziedziny jest nikły i z pewnością nie *znaczny*.

Poziom warsztatu technicznego

W przypadku prac z zakresu kryptografii krytycznym aspektem jest precyzja i jednoznaczność specyfikacji. Inaczej niż częstokroć w innych działach informatyki drobne niedopowiedzenia czy przekłamania mogą prowadzić do błędów o charakterze krytycznym, skutkujących całkowitym brakiem skuteczności projektowanych rozwiązań kryptograficznych. Niestety, rozprawa przedstawiona przez Kandydata posiada szereg wad o takim charakterze. Nie są to drobne usterki, które zawsze mogą wystąpić z powodu niedopatrzenia, ale raczej systematyczny brak precyzji dyskwalifikujący w przypadku ubiegania się o stopień doktora habilitowanego. Niekiedy chodzi tu o podstawowy warsztat obejmujący zakres materiału na studiach magisterskich. Poniżej podaję kilka przykładów tego typu problemów

MR

z kilku stron rozprawy:[3]

1. *str. 31, definicja problemu NP:* autor pisze o prawdopodobieństwie rozwiązania problemu w czasie wielomianowym przez maszynę deterministyczną. W przypadku maszyny deterministycznej prawdopodobieństwo to dla konkretnej instancji jest zawsze równe 1 albo 0. Mówienie o stałej $\delta \in [0, \frac{1}{2}]$ jest nieprawidłowe również, gdy z dobrą wolą zastąpimy *maszynę deterministyczną* przez *maszynę niedetrministyczną*. Liczba ścieżek nie prowadzących do rozwiązania problemu może być bowiem eksponencjalna przy pojedynczej ścieżce prowadzącej do rozwiązania problemu.

2. *str. 32, pierwsze zdanie:* Definicja 2.1 stoi w sprzeczności z komentarzem, według którego funkcja n^{-2} jest pomijalnie mała.

3. *str. 32, Definicja 2.3:* definicja algorytmu zrandomizowanego czasu wielomianowego jest nieprawidłowa. Zgodnie z proponowanym zapisem, w najgorszym wypadku czas wykonania jest wielomianowy. Taki algorytm bardzo łatwo byłoby zmienić na wielomianowy algorytm deterministyczny - zastępując elementy losowe przez elementy wybierane w dowolny deterministyczny sposób.

   Oczywiście, prawidłowa definicja algorytmów randomizowanych jest subtelniejsza.

4. *str. 32, komentarze do bezpieczeństwa bezwarunkowego:* trudno się zgodzić z komentarzem mówiącym, że bezpieczeństwo bezwarunkowe oznacza, iż adwersarz nie jest w stanie odróżnić *od innego elementu tej przestrzeni*. *Odróżnianie* jest bezpośrednim wskazaniem na bezpieczeństwo obliczeniowe – w przypadku bezpieczeństwa bezwarunkowego rozkłady prawdopodobieństwa mają być identyczne a nie jedynie nierozróżnialne obliczeniowo.

5. *str. 33, opis mechanizmu redukcji:* mowa jest o adwersarzu przełamującym schemat z pomijalnie małym prawdopodobieństwem. W istocie redukcja abstrahuje od tego jakie jest to prawdopodobieństwo – wazny jest jedynie związek pomiędzy prawdopodobieństwem sukcesu dla tego adwersarza a prawdopodobieństem złamania problemu bazowego przy użyciu algorytmu wynikającego z redukcji. Akurat przypadek pomijalnego prawdopodobieństwa wyjsciowego jest tu zupełnie nieistotny.

6. *str. 33-34, tzw. podejście asymptotyczne i podejście konkretne:* rozróżnienie jest mało przekonywujące, albowiem w każdym przypadku należy udowodnić, że prawdopodobieństwo złamania problemu bazowego za pomocą redukcji nie jest zaniedbywalnie małe w stosunku do prawdopodobieństwa ataku na schemat wyjściowy. Odpowiednie szacowania (mniej lub bardziej dokładne) zawsze muszą być przeprowadzone.

7. *str. 34, rozdział 2.1.3:* wbrew temu co twierdzi Autor, nie jest konieczne, aby redukcja dawała wyniki w przypadku każdej instancji problemu. Wystarczy,

[3] Należy jednak zaznaczyć, że wybrany został fragment rozprawy, gdzie problemy te mają charakter wyjątkowo drastyczny

elk

że frakcja instancji problemu, dla których się to udaje nie jest zaniedbywalnie mała.

8. *str. 35, punkt widzenia adwersarza $\mathcal{A}$:* nie wystarczy, by rozkład *losowy* był podobny. Aby argument o symulacji zadziałał, rozkład ten powinien być nierozróżnialny dla $\mathcal{A}$.

   W istocie, omawiany dowód przez *symulację* jest uszczegółowieniem mechanizmu redukcji omawianego w rozdziale 2.1.2.

9. *str. 36, opis mechanizmu gier:* niepotrzebne jest założenie, że prawdopodobieństwa zdarzeń E_i różnią się jedynie w zaniedbywalny sposób. W znacznej liczbie dowodów prowadzonych tą techniką prawdopodobieństwa istotnie się różnią. Ponadto, przejście do następnej gry może w ogóle się nie udać z pewnym (ograniczonym) prawdopodobieństwem.

10. *str. 37, komentarze dotyczące ROM:* nie jest prawdziwe kategoryczne stwierdzenie, że *Schematy, w przypadku których dowiedziono, że są bezpieczne w modelu standardowym, są mniej efektywne niż schematy bezpieczne w modelu ROM.* Często jest to prawdą, ale nie stanowi to faktu uniwersalnego.

11. *str. 37, Definicja 2.5:* nie jest to definicja, ale twierdzenie.

12. *str. 39, notacja $x \in_R S$:* fraza *które bezpośrednio nie zależą od x* wymaga wyjaśnienia co to znaczy *pośrednio zależą od x*. Jest to przykład sformułowania nieostrego pod względem znaczenia – zwykle przyjmuje się że $x \in_R S$ oznacza wybranie elementu z S zgodnie z jednostajnym rozkładem prawdopodobieństwa i niezależnie od dotychczasowej historii obliczeń.

Warto jednak wspomnieć, że omawiane powyżej strony są wyraźnie najmniej precyzyjne w całej rozprawie.

Ocena przedstawionych prac z dorobku

Niniejszym przedstawiam krótkie omówienie i ocenę prac dostarczonych wraz z rozprawą habilitacyjną. Kolejność omówienia prac wynika z porządku w jakim zostały przedstawione przez Autora.

praca nr 1: *A practical Certificate and Identity Based Encryption Scheme and Related Security Architecture* (CISIM 2013, LNCS 8104).

Praca ta jest uogólnieniem innej pracy tych samych autorów z CISIM 2012. Nowy element to szyfrowanie tekstów dowolnej długości. Hybrydowa konstrukcja jest oczywista - poprzedni schemat jest używany wyłącznie do zaszyfrowania losowego klucza, który użyty jest do zaszyfrowania długiej wiadomości. Jest to konstrukcja podręcznikowa i decyzja o publikacji tej pracy wydaje się nieuzasadniona.

Poważną wadą warsztatową pracy są braki w specyfikacji (np. brak definicji pewnych parametrów - takich jak X_d w (2)). Definicja 2 jest nie jest w istocie definicją - nie pozwala na odtworzenie schematu. Liczba szczegółów jest za duża (i tak trzeba się cofnąć do cytowanej pracy [1]) a jednocześnie za mała by zorientować się w mechaniźmie schematu.

ell

praca nr 2: *Long-term preservation of digital signatures for multiple groups of related documents* (IET Information Security, 2012, 6.3).

Praca ta zajmuje się problemami związanymi z utratą ważności certyfikatów - a tym samym niemożności weryfikacji dokumentów cyfrowych w klasyczny sposób. Środek zaradczy - tworzenie łańcuchów *time-stamps* teoretycznie pozwala na rozwiązanie tego problemu, jednak w praktyce jest mało użyteczna ze względu na lawinę czynności jakie należałoby wykonywać. Ten problem nieskalowalności jest przedmiotem pracy, której zawartość można w zasadzie streścić do zdania: zamiast odnawiać time stamp dla każdego pojedynczego dokumentu z osobna można dokumenty łączyć w grupy, w grupie obliczać łańcuch haszy, i dopiero wynik opatrywać przy pomocy time-stamp.

Zawartość merytoryczna pracy jest bardzo niewielka - zaproponowana technika należy do folkloru. Tego typu publikacja razi nieco w skądinąd dobrym czasopiśmie.

praca nr 3: *Certificate-Based Encryption Scheme with General Access Structure* (CISIM 2012, LNCS 7564).

Praca ta przedstawia dosyć skomplikowany schemat szyfrowania o szczególnych własnościach – możliwość deszyfrowania przez grupy użytkowników wskazane w *access structure*. Schemat wykorzystuje wiele wysublimowanych technik. Jego wadą zdaje się jednak być brak formalnego dowodu bezpieczeństwa. Szkic zamieszczony na stronie 52 wydaje się odnosić do adwersarza usiłującego wydobyć tekst jawny za pomocą procedury opisanej w schemacie. Niestety, adwersarz nie musi tak postępować, a najistotniejszym elementem dowodu powinno być pokazanie, że alternatywne drogi deszyfrowania nie istnieją. Tak więc propozycję schematu należy raczej potraktować jako wstępny szkic, tym bardziej że liczba szczegółów jest duża i doświadczenie uczy, że w takiej sytuacji łatwo jest nie zauważyć jakiegoś scenariusza ataku.

praca nr 4: *Authentication protocol for software and hardware components in distributed electornic signature creation system* (Przegląd Elektrotechniczny. 10b/2012).

Praca opisuje architekturę służącą do składania podpisu przy pomocy serwerów przejmujących rolę SSCD. Praca nie zawiera treści kontrowersyjnych, ale brak jest również rozwiązań o charakterze nowatorskim pod względem kryptograficznym. Jest to niewątpliwie jedna z propozycji jak powinny wyglądać tzw. podpisy serwerowe.

Słabością pracy jest publikowanie w czasopiśmie zupełnie niewidocznym w międzynarodowym środowisku kryptograficznym. Nawet bardzo dobra praca opublikowana w Przeglądzie Elektrotechnicznym zapewne zostałaby zupełnie niezauważona.

praca nr 5: *Secure Archive for Long-Term Electronic Document Storage with Provable Authenticity* (Pomiary, Automatyka, Kontrola, 2011, 7).

Praca zawiera modyfikację schematu Theodore M. Wong, Chenxi Wang oraz Jeannette M. Wing z 2002 roku. Zawiera pomysł wykorzystania dwóch różnych kluczy i mechanizmu podobnego do *Pedersen commitment*. Algorytm jest

MK

dość elegancki. Najpoważniejszą wadą jest brak jasnego argumentu dlaczego proponowane rozwiązanie jest bardziej przydatne od poprzednich (pomijając relatywnie interesującą koncepcję matematyczną).

praca nr 6: *Identity verification based on certificateless public key cryptography* (Pomiary, Automatyka, Kontrola, 2010, 12).

Praca przedstawia protokół uwierzytelniania pomiędzy klientem a serwerem z wykorzystaniem serwera tożsamości. Protokoły tego typu są dość często stosowane w praktyce biznesowej – artykułowi brakuje przesłania w jaki sposób miałaby być eliminowana jakaś wada rozwiązań standardowych.

Sam opis protokołu budzi pewne wątpliwości: przekazywane są jedynie podpisy, więc np. w jaki sposób B poznaje IDT_A? Oczywiście mogą to być podpisy typu *message recovery*, jednak w obliczu wielkości podpisywanych danych wydaje się to mało efektywne. Opis protokołu na rysunku nie do końca zgodny jest z zapisem w tekście. Niestandardowa notacja nosi znamiona obfuskacji.

praca nr 7: *Non-repudation of Electronic Health Records in distributed healthcare systems* (Pomiary, Automatyka, Kontrola, 2010, 10).

Artykuł opisuje proponowany sposób ewidencjonowania dokumentów medycznych. Nie zauważyłem pracy żadnych istotnych elementów, które mógłbym nazwać rezultatem naukowym bądź technologicznym.

praca nr 8: *Directed threshold signcryption scheme from bilinear pairing under controle of designated signcrypter* (Metody Informatyki Stosowanej, 4/2008).

Artykuł ten wyróżnia się pozytywnie na tle innych publikacji zarówno pod względem edycyjnym jak i zawartości merytorycznej. Sama idea rozwiązania korzysta intensywnie z własności odwzorowań dwuliniowych - umożliwiających sprawdzenie szeregu zależności algebraicznych.

Wadą pracy jest brak szczegółowych dowodów bezpieczeństwa, jakich oczekiwać by można od artykułu w czasopiśmie. Najpoważniejszym mankamentem jest brak wykazania ulepszeń pod względem efektywności schematu w porównaniu do klasycznego scenariusza *signature-then-encryption*. Ponieważ ulepszenia pod względem złożoności obliczeniowej są podstawowym uzasadnieniem dla stosowania signcryption, wartość pracy jest niejasna, tym bardziej, że schemat jest stosunkowo skomplikowany i oparty na specjalnych strukturach algebraicznych.

praca nr 9: *Signed electronic document and its probative value in certificate and certificateless public key cryptosystem infrastructures* (Elektronika, 11/2009).

Artykuł ten ma bardziej charakter popularno-naukowy i nie zawiera oryginalnych rezultatów naukowych.

Ogólna ocena działalności publikacyjnej

Dorobek publikacyjny widoczny w renomowanych bazach bibliograficznych jest dosyć skromny. W bazie DBLP widoczne są dwie publikacje w CISIM - prawie nie-

dlR

znanej w środowisku kryptograficznym, jednej publikacji w stosunkowo dobrym czasopiśmie *IET Information Security*, oraz rozdziału w książce *Handbook of Information and Communication Security 2010*. Podobnie dane z Researchgate potwierdzają brak oddźwięku publikacji Kandydata - cytowania tam wymienione wskazują na 2 prace (w liczących się wydawnictwach) i jedno cytowanie przez autorów ze środowiska szczecińskiego.

Właściwie brak publikacji na forum międzynarodowym i w liczących się wydawnictwach poświęconych omawianej tematyce jest symptomatyczny – świadczy raczej o poziomie uniemożliwiającym przyjęcie do druku niż o polityce "ukrywania wyników w szufladzie".

Oceniając wagę opublikowanych wyników mam poważne wątpliwości, czy byłyby zaakceptowane w dobrych ośrodkach (takich jak Uniwersytet Warszawski) jako podstawa ubiegania się o stopień doktora.

Mirosław Kutyłowski