Instytut Podstaw Informatyki
Polska Akademia Nauk
ul. Jana Kazimierza 5, 01-248 Warszawa

tel +(48) 22 38-00-500
836-28-62
836-28-85
836-37-09
fax: +(48) 22 38-00-510

Warszawa, 20.07.2014

Recenzja rozprawy habilitacyjnej i ocena dorobku naukowego dra inż. Jerzego Pejasia

Niniejszą opinię przedstawiam na prośbę Rady Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technicznego w Szczecinie w ramach przewodu habilitacyjnego dra inż. Jerzego Pejasia.

I. Recenzja rozprawy habilitacyjnej

Przedmiotem oceny jest rozprawa habilitacyjna dra inż. Jerzego Pejasia p.t. „Schematy podpisu cyfrowego z jawnymi i niejawnymi certyfikatami w infrastrukturze z wieloma urzędami zaufania" wydana w Szczecinie w roku 2013 przez Stowarzyszenie Przyjaciół Wydziału Informatyki w serii Monografie Informatyczne.

Temat pracy i jego praktyczne znaczenie

Temat pracy obejmuje jedno z najważniejszych praktycznych zagadnień współczesnej kryptografii klucza publicznego, które związane jest z budową infrastruktury zaufania na potrzeby schematów szyfrowania i podpisów cyfrowych. Potrzeba ta wynika z podstawowego dylematu każdego użytkownika schematów kryptografii klucza publicznego, sprowadzającego się do konieczności udzielenia sobie odpowiedzi na proste pytanie: do kogo należy dany klucz publiczny?

W tradycyjnej infrastrukturze klucza publicznego (PKI) odpowiedzi na to pytanie można udzielić na podstawie zaufania do certyfikatu klucza publicznego, właściwie do wystawcy certyfikatu. Kontrolowanie zaufania w tej sytuacji polega przede wszystkim na śledzeniu statusu kluczy publicznych, a dokładniej, statusu związanych z nimi certyfikatów. Ta część architektury PKI jest uważana za najbardziej uciążliwą w implementacji i stosowaniu. Jednocześnie ta wada jest przyczyną poszukiwania nowych rozwiązań, które mogłyby zastąpić tradycyjną infrastrukturę klucza publicznego.

Obecnie za jeden z najbardziej obiecujących obszarów badań uważa się kryptografię klucza publicznego opartą na odwzorowaniach dwuliniowych, nazywanych iloczynami dwuliniowymi albo kryptografią na funkcji pary (ang. Pairing Based Cryptography, PBC). Ogromne zainteresowanie tym obszarem badań wynika z możliwości wyeliminowania certyfikatów ze schematów szyfrowych i konieczności zarządzania statusem certyfikatów. Tak jest w przypadku schematów opartych na tożsamości, schematów bezcertyfikatowych, a także schematów opartych na certyfikatach niejawnych, tj. certyfikatach, które łączą tożsamość i klucz publiczny użytkownika, ale nie są publicznie znane. W praktyce okazuje się, że zastosowanie wymienionych klas schematów PBC przenosi problem zarządzania certyfikatami na problem zarządzania tożsamością użytkownika oraz dodatkowo generuje problem dystrybucji kluczy publicznych. Istotnym przykładem tego ostatniego problemu jest podatność schematów na podmianę kluczy publicznych, a tym samym podatność na ataki typu DoD (ang. Denial of Decryption) - odbiorca nie może odszyfrować wiadomości i DoSV (ang. Denial of Signature Verification) - adresat nie jest w stanie zweryfikować poprawności podpisu.

Obszar badawczy będący przedmiotem rozprawy jest bardzo aktualny i ma duże znaczenie praktyczne. Połączenie wielu urzędów zaufania w ramach jednej architektury zaufania

i zarządzania kluczami (TKMA) pozwala na ich hierarchiczne wiązanie lub wiązanie różnych domen certyfikacji z najwyższymi w hierarchii głównymi urzędami zaufania. Główne problemy badawcze na tym polu dziś dotyczą efektywnego powiązania schematów kryptografii funkcji pary z architekturami urzędów zarządzania kluczami.

Jak słusznie zauważa autor punktem wyjścia do tego typu powiązania są schematy na odwzorowaniach dwuliniowych o wspólnych parametrach systemowych. Ich integracja w ramach jednej architektury urzędów zarządzania kluczami wymaga jednak zaprojektowania odpowiedniego schematu podpisu w środowisku kryptografii na funkcjach pary.

Cel pracy i problem badawczy

Głównym celem pracy jest rozwiązanie problemu badawczego nazwanego przez autora rozprawy problemem MTA-TKMA (od ang. Multiple Trust Authority – Trusted Key Management Authority). Problem ten autor sprowadził do opracowania nowej architektury zaufania i zarządzania kluczami (TKMA) z wieloma urzędami zaufania (MTA), przystosowanej do współpracy ze schematami podpisu cyfrowego z szyframi na odwzorowaniach dwuliniowych i wykorzystującymi certyfikaty jawne oraz certyfikaty niejawne. Architektura ta musi zapewniać, że „certyfikaty jawne i niejawne są ze sobą powiązane, ale w taki sposób by nikt, w tym także właściciel tych certyfikatów ani ich wystawca (urząd certyfikacji), nie był w stanie odtworzyć certyfikatu niejawnego mając dany certyfikat jawny".

Proponowana w rozprawie architektura TKMA jest trójwarstwowa. W warstwie najwyższej znajdują się modele zaufania, w pośredniej warstwie modele certyfikacji, zaś w najniższej - schematy podpisu cyfrowego (lub schematy szyfrowania). Autor pracy założył, że przyjęty model zaufania i model certyfikacji powinien mieć wpływ na schemat podpisu cyfrowego zastosowany w warstwie najniższej. Ogólna postać tego typu schematu została określona w definicji 1.1. Podstawą tego schematu są wspólne parametry systemowe oraz parametry dodatkowe urzędów TA wchodzących w skład architektury TKMA. Przy takiej definicji schematu każdy projektant schematu podpisu cyfrowego może najpierw określić pożądany model zaufania (np. wyspowy model zaufania z pojedynczymi niezależnymi urzędami zaufania, model siatkowy lub model hierarchiczny), łączący modele certyfikacji z warstwy drugiej, a następnie dobrać odpowiadający mu schemat podpisu cyfrowego. Jest to bardzo ważne stwierdzenie, które autor konsekwentnie uzasadnia w kolejnych rozdziałach, zwłaszcza w rozdziale czwartym recenzowanej rozprawy.

Struktura rozprawy

Praca liczy 174 strony i składa się z 4 rozdziałów, podsumowania, trzech załączników obejmujących „pomocniczy" słownik podstawowych pojęć, skróty i oznaczenia stosowane w pracy oraz szczegółowe dowody lematów sformułowanych w pracy, spis literatury zawierający 167 pozycji oraz streszczenie pracy w języku angielskim.

Kolejne rozdziały pracy obejmują opis kontekstu głównych zagadnień i podstawowe pojęcia (m. in. definicję i własności iloczynu dwuliniowego oraz definicje problemów trudnych obliczeniowo, na których opierają się schematy podpisów zaproponowane w pracy), standardowe infrastruktury zaufania na potrzeby kryptografii klucza publicznego oraz ich alternatywne odpowiedniki w przypadku zastosowania schematów podpisu oraz obszerny opis rozwiązania sformułowanego problemu badawczego.

Zakończeniem pracy jest podsumowanie zawierające uwagi końcowe oraz sformułowanie otwartych problemów i interesujących kierunków przyszłych badań.

Ocena merytoryczna pracy

Układ pracy podporządkowany jest zastosowanemu przez autora podejściu do rozwiązania problemu MTA-TKMA. W rozdziale pierwszym, oprócz wspomnianych już definicji celu i problemu badawczego, podano także jego obszerne uzasadnienie wraz z przykładami komercjalizacji istniejących schematów kryptografii z funkcją pary oraz wspierającymi je specyfikacjami i normami technicznymi.

Z punktu widzenia celu pracy istotnym elementem tego rozdziału jest przedstawiona w nim

propozycja podziału na trzy kategorie znanych dotąd schematów e-podpisu z funkcją pary:

(a) kategoria I - schematy kryptografii klucza publicznego oparte na jawnym certyfikacie (do tej kategorii należą m.in. tradycyjne schematy oparte na PKI);
(b) kategoria II - schematy kryptografii klucza publicznego oparte na tożsamości;
(c) kategoria III - schematy kryptografii klucza publicznego oparte na niejawnym certyfikacie;

Szczegółowa analiza cech schematów należących do poszczególnych kategorii umożliwiła autorowi zaproponowanie nowej, czwartej kategorii schematów kryptografii klucza publicznego opartych na jawnym i niejawnym certyfikacie. Schematy tej kategorii leżą pomiędzy schematami kategorii III oraz kategorii I. Mają cechy obu tych kategorii. Co więcej, schematy kategorii IV można redukować do schematów kategorii III. Jest to cecha schematów PBC uzyskana dzięki oparciu ich na certyfikatach jawnych i niejawnych.

W rozdziale drugim przedstawiono podstawowe definicje i metody dowodzenia wiarygodności (bezpieczeństwa, ang. security) schematów kryptografii klucza publicznego. Podano definicję i własności iloczynu dwuliniowego. Istotne w tym rozdziale są sformułowane przez autora dwa nowe problemy trudne obliczeniowo: rozszerzony obliczeniowy problem ilorazowy Diffiego-Hellmana (*extended* DCDH, od ang. Division Computational Diffie-Hellman) oraz problem *advanced* k-CAA (od ang. Collusion Attack Algorithm with k-traitors; pol. algorytm ataku przez zmowę k nieuczciwych użytkowników). Oba są bardzo interesującymi wersjami klasycznego sformułowania Diffiego-Hellmana. Pierwszy zdefiniowany jest jako problem obliczania $g^{bc/a}$ (zamiast klasycznego g^{ab}), a drugi z wykładnikiem jeszcze znacznie bardziej skomplikowanym.

Autor udowodnił, że rozszerzony problem ilorazowy Diffiego-Hellmana (*extended* DCDH) jest równoważny obliczeniowemu problemowi ilorazowemu Diffiego-Hellmana (DCDH), oraz że dopóki problem *k*-CAA jest trudny obliczeniowo, dopóty nie istnieje algorytm czasu wielomianowego dla *advanced k*-CAA. Na trudności obliczeniowej obu wymienionych problemów oparte są schematy podpisu zaproponowane w rozdz. IV, a także przedstawione tam dowody wiarygodności (bezpieczeństwa) tych schematów.

Rozdział trzeci wprowadza definicje pojęcia zaufania, modelu certyfikacji, modelu zaufania oraz domeny zaufania. Pojęcia te są istotne z punktu widzenia trójwarstwowej architektury TKMA. Zostały tak sformułowane, aby obejmowały standardowe (PKI) i niestandardowe modele zaufania. W przypadku modeli standardowych autor wprowadza główne idee i problemy dotyczące rodzajów modeli zaufania i ich wzajemnych powiązań. Zaprezentował także reprezentatywny przegląd znanych dotąd modeli z literatury badawczej w tej dziedzinie. Natomiast niestandardowym modelom zaufania poświęcono w literaturze bardzo mało uwagi. Podjęta przez autora udana próba znalezienia niestandardowych modeli zaufania, które są odpowiednikami modeli zaufania PKI jest godna uwagi, zwłaszcza w przypadku modeli budowanych w oparciu o urzędy zaufania korzystając z izomorficznych grup algebraicznych.

W rozdziale czwartym przedstawione są najważniejsze wyniki rozprawy rozwijające oryginalną obserwację, że pewne cechy odwzorowań dwuliniowych na starannie dobranych grupach umożliwiają dwa różne sposoby weryfikowania pewnych istotnych zależności kryptograficznych. Dr Pejaś elegancko wykorzystuje to do zaprojektowania nowego schematu podpisu cyfrowego, głównego bohatera rozprawy, który nazwał IE-RCIBS (Implicit and Explicit Revocable Certificate and Id-Based Signature). Schemat stosuje odwzorowania dwuliniowe. Prezentację nowego schematu podpisu poprzedził dyskusją o możliwości wyeliminowania certyfikatu z niestandardowych schematów PBC, a następnie na tej podstawie uzasadnił propozycję wprowadzenia czwartej kategorii schematów. Następnie autor pokazał, że weryfikacja autentyczności podpisu może być wykonywana na dwa sposoby: raz ze zwykłym jawnym certyfikatem i drugi raz z certyfikatem niejawnym, czyli na podstawie kluczy publicznie znanych i danych o tożsamości osoby (podmiotu), która ten podpis złożyła. Wynika stąd, że schematy z certyfikatami jawnymi i niejawnymi mogą pracować w trybie zgodności ze schematami kategorii III oraz w trybie zgodności ze schematami opartymi tylko na certyfikatach jawnych (schematy kategorii I). W rozdziale tym wykazano także, że w modelu losowej wyroczni proponowany schemat IE-RCIBS jest odporny na egzystencjalne fałszerstwo

w warunkach ataku z adaptacyjnie wybraną wiadomością EUF-CMA, przy założeniu że problemy *advanced k*-CAA oraz *extended* DCDH w grupie są trudne obliczeniowo.

Schemat IE-RCIBS autor uogólnił następnie na całą rodzinę schematów F-IE-RCIBS z jednym urzędem TA, a następnie na schematy z wieloma urzędami zaufania. Uzyskane w efekcie schematy podpisu cyfrowego wspierają trzy różne niestandardowe modele zaufania: płaski model wyspowy, model siatkowy i model hierarchiczny. Wszystkie uzyskane modele zaufania pozwalają na weryfikację podpisów cyfrowych w oparciu o dwie procedury weryfikacji (z użyciem certyfikatu jawnego i bez jego użycia). Dotyczy to także podpisu cyfrowego w hierarchicznym modelu zaufania. Chociaż dr Pejaś pokazał, że weryfikacja podpisu tylko na podstawie certyfikatu niejawnego może być raczej uciążliwa w przypadku liczby poziomów większej niż trzy.

W mojej ocenie przedstawiona powyżej analiza merytorycznej zawartości poszczególnych rozdziałów pracy pokazuje, że sformułowany w pracy problem MTA-TKMA został przez autora rozwiązany i tym samym postawiony cel pracy został osiągnięty. Do rozwiązania problemu MTA-TKMA zastosowano metodę od szczegółu do ogółu. Takie podejście w przypadku problemu MTA-TKMA jest uzasadnione i wynika z zaproponowanej trójwarstwowej architektury zaufania i zarządzania kluczami.

Osiągnięcia badawcze przedstawione w rozprawie

Osiągnięcia badawcze dr inż. Jerzego Pejasia należy rozpatrywać w kontekście sformułowanego w pracy i rozwiązanego problemu architektury zaufania i zarządzania kluczami z wieloma urzędami zaufania (MTA-TKMA) oraz możliwości jej integrowania z tradycyjnymi architekturami PKI zarządzania kluczami .

Stąd do głównych osiągnięć autora należy zaliczyć:

- wprowadzenie do kryptografii nowego paradygmatu nazwanego przez autora kryptografią klucza publicznego opartą na jawnym i niejawnym certyfikacie; podstawą tego paradygmatu są dwa certyfikaty (jawny i niejawny), które są ze sobą powiązane, ale w taki sposób, że na podstawie certyfikatu jawnego obliczeniowo trudne jest odtworzenie certyfikatu niejawnego, i odwrotnie, na podstawie certyfikatu niejawnego obliczeniowo trudne jest odtworzenie certyfikatu jawnego; schematy szyfrowe oparte na tym paradygmacie autor zaliczył do jednej z czterech zaproponowanych przez siebie kategorii schematów kryptografii klucza publicznego; kategoria IV, do której należą schematy spełniające wprowadzony paradygmat, leży pomiędzy kategorią schematów opartych na certyfikatach niejawnych, a kategorią schematów opartych na certyfikacie jawnym (w tym wspieranych przez tradycyjną infrastrukturę PKI);
- zdefiniowanie trójwarstwowej architektury zaufania i zarządzania kluczami (TKMA) składającej się z trzech warstw, przy czym dwie dolne warstwy odpowiadają tradycyjnej architekturze zarządzania kluczami typu PKI; autor podał także ogólną definicję schematu podpisu cyfrowego z jawnym i niejawnym certyfikatem w infrastrukturze z wieloma urzędami zaufania, jego cechy oraz cechy modelu certyfikacji, który go wspiera; należy zauważyć, że sformułowana definicja schematu wpływa zarówno na warstwę najwyższą (modele zaufania) architektury TKMA, jak również na warstwę pośrednią (modele certyfikacji) tej architektury;
- sformułowanie dwóch nowych problemów trudnych obliczeniowo: problemu *extended* DCDH i problemu *advanced k*-CAA; trudność obliczeniowa tych problemów została wykazana w sposób prawidłowy, a następnie poprawnie technicznie wykorzystana w dowodzie bezpieczeństwa nowego schematu podpisu IE-RCIBS;
- zaprojektowanie konkretnego schematu podpisu cyfrowego IE-RCIBS opartego na certyfikacie jawnym i niejawnym, a tym samym spełniającego nowy paradygmat kryptografii klucza publicznego oparty na jawnym i niejawnym certyfikacie; na potrzeby tego schematu autor wprowadził odpowiedni model bezpieczeństwa i wykazał, że w tym modelu schemat podpisu IE-RCIBS jest bezpieczny przy

założeniu, że problemy *advanced k*-CAA oraz *extended* DCDH są obliczeniowo trudne;

- opracowanie na podstawie schematu podpisu cyfrowego IE-RCIBS rodziny schematów F-IE-RCIBS; dla opracowanych schematów autor zaproponował nowe modele certyfikacji oraz wykazał, że schematy rodziny F-IE-RCIBS mogą pracować w trybie schematów podpisu z certyfikatem niejawnym oraz w trybie tradycyjnych schematów wspieranych przez PKI.

Wszystkie zaproponowane w rozprawie dra Pejasia schematy podpisu cyfrowego korzystają z odwzorowań dwuliniowych, których ciekawe własności, m.in. możliwość jednoczesnej pracy z dwoma lub trzema grupami algebraicznymi, pozwalają na przynajmniej dwuwariantowe weryfikowanie podpisów cyfrowych, a także tworzenie zagregowanych certyfikatów ułatwiających weryfikacje podpisów w infrastrukturach zaufania z wieloma urzędami zaufania (zwłaszcza z hierarchicznie powiązanymi).

Zaproponowane schematy są efektywne. W Tab. 4.1 autor przedstawił porównanie proponowanego schematu IE-RCIBS z innymi znanymi schematami opartymi na tożsamości, bezcertyfikatowymi oraz z certyfikatem niejawnym. Porównanie to wypada korzystnie dla schematu IE-RCIBS, nawet w przypadku uwzględnienia dodatkowych nakładów obliczeniowych ponoszonych na ocenę statusu certyfikatu.

Uwagi formalne

Monografia dra Pejasia napisana jest bardzo elegancko i klarownie, choć obejmuje bardzo trudne techniczne zagadnienia. Kolejne fragmenty są logicznym następstwem wcześniejszych lub je logicznie dopełniają. Styl pracy nie budzi zastrzeżeń. Całość jest starannie zredagowana. Można znaleźć i wytknąć tylko drobne (nieliczne) usterki formalne, właściwie literówki. Są to między innymi:

- str. 23, linia 11 od góry: jest „uzyskanie poziomu zaufania 3 wg GiraultaGirault", powinno być „uzyskanie poziomu zaufania 3 wg Giraulta";
- str. 41, linia 12 od góry: jest „cyklicznych i addytywnych group", powinno być „cyklicznych i addytywnych grup";
- str. 43, linia 2 powyżej wzoru (2.6): jest „skonstruowanie odwzorowania wielo-liniowego", powinno być „skonstruowanie odwzorowania wieloliniowego";
- str. 47, Definicja 2.21: jest „problem *advanced k*-CAA problem", powinno być „problem *advanced k*-CAA";
- str. 49, linia 3 od dołu: jest „Sformuowane definicje", powinno być „Sformułowane definicje";
- str. 51, linia 3 od góry: jest „rozwiązany przez Al-Riyami'ego i Patersona", powinno być „rozwiązany przez Al-Riyamiego i Patersona";
- str. 86, linia 6 od góry: jest „odwzorowania wielo-liniowe zawężają", powinno być „odwzorowania wieloliniowe zawężają";
- str. 117, Lemat 4.2, linia 5: jest „q_R zapytańdo", powinno być jest „q_R zapytań do";
- str. 137, algorytm **TASetup**: jest „oznacza odpowiednio klucz publiczny i klucz prywatny TA_t", powinno być „oznacza odpowiednio klucz sekretny i klucz publiczny TA_t";
- str. 138, punkt (b): błędny wzór $S'_{TA_t} = \overline{S}_{TA_{t-1}} + V_{TA_t}$, powinno być $\overline{S}_{TA_t} = \overline{S}_{TA_{t-1}} + V_{TA_t}$;
- str. 138, algorytm, powyżej wzoru 4.26: jest „częściowy klucz prywatny S'_{TA_t} nie jest zaciemniony"; powinno być „częściowy klucz prywatny $\overline{S}_{TA_t}$ nie jest zaciemniony";
- str. 168: pozycje [81] i [82] pokrywają się, [83] i [84] też.

Wskazane usterki formalne nie wpływają w żaden sposób na merytoryczną ocenę pracy jako całości.

Podsumowanie

Główny wynik rozprawy, jakim jest zaproponowana nowa rodzina schematów podpisu cyfrowego (w tym także z certyfikatem jawnym i niejawnym) w paradygmacie kryptografii klucza publicznego na odwzorowaniach dwuliniowych, jest bardzo interesujący z punktu widzenia badawczego i możliwych praktycznych zastosowań. Wynik ten i przeprowadzone w rozprawie dowody wiarygodności (bezpieczeństwa) i oszacowania złożoności obliczeniowej dobrze wpisują się w jeden z głównych nurtów modnych obecnie na świecie badań w zakresie kryptografii klucza publicznego.

Monografia zawiera wiele nowych interesujących wyników i rozwiązań stanowiących oryginalne osiągnięcia autora w zakresie dotychczas znanych metod budowania infrastruktury zaufania na potrzeby podpisu cyfrowego i nowych rozwiązań algorytmicznych opartych na schematach z funkcją pary. Praca zawiera nowe wyniki teoretyczne, ale jest jednak mocno osadzona w realiach praktyki. Niewątpliwie wynika to z ogromnego doświadczenia dra Pejasia w zakresie projektowania i implementowania usług PKI na gigantyczną skalę wielu milionów użytkowników. Świadczą o tym odniesienia do rzeczywistych modeli zaufania i modeli certyfikacji stosowanych w komercyjnych infrastrukturach klucza publicznego PKI w Polsce, a także analiza możliwości zbudowania podobnych modeli w ramach zaproponowanej architektury TKMA i ich integracji z systemami PKI. Z tego ostatniego powodu ciekawa jest dyskusja dotycząca praktycznego znaczenia certyfikatów w schematach PBC przedstawiona w rozdziale 4.1 oraz podsumowana w rozdziale 5.1.

W podsumowaniu autor sformułował kilka bardzo interesujących problemów do dalszych badań. Jednym z nich jest implementacja architektury zaufania i zarządzania kluczami wspierającej schematy podpisu w paradygmacie kryptografii na odwzorowaniach dwuliniowych. Inny problem to wykorzystanie nowego paradygmatu kryptografii klucza publicznego z certyfikatami jawnym i niejawnym do konstrukcji nowych schematów szyfrowania. Jest to szczególnie interesujące w kontekście wspomnianego powyżej ataku z odmową odszyfrowania (DoD). Powinno dostarczyć mechanizm z certyfikatem jawnym przeciwdziałający tego typu atakom.

W kontekście powyższych uwag i stwierdzeń uważam, że praca dra inż. Jerzego Pejasia spełnia w pełni wymagania stawiane pracom habilitacyjnym zarówno z punktu widzenia jej formy, jak i zawartości merytorycznej i warsztatowej.

Uwagi krytyczne i polemiczne

W tym miejscu pozostaje odnotować pewien dyskomfort recenzenta z powodu notorycznego niepotrzebnego zaśmiecania języka polskiego przez autora monografii. Na przykład „walidacja”, odmieniana w monografii wielokrotnie przez wszystkie przypadki deklinacji. Zamiast prostego i zrozumiałego słownikowego tłumaczenia ang. *validation*: uprawomocnienie, stwierdzenie ważności (np. certyfikatu). Czytelnikowi monografii pomaga w pewnym stopniu załączony do niej pomocniczy słownik pojęć. Terminologia na ogół oddaje istotne intuicje. Młodzi Anglicy i Amerykanie od razu je znają. 99% Polaków nie ma szans na to, jeśli nie zadbamy o dobre tłumaczenie. Inny przykład to „prymitywy kryptograficzne”. (Na wszelki wypadek od razu wyjaśniam, iż w monografii dra Pejasia nie jest to epitet wobec nieuków nie znających się na kryptografii.)

Druga uwaga to poczucie niedosytu merytorycznego wywołanego zdefiniowaniem na całą monografię pojęcia efektywności obliczeniowej algorytmów jako złożoności wielomianowej. Z dzisiejszej perspektywy wymaganie czasu wielomianowego jest zbyt słabe dla efektywności algorytmów mających mieć znaczenie praktyczne. Słynny algorytm AKS deterministycznego testowania pierwszości liczb całkowitych, mający już ponad 10 lat, działa w czasie wielomianowym. Tylko stopień tego wielomianu jest niestety zbyt wysoki. Dla liczb o rozmiarach mających obecnie praktyczne znaczenie algorytm AKS wymaga czasu niemożliwego dziś do realizacji w praktyce. Mimo, że jest wielomianowy. Z dość nawet wydawałoby się niskim stopniem tego wielomianu równym 7. Przy tym pojęcie praktycznej

efektywności powinno obejmować nie tylko efektywność czasową, ale też pamięciową (ang. space) i inne zasoby (np. liczbę procesorów we współbieżnych wykonaniach). Jest to zagadnienie na osobną dyskusję naukową.

Kolejna (ostatnia już) uwaga ma jeszcze bardziej polemiczny charakter. Dotyczy ogólnego kierunku badań i rozwiązań w dotychczasowym dorobku publikacyjnym dra Pejasia. Można określić ten kierunek jako *kryptografia z Wielkim Bratem*. Wszystko jest tu oparte na zaufaniu do wyższej instancji. Na ogół nazywa się ją obdarzoną zaufaniem trzecią stroną (ang. trusted third party). W pracach dra Pejasia są to urzędy certyfikacji. Mają większe uprawnienia niż zwykły „szary" użytkownik systemu i są hierarchicznie scentralizowane. *Jeszcze Większy Brat* pilnuje każdego urzędu. Takie podejście ma pewne praktyczne zalety organizacyjne i komercyjne, oczywiście.

Tymczasem obecnie nowoczesna kryptografia wychodzi z innego dobrze znanego założenia, iż „najciemniej jest pod latarnią". (Szczególnie w Polsce mamy tego świadomość.) Od fundamentalnej w tym nurcie pracy Diffiego i Hellmanna z 1976 roku wiadomo już, że w wielu sytuacjach technologicznie możliwa jest weryfikacja poprzez publicznie dostępne klucze służące do szyfrowania lub odszyfrowywania. Od ponad 30 lat weryfikacja autentyczności podpisu elektronicznego przeprowadzona może być przez każdego zainteresowanego użytkownika, nie tylko przez jakiś podejrzany centralny podmiot. Ta koncepcja jest w pewnej mierze zakłócona w praktyce często przez wprowadzanie hierarchii certyfikatów kluczy, czyli zaświadczeń kto jest właścicielem danego klucza dostępnego publicznie (i odpowiadającego mu klucza prywatnego). Trudno oprzeć się pokusie, by takie certyfikaty wydawane były przez powoływany w tym celu specjalny urząd. Wtedy certyfikat musi być podpisany cyfrowo kluczem urzędu, który z kolei sam poświadczany jest przez jakiś wyższy (Ober)urząd. Podpis pod takim poświadczeniem przez jeszcze wyższy. I tak dalej. Aż do centrali nazywanej głównym urzędem. Rozprawa habilitacyjna dra Pejasia jest właściwie festiwalem hierarchii urzędów certyfikacji, recitalem Wielkiego Brata.

Z drugiej strony zupełnie inaczej rozwiązuje to najbardziej znany i popularny na całym świecie system PGP (Pretty Good Privacy, pol. Całkiem Dobra Prywatność) podpisu elektronicznego i zabezpieczania komunikacji elektronicznej. Udostępnione publicznie ponad 20 lat temu oprogramowanie PGP ma wyraźnie sformułowaną motywację ochrony prywatności obywateli przed urzędowym Wielkim Bratem. (Por. Philip Zimmermann *Why I Wrote PGP*, June 1991, https://www.philzimmermann.com/EN/essays/WhyIWrotePGP.html, dostęp 16.07.2014, oraz jego podręcznik (ang. manual) PGP wersja 2.0.) Infrastruktura kluczy publicznych (i certyfikatów) PGP implementuje zdecentralizowany model zaufania nazwany sieciami zaufania (ang. webs of trust). Zamiast modelu centralnego zarządzania w hierarchii urzędów. Wybrane przeze mnie osoby, firmy lub instytucje, które znam i mam do nich zaufanie, poświadczają posiadanie przeze mnie danego klucza. Informacja o tym zostaje przez nich podpisana elektronicznie. Np. poprosiłbym dra Pejasia o wystawienie mi i podpisanie certyfikatu. (Niebawem już dr hab. Pejasia, prof. nadzw. ZUT.) Poprosiłbym też o to jeszcze kilka innych znanych osób. Wiarygodność (ang. security) opiera się na ich autorytecie i niezależności, także niezależności od „tajnych służbowych" nacisków.

Innym przykładem zastąpienia centrali urzędowej, obdarzonej zaufaniem (a de facto pierwszej podejrzanej), metodą sieci przejrzystej (transparentnej) i publicznej kontroli jest całkowicie nowe rozwiązanie tego problemu w technologii waluty cyfrowej Bitcoin. Jej sedno tworzy publicznie dostępna księga-rejestr (ang. ledger) wszystkich transakcji, nazwana łańcuchem bloków (ang. blockchain). Prowadzona jest i aktualizowana automatycznie współbieżnie na komputery wszystkich użytkowników. W każdym bloku można umieścić wiele krótkich informacji. Jak się wydaje, tego rodzaju zapis może pełnić rolę notarialnego potwierdzania (uwierzytelniania) dokumentów, autentyczności podpisu, głosu oddanego w elektronicznym głosowaniu itp. (Por. [*The Mega-Master Blockchain List*, http://ledracapital.com/blog/2014/3/11/bitcoin-series-24-the-mega-master-blockchain-list].)

Opisałem powyżej ten problem (dość szczegółowo) jako konkretny przykład zdecentralizowanego podejścia, w celu wywołania polemicznej dyskusji. Z nadzieją, że może stanie się to inspiracją na przyszłość dla dzisiejszego Habilitanta, Jego współpracowników

i uczniów. Nie jest to tylko akademicki problem teoretyczny. Ze względu na olbrzymią rolę podpisu w obiegu prawnym i gospodarczym, modele infrastruktury technologicznej podpisu elektronicznego wydają się decydujące dla ustroju całej przyszłej gospodarki elektronicznej, więc i ustroju Państwa. Z materiałów ujawnionych przez Edwarda Snowdena wiemy, jak bardzo jest to istotne.

Powyższe uwagi krytyczne i polemiczne w żaden sposób nie umniejszają merytorycznej wartości recenzowanej monografii i nie obniżają mojej bardzo wysokiej oceny wyników dra Pejasia zawartych w przestawionej monografii habilitacyjnej i jego dorobku publikacyjnym.

II. Ocena dorobku naukowego dra inż. Jerzego Pejasia po uzyskaniu stopnia doktora

Dr inż. Jerzy Pejaś ukończył studia na Wydziale Informatyki i Zarządzania Politechniki Wrocławskiej uzyskując w roku 1978 tytuł magistra inżyniera informatyki w zakresie teorii i techniki systemów. Pierwszą pracę podjął w Hucie „Szczecin", skąd po roku przeniósł się na Zachodniopomorski Uniwersytet Technologiczny w Szczecinie (dawnej Politechnika Szczecińska), gdzie pracuje do chwili obecnej. W roku 1988 na Wydziale Elektrycznym Politechniki Gdańskiej obronił pracę doktorską z zakresu automatyki okrętowej p.t. „Zastosowanie obserwatora adaptacyjnego w syntezie adaptacyjnego układu stabilizacji ruchu statku wzdłuż zadanej trajektorii prostoliniowej".

Od samego początku praca naukowa Habilitanta przeplatała się z praktyką i działalnością ekspercką. Dr inż. Jerzy Pejaś zajmował się badaniem, projektowaniem i instalowaniem systemów sterowania ruchem statków i aparatów podwodnych, zastosowaniami technologii potwierdzania tożsamości przy pomocy kart elektronicznych (karty stykowe i bezstykowe) w systemach płatniczych, zaś od roku 1998 roku do chwili obecnej – kryptografią i jej zastosowaniami, w tym głównie infrastrukturą klucza publicznego (PKI), podpisem elektronicznym, kryptograficznymi metodami kontroli dostępu oraz kryptografią na iloczynach dwuliniowych (ang. Pairing Based Cryptography, PBC).

Dr inż. Jerzy Pejaś jest znanym i uznanym w Polsce, a także w obrębie Unii Europejskiej, wybitnym ekspertem w zakresie podpisu elektronicznego i elektronicznych metod ustalania i potwierdzania tożsamości (ang. identification).

Dorobek naukowo-badawczy

Obszary zainteresowań badawczych dra Pejasia można podzielić na dwa główne okresy: do roku 1990 - automatyka okrętowa; i od roku 1991 do dziś – kryptograficzna ochrona informacji.

Pierwszy okres zainteresowań naukowych Habilitanta, chociaż odległych od obecnych, jest jednak bardzo istotny i bogaty przede wszystkim w osiągnięcia na styku badań naukowych i praktycznych zastosowań. Badania dra Pejasia koncentrowały się w tamtym okresie głównie na określeniu właściwych metod filtracji sygnałów pomiarowych i wykorzystaniu ich do syntezy układów sterowania ruchem obiektów pływających. Habilitant opracował system dynamicznego pozycjonowania położenia statku (np. statku wiertniczego) oraz system prowadzenia statku wzdłuż zadanej trajektorii z małymi lub dużymi prędkościami. Wyniki te zostały zastosowane w praktyce na statku typu B-90 Granit w postaci systemu ręcznego sterowania z możliwością automatycznego wspomagania stabilizacji kursu i prędkości statku oraz w postaci płetwowego układu aktywnej stabilizacji kołysań bocznych statku.

W tym okresie dr Pejaś przeprowadził też badania modelu systemu dynamicznego pozycjonowania wykonane na specjalnym basenie modelowym podczas stażu naukowego na Uniwersytecie Technicznym w Rostocku (Niemcy). Należy tylko żałować, że ze względu na zmiany polityczne i kadrowe w Niemczech po roku 1990 nie skonsumował tych wyników w formie pracy habilitacyjnej.

Od roku 1990 prace badawcze dra inż. Jerzego Pejasia konsekwentnie związane są z ochroną informacji, w szczególności z badaniem, projektowaniem i wdrażaniem infrastruktur certyfikacji wspomagających algorytmy szyfrowania z kluczem znanym publicznie. Droga

Habilitanta do tego typu zagadnień jest dość nietypowa - prace badawcze z zakresu infrastruktur zaufania rozpoczął bowiem od prac wdrożeniowych wykonywanych na zlecenie dużych firm, m. in. Unizeto Technologies S.A., Zakład Ubezpieczeń Społecznych, Powszechny Zakład Ubezpieczeń. Niemal natychmiastowe wdrożenia wyników w rzeczywistych systemach stanowią świetną motywację dla naukowca.

Na dorobek naukowy dr inż. Jerzego Pejasia po doktoracie składa się imponująca liczba 130 publikacji po roku 1990 w czasopismach, książkach oraz w materiałach znaczących konferencji krajowych i międzynarodowych. Łączna liczba publikacji punktowanych wg listy ministerialnej (Ujednolicony Wykaz Czasopism Punktowanych opracowany przez MNiSW (komunikat z dnia 25.06.2010 r. oraz Karta Oceny Jednostki Naukowej dla nauk ścisłych, technicznych i nauk o życiu (Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 25 maja 2010 r., Dz.U. Nr 93, Poz. 599) wynosi 84, na łączną sumę 365 punktów (ok. 203 punktów po uwzględnieniu procentowego udziału współautorów). W czasopismach z Ujednoliconego Wykazu Czasopism Punktowanych MNiSW - 16 publikacji, w tym 3 w części A tego wykazu.

Dorobek dra Pejasia obejmuje także 39 recenzowanych pozycji książkowych, których jest autorem lub współautorem – jedną książkę napisał samodzielnie, innej był współautorem i był redaktorem naczelnym 10 książek, a także napisał 27 rozdziałów w publikacjach wieloautorskich. Większość (24 prace) została napisana w języku angielskim i trafiła do obiegu za pośrednictwem wydawnictw o uznanym szerokim lub światowym zasięgu, m. in. wydawnictwa Springer Verlag, Kluwer Academic Publishers oraz Interscience Enterprises Ltd.
Niewątpliwie najciekawsze wyniki Habilitant opublikował po roku 2007. W pracach:

(a) Jerzy Pejaś *Schematy podpisu cyfrowego z jawnymi i niejawnymi certyfikatami w infrastrukturze z wieloma urzędami zaufania*. Wyd. Stowarzyszenie Przyjaciół Wydziału Informatyki w Szczecinie. Seria: Monografie Informatyczne, Tom II, ISBN 978-83-936799-1-1, Szczecin, 2013
(b) Tomasz Hyla, Jerzy Pejaś *A practical certificate and identity based encryption scheme and related security architecture*. K. Saeed, R. Chaki, A. Cortesi, S. Wierzchon (Eds.), CISIM 2013, Lectures Notes on Computer Science, Vol. 8104, Springer-Verlag, 2013, str. 178-193
(c) Tomasz Hyla, Imed El Fray, Jerzy Pejaś, Witold Maćków *Long-term Preservation of Digital Signatures for Multiple Groups of Related Documents*, IET Information Security, Vol. 6, Issue 3, 2012, str. 219-227
(d) Tomasz Hyla, Jerzy Pejaś *Certificate-Based Encryption Scheme with General Access Structure*. W: Cortesi, A. et al. (Eds.), CISIM 2012, Lecture Notes in Computer Science, Vol. 7564, Springer-Verlag, 2012, str. 41–55
(e) Witold Maćków, Jerzy Pejaś *Secure Archive for Long-Term Electronic Document Storage with Provable Authenticity*, Pomiary Automatyka Kontrola, No 7, 2011, str. 764-769
(f) Jerzy Pejaś, Tomasz Klasa *Identity verification based on certificateless public key cryptography*, Pomiary Automatyka Kontrola, R. 56, Nr 12, 2010, str. 1533-1536
(g) Tomasz Hyla, Włodzimierz Bielecki, Jerzy Pejaś *Non-repudiation of Electronic Health Records in distributed healthcare systems*, Pomiary Automatyka Kontrola, R. 56, Nr 10, 2010, str. 1170-1173
(h) Jerzy Pejaś *Signed Electronic Document and its Probative Value in Certificate and Certificateless Public Key Cryptosystem Infrastructures*, Elektronika: konstrukcje, technologie, zastosowania, Nr 11, 2009, str. 30-34
(i) Jerzy Pejaś *Directed Threshold Signcryption Scheme from Bilinear Pairing under Sole Control of Designated Signcrypter*. Metody Informatyki Stosowanej, Nr 4, 2008, str. 161-172

Wszystkie te publikacje należą do głównego nurtu badań Habilitanta związanego z podpisem elektronicznym, jego wartością prawno-dowodową oraz infrastrukturą zaufania dla usług związanych z e-podpisem. W pracach (c), (e), (g) i (h) przedstawione zostały propozycje rozwiązania problemu efektywnego utrzymywania długookresowej ważności podpisu elektronicznego jako pochodnej ograniczonego okresu ważności certyfikatów klucza

publicznego. Ich istotą jest minimalizacja liczby operacji kryptograficznych wymaganych podczas przedłużania na kolejne okresy ważności certyfikatów i związanych z tym dokumentów. Ogólna metoda, preferowana przez dra Pejasia, polega na wyeliminowaniu pojedynczych punktów zaufania i pojedynczych punktów awarii. Wyeliminowanie pojedynczych punktów zaufania do autentyczności dokumentów przechowywanych elektronicznie pozwala na zwiększenie ich wartości prawnej oraz na dopuszczenie ich jako dowodów w postępowaniach sądowych. Z drugiej strony, podział informacji pomiędzy wiele węzłów systemu chroni przed utratą informacji i pozwala na ich odtworzenie w przypadku awarii. Podejście takie zaprezentowano w pracy (e), a następnie uogólniono je w (c) w oparciu o tzw. dokumentację poświadczeń grupowych (ang. Group Evidence Records, GER).

Zarządzanie certyfikatami, w tym także wspomniane wyżej ograniczone okresy ważności certyfikatów, są od wielu lat przyczyną poszukiwania przez badaczy alternatyw dla tradycyjnych infrastruktur zaufania PKI. Publikacje (a), (b), (d), (f), (h) i (i) wpisują się w ten ogólnoświatowy trend z zastosowaniem kryptografii klucza publicznego skojarzonej z iloczynami dwuliniowymi (Pairing Based Cryptography, PBC). Nie trudno zauważyć, że monografia habilitacyjna dra Pejasia jest bezpośrednio w ten kierunek badań, a wyniki przedstawione w wymienionych publikacjach są oryginalnymi osiągnięciami Habilitanta w dziedzinie nowoczesnej kryptografii i zabezpieczeń sieci teleinformatycznych (ang. network security), wymagającymi jeszcze szerszego rozpowszechnienia.

To ostatnie stwierdzenie dotyczy w szczególności sformułowanego przez Habilitanta niedawno nowego paradygmatu kryptografii klucza publicznego z jawnym i niejawnym certyfikatem. Paradygmat ten pozwala na takie projektowanie schematów podpisu cyfrowego (w mojej ocenie, także schematów szyfrowania), które pozwalają na generowanie podpisów cyfrowych w sposób umożliwiający weryfikację za pomocą certyfikatu jawnego i niejawnego lub tylko niejawnego. Co więcej, schematy te, przy założeniu, że pracują na wspólnych lub izomorficznych grupach, można uogólniać na schematy z wieloma urzędami zaufania i budować w ten sposób złożone (także hierarchiczne) infrastruktury zaufania.

Schematy szyfrowania przedstawione w publikacjach (b) i (d) są połączeniem typowego szyfrowania PBC z ogólnymi strukturami dostępu. Uzyskany efekt jest porównywalny ze schematami szyfrowania grupowego, w których jedynie uprawniona grupa użytkowników może odszyfrować określony szyfrogram. Połączenie struktur dostępu i algorytmów szyfrowania z funkcją pary (PBC) daje duże możliwości formułowania różnych polityk dostępu (np. polityk ORCON) i ich egzekwowania w systemach dostępu do informacji wrażliwych. Stanowi to istotne osiągnięcie dra inż. Jerzego Pejasia, otrzymane w ramach projektu *Innowacyjny model bezpiecznego zarządzania informacją klasyfikowaną* i realizowanego jeszcze obecnie projektu *Mobilne urządzenie do ochrony informacji niejawnej*.

Za wyróżniającą należy uznać nie tylko działalność badawczą, ale też wdrożeniową i ekspercko-naukową dra inż. Jerzego Pejasia. Habilitant brał udział:

(a) w czterech projektach naukowo–badawczych, przy czym w przypadku dwóch był kierownikiem zadań realizowanych przez Zachodniopomorski Uniwersytet Technologiczny w Szczecinie (jeden z nich jest nadal realizowany);
(b) w sześciu podstawowych pracach rozwojowo-wdrożeniowych z zakresu badania, projektowania i wdrażania infrastruktury klucza publicznego PKI;
(c) w opracowaniu kilkunastu projektów i specyfikacji technicznych dotyczących usług zaufania w infrastrukturze PKI, urządzeń do składania bezpiecznych podpisów zgodnie z Ustawą o podpisie elektronicznym, oraz systemów przechowywania dokumentów elektronicznych;
(d) w opracowaniu profilu certyfikatów kwalifikowanych wg Ustawy o podpisie elektronicznym; profil ten powstał w ramach prac Zespołu ds. Podpisu Elektronicznego przy Ministrze Gospodarki, którego członkiem był Habilitant.

W ostatnich latach dr Pejaś brał udział w opracowaniu szeregu raportów i ekspertyz związanych z podpisem elektronicznym. Do najważniejszych należą:

(a) *IDABC European eGovernment Services - Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications - NATIONAL PROFILE POLAND*, Report for European Commission Directorate General Enterprise, April 2007;
(b) *Wspólnotowe prace legislacyjne nad rozporządzeniem Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eID*AS). Ekspertyza wykonana na zlecenie Ministerstwa Gospodarki, grudzień 2012 r.

Był także recenzentem 12 artykułów nadesłanych do opublikowania w renomowanych czasopismach (w tym Information Sciences oraz Journal of Systems and Software) oraz recenzentem 9 wniosków projektowych zgłoszonych lub realizowanych w ramach konkursów ogłaszanych przez KBN, Ministerstwo Rozwoju Regionalnego - Program Operacyjny Innowacyjna Gospodarka na lata 2007-2013, i NCBiR.

Wart odnotowania jest także fakt otrzymania przez dr inż. Jerzego Pejasia w roku 2013 nagrody zespołowej I stopnia Rektora Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie za osiągnięcia naukowe.

Podsumowując tę część oceny dorobku dra inż. Jerzego Pejasia stwierdzam, że dorobek publikacyjny - badawczy, wdrożeniowy i ekspercko-naukowy - jest ilościowo i jakościowo znaczącym wkładem w rozwój dyscypliny informatyka. Z formalnego punktu widzenia dorobek ten jest w pełni wystarczający do ubiegania się o stopień doktora habilitowanego.

Dorobek dydaktyczny i popularyzatorski

Dr inż. Jerzy Pejaś od ponad 30 lat prowadzi zajęcia ze studentami. Najpierw na kierunku automatyka i robotyka w Instytucie Okrętowym Politechniki Szczecińskiej (obecnie Wydział Techniki Morskiej ZUT w Szczecinie), następnie na kierunku informatyka (od roku 1991 w ramach Wydziału Techniki Morskiej, a obecnie w ramach Wydziału Informatyki). Prowadził także zajęcia dla studentów na kierunku Zarządzanie i Inżynieria Produkcji oraz dla studentów studiów podyplomowych. Od roku 2006 prowadzi także zajęcia na kierunku Informatyka Stargardzkiej Szkoły Wyższej STARGARDINUM.

Zajęcia Habilitanata obejmują wszystkie formy dydaktyki: wykłady, ćwiczenia audytoryjne, laboratoria, projekty oraz seminaria przedmiotowe i dyplomowe. Habilitant prowadzi lub prowadził na kierunkach studiów Informatyka oraz Zarządzanie i Inżynieria Produkcji ponad 20 różnych kursów akademickich. Do najważniejszych należy zaliczyć: wstęp do algorytmizacji, systemy operacyjne, podstawy ochrony informacji, wybrane metody kryptografii (wykład na studiach doktoranckich), architektury zabezpieczeń i aplikacje oparte na technologiach PKI, bezpieczne systemy internetowe, komponenty bezpiecznych systemów informatycznych, infrastruktura klucza publicznego, zaawansowane metody tworzenia bezpiecznych aplikacji oraz bezpieczeństwo transakcji elektronicznych.

Wymienione powyżej zajęcia były lub są prowadzone przez Habilitanta na podstawie autorskich konspektów i instrukcji laboratoryjnych, umieszczonych w Intranecie Wydziału Informatyki ZUT oraz dwóch autorskich podręczników akademickich. Podczas swoich zajęć Habilitant korzysta także z podręcznika A.J. Menezes, P. C. Van Oorshot, S. A Vanstone *Kryptografia stosowana*, Wydawnictwo Naukowo Techniczne, Warszawa 2005, którego był jednym z czterech współtłumaczy.

Dr inż. Jerzy Pejaś był promotorem łącznie 148 prac inżynierskich i magisterskich. Jedna z tych prac, praca magisterska napisana przez Tomasza Klasę i zatytułowana "Electronic identity verification system based on certificateless public key cryptography", została wyróżniona I nagrodą w konkursie *Cyberprzestępczość i sposoby zabezpieczeń systemów informatycznych* ogłoszonego pod patronatem Polskiego Towarzystwa Informatycznego w ramach Sejmiku Młodych Informatyków, Międzyzdroje 2010. Jest także opiekunem Studenckiego Koła Naukowego TAO, zarejestrowanego przez Rektora ds. Studenckich na wniosek studentów Wydziału Informatyki ZUT interesujących się problemami ochrony informacji.

Habilitant brał udział w opracowaniu programów zajęć (ang. syllabus) oraz treści programowych dla kierunków Informatyka, Bioinformatyka, Zarządzanie i Inżynieria Produkcji

oraz Inżynieria Cyfryzacji, w tym m.in. treści programowych i programów zajęć dla kierunku dyplomowego Inżynieria Bezpieczeństwa Systemów Informatycznych oraz Studium Podyplomowego Inżynieria Zarządzania Bezpieczeństwem Systemów.

Praca dydaktyczna dr inż. Jerzego Pejasia została doceniona przez Rektora Zachodniopomorskiego Uniwersytetu Technologicznego, który przyznał mu w roku 2011 nagrodę indywidualną II stopnia za szczególne osiągnięcia dydaktyczne.

Bardzo znacząca jest także działalność popularyzatorska Habilitanta w dyscyplinie Informatyka. Dr inż. Jerzy Pejaś wystąpił z 28 referatami na konferencjach międzynarodowych, oraz 30 na konferencjach krajowych. Prowadził gościnne wykłady w Międzynarodowym Centrum Matematycznym im. Stefana Banacha (1 wykład), Instytucie Podstaw Informatyki PAN (3 wykłady) i na Uniwersytecie Warszawskim (1 wykład), a także wykłady popularne w ramach Zachodniopomorskich Spotkań z Nauką (8 wykładów) oraz Uniwersytetu 3 Wieku (1 wykład). Publikował artykuły w czasopismach o charakterze popularnym (m.in. Normalizacja, Электронный регион, Wiedza i Praktyka) oraz w internetowych portalach informacyjnych (np. portalkadrowy.pl, unizeto.pl), popularyzując przede wszystkim podpis elektroniczny i jego zastosowania w administracji, służbie zdrowia oraz w sądownictwie. Prowadził szkolenia i warsztaty z zakresu infrastruktury klucza publicznego, podpisu elektronicznego, ochrony danych wrażliwych, m.in. na potrzeby Unizeto Technologies S.A., Ministerstwa Sprawiedliwości, Urzędu Marszałkowskiego województwa Zachodniopomorskiego.

Uważam, że dorobek dydaktyczny i popularyzatorski dr inż. Jerzego Pejasia spełnia z nadmiarem wymagania stawiane przez Ustawę o tytule i stopniach naukowych oraz stopniach i tytule w zakresie sztuki.

Dorobek organizacyjny

Działalność organizacyjna dra inż. Jerzego Pejasia jest wszechstronna i prowadzona systematycznie od wielu lat. Habilitant powadził lub prowadzi znaczącą działalność na rzecz własnej uczelni. Był m.in.: członkiem Rady Wydziału Informatyki ZUT (WI ZUT), październik 2008 – wrzesień 2011; przewodniczącym Wydziałowej Komisji ds. Nagród WI ZUT, wrzesień 2008 – wrzesień 2011; członkiem Senackiej Komisji ZUT ds. Nagród i Odznaczeń, październik 2006 - czerwiec 2010; członkiem Senackiej Komisji ZUT ds. Bibliotecznych, październik 2004 – wrzesień 2006; kierownikiem Studium Podyplomowego Informatyki dla Nauczycieli w Gorzowie, 1 listopad 1999 r. – 2002 r.; kierownikiem Zakładu Technik Informacyjnych i Sterowania w Instytucie Informatyki ZUT, 1 wrzesień 1996 r. - 31 sierpień 1999 r.; zastępcą Dyrektora ds. Dydaktyki w Katedrze Informatyki i Automatyki Morskiej, Wydziału Techniki Morskiej ZUT, 1 wrzesień 1993 r. - 31 sierpień 1994 r.; prodziekanem ds. Studenckich Wydziału Techniki Morskiej, 1 wrzesień 1994 r. - 31 sierpień 1996 r.

Od roku 2002 jest kierownikiem Zespołu Ochrony Informacji w Zakładzie Symulacji Komputerowej i Ochrony Informacji na Wydziale Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

Uczestniczył także w pracach różnych grup doradczych i eksperckich, np. takich jak Zespół ds. Podpisu Elektronicznego przy Ministrze Gospodarki, ekspert Polskiej Izby Informatyki i Telekomunikacji w pracach nad projektem Ustawy o podpisach elektronicznych, członek Normalizacyjnego Komitetu Technicznego 182 ds. Ochrony Informacji w Systemach Teleinformatycznych (Polski Komitet Normalizacyjny).

Jest wieloletnim organizatorem i przewodniczącym Komitetu Organizacyjnego międzynarodowej konferencji Advanced Computer Systems, niezwykle ważnej dla całego środowiska kryptologii w Polsce. Trudno wręcz wyobrazić sobie tę konferencję bez dra Pejasia. Jest pomysłodawcą i organizatorem krajowej konferencji „Inżynieria Oprogramowania i Zabezpieczeń Systemów Informacyjnych", SoftSec. Walnie przyczynił się także do powstania idei i powołania do życia Europejskiego Forum Podpisu Elektronicznego, cyklicznej konferencji międzynarodowej promującej usługi zaufania, w tym podpis elektroniczny i systemy identyfikacji elektronicznej. Konferencja ta na stałe wpisała się w kalendarz wielu instytucji krajowych oraz Unii Europejskiej, a także unijnych gremiów normalizacyjnych z CEN (Comité Européen de Normalisation) i ETSI (European Telecommunications Standards

Institute) na czele.

Był także członkiem lub przewodniczącym komitetów programowych 20 cyklicznych konferencji krajowych i międzynarodowych, m. in. *European Forum on Electronic Signature* (przewodniczący komitetu programowego w latach 2012-14), *International Conference on Computer Applications ICCA 2010* (24-27 December, 2010, Pondicherry, India), *World Congress on Nature and Biologically Inspired Computing & 8th International Conference on Computer Information Systems and Industrial Management Applications* (NaBIC-CISIM'09, Coimbatore, India, Dec 09-11, 2009) oraz *International Conference on Advances in Intelligent Systems: Theory and Applications AISTA'2004* (15-18 November 2004, Luxembourg-Kirchberg).

Za swoją działalność dr inż. Jerzy Pejaś otrzymał Złoty Medal za Długoletnią Służbę nadany w roku 2011 przez Prezydenta RP B. Komorowskiego, Medal „Za Zasługi dla Politechniki Szczecińskiej" nadany w roku 2008 przez Senat Politechniki Szczecińskiej, Srebrny Krzyż Zasługi nadany w roku 2002 przez Prezydenta RP A. Kwaśniewskiego.

Na podstawie przedłożonych przez Habilitanta i pokrótce podsumowanych powyżej informacji o jego aktywności organizacyjnej uważam, że dorobek ten jest wyróżniający i upoważnia do ubiegania się o stopień doktora habilitowanego.

III. Konkluzja

Podsumowując stwierdzam, że monografia habilitacyjna dra inż. Jerzego Pejasia przedstawia oryginalne, interesujące podejście i wiele nowych interesujących wyników badawczych autora. Główne wyniki i rozwiązania stanowią oryginalne osiągnięcia autora. Zarówno w zakresie dotychczas znanych metod budowania infrastruktury technologicznej podpisu elektronicznego, jak i nowych rozwiązań algorytmicznych opartych na operacji pary (ang. *Pairing Based Cryptography*). Niektóre z tych wyników były opublikowane przez dra Pejasia wcześniej w recenzowanych artykułach naukowych [76-79, 110, 125, 129, 130]. W tym dwa artykuły w tomach wiodącej serii LNCS Springera o wyjątkowo szerokim zasięgu międzynarodowym.

Stwierdzam, iż w mojej ocenie wyniki badawcze dra inż. Jerzego Pejasia opublikowane w przedstawionej do przewodu habilitacyjnego monografii oraz w innych publikacjach po doktoracie stanowią istotny wkład do wiedzy w dziedzinie informatyki. Moim zdaniem spełniają wszystkie ustawowe i zwyczajowe kryteria wymagane w przewodach habilitacyjnych. Wobec tego wnoszę o dopuszczenie pana dra inż. Jerzego Pejasia do dalszych etapów przewodu habilitacyjnego.