



UMCS

Zachodniopomorski Uniwersytet
Technologiczny w Szczecinie

26. 08. 2019

W P Ł Y N Ę Ł O
Wydział Informatyki

UNIwersytet Marii Curie-Skłodowskiej w Lublinie
Wydział Matematyki, Fizyki i Informatyki

dr hab. Bogdan Księżopolski, prof. UMCS | Zakład Cyberbezpieczeństwa, Instytutu Informatyki

Lublin, 20.08.2019 r.

**Recenzja pracy habilitacyjnej doktora Tomasza Hyli pt.
„Nowe metody zapewnienia bezpieczeństwa dokumentom elektronicznym”
oraz dorobku naukowego i dydaktycznego.**

Niniejsza recenzja została przygotowana w odpowiedzi na list Pana profesora Jerzego Pejasia Dziekana Wydziału Informatyki Zachodniopomorskiego Uniwersytetu Technicznego w Szczecinie informujący, że Centralna Komisja ds. Stopni i Tytułów powołał mnie na recenzenta i członka komisji w postępowaniu habilitacyjnym doktora inżyniera Tomasza Hyli w dziedzinie nauk technicznych, w dyscyplinie informatyka.

Recenzja została przygotowana w oparciu o materiały prezentujące (1) osiągnięcie naukowe doktora inżyniera Tomasza Hyli wraz z autoreferatem oraz (2) dorobek naukowy, w szczególności wykaz opublikowanych prac naukowych, a także informacje o działalności naukowej. Na początku wyrażę opinię na temat osiągnięcia doktora inżyniera Tomasza Hyli, a następnie odniosę się do dorobku naukowego oraz dydaktycznego.

Ocena osiągnięcia naukowego

Przedmiotem oceny jest osiągnięcie naukowe w formie cyklu publikacji powiązanych ze sobą tematycznie, obejmujących 7 pozycji opublikowanych w latach 2012-2019 (jedna praca w druku). Prace te są opublikowane: w czasopismach z listy JCR (4 pozycje) oraz w materiałach konferencyjnych LNCS (3 pozycje). Osiągnięcie jest zatytułowane: „**Nowe metody zapewnienia bezpieczeństwa dokumentom elektronicznym**”. Są to wyszczególnione poniżej publikacje (w porządku chronologicznym):

1. Tomasz Hyla, Jerzy Pejaś, 2012, **Certificate-Based Encryption Scheme with General Access Structure**, A. Cortesi, N. Chaki, K. Saeed, S. Wierzchoń (edyt.), Computer Information Systems and Industrial Management CISIM 2012, Lecture Notes in Computer Science, tom 7564, Springer, Berlin, Heidelberg, str. 41-55.
2. Tomasz Hyla, Imed El Fray, Witold Maćków, Jerzy Pejaś, 2012, **Long-term preservation of digital signatures for multiple groups of related documents**, IET Information Security, tom 6, nr 3, str. 219-227.
3. Tomasz Hyla, Witold Maćków, Jerzy Pejaś, 2014, **Implicit and Explicit Certificates-Based Encryption Scheme**, K. Saeed, V. Snasel (edyt.), Computer Information Systems and Industrial Management CISIM 2014, Lecture Notes in Computer Science, tom 8838, Springer, Berlin, Heidelberg, str. 651-666.



4. Tomasz Hyla, Jerzy Pejaś, 2016, **Secure Outsourced Bilinear Pairings Computation for Mobile Devices**, J. Chen, V. Piuri, C. Su, M. Yung (edyt.) Network and System Security NSS 2016, Lecture Notes in Computer Science, tom 9955, Springer, Cham, str. 519-529.
5. Tomasz Hyla, Jerzy Pejaś, 2017, **A Hess-like Signature Scheme based on Implicit and Explicit Certificates**, The Computer Journal, tom 60, nr 4, str. 457-475.
6. Tomasz Hyla, Jerzy Pejaś, 2018, **Demonstrably Secure Signature Scheme Resistant to k-Traitor Collusion Attack**, IEEE Access, tom 6, str. 50154-50168.
7. Tomasz Hyla, 2019, **Local and Outsourced Simultaneous Verification of Pairing-based Signatures**, Journal of Internet Technology, nr 4/2019. (artykuł w druku)

Przedstawiony cykl prac opublikowany w rozpoznawalnych czasopismach i materiałach konferencyjnych LNCS. Prace dotyczą czterech grup problemów.

- a. Wykorzystania łańcuchów bloków do zapewnienia niezaprzeczalności dokumentów.
- b. Szyfrowania grupowego dokumentów z wykorzystaniem struktury dostępu.
- c. Schematów podpisu i szyfrowania opartych o certyfikaty jawne i niejawne.
- d. Przyspieszenia wykonania weryfikacji i tworzenia podpisów.

Problemy te są spójne tematycznie i dotyczą ogólnego problemu bezpieczeństwa przetwarzania i przechowywania dokumentów elektronicznych. Warto zwrócić uwagę, że habilitant jest pierwszym autorem we wszystkich wskazanych pracach.

Pierwszym poruszonym zagadnieniem jest zapewnienie długookresowej niezaprzeczalności dokumentów [2]. Zagadnienie to jest szczególnie istotne w archiwach cyfrowych. Habilitant wprowadził schemat GER (Group Evidence Record), który stanowi rozszerzenie istniejącego schematu ERS (Evidence Record Syntax). Zaproponowane rozwiązanie pozwala długoterminowo zapewnić niezaprzeczalność grupy dokumentów z zachowaniem określonego ich porządku.

Drugie zagadnienie dotyczy problemu szyfrowania dokumentów w rozproszonym środowisku, ale w taki sposób, że użytkownik ma dostęp wyłącznie do tych danych, do których został przydzielony mu dostęp [1]. Problem ten nie jest nowy i w literaturze są propozycje rozwiązania tego zagadnienia. Habilitant zaproponował schemat CIBE-GAS (Certificate and ID-based Group Oriented Decryption Scheme with General Access Structure), który daje dodatkowe możliwości z punktu widzenia zarządzania całym procesem. Moim zdaniem sam wynik z punktu widzenia naukowego nie jest fundamentalny, ale warto zwrócić uwagę na aspekt praktyczny. Schemat CIB-GAS został zaimplementowany i przetestowany w ramach projektu MobInfoSec. Dzięki temu rozwiązaniu można przenieść operacje kryptograficzne z urządzenia mobilnego na zdalny serwer. Takie rozwiązanie jest szczególnie istotne dzisiaj, ponieważ tak powszechnie tworzone systemy Internetu Rzeczy, czy sieci 5G są zazwyczaj urządzeniami z ograniczonymi zasobami.



Trzeci poruszony problem dotyczy schematu podpisów cyfrowych opartych o certyfikaty jawne i niejawne. W pracy [3] Habilitant zaproponował paradygmat (IEC-PKC), który zabezpiecza przed atakiem odmowy deszyfrowania (ang. DoD). Istotnym wkładem jest zaproponowanie schematu implementującego wspomniany paradygmat (IE-CBE). Schemat ten składa się z 8 algorytmów. W pracy wykazano jego odporność na atak DoD w modelu z losową wyrocznią. Postawiony problem, kontynuowany był w kolejnej pracy [5], w ramach której Habilitant zaproponował pierwszy schemat podpisu odporny na atak DoSV (Denial of Signature Verification) oparty na certyfikatach jawnych i niejawnych. Kolejne badania dotyczące tego problemu [6] dotyczyły metody konstrukcji klucza, która wykorzystuje problem logarytmu dyskretnego opartego o asymetryczne odwzorowania dwuliniowe. Dzięki takiemu rozwiązaniu znacznie została zwiększona wydajność proponowanego rozwiązania.

Ostatni poruszany problem dotyczy przyśpieszenia weryfikacji oraz tworzenia podpisów cyfrowych w środowisku rozproszonym. W pracy [4] Habilitant zaproponował schemat bezpiecznego delegowania szczególnie kosztownych obliczeniowo operacji kryptograficznych (odwzorowania dwuliniowe) do bardziej wydajnego środowiska obliczeniowego (chmura obliczeniowa). Autor wykazał, że w pewnych warunkach przeniesienie tych obliczeń do chmury obliczeniowej jest korzystne. Ta tematyka została poruszona również w pracy [7], gdzie zostały zmodyfikowane wcześniej zaproponowane algorytmy IE-CBHS [5], w taki sposób, który umożliwia delegowanie obliczeń odwzorowań dwuliniowych do zdalnych serwerów obliczeniowych. Przeprowadzone badania w ramach prac [4,7] wykazały zasadność bezpiecznego delegowania obliczeń w przypadku urzędzeń z ograniczonymi zasobami.

W wyniku analizy przedstawionych prac można stwierdzić, że głównym osiągnięciem naukowym habilitanta jest opracowanie nowych schematów kryptograficznych zapewniających bezpieczeństwo dokumentom elektronicznym. W tym kontekście opracowanie, analiza oraz wykazanie praktycznego zastosowania dla nowych schematów kryptograficznych można uznać za istotne oryginalne osiągnięcie naukowe wnoszące wkład do rozwoju informatyki.

Biorąc pod uwagę powyższe, uważam, że przedstawione osiągnięcie spełnia wymogi stawiane w procesie habilitacyjnym.

Ocena dorobku naukowego

Doktor inżynier Tomasz Hyla ukończył w roku 2007 studia magisterskie na kierunku informatyka, na Wydziale Informatyki Politechniki Szczecińskiej. W roku 2011 obronił doktorat na Wydziale Informatyki Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie.

Tematyka badań doktora inżyniera Tomasza Hyla dotyczy kryptografii oraz metod ochrony informacji. Do najważniejszych należą badania dotyczące bezpiecznego przechowywania, przetwarzania oraz kontroli dostępu do dokumentów elektronicznych, ze szczególnym



uwzględnieniem danych medycznych. Innym wyraźnym nurtem jest tworzenie schematów przetwarzania operacji kryptograficznych dla urządzeń mobilnych.

Warto podkreślić, że duża część prac zawiera nie tylko rozważania teoretyczne, ale przedstawia podejście praktyczne, wraz z ich implementacją w postaci narzędzi lub systemów.

W bazie DBLP jest indeksowanych 16 publikacji habilitanta, w bazie Scopus 25 publikacji, w bazie WoS 21 prac. Indeks Hirsha: WoS - 6, Scopus - 6, Google Scholar - 7. Liczba cytowań: WoS - 99 (bez autocytowań - 69), Scopus - 110 (bez autocytowań - 55), Google Scholar - 131. Według mnie jest to poziom zadawalający na tym etapie rozwoju naukowego. Należy przyjąć, że z czasem ta liczba będzie wzrastała, ze względu na aktualność poruszanych tematów badawczych.

Wartym zauważenia jest uczestnictwo Habilitanta jako wykonawcy w 4 projektach badawczo-rozwojowych finansowanych ze środków NCBiR oraz 4 projektów dla młodych naukowców. Pewnym minusem jest brak uczestnictwa w projektach badawczych realizowanych w szerszej współpracy naukowej z ośrodkami zagranicznymi.

Habilitant uczestniczył w prestiżowym programie Top 500 Innovators, w ramach którego odbył 3 miesięczny staż na Uniwersytecie w Cambridge. Moim zdaniem taki staż był bardzo wartościowy, ponieważ obecnie brakuje nam badań naukowych, których wyniki mają potencjał do komercjalizacji.

Doktor inżynier Tomasz Hyla w ciągu 6 lat wygłosił 16 referatów na międzynarodowych konferencjach naukowych, z czego 12 odbyły się zagranicą, a 4 w Polsce. To bardzo wysoka aktywność i zasługuje na podkreślenie.

Podsumowując, oceniam dorobek naukowy habilitanta jako dobry i spełniający wymagania stawiane w procesie habilitacyjnym.

Ocena dorobku dydaktycznego i popularyzatorskiego

Habilitant bierze aktywny udział w realizacji procesu dydaktycznego. Wypromował 6 magistrów oraz 12 inżynierów.

Warto zwrócić uwagę na działalność doktora Tomasza Hyli jako członka komitetu organizacyjnego 7 międzynarodowych konferencji naukowych. Dwukrotnie był przewodniczącym komitetu organizacyjnego.

O rosnącej rozpoznawalności naukowej habilitanta świadczy fakt wykonania 16 recenzji dla czasopism naukowych, w tym 13 z listy JCR, a także wykonania 2 recenzji projektów zleconych przez NCBiR.



UMCS

UNIWERSYTET MARII CURIE-SKŁODOWSKIEJ W LUBLINIE
Wydział Matematyki, Fizyki i Informatyki

dr hab. Bogdan Księżopolski, prof. UMCS | Zakład Cyberbezpieczeństwa, Instytutu Informatyki

Pozytywnie oceniam działalność dydaktyczną i popularyzatorską habilitanta, który aktywnie bierze udział w życiu społeczności naukowej i wspierania młodej kadry.

Konkluzja końcowa

Biorąc pod uwagę osiągnięcia związane z przedstawionym cyklem publikacji oraz dorobkiem naukowym, stwierdzam, że wymagania określone w ustawie o stopniach i tytule naukowym są spełnione i na tej podstawie wnoszę o przejście do następnego etapu postępowania habilitacyjnego w celu nadania doktorowi inżynierowi Tomaszowi Hyli stopnia naukowego doktora habilitowanego nauk technicznych w dziedzinie informatyka.