

w Warszawie. Stopień naukowy doktora w zakresie dyscypliny nauki o polityce uzyskał na Wydziale Nauk Społecznych Uniwersytetu im. Adama Mickiewicza w Poznaniu.

Naukowo związany jest z Zakładem Polityki Publicznej w Instytucie Politologii Uniwersytetu Zielonogórskiego. Jest także członkiem Zielonogórskiego Oddziału Polskiego Towarzystwa Nauk Politycznych (PTNP). Piastował również stanowisko kierownika studiów podyplomowych *Zarządzanie środkami bezzwrotnej pomocy Unii Europejskiej z elementami prawa europejskiego*. Jest autorem ponad 100 artykułów popularnych, popularno-naukowych i naukowych z zakresu polityki regionalnej, wykorzystania funduszy Unii Europejskiej, samorządu terytorialnego, integracji europejskiej i polityki rolnej.

Pracę zawodową w administracji rozpoczął w roku 1997 w Urzędzie Wojewódzkim w Zielonej Górze. Współuczestniczył w realizacji pilotażowego programu „Ekorozwój w Euroregionie Sprewa-Nysa-Bóbr” realizowanego w ramach Phare INRED. Od stycznia 1999 r. pracował w Urzędzie

Marszałkowskim Województwa Lubuskiego pełniąc funkcje od starszego referenta do zastępcy dyrektora Departamentu Polityki Regionalnej. Od lutego 2007 r. jako zastępca burmistrza miasta Żagań odpowiadał między innymi za realizację inwestycji współfinansowanych ze środków Unii Europejskiej. W okresie tym reprezentował miasto Żagań w zarządzie Łużyckiego Związku Gmin. Od listopada 2008 r. pełnił funkcję dyrektora Departamentu Rozwoju Regionalnego i Planowania Przestrzennego, a od lutego 2009 r. do lutego 2010 r. dyrektora Departamentu Lubuskiego Regionalnego Programu Operacyjnego w Urzędzie Marszałkowskim Województwa Lubuskiego. Od 2 marca 2010 roku do 21 października 2011 roku pełnił funkcję Podsekretarza Stanu w Ministerstwie Rozwoju Regionalnego. 9 października 2011 roku uzyskał mandat Posła na Sejm RP dzięki poparciu mieszkańców województwa lubuskiego.

Jarosław Flakowski

NAGRODA SPECJALNA I WYRÓŻNIENIE DLA WMIiE W KONKURSIE POLSKI PRODUKT PRZYSZŁOŚCI!

W XVII edycji Konkursu Polski Produkt Przyszłości organizowanego przez Polską Agencję Rozwoju Przedsiębiorczości Wydział Matematyki, Informatyki i Ekonometrii odnotował wielki sukces, zdobywając jedno z trzech wyróżnień w kategorii „Produkt przyszłości jednostki naukowej” oraz nagrodę specjalną w kategorii „Projekt z branży ICT” dla autorskiego projektu dr. inż. Janusza Jabłońskiego „System kryptograficzny”. Wybrane projekty, nagrodzone i wyróżnione w Konkursie, zgłaszane są co roku przez PARP m.in. do Nagrody Gospodarczej Prezydenta RP i do Konkursu „Teraz Polska”, odnosząc niejednokrotnie znaczące sukcesy w tych przedsięwzięciach.

Nagrodę i wyróżnienie z rąk wicepremiera Janusza Piechocińskiego odebrali 1 grudnia 2014 r. podczas uroczystej gali w Pałacu Łazienkowskim: prorektor ds. rozwoju prof. Andrzej Pieczyński, dziekan WMIiE prof. Longin Rybiński oraz autor projektu dr inż. Janusz Jabłoński. Przy wręczeniu statuetki zwrócono uwagę, że projekt jest nowatorskim połączeniem głębokiej znajomości narzędzi informatycznych z potęgą metod matematycznych, co staje się wyróżnikiem prac badawczych Wydziału i kształcenia na innowacyjnym kierunku studiów *inżynieria danych*.

Galę uświetnił recital Krzysztofa Kiliańskiego.

SYSTEM KRYPTOGRAFICZNY

Proponowane rozwiązanie pozwala na realizację bezwarunkowo bezpiecznego systemu kryptograficznego do zastosowań w teleinformatyce, e-usługach systemach elektronicznego obiegu dokumentów, podnosząc poziom bezpieczeństwa: szyfrowania danych, podpisu cyfrowego, autoryzacji i kontroli dostępu.

Opis rozwiązania

Bezpieczeństwo informacyjne opiera się na zaufaniu w siłę



systemów kryptograficznych wykorzystywanych w przetwarzaniu informacji. Kryptologia jest powszechnie stosowana w zapewnianiu bezpieczeństwa usług handlu elektronicznego, e-administracji, e-zdrowiu oraz w innych e-systemach wymagających ochrony danych osobowych, podpisu cyfrowego oraz autoryzacji i kontroli dostępu. Zaufanie do systemów rośnie wraz ze wzrostem poziomu bezpieczeństwa jako siły wykorzystywanych kryptosystemów. Najbezpieczniejsze, określane również *bezwzględnie bezpiecznymi* korzystają z reguł jednorazowych kluczy szyfrowania (OTP, ang. *One-Time-Pad*).

Ideę proponowanego *bezwzględnie bezpiecznego systemu kryptograficznego* można wyjaśnić w oparciu o *Szyfr Cezara*. Znając tajny klucz szyfrowanie i deszyfrowanie znaków wiadomości jest łatwe, natomiast nie znając generowane są nieczytelne komunikaty. Jednakże, można próbować deszyfrować możliwymi wartościami kluczy oraz wybrać jako klucz tę wartość, dla której komunikat ma sens. Tak ujawniony klucz, umożliwia odczytywanie wiadomości przez nieuprawnionych, powoduje przełamanie systemu kryptograficznego. Zwiększenie nakładu pracy na odtworzenie wiadomości przez nieuprawnionego znajduje odzwierciedlenie we współczynniku określającym poziom bezpieczeństwa obliczeniowego kryptosystemu. Stosując w powyższym przykładzie wymogi OTP, każdy znak każdej z wiadomości byłby szyfrowany innym kluczem, zatem wynikiem deszyfrowania opartego na możliwych kluczach będą dowolne komunikaty rozmiaru szyfrogramu. Tak więc, nie znając utajonego klucza, deszyfrowanie będzie generowało wiele sensownych komunikatów i bez względu na nakład pracy wskazanie komunikatu będącego wiadomością przypomina zgadywanie z poglądowego rysunku. Jednakże, nierozwiązanym pozostaje problem generowania i dystrybucji kluczy jednorazowych (PKD, ang. *Problem Key Distribution*).

Wprowadzone nowości

Nowatorstwo proponowanego rozwiązania polega na zaadoptowaniu reguł OTP w schemacie RSA i generowanie jednorazowych kluczy szyfrowania działaniem przyrostowo-różnicowym oraz wykorzystaniem układów rekonfigurowalnych (FPGA ang. *Field Programmable Gate Array*) w adaptacji kryptoprocatora do zmieniających się wartości kluczy. Zasadniczo problem PKD łagodzony jest systemach kryptograficznych z kluczem publicznym. W takich systemach klucze szyfrowania i deszyfrowania są różne i nie dają się w łatwy sposób wyznaczyć jeden z drugiego, przy czym w zależności od zastosowania jeden z kluczy jest upubliczniony. Często wykorzystywanym kryptosystemem z kluczem publicznym jest RSA. Bezpieczeństwo RSA opiera się na nierozwiązanym problemie logarytmu dyskretnego (DLP, ang. *Discret Logarithm Problem*). Jednakże, upublicznienie jednego z kluczy umożliwia ataki kryptoanalityczne, oparte na faktoryzacji dużych liczb i przełamanie bezpieczeństwa kryptosystemu przez wyznaczenie tajnego klucza RSA. Algorytmy faktoryzacji dużych liczb o złożoności podwykładniczej, takie jak sito ciał liczbowych (GNFS, ang. *General Number Field Sieve*), zdecydowanie obniżają bezpieczeństwo RSA, a próby utrzymania akceptowalnego poziomu bezpieczeństwa powodują spadek efektywności i atrakcyjności tego rozwiązania. Oryginalny pomysł, aby nie publikować podatnej na kryptoanalizę wartości składnika kluczy RSA, ale ukryć go przez „zaszyfowanie” w urządzeniu szyfrującym, spowoduje uodpornienie na efektywne ataki metodami faktoryzacji przy zachowaniu liczność różnych kluczy wystarczającej do re-



FOT. Z WYDZIAŁU MATEMATYKI, INFORMATYKI I EKONOMETRII

alizacji reguł OTP. Publikowana będzie informacja o przyroście zmieniającym wartość klucza. W takim rozwiązaniu, nie znając poprzedniej wartości klucza, można wygenerować wiele różnych i sensownych komunikatów, a wskazanie, który jest wiadomością wymaga zgadywania.

Korzyści wynikające z zastosowania rozwiązania

Proponowane rozwiązanie pozwala realizować bezwarunkowo bezpieczne i odporne na znane metody kryptoanalizy systemy kryptograficzne o szerokim spektrum zastosowań. Każdorazowe użycie systemu powoduje zmianę wartości kluczy, zatem spełnione są obostrzenia dotyczące siły oraz czasu życia kluczy jako haseł, co jest istotne dla spełnienia wymogów formalno-prawnych w większości systemów przetwarzających dane wrażliwe nie tylko w e-administracji. Ponadto podniesienie poziomu bezpieczeństwa kryptosystemu RSA realizowane jest przy znaczącym zmniejszeniu rozmiaru kluczy, co powoduje istotne zmniejszenie zużycia zasobów, takich jak energia, pamięć i powierzchnia układu cyfrowego. Podnosi to atrakcyjność rozwiązania również w systemach mobilnych. Natomiast implementacja rozwiązania z wykorzystaniem układu typu FPGA może znacząco wydłużyć czas życia urządzeń, wpływając korzystnie nie tylko na ekologię.

Porównanie z aktualnym stanem techniki

Współcześnie kryptologia łączy wiedzę matematyczną oraz informatyczną w realizacji kryptosystemów asymetrycznych i symetrycznych dla systemów informatycznych przetwarzających informacje wrażliwe. Liczne incydenty przełamania bezpieczeństwa wskazują, że aktualnie stosowane rozwiązania, takie jak 3DES, AES128, RSA1024, ECC160 oraz inne akceptowane przez uznaną amerykańską jednostkę standaryzującą przetwarzanie informacji NIST (ang. *National Institute of Standards and Technology*), w połączeniu z ułomnymi metodami dystrybucji kluczy nie dają gwarancji bezpieczeństwa na najbliższą przyszłość. Natomiast zaproponowane rozwiązanie umożliwi implementację bezwarunkowo bezpiecznego systemu kryptograficznego z możliwościami wykorzystania w dwuskładnikowym uwierzytelnianiu, które aktualnie zalecane jest jako niezbędne w podnoszeniu bezpieczeństwa e-usług.

Konkurs Polski Produkt Przyszłości promuje i upowszechnia osiągnięcia twórców innowacyjnych wyrobów i technologii. Stanowi również narzędzie służące zmianie postaw

i świadomości w zakresie potrzeby wdrażania innowacji i korzyści wynikających ze współpracy sektora B+R i biznesu.

W siedemnastoletniej historii Konkursu, organizowanego przez Polską Agencję Rozwoju Przedsiębiorczości pod patronatem Ministra Gospodarki, zgłoszono już blisko 800 innowacyjnych projektów. Są to nowości z różnych obszarów techniki, szczególnie z branż: medycznej, farmaceutycznej, elektronicznej i chemicznej. Kapituła Konkursu dotychczas nagrodziła 43 projekty, a 83 przyznała wyróżnienia.

Szereg produktów, opracowanych na bazie prac konkursowych, odniosło sukces rynkowy, zarówno w kraju, jak i za granicą. Wśród laureatów Konkursu są firmy notowane na giełdowym rynku NewConnect, gdzie trafiają młode i nowoczesne spółki z perspektywami rozwoju i wzrostu wartości. Wielu laureatów Konkursu reprezentujących jednostki naukowe może poszczycić się najwyższą kategorią naukową A+, oznaczającą poziom wiodący.

Nagroda i wyróżnienia przyznawane są za produkt, którego projekt:

__ jest doprowadzony najdalej do etapu prac wdrożeniowych (projekt niewdrożony), albo
__ został wdrożony do praktyki produkcyjnej - w okresie od 12 miesięcy do 21 miesięcy przed datą zgłoszenia projektu do Konkursu (projekt wdrożony).

Laureaci Konkursu otrzymują statuetkę, dyplom oraz **prawo do posługiwania się znakiem i hasłem „Polski Produkt Przyszłości”**.

Nagrodą jest również pomoc Agencji w promocji produktu przez m.in.:

__ prezentację na krajowych i zagranicznych targach i wystawach innowacyjności,
__ prezentację w katalogu laureatów Konkursu, przygotowanym w dwóch wersjach językowych, dystrybuowanym w kraju i przez polskie placówki dyplomatyczne za granicą,
__ prezentację na Portalu Innowacji www.pi.gov.pl,
__ udział laureatów Konkursu w konferencjach, seminariach, programach radiowych i telewizyjnych poświęconych tematyce innowacyjności.

Wybrane projekty, nagrodzone i wyróżnione w Konkursie Polski Produkt Przyszłości, zgłaszane są co roku przez PARP m.in. do Nagrody Gospodarczej Prezydenta RP i do Konkursu „Teraz Polska”.

zebrata: redakcja

PROF. RYSZARD RYBSKI UHONOROWANY MEDALEM HUGO-VON-RITGENA

Dr hab. inż. Ryszard Rybski, prof. UZ z Wydziału Elektrotechniki, Informatyki i Telekomunikacji Uniwersytetu Zielonogórskiego **został uhonorowany przez niemiecką uczelnię - Technische Hochschule Mittelhessen medalem Hugo-von-Ritgena**. Jest to najważniejsze wyróżnienie tej uczelni przyznawane osobom w szczególny sposób zasłużonym dla TH Mittelhessen. Profesor Rybski jest dopiero piątym laureatem tej nagrody przyznawanej od 2005 r.

Decyzję o przyznaniu wyróżnienia podjął jednogłośnie senat THM w kwietniu 2014 r., natomiast uroczystość wrę-

czenia medalu odbyła się w Giessen 13 listopada 2014 r.

TH Mittelhessen jest uczelnią techniczną, w której na 11 wydziałach kształcą się ok. 14 tysięcy studentów. Jej główna siedziba znajduje się w Giessen, 80 tysięcznym mieście leżącym w pobliżu Frankfurtu nad Menem. Warto dodać, że w Giessen mieści się również założony w 1607 r. klasycy uniwersytet (Justus-Liebig-Universität), na którym studiuje ok. 25 tysięcy studentów.

Hugo von Ritgen, którego imię nosi wspomniany medal, był znanym, żyjącym w XIX wieku niemieckim architektem