Autoreferat

1. Imię i Nazwisko: dr inż. Tomasz Hyla

2. Posiadane dyplomy, stopnie naukowe – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej

10.2007 – 09-2011 Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Wydział Informatyki, studia doktoranckie, zakończone nadaniem tytułu doktora nauk technicznych, specjalizacja: kryptografia danych

- rozprawa doktorska na temat: *Metoda długookresowego przechowywania elektronicznych dokumentów zdrowotnych*
- pełniłem funkcję przewodniczącego samorządu Doktorantów Wydziału Informatyki ZUT
- rozprawa doktorska została uznana za innowacyjną w ramach projektu systemowego realizowanego przez Wojewódzki Urząd Pracy w Szczecinie „*Inwestycja w wiedzę motorem rozwoju innowacyjności w regionie*" (2009)
- Wyróżnienie w kategorii prac doktorskich w V edycji konkursu (2012) na najlepszą prace dyplomową organizowanego przez Regionalne Centrum Innowacji i Transferu Technologii Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie, przy wsparciu Polskiej Fundacji Przedsiębiorczości, Zachodniopomorskiej Grupy Doradczej Sp. z o.o. oraz INVESTIN Sp. z o.o.

10.2002 – 06.2007 Politechnika Szczecińska, Wydział Informatyki, studia magisterskie zakończone nadaniem tytułu zawodowego magistra inżyniera
kierunek: Informatyka
specjalność: Sieci komputerowe i telekomunikacyjne
kierunek dyplomowania: Inżynieria bezpieczeństwa systemów informatycznych
praca magisterska: "*Smart card implementation of a Fingerprint Feature Extraction and Matching Algorithm compliant with ISO/IEC 19794-8 standard*", na zlecenie firmy Giesecke & Devrient www.gi-de.com, oceniona na ocenę bardzo dobrą.

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych

10.2016 – dziś kierownik Zakładu Ochrony Informacji, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie oraz pełnomocnik Dziekana ds. obsługi projektów

10.2012 – dziś adiunkt, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Wydział Informatyki, Katedra Inżynierii Oprogramowania, Zakład Ochrony Informacji

10.2011 – 09.2012	asystent, Zachodniopomorski Uniwersytet Technologiczny w Szczecinie, Wydział Informatyki, Katedra Inżynierii Oprogramowania, Zespół Ochrony Informacji
02.2012 – 07.2012	wykładowca, Zachodniopomorska Szkoła Biznesu, Szczecin

4. Wskazanie osiągnięcia* wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. 2016 r. poz. 882 ze zm. w Dz. U. z 2016 r. poz. 1311.):

a) tytuł osiągnięcia naukowego

Nowe metody zapewnienia bezpieczeństwa dokumentom elektronicznym

b) (autor/autorzy, tytuł/tytuły publikacji, rok wydania, nazwa wydawnictwa, recenzenci wydawniczy)

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.
   https://link.springer.com/content/pdf/10.1007/978-3-642-33260-9_3.pdf
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.
   http://dx.doi.org/10.1049/iet-ifs.2011.0344
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.
   https://doi.org/10.1007/978-3-662-45237-0_59
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.
   https://doi.org/10.1007/978-3-319-46298-1_34
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.
   https://doi.org/10.1093/comjnl/bxw052
6. Tomasz Hyla, Jerzy Pejaś, **2018,** *Demonstrably Secure Signature Scheme Resistant to k-Traitor Collusion Attack*, IEEE Access, tom 6, str. 50154-50168.
   https://doi.org/10.1109/ACCESS.2018.2868512
7. Tomasz Hyla, **2019**, *Local and Outsourced Simultaneous Verification of Pairing-based Signatures,* Journal of Internet Technology, nr 4/2019. (*artykuł w druku)*

c) omówienie celu naukowego ww. prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

I. Wstęp

Tematyka badań przedstawionych w ramach osiągnięcia naukowego dotyczy nowych metod z zakresu zabezpieczeń dokumentów elektronicznych. Badania należą do dziedziny nauk technicznych do dyscypliny informatyka (dziedzina nauk technicznych) (wg nowej klasyfikacji dziedzin: jest to dziedzina nauk inżynieryjno-technicznych, dyscyplina informatyka techniczna i telekomunikacja). Badania dotyczą cyberbezpieczeństwa, ochrony informacji i kryptografii.

Cyberbezpieczeństwo jest jednym z ważniejszych aspektów bezpieczeństwa państwa, jak również bezpieczeństwa poszczególnych organizacji i przedsiębiorstw. Coraz większa liczba ataków na systemy informatyczne powoduje, że bezpieczeństwo systemów informatycznych staje się nieodłącznym elementem związanym z obroną państwa. Moje badania dotyczą głównie opracowywania nowych mechanizmów zabezpieczeń dla systemów informatycznych, które umożliwią ochronę przed nowymi cyberatakami. Samo wykrywanie i blokowanie cyberataków jest niewystraczające, ważne jest zapewnienie tzw. „bezpieczeństwa przez projekt" (*ang. security by design*).

Systemy informatyczne powinny być zaprojektowane w sposób uniemożliwiający przeprowadzenie jak największej liczby cyberataków. Podstawowe zagrożenia bezpieczeństwa związane z dokumentami elektronicznymi to fałszowanie tożsamości autora lub adresata dokumentu, dostęp nieuprawnionych podmiotów, utrata autentyczności czy utrata wartości prawnej w dłuższym okresie przechowywania. Zagrożenia te powodują, że konieczne jest ciągłe opracowywanie nowych mechanizmów zabezpieczeń dostosowanych do coraz nowszych technologii.

W Polsce problemowi ochrony cyberprzestrzeni poświęcona jest *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020*, która w rozdziale 6 stwierdza, że zachodzi konieczność intensyfikacji działań badawczych i rozwojowych dotyczących nowych zagrożeń związanych z rozwojem rynku usług cyfrowych. Jest to związane z ciągle rosnącą liczbą cyberataków. Dodatkowo w ostatnich latach coraz więcej ataków pochodzi od organizacji będących częścią służb różnych państw. Takie organizacje posiadają dużo większe zasoby oraz są w stanie przeprowadzić dużo bardziej zaawansowane ataki, co wymaga zwiększenia bezpieczeństwa systemów informatycznych, a w szczególności systemów obsługujących infrastrukturę krytyczną.

W niniejszym autoreferacie pojęcie dokumentu jest rozumiane (zgodnie z Ustawą z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2017 poz. 570), jako „stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych". W takim rozumieniu może to być plik pdf, tekstowy, xml lub plik o innym zdefiniowanym formacie. Dokument przechowywany w różnych bazach danych, archiwach, czy rejestrach elektronicznych musi posiadać podstawowe atrybuty bezpieczeństwa. Inna, podobna definicja dokumentu elektronicznego przedstawiona przez Międzynarodową Radę Archiwalną (International Council on Archives, MRA) mówi wprost o konieczności posiadania atrybutów bezpieczeństwa przez dokument elektroniczny. MRA określa, że dokument elektroniczny to „specyficzny fragment wygenerowanej informacji, otrzymanej w wyniku wprowadzenia przy użyciu komputera, która zarazem daje się wprowadzić lub uzupełnić w wyniku działania, zaś ten fragment informacji

powinien obejmować wystarczającą treść (zawartość), kontekst i strukturę, co pozwoli na wykazanie autentyczności dokumentu elektronicznego".

Najbardziej znane ogólne modele opisujące podstawowe właściwości bezpieczeństwa to triada CIA oraz heksada Parkera [8]. Triada CIA posiada następujące atrybuty: poufność, integralność, dostępność i jest często rozszerzana o atrybuty takie jak autentyczność i niezaprzeczalność. Z kolei heksada Parkera definiuje: poufność, integralność, dostępność, autentyczność, posiadanie lub kontrolę i użyteczność.

Badania przedstawione w przedłożonym do oceny cyklu publikacji dotyczą metod z zakresu zabezpieczeń dokumentów elektronicznych. Problemy badawcze dotyczą głównie poufności, autentyczności i integralności dokumentów oraz grup dokumentów. Technologie opisywane w ramach cyklu publikacji mogą być także wykorzystane do zapewniania niezaprzeczalności (w szczególności niezaprzeczalności pochodzenia, czasu utworzenia czy czasu odbioru przez system).

Atrybuty bezpieczeństwa muszą być zachowane podczas całego cyklu życia dokumentu. W przypadku długookresowego przechowywania dokumentów konieczne są dodatkowe atrybuty. Wynika to m.in. z tego, że podpis cyfrowy jest tak długo ważny jak certyfikat kwalifikowany z nim powiązany, a więc zwykle przez okres 2 lat. Po upływie tego okresu należy podjąć dodatkowe działania, aby dokumenty te posiadały nadal atrybuty autentyczności i niezaprzeczalności.

W ramach badań zostały poruszone zagadnienia należące do czterech poniższych grup problemów.

1. Pierwsze zagadnienie dotyczy wykorzystania łańcuchów bloków do zapewnienia niezaprzeczalności dokumentów. W ramach prac związanych z tym zagadnieniem poruszono problem związany z integralnością i niezaprzeczalnością dużej liczby pogrupowanych dokumentów przechowywanych w długim okresie.
2. Drugie zagadnienie dotyczy problemu szyfrowania grupowego dokumentów opartych o struktury dostępu umożliwiające dowolne zdefiniowanie podmiotów mających prawo odszyfrowania dokumentu, a także umożliwiające odbieranie tego prawa.
3. Trzecie poruszone zagadnienie dotyczy problemu certyfikatów, które są uznawane przez wielu ekspertów za źródło wad infrastruktury klucza publicznego (*ang. Public Key Infrastructure, PKI*). Stąd powszechnie uważa się, że ich brak jest źródłem wielu zalet w systemach bezcertyfikatowych oraz w systemach opartych o tożsamość wykorzystujących odwzorowania dwuliniowe. Jednakże problem bezpiecznej dystrybucji klucza publicznego pozostaje w tych systemach nadal otwarty i wymaga dobrego uwierzytelnienia dowolnej kopii klucza publicznego używanego przez osobę podpisującą lub szyfrującą dokument. W ramach prac nad tym zagadnieniem zostały opracowane schematy podpisu i szyfrowania łączące zalety PKI z schematami bezcertyfikatowymi bądź wykorzystującymi certyfikaty niejawne.
4. Ostatnie zagadnienie dotyczy problemów szybkości działania schematów szyfrowania i podpisu opartych na odwzorowaniach dwuliniowych. Operacje obliczenia odwzorowania dwuliniowego, a także niektóre operacje na krzywych eliptycznych są czasochłonne obliczeniowo. W przypadku niewystarczającej mocy obliczeniowej urządzeń wykonujących obliczenia konieczne jest oddelegowanie tych obliczeń do innych wydajniejszych urządzeń. Celem badań nad tym zagadnieniem było sprawdzenie możliwości oraz zaproponowanie sposobu bezpiecznego delegowania tych obliczeń do

niezaufanych serwerów, które nie mogą poznać argumentów obliczeń. Powinna także istnieć możliwość weryfikacji wyniku otrzymanego od niezaufanych serwerów.

Wyniki badań naukowych zawartych w cyklu publikacji mogą być wykorzystane przy budowie nowoczesnych systemów informatycznych zarządzających dokumentami elektronicznymi oraz w systemach zapewniających bezpieczeństwo dokumentów i transakcji elektronicznych, tj. infrastruktura klucza publicznego. PKI umożliwia praktycznie wykorzystanie podpisów elektronicznych w gospodarce. W Polsce proces cyfryzacji postępuje praktycznie we wszystkich dziedzinach gospodarki, zaczynając od systemów podatkowych i kończąc na ochronie zdrowia. Jednocześnie zwiększające się wymagania dotyczące PKI powodują konieczność ciągłej jej modernizacji. Modernizacja PKI podąża w kierunku zastosowania nowych algorytmów i schematów podpisu, a także nowych schematów zarządzania certyfikatami, które spowodują zmniejszenie zaufania do środków organizacyjnych i zwiększenie odporności na większy zakres cyberataków, przy jednoczesnej optymalizacji wykorzystania zasobów w celu zmniejszenia kosztów działalności operacyjnej.

Obecnie poufność w systemach informatycznych jest głównie zapewniania przez kontrolę dostępu. Jedną z zyskujących na popularności metod kontroli dostępu jest tzw. kryptograficzna kontrola dostępu, w której uzyskanie dostępu do zasobu wymaga posiadania odpowiedniego klucza deszyfrującego. Takie podejście zwiększa bezpieczeństwo, gdyż ogranicza liczbę komponentów systemu, które muszą posiadać dostęp do zasobów. Jednakże kryptograficzna kontrola dostępu jest dużo trudniejsza do implementacji w przypadku, gdy istnieje wiele podmiotów mających dostęp do wybranego zasobu. W związku z tym istnieje potrzeba opracowywania nowych schematów szyfrowania, które można by wykorzystać przy tworzeniu takich systemów.

W dalszej części autoreferatu przedstawiono kolejno: opis rozwiązanych problemów badawczych, najważniejsze osiągnięcia naukowe, szczegółowy opis osiągnięć naukowych w podziale na cztery wymienione wyżej grupy problemów oraz inne osiągnięcia naukowe niewchodzące w skład jednotematycznego cyklu publikacji. W ostatniej części autoreferatu został zamieszczony słownik skrótów oraz odnośniki do literatury naukowej.

II. Problemy badawcze i osiągnięcia naukowe

W ramach prac dotyczących zabezpieczeń dokumentów elektronicznych skupiono się na rozwiązaniu szeregu problemów naukowych dotyczących ich długoterminowego przechowywania, ich szyfrowania dla grup użytkowników, odporności schematów podpisu i szyfrowania na ataki odmowy weryfikacji i deszyfrowania. Prace dotyczyły także problemów związanych z wykorzystaniem schematów podpisu cyfrowego i szyfrowania w systemach o ograniczonej mocy obliczeniowej.

Pierwszy problem badawczy dotyczy długoterminowego przechowywania podpisanych cyfrowo dokumentów [2]. Jest to bardzo istotny problem, gdyż w archiwach cyfrowych przechowywana jest coraz większa liczba dokumentów, które w wielu przypadkach są podpisane cyfrowo. W przeciwieństwie do podpisów odręcznych, podpisy cyfrowe nie są ważne bezterminowo. Ich ważność upływa z końcem okresu ważności certyfikatu klucza publicznego wiążącego tożsamość użytkownika z kluczem publicznym, który zwykle nie przekracza okresu 2-3 lat. W przypadku archiwów długookresowych, np. przechowujących dane medyczne, konieczne jest podjęcie czynności, które spowodują przedłużenie ważności podpisu. Podczas projektowania metody przedłużania ważności podpisów związanych z dużą liczbą dokumentów należy uwzględnić kwestie związane z wydajnością systemu. Wiele dokumentów przechowywanych w archiwach długookresowych często dotyczy jednej osoby lub jednego podmiotu. Pojawia się też problem trwałości przechowywanej informacji. Na poziomie pojedynczego dokumentu, integralność, autentyczność i niezaprzeczalność dokumentu można zapewnić za pomocą podpisów cyfrowych i zaufanych znaczników czasu. Jednak zapewnienie możliwości technicznej weryfikacji, umożliwiającej wykazanie, że wszystkie dokumenty należące do tego samego podmiotu są obecne, że żaden dokument nie został usunięty lub dodany do archiwum w sposób nieautoryzowany, wymaga zastosowania dodatkowych mechanizmów zabezpieczeń.

Kolejny problem dotyczy szyfrowania dokumentów na potrzeby wielu użytkowników należących do wielu grup [1]. Obecnie mobilność użytkowników musi być brana pod uwagę przy projektowaniu systemów informatycznych. Użytkownicy przetwarzają informacje wrażliwe, tj. dane osobowe czy plik z wartościową zawartością (umowy, projekty, itp.). Dane są często przechowywane w chmurach zarządzanych przez trzecie strony. Takie podejście jest wygodne, ale powoduje powstanie ryzyk związanych z ochroną informacji, a w szczególności związanych z nieautoryzowanym dostępem oraz brakiem faktycznej kontroli nad danymi. Jedną z metod zredukowania tych ryzyk jest przechowywanie plików w zaszyfrowanej formie. W przypadku organizacji, która przechowuje wiele plików i posiada wielu użytkowników, zaszyfrowanie wszystkiego jednym kluczem zapisanym np. wewnątrz aplikacji nie jest zbyt bezpiecznym podejściem. Użytkownicy powinni mieć dostęp do informacji zgodnie z posiadanymi prawami dostępu. W przypadku, gdy prawo dostępu jest równoznaczne z posiadaniem klucza deszyfrującego, mechanizm szyfrujący powinien umożliwiać szyfrowanie na takim poziomie, aby odzwierciedlić przyznane prawa dostępu, w tym przynależności do grup. Mechanizm taki nie powinien również wymagać od podmiotu szyfrującego wskazania konkretnych użytkowników, a tylko grup.

Następne problemy badawcze są związane z nowymi schematami podpisu i szyfrowania opartymi na odwzorowaniach dwuliniowych [3, 5, 6]. Odwzorowania dwuliniowe umożliwiły zaimplementowanie wielu nowych idei, np. schematów podpisu i szyfrowania opartych na tożsamości. Głównym celem schematów opartych o tożsamość, schematów bezcertyfikatowych i wykorzystujących certyfikaty niejawne było uniknięcie problemu zarządzania certyfikatami.

Jednak w praktyce problem ten został przeniesiony na problemy związane z zarządzaniem tożsamością. Certyfikatem niejawnym jest nazywana wartość liczbowa wiążąca tożsamość użytkownika z kluczem publicznym, która jest sekretem. Czasami pomijana jest nazwa niejawny (*ang. implicit*), co może na pierwszy rzut wprowadzać w błąd sugerując, że są to takie same certyfikaty jak w obecnie używanej infrastrukturze klucza publicznego. Dodatkowo rozwiązanie te generują problemy związane z dystrybucją kluczy publicznych (podatność na ataki podmiany klucza publicznego) i tworzą podatność na atak odmowy deszyfrowania (*ang. Denial of Decryption, DoD*) lub odmowy weryfikacji podpisu (*ang. Denial of Signature Verification, DoSV*). W przypadku ataku DoSV adwersarz nie może podrobić podpisu, ale także autoryzowany użytkownik nie może poprawnie go zweryfikować.

Szyfrowanie bezcertyfikatowe nie wymaga od użytkownika pobrania certyfikatu w celu zaszyfrowania wiadomości, ale brak certyfikatu uniemożliwia także zweryfikowanie przypisania klucza publicznego do tożsamości. W rezultacie podmiot szyfrujący wiadomość może wybrać niepoprawny klucz publiczny lub użyć inny, który nigdy nie był powiązany z odpowiednią osobą, co spowoduje, że odbiorca nie będzie mógł odszyfrować wiadomości. Atak odmowy szyfrowania (DoD) został opisany po raz pierwszy przez Liu et al. [9]. W tym ataku adwersarz nie może zdobyć żadnej sekretnej informacji, ale autoryzowany użytkownik nie jest także w stanie odczytać tej informacji i używać usługi. Ataki DoD i DoSV są atakami na dostępność usługi i umożliwiają sparaliżowanie systemu. Adwersarz jest w stanie przeprowadzić te ataki, ponieważ nie jest poddany procesowi sprawdzenia, czy dany klucz jest rzeczywiście przypisany do danej osoby czy nie.

Ostatnia grupa problemów badawczych jest związana z niewystarczającą mocą obliczeniową urządzeń mobilnych lub serwerów aplikacji [4, 7]. Chmura może być użyta do oddelegowania przechowywania danych lub obliczeń. Delegowanie obliczeń umożliwia przeniesienie intensywnych obliczeniowo operacji poza urządzenie mobilne. Wiele schematów opartych o odwzorowania dwuliniowe umożliwia szyfrowanie dokumentów. W związku z powszechnym użyciem urządzeń mobilnych, konieczne jest także zaimplementowanie aplikacji klienckich dla urządzeń mobilnych, których możliwości obliczeniowe są znacznie mniejsze niż komputerów stacjonarnych. W związku z tym wykonanie zaawansowanych operacji kryptograficznych może odbywać się zbyt wolno, aby zapewnić pozytywne doświadczenie użytkownika. W szczególności w kryptografii opartej o odwzorowanie dwuliniowe występuje klika operacji (obliczenie odwzorowania dwuliniowego, operacje na punktach krzywych eliptycznych), których czas wykonania mierzy się w mili sekundach lub dziesiątkach a nawet setkach milisekund. Dlatego konieczne są metody pozwalające na bezpieczne oddelegowanie obliczeń do chmury. Przy czym najbardziej dostępne są chmury publiczne, co powoduje, że dane przesyłane do obliczenia do chmury muszą zostać przetworzone w taki sposób, aby chmura nie była w stanie poznać oryginalnych argumentów obliczeń, a także musi istnieć sposób weryfikacji wyniku otrzymanego z chmury.

Podobny problem, tylko związany z bardzo dużą liczbą operacji weryfikacji podpisów, występuje w wielu aplikacjach serwerowych. Szczególnie dotyczy to systemów przetwarzających dużą liczbę dokumentów jednocześnie, np. systemów finansowych czy ochrony zdrowia. Jednoczesna weryfikacja dużej liczby podpisów, sięgająca nawet 100 tysięcy podpisów jest wyzwaniem obliczeniowym. Taka sytuacja występuje głównie wtedy, gdy liczba wymaganych weryfikacji podpisów na sekundę zmienia się w czasie i nie opłaca się utrzymywać infrastruktury, która byłaby wykorzystywana tylko kilka dni w roku.

Prowadzone przeze mnie badania miały na celu rozwiązanie przedstawionych powyżej problemów badawczych.

Za najważniejsze wyniki (osiągnięcia) naukowe uznaję:

1) Schemat GER (Group Evidence Record), który jest rozwiązaniem rozszerzającym funkcje specyfikacji ERS (Evidence Record Syntax) [10] i umożliwiającym udowodnienie istnienia grupy dokumentów w długim okresie, zaproponowany w artykule [2].
2) Nowy schemat szyfrowania grupowego wykorzystujący ogólne struktury dostępu, pozwalający na elastyczny wybór grup użytkowników mających prawo do odczytu informacji, bez wymogu znajomości składu grup i umożliwiający użytkownikowi m. in. weryfikację czy jest członkiem autoryzowanej grupy, zaproponowany w artykule [1].
3) Nowy paradygmat nazwany Kryptografią Klucza Publicznego oparty o Certyfikaty Jawne i Niejawne (*ang. Implicit and Explicit Certificates - Based Public Key Cryptography, IEC-PKC*), którego główną zaletą jest zabezpieczenie przed atakiem odmowy deszyfrowania i schemat implementujący ten paradygmat (IE-CBE), zaproponowany w artykule [3].
4) Nowy schemat podpisu cyfrowego oparty o certyfikatach jawnych i niejawnych *(ang. Implicit and Explicit Certificates-Based Hess's Signature, IE-CBHS*), który jest odporny na ataki odmowy podpisu (DoSV). Dodatkowo dla TA niemożliwie jest odtworzenie częściowe klucza prywatnego nawet przy współpracy z podpisującym. Schemat został zaproponowany w artykule [5].
5) Pierwszy schemat podpisu (IE-CBS-kCAA) bazujący na jawnych i niejawnych certyfikatach wykorzystujący metodę konstrukcji klucza zaproponowaną przez Sakai-Kasahara. Bezpieczeństwo tego schematu zależy od trudności rozwiązania problemu obliczeniowego *k*-mCAA, zaproponowanego w artykule [6].
6) Analizę trzech modeli delegowania obliczeń (*ang. computation outsourcing*) do chmury z urządzeń mobilnych oraz propozycję zmodyfikowanej wersji schematu IE-CBE umożliwiającą delegowanie obliczeń do chmury, które zostały opisane w artykule [4].
7) Propozycje zmodyfikowanych algorytmów weryfikacji dla trzech schematów podpisu (CLS scheme [11], CBS scheme II [12], IE-CBHS [4]) umożliwiających bezpieczne delegowanie obliczeń odwzorowania dwuliniowego oraz mnożenia punktu na krzywej eliptycznej przez skalar. W ramach badań przeprowadzono szereg eksperymentów obliczeniowych uwzgledniających różne warianty jednoczesnej weryfikacji 100 tysięcy podpisów, uwzględniającej weryfikacje lokalną, stosującą weryfikację wsadową (*ang. batch verification*) oraz stosującą delegowanie obliczeń do zaufanej chmury, a także bezpieczne delegowanie obliczeń do niezaufanej chmury.

W następnej sekcji autoreferatu zostały opisane szczegółowo osiągnięte wyniki.

III. Opis poszczególnych osiągnięć naukowych

a. Wykorzystanie łańcuchów bloków do zapewnienia długookresowej niezaprzeczalności dokumentów

Prace pokrewne

Najprostszym rozwiązaniem umożliwiającym przedłużenie ważności podpisów cyfrowych jest zastosowanie specyfikacji XADES-A [13], w której opisano sposób ponownego podpisywania dokumentu przed upływem ważności podpisu. Z uwagi na konieczność generowania znacznika czasu dla każdego dokumentu osobno, utworzono specyfikację ERS (Evidence Record Syntax) [10], w której do redukcji liczby wymaganych znaczników czasu wykorzystywane są drzewa Merkla [14]. Propozycje archiwum cyfrowego wykorzystującego ERS przedstawił Blazic et al. [15]. Inne propozycje redukcji wymaganej liczby znaczników czasu przy operacji przedłużania ważności przedstawił Pharow and Blobel [16]. Metody umożliwiające wykrywanie brakujących dokumentów bazują głównie na różnych metodach opartych o łańcuchy skrótów (łańcuchy bloków), czy na bardziej zaawansowanych metodach, np. schematach Haber–Stornetta [17, 18] i Benaloh de Mare [19].

Wkład

W artykule [2] został zaproponowany schemat GER (Group Evidence Record), który jest rozwiązaniem rozszerzającym funkcje ERS i umożliwia udowodnienie istnienia grupy dokumentów w długim okresie. GER podobnie jak ERS używa drzew Merkla do wyliczenia skrótu z rundy, dla którego tworzy się znacznik czasu. Natomiast inaczej niż w ERS tworzone są powiązania pomiędzy skrótami w rundzie i grupie dokumentów, co umożliwia otrzymanie nowych, dodatkowych właściwości, tj.:

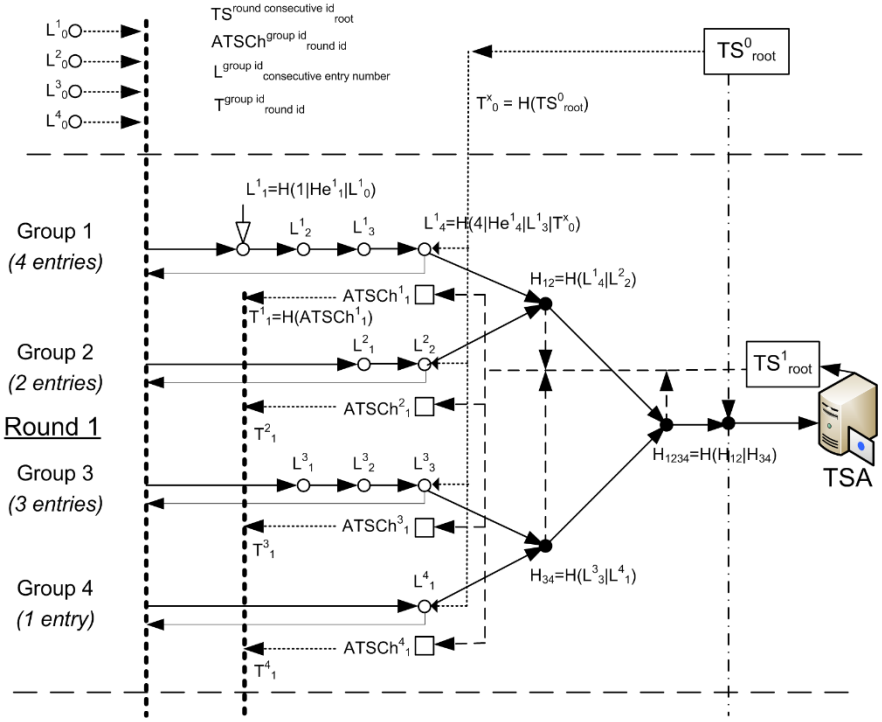
a) Zapewnienie niezaprzeczalności grupy dokumentów w długim okresie, gdzie niezaprzeczalność grupy dokumentów jest osiągana wtedy, gdy spełniony jest wymóg dotyczący integralności grupy dokumentów oraz każdy z dokumentów wchodzących w skład grupy posiada właściwości niezaprzeczalności. Integralność grupy dokumentów oznacza, że można stwierdzić, iż wszystkie dokumenty wchodzące w skład grupy są obecne i porządek w jakim zostały dodane jest zachowany.
b) Optymalizacja operacje ponownego znakowania czasem.

Opis głównych wyników

Dokumenty podpisane cyfrowo przekazywane do archiwum elektronicznego są przetwarzane w rundach. Rundy te są zdefiniowane przez okres *t* lub według maksymalnej liczby dokumentów. Pod koniec każdej rundy, dokumenty są dzielone zgodnie z identyfikatorem grupy. Do każdej grupy dokumentów jest przypisany jeden rekord z poświadczeniami (*ang. evidence rekord*).

Proponowany w ramach schematu algorytm utrzymania ważności podpisu (*ang. Signature Preservation Algorithm, SPA*) składa się z dwóch faz. W pierwszej fazie dokumenty wewnątrz każdej grupy są łączone ze sobą za pomocą jednokierunkowej kryptograficznej funkcji skrótu. Każdy dokument jest powiązany z poprzednim. Pierwszy dokument w danej rundzie jest powiązany z ostatnim dokumentem z poprzedniej rundy i z poprzednim archiwalnym znacznikiem czasu. W drugiej fazie skróty łączące ostatni dokument z każdej grupy są zbierane i stanowią liście drzewa skrótów (patrz Rys. 1). Korzeń drzewa skrótów jest wysyłany do zaufanej

usługi znakowania czasem. Oznaczony czasem skrót jest przechowywany wraz z dodatkowymi informacjami w rekordach poświadczeń osobno dla każdej grupy, do której został dodany dokument w danej rundzie. Ta czynność kończy aktualizację poświadczeń.



Rysunek 1. Obliczanie archiwalnego znacznika czasu w GER (źródło: Fig. 2 [2])

Bezpieczeństwo schematu oparte jest na bezpieczeństwie: jednokierunkowych kryptograficznych funkcji skrótu, algorytmów podpisów cyfrowych i na bezpieczeństwie zaufanej usługi znacznika czasu. Weryfikacja niezaprzeczalności grupy dokumentów jest trzyetapowa i bazuje na rekordach poświadczeń przechowywanych oddzielnie dla każdej grupy. W pierwszym etapie weryfikowane jest powiązanie za pomocą skrótów w danej grupie. W drugim etapie weryfikowane są znaczniki czasu wystawione przez zaufany urząd. W ostatnim kroku weryfikowane są podpisy cyfrowe dołączone do każdego dokumentu w grupie.

b. Szyfrowanie grupowe z wykorzystaniem struktury dostępu

Prace pokrewne

Koncepcja kryptosystemów zorientowanych na grupy (*ang. group-oriented cryptosystem*) została po raz pierwszy zaproponowana przez Desmedt [20] i bazuje na kooperacji wskazanego zbioru autoryzowanych użytkowników tworzących tzw. struktury dostępu.

Wiele schematów szyfrowania grupowego bazuje na tradycyjnej infrastrukturze klucza publicznego (PKI), która opiera się na certyfikatach. Jednakże z uwagi na problemy związane z utrzymaniem infrastruktury do obsługi certyfikatów powstały rozwiązania wykorzystujące kryptografię klucza publicznego opartą na tożsamości *(ang. Identity-based Public Key Cryptography, ID-PKC*) oraz bezcertyfikatową kryptografię klucza publicznego (*ang. Certificateless Public Key Cryptography* CL-PKC). Gentry [21] zaproponował także rozwiązanie wykorzystujące certyfikaty, z tym że w tym przypadku certyfikat jest liczbą używaną podczas szyfrowania lub obliczania podpisu i jest niejawny w przeciwieństwie do tradycyjnej infrastruktury klucza publicznego, gdzie certyfikat jest plikiem (strukturą danych) wiążącą tożsamość użytkownika z

kluczem publicznym. Zaproponowano wiele schematów progowych bazujących na kryptografii opartej o tożsamość, np. [22, 23]. Schematy progowe w porównaniu do schematów bazujących na strukturach dostępu są mniej elastyczne (nieformalnie można stwierdzić, że struktura dostępu pozwala opisać dowolną kombinację użytkowników mających prawo dostępu do zasobu). Jedne z propozycji takich schematów zostały zaproponowane przez Chang et al. [24] i Xu et al. [25].

Wkład

W artykule [1] został zaproponowany schemat CIBE-GAS (*Certificate and ID-based Group Oriented Decryption Scheme with General Access Structure*). Schemat CIBE-GAS jest bardziej elastyczny w porównaniu do schematów progowych i łączy trzy różne idee: metodę podziału sekretu [26], dostępne publiczne dowody przynależności do konkretnej grupy [27] i schemat Sakai-Kasahara IBE (SK-IBE) [28] z modyfikacjami wprowadzonymi przez Fujisaki i Okamoto [29]. Takie podejście pozwoliło na uzyskanie następujących nowych cech:

a) twórca (*ang. originator*) podczas szyfrowania dokumentu nie musi znać struktury zbiorów kwalifikowanych, czyli członków zbioru mających prawo do odczytania informacji;
b) schemat nie wymaga wskazania konkretnego odbiorcy zaszyfrowanej informacji, dodatkowo wysyłający może tymczasowo pozbawić niektóre podgrupy praw dostępu do zaszyfrowanej informacji;
c) schemat jest połączeniem podejścia opartego na tożsamości i certyfikatach zrealizowanego w taki sposób, że częściowy klucz utworzony przez TA jest publikowany jako certyfikat co umożliwia uproszczenie weryfikacji tożsamości użytkownika;
d) konstrukcja jednego z komponentów publicznych ($k_{i,j}$) umożliwia ochronę przeciwko nieautoryzowanym zmianom wartości sekretnych będących w posiadaniu wszystkich udziałowców, a także pozwala udziałowcowi na sprawdzenie, czy jest członkiem autoryzowanej grupy.

Opis głównych wyników

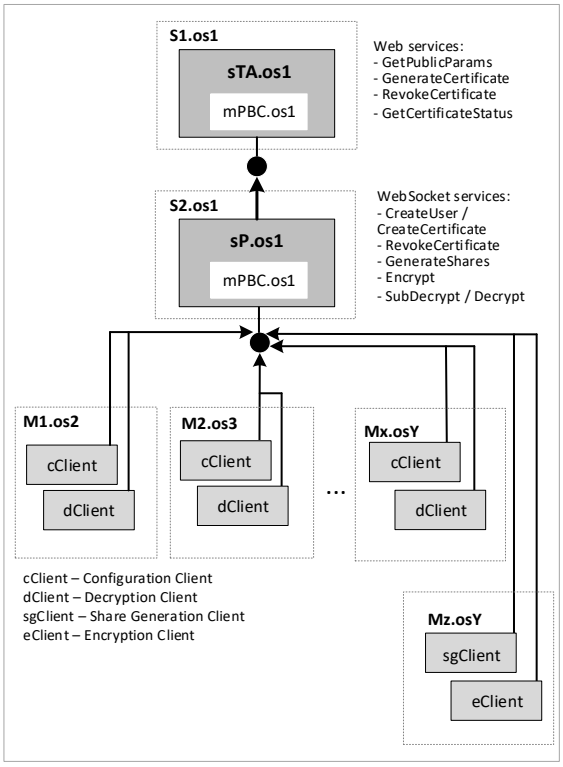
Schemat CIBE-GAS składa się z 8 algorytmów: *Setup*, *SetSecretValue*, *CertGen*, *SetPublicKey*, *ShareDistribution*, *Encryption*, *SubDecrytpion* oraz *Decryption*. Zakłada się, że dany jest: zbiór n elementowy zawierający wszystkich udziałowców $U = \{u_1, u_2, \dots, u_n\}$, rozdający (*ang. dealer*) $D \notin U$ i łączący (*ang. combiner*) $Com \in U$. Działania poszczególnych algorytmów są następujące:

1. *Setup* – algorytm jest uruchamiany przez zaufany urząd (TA), który wybiera losowo klucz prywatny s_i i publiczny P, P_0, a następnie publikuje parametry publiczne.
2. *SetSecretValue* – algorytm jest uruchamiany przez każdego udziałowca oraz rozdającego, którzy losują liczbę losową $s_i \in_R Z_q^*$ oraz obliczają swoje klucze publiczne $Pk_i = (X_i, Y_i)$.
3. *CertGen* – TA dla każdego z użytkowników oblicza i publikuje certyfikat $Cert_i$.
4. *SetPublicKey* – każdy udziałowiec publikuje swój klucz publiczny po sprawdzeniu poprawności certyfikatu.
5. *ShareDistribution* – algorytm jest wykonywany przez rozdającego, który generuje udziały zgodnie z ogólną strukturą dostępu oraz dowody dla każdego z udziałowców i następnie publikuje jawną część danych.
6. *Encryption* – algorytm jest wykonywany przez rozdającego, który dla wiadomości $M \in \{0,1\}^p$ oblicza kryptogram $C = (C_1, C_2, C_3, C_4, C_5, C_6)$.

7. *SubDecryption* – algorytm jest wykonywany przez każdego udziałowca z uprzywilejowanego podzbioru $u_{ij} \in A_j \in \Gamma$, który częściowo deszyfruje wiadomość używając swojego udziału $s_{i,j}$ i zwraca ją łączącemu.
8. *Decryption* – algorytm jest wykonywany przez łączącego (zwykle jednego z użytkowników zbioru uprzywilejowanego), który na podstawie częściowych wartości odszyfrowuje wiadomość *M* oraz sprawdza, czy została poprawnie odszyfrowana.

Przedstawiony schemat CIBE-GAS jest odporny na ataki z wybranym tekstem jawnym (IND-CID-GO-CPA) w modelu z losową wyrocznią (*ang. random oracle model*).

Schemat CIB-GAS został zaimplementowany i przetestowany w ramach projektu MobInfoSec [89]. Utworzona została aplikacja demonstracyjna oparta o chmurę, która składa się dwóch logicznych serwerów udostępniających dwa zestawy usług (patrz Rys. 2). Serwer *sTA* (*ang. Trusted Authority server*) zlokalizowany na serwerze S1 jest odpowiedzialny za zarządzanie parametrami systemowymi, użytkownikami i certyfikatami oraz wykorzystuje bibliotekę mPBC. Biblioteka mPBC zawiera m. in. zaimplementowane algorytmy schematu CIBE-GAS. Drugi serwer *sP* (*ang. secret Protection server*) dostarcza usługi gniazd internetowych, które zawierają operacje kryptograficzne ze schematu CIBE-GAS (m. in. szyfrowanie i częściowe deszyfrowanie), które normalnie byłyby uruchamiane na urządzeniu mobilnym.



Rysunek 2. Architektura aplikacji demonstracyjnej CIBE-GAS oparta o chmurę (źródło: [89])

Przeniesienie operacji kryptograficznych do serwera *sP* z urządzenia mobilnego, eliminuje potrzebę tworzenia biblioteki mPBC dla każdego mobilnego systemu operacyjnego, ale wymaga zapewniania bezpiecznych kanałów komunikacyjnych. Wymaga także, aby serwer *sP* był zaufany i zapewniał przynajmniej taki sam poziom bezpieczeństwa jak serwer *sTA*. Taki wymóg można byłoby uznać za wadę, ale takie podejście upraszcza tworzenie aplikacji klienckich dla urządzeń mobilnych i redukuje liczbę zagadnień związanych z bezpieczeństwem, które należy rozważyć.

c. Schematy podpisu i szyfrowania oparte o certyfikaty jawne i niejawne

Prace pokrewne

Jedną z głównych wad związanych z infrastrukturą klucza publicznego jest konieczność zarządzania wydanymi certyfikatami. Aby rozwiązać ten problem Shamir [30] zaproponował kryptografię opartą na tożsamości (*ang. Identity-based Public Key Cryptography, ID-PKC*). W ID-PKC kluczem publicznym jest tożsamość użytkownika. Jednak główną wadą ID-PKC jest tzw. problem odtworzenia klucza (*ang. key escrow problem*), który polega na tym, że zaufany urząd (*ang. Trusted Authority, TA*) zna klucze prywatne wszystkich użytkowników.

Problem ten został rozwiązany w kryptografii bezcertyfikatowej klucza publicznego (CL-PKC) zaproponowanej przez Al-Riyami and Paterson [31]. W CL-PKC zaufany urząd jest zaangażowany w wydawanie częściowych kluczy prywatnych użytkownika obliczonych z użyciem jego głównego sekretu. Dodatkowo użytkownik niezależnie generuje wartość sekretną, która wchodzi w skład klucza prywatnego. W związku z tym TA nawet znając część klucza prywatnego, nie jest w stanie podszyć się pod użytkownika. Możliwość odtworzenia klucza przez TA jest jedną z głównych wad w szyfrowaniu opartym o tożsamość. Jednakże w związku z brakiem jawnej weryfikacji kluczy publicznych niektóre schematy CL-PKC są podatne na atak podmiany kluczy publicznych (*ang. key replacement attack)*, co zostało wykazane przez Huang et al. [32]. Rozwiązaniem tego ataku było rozwiązanie z użyciem (niejawnych) certyfikatów zaproponowane przez Gentry [21, 33] dotyczące schematu szyfrowania, które szybko zostało uogólnione do certyfikatowych schematów podpisu (Kang et al. [34], Li et al. [35], Li et al. [36] and Wu et al. [12]). W zaproponowanych schematach certyfikat jest w praktyce częścią klucza prywatnego, który jest tajny. Tajność certyfikatu oznacza, że weryfikator podpisu może sprawdzić pośrednio autentyczność certyfikatu i tożsamości, ale nie może już sprawdzić ważności certyfikatu.

Szyfrowanie bezcertyfikatowe (CLE) nie wymaga od użytkownika pobrania certyfikatu w celu zaszyfrowania wiadomości, ale brak certyfikatu uniemożliwia zweryfikowanie przypisania klucza publicznego do tożsamości. W rezultacie podmiot szyfrujący wiadomość może wybrać niepoprawny klucz publiczny. Atak ten został opisany po raz pierwszy przez Liu et al. [9] i został nazwany atakiem odmowy szyfrowania (*ang. Denial of Decryption, DoD*). Niestety schemat szyfrowania oparty o certyfikaty (*ang. Certificate-Based Encryption, CBE*) wprowadzony przez Gentry w 2003 [21], także nie jest odporny na atak DoD. Wynika to głównie z faktu, że wydawany certyfikat jest częścią klucza prywatnego i jest to certyfikat niejawny, który musi pozostać sekretem. Certyfikat ten wiąże klucz publiczny z tożsamością, ale nie może być wykorzystany do weryfikacji klucza publicznego.

W literaturze istnieją rozwiązania problemu DoD (np. [9, 37, 38]), ale nie ma rozwiązania problemu DoSV. Oczywiście rozwiązanie problemu odporności na atak odmowy szyfrowania (DoSV) jest naturalne w tradycyjnej infrastrukturze klucza publicznego, gdzie wykorzystanie jawnych certyfikatów eliminuje ten problem.

Jedno z pierwszych rozwiązań problemu DoD przedstawili Liu et al. [9], którzy zaproponowali ideę auto-generowanych certyfikatów (*ang. Self-Generated Certificate Public Key Encryption, SGC-PKE*), która wymaga istnienia dwóch kluczy prywatnych. W tych schematach wysyłający może uwierzytelnić swój klucz szyfrujący. Procedura ta przypomina tradycyjne systemy oparte o PKI, ponieważ podmiot wysyłający wiadomość musi pobrać i zweryfikować swój auto-generowany certyfikat. Różnica sprowadza się do innego procesu certyfikacji, gdzie w SGC-PKE certyfikat jest generowany i zarządzany przez użytkownika, a w PKI przez zaufany urząd certyfikacji. Jednak w przypadku systemów globalnych nie stanowi to zaleta.

Schemat IE-CBHS [5] bazuje na schemacie podpisu Hess'a [31, 39, 40], który według technik pokazanych w [41, 42] jest bezpieczny w modelu z losową wyrocznią przy założeniu, że problem Diffiego-Hellmana jest problemem trudnym obliczeniowo. Schemat Hess'a został zaadaptowany w ISO/IEC 14888-3 pod nazwą ISO/IEC 14888-3 IBS-1 [43] oraz w schemacie bezcertyfikatowym AP-CLS (Al-Riyami i Paterson [31]). Niestety AP-CLS w modelu bezpieczeństwa [44] jest podatny na ataki opisane w [32, 45]. W schematach bezcertyfikatowych można wyeliminować możliwość tych ataków stosując ulepszenia zastosowane w [12, 46-48].

Schemat IE-CBS-kCAA bazuje na wariancie trudnego problemu obliczeniowego *k*-CAA, który został zaproponowany przez Mitsunari et al. [49]. Jednym z pierwszych praktycznych przykładów użycia problemu *k*-CAA jest schemat szyfrowania zaproponowany w 2003 roku przez Sakai oraz Kasahara [50], który został później ulepszony przez Zhang et al. [51] i Scott [52]. Konstrukcja klucza bazująca na konstrukcji klucza w schemacie Sakai-Kasahara została zastosowana także w schematach podpisu. Jednym z pierwszych takich schematów podpisu jest schemat ZSS (*ang. ID-based short signature scheme*) zaproponowany w 2004 roku przez Zhang et al. [51]. Hu et al. [53] zademonstrował, że schemat ten jest podatny na ataki podmiany wiadomości i klucza (*ang. message-and-key replacement*). Jednakże schemat jest podstawą wielu schematów podpisu (np. Barreto et al. [54], Du i Wen [55]).

Jednym z pierwszych bezcertyfikatowych schematów podpisu bazujących na problemie *k*-CAA był schemat podpisu zaproponowany przez Du i Wen [56]. Jednakże w 2011 roku Fan et al. [57] i Choi et al. [58] niezależnie pokazali, że schemat nie chroni przez adwersarzem typu *Super Type I* i nie zapewnia 3 poziomu bezpieczeństwa wg skali zaproponowanej przez Girault [66]. Ulepszona wersja schematu [56] zaproponowana przez Fan et al. [57] także nie osiąga 3 poziomu bezpieczeństwa, co zostało pokazane m. in. w pracach [59-61]. Schemat Du i Wen jest podatny na ataki z udziałem adwersarza typu 1, ponieważ nie jest randomizowany. Algorytm randomizowany podczas tworzenia podpisu wykorzystuje liczby losowe, co powoduje, że każdy podpis jest inny.

c.1 Schemat szyfrowania IE-CBE

Wkład

W artykule [3] przedstawiono nowy paradygmat nazwany Kryptografia Klucza Publicznego oparta o Certyfikaty Jawne i Niejawne (*ang. Implicit and Explicit Certificates - Based Public Key Cryptography, IEC-PKC*), który zabezpiecza przed atakiem odmowy deszyfrowania (*ang. Denial of Decryption, DoD*). W artykule tym również zaproponowano schemat implementujący ten paradygmat (IE-CBE). Schemat zachowuje wszystkie zalety kryptografii opartej o certyfikaty (*ang. Certificate-Based Public Key Cryptography, CB-PKC),* tzn. każdy użytkownik otrzymuje od TA certyfikat niejawny jako część swojego klucza prywatnego oraz może wygenerować swój klucz prywatny i odpowiadający mu klucz publiczny. Dodatkowo w schemacie IE-CBE, TA generuje certyfikat jawny dla użytkownika z konkretną tożsamością i kluczem publicznym. Funkcja certyfikatu jawnego jest podobna do funkcji certyfikatu generowanego samodzielnie (*ang. Self-Generated Certificate Public Key Encryption, SGC-PKE*) i funkcji certyfikatu w tradycyjnej kryptografii klucza publicznego (PKC). Jednakże w porównaniu do schematów SGC-PKE, IEC-PKC wymaga wygenerowania jednego sekretnego klucza zamiast dwóch. W porównaniu do SGC-PKE w schemacie IE-CBE TA podpisuje tożsamość użytkownika i klucza publicznego, zamiast podpisywania przez użytkownika swojego certyfikatu z użyciem klucza częściowego wydanego przez TA. Dodatkowo certyfikaty jawne i niejawne są ze sobą powiązane w taki sposób, że nikt nie jest w stanie odtworzyć certyfikatu niejawnego na podstawie certyfikatu jawnego.

Opis głównych wyników

W artykule [3] zaproponowano schemat IE-CBE składający się z 8 algorytmów: *Setup, Create-User, Extract-Partial-Private-Key, Certificate-Generate, Set-Public-Key, Set-Private-Key, Encrypt* oraz *Decrypt.* Konstrukcja schematu bazuje na szyfrowaniu opartym o tożsamość zaproponowanym przez Sakai-Kasahara [28, 62] i szyfrowaniu opartym o certyfikaty zaproponowanym przez Y. Lu i J. Li [63]. Funkcje algorytmów są następujące:

1. *Setup* – TA inicjuje i publikuje wspólne parametry oraz losuje swój klucz prywatny oraz oblicza klucz publiczny.
2. *Create-User* – użytkownik *R* generuje materiał na klucz zawierający klucz prywatny *R* i częściowy klucz publiczny.
3. *Extract-Partial-Private-Key* – TA oblicza zaciemniony częściowy klucz prywatny dla *R*.
4. *Certificate-Generate* – TA używając parametrów otrzymanych od *R* i wartości obliczonych podczas uruchomienia algorytmu *Extract-Partial-Private-Key,* generuje certyfikat jawny dla R.
5. *Set-Private-Key* – podmiot *R* oblicza pełny klucz prywatny.
6. *Encrypt* – wysyłający *S* aby zaszyfrować wiadomość *m* po pierwsze sprawdza autentyczność certyfikatu, wybiera liczbę losową i oblicza szyfrogram *C=(U,V,W)*.
7. *Decrypt* – użytkownik *R* rekonstruuje wiadomość *m* używając szyfrogramu *C*.

Schemat IE-CBE jest IND-CCA2$^-$ bezpieczny i odporny na atak DoD w modelu z losową wyrocznią przy założeniu, że problemy p-BDHI i *k*-CCA są trudnymi problemami obliczeniowymi. W schemacie IE-CBE certyfikaty jawne i niejawne bazują na krótkich schematach podpisu [65, 66] których bezpieczeństwo zależy od rozwiązania trudnego problemu obliczeniowego *k*-CAA. Co oznacza, że jeżeli adwersarz nie jest w stanie podrobić jawnego certyfikatu, to nie jest w stanie przeprowadzić ataku DoD i schemat IE-CBE jest bezpieczny dopóki problem *k*-CCA jest trudnym problemem obliczeniowym. Ponieważ schemat IE-CBE to schemat I-CBE (schemat tylko z certyfikatem niejawnym) wraz z algorytmem *Certificate-Generate*, dlatego w dowodzie bezpieczeństwa zastosowano podobne podejście jak w [9, 37, 38], w którym najpierw pokazano, że schemat I-CBE jest IND-CCA2$^-$ bezpieczny, a w następnym kroku, że IE-CBE jest odporny na atak DoD.

c.2 Schematy podpisu IE-CBHS i IE-CBS-kCAA

Wkład

Pierwszy schemat podpisu odporny na atak DoSV oraz oparty na certyfikatach jawnych i niejawnych został zaproponowany w artykule [5] (*ang. Implicit and Explicit Certificates-Based Hess's Signature, IE-CBHS*). Zastosowanie certyfikatów jawnych i niejawnych łączy cechy tradycyjnej kryptografii klucza publicznego z cechami systemów opartych o certyfikaty niejawne. Schemat jest rozszerzeniem schematów podpisu zaproponowanych przez Hess [39], Wu et al. [12], Huang et al. [46] i jest pierwszym zastosowaniem paradygmatu IEC-PKC dla schematów podpisu. Najważniejsze cechy schematu to:

a) weryfikacja podpisu może być dokonana w dwóch trybach: z użyciem certyfikatu jawnego lub z użyciem wyłącznie certyfikatu niejawnego;
b) oba elementy dwu-komponentowego klucza prywatnego są znane wyłącznie podpisującemu;

c) zastosowanie powiązania pomiędzy funkcjami skrótu H_1, H_2 i H_3, aby spowodować zależność, $H_1 \prec H_2 \prec H_3$, które upraszcza dowody bezpieczeństwa [64];
d) certyfikat jawny podmiotu podpisującego jest publiczny; weryfikacja certyfikatu przed weryfikacją podpisu jest podobnym podejściem jak w systemach PKI i powoduje, że schemat jest odporny na ataki DoSV. W przeciwieństwie do tradycyjnych systemów PKI, jawny certyfikat jest liczbą Z_p^*, która jest używana bezpośrednio w równaniach dotyczących weryfikacji podpisu, co upraszcza algorytm weryfikacji certyfikatu.

Następne badania doprowadziły do powstania schematu IE-CBS-kCAA (*ang. Implicit and Explicit Certificate-Based Signature Scheme using Sakai-Kasahara's type keys*). Schemat został opublikowany w artykule [6] i w porównaniu do schematu IE-CBHS posiada inną budowę. Metoda konstrukcji klucza bazuje na metodzie zaproponowanej przez Sakai-Kasahara, a jego bezpieczeństwo zależy od obliczeniowej trudności rozwiązania problemu *k*-mCAA oraz problemu logarytmu dyskretnego. Jest on także skonstruowany w oparciu o asymetryczne odwzorowania dwuliniowe. Taka konstrukcja powoduje uzyskanie schematu o lepszych parametrach wydajnościowych, w szczególności podpisywanie nie wymaga obliczania odwzorowania dwuliniowego, które jest najbardziej czasochłonną operacją.

Opis głównych wyników

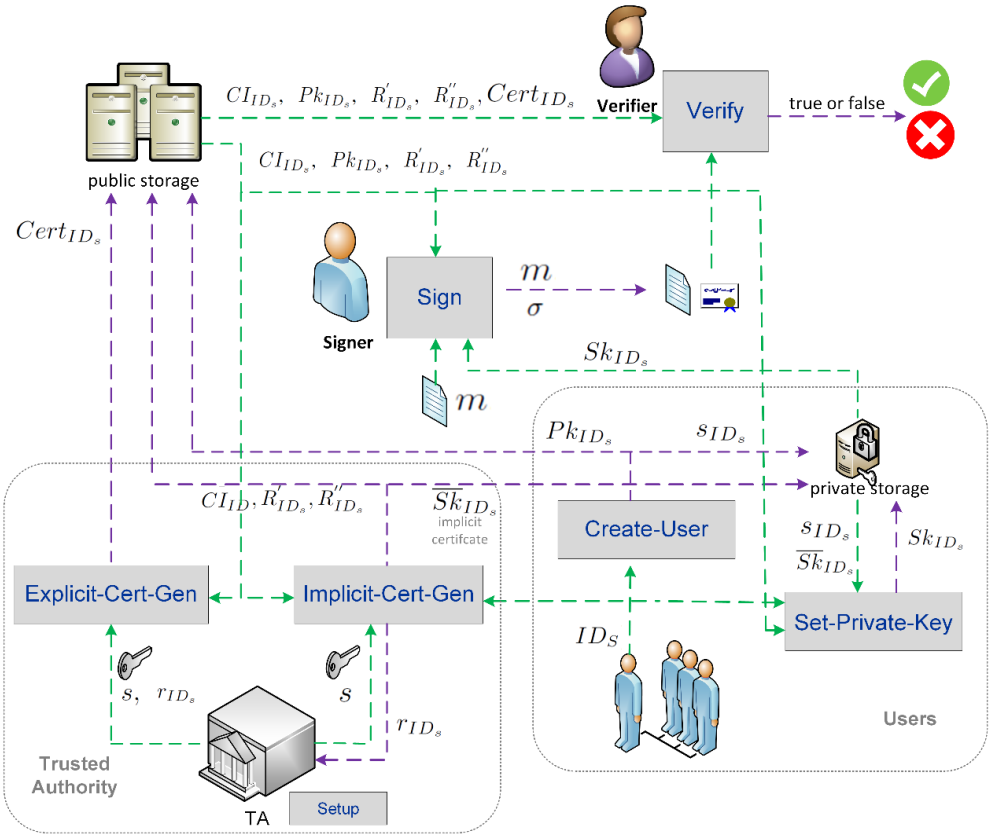
Schemat IE-CBHS obejmuje trzech aktorów: zaufaną stronę (TA), która wydaje certyfikaty jawne i niejawne, podpisującego *S*, który tworzy podpisy oraz odbiorcę wiadomości *R,* który weryfikuje wiadomości. Schemat składa się z 7 algorytmów działających w czasie wielomianowym: *Setup*, *Create-User*, *Implicit-Cert-Gen*, *Explicit-Cert-Gen*, *Set-Private-Key*, *Sign* i *Verify*, których działanie jest następujące:

1. *Setup* – TA ustanawia parametry publiczne oraz swój klucz prywatny i publiczny.
2. *Create*-User – *S* wybiera liczbę sekretną s_{ID_S}oraz tworzy klucz publiczny $Pk_S = s_{ID_S}P$;
3. *Implicit-Cert-Gen* – TA na podstawie tożsamości *S* i jego klucza publicznego Pk_S , generuje częściowy klucz prywatny $\overline{Sk}_{ID_S}$ (niejawny certyfikat), który wraz z dodatkowymi parametrami wysyła sekretnie do *S.*
4. *Explicit-Cert-Gen* – TA używając parametrów otrzymanych od *S* i wartości obliczonych podczas działania algorytmu *Implicit-Cert-Gen,* generuje certyfikat jawny $cert_{ID_S}$.
5. *Set-Private-Key – S* sprawdza $\overline{Sk}_{ID_S}$ i formułuje swój klucz prywatny $Sk_{ID_S} = \left(\overline{Sk}_{ID_S}, s_{ID_S}\right)$.
6. *Sign – S* podpisuje wiadomość *m*, wykorzystując swój klucz prywatny. Dla każdego podpisu wybierane są dwie liczby losowe.
7. *Verify – R* sprawdza podpis wykorzystując certyfikat jawny i klucz publiczny.

W przyjętym w artykule [5] modelu z losową wyrocznią uwzględniono notację bezpieczeństwa (*ang. security notion*) EUF-CMA (*ang. Existential Unforgeability under Chosen Message Attack*). W modelu tym adwersarz może co prawda spowodować, że użytkownik podpisze dowolną adaptacyjnie wybraną przez adwersarza wiadomość, to mimo to nie jest samodzielnie w stanie wygenerować prawidłowej pary wiadomość – podpis. Podobnie jak w notacji zaproponowanej przez Kanga et al. [34] i Gentry et al. [21] oraz innych uwzględniono dwóch adwersarzy. Adwersarz Typu I modeluje rolę nieuczciwego użytkownika, czyli każdego oprócz TA. Natomiast Adwersarz Typu II modeluje rolę nieuczciwego zaufanego urzędu (TA), który zna główny sekret, ale nie może podmienić kluczy publicznych.

Schemat IE-CBS-kCAA jest zdefiniowany przez 7 algorytmów wykonywanych w czasie wielomianowym. Jego konstrukcja jest podobna do schematu IE-CBHS z uwagi na to, że są to

schematy implementujące ten sam paradygmat IE-PKC. Na rys. 3 pokazano przepływ danych, gdy wykonywane są poszczególne algorytmy ze schematu. Działanie algorytmów jest następujące:



Rysunek 3. Przepływ danych w schemacie IE-CBS-kCAA (źródło: [6], graficzny abstrakt dostępny online)

1. *Setup* – TA ustanawia parametry publiczne oraz swój klucz prywatny i publiczny.
2. *Create*-User – użytkownik wybiera liczbę sekretną s_{ID_S} oraz tworzy klucz publiczny $Pk_s = s_{ID_S}P$.
3. *Implicit-Cert-Gen* – TA na podstawie tożsamości S i jego klucza publicznego Pk_s, generuje częściowy klucz prywatny $\overline{Sk}_{ID_S}$ (niejawny certyfikat), informacje o certyfikacie użytkownika CI_{ID_S} oraz dwa komponenty (R'_{ID_S}, R''_{ID_S}), które zawierają klucz sekretny r_{ID_S} certyfikatu jawnego i niejawnego.
4. *Explicit-Cert-Gen* – *TA* używając swojego głównego klucza prywatnego *s,* informacji o certyfikacie użytkownika CI_{ID_S} oraz klucz sekretnego r_{ID_S}, generuje certyfikat jawny $Cert_{ID_S}$.
5. *Set-Private-Key* – użytkownik na podstawie danych otrzymanych po wykonaniu algorytmu *Implicit-Cert-Gen* sprawdza $\overline{Sk}_{ID_S}$ i formułuje swój klucz prywatny $Sk_{ID_S} = (\overline{Sk}_{ID_S}, s_{ID_S})$.
6. *Sign* – użytkownik podpisuje wiadomość *m*, wykorzystując swój klucz prywatny. Dla każdego podpisu wybierane są dwie liczby losowe.
7. *Verify* – weryfikator sprawdza podpis wykorzystując informacje o certyfikacie użytkownika CI_{ID_S}, certyfikat jawny $Cert_{ID_S}$, komponenty (R'_{ID_S}, R''_{ID_S}) oraz klucz publiczny Pk_s.

W artykule [6] został, podobnie jak dla schematu IE-CBHS, umieszczony formalny dowód bezpieczeństwa. Model bezpieczeństwa jest definiowany przez dwie gry prowadzone przez pretendenta (*ang. challenger) C* i adwersarza *A* przy założeniu, że adwersarz wybiera w którą grę zagrać. W obu przypadkach adwersarz $A=(A_1, A_2)$ próbuje przełamać bariery bezpieczeństwa EUF-CMA schematu IE-CBS-kCAA, tzn. formalnego modelu opisującego egzystencjalne fałszerstwo (*ang. existential unforgeability*).

W Tabeli 1 porównano schematy IE-CBHS i IE-CBS-kCAA ze schematami opartymi na certyfikatach niejawnych. W tabeli pokazano liczbę najbardziej czasochłonnych operacji (M_G oznacza mnożenie skalarne (*ang. scalar multiplication*), $\hat{e}$ odwzorowanie dwuliniowe, a P_{GT} potęgowanie w grupie G_T). W związku z podobną konstrukcją ciekawe jest porównanie schematu IE-CBHS do schematu WMSH Scheme II (W. Wu et al. [12]). Zakładając, że certyfikat jawny nie jest dołączony do podpisu (jest to spójne z podejściem stosowanym w PKI), długość podpisu w obu schematach jest taka sama. Obliczenie podpisu jest szybsze w schemacie IE-CBHS, przy wolniejszej weryfikacji. Natomiast schemat IE-CBS-kCAA wymaga podobnej liczby czasochłonnych operacji i jest trochę wydajniejszy od schematu IE-CBHS, szczególnie obliczanie podpisu jest szybsze (potęgowanie w G_T jest szybsze od obliczenia odwzorowania dwuliniowego).

Tabela 1. Porównanie wydajności schematów podpisu (źródło: [5, 6])

Schemat	Typ	Rozmiar klucza publicznego	Rozmiar podpisu	*Sign*	*Verify*	Poziom bezpieczeństwa (typ adwersarza)
LHMSW (J. Li *et al.* [60])	I-CBS	$\|G_1\|$	$2\|G_1\|$	$3 M_G$	$3 \hat{e}$	Normal A_1 i Normal A_2
LHZX (J. Li *et al.* [72])	I-CBS	$2\|G_1\|$	$\|G_1\|$	M_G	$\hat{e}+ M_G$	Normal A_1 i Super A_2
CBSa (Kang *et al.* [58])	I-CBS	$\|G_1\|$	$3\|G_1\|$	$3 M_G$	$3\hat{e}+2 M_G$	Strong A_1 i Strong A_2
WMSH Scheme II (Wu, W., *et al.* [73])	I-CBS	$\|G_1\|$	$\|G_1\| +2\|Z_p\|$	$\hat{e}+4 M_G$	$2\hat{e}+3 M_G$	Super A_1 i Super A_2
IE-CBHS	IE-CBS	$\|G_1\|$	$\|G_1\| +2\|Z_p\|$	$\hat{e}+3 M_G$	$2\hat{e}+7 M_G$	Super A_1 i Super A_2
IE-CBS-kCAA	IE-CBS	$\|G_1\|$	$\|G_2\| +3\|Z_p\|$	$2 M_G + P_{GT}$	$2\hat{e}+6M_G$	Super A_1 i Super A_2

d) Przyspieszenie wykonania weryfikacji i tworzenia podpisów

Prace dotyczące przyspieszenia operacji weryfikacji i tworzenia podpisów z wykorzystaniem delegowania obliczeń były podzielone na dwie części. Pierwsza część dotyczyła przyspieszenia operacji podpisywania na urządzeniach mobilnych, a druga jednoczesnej weryfikacji bardzo dużej liczby podpisów na serwerze.

Prace pokrewne

Delegowanie obliczeń umożliwia przeniesienie złożonych obliczeń poza urządzenia mobilne. W przypadku, gdy obliczenia są delegowane do niezaufanych serwerów (chmur) należy uwzględnić dwie kwestie. Po pierwsze, że dane wysyłane jako argumenty obliczeń mają pozostać prywatne i po drugie, że ważna jest możliwość weryfikacji zwracanego rezultatu. Wiele technik weryfikacji wyników zwracanych przez niezaufane serwery zostało opisanych przez Gennaro et al [67]. Formalne definicje, modele i notacje dla technik bezpiecznego delegowania obliczeń zostały opisane przez Hohenberger i Lysyanskaya [68]. Wcześniej w 2005 roku Girault and Lefranc [69] opisali koncepcję weryfikacji wspomaganej serwerem (*ang. Server-Aided Verification, SAV*).

Jedna z pierwszych prac dotyczących samego delegowania obliczeń odwzorowań dwuliniowych została opublikowana przez Chevallier-Mames et al. [70]. Jednakże całkowity czas wykonania zaproponowanych algorytmów jest dłuższy od czasu lokalnego obliczenia odwzorowania dwuliniowego. Jeden z algorytmów osiąga bezwarunkowe bezpieczeństwo, tzn. nie jest oparty o żadne założenia bezpieczeństwa. Conard et al. [71] zaproponowali bardziej wydajną wersję algorytmu bezpiecznego delegowania obliczeń. Następnie Chen et al. [72] zaproponował algorytm *Pair*. *Pair* jest dużo szybszy, ale jest bezpieczny w modelu OMTUP (*ang. one-malicious version of two untrusted program model)* [68]. W tym modelu istnieją dwa niezaufane serwery U_1 i U_2 z których jeden jest na pewno uczciwy i które nie mogą się same bezpośrednio komunikować. Później Tian et al. [73] zaproponowali ulepszone wersje algorytmu *Pair*, tj. *Algorithm A* i *Algorithm B,* które bazują na podobnej konstrukcji. Kolejne ulepszone wersje tych algorytmów zostały zaproponowane przez Dong et al. [74] i Dong wraz z Ren [75].

Pozostałe obliczeniowo złożone operacje w kryptografii opartej o odwzorowania dwuliniowe to mnożenie punktu na krzywej eliptycznej przez skalar (*ang. scalar multiplication*) i potęgowanie modularne (*ang. modular exponentiation*). Algorytm bezpiecznego delegowania mnożenia skalarnego do chmury przedstawili Hohenberger i Lysyanskaya [68]. Następnie bardziej wydajny algorytm *Exp* zaproponował Chen et al. [75, 77]. Później Wang et al. [78] zaprezentowali wydajny algorytm delegowania potęgowania modularnego, który trudno przekonwertować na algorytm mnożenia punktu na krzywej eliptycznej przez skalar (a w większości przypadku jest to bardzo proste zadanie). Inne prace dotyczące bezpiecznego delegowania potęgowania modularnego opublikowali Ding et al. [79], Nguyen et al. [80], Dijk et al. [81] oraz Zhou i Ren [82].

Podpisy można także weryfikować używając przetwarzania wsadowego. Wsadowy algorytm weryfikacji zwraca prawdę, gdy wszystkie podpisy są poprawne i fałsz w przeciwnym przypadku. Przy czym nie dla każdego algorytmu podpisu istnieje lub da się utworzyć wsadowy algorytm weryfikacji, a wynika to głównie ze względów bezpieczeństwa. Pierwszy algorytm zaproponował Fiat [83], a później kolejny Harn [84]. Algorytmy weryfikacji wsadowej dla schematów opartych o tożsamość zaproponowali Yoon et al. [85] oraz Shi et al. [86], a dla schematów bezcertyfikatowych Geng wraz Zhang [87] i Fan et al. [88].

Wkład

W artykule [5] rozważono różne opcje bezpiecznego delegowania (*ang. secure outsourcing*) obliczeń odwzorowań dwuliniowych do prawdopodobnie nieuczciwych serwerów. Opisano trzy modele delegowania obliczeń, zaproponowano zmodyfikowaną wersję schematu IE-CBE oraz przeprowadzono szereg eksperymentów, które pokazały, że w pewnych warunkach delegowanie obliczeń odwzorowań do chmury przyspiesza całkowity czas obliczeń.

Natomiast w ramach artykułu [7] zostały zmodyfikowane algorytmy weryfikacji z trzech schematów podpisu (CLS scheme [11], CBS scheme II [12], IE-CBHS [5]), w taki sposób aby umożliwić bezpieczne delegowanie obliczeń odwzorowań dwuliniowych oraz mnożenia punktu na krzywej eliptycznej przez skalar. Przeprowadzono szereg eksperymentów obliczeniowych uwzgledniających różne warianty jednoczesnej weryfikacji 100 tysięcy podpisów, włączając weryfikacje lokalną, weryfikację wsadową (*ang. batch verification*) oraz delegowanie obliczeń do zaufanej chmury, a także bezpieczne delegowanie obliczeń do niezaufanej chmury.

Opis głównych wyników

Obliczenie odwzorowania dwuliniowego $\propto = \hat{e}(A, B)$ może być oddelegowane z urządzenia mobilnego T do serwera U używając następujących modeli:

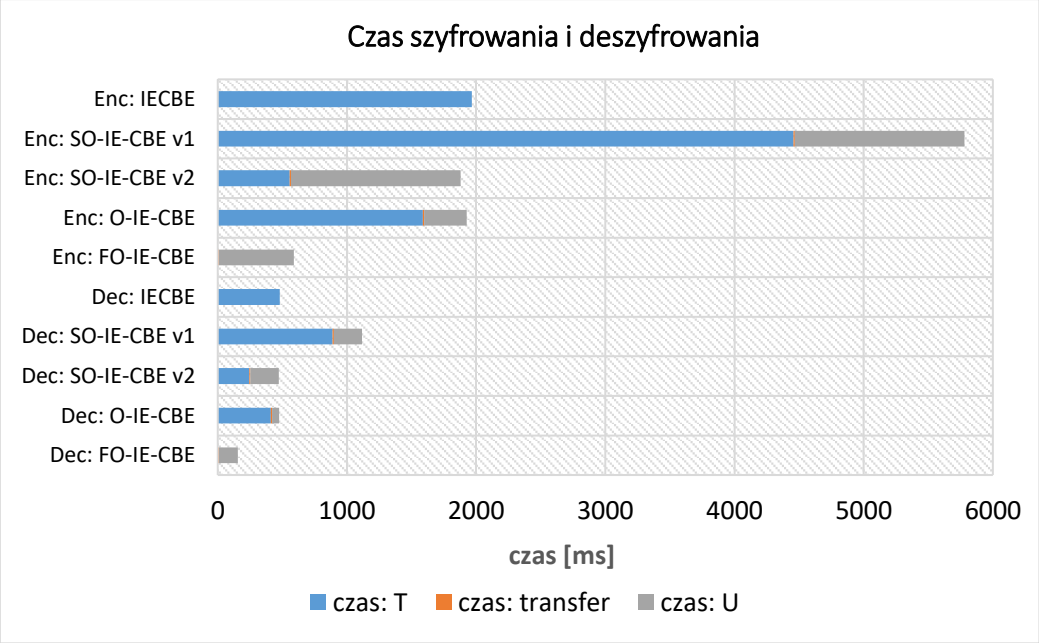
- *Model 0 – No Outsourcing:* obliczenia są dokonywane wyłącznie na urządzeniu mobilnym.
- *Model 1 - Semi-Secure Outsourcing*: U nie zna A i B. Gdy U jest nieuczciwe to nie istnieje mechanizm umożliwiający T weryfikacje, czy $\propto$ jest poprawne.
- *Model 2 - Secure Outsourcing*: U nie zna A i B. T może zweryfikować $\propto$ i U może być nieuczciwy.
- *Model 3 - Full Outsourcing*: urządzenie mobilne jest tylko „cienkim klientem" (*ang. thin client*) i wymaga w pełni zaufanego U. A i B są przesyłane w jawnej formie do U.

Aby umożliwić zastosowanie drugiego z powyższych modeli do schematu IE-CBE, schemat ten został zmodyfikowany i nazwany SO-IE-CBE. Schemat IE-CBE obejmuje trzy podmioty: zaufany urząd (TA), szyfrującego S i deszyfrującego R. Podmioty S i R wykonują cztery algorytmy ze schematu IE-CBE: dwa w fazie konfiguracji (*Create-User, Set-Private-Key*) i dwa algorytmy (*Encrypt, Decrypt*), które mogą być wywoływane wiele razy. Należy zauważyć, że algorytm *Create-User* nie wymaga obliczania odwzorowań dwuliniowych. W artykule [4] zaproponowano dwie wersje schematu IE-CBE wykorzystujące delegowanie obliczeń:

- SO-IE-CBE: ten schemat posiada trzy zmodyfikowane algorytmy (*SO-Set-Private-Key, SO-Encrypt, SO-Decrypt*). Schemat wykorzystuje algorytm bezpiecznego delegowania obliczeń *SO-PAR* do delegowania obliczeń odwzorowań dwuliniowych. Algorytm *SO-PAR* jest bezpiecznym algorytmem delegowania obliczeń symetrycznych odwzorowań dwuliniowych, który na wejściu ma $A, B \in G_1$ i zwraca $\hat{e}(A, B) \in G_2$.
- O-IE-CBE: ten schemat również posiada trzy zmodyfikowane algorytmy (*O-Set-Private-Key, O-Encrypt, O-Decrypt*), ale wykorzystuje częściowo bezpieczny algorytm *O-PAR*, czyli taki który nie sprawdza czy otrzymana wartość odwzorowania została rzeczywiście obliczona prawidłowo przez U.

Schematy SO-IE-CBE i O-IE-CBE opierają się na różnych algorytmach delegowania obliczeń odwzorowania dwuliniowego. W algorytmie *O-Encrypt* występuje także opcjonalny dodatkowy krok umożliwiający wykrycie błędów obliczenia odwzorowania. Zastosowanie bezpiecznego

delegowania obliczeń nie powinno zmienić modelu bezpieczeństwa schematu. W szczególności w przypadku zastosowania bezwarunkowo bezpiecznego algorytmu delegowania obliczeń.



Rysunek 4. Porównanie czasów wykonania dla różnych wariantów delegowania obliczeń (źródło: Fig.1 [4])

Na Rys. 4 pokazano czasy obliczeń operacji szyfrowania i deszyfrowania IE-CBE w środowisku testowym oraz zmodyfikowanej wersji algorytmu wykorzystującej różne modele delegowania obliczeń. Wersja algorytmu z bezpiecznym delegowaniem obliczeń wymaga takiego samego czasu całkowitego lub jest szybsza od algorytmu wykonywanego lokalnie (zależy to od czasu transmisji danych do U oraz różnicy wydajności T i U).

Jednoczesna weryfikacja dużej liczby podpisów wymaga dużej mocy obliczeniowej. Całkowity czas może zostać zmniejszony dziesięciokrotnie przy użyciu wydajniejszych procesorów z dziesięcioma lub więcej rdzeniami. Takie samo przyspieszenie osiągnięto w środowisku testowym przy użyciu bezpiecznego outsourcingu operacji BP (*ang. bilinear pairing*, odwzorowanie dwuliniowe) i SM (*ang. scalar multiplication*), co może przyspieszyć obliczenia o około 10 do 40 razy w zależności od schematu podpisu i konfiguracji chmury. Korzystając z tej samej konfiguracji chmury, możliwe jest osiągnięcie stukrotnego współczynnika przyspieszenia, gdy serwer lokalny byłby 2-3 razy wydajniejszy.

Weryfikacja wsadowa jest prostym rozwiązaniem problemu weryfikacji wielu podpisów jednocześnie w przypadkach, w których wszystkie zweryfikowane podpisy powinny być poprawne. W testowanych przypadkach operację BP w każdym podpisie można było zamienić na jedną operację SM, co znacząco przyspieszyło weryfikację. Jednak, aby utworzyć wsadowy algorytm weryfikacji podpisu, algorytm weryfikacji musi mieć liniową strukturę równania, która zawiera operacje BP i SM. Delegowanie tylko najbardziej czasochłonnych operacji upraszcza proces tworzenia delegowanych wersji algorytmów weryfikacji. W porównaniu z protokołami SAV, zaprojektowanymi oddzielnie dla każdego schematu, bezpieczeństwo schematu używającego delegowanie obliczeń zależy od modelu bezpieczeństwa wykorzystywanego w algorytmie delegowania obliczeń. W Tabeli 3 przedstawiono ogólne porównanie różnych metod jednoczesnej weryfikacji wielu podpisów.

Nawet w przypadku delegowania obliczeń BP i SM do zaufanej chmury trudno jest skrócić całkowity czas weryfikacji 100 tysięcy podpisów do kilku sekund, co wynika z czasu transferu danych i konieczności lokalnego wykonania pozostałych, nieintensywnych obliczeniowo operacji składających się na dany algorytm. Nawet, jeśli całe algorytmy weryfikacji zostaną przekazane do chmury zewnętrznej, trudno będzie zmniejszyć całkowity czas weryfikacji do kilku sekund, gdy podpisane pliki są duże. Jednak powinna istnieć możliwość niewielkiej zmiany schematów (tj. zamiana w algorytmie dokumentu na skrót z dokumentu), co zmniejszy całkowity czas transferu, ale wymaga lokalnego obliczenia skrótów. Po takich modyfikacjach, schematy będą podobne do schematów podpisów używanych obecnie w infrastrukturze klucza publicznego, gdzie w większości przypadków wymagane jest tylko przesłanie skrótu z pliku do chmury w celu przeprowadzenia zewnętrznej weryfikacji.

Tabela 3. Porównanie różnych metod weryfikacji (źródło: Tab. 4 [7])

Metoda	Obliczenia		Całkowita złożoność implementacji	Chmura: wymagania odnośnie implementacji	Chmura: wymagania bezpieczeństwa
	lokalne	zdalne			
weryfikacja lokalna	tak	nie	niska	nie dotyczy	nie dotyczy
weryfikacja wsadowa	tak	nie	średnia	nie dotyczy	nie dotyczy
delegowanie całego algorytmu	nie	tak	niska	cały algorytm weryfikacji	wysokie
delegowanie tylko operacji intensywnych obliczeniowo	tak	tak	średnia	tylko wybrane operacje: BP, SM	wysokie
bezpieczne delegowanie tylko operacji intensywnych obliczeniowo	tak	tak	wysoka	tylko wybrane operacje: BP, SM	niska
bezpieczne delegowanie tylko operacji intensywnych obliczeniowo w modelu OMTUP	tak	tak	wysoka	tylko wybrane operacje: BP, SM	średnie

Eksperymenty pokazują, że korzystanie z bezpiecznego delegowania (outsourcingu) obliczeń z użyciem modelu OMTUP jest tylko około 1,8 do 3,3 razy wolniejsze (w zależności od schematu) niż delegowanie do zaufanej chmury. Dalsze przyspieszenie algorytmów bezpiecznego outsourcingu obliczeń minimalizacji czasu lokalnej weryfikacji otrzymanego wyniku. Istniejące algorytmy o współczynniku wydajności około 0,30 (stosunek operacji wspomagających delegowanie (zaciemnianie argumentów obliczeń, weryfikacja otrzymanego wyniku) wykonywane lokalnie do lokalnego czasu wykonania) wymagają minimum kilku godzin aby zweryfikować 100 tysięcy podpisów.

5. Omówienie pozostałych osiągnięć naukowo – badawczych

5.1 Projekt MobInfoSec

W latach 2012-2015 uczestniczyłem w projekcie pt. *Mobilne urządzenie do ochrony informacji niejawnej* (MobInfoSec) finansowanym przez NCBR w ramach Programu Badań Stosowanych przez konsorcjum Zachodniopomorskiego Uniwersytetu Technologicznego w Szczecinie, Wojskowej Akademii Technicznej z Warszawy oraz Unizeto Technologies SA (obecnie Asseco Data Systems SA). W ramach tego projektu moje osiągnięcia to współudział w opracowaniu systemu MobInfoSec oraz opracowane w ramach jednego z zadań biblioteki mPBC [89], opisanej wcześniej w ramach opisu osiągnieć naukowych.

Problem rozwiązywany przez system MobInfoSec to problem wynikający z braku na rynku oferty dotyczącej transparentnie wymuszanej ochrony informacji wrażliwej pobieranej z różnych źródeł i przechowywanej na urządzeniach mobilnych oraz zapobiegającej jej przekazywaniu osobom trzecim bez zgody dysponenta informacji. Dotyczy on użytkowników urządzeń mobilnych, osób prywatnych, jak również pracowników firm i organizacji, którzy przechowują na urządzeniach mobilnych informacje wrażliwe.

System MobInfoSec jest skierowany do użytkowników (osób fizycznych i prawnych), którzy korzystają (lub chcą korzystać) z systemów kryptograficznej ochrony danych wrażliwych za pomocą urządzeń mobilnych. MobInfoSec jest rozproszonym, modułowym i konfigurowalnym systemem kryptograficznej kontroli dostępu do informacji wrażliwych, działającym w środowisku publicznym. Ponadto posiada jednolity interfejs, pozwalający na korzystanie z wbudowanych w system funkcji. Podstawowe cechy systemu to:

- kryptograficzna ochrona informacji wrażliwej zgodnie z zasadami ORCON określonymi w polityce dostępu;
- ochrona mobilnej informacji oraz zwolnienie użytkownika z obowiązku nadzorowania każdej informacji (w szczególności przed nieautoryzowanym kopiowaniem zabezpieczonych danych);
- umożliwienie stworzenia wiarygodnego mobilnego urządzenia, które będzie realizowało zasady kontroli dostępu do informacji niejawnej zgodne z modelem ORCON;
- umożliwienie zbudowania zaufania do komponentów sprzętowo-programowych urządzenia mobilnego oraz zaufania do innych urządzeń.

W ramach projektu powstał projekt systemu oraz jego wersja demonstracyjna. MobInfoSec otrzymał srebrny medal podczas 113 międzynarodowych targów w Paryżu „Concours Lépine" oraz nagrodę za osiągniecia innowacyjne w 2014 roku na arenie międzynarodowej „Giełda Wynalazków 2015" organizowaną przez Ministra Nauki i Szkolnictwa Wyższego RP.

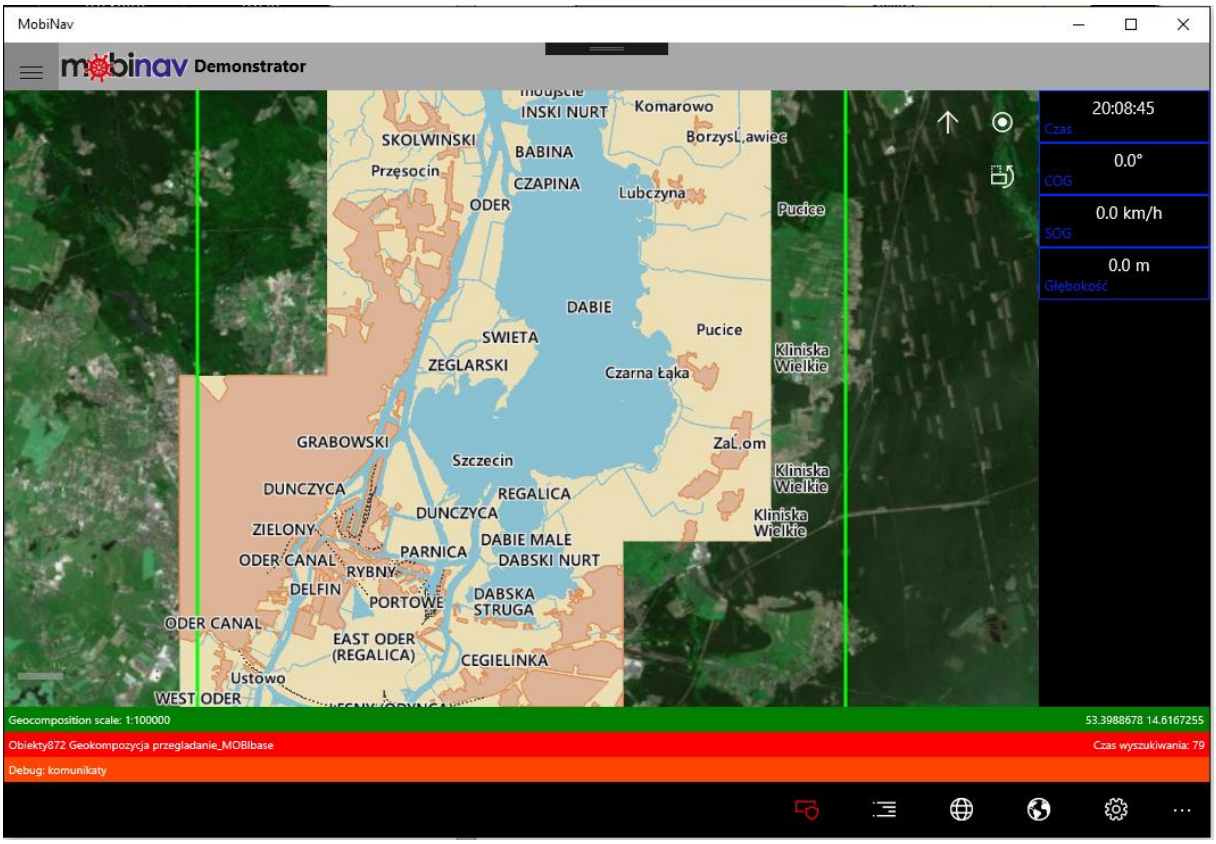
5.2. Projekt MOBINAV

W projekcie pt. *Mobilna nawigacja śródlądowa* (MOBINAV) finansowanym przez NCBR w ramach programu Lider i realizowanym przez Marine Technology Sp. z o.o. brałem udział w latach 2012-2015. W ramach tego projektu moje dwa główne osiągnięcia to opracowanie systemu wspomagania decyzji odnośnie wyznaczania izobaty bezpieczeństwa [90] (wspólnie z dr inż. N. Wawrzyniak) oraz utworzenie demonstratora technologii MOBINAV, gdzie byłem główną osobą odpowiedzialną za prace programistyczne.

W artykule [90] zaproponowano system wspomagania decyzji umożliwiający automatyczne wyznaczanie izobaty bezpieczeństwa wyznaczającej nieżeglowany obszar, na podstawie batymetrycznych danych przestrzennych oraz innych danych takich jak pozycja geograficzna,

wiek danych, typ akwenu i poziom wody. Z uwagi na dużą niepewność danych rozwiązanie wykorzystuje teorię zbiorów przybliżonych do tworzenia reguł decyzyjnych. Reguły decyzyjne zostały utworzone z wykorzystaniem danych eksperymentalnych (rzeczywistych pomiarów głębokości za pomocą echosondy) zebranych na akwenach w okolicach Szczecina.

Demonstrator technologii MOBINAV jest aplikacją uniwersalną Windows 10 zbudowaną przy pomocy Microsoft Visual Studio. Takie podejście umożliwia utworzenie jednej aplikacji, która będzie mogła być uruchomiona na wszystkich urządzeniach mobilnych pracujących pod kontrolą Windowsem 10. Jednocześnie aplikacja posiada interfejs, który się zmienia i dostosowuje w zależności od rodzaju urządzania. Np. na tablecie w pozycji pionowej część pól informacyjnych wyświetla się po prawej stronie (Rys. 5), a na smartfonie w pozycji pionowej te same pola wyświetlają się u góry ekranu.



Rysunek 5. Zrzut ekranu demonstratora systemu MOBINAV działającego na tablecie

Najważniejsze funkcje zaimplementowane w ramach demonstratora systemu to:

- obsługa pliku typu gml (MODEF) z komórką zawierającą mapę zakodowaną wg opracowanego w ramach projektu formatu, wraz z obsługą geometrii zgeneralizowanej w przypadku jej wystąpienia w komórce z mapą;
- obsługa pliku typu json (MONAKO) zawierającego: model wyświetlania poszczególnych jednostek prezentacji kartograficznych w różnych stylach, opis zawartości poszczególnych geokompozycji oraz geokompozycji składowych;
- algorytm wyświetlania obiektów odczytanych z pliku gml MODEF oraz wg definicji z pliku json MONAKO oraz algorytm automatycznego wyboru geokompozycji, a także obsługę WMS;

- obsługa alarmów m. in.: człowiek za burtą, zbliżania do przeszkody nawigacyjnej, zbliżania do obszaru niebezpiecznych głębokości, zbliżania do obszaru niebezpiecznego oraz komunikatów informacyjnych;
- obsługa funkcji związanych z analizami przestrzennymi;
- funkcje związane z sensorami: integracja i wyświetlanie danych z sensorów wewnętrznych urządzenia (pozycja, prędkość, kurs) oraz z sensorów zewnętrznych (m. in. AIS, głębokość) pozyskanych poprzez Wi-Fi.

5.3 Artkuły w recenzji

5.3.1 Certificate-based Group Signature Scheme with Publicly Verifiable General Access Structure

Artykuł został napisany wspólnie z J. Pejasiem i jest w recenzji w czasopiśmie Journal of Computer and System Sciences (IF = 1,497) od września 2017 roku. Mój wkład w powstanie tej pracy polegał na: przygotowaniu analizy prac pokrewnych, współudziale w opracowaniu koncepcji schematu i przygotowaniu dowodu bezpieczeństwa, oraz zaimplementowaniu schematu i wykonaniu testów. Mój udział procentowy szacuje na 50%.

W artykule zaproponowano schemat podpisów grupowych opartych o struktury dostępu. Schemat bazuje na schemacie podziału sekretu (Sang et al. [26]) i schemacie podpisu (Zhang et al. [91]). Schemat jest uogólnionym schematem podpisu grupowego opartym na certyfikatach, który spełnia wymagania dla uogólnionych schematów podpisu, z których najważniejsze to:

- *„forward security”,* które powoduje, że osoba opuszczająca grupę (autoryzowany zbiór) nie może już tworzyć podpisów;
- udziały użytkowników mogą być publicznie weryfikowane;
- schemat zapewnia anonimowość członków autoryzowanego zbioru;
- w przypadku sporu możliwa jest publiczna weryfikacja tożsamości członków danego zbioru;
- autoryzowane zbiory mogą być dynamiczne modyfikowane.

Schemat spełnia wymagania dla schematów podpisu grupowego (*ang. correctness, anonymity, unlinkability, exculpability, traceability, coalition-resistance, forward security*) i jest egzystencjalnie niepodrabialny w przypadku ataku z wybranym tekstem jawnym (EUF-CMA) w modelu z losową wyrocznią zakładając, że problem CDH (*ang. Computational Diffie-Hellman*) jest problemem trudnym obliczeniowo.

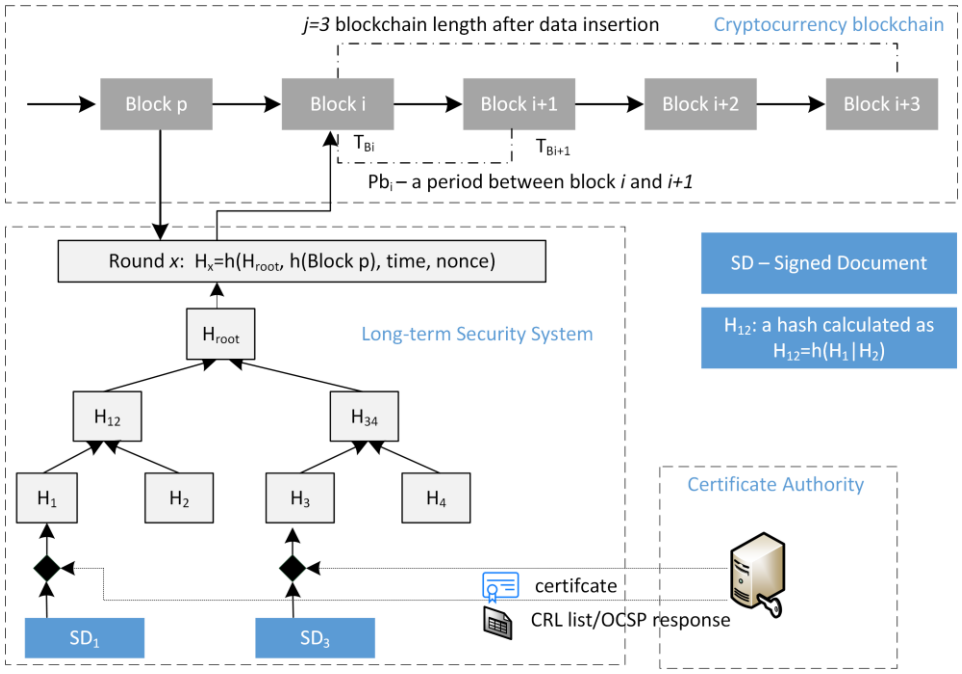
5.3.2 Long-term Verification of Signatures Based on a Blockchain

Artykuł został napisany wspólnie z J. Pejasiem i jest w recenzji w czasopiśmie Computers & Electrical Engineering (IF = 1,747) od października 2018 roku. Mój wkład w powstanie tej pracy polegał na: przygotowaniu wstępu, opracowaniu schematu RBTS i współudziale w wykonaniu analizy bezpieczeństwa. Mój udział procentowy szacuje na 60%.

W artykule zaproponowano schemat Round-based Blockchain Time-stamping Scheme (RBTS) umożliwiający utrzymanie ważności dużej liczby podpisów cyfrowych używając łańcuchów bloków (blockchain) kryptowalut oraz przedstawiono analizę jego bezpieczeństwa. Schemat nie wymaga zastosowania znaczników czasu pochodzących od zaufanych trzecich stron. Bazuje na schemacie Haber-Stornetta [17] i OpenTimestamps [92]. W porównaniu do OpenTiemstamps schemat zawiera nowy algorytm weryfikacji podpisów zgodnie z „*modified shell*

model" [93]. Pozostałe algorytmy zostały także dostosowane w celu wspierania podpisów cyfrowych.

Główną zaletą schematu RBTS jest to, że po dodaniu dokumentów do blockchain'a kryptowaluty, użytkownik może przechowywać podpisany dokument w swoim archiwum bez potrzeby wykonywania czynności konserwacyjnych w przyszłości. Jest to sytuacja przeciwna do występującej w obecnie stosowanej w infrastrukturze klucza publicznego (poza monitorowaniem bezpieczeństwa algorytmów kryptograficznych, które należy także monitorować również w obecnej infrastrukturze klucza publicznego). Schemat jest skalowalny, wymaga wbudowywania stałej liczby bajtów do blockchain'a niezależnie od liczby dokumentów wejściowych. Na Rys. 6 zaprezentowano diagram przedstawiający proces wstawiania dokumentów zgodnie z RBTS.



Rysunek 6. Ilustracja dodawania dokumentów w schemacie RBTS

5.3.3 eHealth Integrity Model Based on a Permissioned Blockchain

Artykuł został napisany wspólnie z J. Pejasiem i jest w recenzji w czasopiśmie Future Internet od stycznia 2019 roku. Jest to wersja rozszerzona artykułu z konferencji ICCSCS 2018 [94]. Mój wkład w powstanie tej pracy polegał na: przygotowaniu koncepcji artykułu, współudziale w opracowaniu modelu i wykonaniu jego analizy, przygotowaniu wstępnej wersji artkułu. Mój udział procentowy szacuje na 60%.

Artykuł zawiera oparty o technologię blockchain model ochrony integralności danych w systemach e-Zdrowia (*ang. Blockchain based eHealth Integrity Model, BEIM*). W modelu wykorzystywane są prywatne blockchain'y (*ang. permissioned blockchain*) oraz przechowywanie informacji poza blockchain *(ang. off-chain storage of information*). W przeciwieństwie do istniejących rozwiązań model umożliwia usuwanie informacji z systemu e-Zdrowia (danych medycznych, czy innych logów). Zwykle w systemach e-Zdrowia dodaje się nowy rekord, a stary oznacza jako nieaktualny i zachowuje, ale istnieją rzadkie przypadki wymagane przez prawo wymagające usuwania rekordów.

W artykule umieszczono także dyskusję na temat problemów związanych z bezpieczeństwem związanych z technologią blockchain, które powinny być rozważane podczas wykorzystania jej w systemach e-Zdrowia. Zaproponowany model można łatwo zintegrować z systemami wykorzystującymi architekturę zorientowaną na usługi. Głównym pytaniem badawczym było ustalenie, czy możliwe jest zaprojektowanie modelu pozwalającego uzyskać transparentność transakcyjną w systemach e-zdrowia, który nie wymaga zaufanych stron trzecich i wspiera usuwanie dokumentów.

Technologia blockchain może być używana do przechowywania kompletnych danych medycznych lub do przechowywania danych związanych z bezpieczeństwem. W BEIM blockchain służy głównie do implementacji usługi integralności danych. Ta usługa może być zaimplementowana przy użyciu innych mechanizmów, ale blockchain zapewnia rozwiązanie, które nie wymaga zaufanych stron trzecich. Ponadto pozwala łączyć ze sobą zapisy dotyczące jednego pacjenta, które są wytwarzane jednocześnie w wielu placówkach opieki zdrowotnej.

Słownik skrótów

BEIM	Blockchain based eHealth Integrity Model
BP	Bilinear Pairing
CBE	Certificate-Based Encryption, szyfrowanie oparte o certyfikaty
CDH	Computational Diffie-Hellman (problem)
CIBE-GAS	Certificate and ID-based Group Oriented Decryption Scheme with General Access Structure
CL-PKC	Certificateless Public Key Cryptography, bezcertyfikatowa kryptografia klucza publicznego
CLE	Certificateless Encryption, szyfrowanie bezcertyfikatowe
DoD	Denial of Decryption, (atak) odmowy szyfrowania
DoSV	Denial of Signature Verification, (atak) odmowy weryfikacji podpisu
ERS	Evidence Record Syntax
GER	Group Evidence Record
ID-PKC	ID-based Public Key Cryptography, kryptografia klucza publicznego oparta o tożsamość
IEC-PKC	Implicit and Explicit Certificates-Based Public Key Cryptography, kryptografia klucza publicznego oparta o certyfikaty jawne i niejawne
IE-CBE	Implicit and Explicit Certificates-Based Encryption
IE-CBHS	Implicit and Explicit Certificates-Based Hess's Signature
IE-CBS-kCAA	Implicit and Explicit Certificate-Based Signature Scheme using Sakai-Kasahara's type keys
O-IE-CBE	Outsourcing-Implicit and Explicit Certificates-Based Encryption
OMTUP	One-Malicious version of Two Untrusted Program model
PKI	Public Key Infrastructure, infrastruktura klucza publicznego
RBTS	Round-based Blockchain Time-stamping Scheme
SAV	Server-Aided Verification, weryfikacja wspomagana serwerem
SK-IBE	Sakai-Kasahara Identity-Based Encryption
SM	Scalar Multiplication
SO-IE-CBE	Secure Outsourcing-Implicit and Explicit Certificates-Based Encryption
sP	secret Protection server
SPA	Signature Preservation Algorithm, algorytm utrzymania ważności podpisu
sTA	Trusted Authority server
TA	Trusted Authority, zaufany urząd

Referencje

Referencje 1-7 to referencje do publikacji z cyklu, przedstawione na stronie 2.

8. Parker, D. B.: *Fighting Computer Crime*, New York, NY, John Wiley & Sons, ISBN 0-471-16378-3, 1998.
9. Liu, J., Au, K., Susilo, W.: *Self-Generated-Certificate Public Key Cryptography and certificateless signature/encryption scheme in the standard model: Extended abstract*. In: Bao, F., Miller, S. (eds.) ASIACCS 2007, pp. 273–283. ACM Press, 2007.
10. Gondrom, T., Brandner, R., Pordesch, U.: *RFC 4998 evidence record syntax (ERS*), 2007.
11. Zhang, L., Zhang, F.: *A New Provably Secure Certificateless Signature Scheme*, 2008 IEEE International Conference on Communications, Beijing, China, pp. 1685-1689, 2008.
12. Wu, W., Mu, Y., Susilo, W., Huang, X.: *Certificate-based signatures revisited*, Journal of Universal Computer Science, Vol. 15, No. 8, pp. 1659-1684, April, 2009.
13. ETSI, TS 101 903, *XML advanced electronic signatures (XAdES),* v1.4, 2009.
14. Merkle, R.C.: *Method of providing digital signatures*, US patent number 4309569, 1982
15. Blazic, A.J., Klobucar, T., Jerman, B.D.: *Long-term trusted preservation service using service interaction protocol and evidence records,* Comput. Stand. Interfaces, 29, pp. 398–412, 2007.
16. Pharow, P., Blobel, B.: *Electronic signatures for long-lasting storage purposes in electronic archives*, Int. J. Med. Inform., 74, pp. 279–287, 2005.
17. Haber, S., Stornetta, W.S.: *How to time-stamp a digital document*, J. Cryptol., 3, (2), pp. 99–111, 1991.
18. Bayer, D., Haber, S., Stornetta, W.S.: *Improving the efficiency and reliability of digital time-stamping*, in Capocelli, R.M., DeSantis, A., Vaccaro, U. (Eds.): 'Sequences'91: methods in Communication, Security, and Computer Science', Springer-Verlag, pp. 329–334, 1992.
19. Benaloh, J., de Mare, M.: *Efficient broadcast time-stamping,* Technical report 1, Department of Mathematics and Computer Science, Clarkson University, August 1991.
20. Desmedt, Y.: *Society and Group Oriented Cryptography: A New Concept*. In: Pomerance, C. (ed.) CRYPTO 1987. LNCS, vol. 293, pp. 120–127. Springer, Heidelberg, 1988.
21. Gentry, C.: *Certificate-based Encryption and the Certificate Revocation Problem*. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 272–293. Springer, Heidelberg, 2003.
22. Baek, J., Zheng, Y.: *Identity-Based Threshold Decryption*. In: Bao, F., Deng, R., Zhou, J. (eds.) PKC 2004. LNCS, vol. 2947, pp. 262–276. Springer, Heidelberg, 2004.
23. Long, Y., Chen, K., Liu, S.: *ID-based threshold decryption secure against adaptive chosen ciphertext attack*. Computers and Electrical Engineering 33(3), 166–176, 2007.
24. Chang, T.-Y.: *An ID-based group-oriented decryption scheme secure against adaptive chosen-ciphertext attacks*. Computer Communications 32(17), 1829–1836, 2009.
25. Xu, C., Zhou, J., Xiao, G.: *General Group Oriented ID-Based Cryptosystems with Chosen Plaintext Security*. International Journal of Network Security 6(1), 1–5, 2008.
26. Sang, Y., Zeng, J., Li, Z., You, L.: *A Secret Sharing Scheme with General Access Structures and its Applications*. International Journal of Advancements in Computing Technology 3(4), 121–128, 2011.
27. Long, Y., Chen, K.-F.: *Construction of Dynamic Threshold Decryption Scheme from Pairing*. International Journal of Network Security 2(2), 111–113, 2006.
28. Sakai, R., Kasahara, M.: *ID based cryptosystems with pairing on elliptic curve*. Cryptology ePrint Archive, Report 2003/054, 2003.
29. Fujisaki, E., Okamoto, T.: *Secure Integration of Asymmetric and Symmetric Encryption Schemes*. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 537–554. Springer, Heidelberg, 1999.
30. Shamir, A.: *Identity-Based Cryptosystems And Signature Schemes.* Advances in Cryptology: Proc. Of Crypto'84 A Workshop on the Theory and Application of Cryptographic Techniques, University of California, Santa Barbara, USA, August 19–22, 1984, LNCS , vol. 196, pp. 47–53. Springer-Verlag, Berlin, 1984.
31. Al-Riyami, S.S., Paterson, K.G.: *Certificateless Public Key Cryptography.* Advances in Cryptology – ASIACRYPT 2003, 9th Int. Conf. on the Theory and Application of Cryptology and Information Security, Taipei, 2003.
32. Huang, X., Susilo, W., Mu, Y. , Zhang, F. : *On the Security of Certificateless Signature Schemes from Asiacrypt 2003*. Cryptology and Network Security, 4th Int. Conf., CANS 2005, Xiamen, China, December 14–16, Lecture Notes in Computer Science 3810, pp. 13–25. Springer, Berlin, 2005.
33. Lu, Y. , *Efficient certificate-based proxy re-encryption scheme for data sharing in public clouds.* KSII Trans. Internet Inf. Syst., 9(7), 2703–2718, 2015.
34. Kang, G., Park, J. H. and Hahn, S. G., *A Certificate-Based Signature Scheme*. Topics in Cryptology – CT-RSA 2004, The Cryptographers' Track at the RSA Conf. 2004, San Francisco, CA, USA, February 23–27, Lecture Notes in Computer Science 2964, pp. 99–111, Springer-Verlag, Berlin, 2004.
35. Li, J., Xu, L., Zhang, Y.: Provably secure certificate based proxy signature schemes. J. Comput., 4, 444–452, 2009.

36. Li, J., Huang, X., Mu, Y., Susilo, W. , Wu, Q.: *Certificate-Based Signature: Security Model and Efficient Construction*. Public Key Infrastructure, 4th European PKI Workshop: Theory and Practice, EuroPKI 2007, Palma de Mallorca, Spain, June 28-30, Lecture Notes in Computer Science 4582, pp. 110–125. Springer-Verlag, Berlin, 2007.
37. Lai, J., Kou, W.: *Self-generated-certificate public key encryption without pairing*. In: Okamoto, T., Wang, X. (eds.) PKC 2007. LNCS, vol. 4450, pp. 476–489. Springer, Heidelberg, 2007.
38. Dent, A.W.: *A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures*. In: Martinelli, F., Preneel, B. (eds.) EuroPKI 2009. LNCS, vol. 6391, pp. 1–16. Springer, Heidelberg, 2010.
39. Hess, F.: *Efficient Identity Based Signature Schemes Based on Pairings. Selected Areas in Cryptography*, 9th Annual Int. Workshop, SAC 2002 St. John's, Newfoundland, Canada, August 15–16, 2002, Lecture Notes in Computer Science 2595, pp. 310–324, Springer, Berlin, 2002.
40. Barreto, P.S.L.M., Libert, B., McCullagh, N. and Quisquater, J. J.:*Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps*. Advances in Cryptology - ASIACRYPT 2005, 11th Int. Conf. on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8, Lecture Notes in Computer Science 3788, pp. 515–532. Springer-Verlag, Berlin, 2005.
41. Pointcheval, D., Stern, J.: *Security Proofs for Signature Schemes.* Advances in Cryptology — EUROCRYPT'96, Int. Conf. on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, Lecture Notes in Computer Science 1070, pp. 387–398. Springer, Berlin, 1996.
42. Pointcheval, D. , Stern, J. :Security arguments for digital signatures and blind signatures. J. Cryptol., 13, 361–396, 2000.
43. ISO/IEC 14888-3 Information Technology – Security Techniques – Digital Signatures with Appendix – Part 3: Discrete Logarithm Based Mechanisms, International Organization for Standardization, Geneva, Switzerland, 2006.
44. Dent, A.W.: *A Brief Introduction to Certificateless Encryption Schemes and Their Infrastructures*. Public Key Infrastructures, Services and Applications, 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10–11, Lecture Notes in Computer Science 6391, pp. 1–16. Springer, Berlin, 2010.
45. Au, M.H., Chen, J., Liu, J.K., Mu, Y., Wong, D.S., Yang, G.: *Malicious KGC Attacks in Certificateless Cryptography.* 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS 2007), Singapore, March 20–22, 2007, pp. 302–311. ACM Press, New York, 2007.
46. Huang, X., Mu, Y., Susilo, W., Wong, D.S., Wu, W.: *Certificateless signatures: new schemes and security models.* Comput. J., 55, 457–474, 2011.
47. Cheng, Z.H. and Comley, R. (2005) *Efficient certificateless public key encryption*. Cryptology ePrint Archive, Report 2005/012. http://eprint.iacr.org/2005/012.
48. Libert, B. and Quisquater, J.J. (2006) *On Constructing Certificateless Cryptosystems from Identity Based Encryption*. Public Key Cryptography - PKC 2006, 9th Int. Conf. on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24–26, Lecture Notes in Computer Science 3958, pp.474–490. Springer, Berlin.
49. Mitsunari, S., Sakai, R., Kasahara, M.: *A new traitor tracing*, IEICE Trans. Fundam. Electron., Commun. Comput. Sci., vol. E85-A, no. 2, pp. 481-484, [Online]. Available: http://ci.nii.ac.jp/naid/110003216755/en/, 2002.
50. Sakai, R, Kasahara, M.: *Id based cryptosystems with pairing on elliptic curve*, IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 2003/054, [Online]. Available: http://eprint.iacr.org/2003/054, 2003.
51. Zhang, F., Safavi-Naini, R., Susilo, W.: *An efficient signature scheme from bilinear pairings and its applications*, in Proc. Int. Workshop Public Key Cryptogr., F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany: Springer, 2004, pp. 277-290.
52. Scott, M.: *Computing the Tate pairing*, in Proc. Cryptographers' Track RSA Conf., A. Menezes, Ed. Berlin, Germany: Springer, 2005,pp. 293-304.
53. Hu, B. C., Wong, D. S., Zhang, Z., Deng, X.: *Certicateless signature: A new security model and an improved generic construction* Des., Codes Cryptogr., vol. 42, no. 2, pp. 109-126, 2007.
54. Barreto, P. S. L. M. , Libert, B., McCullagh, N., Quisquater, J.-J.: *Efficient and provably-secure identity-based signatures and signcryption from bilinear maps*, in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur., B. Roy, Ed. Berlin, Germany: Springer, pp. 515-532, 2005.
55. Du, H., Wen, Q.: *An efficient identity-based short signature scheme from bilinear pairings*, in Proc. Int. Conf. Comput. Intell. Secur. (CIS), pp. 725-729, Dec. 2007.
56. Du, H., Wen, Q.: *Efficient and provably-secure certificateless short signature scheme from bilinear pairings,* Comput. Standards Inter., vol. 31, no. 2, pp. 390-394, 2009.
57. Fan, C.-I., Hsu, R.-H., Ho, P.-H.: *Truly non-repudiation certificateless short signature scheme from bilinear pairings*, J. Inf. Sci. Eng., vol. 27, no. 3, pp. 969-982, 2011.
58. K. Y. Choi, J. H. Park, and D. H. Lee, ``A new provably secure certificateless short signature scheme,'' Comput. Math. Appl., vol. 61, no. 7, pp. 1760-1768, 2011. [Online].
59. Chen, Y. C., Horng, G.: *On the security models for certificateless signature schemes achieving level 3 security*, IACR Cryptol. ePrint Arch., NV, USA, Tech. Rep. 554, 2011.
60. Sharma, G., Bala, S., Verma, A. K.: *On the security of certificateless signature schemes*,' Int. J. Distrib. Sensor Netw., vol. 9, no. 6, p. 102508, 2013.
61. Chen, Y.-C., Tso, R., Horng, G., Fan, C.-I., Hsu, R.-H.: *Strongly secure certificateless signature: Cryptanalysis and improvement of two schemes*, J. Inf. Sci. Eng., vol. 31, no. 1, pp. 297314, 2015.
62. Chen, L., Cheng, Z.: *Security proof of Sakai-Kasahar's identity-based encryption scheme*. In: Smart, N.P. (ed.) Cryptography and Coding 2005. LNCS, vol. 3796, pp. 442–459. Springer, Heidelberg, 2005.

63. Lu, Y., Li, J.: *Constructing Efficient Certificate-based Encryption with Paring*. Journal of Computers 4(1), January 2009.
64. Chatterjee, S. and Kamath, Ch., A closer look at multiple forking: leveraging (In)dependence for a tighter bound. Algorithmica, 74, 1321–1362 , 2016.
65. Huang, X., Mu, Y., Susilo, W., Wong, D. S. , Wu, W.: *Certificateless signatures: New schemes and security models*, Comput. J., vol. 55, no. 4, pp. 457474, Apr. 2012.
66. Girault, M.: *Self-certified public keys,* in Proc. Workshop Theory Appl. Cryptograph. Techn., D. W. Davies, Ed. Berlin, Germany: Springer, pp. 490-497, 1991.
67. Gennaro, R., Gentry, C., Parno, B.: *Non-interactive verifiable computing: Outsourcing computation to untrusted workers*. In: Rabin, T., (ed.) CRYPTO 2010. LNCS 6223, pp. 465–482, Springer, Heidelberg, 2010.
68. Hohenberger, S., Lysyanskaya, A.: *How To Securely Outsource Cryptographic Computations*. In: Kilian, J. (ed.) TCC 2005. LNCS 3378, pp. 264–282, Springer, Heidelberg, 2005.
69. Girault, M., Lefranc, D.: *Server-Aided Verification*: Theory and Practice, in: B. Roy (Ed.) ASIA CRYPT 2005, Chennai (Madras), India, Lecture Notes in Computer Science, Vol. 3788, pp. 605–623, IACR, 2005.
70. Chevallier-Mames, B., Coron, J.S., McCullagh, N., Naccache, D., Scott, M.: *Secure delegation of elliptic-curve pairing*. In: Gollmann, D., Lanet, J.-L., Iguchi-Cartigny, J., (eds.) CARDIS 2010. LNCS 6035, pp. 24–35, Springer, Heidelberg, 2010.
71. Canard, S.: *Delegating a Pairing Can Be Both Secure and Efficient*, in: I. Boureanu, P. Owesarski, and S. Vaudenay (Eds.) International Conference on Applied Cryptography and Network Security 2014, Lausanne, Switzerland, Lecture Notes in Computer Science, Vol. 8479, pp. 549-565, Springer International Publishing, Switzerland, 2014.
72. Chen, X., Susilo, W., Li, J., Wong, D.S., Ma, J., Tang, S., Tang, Q.: *Efficient algorithms for secure outsourcing of bilinear pairings*. Theor. Comput. Sci. 562, 112–121, 2015.
73. Tian, H. , Zhang, F., Ren, K.: *Secure Bilinear Pairing Outsourcing Made More Efficient and Flexible*, in: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, Singapore, Republic of Singapore, pp. 417-426, 2015.
74. Dong, M., Ren, Y., Zhang X*., Fully Verifiable Algorithm for Secure Outsourcing of Bilinear Pairing in Cloud Computing*, KSII Transactions on Internet and Information Systems, Vol. 11, No. 7, pp. 3648-3663, July, 2017.
75. Dong, M., Ren, Y. L.: *Efficient and secure outsourcing of bilinear pairings with single server*, Science China Information Sciences, vol. 61(3): 039104, 2018.
76. Chen, X., Li, J., Ma, J., Tang, Q., Lou, W.: *New Algorithms for Secure Outsourcing of Modular Exponentiations*, in: S. Foresti, M. Yung, and F. Martinelli (Eds.) European Symposium on Research in Computer Security 2012, Pisa, Italy, Lecture Notes in Computer Science, Vol. 7459, pp. 541–556, Springer, Heidelberg, 2012.
77. Chen, X., Li, J., Ma, J., Tang, Q., Lou, W.: *New algorithms for secure outsourcing of modular exponentiations*, IEEE Transactions on Parallel and Distributed Systems, Vol. 25(9), pp. 2386-2396, September, 2014.
78. Wang, Y., et al.: *Securely Outsourcing Exponentiations with Single Untrusted Program for Cloud Storage*, in: M. Kutyłowski and J. Waidya (Eds.): European Symposium on Research in Computer Security 2014, Wroclaw, Poland, Lecture Notes in Computer Science, Vol. 8712, pp. 326-343, Springer International Publishing, Switzerland, 2014.
79. Ding, Y., et al.: *Secure outsourcing of modular exponentiations under single untrusted programme model*, Journal of Computer and System Sciences, Vol. 90, pp. 1-13, December, 2017.
80. Nguyen, P. Q., Shparlinski, I. E., Stern, J.: *Distribution of Modular Sums and the Security of the Server Aided Exponentiation*, in: K. Y. Lam, I. Shparlinski, H. Wang, C. Xing (Eds.), Cryptography and Computational Number Theory. Progress in Computer Science and Applied Logic, Vol. 20, pp. 331-342, Birkhauser Verlag, Basel, Switzerland, 2001.
81. Dijk, M.V., Clarke, D., Gassend, B., Suh, G. E., Devadas*,* S.: *Speeding up Exponentiation using an Untrusted Computational Resource*, Designs, Codes and Cryptography, Vol. 39, No. 2, pp. 253–273, Springer Science+Business Media, May, 2006.
82. Zhou, K., Ren, J.: *Secure Outsourcing of Scalar Multiplication on Elliptic Curves*, IEEE ICC 2016 Communication and Information Systems Security Symposium, Kuala Lumpur, Malaysia, pp. 1-5, 2016.
83. Fiat, A., *Batch RSA*, Journal of Cryptology, Vol. 10, No. 2, pp. 75–88, March, 1997.
84. Harn, L., *Batch verifying multiple RSA digital signatures*, Electronics Letters, Vol. 34, No. 12, pp. 1219–1220, June, 1998.
85. Yoon, H., Cheon, J. H., Kim, Y.: *Batch verifications with ID-based signatures*, in Proceedings of International Conference on Information Security and Cryptology 2004, Seoul, Korea, pp. 233–248, 2004.
86. Shi, C., Pu, D., Choong, W. C.: *An efficient identity-based signature scheme with batch verifications*, in InfoScale '06 Proceedings of the 1st international conference on Scalable information systems, Hong Kong, pp. 1–6, 2006.
87. Geng, M., Zhang, F.: *Batch verification for certificateless signature schemes*, in Proceedings of the International Conference on Computational Intelligence and Security 2009, Beijing, China, pp. 288–292, 2009.
88. Fan, C.-I., Ho, P.-H., Tseng, Y.-F.: *Strongly Secure Certificateless Signature Scheme Supporting Batch Verification*, Mathematical Problems in Engineering, vol. 2014, Article ID 854135, doi:10.1155/2014/854135, 2014.
89. Hyla, T., *Implementation of a Group Encryption System in a Cloud-based Environment*, IARIA XPS Press, ThinkMindTM Digital Library, ICONS2015, ISBN 978-1-61208-399-5, str. 14-18, 2015.
90. Wawrzyniak, N., Hyla, T., *Managing Depth Information Uncertainty in Inland Mobile Navigation Systems,* M. Kryszkiewicz, C. Cornelis, D. Ciucci, J. Medina-Moreno, H. Motoda, Z.W. Raś (edyt.), Rough Sets and Intelligent Systems Paradigms RSEISP 2014, Lecture Notes in Computer Science, tom 8537, Springer, Cham, str. 343-350, 2014.
91. Zhang, Y., Li, J., Wang, Z., Yao, W.: *A New Efficient Certificate-Based Signature Scheme.* Chinese J. Electron. 24, 776–78, 2015.
92. Todd, P.: *Opentimestamps: Scalable, trust-minimized, distributed timestamping with bitcoin*, https://petertodd.org/2016/opentimestampsannouncement, 2016.

93. Baier, H., Karatsiolis, V.: *Validity models of electronic signatures and their enforcement in practice*, in: F. Martinelli, B. Preneel (Eds.), Public Key Infrastructures, Services and Applications: 6th European Workshop, EuroPKI 2009, Pisa, Italy, September 10-11, 2009, Revised Selected Papers, Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 255-270, 2010.
94. Hyla, T.; Pejaś, J., *eHealth Integrity Model Based on a Permissioned Blockchain*, Intern. Conf. on Cyber Security & Communication Systems, Dec. 10-12 2018, Melbourne, Australia; Agbinya, J.I., Ed. Melbourne Institute of Technology, pp. 238–247, 2018.

Tomasz Hyla 08.05.2019