Marek Klonowski

- rok urodzenia: 1979
- e-mail: Marek.Klonowski@pwr.wroc.pl

Przebieg nauki i pracy zawodowej

- od 2006 – praca w Instytucie Matematyki i Informatyki Politechniki Wrocławskiej (asystent, adiunkt)
- 2005 – obrona rozprawy doktorskiej na Uniwersytecie im. Adama Mickiewicza w Poznaniu (nauki matematyczne, informatyka); Tytuł rozprawy: „Algorytmy zapewniające anonimowość i ich analiza", Promotor: prof. Mirosław Kutyłowski
- 2003-2008 – studia doktoranckie na Politechnice Wrocławskiej; dyscyplina matematyka
- 1998-2003 – studia magisterskie na Politechnice Wrocławskiej: kierunek matematyka na Wydziale Podstawowych Problemów Techniki
- 1998-2003 – studia magisterskie na Politechnice Wrocławskiej: kierunek informatyka na Wydziale Informatyki i Zarządzania

Zainteresowania naukowe

- Anonimowa komunikacja
- E-Voting
- Podpisy cyfrowe
- Algorytmy dla systemów urządzeń o silnie ograniczonych zasobach

Anonimowa komunikacja Początkowym obiektem moich badań były protokoły mające zapewnić anonimowość w środowisku rozproszonym, w szczególności te najbardziej znane - *MIX* oraz *onion routing*. Z tematyką tą związane są moje obie rozprawy doktorskie. Mocno upraszczając, protokoły te mają zapewnić, że adwersarz obserwując ich przebieg nie jest w stanie stwierdzić czy dwie strony prowadzą między sobą komunikację.

W tym nurcie badań wraz z M. Kutyłowskim i M. Gomułkiewiczem napisałem pracę, która w formalny sposób bada anonimowość uzyskiwaną w systemie wyborów elektronicznych Davida Chauma ([23]). Główny wynik pracy pokazywał wysoki poziom bezpieczeństwa badanego protokołu już po stałej liczbie kroków (to znaczy niezależnie rozmiaru danych wejściowych). Analiza ta ma zastosowanie dla wszystkich schematów opartych o protokół MIX, który używa metody *ranomized partial checking*.

W tym samym gronie autorów napisaliśmy też pracę badającą protokół onion routing w tak zwanym modelu BFT ([21]). Głównym rezultatem było wykazanie, że wystarczy $O(\log(n))$ kroków, aby uzyskać wysoki poziom anonimowości. Jest to istotna poprawa wyniku zaprezentowanego w innych publikacjach na ten temat. W kolejnej pracy napisanej wspólnie z M. Kutyłowskim badana była *równoległa kaskada MIXów -PMC* ([18]). Analiza zawarta w wymienionych pracach oparta była w dużej mierze na badaniu łańcuchów Markowa i korzystała z metod *couplingowych*.

Inne wyniki dotyczące anonimowej komunikacji, pisane z różnymi współautorami dotyczyły modyfikacji protokołu *onion routing* mających na celu uodpornienie go na tak zwany *atak powtórzeniowy* ([2, 20]) oraz dostosowanie protokołu do możliwości sieci o ograniczonych mocach obliczeniowych ([19]). Inna praca z tego cyklu prezentuje protokół odporny na awarie serwerów co czyni go możliwym do zaimplementowania w sieciach o dużej dynamice ([22]).

Problem anonimowej komunikacji poruszany był także w pracach [3] oraz [15].

E-Voting Zajmowałem się także tematyką wyborów elektronicznych w kontekście szerszym niż jedynie analiza anonimowości głosujących jaką muszą zapewniać. Jestem współautorem pracy, która przedstawia nowy protokół wyborów elektronicznych, zapewniający szereg pożądanych cech – między innymi weryfikowalność oraz odporność na sprzedaż głosów ([16]). Przyczyniłem się też do powstania pracy, która prezentuje kilka nowych klas ataków na uznane protokoły wyborów elektronicznych, opartych głównie o techniki *kleptograficzne* ([13]). Ostatnio, wspólnie z J.Boroń zaproponowałem uogólniony schemat wyborów Ivona Desmedta (z ISC 2005) dla ordynacji SVT (Single-Transferabel-Vote). Wynik ten został zgłoszony do publikacji.

Podpisy cyfrowe W latach 2004-2007 pracowałem nad zagadnieniami związąnymi z technologiami podpisu cyfrowego. Wraz z M. Kutyłowskim, A. Lauks oraz F. Zagórskim w pracy [14] zaprezentowałem schemat podpisu cyfrowego, który może być zweryfikowany dopiero po ujawnieniu innego podpisu. Co ważne, drugi podpis nie musi istnieć w momencie tworzenia pierwszego.

Praca [12] napisana w tym samym zespole prezentuje schemat podpisu *reszyfrowalnego*, który może zostać reszyfrowany wielokrotnie przed weryfikacją. W pracy [10], wraz z A.Lauks pokazaliśmy kilka schematów podpisów cyfrowych, które umożliwiają trzeciej, częściowo zaufanej stronie modyfikowanie podpisanej wiadomości, tak aby podpis pod wiadomością pozo-

stawał ważny. Schemat zapewnia jednak, że klasa modyfikacji *dozwolonych* jest ściśle ograniczona. Zajmowałem się także innymi klasami podpisów ([5, 11]).

Algorytmy dla systemów urządzeń o silnie ograniczonych zasobach W ostatnich dwóch latach głównym nurtem moich zainteresowań są algorytmy dla urządzeń o bardzo ograniczonych zasobach. Szczególnie dużo czasu poświęciłem na badanie bezpieczeństwa systemów identyfikacji opartych o tzw. RFID-tagi. W pracy [9] zaproponowaliśmy wraz z M. Kutyłowskim oraz J. Cichoniem prosty protokół umożliwiający ochronę przed śledzeniem posiadaczy RFID-tagów. Schemat ten, nie wymaga od RFID-tagów praktycznie żadnych mocy obliczeniowych, dlatego może być stosowany w rzeczywiście istniejących, rozpowszechnionych systemach. W ramach tego nurtu badań w pracy [4] zaproponowaliśmy kolejny schemat budowania mechanizmów bezpieczeństwa w systemach RFID-tagów (szyfrowanie, uwierzytelnianie). Zaproponowane protokoły cechują bardzo małe wymagania sprzętowe (mogą być realizowane przez urządzenia o zaledwie kilkudziesięciu bramkach logicznych) a jednocześnie zapewniają one *dowodliwe* bezpieczeństwo, przy założeniu pewnych realistycznych ograniczeń strony atakującej. Badanie bezpieczeństwa i efektywności zaproponowanych schematów oparte zostało głównie o analizę dyskretnych procesów stochastycznych.

Zajmowałem się także bezpieczeństwem sieci sensorów. W pracy [7] z M. Kutyłowskim, M. Renem i K. Rybarczyk zaproponowaliśmy schemat szyfrowania komunikacji dla sieci sensorów, który zapewnia jednocześnie własności *forward i backward security* i wymagają bardzo małych mocy obliczeniowych.

W ostatnim czasie zajmuję się także podstawowymi algorytmami dla sieci ad-hoc, jak rozgłaszanie czy wybór lidera.

Inne Okazjonalnie pracuję też nad innymi tematami. W pracy [6] wraz z T. Srumińskim zaproponowałem mechanizm *dowodów komunikacji* (proof-of-communication), który stanowi analog dowodów pracy (proof-of-work) R. Rivesta. Wykazaliśmy użyteczność tego narzędzia do walki ze SPAMem poprzez stworzenie implementacji.

Brałem także udział w badaniach zainicjowanych i kierowanych przez J Cichonia, których efektem była formalna analiza obciążenia węzłów w popularnym protokole P2P Chord i jego modyfikacjach ([8]). Temat sieci P2P poruszany był też w pracy [17].

Ostatnio wraz z T. Strumińskim i M. Przykuckim zaproponowałem sposób kodowania danych, który umożliwia trwałe usuwanie zawartości dysków magnetycznych ([1]). Formalna analiza algorytmu wykazała, że schemat ten oferuje bardzo wysoki poziom bezpieczeństwa nawet w obecności adwersarza o bardzo dużych możliwościach.

Najważniejsze Publikacje

[1] **Marek Klonowski**, Michał Przykucki, Tomasz Strumiński. „Data deletion with provable security ” Praca prezentowana na Workshop on Information Security Applications 2008 i zaakceptowana do druku w serii LNCS.

[2] **Marek Klonowski**, Mirosław Kutyłowski, Anna Lauks, „Repelling Detour Attack against Onions with Re-Encryption”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 5037. Zaprezentowana na Applied Cryptography and Network Security 2008.

[3] Jacek Cichoń, **Marek Klonowski**, Mirosław Kutyłowski, „Distributed Verification of Mixing - Local Forking Proofs Model”,Seria Lecture Notes in Computer Science (Springer Verlag) vol. 5107. Zaakceptowana do zaprezentowania na ACISP 2008.

[4] Jacek Cichoń, **Marek Klonowski**, Mirosław Kutyłowski, „Privacy Protection for RFID's – Hidden Subset Identifiers”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 5013. Zaprezentowana na PERVASIVE 2008.

[5] **Marek Klonowski**, Przemysław Kubiak, Mirosław Kutylowski, „ Practical Deniable Encryption”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4910.

[6] **Marek Klonowski**, Tomasz Strumiński, „Proofs of communication and its application for fighting spam”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4910.

[7] **Marek Klonowski**, Mirosław Kutyłowski, Michał Ren, Katarzyna Rybarczyk, „Forward-secure Key Evolution Protocol in Wireless Sensor Networks”. Praca prezentowana na 6th International Conference Cryptology & Network Security, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4856.

[8] Jacek Cichoń, **Marek Klonowski**, Łukasz Krzywiecki, Bartłomiej Różański, Paweł Zieliński, „Random Subsets of Interval and P2P Protocols”,Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4627. Praca prezentowana na RANDOM 2007.

[9] J.Cichoń, **Marek Klonowski**, Mirosław Kutyłowski, „Privacy Protection for Dynamic Systems Based on RFID Tags”, Wydana w *Proceedings of PERCOM 2007 Workshops, IEEE Computer Society*. Praca zaprezentowana na 4th IEEE International Workshop on Pervasive Computing and Communication Security.

[10] **Marek Klonowski**, Anna Lauks, „Extended Sanitizable Signatures”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4296. Praca prezentowana na International Conference on Information Security and Cryptology 2006.

[11] **Marek Klonowski**, Przemyslaw Kubiak, Miroslaw Kutylowski, Anna Lauks, „How to Protect a Signature from Being Schown to a Third Party”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 4083.

[12] **Marek Klonowski**, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski,„Universal Re-Encryption of signatures and controlling anonymous information flow”, Tatra Mountains Mathematical Publications 33(2006).

[13] Marcin Gogolewski, **Marek Klonowski**, Miroslaw Kutylowski, Przemyslaw Kubiak, Anna Lauks,Filip Zagorski, „ Kleptographic Attacks on E-voting Schemes”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3995.

[14] **Marek Klonowski**, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski, „Conditional Digital Signatures”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3592.

[15] Marcin Gogolewski, **Marek Klonowski**, Mirosław Kutyłowski, „Local View Attack on Anonymous Communication”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3679. Praca prezentowana na ESORICS 2005 - European Symposium on Research in Computer Security.

[16] **Marek Klonowski**, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski, „A Practical Voting Scheme with Receipts”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3650.

[17] **Marek Klonowski**, Mirosław Kutyłowski, Bartłomiej Różański, „Hiding Data Sources in P2P Networks”, IOS Press, Amsterdam.

[18] **Marek Klonowski**, Mirosław Kutyłowski, „Provable Anonymity for Networks of Mixes”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3727.

[19] **Marek Klonowski**, Mirosław Kutyłowski, Filip Zagórski, „Anonymous communication with on-line and off-line onion encoding”,Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3381.

[20] Marcin Gomułkiewicz, **Marek Klonowski**, Mirosław Kutyłowski, „Onion Routing Based on Universal Re–Encryption Immune against Repetitive Attack”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3325.

[21] Marcin Gomułkiewicz, **Marek Klonowski**, Mirosław Kutyłowski, „Provable Unlinkability Against Traffic Analysis already after $O(\log(n))$ steps !”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 3225.

[22] Jan Iwanik, **Marek Klonowski**, Mirosław Kutyłowski, „DUO–Onions and Hydra–Onions – failure and adversary resistant onion protocols ”, Communications and Multimedia Security, Springer Verlag 2005.

[23] Marcin Gomułkiewicz, **Marek Klonowski**, Mirosław Kutyłowski, „Rapid mixing and security of Chaum’s visual electronic voting”, Seria Lecture Notes in Computer Science (Springer Verlag) vol. 2808. Praca prezentowana na ESORICS 2003 – European Symposium on Research in Computer Security.