Applied Cryptographic Schemes Based on Discrete Logarithm Problem

mgr inż. Anna Lauks-Dutka

Streszczenie

Niniejsza rozprawa poświęcona jest zagadnieniom związanym z tworzeniem *podpisów cyfrowych* oraz ustanawianiem *anonimowej komunikacji*. W zakresie podpisów cyfrowych zaproponowano rozwiązania, które pozwalają osiągnąć pewne dodatkowe, niestandardowe funkcjonalności istotne z punktu widzenia zastosowań praktycznych. W pracy przedstawiono formalne modele, konstrukcje oparte na problemie Dyskretnego Logarytmu oraz analizy bezpieczeństwa dla trzech wybranych schematów podpisu: *warunkowego podpisu cyfrowego*, *dedykowanego podpisu cyfrowego* i *podpisów modyfikowalnych*.

- W modelu warunkowego podpisu cyfrowego weryfikacja ważności podpisu jest możliwa wyłącznie w przypadku istnienia podpisu dla innej wiadomości. Umożliwia to tworzenie podpisów, które są "uruchamiane" przez inne zdarzenie - podpisanie określonej wiadomości przez stronę trzecią. Przykładową wiadomością może być *"minął moment czasu t"*.

- Model dedykowanego podpisu cyfrowego wprowadza dla wyznaczonego weryfikującego funkcje kary za pokazanie podpisu osobom trzecim. Zaproponowane rozwiązanie wprowadza niezwykle drastyczne konsekwencje: ujawnienie klucza prywatnego wyznaczonego weryfikującego bądź też ujawnienie podpisu wyznaczonego weryfikującego pod pewną niekorzystną dla niego wiadomością.

- Charakterystyczną cechą zaproponowanych w rozprawie tzw. rozszerzonych podpisów modyfikowalnych jest możliwość ściśle ograniczonej modyfikacji pewnych części już podpisanej wiadomości przez wyznaczoną stronę zwaną *cenzorem* bez interakcji z podpisującym i w taki sposób, że podpis pod zmodyfikowaną wiadomością pozostaje ważny.

W dziedzinie anonimowej komunikacji zaproponowano pewne rozszerzenia klasycznego protokołu *trasowania cebulkowego* wykorzystujące metodę *uniwersalnego reszyfrowania*. Zaproponowane rozwiązania, ponownie oparte na

problemie Logarytmu Dyskretnego, są odpowiednie dla środowisk rozproszonych. Są one odporne nie tylko na tzw. *ataki powtórzeniowe* i *przekierowujące* znane z literatury, ale także na pewne nowe ataki aktywne opisane w niniejszej rozprawie: atak polegający na zgadywaniu ścieżki oraz tzw. atak *dwuskokowy*. Rozwiązania przedstawione w rozprawie opierają się na klasycznych technikach El Gamala. Celem były nie tylko nowe funkcjonalności, lecz również osiągnięcie ich na możliwie najprostszej drodze. Jest to motywowane praktyką przemysłową, gdzie prostota rozwiązania oraz powtórne użycie istniejących komponentów jest istotną zaletą.

Rozprawa stanowi podsumowanie rezultatów opublikowanych w następujących artykułach:

1. Marek Klonowski, Mirosław Kutyłowski, Anna Lauks, Filip Zagórski: Conditional Digital Signatures. In: TrustBus'2005, volume 3592 of Lecture Notes in Computer Science, 206-215, 2005.

2. Marek Klonowski, Przemysław Kubiak, Mirosław Kutyłowski, Anna Lauks: How to Protect a Signature from Being Shown to a Third Party. In: TrustBus'2006, volume 4083 of Lecture Notes in Computer Science, 192-202, 2006.

3. Marek Klonowski, Anna Lauks: Extended Sanitizable Signatures. In: ICISC'2006 (Information Security and Cryptology), volume 4296 of Lecture Notes in Computer Science, 343-355, 2006.

4. Klonowski, M., Kutyłowski, M., Lauks, A.:*Repelling Detour Attack against Onions with Re-Encryption*. In: ACNS'2008 (Applied Cryptography and Network Security Conference), volume 5037 of Lecture Notes in Computer Science, 296-308, 2008.

5. Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dutka: Attacking and Repairing the Improved ModOnions Protocol. In: ICISC'2009 (Information, Security and Cryptology), volume 5984 of Lecture Notes in Computer Science, 258-273, 2009.

6. Nikita Borisov, Marek Klonowski, Mirosław Kutyłowski, Anna Lauks-Dutka: Attacking and Repairing the Improved ModOnions Protocol-Tagging Approach. KSII Transactions on Internet and Information Systems 4(3), 380-399, 2010.