mgr Ashutosh Dhar Dwivedi
Cryptanalysis of lightweight ciphers – Rozprawa doktorska
Promotor: dr hab. Paweł Morawiecki, prof. IPI PAN

Streszczenie

Głównym celem pracy jest ocena marginesu bezpieczeństwa wybranych szyfrów kryptografii lekkiej czyli algorytmów działających w środowiskach o mocno ograniczonych zasobach obliczeniowych i pamięciowych. Podstawową techniką w realizacji założonego celu będą współczesne metody i techniki kryptoanalityczne wzbogacone o autorskie udoskonalenia.

W ciągu ostatnich dwóch dekad powstało wiele inicjatyw mających na celu powstanie nowych, bezpiecznych szyfrów. Należą do nich: konkursy Advanced Encryption Standard (AES) oraz Competition for Authenticated Encryption: Security, Applicability and Robustness (CAESAR). Dla nowo zaprojektowanych algorytmów konieczne jest przeprowadzenie szeroko zakrojonej kryptoanalizy, potwierdzającej niezawodność i bezpieczeństwo szyfrów.

Rozprawa rozpoczyna się ogólnym wprowadzeniem do struktur prymitywów kryptograficznych oraz technikami kryptoanalitycznymi, a następnie wynikami dla różnych szyfrów blokowych. W szczególności skupiam się na dwóch szyfrach pochodzących z konkursu CAESAR, a mianowicie na szyfrze blokowym Scream i ASCON. Konkurs CAESAR rozpoczął się w 2014 roku i zyskał dużą uwagę środowiska naukowego. W pierwszej rundzie do CAESARa zgłoszono 57 algorytmów. Scream był jednym z 29 kandydatów, którzy znaleźli się w drugim etapie konkursu, natomiast ASCON jest zwycięzcą jednej z kategorii. Do oceny bezpieczeństwa Scream używam różnych technik kryptoanalitycznych. Po pierwsze, stosuję kryptoanalizę liniową i rozszerzam tę analizę o część różnicową (znaną jako analiza różnicowo-liniowa). Ponadto analizuję szyfr za pomocą niemożliwej kryptoanalizy różnicowej (ang. impossible differential), a następnie badam ścieżkę różnicowo-liniową w scenariuszu z kluczem związanym (ang. related-key). Dla szyfru ASCON stosuję kryptoanalizę SAT w celu odzyskiwania stanu za pomocą narzędzia SAT solver. Uzyskane wyniki prowadzą do wniosku, że ASCON ma wystarczający margines bezpieczeństwa przeciwko kryptoanalizie opartej na problemie spełnialności formuł boolowskich.

W kolejnych rozdziałach koncentruję się na kryptoanalizie różnicowej szyfru SPECK, który został zaprojektowany przez amerykańską Agencję Bezpieczeństwa Narodowego (NSA). Szyfr SPECK należy do klasy szyfrów ARX i jest dedykowany dla środowisk o ograniczonych możliwościach pamięciowo-obliczeniowych. Algorytmy ARX używają trzech operacji: dodawania modulo, rotacji bitowej i operacji eXclusive-OR. Algorytmy te są zwykle mniejsze i szybsze niż projekty oparte na S-boxach. To co z kolei stanowi wyzwanie to kryptoanaliza. W szyfrach typu AES, S-box jest zwykle 8- lub

4-bitowy i taki rozmiar pozwala obliczyć pełny profil różnicowy S-boxa. W przypadku szyfrów ARX źródłem nieliniowości jest operacja dodawania modulo. Rozmiar słowa w takich szyfrach jest zazwyczaj 32- lub 64-bitowy, a przez to skonstruowanie kompletnego profilu różnicowego jest niewykonalne (wymaga $2^{3n} \times 4$ bajtów pamięci dla n-bitowych słów). Dlatego też potrzebujemy wydajnych heurystyk, aby ominąć to ograniczenie. W tym celu zaproponowałem algorytm zainspirowany przez Nested Monte-Carlo Search, aby znaleźć ścieżki różnicowe w szyfrze SPECK i LEA. Zaproponowana metoda osiąga porównywalne wyniki do "state-of-the-art", będąc koncepcyjnie prostszą.

mgr Ashutosh Dhar Dwivedi
Cryptanalysis of lightweight ciphers – Rozprawa doktorska
Promotor: dr hab. Paweł Morawiecki, prof. IPI PAN

ABSTRACT

The goal of the thesis is to evaluate the security margin for selected lightweight ciphers. We focus on two applications: lightweight cryptography and authenticated encryption. The first one is about providing secure communication to devices with constrained resources such as memory and computing power. The authenticated encryption tries to provide confidentiality and authenticity into a single, efficient algorithm.

Recently there have a dozen of interesting, new algorithms, partly as a response to the CAESAR competition (Competition for Authenticated Encryption: Security, Applicability, and Robustness). These new designs can be used in many cryptographic scenarios; therefore, it is necessary to undertake extensisve cryptanalysis, proving its reliability and security. The cryptographic community has invented multiple levels of cryptanalytic methods that target different possible designs and aim to exploit their weaknesses into successful and potentially practical attacks.

The dissertation begins with a general introduction to the structures of cryptographic primitives, and cryptanalytic techniques followed by cryptanalytic results on different block ciphers. In particular, we focus on two ciphers from the CAESAR competition: Scream and ASCON. The CAESAR contest has started in 2014 and received worldwide attention. In the first round, 57 algorithms were submitted to CAESAR and Scream was one of the 29 CAESAR round two candidates, while ASCON has been the winner in the lightweight cryptograhy category. We evaluate the security of Scream using different cryptanalytic techniques. Firstly we apply linear cryptanalysis to the cipher and then we extend this linear analysis with a differential part (known as differential-linear analysis). Further, we analyse the cipher with impossible differential cryptanalysis and then investigate the differential-linear path in the related-key scenario. For ASCON, we apply SAT-based cryptanalysis with an aim at the state recovery, using a SAT solver as the main tool. A SAT solver decides whether a given boolean formula has a satisfying valuation or not. It takes a boolean satisfiability problem and finds the solution to such the problem. We conclude the ASCON has a sufficient security margin against SAT-based cryptanalysis.

Furthermore, we focus on differential cryptanalysis of the lightweight ARX (Addition/Rotation/XOR) block cipher SPECK and LEA. SPECK was designed by the U.S National Security Agency (NSA). ARX algorithms use three operations: modular addition, bitwise rotation, and eXclusive-OR. These algorithms are usually smaller and faster for software implementation than S-box based designs. However, in AES-

like ciphers, an S-box is typically 8- or 4-bit. Such a size allows to compute the full distribution difference table (DDT) and investigate differential properties of the S-box and the algorithm. On the other hand, ARX-based designs use modular addition rather than S-boxes as a source of non-linearity. A word size in such ciphers are typically 32- or 64-bit and constructing a complete DDT is infeasible (It requires $2^{3n} \times 4$ bytes of memory for n-bit words). This is the reason we need some clever heuristics to circumvent this limitation. For this purpose, we propose an algorithm inspired by Nested Monte-Carlo Search to find the differential paths in SPECK and LEA. This method provides state-of-the-art (or close to) results but within a simpler framework.