UNIWERSYTET WARSZAWSKI

Wydział Matematyki, Informatyki i Mechaniki

Warszawa, 6 marca 2014

dr hab. Stefan Dziembowski
Instytut Informatyki
Uniwersytet Warszawski

RECENZJA ROZPRAWY DOKTORSKIEJ MGRA PIOTRA SUCHA PT. „SZYFROWANIE Z UŻYCIEM AUTOMATÓW DWUWYMIAROWYCH

Omówienie zawartości pracy wraz z jej oceną

Praca zawiera konstrukcję szyfru blokowego w oparciu o teorię dwuwymiarowych automatów komórkowych. Praca składa się z 6 rozdziałów. W pierwszym z nich autor dokonuje wprowadzenia do teorii automatów komórkowych. W drugim przedstawia historię stosowania tych automatów w kryptografii. Rozdział trzeci zawiera opis zaproponowanego szyfru blokowego. Jest on złożeniem trzech niezależnych automatów. Dodatkowo, automaty przekształcane są geometrycznie poprzez podzielenie ich zawartości na kwadraty i obracanie każdego z nich niezależnie. Bezpieczeństwo tego szyfru jest analizowane w rozdziale czwartym, gdzie przedstawiony jest szereg testów statystycznych dokonanych na nim, oraz rozdziale piątym, w którym autor pokazuje nieliniowe właściwości zaproponowanego szyfru oraz jego odporność na kryptoanalizę różnicową. Konstrukcja jest wydajna w praktyce, co autor wykazuje w Rozdziale 6. Konstrukcja zaproponowana przez autora jest ciekawa, oryginalna i stanowi cenny wkład w teorię szyfrów opartych o automaty komórkowe.

Uwagi krytyczne

Moim zdaniem największą wadą złożonej rozprawy jest wybór jej tematyki, która znajduje się obecnie na peryferiach głównego nurtu kryptografii. Pomysł tworzenia szyfrów w oparciu o teorię automatów komórkowych nie jest nowy: pojawiał się już wielokrotnie przynajmniej od lat osiemdziesiątych ubiegłego wieku. Wynika on z naturalnej obserwacji, że automaty komórkowe wykazują pewne pseudolosowe własności, które wydają się pożądane w kryptologii. Niestety szyfry konstruowane w oparciu o tę teorię, choć pozornie bezpieczne, okazywały się z reguły łatwe do złamania. Jest to zresztą sytuacja dość częsta w kryptografii (podobny przypadek stanowiły szyfry oparte o teorię chaosu deterministycznego). Z tego powodu kryptografia oparta o tę teorię od dłuższego czasu nie cieszy się dobrą opinią w społeczności kryptograficznej i badania nad jej zastosowaniami w szyfrowaniu nie znajdują się obecnie w centrum zainteresowań kryptografów.

dr hab. Stefan Dziembowski
Instytut Informatyki, Uniwersytet Warszawski
ul. Banacha 2, 02-097 Warszawa
e-mail: S.Dziembowski@crypto.edu.pl
telefon: +48 22 55 44 154

Jest to oczywiście do pewnego stopnia kwestia subiektywnych uprzedzeń większości badaczy, ale w gruncie rzeczy ma to bardzo dobre uzasadnienie praktyczne, gdyż bezpieczeństwo szyfru jest bardziej wiarygodne jeśli jest on w jakimś stopniu podobny do szyfrów które przez wiele lat nie zostały złamane. Przykładem mogą tu być kryptosystemy oparte o teorię liczb, której historia użycia w kryptografii jest o wiele lepsza niż teoria automatów komórkowych.

Oczywiście nie neguje to sensu dalszych badań możliwości użycia automatów komórkowych do tworzenia szyfrów, ale nakazuje ostrożność. W szczególności aby praca naukowa zyskała zainteresowanie jej autor powinien w przekonujący sposób wykazać jaki jest jego nowatorski pomysł, który podważa dotychczasowe przekonanie, że konstrukcje oparte o teorię automatów są niebezpieczne. Mój główny zarzut w stosunku do pracy doktorskiej pana Sucha polega właśnie na tym, że autor nie przekonał mnie w żaden sposób, że jego praca zawiera jakiś dramatycznie nowy pomysł. Według tego co autor pisze we wstępie, głównym nowym pomysłem zawartym w pracy jest użycie trzech automatów zamiast jednego. Niestety autor nie uzasadnia dlaczego ta zmiana miałaby w sposób fundamentalny poprawić bezpieczeństwo konstruowanych szyfrów. Takim uzasadnieniem byłaby np. analiza dotychczasowych ataków na szyfry oparte o automaty komórkowe i wskazanie dlaczego zwiększenie liczby automatów do trzech sprawia że ataki te (oraz ich warianty) nie działają. Podobne zarzuty można postawić wobec innych cech wymienionych przez autora jako nowatorskie w jego podejściu (zastosowanie dwuwymiarowych automatów zamiast jednowymiarowych oraz idea przekształceń geometrycznych niezależnych kwadratów).

Aby lepiej wyjaśnić mój zarzut, pozwolę sobie na uwagę natury ogólnej. Otóż właściwym pytaniem odnośnie konstrukcji nowych szyfrów nie jest: „czy dany szyfr jest bezpieczny?", tylko: „jakie mamy powody żeby wierzyć, że dany szyfr jest bezpieczny?". Ponieważ żaden z obecnie używanych szyfrów nie posiada pełnego dowodu bezpieczeństwa, to argumenty za ich bezpieczeństwem są z natury nieformalne. Jednym z argumentów tego typu mogą być testy statystyczne (które autor przeprowadza w Rozdziale 4), jednak nie jest to w żaden sposób argument decydujący, gdyż bezpieczeństwa systemów informatycznych z natury rzeczy nie można udowodnić w sposób eksperymentalny. Względną pewność, że dany szyfr nadaje się do użycia uzyskujemy tylko jeśli został on dogłębnie zbadany przez społeczność naukową.

Konsekwencje praktyczne tego faktu są takie, że zainteresowanie społeczności naukowej jest warunkiem uznania konstrukcji za ważną (to swoiste odwrócenie sytuacji z innych dziedzin nauki jest szczególną cechą kryptografii). Oczywiście nie jest to system do końca sprawiedliwy, gdyż znani badacze mają większe szanse na zainteresowanie pozostałych swoimi szyframi. Na szczęście również naukowcy z niewielkim dorobkiem mają szanse na uzyskanie zainteresowania swoją pracą poprzez zgłaszanie ich do konkursów na nowe szyfry (konkursy te są organizowane przez krajowe lub międzynarodowe organizacje techniczne i polegają na wieloletniej publicznej analizie nadesłanych prac) lub na konferencje naukowe. Sam fakt publikacji szyfru na dobrej konferencji nie oznacza oczywiście, że jest on bezpieczny, gdyż potencjalny przeciwnik z reguły dysponuje o

dr hab. Stefan Dziembowski
Instytut Informatyki, Uniwersytet Warszawski
ul. Banacha 2, 02-097 Warszawa
e-mail: S.Dziembowski@crypto.edu.pl
telefon: +48 22 55 44 154

wiele większymi zasobami czasu niż kilku recenzentów konferencyjnych. Tym niemniej jeśli taki szyfr nie został przez parę lat załamany, to najprawdopodobniej posiada on pewien potencjał.

W tym kontekście z przykrością odnotowuję fakt, że konstrukcje proponowane w doktoracie pana Sucha zostały opublikowane jedynie na konferencji *Advanced Computer Systems*, której rozpoznawalność w świecie kryptograficznym jest znikoma. Praca ta, mimo że od jej publikacji minęła ponad dekada, została zacytowana tylko raz (wg. Google Scholar, bez auto-cytowań) i to na dodatek w kontekście „tego typu konstrukcje były proponowane w (i tu długa lista prac)". Ponadto, fakt, że złożona praca została napisana została w języku polskim i to w sposób dość mało staranny (o czym piszę poniżej), dodatkowo zmniejsza szanse, że ktokolwiek na poważnie spróbuje przystąpić do łamania zaproponowanego w niej szyfru. W mojej ocenie zatem przesłanki że szyfr zaproponowany przez pana Sucha jest bezpieczny są bardzo słabe. Ponadto, przy obecnym stanie rzeczy, nawet jeśli szyfr ten nie zostanie złamany przez następne dziesięciolecia, to i tak nie będzie to stanowiło żadnego argumentu za bezpieczeństwem tego szyfru, gdyż minimalna będzie liczba osób które przez ten czas próbowały go złamać.

Innym moim zarzutem jest to, że praca jest też napisana w sposób mało staranny. Nieczytelne są pseudo-kody procedur, a nawet rysunki (np. Rys. 4, obrazujący główną konstrukcję, jest rozdzielony na dwie strony), co szczególnie razi biorąc pod uwagę, że praca ma aspekt „geometryczny" i dobre rysunki są niezbędne do jej zrozumienia.

Konkluzja

Pomimo przedstawionych wyżej zastrzeżeń, sama konstrukcja wydaje się interesująca. Dlatego uważam, że złożona rozprawa mgra Piotra Sucha spełnia wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora w dziedzinie nauk technicznych w zakresie informatyki.

(-) Stefan Dziembowski

dr hab. Stefan Dziembowski
Instytut Informatyki, Uniwersytet Warszawski
ul. Banacha 2, 02-097 Warszawa
e-mail: S.Dziembowski@crypto.edu.pl
telefon: +48 22 55 44 154