Szyfrowanie z użyciem automatów komórkowych dwuwymiarowych

Streszczenie

Celem tej pracy jest przedstawienie nowego symetrycznego szyfru blokowego o nazwie 2DCARotate, opartego na dwuwymiarowych automatach komórkowych oraz pewnych nieafinicznych przekształceniach geometrycznych. Szyfr ten charakteryzuje się prostą budową, która może być implementowana za pomocą prostych układów logicznych. Zastosowane automaty komórkowe i specyficzne, starannie dobrane nieafiniczne przekształcenia geometryczne dają łatwą możliwość zrównoleglenia przetwarzania (szyfrowania i deszyfrowania), dzięki temu szyfr ten przy odpowiedniej implementacji można uważać za bardzo wydajny.

Nowością tej pracy jest przede wszystkim zastosowanie do szyfrowania danych trzech dwuwymiarowych automatów. Nie jest to jeden automat, ale trzy współpracujące ze sobą w celu przetwarzania danych. Zastosowane operacje przekształceń danych (reguły automatu) są przekształceniami odwracalnymi i nieodwracalnymi, co także jest nowym rozwiązaniem zastosowanym w automatach dwuwymiarowych. Drugim elementem nowatorskim zawartym w konstrukcji szyfru 2DCARotate jest zastosowanie pewnych geometrycznych przekształceń opartych na kwadratach. Przekształcenia te, oprócz tego, że charakteryzują się wysokim poziomem nieliniowości, zostały dobrane w taki sposób, aby można było je wykonywać w trybie równoległym. Łącząc dwuwymiarowe automaty komórkowe z omawianymi przekształceniami geometrycznymi, uzyskujemy szyfr hybrydowy, charakteryzujący się dobrą jakością szyfrogramów, jak i wysoką wydajnością i prostotą implementacji.

Ważną częścią tej pracy jest także implementacja tego szyfru (oprócz implementacji na komputery PC) na układzie cyfrowym typu FPGA[1] za pomocą języka opisu sprzętu VHDL[2] i narzędzia Quartus II 9.0 Web Edition[3]. Celem tej implementacji było wykazanie wysokiej wydajności szyfru 2DCARotate w przypadku implementacji sprzętowej, tak aby można było się odnieść do implementacji sprzętowych znanych szyfrów, np. DES, 3DES, AES-Rijndael. Dzięki możliwości równoległego przetwarzania danych oferowanej przez automaty komórkowe i omawiane przekształcenia graficzne uzyskano bardzo obiecujące wyniki.

W tym miejscu należy także wymienić pozostałe założenia, jakie przyświecały budowie szyfru. Jednym z ważnych założeń było zbudowanie szyfru hybrydowego oraz zastosowanie automatów komórkowych jako architektury równoległej. Jak zwykle w podobnych sytuacjach w pracy tej przedstawiona jest właściwie rodzina szyfrów. Dobierając parametry (np. długość klucza) ustala się konkretny szyfr.

Projekt szyfru jest głównym celem tej pracy, jednak nie jedynym. Każdy nowy szyfr należy zbadać od strony możliwości ataków na niego różnymi znanymi obecnie metodami.

---

[1] FPGA (ang. Field Programmable Gate Array) - dosł. "bezpośrednio programowalna macierz bramek", to rodzaj programowalnego układu logicznego, który może być wielokrotnie przeprogramowany przez użytkownika w zakupionym urządzeniu docelowym (pralka, lodówka, MP3).

[2] (ang. Very High Speed Integrated Circuits Hardware Description Language) jest językiem specyfikacji i opisu sprzętu używanym do komputerowego projektowania układów cyfrowych.

[3] Altera Quartus II Web Edition Software, http://www.altera.com/products/software/quartus-ii/web-edition/qts-we-index.html, dostęp 02.02.2013.

Szyfry dobrej jakości powinny opierać się takim atakom. W związku z tym w pracy przedstawiono badania statystycznymi metodami weryfikacji jakości systemów szyfrowania, jednocześnie więc i poprawności algorytmów szyfrowania, ich wiarygodności, nazywanej też „bezpieczeństwem". Szyfrogramy otrzymywane na wyjściu dobrego algorytmu szyfrowania powinny mieć cechy ciągów losowych. Odstępstwa od losowego charakteru rozkładu bitów mogłyby bowiem zostać wykorzystane jako dogodny punkt umożliwiający różnego rodzaju ataki w celu złamania szyfru. Przez złamanie szyfru rozumie się znalezienie możliwej do stosowania w praktyce (ang. *feasible*) metody odszyfrowywania przez osoby nieuprawnione, nie mające odpowiedniego klucza.

W tej pracy zawarte są wyniki eksperymentalne testów statystycznych naszego szyfru i porównanie ich z tymi samymi testami na czterech renomowanych szyfrach DES, 3DES, AES-Rijndael i Blowfish. Dobre wyniki naszego 2DCARotate są, oczywiście, dla nas miłą niespodzianką.

Szyfr, oprócz dobrych właściwości statystycznych, powinien być także odporny na metody ataku znanymi technikami kryptoanalizy liniowej i różnicowej. W pracy zawarto wyniki dotyczące nieliniowości algorytmu 2DCARotate, które dają uzasadnioną nadzieję na odporność szyfru na kryptoanalizę liniową. Skontrowany jest także ewentualny atak metodą kryptoanalizy różnicowej.

Automaty komórkowe (ang. *cellular automata, CA)* wprowadził John von Neumann w 1966 roku - zdefiniował pojęcie automatu komórkowego jako model obliczeń alternatywny wobec maszyn Turinga, umożliwiający modelowanie obliczeń współbieżnych, oraz przedstawił intrygujący automat powielający swoją własną strukturę. W połowie lat 80. Stephen Wolfram zastosował automaty komórkowe w kryptologii. Na podstawie jego doświadczeń Howard Gutowitz dziesięć lat później zbudował kryptosystem oparty na automatach komórkowych.

Później pojawiły się następne próby zastosowania automatów jedno- czy dwuwymiarowych w kryptografii (Guan, 1987) (Nandi, Kari i Chaudhuri, 1994), (Sen, Chowdhuri i Ganguly, grudzień 2002). Opinie na temat automatów komórkowych do tej pory nie były jednoznaczne (Kari, J., 1990), (Toffoli i Margouls, Invertible cellular automata: A review, 1990), (Blackburn, Murphy i Paterson, 1995). Przykładem takiego stanu są udane próby łamania niektórych szyfrów opartych na automatach komórkowych (Blackburn, Murphy i Paterson, 1995), (Bao, grudzień 2004).

Motywacją tej pracy było także zwrócenie uwagi na automaty dwuwymiarowe i pokazanie, że mogą one być skutecznie wykorzystywane w kryptografii, szczególnie w hybrydowym połączeniu z nieafinicznymi przekształceniami boolowskimi.

Praca Gutowitza z 1996 była inspiracją do zaprojektowania szyfru 2DCARotate, opartego o automaty dwuwymiarowe. Z niej została zaczerpnięta idea reguł lewo- i prawostronnie przełączających, stosowanych dotąd w automatach jednowymiarowych. Idea ta została zmodyfikowana i zastosowana w automacie CACrypt. Zastosowanie odpowiedniego otoczenia (sąsiedztwa) jest podstawą do wprowadzenia dwuwymiarowych reguł lewo- czy prawostronnie przełączających, które daąe efekt lawinowy i przede wszystkim są oparte o otoczenie dwuwymiarowe. Szyfr 2DCARotate jest zbudowany z trzech dwuwymiarowych automatów komórkowych CACrypt, CATop, CALink. Automaty te współpracują ze sobą. Proces szyfrowania został podzielony na trzy fazy: szyfrującą, przełączającą i rozpraszającą. Dwie pierwsze fazy oparte są o interakcje pomiędzy tymi trzema automatami, dzięki którym można uzyskać silny efekt lawinowy nawet na bardzo podobnych danych wejściowych. Trzecia faza daje algorytmowi wysoki poziom nieafiniczności, dzięki czemu ataki metodą kryptoanalizy liniowej są trudne, o ile w ogóle są możliwe. Trzecia faza oparta o stosunkowo proste

przekształcenia geometryczne na kwadratach daje efekt podobny do podstawień przy pomocy tzw. skrzynek podstawieniowych [ang. *substitution box, S-box*]. Podsumowując, nowe rozwiązania zawarte w konstrukcji szyfru 2DCARotate można wymienić w punktach:

- szyfr oparty o dwuwymiarowe automaty,
- zastosowanie trzech współpracujących ze sobą automatów,
- specyficzny kształt otoczenia dający efekt lawinowy w 2D automatach,
- proste przekształcenia graficzne (obroty), dzięki którym jednak można uzyskać wysoki poziom nieafiniczności szyfru,
- specjalna budowa szyfru nastawiona na równoległe przetwarzanie danych.

Natomiast do najważniejszych technicznych zalet szyfru 2DCARotate można zaliczyć:

- wysoką jakość kryptograficzną szyfrogramów,
- prostotę budowy i łatwość implementacji za pomocą prostych układów logicznych,
- równoległość przetwarzania, skutkującą dość wysoką wydajnością szyfru.

Prezentowany szyfr został poddany testom statystycznym z użyciem narzędzia udostępnianego przez NIST[4]. Wyniki przeprowadzonych testów są bardzo obiecujące. Przeprowadzono wszystkie 16 testów. Wyniki statystyczne prezentowanego szyfru 2DCARotate nie odbiegają jakością od szyfrów DES, 3DES, AES-Rijndael, a nawet w części przypadków są od nich lepsze. Dobry szyfr oprócz dobrych właściwości statystycznych powinien być także odporny na znane metody ataku techniką kryptoanalizy liniowej i różnicowej technik. W pracy pokazano, że poziom nieliniowości przekształceń graficznych opartych na kwadratach wynosi 24. Jest to bardzo wysoka nieliniowość. Obecnie znane są na świecie opracowania, gdzie dla funkcji boolowskiej 6 argumentowej zrównoważonej (ang. balanced) uzyskano maksymalną nieliniowość rzędu 26. Wysoka nieliniowość daje lepszą gwarancję odporności szyfru na kryptoanalizę liniową. Podobnie bardzo dobre wyniki dała analiza profilu XOR, praktycznie wykluczając atak różnicowy.

W celu sprawdzenia rzeczywistej wydajności szyfru 2DCARotate, w oparciu o narzędzia Quartus II 9.0 Web Edition i język VHDL zbudowano implementację szyfru, która może zostać wgrana do układów cyfrowych typu FPGA. Ten sam algorytm zakodowany na komputerze PC uzyskiwał wydajność 1 Mb/60s, zaś po zakodowaniu go na o wiele słabszym urządzeniu cyfrowym uzyskano wydajność 16 Mb/s. Po dokonaniu pewnych optymalizacji i zastosowaniu wydajniejszego układu scalonego FPGA, np. taktowanego z szybkością 1.5 GHz http://www.pldesignline.com/showArticle.jhtml?articleID=210601830&cid=NL_pldl, możliwe wydaje się zwiększenie szybkości działania algorytmu o rząd, a być może o dwa rzędy wielkości, osiągając przepustowość na poziomie ok. 1 Gb/s.

Analizując wyniki i opierając się na uzyskanym doświadczeniu autora, w konkluzji rozprawy przedstawione zostały ewentualne kierunki dalszych prac, mające na celu zwiększenie zarówno wydajności, jak i uzyskanie optymalnie największej „komplikacji" szyfru przy dużej odporności na znane metody ataków kryptoanalitycznych.

Szyfr prezentowany w tej pracy jest to pierwszą próbą zastosowania szyfru hybrydowego opartego na wielu automatach komórkowych dwuwymiarowych i pewnych przekształceniach geometrycznych. Zastosowano w nim reguły nieodwracalne i odwracalne, co dodatkowo zwiększa siłę kryptograficzną algorytmu. Stosunkowo proste przekształcenia geometryczne

[4] NIST Random Number Generation, http://csrc.nist.gov/groups/ST/toolkit/rng/index.html, dostęp 02-03-2012

na kwadratach dają nieafiniczny efekt, podobny do podstawień przy pomocy tzw. skrzynek podstawieniowych (ang. *substitution box, S-box).*

Struktura pracy jest następująca.

W rozdziale 1 przypomniane są najważniejsze fakty dotyczące budowy i działania automatów komórkowych. W rozdziale 2 przedstawiony jest aktualny stan wiedzy na temat automatów komórkowych i stosowania ich w dziedzinie kryptografii. W rozdziale 3 wyjaśnione są szczegółowo zasady konstrukcji i działania nowego szyfru 2DCARotate – budowa szyfru, sposoby działania reguł, budowa klucza, jak i poszczególne fazy działania algorytmu.

Rozdział 4 przedstawia wyniki badań statystycznych jakości nowego szyfru wraz z krótkim opisem sposobu przeprowadzenia testów statystycznych, jakie zostały wykonane na szyfrogramach uzyskiwanych z szyfrów: 2DCARotate, DES, 3DES, AES-Rijndael i Blowfish.

Rozdział 5 opisuje metodę, jaka została wybrana w celu analizy poziomu nieliniowości przekształceń geometrycznych użytych do konstrukcji szyfru 2DCARotate, oraz wynikające z tego wnioski, dotyczące odporności szyfru na ataki metodą kryptoanalizy liniowej. Przedstawione są tu też trudności, na jakie natrafia kryptoanaliza różnicowa przy ewentualnej próbie ataku na 2DCARotate.

Rozdział 6 przedstawia implementację sprzętową szyfru 2DCARotate za pomocą języka opisu sprzętu VHDL. W tym rozdziale przedstawione są także wyniki, dotyczące wydajności szyfru 2DCARotate w ewentualnej implementacji sprzętowej.

Pracę zamyka rozdział 7 będący krótkim podsumowaniem całej pracy, opisujący uzyskane wyniki statystyczne, wyniki badania nieliniowości i profilu XOR oraz wyniki badań wydajności szyfru. Zasygnalizowane są też tam najważniejsze i najciekawsze problemy i kierunki dalszych badań.