Polskie krypto-odkrycie

Tomasz Marcinek

Z Bartoszem Żółtakiem, twórcą szyfru strumieniowego opartego na samodzielnie odkrytej funkcji jednokierunkowej VMPC, rozmawia Tomasz Marcinek.

Właśnie się dowiedzieliśmy, że stworzył Pan coś, co przez czołowych światowych specjalistów w dziedzinie teorii szyfrowania jest uważane za jedno z ważnych odkryć kryptografii teoretycznej i użytkowej. W kraju nie było o Panu słychać. Skąd to nagłe objawienie?

Nie ma w tym nic nagłego. Moja praca nad nowym algorytmem kryptograficznym trwa już mniej więcej pięć lat. Wolałem nie nadawać sprawie przedwczesnego rozgłosu. Przez pierwsze dwa lata szlifowałem podstawy teoretyczne odkrytej przeze mnie funkcji, zaś kolejne dwa lata zajęło mi teoretyczne i praktyczne badanie mocy kryptograficznej bazującego na niej algorytmu szyfrowania. Poza tym stale szukałem podobnych rozwiązań. Chciałem się upewnić, czy to, co przyszło mi do głowy, nie zostało już kiedyś przez kogoś wymyślone albo, co gorsza, porzucone jako nienadające się do zastosowań kryptograficznych. Swoje prace opublikowałem dopiero w połowie ub.r.

Dlaczego wszystkie materiały publikuje Pan w języku angielskim? Czy Pana odkrycie nie znalazło zainteresowania w Polsce? Może, będąc osobą "spoza branży", nie wzbudza Pan zaufania? W końcu zamiast matematyki czy fizyki skończył Pan marketing i zarządzanie na Politechnice Wrocławskiej...

Tu nie chodzi o "politykę", tylko o wiedzę. Podstawowy problem z kryptografią polega na tym, że na najwyższym poziomie zajmuje się nią bardzo wąskie grono osób. Naprawdę dobrych teoretyków kryptografii mamy na świecie niewielu. Z drugiej strony, osoby zawodowo zajmujące się szyfrowaniem poruszają się zwykle w ramach już istniejących algorytmów kryptograficznych i opartych na nich rozwiązań. Inaczej rzecz ujmując, w kraju nie bardzo jest z kim dyskutować o tym, na ile wymyślona przeze mnie metoda jest przełomowa.

Tymczasem, tak jak w przypadku wielu wynalazków, jeden problem w tym, aby coś wymyślić, ale drugi - aby udowodnić, że ma się rację i przekonać innych. Aby zaś udowodnić, po drugiej stronie trzeba mieć osobę znającą się na rzeczy. To dlatego kontaktowałem się do pewnego czasu głównie z osobami udzielającymi się na światowych listach dyskusyjnych poświęconych kryptografii. Pomysł wzbudził duże zainteresowanie, choć nawet i na liście nie brak było osób posądzających mnie o szarlatanerię. Wśród osób wyrażających się z uznaniem dla mojego odkrycia są takie sławy kryptografii, jak Greg Rose czy Scott Fluhrer. Łatwo to sprawdzić - lista sci.crypt jest ogólnie dostępna. Zainteresowanie okazało się tak duże, że zostałem zaproszony do wygłoszenia referatu o VMPC na międzynarodowej konferencji kryptograficznej IACR - Fast Software Encryption 2004 w Delhi. To jedno z najbardziej prestiżowych wydarzeń naukowych w branży. Właśnie z niej wróciłem.

Nie jest jednak tak, że w Polsce zupełnie mnie zignorowano. Konsultowałem swoje odkrycie z kilkoma osobami, m.in. z profesorem Kutyłowskim z Politechniki Wrocławskiej oraz dr. Wittlinem z Polskiej Akademii Nauk. Zwłaszcza w tym ostatnim przypadku zyskałem wsparcie, a nawet otrzymałem zaproszenie do zaprezentowania VMPC na seminarium kryptologicznym w PAN, które odbędzie się w połowie marca br. w Warszawie. Poza tym mój wyjazd do Delhi sponsorował m.in. prezydent Wrocławia.

Jakie reakcje wzbudziło Pana wystąpienie na konferencji w Delhi? Jak temat Pana referatu wypadł na tle innych wystąpień?

Konferencja trwała trzy dni. Większość wystąpień była poświęcona szyfrom strumieniowym, nie blokowym. Może to być zwiastunem, że szyfry strumieniowe są przyszłością kryptografii, choć

sądzę, że szyfry blokowe, ze względu na swoją powszechność, będą stosowane jeszcze przez wiele lat. Moje wystąpienie również dotyczyło szyfrów strumieniowych, a dokładnie opracowanego przeze mnie strumieniowego algorytmu szyfrującego wykorzystującego niezwykłe właściwości funkcji jednokierunkowej nazwanej przeze mnie VMPC - Variably Modified Permutation Composition - Zmiennie Modyfikowane Złożenie Permutacji.

Tuż po zakończeniu mojego wystąpienia podszedł do mnie nie kto inny, jak sam Adi Shamir (jeden z twórców algorytmu RSA - przyp. red.). Przedstawił mi kilka swoich uwag i sugestii, nie podważał jednak własności funkcji czy bezpieczeństwa szyfru VMPC. Podszedł do mnie także Jovan Golic, znany z sukcesów w wyszukiwaniu słabości w algorytmach szyfrujących. Zapowiedział, że będzie próbować szukać sposobu na złamanie VMPC, ale o samej koncepcji wypowiadał się bardzo pozytywnie. Największym zaskoczeniem była dla mnie kończąca konferencję sesja luźnych wniosków i komentarzy, tzw. rump session. Na sześć wystąpień, które miały miejsce w jej trakcie, trzy odnosiły się do mojego referatu! To dobrze wróży na przyszłość.

Opracowana przez Pana metoda szyfrowania jest bardzo wydajna nawet bez wspomagania sprzętowego. Czy to zapowiedź nowej klasy produktów kryptograficznych? A jeśli tak, to czy próbował Pan opatentować swoje odkrycie lub w inny sposób je skomercjalizować?

Szyfr VMPC rzeczywiście jest bardzo wydajny, co ma związek z jego prostotą. Zamiast kilkunastu czy kilkuset etapów, algorytm VMPC składa się raptem z trzech podstawowych operacji. Według moich wyliczeń do zaszyfrowania jednego bajta danych potrzebne jest mniej więcej 12, 13 cykli procesora. Nie przymierzając, to dwukrotnie szybciej niż w przypadku uważanego za bardzo wydajny i uznanego za standard szyfru AES. AES jest z kolei znacznie wydajniejszy niż algorytm 3DES stosowany powszechnie w protokołach IPsec czy SSL. Największą zaletą VMPC jest to, że jego duża wydajność i prostota nie wpływają na obniżenie bezpieczeństwa. Według moich wyliczeń do złamania szyfru VMPC najlepszą znaną metodą wymagane jest średnio 2^{900} (2 do potęgi 900) operacji, natomiast do pokonania tylko jego jądra, a więc do odwrócenia funkcji VMPC - 2^{260} (2 do potęgi 260).

Nie ma i nie będzie w możliwej do przewidzenia przyszłości takiej mocy obliczeniowej, która pozwoliłaby choćby na zbliżenie się do niższej z tych liczb (2^{260}). Aktualnie za wystarczający poziom bezpieczeństwa w zastosowaniach kryptograficznych uważa się pierwiastek tej liczby - 2^{128} Co do komercjalizacji, owszem, jestem zainteresowany, ale patentowanie szyfrów w dzisiejszych czasach skazuje je na niebyt. Jeżeli szyfr ma być powszechnie używany, a tego bym właśnie chciał, jego specyfikacja musi być otwarta. Nie uważam, żebym z tego powodu miał ponieść poważną stratę. Sam fakt dopuszczenia mojej pracy naukowej do prezentacji na konferencji FSE, na której występowali najznamienitsi kryptolodzy cywilni świata, m.in. Adi Shamir, David

Wagner, Phil Rogaway, Jovan Golic, Willi Meier, jest dla mnie nobilitacją. To otwiera wiele drzwi, więc o przyszłość się nie martwię. Na razie nigdzie nie pracuję - kontynuuję pracę nad odkryciem, a utrzymują mnie rodzice.

Jakie są Pana plany na najbliższą przyszłość?

Rozpocząłem pracę nad kolejnym algorytmem, który ma służyć do obliczania sum kontrolnych, tzw. MAC (Message Authentication Code). Chodzi o sprawdzanie spójności danych po deszyfracji. Obecne rozwiązania w tej dziedzinie, szczególnie dla szyfrów strumieniowych, są mało wydajne. W ogóle to słabo rozwinięta dziedzina, choć jej praktyczne znaczenie jest ogromne. Moim pomysłem bardzo zainteresował się Adi Shamir - korespondujemy w tej sprawie. Z publikacją jeszcze poczekam, aż rozwieją się wszystkie wątpliwości.