mgr Karol Żebrowski

Analiza prostego odświeżania w zaszumionym modelu wycieku informacji

Autoreferat rozprawy doktorskiej

June 2024

1 Wprowadzenie

Rozprawa bazuje na publikacji *Simple Refreshing in the Noisy Leakage Model* autorstwa Stefana Dziembowskiego, Sebastiana Fausta i Karola Żebrowskiego [6].

Schematy maskujące są znaczącym środkiem zaradczym zapobiegajacym analizie mocy [3]. Idea schematów maskujących polega na wprowadzeniu losowości do obliczenia poprzez dzielenie wrażliwych wartości. Klasycznie używany jest addytywny schemat n z n wartości, zatem każda wrażliwa wartość jest kodowana jako suma n wartości, gdzie n jest parametrem bezpieczeństwa. Następnie, zakładając obwodowy model obliczenia, aby bezpiecznie wykonać dane obliczenie, włączając w to dodawanie i mnożenie, często używane są tak zwane *gadżety* – podobwody wykonujące odpowiadające operacje na zakodowanych wartościach.

Kluczowym elementem konstrukcyjnym umożliwiającym bezpieczne składanie wielu maskowanych operacji jest tzw. *schemat odświeżający*. Jego wejściem jest pewne kodowanie, a wyjściem nowe kodowanie tej samej wrażliwej wartości. W ten sposób wprowadza świeżą losowość w obliczeniach i zapobiega gromadzeniu się wycieków z kodowań.

Naukowcy zaproponowali różne schematy odświeżania, poczynając od Ishai, Sahai i Wagnera w [8], gdzie dokonano tego poprzez „sztuczne" pomnożenie przez 1 w złożoności $O(n^2)$. Inna obserwacją, która pozwala skonstruować schemat odświeżania jest to, że wystarczy wygenerować jednostajnie losowe kodowanie 0 i dodać je, przewód po przewodzie, do odświeżanego kodowania. Jeden z takich schematów, nazywany przez nas *prostym odświeżaniem*, zaproponowali Rivain i Prouff [11]. Prosty schemat odświeżania jest optymalny pod względem złożoności i używanej losowości,

ponieważ używa tylko $< 2n$ operacji i $n - 1$ losowych bramek, gdzie n jest parametrem bezpieczeństwa. Niestety, okazało się, że po złożeniu z pewnymi operacjami arytmetycznymi schemat ten okazał się niebezpieczny w klasycznym modelu wycieku *t-sondowania* [4]. W modelu tym przeciwnik może poznać wybrane wartości t przewodów obwodu.

2 Streszczenie Wyników

Rodzi się zatem naturalne pytanie: „Czy proste odświeżanie jest bezpieczne w słabszym model wycieku?" Praca bada bezpieczeństwo prostego schematu odświeżania w modelu *zaszumionego* wycieku, zaproponowanym przez Prouff i Rivain [10], i odpowiada na to pytanie twierdząco. Model zaszumionego wycieku zakłada, że przeciwnik poznaje tylko „zaszumiony rozkład" wartości na przewodach obwodu. Model ten jest uważany za wiernie odpowiadający rzeczywistym fizycznym wyciekom. Później model ten był dopracowany oraz zredukowany do modelu *p-losowego sondowania* przez Duc et al. [5], w którym to każdy drut wycieka swoją wartość niezależnie, z prawdopodobieństwem p. Stąd, analiza przedstawiona w rozprawie skupia się na modelu losowego sondowania.

Naszą analizę rozpoczynamy od nieformalnego przedstawienia dowodu bezpieczeństwa w uproszczonym przypadku wielorundowego obwodu odświeżającego, w którym zakodowany sekret jest tylko odświeżany wiele razy i nie są na nim wykonywane żadne rzeczywiste obliczenia. Aby przeanalizować bezpieczeństwo schematu odświeżania, zadajemy naturalne pytanie: „Czy możemy scharakteryzować wycieki, które pozwalają przeciwnikowi obliczyć sekret?" Okazuje się, że istnieje dość proste rozróżnienie pomiędzy konfiguracjami wyciekających przewodów, które naruszają bezpieczeństwo sekretu i te, które tego nie robią. Jest to możliwe dzięki wprowadzonemu pojęciu *diagramu wycieku* – specjalnego grafu reprezentującego zbiór wyciekających przewodów. Rozróżnienie pomiędzy wyciekami naruszającymi bezpieczeństwo i bezpiecznymi polega na obserwacji diagramu wycieku i sprawdzeniu, czy jego podgrafy, mianowicie te które nazywamy „skrajnie lewę stroną" i „skrajnie prawą stroną", są połączone. Reszta analizy bezpieczeństwa polega na ograniczeniu z góry prawdopodobieństwa, że strony diagramu wycieków są połączone.

Pozostała część pracy poświęcona jest uogólnieniu idei przedstawionych w części nieformalnej. Dotyczy wykonywania obliczeń maskowanych, gdy

obwód używa prosty schemat odświeżania. Proponujemy konstrukcję prywatnego obwodu złożoną z gadżetów z prostym odświeżaniem, który wykonuje dowolne obliczenia. Analiza konstrukcji wymaga:

1. Zdefiniowania gadżetu, który może być użyty w naszej konstrukcji. Własności uchwycone w definicji wraz z własnościami prostego odświeżania sprawiają, że gadżety można składać razem z prostym odświeżaniem. Definicja jest podobna w duchu do istniejących definicji w modelu t-sondowania, natomiast bierze również pod uwagę *kolejność wejściowych oraz wyjściowych drutów* gadżetu. W rozprawie przedstawiamy też dowód, że klasyczny gadżet mnożący ISW spełnia naszą definicję.

2. Generalizacji pojęcia diagramu wycieku, aby reprezentował wyciek w konstrukcji złożonej z gadżetów. Nasza definicja gadżetu pozwala „zrzutować" wyciekające druty z każdego gadżetu na odpowiadającą ścieżkę w diagramie wycieku, a zatem reprezentować wyciek w całym prywatnym obwodzie.

3. Udowodnienia twierdzenia o prywatności naszej konstrukcji w ogólnym przypadku. Rozprawa przedstawia wszystkie potrzebne techniczne pojęcia oraz dowody niewłączone do oryginalnej publikacji. Dowód bezpieczeństwa naszej konstrukcji jest oparty na, powszechnie używanym w kryptografii, argumencie hybrydowym. Definiujemy ciąg eksperymentów hybrydowych, w których powstaje widok przeciwnika. Następnie uzasadniamy, że każde dwa kolejne eksperymenty w ciągu tworzą taki sam widok przeciwnika, co implikuje że pierwszy i ostatni widok są identyczne. W konsekwencji pokazujemy, że widok przeciwnika może być zasymulowany *nie znając sekretu*, co gwarantuje prywatność naszej konstrukcji.

Nasza konstrukcja osiąga konkretne wyniki nawet dla małych parametrów bezpieczeństwa n, w przeciwieństwie do bardziej teoretycznych konstrukcji Ajtai [1] oraz Andrychowicza et al. [2]. Konstrukcja jest modułowa i działa dla różnych implementacji gadżetów dodających i mnożących. W naszej konstrukcji *nie robimy* żadnych silnych założeń, takich jak np. o niecieknących komponentach użytych w innych konstrukcjach [7, 9].

Literatura

[1] Miklós Ajtai. Secure computation with information leaking to an adversary. In Lance Fortnow and Salil P. Vadhan, editors, *43rd Annual ACM Symposium on Theory of Computing*, pages 715–724. ACM Press, June 2011.

[2] Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust. Circuit compilers with $O(1/\log(n))$ leakage rate. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology – EUROCRYPT 2016, Part II*, volume 9666 of *Lecture Notes in Computer Science*, pages 586–615. Springer, Heidelberg, May 2016.

[3] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards sound approaches to counteract power-analysis attacks. In Michael J. Wiener, editor, *Advances in Cryptology – CRYPTO'99*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, Heidelberg, August 1999.

[4] Jean-Sébastien Coron, Emmanuel Prouff, Matthieu Rivain, and Thomas Roche. Higher-order side channel security and mask refreshing. In Shiho Moriai, editor, *Fast Software Encryption – FSE 2013*, volume 8424 of *Lecture Notes in Computer Science*, pages 410–424. Springer, Heidelberg, March 2014.

[5] Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. Unifying leakage models: From probing attacks to noisy leakage. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2014*, volume 8441 of *Lecture Notes in Computer Science*, pages 423–440. Springer, Heidelberg, May 2014.

[6] Stefan Dziembowski, Sebastian Faust, and Karol Zebrowski. Simple refreshing in the noisy leakage model. Lecture Notes in Computer Science, pages 315–344. Springer, Heidelberg, December 2019.

[7] Sebastian Faust, Tal Rabin, Leonid Reyzin, Eran Tromer, and Vinod Vaikuntanathan. Protecting circuits from leakage: the computationally-bounded and noisy cases. In Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *Lecture Notes in Computer Science*, pages 135–156. Springer, Heidelberg, May / June 2010.

[8] Yuval Ishai, Amit Sahai, and David Wagner. Private circuits: Securing hardware against probing attacks. In Dan Boneh, editor, *Advances in Cryptology – CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, Heidelberg, August 2003.

[9] Eric Miles. Iterated group products and leakage resilience against NC1. In Moni Naor, editor, *ITCS 2014: 5th Conference on Innovations in Theoretical Computer Science*, pages 261–268. Association for Computing Machinery, January 2014.

[10] Emmanuel Prouff and Matthieu Rivain. Masking against side-channel attacks: A formal security proof. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, Heidelberg, May 2013.

[11] Matthieu Rivain and Emmanuel Prouff. Provably secure higher-order masking of AES. In Stefan Mangard and François-Xavier Standaert, editors, *Cryptographic Hardware and Embedded Systems – CHES 2010*, volume 6225 of *Lecture Notes in Computer Science*, pages 413–427. Springer, Heidelberg, August 2010.