Marcin Płonkowski

Katolicki Uniwersytet Lubelski Jana Pawła II

Wykorzystanie ataku geometrycznego do kryptoanalizy procesu synchronizacji architektur TPCM

Na początku 2002 w [1] został zaproponowany nowy protokół wymiany kluczy wykorzystujący wzajemne uczenie sieci neuronowych. Protokół ten oparty jest na dwóch architekturach zwanych TPM (tree parity machine). W ich implementacji wykorzystuję się liczby całkowite.

W 2005 roku w [6] została przedstawiona modyfikacja architektury TPM, która wykorzystuje w swej konstrukcji liczby zespolone. Została ona nazwana TPCM (tree parity complex machine). Proces synchronizacji oparty na architekturach TPCM, charakteryzuje się wyższym poziomem bezpieczeństwa w stosunku do procesu synchronizacji opartego na architekturach TPM.

Bezpieczeństwo procesu synchronizacji może być zagrożone poprzez zastosowanie ataku geometrycznego [5]. W przypadku architektur TPM, prawdopodobieństwo to jest dość wysokie i zagraża bezpieczeństwu systemu.

W odniesieniu do TPCM została zaimplementowana wersja ataku geometrycznego bazująca na liczbach zespolonych. Jak wykazały testy proces synchronizacji opary na architekturach TPCM, jest odporny na atak geometryczny. Związane jest to z bardziej skomplikowaną strukturą architektury TPCM, jak i działań, na których opiera się proces synchronizacji. Gwarantuje ona zatem wyższy poziom bezpieczeństwa niż klasyczny model oparty na TPM.

[1] I. Kanter, W. Kinzel, E. Kanter, *Secure exchange of information by synchronization of neural networks*, Europhys. Lett. 57, pp. 141-147 (2002).

[2] M. Volkmer, S. Wallner, *Tree Parity Machine Rekeying Architectures*, Cryptology ePrint Archive: REport 2004/216.

[3] M. Rosen-Zivi, I. Kanter, W. Kinzel, *Cryptography based on neural network - analytical results*, cond-mat/0202350.

[4] W. Kinzel, I. Kanter, *Neural Cryptography*, 9th Intern. Conf. On Neural Information Processing, Singapore, Nov. 2002.

[5] A. Klimov, A. Mityaguine, A. Shamir, *Analysis of Neural Cryptography*, ASIACRYPT 2002. Volume 2501 of LNCS., Springer Verlag (2002) 288–298

[6] M. Płonkowski, P. Urbanowicz, *Анализ архитектур нейронных сетей в контексте взаимного обучения и безопасности обмена ключами*, 69-я научно-техническая конференция профессорско-преподавательского состава, научных цотрудников и аспирантов БГТУ, г. Минск, февраль 2005.

[7] M. Płonkowski, P. Urbanowicz, *Использование нейронных сетей в системах криптографического преобразования информации*, Известия Белорусской инженерной академии, 1 (17)/4 2004.