Ferradi, Houda; **Géraud, Rémi**; **Guilley, Sylvain**; **Naccache, David**; **Tibouchi, Mehdi**
Recovering secrets from prefix-dependent leakage. (English) Zbl 1448.94243
J. Math. Cryptol. 14, 15-24 (2020).

Summary: We discuss how to recover a secret bitstring given partial information obtained during a computation over that string, assuming the computation is a deterministic algorithm processing the secret bits sequentially. That abstract situation models certain types of side-channel attacks against discrete logarithm and RSA-based cryptosystems, where the adversary obtains information not on the secret exponent directly, but instead on the group or ring element that varies at each step of the exponentiation algorithm.

Our main result shows that for a leakage of a single bit per iteration, under suitable statistical independence assumptions, one can recover the whole secret bitstring in polynomial time. We also discuss how to cope with imperfect leakage, extend the model to k-bit leaks, and show how our algorithm yields attacks on popular cryptosystems such as (EC)DSA.

MSC:

94A62 Authentication, digital signatures and secret sharing
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:

Galton-Watson process; discrete logarithm problem; cryptanalysis

Software:

BKZ

Full Text: DOI

References:

[1] Diego F. Aranha, Pierre-Alain Fouque, Benoît Gérard, Jean-Gabriel Kammerer, Mehdi Tibouchi and Jean-Christophe Zapalowicz, GLV/GLS Decomposition, Power Analysis, and Attacks on ECDSA Signatures with Single-Bit Nonce Bias, in: ASIACRYPT 2014, Part I (Palash Sarkar and Tetsu Iwata, eds.), LNCS 8873, pp. 262-281, Springer, Heidelberg, December 2014. · Zbl 1306.94023

[2] Aurélie Bauer and Damien Vergnaud, Practical Key Recovery for Discrete-Logarithm Based Authentication Schemes from Random Nonce Bits, in: CHES 2015 (Tim Güneysu and Helena Handschuh, eds.), LNCS 9293, pp. 287-306, Springer, Heidelberg, September 2015. · Zbl 1380.94137

[3] Daniel J. Bernstein and Tanja Lange, Faster Addition and Doubling on Elliptic Curves, in: ASIACRYPT 2007 (Kaoru Kurosawa, ed.), LNCS 4833, pp. 29-50, Springer, Heidelberg, December 2007. · Zbl 1153.11342

[4] Daniel J. Bernstein and Tanja Lange, Complete addition laws for elliptic curves, Talk at Algebra and Number Theory Seminar (Universidad Autonomo de Madrid), 2009, http://cr.yp.to/talks/2009.04.17/slides.pdf. · Zbl 1229.11087

[5] Daniel Bleichenbacher, On the generation of one-time keys in DL signature schemes, Presentation at IEEE P1363 Working Group meeting, 2000.

[6] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao and Pankaj Rohatgi, Towards Sound Approaches to Counteract Power-Analysis Attacks, in: CRYPTO'99 (Michael J. Wiener, ed.), LNCS 1666, pp. 398-412, Springer, Heidelberg, August 1999. · Zbl 0942.68045

[7] Yuanmi Chen and Phong Q. Nguyen, BKZ 2.0: Better Lattice Security Estimates, in: ASIACRYPT 2011 (Dong Hoon Lee and Xiaoyun Wang, eds.), LNCS 7073, pp. 1-20, Springer, Heidelberg, December 2011. · Zbl 1227.94037

[8] Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet and Vincent Verneuil, Square Always Exponentiation, in: INDOCRYPT 2011 (Daniel J. Bernstein and Sanjit Chatterjee, eds.), LNCS 7107, pp. 40-57, Springer, Heidelberg, December 2011. · Zbl 1291.94069

[9] Christophe Clavier and Marc Joye, Universal Exponentiation Algorithm, in: CHES 2001 (Çetin Kaya Koç, David Naccache and Christof Paar, eds.), LNCS 2162, pp. 300-308, Springer, Heidelberg, May 2001.

[10] Jean-Sébastien Coron, Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems, in: CHES'99 (Çetin Kaya Koç and Christof Paar, eds.), LNCS 1717, pp. 292-302, Springer, Heidelberg, August 1999. · Zbl 0955.94009

[11] Dean H. Fearn, Galton-Watson processes with generation dependence, in: Proceedings of the Sixth Berkeley Symposium on Mathematical Statistics and Probability (Univ. California, Berkeley, Calif., 1970/1971), 4, pp. 159-172, 1972.

[12] Houda Ferradi, Rémi Géraud, Sylvain Guilley, David Naccache and Mehdi Tibouchi, Recovering Secrets From Prefix-Dependent Leakage, Cryptology ePrint Archive, Report 2018/798, 2018, http://eprint.iacr.org/2018/798. Full version of this paper.

[13] Wilko Henecka, Alexander May and Alexander Meurer, Correcting Errors in RSA Private Keys, in: CRYPTO 2010 (Tal Rabin, ed.), LNCS 6223, pp. 351-369, Springer, Heidelberg, August 2010. · Zbl 1283.94067

[14] Nadia Heninger and Hovav Shacham, Reconstructing RSA Private Keys from Random Key Bits, in: CRYPTO 2009 (Shai Halevi, ed.), LNCS 5677, pp. 1-17, Springer, Heidelberg, August 2009. · Zbl 1252.94072

[15] Nick Howgrave-Graham and Nigel P. Smart, Lattice Attacks on Digital Signature Schemes, Des. Codes Cryptography23 (2001), 283-290. · Zbl 1006.94022

[16] Marc Joye and Christophe Tymen, Protections against Differential Analysis for Elliptic Curve Cryptography, in: CHES 2001 (Çetin Kaya Koç, David Naccache and Christof Paar, eds.), LNCS 2162, pp. 377-390, Springer, Heidelberg, May 2001. · Zbl 1012.94550

[17] Paul C. Kocher, Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems, in: CRYPTO'96 (Neal Koblitz, ed.), LNCS 1109, pp. 104-113, Springer, Heidelberg, August 1996. · Zbl 1329.94070

[18] Paul C. Kocher, Joshua Jaffe, Benjamin Jun and Pankaj Rohatgi, Introduction to differential power analysis, J. Cryptographic Engineering1 (2011), 5-27.

[19] Noboru Kunihiro, Naoyuki Shinohara and Tetsuya Izu, Recovering RSA Secret Keys from Noisy Key Bits with Erasures and Errors, in: PKC 2013 (Kaoru Kurosawa and Goichiro Hanaoka, eds.), LNCS 7778, pp. 180-197, Springer, Heidelberg, February / March 2013. · Zbl 1314.94081

[20] Peter L Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Mathematics of computation48 (1987), 243-264. · Zbl 0608.10005

[21] Elke De Mulder, Michael Hutter, Mark E. Marson and Peter Pearson, Using Bleichenbacher's solution to the hidden number problem to attack nonce leaks in 384-bit ECDSA: extended version, J. Cryptographic Engineering4 (2014), 33-45.

[22] Phong Q. Nguyen and Igor E. Shparlinski, The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces, Des. Codes Cryptography30 (2003), 201-217. · Zbl 1039.94008

[23] Kenneth G. Paterson, Antigoni Polychroniadou and Dale L. Sibborn, A Coding-Theoretic Approach to Recovering Noisy RSA Keys, in: ASIACRYPT 2012 (Xiaoyun Wang and Kazue Sako, eds.), LNCS 7658, pp. 386-403, Springer, Heidelberg, December 2012. · Zbl 1292.94126

[24] Bertram Poettering and Dale L. Sibborn, Cold Boot Attacks in the Discrete Logarithm Setting, in: CT-RSA 2015 (Kaisa Nyberg, ed.), LNCS 9048, pp. 449-465, Springer, Heidelberg, April 2015. · Zbl 1382.94155

[25] Joost Renes, Craig Costello and Lejla Batina, Complete Addition Formulas for Prime Order Elliptic Curves, in: EUROCRYPT 2016, Part I (Marc Fischlin and Jean-Sébastien Coron, eds.), LNCS 9665, pp. 403-428, Springer, Heidelberg, May 2016. · Zbl 1385.14001