Crypto applications of combinatorial group theory

Ivana Ilić and Spyros S. Magliveras*
CCIS, Department of Math. Sciences, Florida Atlantic University,
Boca Raton, FL 33431, USA
e-mail: iilic@fau.edu, spyros@fau.edu

Abstract. The design of a large number of cryptographic primitives is based on the intractability of the traditional discrete logarithm problem (tDLP). However, the well known quantum algorithm of P. Shor [4] solves the tDLP in linear time, thus rendering all cryptographic schemes based on tDLP ineffective, should quantum computers become a practical reality. In [2] M. Sramka et al. generalize the DLP to arbitrary finite groups. The DLP for a non-abelian group is based on a particular representation of a chosen family of groups, and a choice of a class of generators for these groups. The paper that will appear in the ASI volume goes into the generalized discrete problem for the family of groups $PSL(2, p)$, p a large prime with particular emphasis on weak generating pairs, and strategies for cryptanalysing few of the remaining cases. However, in this talk the emphasis will be on summarizing our successful attack of the $SL(2, 2^n)$-based Tillich Zémor cryptographic hash function [5]. The talk is founded on [1] which in turn is based on a very interesting result of Mesirov and Sweet [3] for finding maximal length chains in the Euclidean algorithm in $\mathbb{F}_2[x]$, starting with any irreducible polynomial. We will show how experimentation led us to conjecture and then construct short collisions between palindromic strings of length $2n + 2$, and how these relate to maximal Euclidean algorithm chains.

2000 Mathematics Subject Classification: 68P25, 94A60.
Keywords. Discrete logarithm, finite groups, intractability, representations and presentations of groups, $PSL(2, p)$, public key cryptosystems, Tillich-Zémor hash function.

References

[1] Markus Grassl, Ivana Ilić, Spyros Magliveras, Rainer Steinwandt. Cryptanalysis of the Tillich-Zémor hash function. To appear in the *Journal of Cryptology*, 2010. Cryptology ePrint Archive: Report 2009/376, 2009. Available at: http://eprint.iacr.org/2009/376

[2] Lee C. Klingler, Spyros S. Magliveras, Fred Richman, Michal Sramka. Discrete logarithms for finite groups. *Computing* **85**, (2009), pp. 3–19.

[3] Jill P. Mesirov and Melvin M. Sweet. Continued Fraction Expansions of Rational Expressions with Irreducible Denominators in Characteristic 2. *Journal of Number Theory* **27** pp. 144–148, 1987.

[4] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. on Computing*, **26**(5), pp. 1484-1509, 1997.

[5] Jean-Piere Tillich and Gilles Zémor. Hashing with SL_2. LNCS 839, Advances in Cryptology – CRYPTO '94, pp. 40–49, 1994.