1020-14-186 **Makoto Sugita*** (m-sugita@ipa.go.jp), 2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591, Japan. *Gröbner Basis based Cryptanalysis of SHA-1.* Preliminary report.

Recently, Wang proposed a new method to cryptanalyze SHA-1 and found collisions of the 58-round SHA-1. The complexity of Wang's method to cryptanalyze the 58-round SHA-1 is 2^{34} SHA-1 computation. Moreover, Wang et al. gave the complexity evaluation against the full SHA-1 which is claimed to be 2^{62}. The aim of this article is to sophisticate and improve Wang's attack by using Gröbner basis techniques and to reduce the complexity of the attack for SHA-1. In this article, we apply Gröbner basis techniques to a cryptanalysis of SHA-1. We introduce a new notion of "semi-neutral bit" and propose an improved message modification technique based on Gröbner basis technique. In the case of the 58-round SHA-1, the complexity of an attack based on our improved message modification is 2^8 message modification which is equivalent to 2^{31} SHA-1 experimentally in our latest implementation. We found many new collisions for the 58-round SHA-1. Moreover, in the case of the full SHA-1, the complexity of our algorithm when it is applied to the first iteration of a two-iteration attack for the full SHA-1 is 2^{51} message modification (symbolic computation), whereas Wang's method needs 2^{62}. (Received August 28, 2006)