Cryptography Final Project Proposal
Team insert team name
HIGHT Algorithm

Christopher Sasarak
Srivinas Sridharan

March 13, 2013

Team Information

Algorithm: HIGHT

Team Name: New HIGHT

Team Members: Christopher Sasarak, Srinivas Sridharan

Email Addresses: cms5347@rit.edu, sxs9716@rit.edu

Algorithm

The HIGHT algorithm[1] is a lightweight block cipher made for use in simple devices such as RFID tag. Its simple design lends itself to implementations not only in software, but also directly in hardware. Indeed, the authors note that their hardware implementation of HIGHT can be implemented with only 3048 logic gates [1]. Other researchers have also evaluated HIGHT for its viability in low-power environments and reached the same conclusion [2].

HIGHT divides the plain-text into blocks of 64-bits in length and then encrypts the data using a key of length 128-bits. Before performing the actual encryption, HIGHT employs a technique called *key whitening* where it uses whitening keys generated from the master key to do an initial transformation on the plain-text before encrypting it with a 32-round algorithm. At the end of the encryption, the text output from these 32 rounds are put through an output transformation using a different set of whitening keys [1].

Attack

We are planning to implement a linear attack against one round of HIGHT. To do this we will need to find out three pieces of information:the sub-keys that are used to encrypt the plain-text and the whitening keys used for both the input transformation and the output transformation. By testing many different known plain-text/cipher-text pairs and exhaustively checking combinations of whitening keys we can determine the sub-keys and break the encryption.

References

[1] Deukjo Hong, Jaechul Sung, Seokhie Hong, Jongin Lim, Sangjin Lee, Bonseok Koo, Changhoon Lee, Donghoon Chang, Jesang Lee, Kitae Jeong, Hyun Kim, Jongsung Kim, and Seongtaek Chee. Hight: A new block cipher suitable for low-resource device. In *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop*, volume 4249 of *Lecture Notes in Computer Science*, pages 46–59. Springer, 2006.

[2] Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, and Dong Hoon Lee. Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks. In *Information Security and Assurance, 2008. ISA 2008. International Conference on*, pages 73–76. IEEE, 2008.