Joux, Antoine. *Algorithmic Cryptanalysis*. Boca Raton: CRC, 2009. Print.

Junod, Pascal, and Anne Canteaut. *Advanced Linear Cryptanalysis of Block and Stream Ciphers*. Amsterdam: IOS, 2011. Print.

This article outlines some advanced methods of determining if an algorithm is cryptographically secure or not, including checking if frequencies of certain bits are above 50% using systems of linear equations, performing chain encryption operations to deduce keys, and tracing difference paths. All of these methods will be good things to look at when attempting to categorize our cryptography method in terms of its security and looking for ways to improve it. This article was published through a well-known and reputable publishing organization, and is probably reliable.

Swenson, Christopher. *Modern Cryptanalysis: Techniques for Advanced Code Breaking*. Indianapolis, IN: Wiley Pub., 2008. Print.

Wolfram, Stephen. "Computation Theory of Cellular Automata." *Communications in Mathematical Physics* 96 (1984): 15-57. Web. 12 Dec. 2013. <http://www.stephenwolfram.com/publications/academic/computation-theory-cellular-automata.pdf>.

Many aspects of general computational theory are evident in cellular automata, most notably the universal computability (Turing-completeness). The formal languages used to describe the state of a cellular automaton are non-entropic and non-decreasing in complexity with time. The limiting properties of a cellular automaton are determined by an infinite computational process, and for Class 3 and 4 automata, there are no mathematical shortcuts to create a finite mathematical description. As such, no simple theory or formula describes these, and their state can only be found by direct simulation or observation. As such, they may be an ideal control mechanism for a cryptographic algorithm, as they would be resistant to most formulaic or mathematical methods of code breaking, and capable of performing encoding operations of arbitrary length. The article was published in a reputable scientific journal, and comes from the author’s earlier years, before he became more eccentric.

Wolfram, Stephen. "Cryptography with Cellular Automata." *Lecture Notes in Computer Science* 218 (1986): 429-32. Web. 12 Dec. 2013. <http://www.stephenwolfram.com/publications/academic/cryptography-cellular-automata.pdf>.

This article outlines a potential method of cryptographic encoding using a cellular automaton as a stream of bits for input obfuscation of a message text. It does not go into specific detail about different aspects of the method’s strengths and weaknesses, and leaves several areas for improvement. This article was published in a reputable journal from a reputable university, and is probably trustworthy.

Wolfram, Stephen. *A New Kind of Science*. 1st ed. Champaign, IL: Wolfram Media, 2002. 598-606. Print.

Knudsen, Lars, and David Wagner. Integral Cryptanalysis. Publication. Belgium: IACR, 2002. Integral Cryptanalysis. IACR, 2002. Web. 22 Feb. 2014.

This article considers the viability of Integral Cryptanalysis in the breaking of ciphers that are normally not vulnerable to differential attacks. Three different methods for implementing Integral Cryptanalysis are examined and an improved method over the currently existing methods is introduced. The paper was presented at a well-respected conference on Cryptanalysis and both authors attend reputable universities. The paper is technical in nature and very little bias is evident.

Biham, Eli, Orr Dunkelman, and Nathan Keller. *New Results on Boomerang and Rectangle Attacks*. Publication. Belgium: IACR, 2002. *New Results on Boomerang and Rectangle Attacks*. IACR, 2002. Web. 22 Feb. 2014.

This paper discusses current tactics of cryptanalysis and the difficulties of applying them to new ciphers that are being developed. Two different approached are analyzed and benefits and detriments of each are presented. In addition to this, the paper provides some suggestions for improvement of both methods. The paper was presented at a respected conference and the authors attend a reputable university.