

To Whom It May Concern

I am an industrial chemical engineer with over 50 years of experience in practical processes and technical documentation with only one other relevant attribute being that I learned symbolic logic forty years ago. I am not a computer geek. I was asked by FortressGB to review draft documents which are and were submitted by FortressGB to the NIST Hash Contest. I was asked to judge, in particular, the clarity, the concepts of the machine, the problems of algebraic complexity and the rationales for the designs. FortressGB needed assurance that the 4 most important documents were complete enough so that an intelligent individual who has no previous knowledge of cryptography could understand their less conventional implementations.

I found the documents to be complete in the sense that I was able to understand the workings of the engine, the place of a hash, stream cipher and random number generator in what they claim to be a very low cost silicon area, which is gratis in smaller applications, and a miniscule silicon addition to chips designed for servers and extremely high speed communications. I understood the concept of total solutions where the engines can work both in tandem for (booting) and also in parallel, importing encrypted or clear text data and simultaneously hash digesting; all this, they claim, with little more silicon than popular random number generators.

I read the following documents in their entirety-

- 1) Bard et al, the new draft article on crypto-complexity on Repeated Words with a request from FortressGB for a conservative estimate of the number of monomials in the Register Bank. Bard declares that a manual check would take months and would be redundant as the Data Churn itself is intractable leading me to understand that Result/Feedback Processor and the Random Controller, and the basis of their estimate of the impossibility of a collision in the first 1,000,000 Message Words.
- 2) The "Understanding the ZK-Crypt" article which first explained their design tenets, demonstrated tandem and parallel configurations of engines, proving ability to encrypt/decrypt and authenticate data transparently and simultaneously at different levels of security.
- 3) In the Introduction and first chapter of the Cryptographic Analysis, I found how the tenets with rationales clearly explain a dynamic development process which they claim is well supported with extensive standard and innovative testing.
- 4) The A-Z of the ZK-Crypt, which is a glossary of the terms. The only unexplained term mentioned in texts 1) to 3) was the Birthday Attack; nicely explained in the A-Z.

I highly recommend that an un-initiated reader start "top down", first with the animated "Gold Rush" cartoon. That may give the mindset of the concept of the engine. Then he/she should be ready to proceed directly to the "Understanding..." article, starting with the tenets of the design which intuitively explains the strength of the number generator, the advantageous configurations and the economics. The first chapter of the cryptanalysis led me to understand rationales and why the designers did what they did.

Sincerely,

Alan Lindblom Consultant (a relative of 2 ZK-Crypt Crew members)

Dedication Farm

Telephone: 1-336-508 0577 Fax: 1-336-508 6231