Structure Attacks on Cryptographic Protocols

Karl Mahlburg
Advisor: Prof. Rett Bull (Pomona),
Second reader: Prof. Francis Su

October 2000

There are two primary branches in the modern field of cryptography. One group is concerned with encryption itself – encoding sensitive data in a secure way. The goal here is to design cryptographic algorithms that can be implemented efficiently but are difficult to break. The other active area of study is concerned with the security properties of cryptographic *protocols*, which are the practical application of encryption. Protocols are a sequence of messages sent and calculations made by two or more parties on a potentially insecure network. A good protocol allows each party to conclude that sensitive data remains secure and to verify the identities of all participants.

Cryptographic protocols are in general difficult to analyze, and many of the protocols placed in commercial software were later discovered to be vulnerable to complicated attacks. In recent years much progress has been made in mathematically formalizing and proving the security properties of protocols. Using mechanical conversion procedures, protocols are encoded into logical statements (usually in a "belief logic" system), as are the desired results of running the protocol. It is then easy to verify the function of the protocol by checking if the desired conclusions can be deduced. An alternative formalization is the *strand space* model, in which protocols are represented by a graphlike structure. Similar deductions about the operation of the protocol can be made based on the relative positions of certain messages in the graph.

However, all of these methods make strong assumptions on the simplicity of messages and encryption, which are never met by a real cryptographic system. The most worrisome assumption is that the space of messages is a *free algebra*. This space is generated by concatenating and encrypting smaller messages, and to say that this is a free algebra means that all of the generated messages are distinct. This is clearly not true in a system limited by finite memory and algorithms using (finite) primes.

I propose to investigate the effects of added algebraic structure to the security results that have already been proven for the simpler case. These results must be extended in two ways:

1. **Guesses** In a finite space of messages random guesses cannot be ignored, as was done in previous work. Instead we use nonstandard analysis to show that the probability of successful attacks based on guesses is negligible.

2. **Structured Attacks** The additional structure may itself be exploitable, so that a provably correct protocol may no longer be secure with added structure. To counteract such attacks we collapse the additional structure into closed subgroups and restrict the set of safe protocols so that any attempted attacks are contained in these subgroups.

Using these extensions, previously known results still hold, so we can still easily analyze protocols.