Proposing a Master One-Way Function
*Polynomial Morphology * Intractability Metric*

Gideon Samid [gideon.samid@case.edu]

Abstract: making an arbitrary binary string fit as a fixed size cipher key (via hashing) one could use an arbitrary string x as both plaintext and key to generate a ciphertext, y defined as "the crypto square of x", while x is the crypto square root of y. Extended to higher powers, this formalism allows for polynomial morphology that combines all one-way functions candidates into a single master function which is at least as intractable as its best ingredient one-way function. The master list has some interesting and useful attributes: at will size for both input and output, controlled forward computational burden, milestone computing, and of course the best practical chance for being one-way.

Encryption of a plaintext, *p*, using a key, *k,* to generate a ciphertext *c* may be written through a multiplication analogy: $c= k \times p\ _{crypto} = k\,p\ _{crypto}$ where the left string is the key, and the right string is the plaintext. The plaintext may be an arbitrary binary string. We shall make the key the same by setting forth the rule that says that any string k* will be hashed to one of the legal key sizes of said cipher system. Any hash, or compression function will do, preferably a "straight compression" where no compression key is needed. This hashing step would allow one to crypto-multiply (as we shall call it) any two arbitrary size binary strings and generate a third (the ciphertext). And hence we can define the *crypto square* of a string as the generated ciphertext, *c*, from a plaintext *p*, which is also used as a key *p=k**, so that a valid key, *k,* for that ciphersystem will be the result of hashing of p. We can write therefore: $c=p^2\ _{crypto}$. And conversely: $p = \sqrt{c}\ _{crypto}$. Namely: *p* is the square root of *c* per the employed ciphersystem. Per the definition of a ciphrsystem, to "crypto-square" a string is a one-way function. For x, and y two binary strings such that: $y = x^2\ _{crypto}$ it is easy to compute $x \rightarrow y$, and difficult to compute y → x. The crypto square root operation of an arbitrary string using a given cipher system may be regarded as a "sterile" metrics of the inherent intractability of that cipher system. For any arbitrary string, per any cipher system there is a decidable answer on how many, if any, 'roots' are there, and what they are. As an intractability metric the square root operation seems less arbitrary than the customary cryptanalysis of some particular English text encrypted with that cipher.

We might further define for every $x = \{0,1\}^s$ and $s, n \in \mathrm{N}$, a string in the form of x^n to be evaluated from right to left: x(x(x….(x(x(xx)))…))): the right most string is crypto-multiplied with the next rightmost string, the resultant ciphertext is multiplied by the next rightmost string and so on until the last string is encountered. Also, by definition, for $y = x^{n,}$ x → y, is easy to compute, and y → x. is difficult. This notation will hold for cryptographic primitives where the ciphertext is larger than the plaintext, and for compression functions.

We may also use the plus symbol to denote concatenation, and hence the following expression is meaningful in the crypto context:

$$y = \sum_i a_i x^i \quad \text{crypto}$$

All the a_i expressions represent string constants that serve as keys to be used over the plaintext string represented by x^i .

We could further extend this notation over all known ciphersystems:

$$y = \sum_j \sum_i a_{ij} x^i$$

Where a_{ij} is the coefficient (string) used in element i for ciphersystem j, and the second summation is taken over all listed ciphersystems. To the extent that even one cipher system in the list is one-way, the above expression certainly is too. The latter expression will be referred to as the *Ciphersystem-Inclusive One-Way Function.*

We may expand this expression to include any type of one-way function candidate, *f,* where an arbitrary string x generates a binary string y, without the use of a cryptographic key. This would be done by formally introducing a key, k, in the form of a concatenation: *$y = f(k + x)$* where the "plus" is interpreted as concatenation. This formalism will render any one-way function candidate into a ciphersystem framework, and hence it could be included in the j summary of the inclusive one-way function concatenation. The summary will now list every known one-way candidate, and thereby referred to as the *One-Way Master Function* that by construction is at least as intractable as any of its listed one-way functions candidates.

For any given string *y* there may or may not be a solution in terms of the independent string variable *x*. And if there is one solution there may be several.

For example, the simple equation $y = x^2$ defined over Vernam cipher will have solutions only for $y = \{1\}^k$ And in that case there are 2^k solutions. Namely all strings in the form $\{0,1\}^k$ will qualify as a solution.

The Master One-Way Function can be adjusted to at-will input size, and at-will output size. To use it for input of size *k* bits and output of size *l* bit do:

$$y = (\sum_j \sum_i a_{ij} x^i)\lambda$$

Where $|x|=k$ and $|\lambda|=l$. We may agree that the last crypto-multiplication (with λ as the plaintext) will be based on the Vernam cipher, so that this crypto-multiplication does not reduce the intractability of the polynomial expression representing the key.

This at-will size attribute is important. The size of the input, x, may be made sufficiently large to hinder any attempt by a cryptanalyst to be ready with a pre computed lookup table, and sufficiently large to delay any brute force computation. The size of the output may be geared towards a human review and comparison, and to reduce to any negligible measure the chance for a lucky guess.

The master one-way function expression can be adjusted to milestone computing, where milestone m will be defined as:

$$y_m = (\sum_j \sum_i^m a_{ij} x^i)\lambda$$

It is "reasonable" to assume milestone-to-milestone intractability. Namely $y_m \rightarrow y_{m+t}$ will be intractable for t=1,2,3,…. To support this assumption let's collapse the Master One-Way function to its most intractable j-function, yielding:

$$y_m = (\sum_i^m a_i x^i)\lambda$$

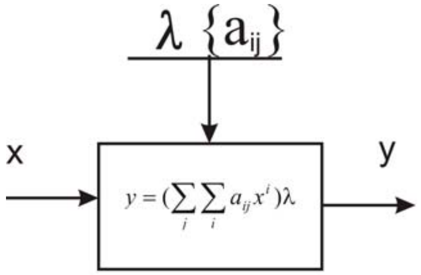
And so we may write:

$$y_{m+t} = (\frac{y_m}{\lambda} + \sum_{i=m+1}^{i=m+t} a_i x^i)\lambda$$

So that knowledge of y_m (without knowledge of x) will leave the cryptanalyst with the challenge of $\sum_{i=m+1}^{i=m+t} a_i x^i$.

The Master One-Way Function may be designed to be of any desired computational burden in the forward direction by picking the number of encryption steps (*m*).

In summary:



Master One-Way (MOW) Function

x,y -- arbitrary size strings
forward computing burden selectable
"Best Bet" one-way function