# A System for Generating Group Elements For Cryptographic Applications

## Detailed Description

A function, E-multiplication, may be computationally difficult to reverse using either a classical or a quantum algorithm. E-multiplication may be used to enable certain cryptographic protocols. Cryptographic protocols may involve subsets of elements of a fixed group, which may be publically assigned by some entity to one or more of the users of the specified protocol. While a given collection of group elements may be public, each element in that collection may be a product of other group elements that are not themselves public.

The search space of a group element whose product is fixed and public may be very large. A function called zCreator may be designed to be sensitive to an application specific Security Level.

## System Data:

A set $X = X_1 \biguplus X_2$, and
a finitely generated group $G_0$ which may act as a group of symmetries on the set $X$.

The action of the group $G_0$ may be specified by the group homomorphism $\theta$

$$\theta: G_0 \to G \subset \mathrm{Sym}(X),$$

where $\mathrm{Sym}(X)$ denotes the entire group of symmetries of the set $X$.

The following criteria are met:

- Elements in the group $G_0$ may be products of finite set of generators, and can be obscured. The method of obscuring an element in the group $G_0$ may be a normal form algorithm or may be an element-rewriting algorithm. The obscuring function of elements in the group $G_0$ may be denoted $\Psi$.

- Given $k \in \mathbb{Z}^{>0}$ such that $k \leq \mathrm{Card}(X_i)$, all $k$ element subsets of $X_i$ may be enumerated. Given a subset $Y \subset X$ it may be possible to specify the group of symmetries of $Y$, $\mathrm{Sym}(Y)$ via a Symmetry Generator.

- A Kernel Element Generator, which may be sensitive to a security parameter (which may be a Security Level as set forth below), may

produce expressions in the generators for the kernel of the group homomorphism $\theta$. Further, given an element $g \in G$, there may be an effectively computable function, the Pre-Image Generator, that may produce an element $g_0 \in G_0$, so that $\theta(g_0) = g$.

- There may exist subgroups of $G_0$, denoted $A, B$ so that:
  (1) every element in $A$ may commute with every element in $B$;
  (2) $A$ respectively, $B$ act trivially on $X_1$, respectively $X_2$; and
  (3) it may be possible to specify elements of high order (as compared to the average case) in subgroups, $\theta(A)$ and $\theta(B)$ via a search of each subgroup.

- A Security Level, denoted $\zeta$, which may be appropriate to the cryptographic application, may be specified.

# The Method:

Figure 1 depicts a module for a function called zCreator.

The element $z \in G_0$ may be the output of the function zCreator. $z$ may depend on a Security Level $\zeta$ and a fixed number $k$, and is described below.

- A Pseudo-Random Number Generator may produce a number $k \leq \text{Card}(X_i)$, for $i = 1,2$. In some instances, the value of $k$ may be specified by the application.

- The value $k$ may be inputted into the Subset Chooser whose output will be subsets of cardinality $k$:

$$Y_1 \subset X_1, \quad \overline{Y_1} \subset X_2$$

$$Y_2 \subset X_2, \quad \overline{Y_2} \subset X_1.$$

- The pairs of subsets $\{Y_1, Y_2\}, \{\overline{Y_2}, \overline{Y_1}\}$ may be inputted into the Union of Complements Evaluator to produce the outputs

$$U_1 = X_1 \sim Y_1 \cup X_2 \sim Y_2$$

$$U_2 = X_1 \sim \overline{Y_2} \cup X_2 \sim \overline{Y_1}.$$

- The subset of $U_2 \subset X$ may be inputted into the Symmetry Generator to produce a one-to-one onto mapping from $\gamma_0' : U_2 \to U_2$. This mapping may be chosen to have high order. The canonical bijection $\iota : U_1 \to U_2$ may be

composed with this outputted symmetry resulting in the one-to-one onto mapping

$$\gamma_0 = \gamma_0' \circ \iota, \ \ \gamma_0 \colon U_1 \to U_2.$$

- The subsets $Y_1, \overline{Y_1}$ and $Y_2, \overline{Y_2}$ each have $k$ elements, and canonical bijections between them:

$$\gamma_1 \colon Y_1 \to \overline{Y_1}, \ \ \gamma_2 \colon Y_2 \to \overline{Y_2}.$$

- The functions $\gamma_0, \gamma_1, \gamma_2$ may be inputted into the Function Compiler to yield an element $z \in G$, a symmetry of the set $X$. The Security Level Evaluator may evaluate SecLev$(z)$, the size of the search space for all possible elements $z$ produced in this manner.

- The element $z$ may be inputted into the Pre-Image Generator to produce an element $z_0 \in G_0$.

- The difference between the originally specified security level, $\zeta$, and SecLev$(z)$ may be evaluated by the Security Difference Evaluator.

- The output of the Security Difference Evaluator, Diff$(\zeta)$, maybe inputted into the Kernel Element Generator. The Kernel Element Generator may produce a kernel element, $z_{\text{Ker,}}$ which may necessitate a search of at least the magnitude Diff$(\zeta)$. The product of the Kernel Element Generator $z_{\text{Ker}}$ and the element z, is the output of the function zCreator:

$$z \ = \ z_{\text{Ker}} \cdot z_0.$$

Figure 2 may depict a Set of Conjugates Generator. The subset of group elements generated may enable a key agreement protocol based on E-Multiplication. Said subset of elements may be appropriate for the case when the subset must be sent over an open channel of communication. In the case of two subsets being sent over an open channel, the method may be used for both parties.

Each element generated may take the form $\Psi(z \ a_i \ z^{-1})$, where the element $a_i \in A$, element $z \ \in G_0$, and $\Psi$ may be the postulated obscuring function. The method to produce the elements $a_i \in A$ is described below.

- Choose a collection of elements $\{\alpha_1, \alpha_2, \ldots, \alpha_{n_1}\} \subset \theta(A)$ each of which may have high order. The cardinality $n_1$ of the set of group elements may be a random number as small as 2 or may relate to the running time of the cryptographic application.

- Input each of the elements $\alpha_1, \alpha_2, \ldots, \alpha_{n_1}$ into the effectively computable Pre-Image generator. The outputs of the Pre-Image Generator may be denoted $a_1, a_2, \ldots, a_{n_1}$. The Pre-Image Generator may evaluate the pre-image of each generator of the group $G$, and use these outputs to evaluate a pre-image for an arbitrary element of $G$.

The element $z \in G_0$ referred to above may be the output of the function zCreator, which may depend on Security Level $\zeta$ and fixed number $k$, is described above.

Claims:

1. A method to generate a set of conjugates, the method comprising:

determining a collection of elements such that the collection of elements is a subset of $\theta(A)$, wherein $\theta$ is a group homomorphism, and $A$ is a subgroup of the group $G_0$;

inputting each element in the collection of elements into a pre-image generator and generating an output set of the pre-image generator, wherein the pre-image generator evaluates a pre-image of each generator of the group $G$;

generating an element $z$ by a zCreator, wherein $z$ is an element of $G_0$, and is based on a security level $\zeta$ and fixed number $k$; and

generating the set of conjugates based on the output set of the pre-image generator and the element $z$.