Examples of One-Way Collections:

(2) **The Robin Function:** The Robin collection of functions has an index set consisting of N, where N is a product of two $(\frac{1}{2}\cdot \log_2 N)$-bit primes, denoted P and Q. The function of index N has domain Z_N^* and maps the domain element x to $x^2 \pmod N$: $\text{Robin}_N(x) = x^2 \pmod N$. The Robin function is not a permutation. It is a 4 to 1 mapping on Z_N^*. Suppose we want to find square root of a modulo $N = PQ$. First we find square roots modulo P and Q: Let $x^2 \equiv a \pmod P$ and $y^2 \equiv a \pmod Q$. Then there are four solutions to the congruence $z^2 \equiv a \pmod N$. Let $c, d \in Z_n$ be the Chinese Remainder Theorem coefficients:

$c \equiv 1 \pmod P$ and $c \equiv 0 \pmod Q$.

$d \equiv 0 \pmod P$ and $d \equiv 1 \pmod Q$.

Then the four solutions modulo N are:

$cx+dy$, $cx-dy$, $-cx+dy$, and $-cx-dy$

We can easily verify the solutions. For example,

$(cx+dy)^2 \equiv c^2x^2 \equiv a \pmod P$ and

$(cx+dy)^2 \equiv d^2y^2 \equiv a \pmod Q$

$\Rightarrow (cx+dy)^2 \equiv a \pmod N$.

Let p be an odd prime and let a be a quadratic residue modulo p. There exists a probabilistic algorithm A running in expected polynomial time such that $A(p, a) = x$ where $x^2 \equiv a \pmod p$.

Inverting Robin $\leq_p$ Factorization : Suppose we are given an instance of inverting the Robin function: $(N, a \pmod N)$, where $N = PQ$ for some primes P and Q, and a is a quadratic residue modulo N. We can easily convert this into an instance of factorization : (N). Suppose we have an efficient algorithm for factorization. Now we can easily get P and Q. There exists a probabilistic algorithm SQRT running in expected polynomial time such that $SQRT(P, Q, N, a) = x$ where $x^2 \equiv a \pmod N$. The algorithm SQRT will first make calls to A to obtain square roots of a modulo each of the primes P and Q. It then combines these square roots, using the Chinese Remainder Theorem, to obtain the required square root. The algorithm SQRT runs as follows :

① Let $A(P, a) = x_1$ and $A(Q, a) = x_2$.

② Use the Chinese Remainder Theorem to find in polynomial time $y \in Z_n$ such that $y \equiv x_1 \pmod P$ and $y \equiv x_2 \pmod Q$ and output y.

Algorithm SQRT runs correctly because $y^2 \equiv x_1^2 \equiv a \pmod P$ and $y^2 \equiv x_2^2 \equiv a \pmod Q \Rightarrow y^2 \equiv a \pmod N$.

Factorization $\leq_p$ Inverting Robin : Suppose we are given an instance of factorization problem: $N = PQ$. We can easily convert this into an instance of Inverting the Robin function : $(N, x^2 \pmod N)$ where $x \in Z_N^*$. Suppose I is an efficient algorithm which on input $N = PQ$, and a a quadratic residue modulo N outputs y such that $a \equiv y^2 \pmod N$.

Now consider the following algorithm B which on input N outputs a nontrivial factor of N:

① Randomly choose $x \in Z_N^*$.

② Set $y = I(N, x^2 \pmod N)$.

③ Check if $x \equiv \pm y \pmod N$. If not then $\gcd(x-y, N)$ is a nontrivial divisor of N. Otherwise, repeat from ①.

Algorithm B runs correctly because $x^2 \equiv y^2 \pmod N \Rightarrow (x+y)(x-y) \equiv 0 \pmod N \Rightarrow N \mid (x+y)(x-y)$. But $N \nmid (x-y)$ because $x \not\equiv y \pmod N$ and $N \nmid (x+y)$ because $x \not\equiv -y \pmod N \Rightarrow \gcd(x-y, N)$ is a nontrivial divisor of N. The congruence $x^2 \equiv a \pmod N$ has either 0 or 4 solutions $\Rightarrow$ if $I(N, x^2) = y$, then $x \equiv \pm y \pmod N$ with probability $\frac{1}{2}$ and hence the above algorithm is expected to terminate in 2 iterations.

From the above two results we can say that from our assumption that the factorization problem is strongly One-way it follows that the Robin function is also strongly one way. This satisfies the second property of One way collection of functions. First property of one way collection of functions is also easy to prove.

On input 1^n, algorithm I_{Robin} selects uniformly two primes, P and Q such that $2^{n-1} \leq P < Q < 2^n$ and terminates with output N, where $N = PQ$. The algorithm D_{Robin}, on input N selects almost uniformly an element in the set $D_N = Z_N^*$ The output of F_{Robin} on input (N, x) is : $Robin_N(x) = x^2 \pmod N$.

Examples of One-Way Collections:

(3) The Discrete-Logarithm Problem: The DLP collection of functions is defined by the triplet of algorithms $(I_{DLP}, D_{DLP}, F_{DLP})$. On input 1^n, algorithm I_{DLP} selects uniformly a prime P, such that $2^{n-1} \le P < 2^n$, and a primitive element G from G^*_P, and outputs (P, G). The algorithm D_{DLP}, on input (P, G) it selects uniformly a residue x modulo $P-1$. Algorithm F_{DLP}, on input $((P,G), x)$, outputs:

$$DLP_{P,G}(x) = G^x \pmod P.$$

Inverting $DLP_{P,G}$ amounts to extracting the discrete logarithm (to base G) modulo P. For every (P, G), the function $DLP_{P,G}$ induces a one to one and onto mapping from G_{P-1} to G^*_P. $DLP_{P,G}$ induces a permutation on the set $\{1, \ldots, P-1\}$. The DLP is believed to be a strongly one way function. $DLP_{P,G}$ is an Isomorphism from G_{P-1} to G^*_P:

Suppose $G^x \equiv G^y \pmod P \Rightarrow G^{x-y} \equiv 1 \pmod P$.
G is a generator of $G^*_P \Rightarrow \phi(P) \mid (x-y)$
$\Rightarrow (P-1) \mid (x-y) \Rightarrow x \equiv y \pmod{(P-1)}$.
$\Rightarrow DLP_{P,G}$ is one to one and onto map from G_{P-1} to $G^*_P \Rightarrow DLP_{P,G}$ is a permutation on the set $\{1, \ldots, P-1\}$. An isomorphism is a mapping $f: G_1 \to G_2$ such that $f(x \circ y) = f(x) \circ f(y)$ and f is one to one.
($\circ$: operator of G_1; $\circ$: operator of G_2)

Trapdoor One-Way Permutations are collections of one-way permutations, $\{f_i\}$, with the extra property that f_i is efficiently inverted once it is given as auxiliary input a "trapdoor" for the index i. The trapdoor for index i, denoted by $t(i)$, cannot be efficiently computed from i, yet one can efficiently generate corresponding pairs $(i, t(i))$.

Let $I : 1^* \longrightarrow \{0,1\}^* \times \{0,1\}^*$ be a probabilistic algorithm and let $I_1(1^n)$ denote the first element of the pair output by $I(1^n)$. A triple of algorithms, (I, D, F), is called a collection of strong trapdoor permutations if the following two conditions hold:

(1) The algorithms induce a collection of one-way permutations: The triple (I_1, D, F) constitutes a collection of strong one-way permutations.

(2) Easy to invert with trapdoor: There exists a deterministic polynomial-time algorithm, denoted F^{-1}, such that for every (i,t) in the range of I and for every $x \in D_i$, it holds that

$$F^{-1}(t, f_i(x)) = x.$$

The RSA Trapdoor: For index $i = (N, e)$, we have the trapdoor $t = (N, d)$, where d is the multiplicative inverse of e modulo $(P-1)\cdot(Q-1)$. The inverting algorithm F^{-1}_{RSA} is identical to the algorithm F_{RSA}: $F^{-1}_{RSA}((N,d), y) = y^d \pmod N$. We can easily verify that $F^{-1}_{RSA}((N,d), F_{RSA}((N,e), x)) \equiv x^{de} \equiv x \pmod N$ for every x (even in case x is not relatively prime to N).