RSA accumulators can efficiently store primes, but are (as far as I know) not efficient with non-prime numbers. My goal is to store arbitrary values, just like you can do in a Merkle tree, but having a shorter proof size. This can have multiple applications, such as in zk-starks, Plasma, etc.

I believe it is possible that we can proof that multiple values are contained in the accumulator with a single 2048

bit witness.

Basic example for three values

Let a

, b

and c

be the values we like to store.

Let $\textit{h}$

be a secure hash function.

Let N

be a 2048

bit RSA modulus with unknown factorization and g

be the generator.

Let p

, q

and r

be three distinct large primes.

The accumulator $A = g^{qr \textit{h}(a)+pr \textit{h}(b)+pq \textit{h}(c)} \mod N$

To proof that a

is stored in the first spot we need a witness $W = g^{r \textit{h}(b)+q \textit{h}(c)} \mod N$

The verifier has to check that $g^{qr \textit{h}(a)}W^{p} \equiv A\mod N$

To proof a fake value a'

is in the accumulator, the forger needs to calculate the p

-root of $g^{qr (\textit{h}(a)-\textit{h}(a'))+pr \textit{h}(b)+pq \textit{h}(c)}\mod N$

. I believe this problem to be computationally infeasible when the RSA trapdoor is unknown.

It is also possible to make a single proof that the accumulator contains multiple values. For example when we want to proof a

and b

are both stored in the accumulator, we need the witness $W = g^{\textit{h}(c)} \mod N$

The verifier has to check that $g^{qr \textit{h}(a)+pr \textit{h}(b)}W^{pq} \equiv A\mod N$

Hash accumulator with n primes

We can generalize this to an accumulator for n

values using n

primes.

Let $x_{1},..,x_{n}$

be the n

values we like to store.

Let $p_{1},..,p_{n}$

be n

distinct large primes.

We define P_S

to be g

to the power of the product of all the primes not contained in the set S

modulo N

$P_S = g^{\prod\limits_{\substack{k=1,k\not\in S}}^n p_{k}} \mod N$

The accumulator $A = \prod\limits_{k=1}^n P_{k}^{\textit{h}(x_k)} \mod N$

To proof x_i

is stored in spot i

we need a witness $W = \prod\limits_{k=1, k\neq i} ^n P_{i,k}^{\textit{h}(x_k)} \mod N$

The verifier has to check that $P_i^{\textit{h}(x_i)} W^{p_i} \equiv A \mod N$

To proof that multiple values from set B are in the accumulator we need a single witness $W = \prod\limits_{k=1, k\not\in B} ^n P_{B,k}^{\textit{h}(x_k)} \mod N$

And the verifier has to check that $\prod\limits_{k\in B} P_{k}^{\textit{h}(x_k)} W^{\prod\limits_{k\in B}p_k} \equiv A \mod N$