Public parameters are supposed to consist of $g_1^{\alpha^i}$ and $g_2^{\alpha^i}$ for $i$ from 1 to $2N$, except $N+1$ is omitted. This document describes and argues security of two procedures, one deterministic and one probabilistic, for determining whether an alleged set of parameters is indeed of this form.

## Notation

For $1 \le i \le 2N, i \ne N+1$, write

$$\begin{aligned} &f_i \text{ to denote the } \mathbb{G}_1 \text{ element that is allegedly } g_1^{\alpha^i} \\ &h_i \text{ to denote the } \mathbb{G}_2 \text{ element that is allegedly } g_2^{\alpha^i} \end{aligned}$$

and for notational convenience, write

$$\begin{aligned} f_0 &= g_1 \\ h_0 &= g_2. \end{aligned}$$

A set of (alleged) parameters

$$\{f_i, h_i\}_{1 \le i \le 2N, i \ne N+1}$$

are *consistent* if $\exists \alpha \notin \{0,1\}$ such that $\forall i, f_i = g_1^{\alpha^i}$ and $h_i = g_2^{\alpha^i}$.

## Deterministic consistency check

Given an alleged set of parameters, the following procedure determines whether they are consistent. In the below discussion, without loss of generality, let $\alpha$ be such that $f_1 = g_1^\alpha$.

1. Check that none of the $f_i$ or $h_i$ are 1, $g_1$, or $g_2$. (This ensures $\alpha \notin \{0,1\}$.)
2. Check that

   $$e(f_i, h_0) = e(f_0, h_i) \quad \text{for all } 1 \le i \le N \text{ and } N+2 \le i \le 2N$$

   This ensures that $\log_{g_1} f_i = \log_{g_2} h_i$ for all $i$ — in other words, the exponents of each $f_i$ and corresponding $h_i$ match. In particular we now know $h_1 = g_2^\alpha$.
3. Check that

   $$e(f_i, h_1) = e(f_{i+1}, h_0) \quad \text{for all } 1 \le i \le N-1$$

   This ensures $f_i = g_1^{\alpha^i}$ (and also $h_i = g_2^{\alpha^i}$ by the previous check) for $1 \le i \le N$. (To see this, consider the $i=1$ case, where we check $e(f_1, h_1) = e(f_2, h_0)$. $e(f_1, h_1) = e(g_1^\alpha, g_2^\alpha)$, so $f_2$ must be $g_1^{\alpha^2}$. Then the $i=2$ check forces $f_3$ to be $g_1^{\alpha^3}$ and so on.)

4. Check that

$$e(f_i, h_N) = e(f_{i+N}, h_0) \quad \text{for all } 2 \le i \le N$$

In other words, check $e(f_{i+N}, g_2) = e(g_1^{\alpha^i}, g_2^{\alpha^N})$, which ensures $f_{i+N} = g_1^{\alpha^{i+N}}$ for $2 \le i \le N$. (This also ensures $h_{i+N} = g_2^{\alpha^{i+N}}$ for $2 \le i \le N$ because we know the exponents of the $f$'s and $h$'s match.)

If all checks pass, then we know that $f_i = g_1^{\alpha^i}$ and $h_i = g_2^{\alpha^i}$ for all $1 \le i \le 2N, i \ne N$, and we know $\alpha \notin \{0, 1\}$. So the parameters are consistent.

## Probabilistic consistency check

A randomized version of the above algorithm can check consistency much more efficiently, using $O(1)$ rather than $O(N)$ pairings, with a soundness error of $O(\frac{1}{|\mathbb{G}_1|})$.

1. Generate $N$ random scalars $r_1, \ldots, r_N$ and compute the following:

$$\begin{aligned}
R_1 &= \prod_{i=1}^{N} f_i^{r_i} \\
R_2 &= \prod_{i=1}^{N} h_i^{r_i} \\
S &= \prod_{i=1}^{N-1} f_i^{r_i} \left( = \frac{R_1}{f_N^{r_N}} \right) \\
T &= \prod_{i=1}^{N-1} f_{i+1}^{r_i} \\
U_1 &= \prod_{i=1}^{N-1} f_{i+N+1}^{r_i} \\
U_2 &= \prod_{i=1}^{N-1} h_{i+N+1}^{r_i}
\end{aligned}$$

2. Check that none of the $f$'s or $h$'s are 1, $g_1$, or $g_2$, just like in the deterministic procedure.

3. Check that

$$e(R_1, h_0) = e(f_0, R_2)$$

In other words, check that

$$e(\prod_{i=1}^{N} f_i^{r_i}, h_0) = e(f_0, \prod_{i=1}^{N} h_i^{r_i})$$

This ensures $e(f_i, h_0) = e(f_0, h_i)$ for all $1 \leq i \leq N$ with soundness error $\frac{1}{|\mathbb{G}_1|}$.

4. Check that

   $$e(U_1, h_0) = e(f_0, U_2)$$

   This ensures $e(f_i, h_0) = e(f_0, h_i)$ for all $N + 2 \leq i \leq 2N$ with soundness error $\frac{1}{|\mathbb{G}_1|}$. Combined with the previous step, this is equivalent to check 2 of the deterministic procedure.

5. Check that

   $$e(S, h_1) = e(T, h_0)$$

   or in other words,

   $$e(\prod_{i=1}^{N-1} f_i^{r_i}, h_1) = e(\prod_{i=1}^{N-1} f_{i+1}^{r_i}, h_0)$$

   This ensures that $e(f_i, h_1) = e(f_{i+1}, h_0)$ for all $1 \leq i \leq N - 1$ with soundness error $\frac{1}{|\mathbb{G}_1|}$. This is equivalent to check 3 of the deterministic procedure.

6. Check that

   $$e(U_1, h_0) = e(T, h_N)$$

   or in other words,

   $$e(\prod_{i=1}^{N-1} f_{i+N+1}^{r_i}, h_0) = e(\prod_{i=1}^{N-1} f_{i+1}^{r_i}, h_N)$$

   This ensures that $e(f_{i+N+1}, h_0) = e(f_{i+1}, h_N)$ for all $1 \leq i \leq N - 1$ (with soundness error $\frac{1}{|\mathbb{G}_1|}$). This is equivalent to check 4 of the deterministic procedure.

If all of the above checks pass, then the parameters are consistent with high probability.

This randomized procedure is equivalent to the deterministic procedure in the previous section but with soundness error $\frac{4}{|\mathbb{G}_1|}$.