In [1] a signature scheme is proposed which admits a reduction to the CDH problem in the standard model, at the cost of the honest signer maintaining and updating state between every signature. This has obvious costs in terms of complexity and fragility of the resulting cryptosystem.

In this note we demonstrate that it is necessary to maintain this state, by considering the case that two signatures $\sigma_1, \sigma_2$ are produced which use the same $s$ but distinct $r$ and distinct messages $M$. **We show that it is possible for an attacker to forge a signature in this case.**

For ease of notation, since $s$ is constant, we will write $\gamma = w^{[\log_2 s]}.h$. Suppose we have two signatures

$$
\sigma_1 = (u^{M_1}v^r d)^{a^1}, \quad s_1 = g^{t_1}, \quad r_1, \quad s
$$

$$
\sigma_2 = (u^{M_2}v^r d)^{a^2}, \quad s_2 = g^{t_2}, \quad r_2, \quad s
$$

We will construct a valid signature for a message $M$. To this end, we write

$$
\begin{align*}
\gamma &= w^{[\log_2 s]}h \\
v &= u^x g^y, d = u^{-xd} g^{yd}
\end{align*}
$$

where $x_v, x_d$ are defined as

$$
\begin{align*}
x_v &= \frac{M_1 - M_2}{r_2 - r_1} \\
x_d &= \frac{r_2 M_1 - r_1 M_2}{r_2 - r_1}
\end{align*}
$$

and the values of $y_v, y_d$ are forced.

Then we notice that for $i = 1, 2,$

$$
\sigma_i = (u^{M_i}v^r d)^{a^i} = (u^{M_i + r_i x_v - x_d} g^{y_v r_i + y_d})^{a^i} = (g^{a^i})^{y_v r_i + y_d}
$$

(1)

since $M_i + r_i x_v - x_d = 0$. (In fact, we obtained the above values of $x_v, x_d$ by starting from this equation and solving. See the use of $x_v, x_d$ by the simulator on page 16 of [1], which coincide with our values in the case $s = i^*$.)

Then [1] lets us isolate $g^{a^1}$ and $g^{yd}$ as

$$
\begin{align*}
A &:= \{\sigma_1 (\sigma_2^{-1})\}^{1/(r_1 - r_2)} = g^{a^1 (r_1 - r_2)/(r_1 - r_2)} \\
B &:= \sigma_1 (g^{a^1})^{r_1} = g^{a^1 r_1}
\end{align*}
$$

Finally, we choose $r = (x_d - M)/x_v,$ and forge a signature as

$$
\begin{align*}
\sigma_1 &= A^r B = (g^{a^1})^{y_v r + y_d} g^{r (r_1 - r_2)/(r_1 - r_2) + r_1} \\
\sigma_2 &= [\sigma_2 (\sigma_2^{-1})]^{r/(r_1 - r_2)} \sigma_2^2 = g^{r (r_1 - r_2)/(r_1 - r_2) + r_1}
\end{align*}
$$

We claim that $\sigma = (\sigma_1, \sigma_2, r, s)$ is a valid signature for the message $M$. To verify correctness, we
use the fact that $M + rx_v - x_d = 0$ to write the verification equation as

$$e(\sigma_1, g) = e((g^a)^{y_v r + y_d}, g)e(\gamma^{(r_1 - r_2)/(r_1 - r_2)} r_1, g)$$

$$= e((g^a)^{y_v r + y_d}, g)e(\gamma, \sigma_2)$$

$$= e((u^M r x_v - x_d g^{y_v r + y_d})^a, g)e(\gamma, \sigma_2)$$

$$= e((u^M (u^v g^{y_v})^r u^{-y_d g^{y_d}})^a, g)e(\gamma, \sigma_2)$$

$$= e((u^M v^d)^a, g)e(\gamma, \sigma_2)$$

$$= e(u^M v^d, g^a)e(\gamma, \sigma_2)$$

References