Short Sigs/Standard Model

Andrew Poelstra
June 2014

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 σ^1, σ^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 $\gamma = w^{\lceil \lg s \rceil} z^s h$. Suppose we have two signatures

$$\sigma_1^1 = (u^{M^1} v^{r^1} d)^a \gamma^{t^1}, \qquad \sigma_2^1, = g^{t^1}, \qquad r^1, \qquad s$$

$$\sigma_1^2 = (u^{M^2} v^{r^2} d)^a \gamma^{t^2}, \qquad \sigma_2^2, = g^{t^2}, \qquad r^2, \qquad s$$

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

$$v = u^{x_v} g^{y_v}, d = u^{-x_d} g^{y_d}$$

where x_v, x_d are defined as

$$x_v = \frac{M^1 - M^2}{r^2 - r^1}$$

$$x_d = \frac{r^2 M^1 - r^1 M^2}{r^2 - r^1}$$

and the values of y_v, y_d are forced.

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

$$\sigma_1^i = (u^{M^i} v^{r^i} d)^a \gamma^{t^i} = (u^{M^i + r^i x_v - x_d} g^{y_v r^i + y_d})^a \gamma^{t^i} = (g^a)^{y_v r^i + y_d} \gamma^{t^i} \tag{1}$$

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^{ay_v} and g^{y_d} as

$$A := \left\{ \sigma_1^1 (\sigma_1^2)^{-1} \right\}^{1/(r^1 - r^2)} = g^{ay_v} \gamma^{(t^1 - t^2)/(r^1 - r^2)}$$
$$B := \sigma^1 (g^{ay_v})^{-r^1} = g^{ay_d} \gamma^{t^1}$$

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

$$\sigma_1 = A^r B = (g^a)^{y_v r + y_d} \gamma^{r(t^1 - t^2)/(r^1 - r^2) + t^1}$$

$$\sigma_2 = \left[\sigma_2^1 (\sigma_2^2)^{-1} \right]^{r/(r^1 - r^2)} \sigma_2^2 = g^{r(t^1 - t^2)/(r^1 - r^2) + t^1}.$$

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

$$\begin{aligned}
e(\sigma_1,g) &= e((g^a)^{y_v r+y_d},g)e(\gamma^{r(t^1-t^2)/(r^1-r^2)+t^1},g) \\
&= e((g^a)^{y_v r+y_d},g)e(\gamma,\sigma_2) \\
&= e((u^{M+rx_v-x_d}g^{y_v r+y_d})^a,g)e(\gamma,\sigma_2) \\
&= e((u^M(u^{x_v}g^{y_v})^r u^{-x_d}g^{y_d})^a,g)e(\gamma,\sigma_2) \\
&= e((u^M v^r d)^a,g)e(\gamma,\sigma_2) \\
&= e(u^M v^r d,g^a)e(\gamma,\sigma_2)
\end{aligned}$$

References

[1] Susan Hohenberger and Brent Waters, *Realizing hash-and-sign signatures under standard assumptions*, Cryptology ePrint Archive, Report 2009/028, 2009, `http://eprint.iacr.org/`.