SNARK-Friendly Weight Threshold Verification

Xiong Fan and Chris Peikert

Algorand, Inc.

July 19, 2022

1 Derivation

For the compact certificate verifier, our goal is to provide a SNARK-friendly verification of the inequality

$$\mathsf{numReveals} \cdot (\log_2(\mathsf{signedWt}) - \log_2(\mathsf{provenWt})) \geq \mathsf{target} \tag{1}$$

for given positive integers $\mathsf{numReveals}, \mathsf{signedWt}, \mathsf{provenWt}$, and a fixed positive integer target. Since SNARKs cannot compute the exact values of logarithms, we need to use suitable approximation bounds, and wish to do so in relatively low complexity and with little approximation loss.

By changing the base-2 logarithms to natural logarithms, Equation (1) is equivalent to

$$\mathsf{numReveals} \cdot (\ln(\mathsf{signedWt}) - \ln(\mathsf{provenWt})) \geq \mathsf{target} \cdot \ln(2). \tag{2}$$

Note that $\mathsf{provenWt}$ is provided as trusted information (from the previous state proof). Therefore, a trusted, precise upper bound on its natural-base logarithm can also be given as input. So, we mainly focus on approximating $\ln(\mathsf{signedWt})$ well enough to establish Equation (2) without much approximation loss.

Claim 1.1. *Suppose that* $\mathsf{signedWt}/2^d \geq 1$ *for some integer* $d \geq 0$, *let* $p = P/2^b \geq \ln(\mathsf{provenWt})$, $t = T/2^b \geq \ln(2) > (T-1)/2^b > 0$ *for some integers* $b, P, T \geq 0$, *and let*

$$Y = \mathsf{signedWt}^2 + 4 \cdot 2^d \cdot \mathsf{signedWt} + 2^{2d} > 0.$$

Then Equation (2) holds if

$$\mathsf{numReveals} \cdot \left(3 \cdot 2^b \cdot (\mathsf{signedWt}^2 - 2^{2d}) + d \cdot (T-1) \cdot Y\right) \geq (\mathsf{target} \cdot T + \mathsf{numReveals} \cdot P) \cdot Y. \tag{3}$$

Observe that Equation (3) is equivalent to the following two conditions, which may be more convenient to use when constructing (rather than just verifying) a certificate, since they give a direct bound on $\mathsf{numReveals}$:

$$D := 3 \cdot 2^b \cdot (\mathsf{signedWt}^2 - 2^{2d}) + (d \cdot (T-1) - P) \cdot Y > 0, \tag{4}$$

$$\mathsf{numReveals} \geq \frac{\mathsf{target} \cdot T \cdot Y}{D}. \tag{5}$$

Also note that it is possible for D to be negative—e.g., if $\mathsf{signedWt}$ is equal to, or even slightly larger than, both 2^d and $\mathsf{provenWt}$—but in this case it is impossible to satisfy Equation (3).

Proof of Claim 1.1. First of all, dividing by $2^b \cdot Y > 0$, Equation (3) implies that

$$\begin{aligned}
&\mathsf{numReveals} \cdot \left(\frac{3(\mathsf{signedWt}^2 - 2^{2d})}{Y} + d\ln(2) - p \right) \\
&> \mathsf{numReveals} \cdot \left(\frac{3(\mathsf{signedWt}^2 - 2^{2d})}{Y} + d \cdot \frac{T-1}{2^b} - p \right) \\
&\geq \mathsf{target} \cdot t. \qquad (6)
\end{aligned}$$

Next, Padé expansion [1, Table 3] gives the lower bound (valid for all $x \geq 1$)

$$\ln x \geq \frac{3(x^2-1)}{x^2+4x+1}. \qquad (7)$$

So, we have

$$\begin{aligned}
&\mathsf{numReveals} \cdot (\ln(\mathsf{signedWt}) - \ln(\mathsf{provenWt})) \\
&\geq \mathsf{numReveals} \cdot \left(\ln \frac{\mathsf{signedWt}}{2^d} + d\ln(2) - p \right) && (p \geq \ln(\mathsf{provenWt})) \\
&\geq \mathsf{numReveals} \cdot \left(\frac{3(\mathsf{signedWt}^2 - 2^{2d})}{Y} + d\ln(2) - p \right) && (\text{Equation (7)}, \mathsf{signedWt}/2^d \geq 1) \\
&> \mathsf{target} \cdot t && (\text{Equation (6)}) \\
&\geq \mathsf{target} \cdot \ln(2). && (t \geq \ln(2))
\end{aligned}$$

This establishes Equation (2), as desired. □

Observe that both sides of Equation (3) involve only integer operations, and are positive. We now show that for typical parameters, both sides are much smaller than the size of the SNARK's underlying field, so there is no overflow in their computation by the SNARK. Since signedWt and provenWt are denominated in micro-Algos, and there can be at most 10^{10} Algos in circulation, both quantities are bounded by $10^{16} < 2^{54}$, so also $d \leq 54$. Now suppose that numReveals is upper bounded by (say) 2^{10}, and the bounds on $\ln(2)$ and $\ln(\mathsf{provenWt})$ are given with up to 16 bits of precision, i.e., $b \leq 16$, so T and P are upper bounded by 2^{16} and 2^{22}, respectively.

Therefore, the left-hand side of Equation (3) is upper bounded by 2^{142}, which is much less than the capacity of the SNARK's underlying field (more than 2^{254}). For the right-hand side of Equation (3), target will be no more than 512, so that side is also upper bounded by 2^{142} (regardless of whether the inequality holds).

2 Approximation Analysis

To analyze the relative cost of using approximations in place of exact amounts, we compare the minimum values of numReveals that satisfy Equation (1) versus Equation (3), and consider their ratio. In summary, for all realistic values of the parameters, the cost is a less-than-1% increase in the value of numReveals.

For Equation (3), we take

$$\mathsf{numReveals} = \frac{\mathsf{target} \cdot T \cdot Y}{3 \cdot 2^b \cdot (\mathsf{signedWt}^2 - 2^{2d}) + (d \cdot (T-1) - P) \cdot Y},$$

and for Equation (1) we take

$$\mathsf{numReveals}' = \frac{\mathsf{target}}{\log_2(\mathsf{signedWt}/\mathsf{provenWt})}.$$

The ratio of the above two quantities is

$$\gamma = \frac{\mathsf{numReveals}}{\mathsf{numReveals}'} = \frac{T \cdot Y \cdot \log_2(\mathsf{signedWt}/\mathsf{provenWt})}{3 \cdot 2^b \cdot (\mathsf{signedWt}^2 - 2^{2d}) + (d \cdot (T-1) - P) \cdot Y}. \tag{8}$$

To analyze the ratio γ for realistic values of the parameters, we wrote a simple python program to compute Equation (8) (see below). We let $d = \lfloor \log_2(\mathsf{signedWt}) \rfloor$ in order to minimize $\mathsf{signedWt}/2^d \geq 1$, and fixed $b = 16$, i.e., we approximate $\ln(2)$ and $\ln(\mathsf{provenWt})$ with 16 bits of precision, and let $T = \lceil 2^b \cdot \ln(2) \rceil$ and $P = \lceil 2^b \cdot \ln(\mathsf{provenWt}) \rceil$. We use the `Decimal` type with a moderately large (fixed) amount of precision in order to ensure sufficient accuracy of the calculations.

The ratio γ is smallest when $\mathsf{signedWt}$ is a power of two, i.e., $\mathsf{signedWt}/2^d = 1$. In this case, there is no error at all in the Padé approximation, so γ is extremely close to 1. (There is still some slight approximation error in T and P, but it is very small due to the use of $b = 16$ bits of precision.) Conversely, γ is largest when $\mathsf{signedWt}$ is slightly less than a power of two, i.e., $\mathsf{signedWt} = 2^{d+1} - 1$, because the error from the Padé approximation of $\ln(x)$ increases with x, and here $x = \mathsf{signedWt}/2^d \approx 2$ is essentially maximized.

Using realistic values $\mathsf{signedWt} \in \{2^{40}-1, 2^{38}-1, 2^{36}-1, 2^{32}-1, 2^{16}-1\}$ and $\mathsf{signedWt}/\mathsf{provenWt} \in \{1.1, 1.2, 1.3, \ldots, 2\}$, the ratio γ is always less than 1.01. That is, the minimal value of $\mathsf{numReveals}$ obtained from Equation (3) is less than 1% larger than the one obtained from Equation (1). The magnitude of $\mathsf{signedWt}$ has almost no effect on γ, whereas the weight ratio $\mathsf{signedWt}/\mathsf{provenWt}$ has a minor effect: as it increases from 1.1 to 2, the value of γ decreases from about 1.009 to about 1.001. So, the relatively large weight ratios that we typically expect to see in practice correspond to lower costs of approximation.

Python code.

```
from math import log, floor, ceil
from decimal import *

getcontext().prec = 32
b = 16
two = Decimal(2)
B = two**b
T = Decimal(ceil(B * Decimal.ln(two)))

def ratio(sigWt, weightRatio):
    d = floor(Decimal.ln(sigWt) / Decimal.ln(two))
    Y = sigWt**2 + two**(d+2) * sigWt + two**(2*d)
    P = Decimal(ceil(B * Decimal.ln(sigWt/weightRatio)))
    denom = 3 * B * (sigWt**2 - two**(2*d)) + (d*(T - 1) - P)*Y
    num = T * Y * Decimal.ln(weightRatio) / Decimal.ln(two)
    return num / denom
```

```
for j in range(0, 10):
    sigWt = two**(40 - j) - 1
    for i in range(0, 10):
        weightRatio = Decimal(2 - i/10)
        result = ratio(sigWt, weightRatio)
        print(f"{40-j},{2-i/10}: {result}")
```

References

[1] Flemming Topsoe. Some bounds for the logarithmic function. https://rgmia.org/papers/v7n2/pade.pdf. Online; accessed March 16 2022.