Formalizing ZkSNARKs

Ashvni Narayanan, Matej Penciak, Daniel Rogozin, Winston Zhang

August 27, 2022

Introduction

In this blueprint we formalize the knowledge soundness proof for the BabySNARK protocol.

The protocol is a toy example of a Zk SNARK protocol defined and implemented in the repository .

The outline of the proof used in this blueprint is a port of the work done by Bolton Bailey in Lean 3 found here .

We will eventually include proofs of knowledge soundness for other protocols as well, and proofs of completeness and zero knowledge.

Chapter 1

Supporting Lemmas

Definition 1.1. *Fix a finite field F. The polynomial $t \in F[X]$ is then defined as $t = \prod_{i=0}^{m-1}(X - r_i)$ for $r_i \in F$ for $0 \leq i \leq m-1$ where $m > 0$.*

Lemma 1.2. *The polynomial t is monic of positive degree $0 < m$.*

Proof. $\square$

Chapter 2

Knowledge Soundness for BabySNARK

Fix natural numbers n, l with $l < n$, and a sequence $a_s = (a_0, \ldots, a_{l-1})$ and $a_w = (a_l, \ldots, a_n)$ (the *statement* and *witness*).

Fix also a collection of polynomials $u_i(X) \in F[X]$ for $0 \leq i < n$ split up into the first l denoted u_s and the last $l - n$ denoted u_w.

Finally, fix strings $(b_0, \ldots, b_m), (h_0, \ldots, h_m), (v_0, \ldots v_m) \in F^m$ where $m = \deg t$. Similarly fix $(b'_i)_{i=l}^{n-l-1}$, $(v'_i)_{i=l}^{n-l-1}$ and $(h'_i)_{i=l}^{n-l-1} \in F^{n-l}$, and $b_\gamma, v_\gamma, h_\gamma, b_{\gamma\beta}, v_{\gamma\beta}$.

Definition 2.1. *Define the polynomials* $V_s = \sum_i^{n-1} a_i u_i(X) = V_{ss} + V_{sw}$, *and*

$$B_w = \sum_{i=0}^{m-1} b_i X^i + b_\gamma Z + b_{\gamma\beta} YZ + \sum_{i=l}^{n-1} b'_i Y u_i(X)$$

$$V_w = \sum_{i=0}^{m-1} v_i X^i + v_\gamma Z + v_{\gamma\beta} YZ + \sum_{i=l}^{n-1} v'_i Y u_i(X)$$

$$H = \sum_{i=0}^{m-1} h_i X^i + h_\gamma Z + h_{\gamma\beta} YZ + \sum_{i=l}^{n-1} h'_i Y u_i(X)$$

Definition 2.2. *Call a sequence* $(a_i)_{i=0}^{n-1}$ satisfying *if*

$$\sum_{i=0}^{l-1} a_i u_i(X) + \sum_{i=l}^{n-1} a_i u_i(X) \equiv 1 \mod t$$

Lemma 2.3. $\forall 0 \leq i < m$, *the coefficient of* X^i *in* B_w *(or* `B_wit`*) is* b_i.

Proof. □

Lemma 2.4. *The coefficient of* Z^2 *in* $Ht + 1$ *is 0.*

Lemma 2.5. *Given* $(a_i)_{i=0}^{l-1}$, *the coefficient of* Z^2 *in* $(b_{\gamma\beta} \cdot Z + \sum_{i=0}^{l-1} a_i u_i(X) + \sum_{j=l}^{n-1} b'_i u_i(X))^2$ *is* $b_{\gamma\beta}^2$.

For the following lemmas assume we are in the setting of the proof of knowledge soundness. In particular, assume:

$$B_w = YV_w \tag{2.1}$$

$$Ht = V^2 - 1 \tag{2.2}$$

Knowledge soundness for BabySNARK follows from the following lemmas:

Lemma 2.6. *Then given a monomial m not having a Y-term, the coefficient of m in B_w is 0.*

Proof. □

Lemma 2.7. $\forall 0 \leq i \leq m-1$, $b_i = 0$.

Proof. □

Lemma 2.8. $b_\gamma = 0$

Proof. □

Lemma 2.9. $B_w = b_{\gamma\beta} ZY + \sum_{i=l}^{n-1} b'_i Y u_i(X)$

Proof. □

Lemma 2.10. $V_w = b_{\gamma\beta} Z + \sum_{i=l}^{n-1} b'_i u_i(X)$

Proof. □

Lemma 2.11. $V(a_i)_{i=0}^{l} = b_{\gamma\beta} Z + \sum_{i=0}^{l-1} a_i u_i(X) + \sum_{i=l}^{n-1} b'_i u_i(X)$

Proof. □

Lemma 2.12. $b_{\gamma\beta} = 0$

Proof. □

Lemma 2.13. $V(a_i)_{i=0}^{l} = \sum_{i=0}^{l-1} a_i u_i(X) + \sum_{i=l}^{n-1} b'_i u_i(X)$

Proof. □

Lemma 2.14. $(Ht+1) \equiv (V(a_i)_{i=0}^{l})^2 (mod\ t)$

Lemma 2.15. $singlify(Ht+1)/t = singlify H$

Proof. □

Theorem 2.16. *If an adversary produces polynomials $B(X,Y,Z), V(X,Y,Z), H(X,Y,Z)$ which satisfy $B_w = YV_w$ and $Ht = V^2 - 1$, then the adversary can extract a satisfying witness.*

Proof. □