

secp256k1_bulletproof
_prove_agg

secp256k1_bulletproof
_verify_agg

derive_ipa_binding
_challenge

```
graph LR; A[secp256k1_bulletproof_prove_agg] --> C[derive_ipa_binding_challenge]; B[secp256k1_bulletproof_verify_agg] --> C;
```

The diagram illustrates a data flow where two separate inputs, 'secp256k1_bulletproof_prove_agg' and 'secp256k1_bulletproof_verify_agg', are combined to produce a single output, 'derive_ipa_binding_challenge'. The output box is shaded gray, while the input boxes are white with black borders. Blue arrows indicate the direction of the flow from the inputs to the output.