Tight State-Restoration Soundness in the Algebraic Group Model

Ashrujit Ghoshal **Stefano Tessaro**

University of Washington

CRYPTO 2021

ZK-proofs gaining adoption in practice

Often, security guarantees **weak** or **non-existent**

Reason: **Fiat-Shamir transform**

Fiat-Shamir (FS) transform [FS86]

Public coin (ZK) IP for NP relation R

{proof, argument}

$\mathrm{P}(x, w)$ $\quad$ $\mathrm{V}(x)$

$$\xrightarrow{a_1}$$
$$\xleftarrow{c_1}$$
$$\vdots$$
$$\xrightarrow{a_r}$$
$$\xleftarrow{c_r}$$
$$\xrightarrow{a_{r+1}}$$

NI(ZK) FS[IP] for R

argument

$\mathrm{P}_{\mathrm{FS}}^{H}(x, w)$ $\quad$ $\mathrm{V}_{\mathrm{FS}}^{H}(x)$

$$\xrightarrow{\pi = (a_1, a_2, \dots, a_r, a_{r+1})}$$

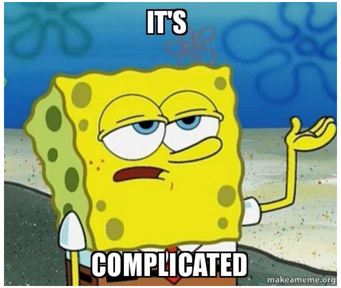
$$c_1 = H(x, a_1)$$
$$c_2 = H(x, a_1, c_1, a_2)$$
$$\vdots$$
$$c_r = H(x, a_1, c_1, a_2, c_2, \dots, a_{r-1}, c_{r-1}, a_r)$$

Common approach to build non-interactive succinct argument systems [BCCGP16, AHIV17, BBBPWM18, WTsTW18, MBKM19, BFS20, GWC20, Lee20, CHMMVW20, Setty20, SL20, LSTW20, BHRRS20, KST21, BHRRS21, …]

Usually, *only* the soundness interactive protocol analyzed

Hope: IP sound $+ \ H\ =$ random oracle $\Rightarrow \mathrm{FS[IP]}$ sound

Is that the case?



Soundness degradation

$\mathcal{P}^*(x)$ $\qquad\qquad$ $\mathrm{V}(x)$

$$\xrightarrow{a_1}$$
$$\xleftarrow{c_1}$$
$$\vdots$$
$$\xrightarrow{a_r}$$
$$\xleftarrow{c_r}$$
$$\xrightarrow{a_{r+1}}$$

snd err.$(t) = \epsilon$

$\mathcal{P}^{*\,\mathrm{RO}}_{\mathrm{FS}}(x)$ $\qquad\qquad$ $\mathrm{V}^{\mathrm{RO}}_{\mathrm{FS}}(x)$

$$\xrightarrow{\pi = (a_1, a_2, \dots, a_r, a_{r+1})}$$

$$c_1 = \mathrm{RO}(x, a_1)$$
$$c_2 = \mathrm{RO}(x, a_1, c_1, a_2)$$
$$\vdots$$
$$c_r = \mathrm{RO}(x, a_1, c_1, a_2, c_2, \dots, a_{r-1}, c_{r-1}, a_r)$$

snd err.$(t) \leq t^{r+1} \cdot \epsilon$

This is very bad

snd err.$(t) \leq t^{r+1} \cdot \epsilon$

Bulletproofs [BBBPWM18, BCCGP16]

- Implemented in Monero, Signal's MobileCoin
- More than constant rounds, hence no meaningful security guarantee

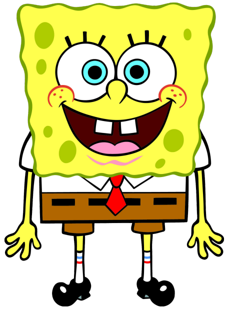
Constant-round protocols

- E.g., Sonic [MBKM19], Plonk [GWC19], Marlin [CHMMVW20]
- For 256-bit curves, $r \geq 4$, secure only for $t \leq 2^{60}$

Overly pessimistic? Expect much better security!

Our work

Security expectations



Tight State-Restoration Soundness
in the Algebraic Group Model

Ashrujit Ghoshal(✉) and Stefano Tessaro

Paul G. Allen School of Computer Science & Engineering,
University of Washington, Seattle, USA
{ashrujit,tessaro}@cs.washington.edu

Proof guarantees

General framework to prove security in the **Algebraic Group Model (AGM)** [FKL17] for

- group-based proof/argument systems
- using the Fiat-Shamir transform

with or without pairings

General framework to prove security in the **(AGM)** [FKL17] for

- group-based proof/argument systems
- using the Fiat-Shamir transform

to prove security in the **Algebraic Group Model (AGM)** [FKL17]

Tight bounds for Bulletproofs [BBBPWM18, BCCGP16], Sonic [MBKM19]

first non-trivial soundness proof for the non-interactive protocol.

Concurrent work: [BMMTV20] — non-tight bounds in the AGM for main component of Bulletproofs

Expect to apply to number of other proof systems

[Groth16,FKL17] soundness analysis in ideal models (GGM/AGM)

No Fiat-Shamir

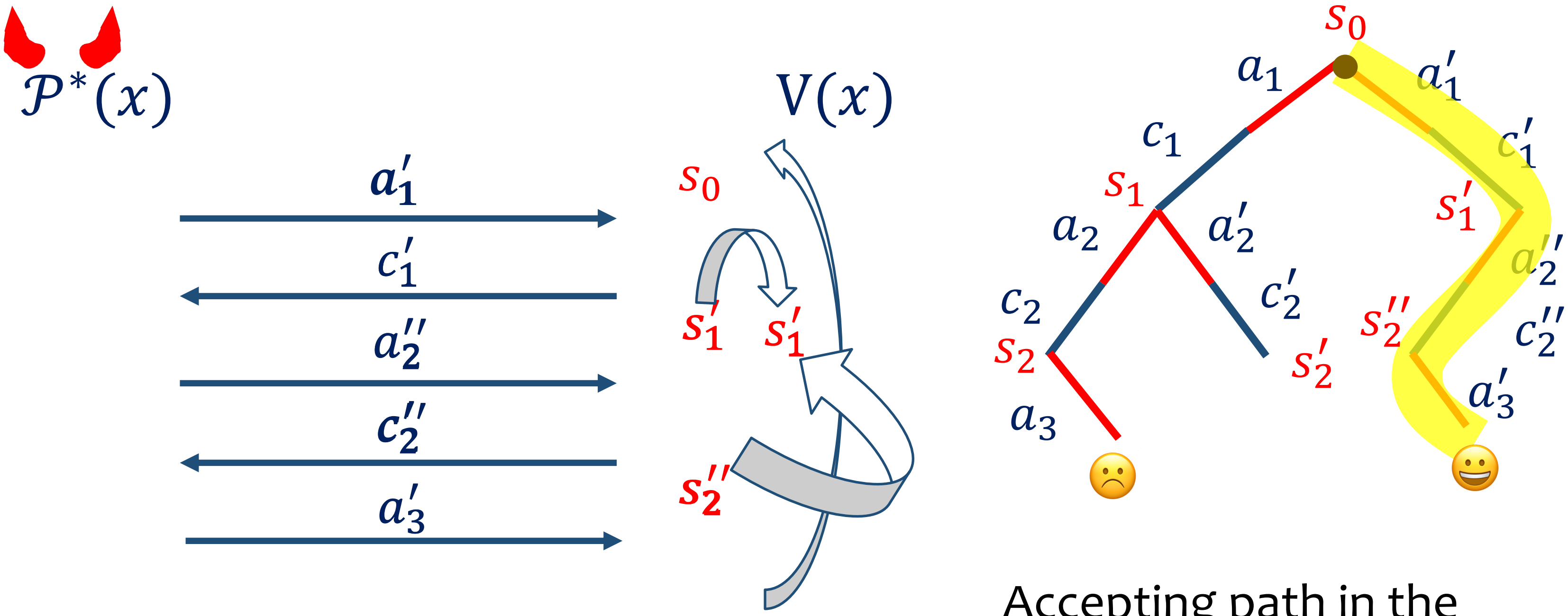
Key ingredient = state-restoration soundness

State-restoration (SR) soundness ⇒ FS soundness, tightly

Theorem. [BCS16]

$$\left(\begin{array}{c}\text{snd err.}\\ \mathrm{FS[IP]}\\ t\ \text{time}\end{array}\right) \leq \left(\begin{array}{c}\text{sr snd err.}\\ \mathrm{IP}\\ t\ \text{time}\end{array}\right) + \frac{t+1}{|\mathrm{Chal\ set}|}\,.$$

State-restoration (SR) soundness [BCS16]



Accepting path in the execution tree ⇒ $\mathcal{P}^*$ wins

$\boxed{\text{sr snd err.} = \Pr[\mathcal{P}^* \text{ wins}]}$

Bounding sr snd err. generically

r-round IP
snd err. $= \epsilon$

earlier

snd err. for $\mathrm{FS}[\mathrm{IP}] \leq t^{r+1} \cdot \epsilon$

running time of FS[IP] prover

sr snd err. $\leq t^{r+1} \cdot \epsilon$

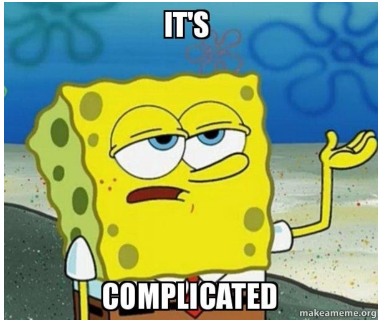
[BCS16]

running time of SR prover

snd err. for $\mathrm{FS}[\mathrm{IP}] \leq t^{r+1} \cdot \epsilon$

running time of FS[IP] prover

Can we prove better bounds for SR soundness?



For certain interactive proofs, YES! [CCHLRR18, CCHLRRW19, JKZ21, HLR21, …]

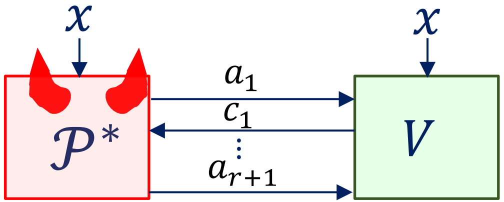
Round-by-round soundness ⇔ SR soundness [Holmgren19]

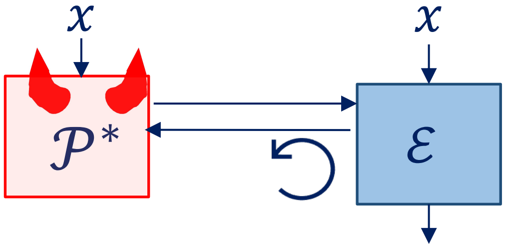
For **arguments** no non-trivial bounds for SR soundness known

Proving soundness of arguments

Witness extended emulation (wee) [Lindell03, GI08]

$\mathrm{IP} = (P, V)$ for NP relation R





$\tau = (x, a_1, c_1, \ldots, a_r, c_r, a_{r+1})$

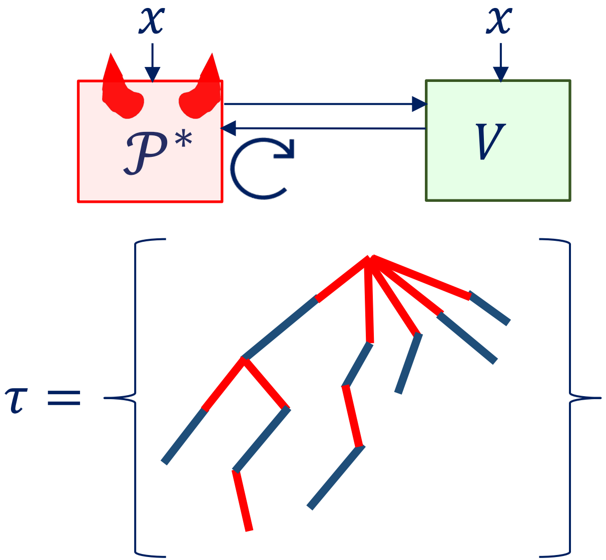
(τ', w)

Goal: τ' identically distributed as τ and $\boxed{\mathrm{Acc}(\tau') \Rightarrow (x, w) \in R}$

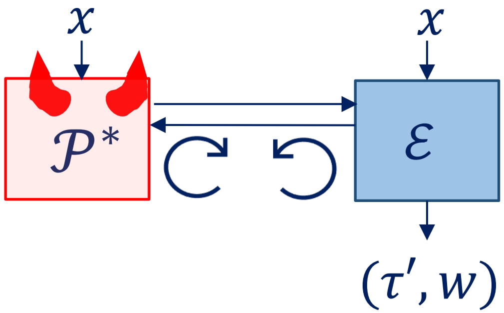
guarantee only computational for arguments

Proof via generalized forking lemma [BCCGP16, JT20, ACK21]

For state-restoration provers



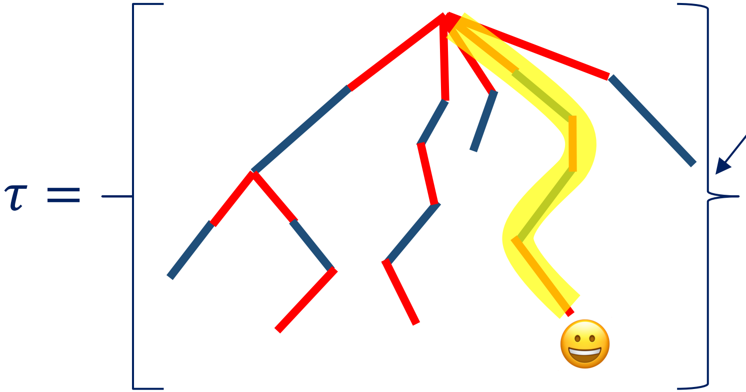
Double rewinding!



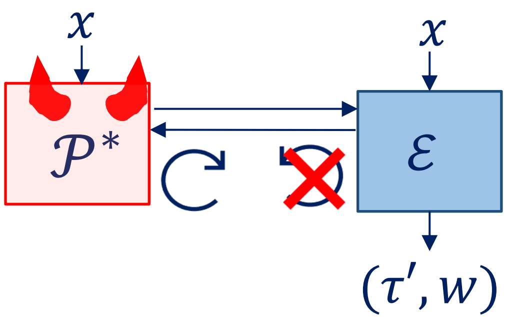
Goal: τ' identically distributed as τ and $\mathrm{Acc}(\tau') \Rightarrow (x, w) \in R$

Extraction strategy unclear ☹️

Idea: online extraction



Extract witness from accepting transcript τ, w/o rewinding



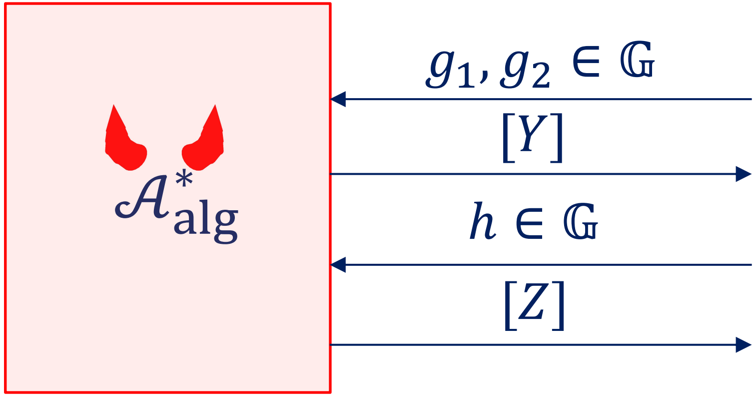
Online extraction supported by

- Knowledge assumptions
- Ideal models (e.g., AGM, GGM, ROM, …)

This paper: SRS in the AGM

Algebraic Group Model (AGM) [FKL17]

Group $\mathbb{G}$



$$[Y] = (Y, y_{g_1}, y_{g_2})$$

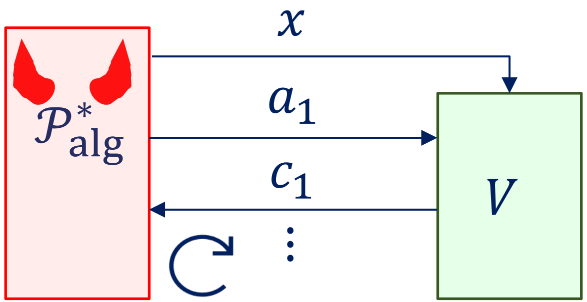
$$Y = g_1^{y_{g_1}} g_2^{y_{g_2}}$$

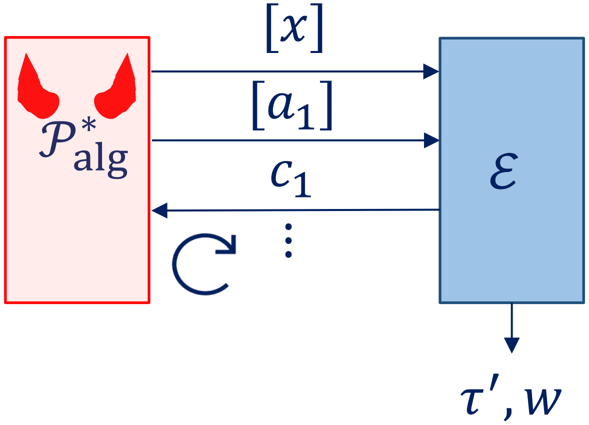
$$[Z] = (Z, z_{g_1}, z_{g_2}, z_h)$$

$$Z = g_1^{z_{g_1}} g_2^{z_{g_2}} h^{z_h}$$

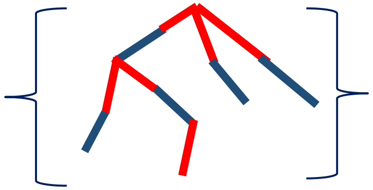
Our target = Adaptive srs-wee in the AGM

$\mathrm{IP} = (P, V)$ for NP relation R





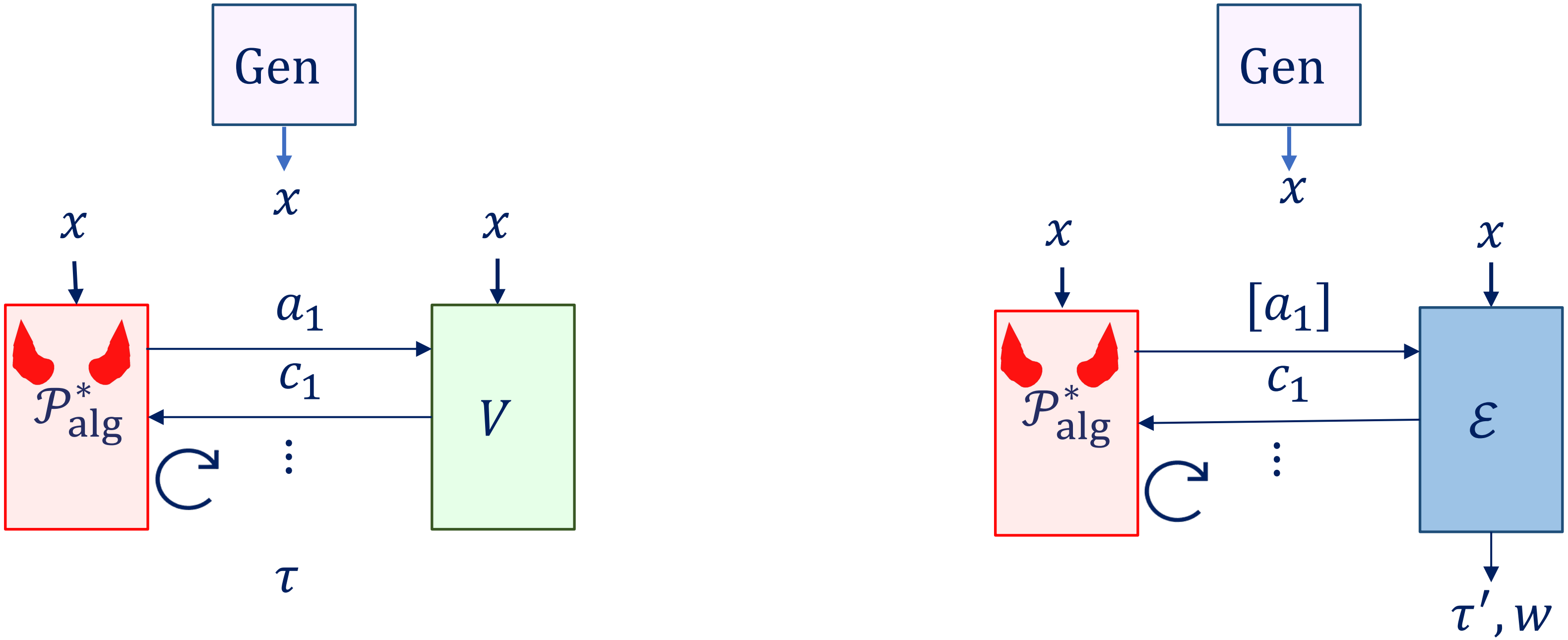
$\tau =$



$$\forall \mathcal{D} \qquad \underbrace{\Pr[\mathcal{D}(\tau) = 1]}_{= p_0} \qquad \approx \qquad \underbrace{\Pr[\mathcal{D}(\tau') = 1 \wedge (\mathrm{Acc}(\tau') \Rightarrow (x, w) \in R)]}_{= p_1}$$

$$\text{srs-wee-adv}_{\mathrm{IP}}\left(\mathcal{P}^*_{\mathrm{alg}}, \mathcal{E}\right) = \max_{\mathcal{D}} |p_1 - p_0|$$

Also in the paper: Non-adaptive srs-wee



Goal: Given IP

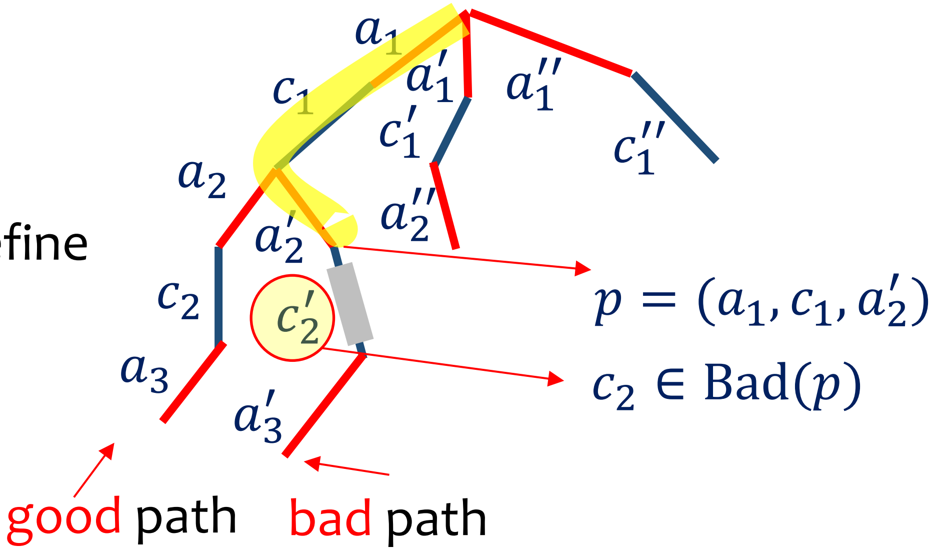
1. define $\mathcal{E}$
2. $\forall \mathcal{P}^*_{\mathrm{alg}}$ running in time t, upper bound $\text{srs-wee-adv}_{\mathrm{IP}}(\mathcal{P}^*_{\mathrm{alg}}, \mathcal{E})$

Our proof framework

Ingredient I

$\forall$ partial paths $p = (a_1, c_1, \ldots, a_i)$, define $\mathrm{Bad}(p) \subseteq$ Chal Set s.t.

$$\frac{|\mathrm{Bad}(p)|}{|\mathrm{Chal\ Set}|} \leq \epsilon$$



Ingredient II

Define (efficient) e s.t.

$$e([x], [\text{acc. path}]) \in \{\perp\} \cup \{w : (x, w) \in R\}$$

Goals:

1. $e([x], [\text{good acc. path}]) \neq \perp$
2. Minimize ϵ

Master Theorem.
Suppose Bad, e are defined for IP. $\exists \mathcal{E} = \mathcal{E}(e)$ s.t. $\forall\, \mathcal{P}^*_{\mathrm{alg}}$ running in time t

$$\text{srs-wee-adv}_{\mathrm{IP}}\left(\mathcal{P}^*_{\mathrm{alg}}, \mathcal{E}\right) \leq t \cdot \epsilon + p^{\mathrm{fail}}_{\mathrm{IP}}(e, \mathcal{P}^*_{\mathrm{alg}})$$

$\Pr[e([x], [\text{good acc. path}]) = \bot]$

For arguments, prove $p^{\mathrm{fail}}_{\mathrm{IP}}(e, \mathcal{P}^*) \leq$ probability of violating an assumption

Applications

Our results

Shown tight via matching attacks

Bulletproofs range proof (BP-RP)

AoK that $C = g^x h^r \in \mathbb{G}$ is a commitment to $x \in [0, 2^n - 1]$

Theorem. $\exists \mathcal{E}$ s.t. $\text{srs-wee-adv}_{\text{BP-RP}}(t, \mathcal{E}) \leq \text{dlog-adv}_{\mathbb{G}}(t) + O\left(\frac{tn}{|\mathbb{G}|}\right)$.

Bulletproofs AoK for arith. circuit satisfiability (BP-ACS), $n =$(#mult gates)

Theorem. $\exists \mathcal{E}$ s.t. $\text{srs-wee-adv}_{\text{BP-ACS}}(t, \mathcal{E}) \leq \text{dlog-adv}_{\mathbb{G}}(t) + O\left(\frac{tn}{|\mathbb{G}|}\right)$.

Sonic AoK for arith. circuit satisfiability, $n =$(#mult gates)

Theorem. $\exists \mathcal{E}$ s.t.

$$\text{srs-wee-adv}_{\text{Sonic}}(t, \mathcal{E}) \leq 4n\text{-dlog-adv}_{\mathbb{G}}(t) + 2 \cdot \text{dlog-adv}_{\mathbb{G}}(t) + O\left(\frac{tn}{|\mathbb{G}|}\right).$$

Prior work: Concrete security analysis of Bulletproofs-ACS

Interactive protocol

GGM

[JT20]

wee-adv $= O\left(\sqrt{\frac{t^2 n^6}{|\mathbb{G}|}}\right)$

Here

srs-wee-adv $= O\left(\frac{t^2}{|\mathbb{G}|} + \frac{tn}{|\mathbb{G}|}\right)$

$$|\mathbb{G}| = 2^{256}, n = 2^{20}$$

Secure for $t \leq 2^{78}$

Secure for $t \leq 2^{128}$

Example - analyzing Bulletproofs [BBBPWM18,BCCGP16]

Input: $(g, h \in \mathbb{G}, \mathbf{g}, \mathbf{h} \in \mathbb{G}^n, \mathbf{W}_L, \mathbf{W}_R, \mathbf{W}_O \in \mathbb{Z}_p^{Q\times n},$
$\quad \mathbf{W}_V \in \mathbb{Z}_p^{Q\times m}, \mathbf{c} \in \mathbb{Z}_p^Q; \mathbf{a}_L, \mathbf{a}_R, \mathbf{a}_O \in \mathbb{Z}_p^n, \boldsymbol{\gamma} \in \mathbb{Z}_p^m)$
$\mathcal{P}$'s input: $(g, h, \mathbf{g}, \mathbf{h}, \mathbf{W}_L, \mathbf{W}_R, \mathbf{W}_O, \mathbf{W}_V, \mathbf{c}; \mathbf{a}_L, \mathbf{a}_R, \mathbf{a}_O, \boldsymbol{\gamma})$
$\mathcal{V}$'s input: $(g, h, \mathbf{g}, \mathbf{h}, \mathbf{W}_L, \mathbf{W}_R, \mathbf{W}_O, \mathbf{W}_V, \mathbf{c})$
Output: $\{\mathcal{V}$ accepts, $\mathcal{V}$ rejects $\}$
$\mathcal{P}$ computes:
$\quad \alpha, \beta, \rho \xleftarrow{\$} \mathbb{Z}_p$
$\quad A_I = h^{\alpha}\mathbf{g}^{\mathbf{a}_L}\mathbf{h}^{\mathbf{a}_R} \in \mathbb{G}$ // *commit to* $\mathbf{a}_L, \mathbf{a}_R$
$\quad A_O = h^{\beta}\mathbf{g}^{\mathbf{a}_O} \in \mathbb{G}$ // *commitment to* $\mathbf{a}_O$
$\quad \mathbf{s}_L, \mathbf{s}_R \xleftarrow{\$} \mathbb{Z}_p^n$ // *choose blinding vectors* $\mathbf{s}_L, \mathbf{s}_R$
$\quad S = h^{\rho}\mathbf{g}^{\mathbf{s}_L}\mathbf{h}^{\mathbf{s}_R} \in \mathbb{G}$ // *commitment to* $\mathbf{s}_L, \mathbf{s}_R$
$\mathcal{P} \to \mathcal{V} : A_I, A_O, S$
$\mathcal{V} : y, z \xleftarrow{\$} \mathbb{Z}_p^{\star}$
$\mathcal{V} \to \mathcal{P} : y, z$
$\mathcal{P}$ and $\mathcal{V}$ compute:
$\quad \mathbf{y}^n = (1, y, y^2, \ldots, y^{n-1}) \in \mathbb{Z}_p^n$ // *challenge per witness*
$\quad \mathbf{z}_{[1:]}^{Q+1} = (z, z^2, \ldots, z^Q) \in \mathbb{Z}_p^Q$ // *challenge per constraint*
$\quad \delta(y, z) = \langle \mathbf{y}^{-n} \circ (\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_R), \mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_L \rangle$ // *independent of the witness*
$\mathcal{P}$ computes:
$\quad l(X) = \mathbf{a}_L \cdot X + \mathbf{a}_O \cdot X^2 + \mathbf{y}^{-n} \circ (\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_R) \cdot X$
$\quad + \mathbf{s}_L \cdot X^3 \in \mathbb{Z}_p^n[X]$
$\quad r(X) = \mathbf{y}^n \circ \mathbf{a}_R \cdot X - \mathbf{y}^n + \mathbf{z}_{[1:]}^{Q+1} \cdot (\mathbf{W}_L \cdot X + \mathbf{W}_O)$
$\quad + \mathbf{y}^n \circ \mathbf{s}_R \cdot X^3 \in \mathbb{Z}_p^n[X]$
$\quad t(X) = \langle l(X), r(X) \rangle = \sum_{i=1}^{6} t_i \cdot X^i \in \mathbb{Z}_p[X]$
$\quad \mathbf{w} = \mathbf{W}_L \cdot \mathbf{a}_L + \mathbf{W}_R \cdot \mathbf{a}_R + \mathbf{W}_O \cdot \mathbf{a}_O$
$\quad t_2 = \langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle - \langle \mathbf{a}_O, \mathbf{y}^n \rangle + \langle \mathbf{z}_{[1:]}^{Q+1}, \mathbf{w} \rangle + \delta(y, z) \in \mathbb{Z}_p$ // $t_2 = d(y, z) + \langle \mathbf{z}_{[1:]}^{Q+1}, \mathbf{c} + \mathbf{W}_V \cdot \mathbf{v} \rangle$
$\quad \tau_i \xleftarrow{\$} \mathbb{Z}_p \quad \forall i \in [1, 3, 4, 5, 6]$
$\quad T_i = g^{t_i} h^{\tau_i} \quad \forall i \in [1, 3, 4, 5, 6]$
$\mathcal{P} \to \mathcal{V} : T_1, T_3, T_4, T_5, T_6$ // *commitments to* t_1, t_3, t_4, t_5, t_6

Protocol 3: Part 1: Computing commitments to $l(X), r(X)$ and $t(X)$

$\mathcal{V} : x \xleftarrow{\$} \mathbb{Z}_p^{\star}$ // *Random challenge* (74)
$\mathcal{V} \to \mathcal{P} : x$ (75)
$\mathcal{P}$ computes: (76)
$\quad \mathbf{l} = l(x) \in \mathbb{Z}_p^n$ (77)
$\quad \mathbf{r} = r(x) \in \mathbb{Z}_p^n$ (78)
$\quad \hat{t} = \langle \mathbf{l}, \mathbf{r} \rangle \in \mathbb{Z}_p$ (79)
$\quad \tau_x = \sum_{i=1, i\neq 2}^{6} \tau_i \cdot x^i + x^2 \cdot \langle \mathbf{z}_{[1:]}^{Q+1}, \mathbf{W}_V \cdot \boldsymbol{\gamma} \rangle \in \mathbb{Z}_p$ // *blinding value for* $\hat{t}$ (80)
$\quad \mu = \alpha \cdot x + \beta \cdot x^2 + \rho \cdot x^3 \in \mathbb{Z}_p$ // *Blinding value for* P (81)
$\mathcal{P} \to \mathcal{V} : \tau_x, \mu, \hat{t}, \mathbf{l}, \mathbf{r}$ (82)
$\mathcal{V}$ computes and checks: (83)
$\quad h'_i = h_i^{y^{-i+1}} \quad \forall i \in [1, n]$ // $\mathbf{h}' = (h_1, h_2^{y^{-1}}, \ldots, h_n^{y^{-n+1}})$ (84)
$\quad W_L = \mathbf{h}'^{\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_L}$ // *Weights for* $\mathbf{a}_L$ (85)
$\quad W_R = \mathbf{g}^{\mathbf{y}^{-n} \circ (\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_R)}$ // *Weights for* $\mathbf{a}_R$ (86)
$\quad W_O = \mathbf{h}'^{\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_O}$ // *Weights for* $\mathbf{a}_O$ (87)
$\quad \hat{t} \stackrel{?}{=} \langle \mathbf{l}, \mathbf{r} \rangle$ // *Check that* $\hat{t}$ *is correct* (88)
$\quad g^{\hat{t}} h^{\tau_x} \stackrel{?}{=} g^{x^2 \cdot (\delta(y,z) + \langle \mathbf{z}_{[1:]}^{Q+1}, \mathbf{c} \rangle)} \cdot \mathbf{V}^{x^2 \cdot (\mathbf{z}_{[1:]}^{Q+1} \cdot \mathbf{W}_V)} \cdot T_1^x$ (89)
$\quad \cdot \prod_{i=3}^{6} T_i^{(x^i)}$ // $\hat{t} = t(x) = \sum_{i=1}^{6} t_i \cdot x^i$ (90)
$\quad P = A_I^x \cdot A_O^{(x^2)} \cdot \mathbf{h}'^{-\mathbf{y}^n} \cdot W_L^x \cdot W_R^x \cdot W_O \cdot S^{(x^3)}$ // *commitment to* $l(x), r(x)$ (91)
$\quad P \stackrel{?}{=} h^{\mu} \cdot \mathbf{g}^{\mathbf{l}} \cdot \mathbf{h}'^{\mathbf{r}}$ // *Check that* $\mathbf{l} = l(x)$ *and* $\mathbf{r} = r(x)$ (92)
if all checks succeed: $\mathcal{V}$ accepts (93)
else: $\mathcal{V}$ rejects (94)

Protocol 3: Part 2: Polynomial identity check for $\langle l(x), r(x) \rangle = t(x)$

Main ingredient: Inner product argument

$x = (Q, \hat{t}) \in \mathbb{G} \times \mathbb{Z}_p$

$w = (\vec{\boldsymbol{l}}, \vec{\boldsymbol{r}}) \in \mathbb{Z}_p^n \times \mathbb{Z}_p^n$

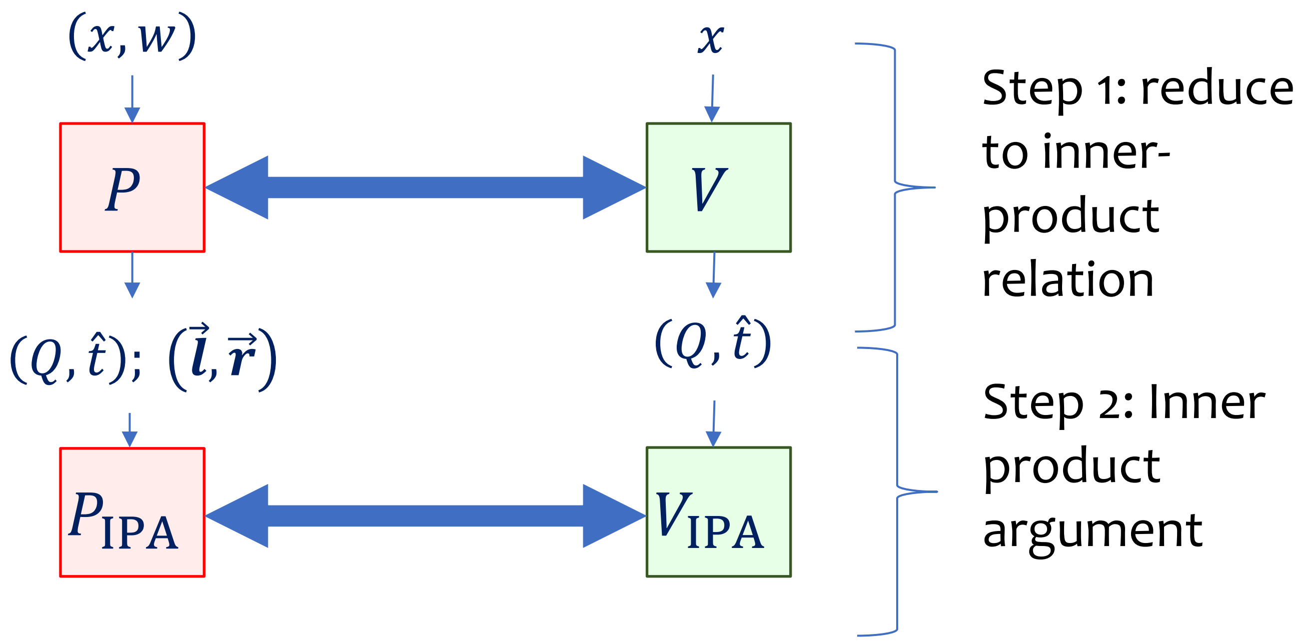
$x = (Q, \hat{t})$

$g_1, \ldots, g_n, h_1, \ldots, h_n =$ generators of $\mathbb{G}$

AoK: Accept iff prover knows $w = (\vec{\boldsymbol{l}}, \vec{\boldsymbol{r}})$ s.t.

1. $Q = g_1^{l_1} \cdots g_n^{l_n} h_1^{r_1} \cdots h_n^{r_n}$
2. $\hat{t} = \langle \vec{\boldsymbol{l}}, \vec{\boldsymbol{r}} \rangle$

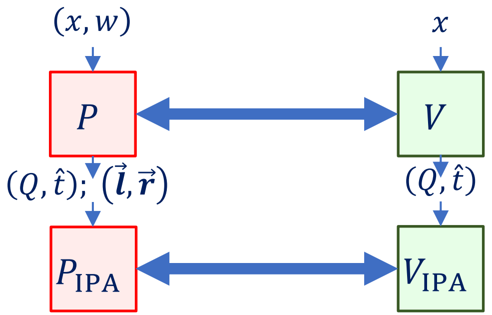
Bulletproofs template for NP relation $\boldsymbol{R}$



$(x, w) \in R$ iff $Q = g_1^{l_1} \cdots g_n^{l_n} h_1^{r_1} \cdots h_n^{r_n}$ and $\hat{t} = \langle \vec{\boldsymbol{l}}, \vec{\boldsymbol{r}} \rangle$ [whp]

Important points in analyzing Bulletproofs

Point 1: Lack of composition in the AGM



Different representations of group elements compared to IPA in isolation

Point 2: Different extraction strategies

Range proof
Extract from input representation

AoK for arith. circuit satisfiability
Extract from first message

Extracting from input representation: Bulletproofs range proof

Range proof: AoK that $C = g^x h^r \in \mathbb{G}$ is a commitment to $x \in [0, 2^n - 1]$

Instance $= C,$ generators $= (g, h)$

adaptive $\mathcal{P}^*_{\mathrm{alg}}$ outputs $[C] = (C, x, r)$ s.t. $C = g^x h^r$

e: return (x, r)

No! Not guaranteed that $x \in [0, 2^n - 1]$

Technical core

$\mathcal{P}^*_{\mathrm{alg}}$ produces good $\mathrm{acc.\ path}$ but
$x \notin [0, 2^n - 1]$
$\Rightarrow$ break DLOG

Conclusions

Invitation to **analyze SR soundness** of interactive protocols

Open problems

- Prove SR soundness for more protocols
- SR soundness in the standard model
- Extend our framework to enable modular analysis in the AGM

Paper: https://eprint.iacr.org/2020/1351