Sumcheck Arguments and their Applications

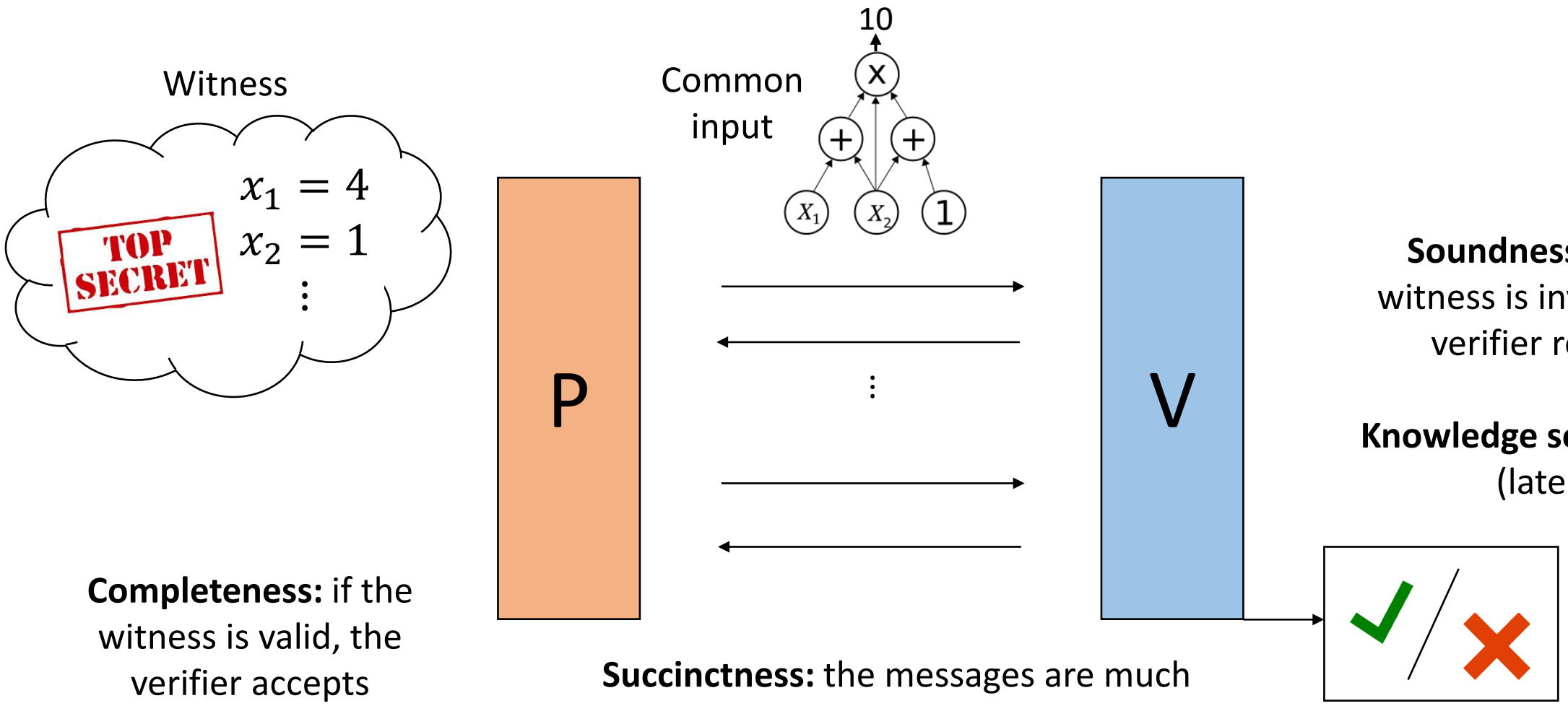
Jonathan Bootle (IBM Research – Zurich)

Alessandro Chiesa (UC Berkeley)

Katerina Sotiraki (UC Berkeley)

https://ia.cr/2021/333

Succinct arguments



Soundness: if the witness is invalid, the verifier rejects

Knowledge soundness: (later)

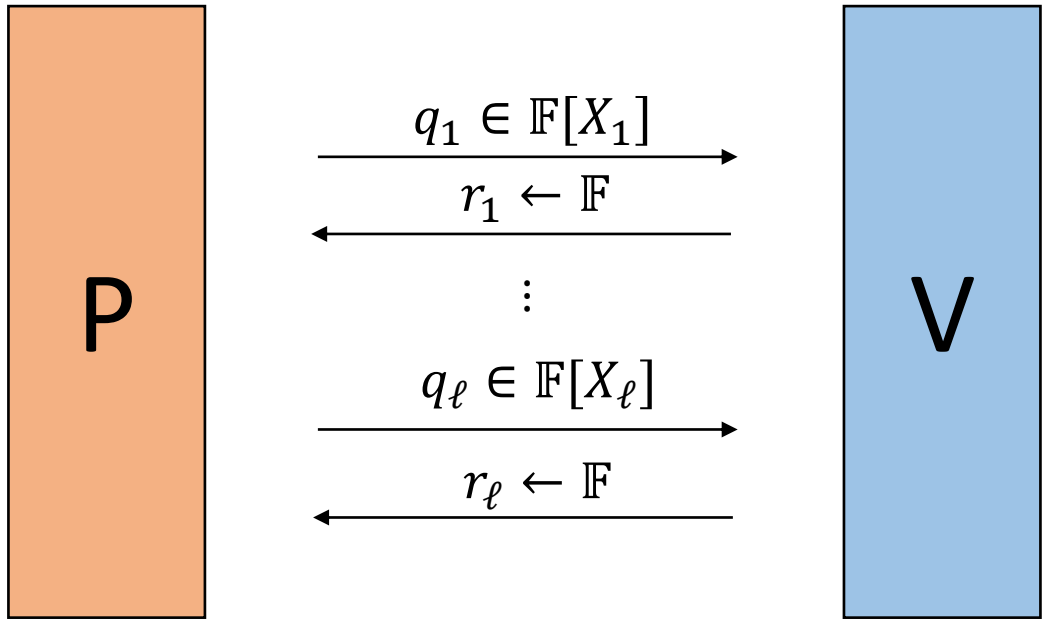
Completeness: if the witness is valid, the verifier accepts

Succinctness: the messages are much smaller than the witness

The sumcheck protocol [LFKN92]

Given a polynomial $p(X_1, \ldots, X_\ell)$ over a field $\mathbb{F}$ and a value $u \in \mathbb{F}$,
prove that $\sum_{\underline{\omega} \in H^\ell} p(\omega_1, \ldots, \omega_\ell) = u$

Computes polynomials
$q_i(X_i) = \sum_{\underline{\omega} \in H^{\ell-i}} p(r_1, .., r_{i-1}, X_i, \omega_{i+1}, .., \omega_\ell)$



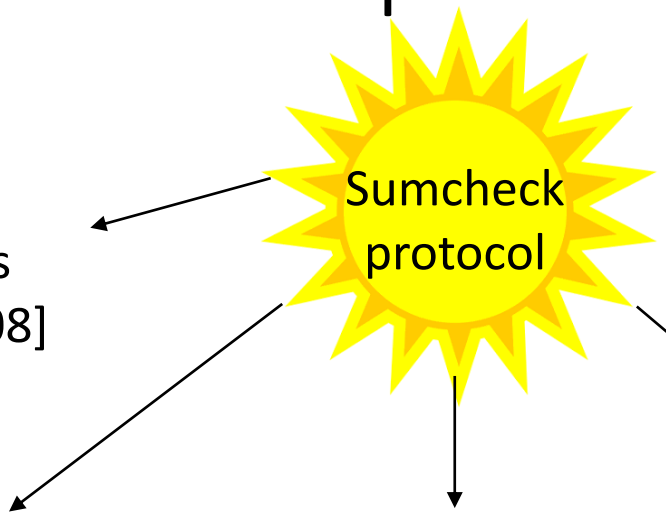
Checks that
$\sum_{\omega_1 \in H} q_1(\omega_1) = u$
$\sum_{\omega_2 \in H} q_2(\omega_2) = q_1(r_1)$
$\vdots$
$\sum_{\omega_\ell \in H} q_\ell(\omega_\ell) = q_{\ell-1}(r_{\ell-1})$

Evaluates p to check that
$p(r_1, \ldots, r_\ell) = q_\ell(r_\ell)$

Communication
$\ell \cdot \deg(p)$ elements of $\mathbb{F}$

Soundness: If $\sum_{\underline{\omega} \in H^\ell} p(\omega_1, \ldots, \omega_\ell) \neq u$ then V accepts with probability at most $\frac{\ell \cdot \deg(p)}{|\mathbb{F}|}$.

The sumcheck protocol is everywhere!



Probabilistic proofs
[BFL91,BFLS91,GKR08]

Sumcheck-based succinct arguments
[Thaler13]

[CMT13], [VSBW13], [W+17], [ZGKPP17], [WTSTW18], [XZZPS19], [Set20]

Univariate-sumcheck-based arguments
[BCRSVS19]

[BCGGRS19], [ZXZS20], [CHMVW20], [COS20], [CFQR20], [BFHVXZ20]

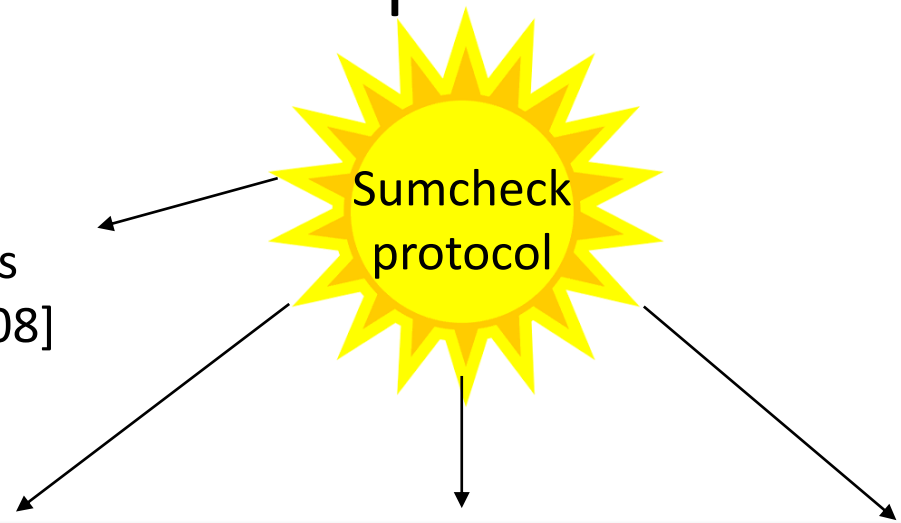
Sumchecks for tensor codes
[Meir13]

[RR20], [BCG20], [BCL20]

Useful properties:

- Linear-time prover [Thaler13,ZXZS20]
- Small space [CMT13] (can be implemented with streaming access)
- Strong soundness properties [CCHLRR18] (can make non-interactive without random oracles)

The sumcheck protocol is everywhere!



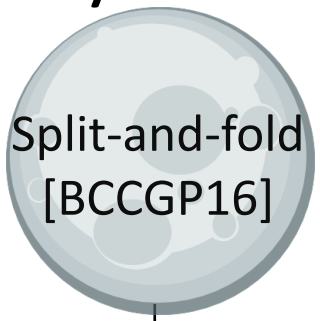
Probabilistic proofs [BFL91,BFLS91,GKR08]

https://zkproof.org/2020/03/16/sum-checkprotocol/

Useful properties:

- Linear-time prover [Thaler13,ZXZS20]
- Small space [CMT13] (can be implemented with streaming access)
- Strong soundness properties [CCHLRR18] (can make non-interactive without random oracles)

Split-and-fold techniques: a separate body of work?



Discrete-log arguments
[BBBPWM18], [PLS19], [HKR19], [BHRRS20]

Pairing-group arguments

[LMR19], [ZGKPP17], [XZZPS19]

Unknown-order-group arguments

[BFS20], [BHRRS21]

Lattice arguments

[BLNS20], [ACK21], [LA20]

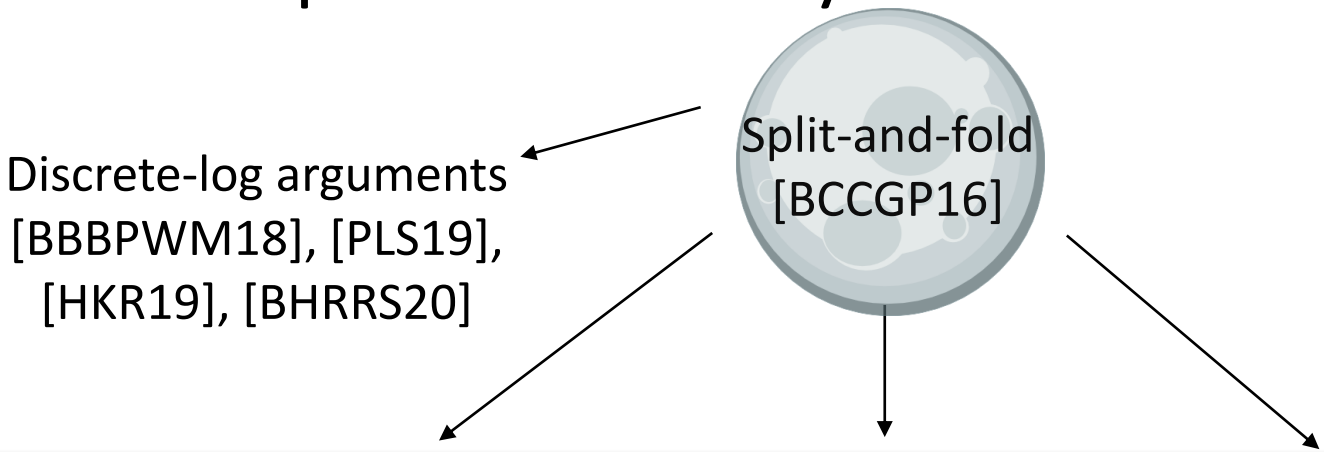
Some unifying abstractions: [BMMTV19,AC20,BDFG21]

Useful properties:

- Linear-time prover

- Streaming prover [BHRRS20], [BHRRS21] (can be implemented in small space)

Split-and-fold techniques: a separate body of work?



[BBBPWM18] implemented in Rust, Haskell, Javascript, and deployed by Blockstream, and in Monero, Mimblewimble and more…

Aim, Fire: Bulletproofs Is a Crypto Privacy Breakthrough

https://www.coindesk.com/aim-fire-bulletproofs-breakthrough-privacy-blockchains

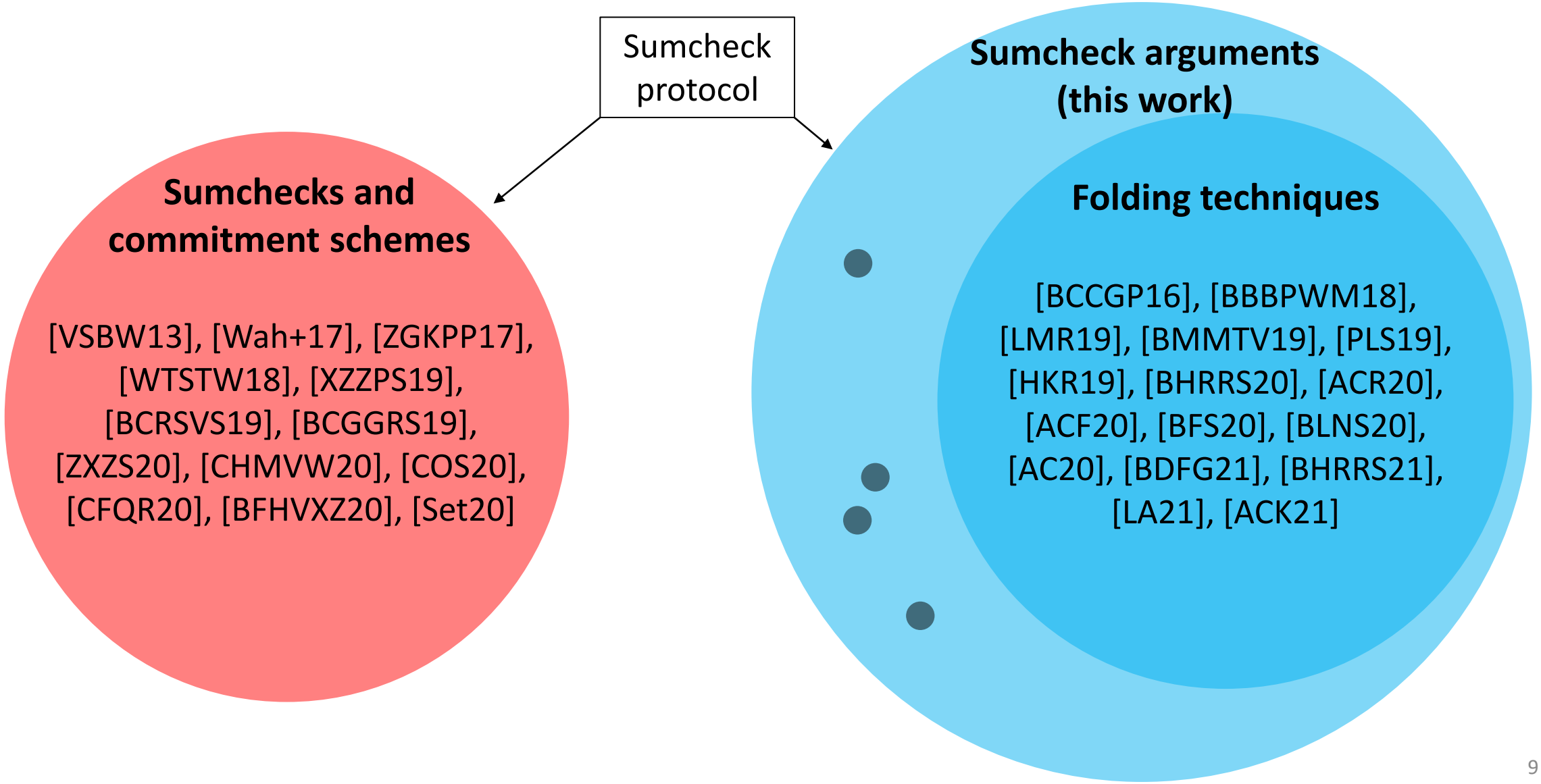
Some unifying abstractions: [BMMTV19,AC20,BDFG21]

Useful properties:

- Linear-time prover
- Streaming prover [BHRRS20], [BHRRS21] (can be implemented in small space)

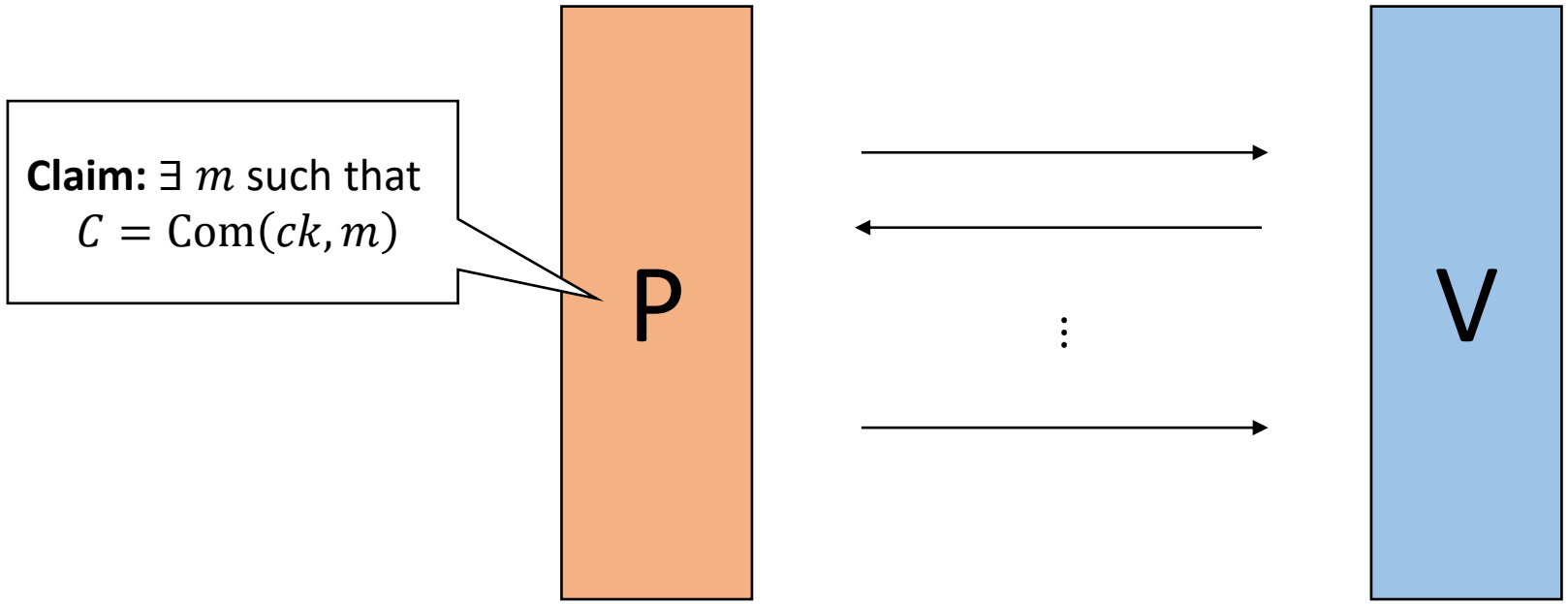
Results

…to a unified perspective



General goal:
succinct arguments for commitment openings

Common input:
- commitment C
- commitment key ck

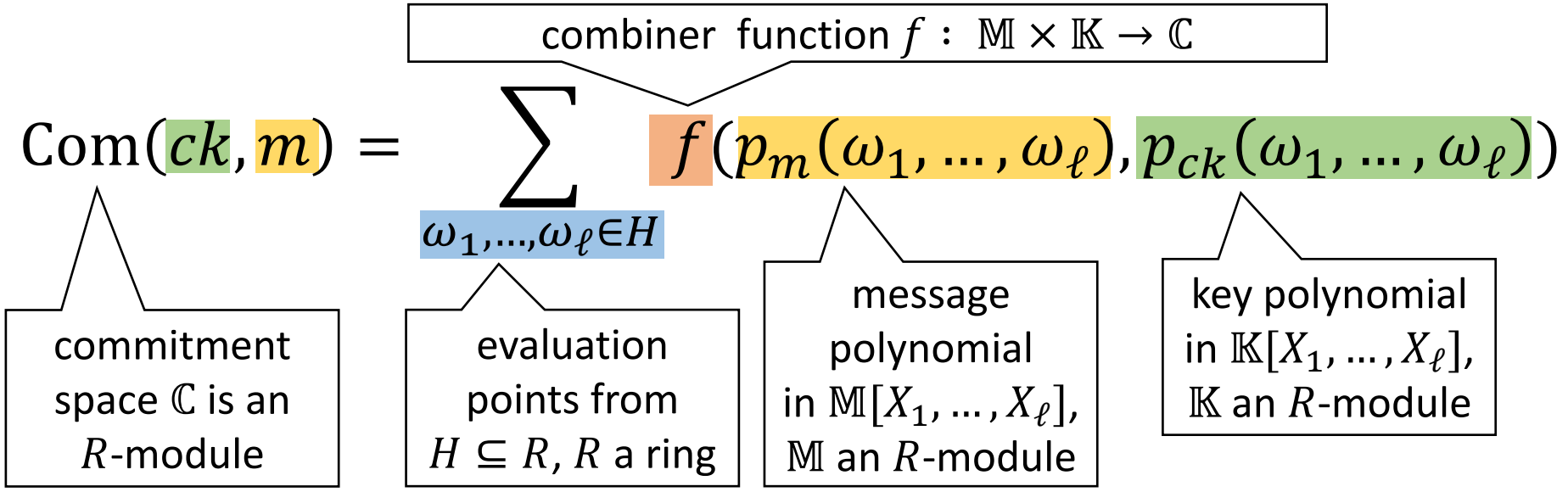


Succinctness goal:
communication $\ll |m|$

Focus: commitments with special structure

A new notion : sumcheck-friendly commitments

Definition: A commitment scheme CM is sumcheck friendly if



Example: Pedersen commitments $C = a_1 \cdot g_1 + \cdots + a_n \cdot g_n$

$H = \{-1,1\}$
$R = \mathbb{F}_p$

$\mathbb{M} = \mathbb{F}_p, \quad p_m(X_1, \dots, X_\ell) = \sum a_{i_1,\dots,i_\ell} X_1^{i_1} \dots X_\ell^{i_\ell}$

$\mathbb{K} = \mathbb{G}, \quad p_{ck}(X_1, \dots, X_\ell) = \sum g_{i_1,\dots,i_\ell} X_1^{i_1} \dots X_\ell^{i_\ell}$

$\mathbb{C} = \mathbb{G}$
$f : (a, g) \to a \cdot g$

Main result: sumcheck arguments

Theorem 1:

Let CM be a commitment scheme which is **sumcheck-friendly** and **invertible**. Given a commitment key ck and a commitment C, the sumcheck protocol applied to

$$p(X_1, \ldots, X_\ell) = f\big(p_m(X_1, \ldots, X_\ell), p_{ck}(X_1, \ldots, X_\ell)\big) \in \mathbb{C}[X_1, \ldots, X_\ell]$$

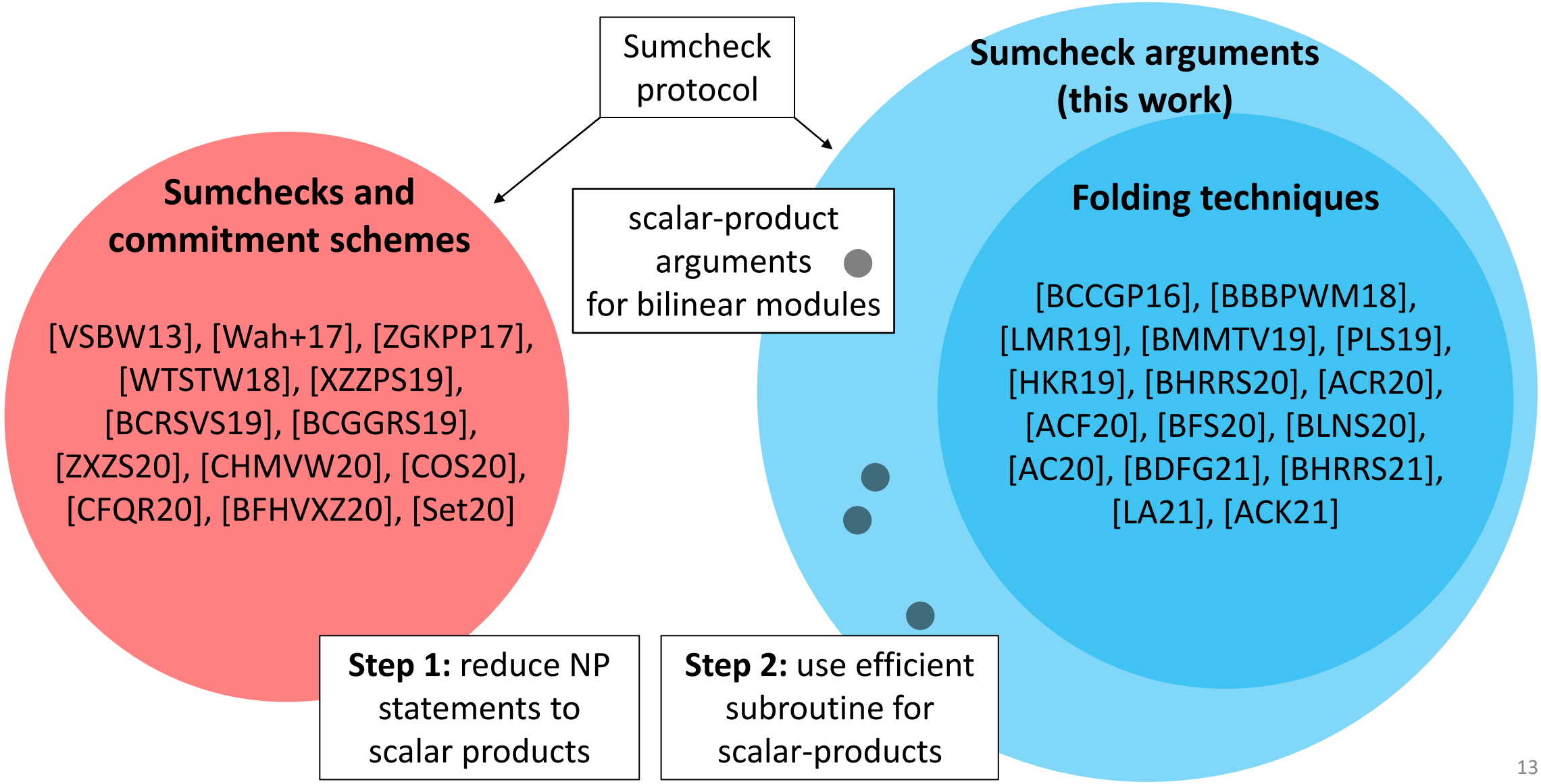
Sumcheck works over rings and modules

(with one extra verifier check) is a succinct argument of knowledge for the claim $\exists m$ such that $C = \mathrm{Com}(ck, m)$, with

- completeness
- soundness
- communication $\ell \cdot \deg(p)$

Think $O(\log |m|)$

Application: succinct arguments for NP



Application to R1CS over rings

R1CS problem over a ring $\boldsymbol{R}$: given matrices $A, B, C \in R^{n \times n}$, does there exist $z \in R^n$ satisfying $Az \circ Bz = Cz$?

Bilinear module: a triple of modules (M_L, M_R, M_T) over the same ring with a bilinear map $e : M_L \times M_R \to M_T$.

Has enough structure for Pedersen and Schnorr

Theorem 2: Let (M_L, M_R, M_T, e) be a "secure" bilinear module where M_L is a ring. Let $I \subseteq M_L$ be a suitable ideal. There is a ZK succinct argument of knowledge for R1CS with

R1CS Ring	Prover time	Verifier time	Proof size
M_L/I	$O(n)$ ops in M_L, M_R, M_T	$O(n)$ ops in M_L, M_R, M_T	$O(\log n)$ elems of M_T

Lattice-based succinct arguments for R1CS

Corollary: Let d be a power of 2, $p \ll q$ primes, $R_p := \mathbb{Z}_p[X]/\langle X^d + 1\rangle$ and similarly for R_q. Then assuming SIS is hard over R_q, there is a zero-knowledge succinct argument of knowledge for R1CS with

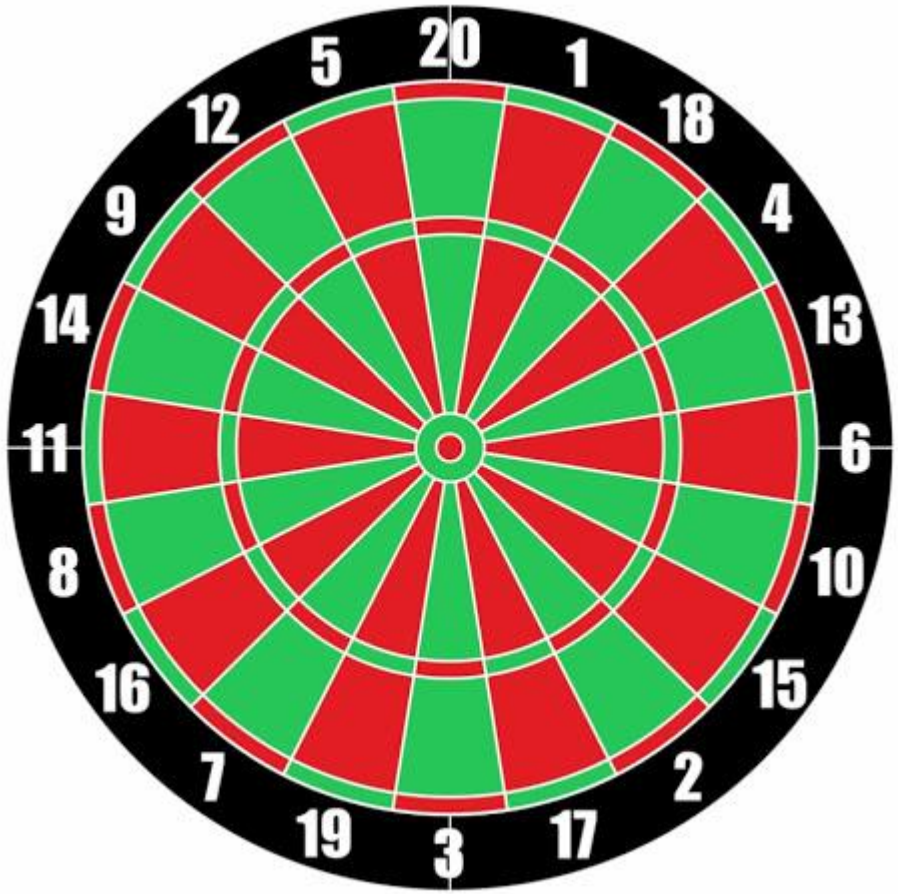
R1CS Ring	Prover time	Verifier time	Proof size
R_p	$O(n)$ ops in R_p, R_q	$O(n)$ ops in R_p, R_q	$O(\log n)$ elems of R_q

Concurrent work:

- [LA21] gives impossibility results and improvements for lattice POKs
- [ACK21] gives lattice-based succinct arguments for NP

Open questions

- Analyse the post-quantum security of sumcheck arguments
- Investigate new lattice instantiations [LA21] and concrete performance improvements
- Give instantiations of [BFS20,Lee21,BHHRS21] in our framework (or a generalization)



Techniques

Sumcheck arguments for commitment schemes

Today:

Many more details and results in the paper!

Pedersen commitments

Scalar-product commitments

Sumcheck-friendly commitments

Generalised sumcheck-friendly commitments

Groups

Rings and modules

Sumcheck argument for Pedersen

Common input:
- commitment $C \in \mathbb{G}$
- key $\underline{G} \in \mathbb{G}^n$

Claim: $\exists \underline{a} \in \mathbb{F}^n$ s.t. $C = \langle \underline{a}, \underline{G} \rangle$

"split-and-fold technique" [BCCGT16] is equivalent! (See App. A in the paper)

Opening:
$\underline{a} \in \mathbb{F}^n$

P

$\underline{a}$

$\underline{r}$

sumcheck protocol for

$$\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}}(\underline{\omega}) = n\,C$$

$\underline{r} \leftarrow \mathbb{F}^{\log(n)}$

$q_1, \ldots, q_{\log(n)}$

$p_{\underline{a}}(\underline{r})$

$q_1(1) + q_1(-1) = nC?$

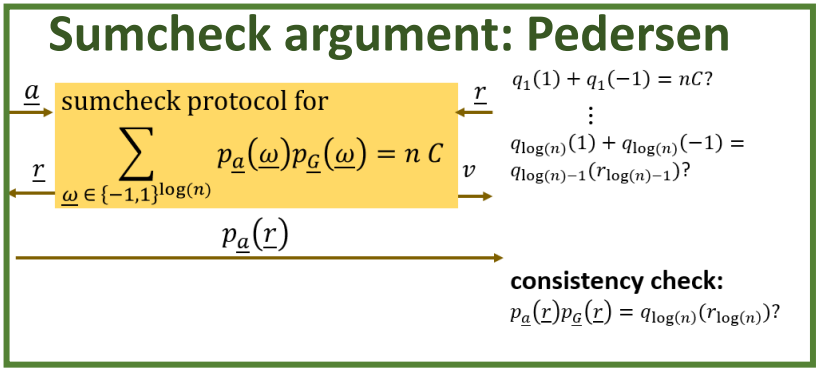
$\vdots$

$q_{\log(n)}(1) + q_{\log(n)}(-1) = q_{\log(n)-1}(r_{\log(n)-1})?$

V

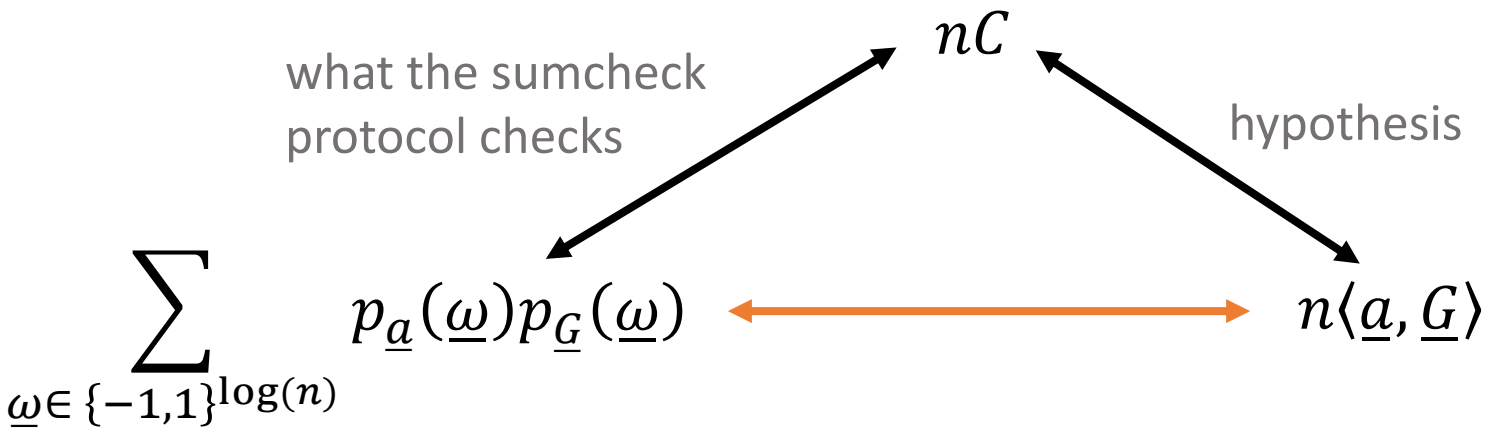
Consistency check:
$p_{\underline{a}}(\underline{r}) p_{\underline{G}}(\underline{r}) = q_{\log(n)}(r_{\log(n)})?$

Communication: $3\log(n)\ \mathbb{G} + (\log(n) + 1)\ \mathbb{F}$
Verifier computation: $O(n)\ \mathbb{G}$



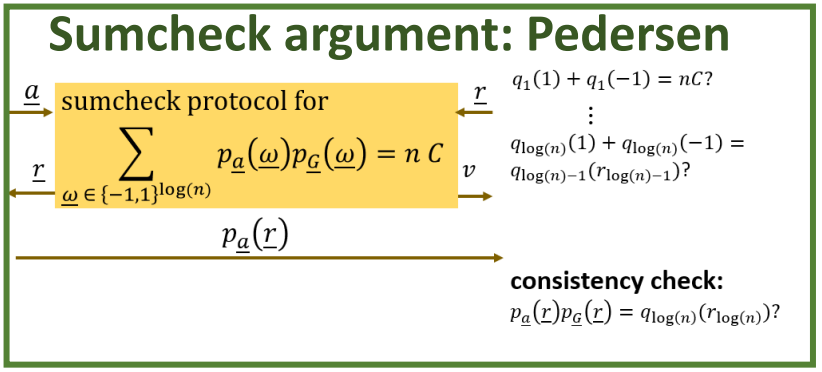
Completeness (part 1)

Lemma: If $\langle \underline{a}, \underline{G} \rangle = C$, then the verifier accepts with probability 1.



It suffices to show the following claim.

Claim: $\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}}(\underline{\omega}) = n\langle \underline{a}, \underline{G} \rangle$ (recall $p_{\underline{r}}(\underline{X}) = \sum_{i=1}^{n} r_{\underline{i}} X_1^{i_1} \cdots X_{\log(n)}^{i_{\log(n)}}$)



Completeness (part 2)

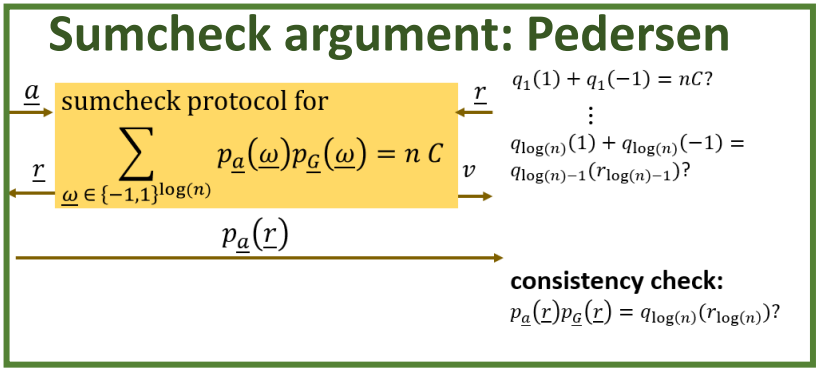
Claim: $\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}}(\underline{\omega}) = n\langle \underline{a}, \underline{G} \rangle$ (recall $p_{\underline{r}}(\underline{X}) = \sum_{i=1}^{n} r_{\underline{i}} X_1^{i_1} \cdots X_{\log(n)}^{i_{\log(n)}}$)

$\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}}(\underline{\omega})$ cancels monomials of odd degree in any variable, e.g., $X_1 X_2^2 X_3^2$

Hence, $\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}}(\underline{\omega})$ receives contributions from monomials $X_1^{2i_1} \cdots X_{\log(n)}^{2i_{\log(n)}}$

$i_1, \ldots, i_{\log(n)} \in \{0,1\}$

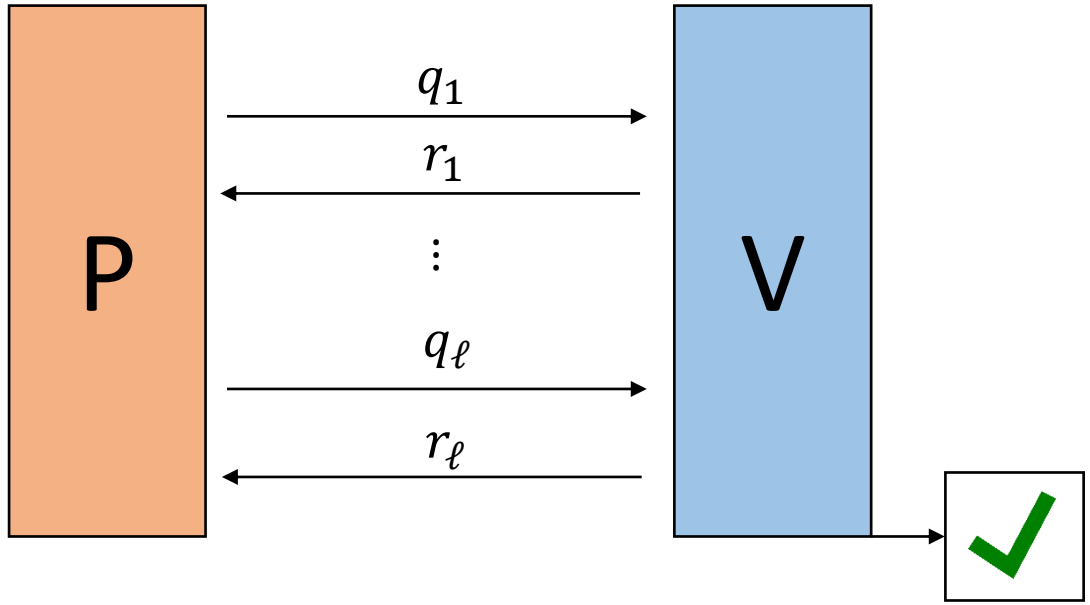
Monomials of the form $X_1^{2i_1} \cdots X_{\log(n)}^{2i_{\log(n)}}$ arise from $\underbrace{a_{\underline{i}} X_1^{i_1} \cdots X_{\log(n)}^{i_{\log(n)}}}_{p_{\underline{a}}(\underline{X})} \cdot \underbrace{G_{\underline{i}} X_1^{i_1} \cdots X_{\log(n)}^{i_{\log(n)}}}_{p_{\underline{G}}(\underline{X})}$

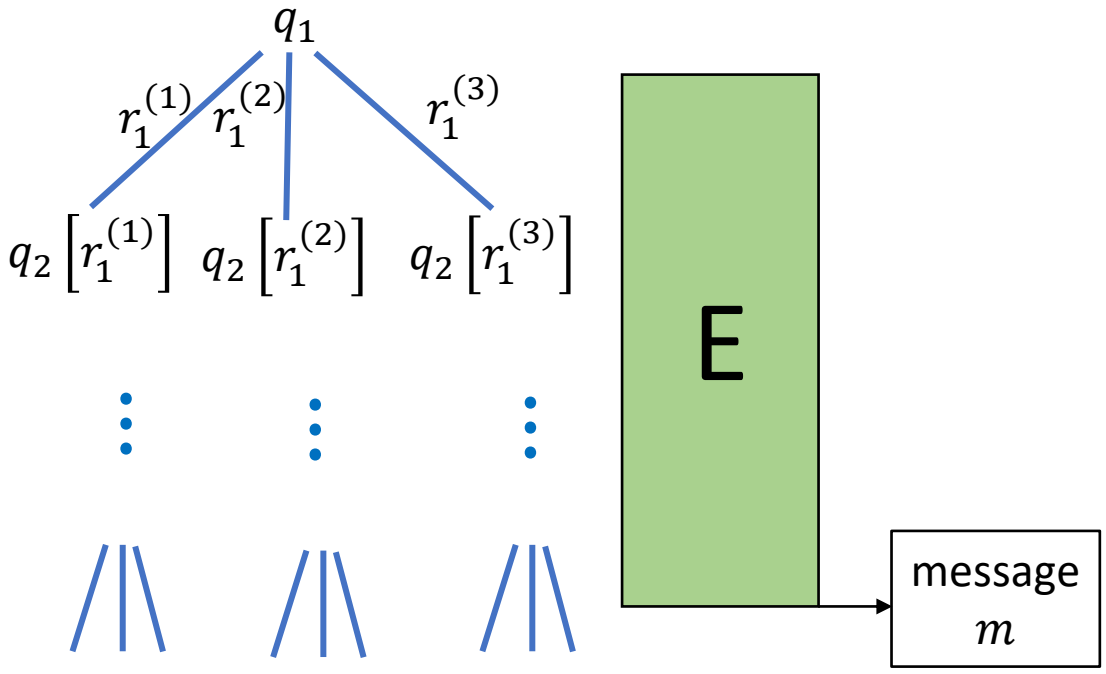


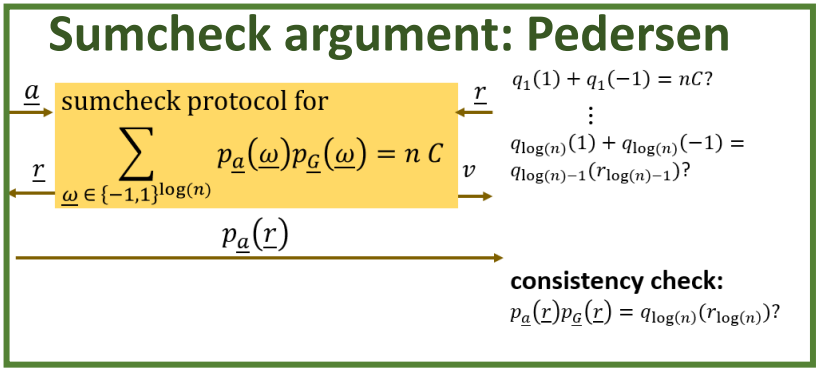
Soundness (part 1)

What kind of soundness? **Knowledge soundness**

There exists an extractor that given a suitable tree of *accepting transcripts* for a commitment key ck and commitment C, finds an opening m such that $C = \mathrm{Com}(ck, m)$.







Soundness (part 2)

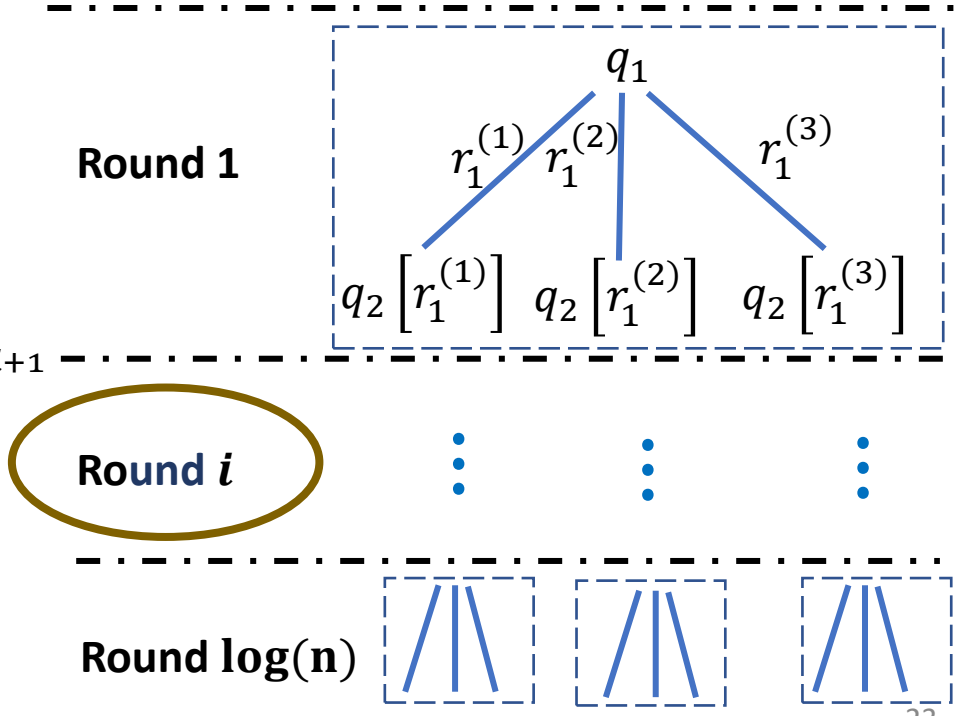
Lemma: There exists an extractor that, given a 3-ary *tree of accepting transcripts* for key $\underline{G}$ and commitment C, finds an opening $\underline{a}$ such that $C = \langle \underline{a}, \underline{G} \rangle$.

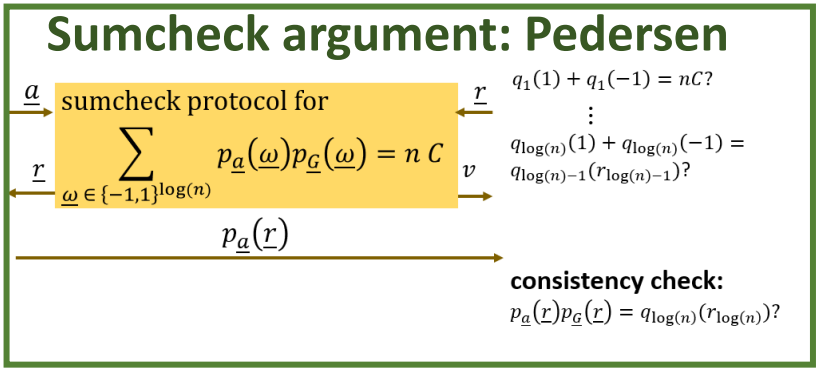
1 opening of size $\mathbf{2^{\log(n)} = n}$ for nC with key $\underline{G} \in \mathbb{G}^n$

$\mathbf{3^{i-1}}$ openings of size $\mathbf{2^{\log(n)-i+1}}$ for $q_{i-1}(r_{i-1})$ with key $\underline{G}_{i-1} \in \mathbb{G}^{2^{\log(n)-i+1}}$ where $\underline{G}_{i-1}$ is the vector of coefficients of $p_{\underline{G}}(r_1, \dots, r_{i-1}, \underline{X})$.

$\mathbf{3^{\log(n)-1}}$ openings of size **2** for $q_{\ell-1}(r_{\ell-1})$ with key $\underline{G}_{\ell-1} \in \mathbb{G}^2$

$\mathbf{3^{\log(n)}}$ openings of size **1** for $q_\ell(r_\ell)$ with key $p_{\underline{G}}(\underline{r}) \in \mathbb{G}$





Soundness (part 3)

Claim: If $\underline{\pi}^{(j)} \in \mathbb{F}^{2^{\ell-i}}$ is opening for $q_i(r_i^{(j)})$ for $j \in [3]$, we can find an opening of size $2^{\ell-i+1}$ for $q_{i-1}(r_{i-1})$.

In the protocol, $q_i(X) = \sum_{\underline{\omega} \in \{-1,1\}^{\ell-i}} p_{\underline{a}}(r_1, \dots, r_{i-1}, X, \underline{\omega}) p_{\underline{G}}(r_1, \dots, r_{i-1}, X, \underline{\omega})$.
So, $q_i(X)$ is **quadratic**.

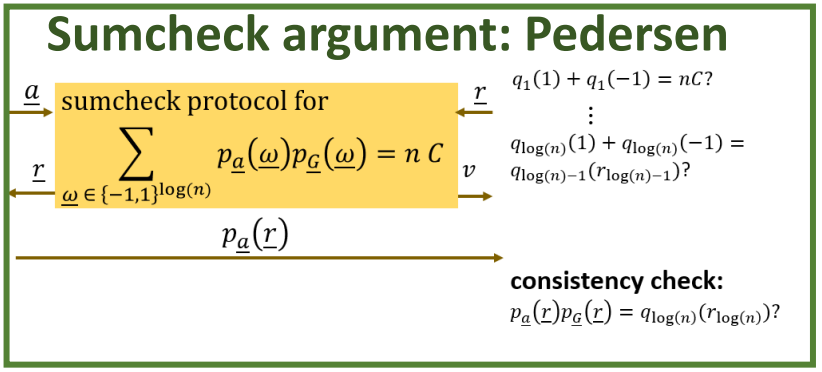
3-ary tree contains **three** evaluations of $q_i(X)$ such that

$\forall j \in [3], \quad q_i\left(r_i^{(j)}\right) = \langle \underline{\pi}^{(j)}, \underline{G}_i \rangle$

Goal: find $\underline{\pi}$ such that $q_i(X) = \langle \underline{\pi}(X), \underline{G}_{i-1} \rangle$

Verifier's check

Then we can find $q_{i-1}(r_{i-1}) = q_i(1) + q_i(-1) = \langle \underline{\pi}', \underline{G}_{i-1} \rangle$



Soundness (part 4)

Claim: If $\underline{\pi}^{(j)} \in \mathbb{F}^{2^{\ell-i}}$ is opening for $q_i(r_i^{(j)})$ for $j \in [3]$, we can find an opening of size $2^{\ell-i+1}$ for $q_{i-1}(r_{i-1})$.

$\underline{G}_k$ is the vector of coefficients of $p_{\underline{G}}(r_1, \ldots, r_k, \underline{X})$

3-ary tree contains **three** evaluations of $q_i(X)$ such that

$$\forall j \in [3], \quad q_i\left(r_i^{(j)}\right) = \langle \underline{\pi}^{(j)}, \underline{G}_i \rangle$$

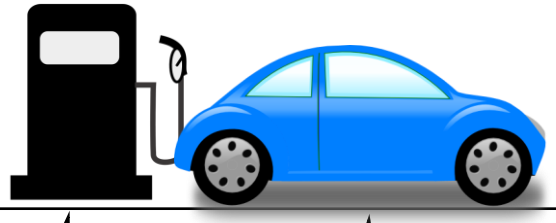
$$= \left\langle \underline{\pi}^{(j)}, (\underline{G}_{i-1,L} + r_i^{(j)} \underline{G}_{i-1,R}) \right\rangle$$

$$= \left\langle \left(\underline{\pi}^{(j)}, r_i^{(j)} \underline{\pi}^{(j)} \right), \underline{G}_{i-1} \right\rangle \xrightarrow{\text{linear algebra}} \underline{\pi} \text{ such that } q_i(X) = \langle \underline{\pi}(X), \underline{G}_{i-1} \rangle$$

Pedersen commitment is *invertible*.

Sumcheck arguments for commitment schemes

Today:



Pedersen commitments

Scalar-product commitments

Sumcheck-friendly commitments

Generalised sumcheck-friendly commitments

Groups

Rings and modules

Sumcheck argument for scalar-product commitments

Common input:

- key $(\underline{G}_1, \underline{G}_2, U) \in \mathbb{G}^{2n+1}$
- commitment $C \in \mathbb{G}^3$

Claim: $\exists(\underline{a}, \underline{b}) \in \mathbb{F}^{2n}$ s.t. $C = (\langle \underline{a}, \underline{G}_1 \rangle, \langle \underline{b}, \underline{G}_2 \rangle, \langle \underline{a}, \underline{b} \rangle U)$

Opening:
$(\underline{a}, \underline{b}) \in \mathbb{F}^{2n}$

P

$(\underline{a}, \underline{b})$

$\underline{r}$

sumcheck protocol for

$$\sum_{\underline{\omega} \in \{-1,1\}^{\log(n)}} \begin{pmatrix} p_{\underline{a}}(\underline{\omega}) p_{\underline{G}_1}(\underline{\omega}) \\ p_{\underline{b}}(\underline{\omega}) p_{\underline{G}_2}(\underline{\omega}) \\ p_{\underline{a}}(\underline{\omega}) p_{\underline{b}}(\underline{\omega}) U \end{pmatrix} = n\, C$$

$\underline{r} \leftarrow \mathbb{F}^{\log(n)}$

$q_1, \ldots, q_{\log(n)}$

$p_{\underline{a}}(\underline{r}), p_{\underline{b}}(\underline{r})$

$q_1(1) + q_1(-1) = nC?$

$\vdots$

$q_{\log(n)}(1) + q_{\log(n)}(-1) = q_{\log(n)-1}(r_{\log(n)-1})?$

V

Consistency check:

$$\begin{pmatrix} p_{\underline{a}}(\underline{r}) p_{\underline{G}_1}(\underline{r}) \\ p_{\underline{b}}(\underline{r}) p_{\underline{G}_2}(\underline{r}) \\ p_{\underline{a}}(\underline{r}) p_{\underline{b}}(\underline{r}) U \end{pmatrix} = q_\ell(r_\ell)?$$

Communication: succinct

Verifier computation: linear

Completeness and soundness

Lemma: The verifier accepts with probability 1.

$$C = \begin{pmatrix} \langle \underline{a}, \underline{G}_1 \rangle \\ \langle \underline{b}, \underline{G}_2 \rangle \\ \langle \underline{a}, \underline{b} \rangle U \end{pmatrix} \longrightarrow \begin{pmatrix} p_{\underline{a}}(\underline{X}) p_{\underline{G}_1}(\underline{X}) \\ p_{\underline{b}}(\underline{X}) p_{\underline{G}_2}(\underline{X}) \\ p_{\underline{a}}(\underline{X}) p_{\underline{b}}(\underline{X}) U \end{pmatrix}$$

Follows from completeness for Pedersen

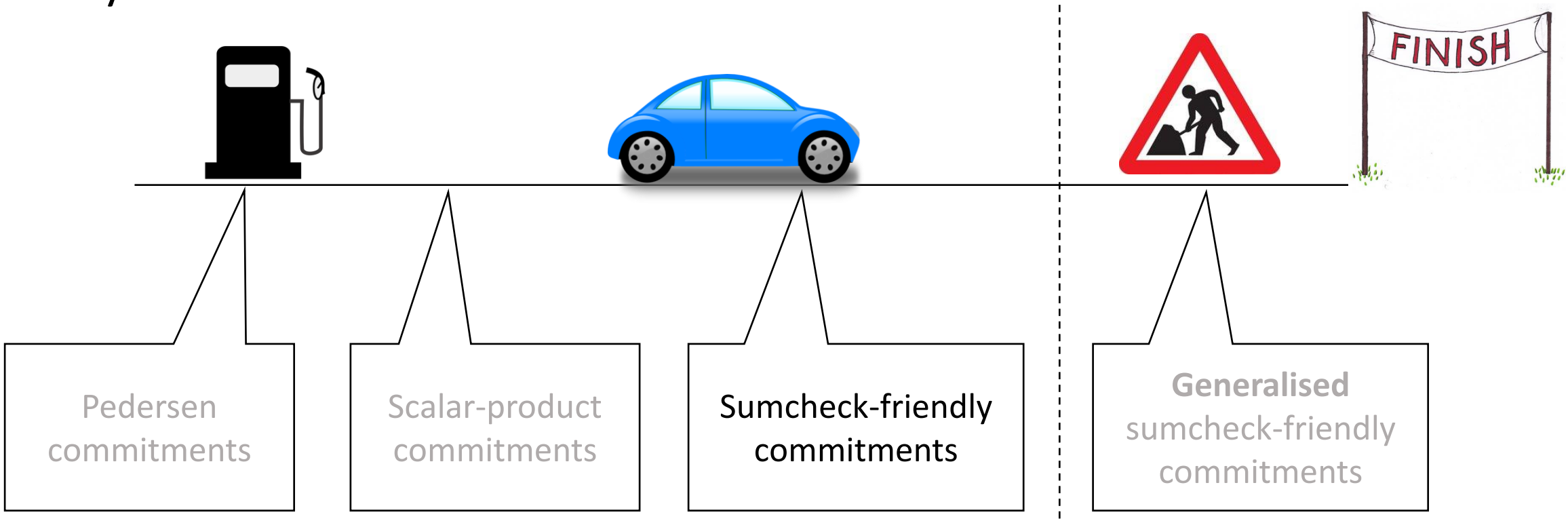
Lemma: **If the commitment scheme is binding**, there exists an extractor that, given a 4-ary *tree of accepting transcripts for key* $(\underline{G}_1, \underline{G}_2)$ and commitment C, finds an opening $(\underline{a}, \underline{b})$ such that $C = \left(\langle \underline{a}, \underline{G}_1 \rangle, \langle \underline{b}, \underline{G}_2 \rangle, \langle \underline{a}, \underline{b} \rangle U\right)$.

Similarly to Pedersen, we extract opening for each components. Using *a computational assumption and the larger tree,* we show that third component is the scalar-product $\langle \underline{a}, \underline{b} \rangle$.

Scalar-product commitment is *invertible.*

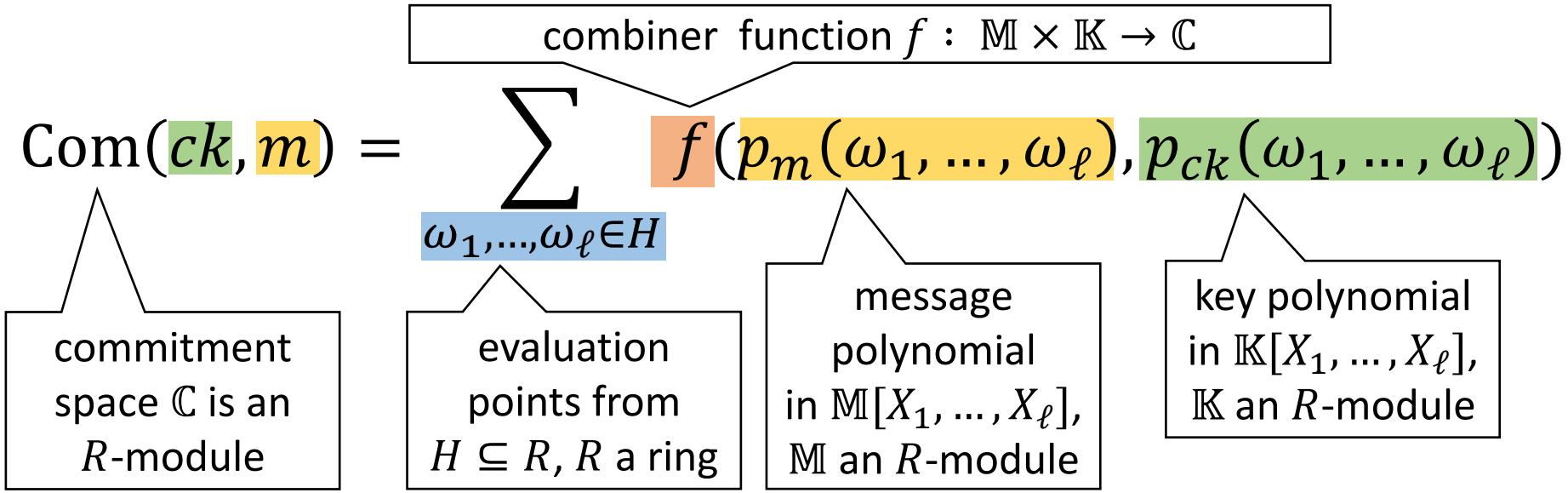
Sumcheck arguments for commitment schemes

Today:



Sumcheck-friendly commitments

Definition: A commitment scheme CM is sumcheck friendly if



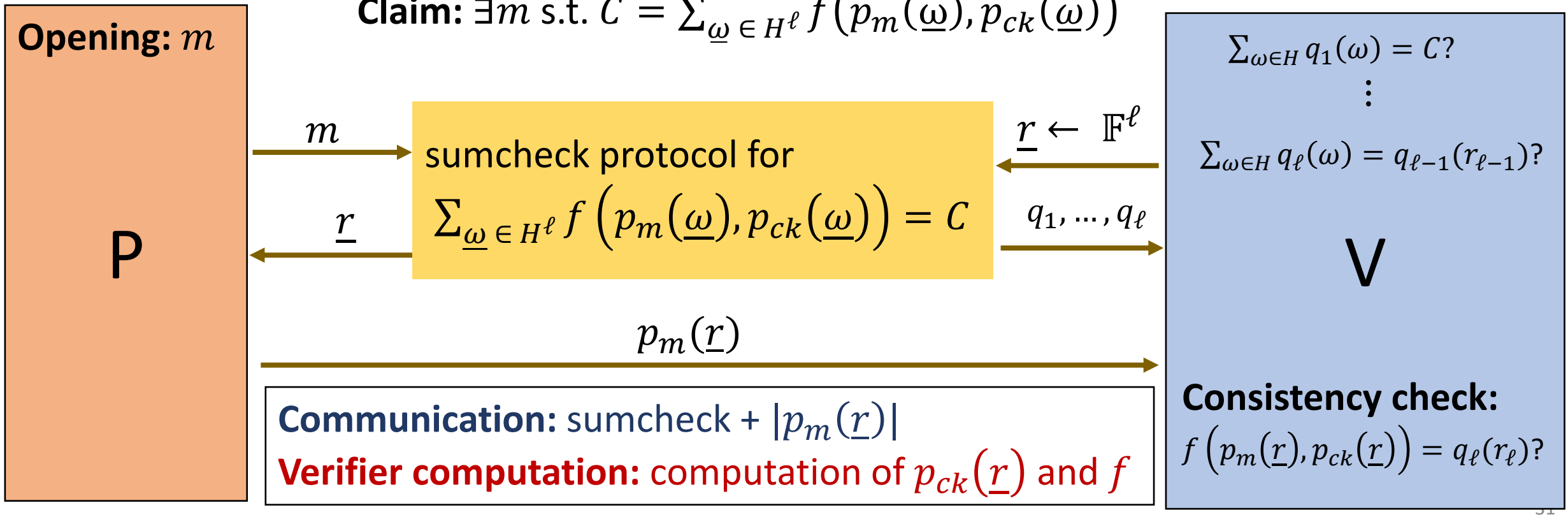
Sumcheck arguments for sumcheck-friendly commitments?

Sumcheck argument for sumcheck-friendly commitments

Common input:

- key ck
- commitment C

Claim: $\exists m$ s.t. $C = \sum_{\underline{\omega} \in H^\ell} f\left(p_m(\underline{\omega}), p_{ck}(\underline{\omega})\right)$



Completeness and soundness

Lemma: The verifier accepts with probability 1.

Follows directly from definition of sumcheck-friendly commitments

Lemma: **If commitment scheme is invertible**, there exists an extractor that, given a suitable *tree of accepting transcripts* for key ck and commitment C, finds an opening m.

Extractor works inductively as in Pedersen using invertibility in each layer

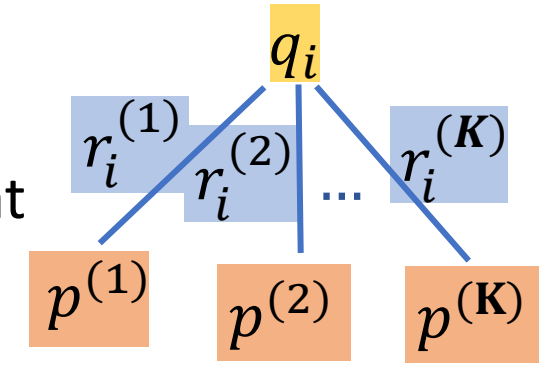
Sumcheck argument:
Sumcheck-friendly commitment

K-Invertibility

Property that allows to climb up the tree from layer to layer.

Given polynomial $q_i(X)$ and "openings" $p^{(1)}(\underline{X}), \dots, p^{(K)}(\underline{X})$ such that

$$\forall j \in [K] : q_i\left(r^{(j)}\right) = \sum_{\underline{\omega} \in H^{\ell-i}} f\left(p^{(j)}(\underline{\omega}), p_{ck}(r_1, \dots, r_i^{(j)}, \underline{\omega})\right)$$



We can find polynomial p such that $\sum_{\omega \in H} q_i(\omega) = \sum_{\underline{\omega} \in H^{\ell-i+1}} f(p(\underline{\omega}), p_{ck}(r_1, \dots, r_{i-1}, \underline{\omega}))$

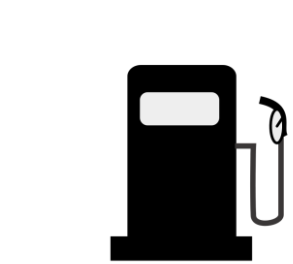
Extra variable X_i: p "bigger" than $p^{(j)}$

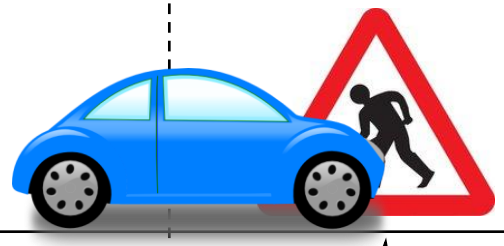
Invertible commitment schemes:

Pedersen commitments, scalar-product commitments, linear-function commitments

Sumcheck arguments for commitment schemes

Today:





Pedersen commitments

Scalar-product commitments

Sumcheck-friendly commitments

Generalised sumcheck-friendly commitments

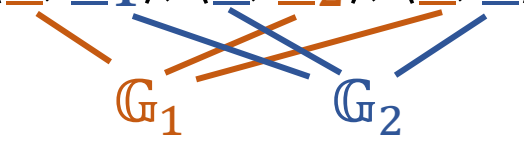
Groups

Rings and modules

From groups to rings

Everything so far extends to general $\mathbb{F}$-vector spaces, e.g., bilinear groups [BMMTV19].

Scalar-product commitments for bilinear groups: $(\langle \underline{\boldsymbol{a}}, \underline{\boldsymbol{G_1}} \rangle, \langle \underline{\boldsymbol{b}}, \underline{\boldsymbol{G_2}} \rangle, \langle \underline{\boldsymbol{a}}, \underline{\boldsymbol{b}} \rangle) \in \mathbb{G}_T^3$



Lattices and groups of unknown order?

Goal: an abstraction for mathematical structures where folding techniques can work

From groups to rings: bilinear modules

R-module M: generalization of vector space over rings

Bilinear module: (M_L, M_R, M_T, e) such that
- M_L, M_R, M_T are R-modules
- $e : M_L \times M_R \to M_T$ is R-bilinear

Messages	Keys	Commitments	Assumption
small M_L	M_R	M_T	Bilinear Relation Assumption

Can define polynomials over message and key spaces

'Multiply' message and key elements using e

Pedersen example: $C = a_1 G_1 + \cdots + a_n G_n = \langle \underline{a}, \underline{G} \rangle$

Hard to find small $\underline{a}$ such that $\langle \underline{a}, \underline{G} \rangle = 0$

Add the pieces together

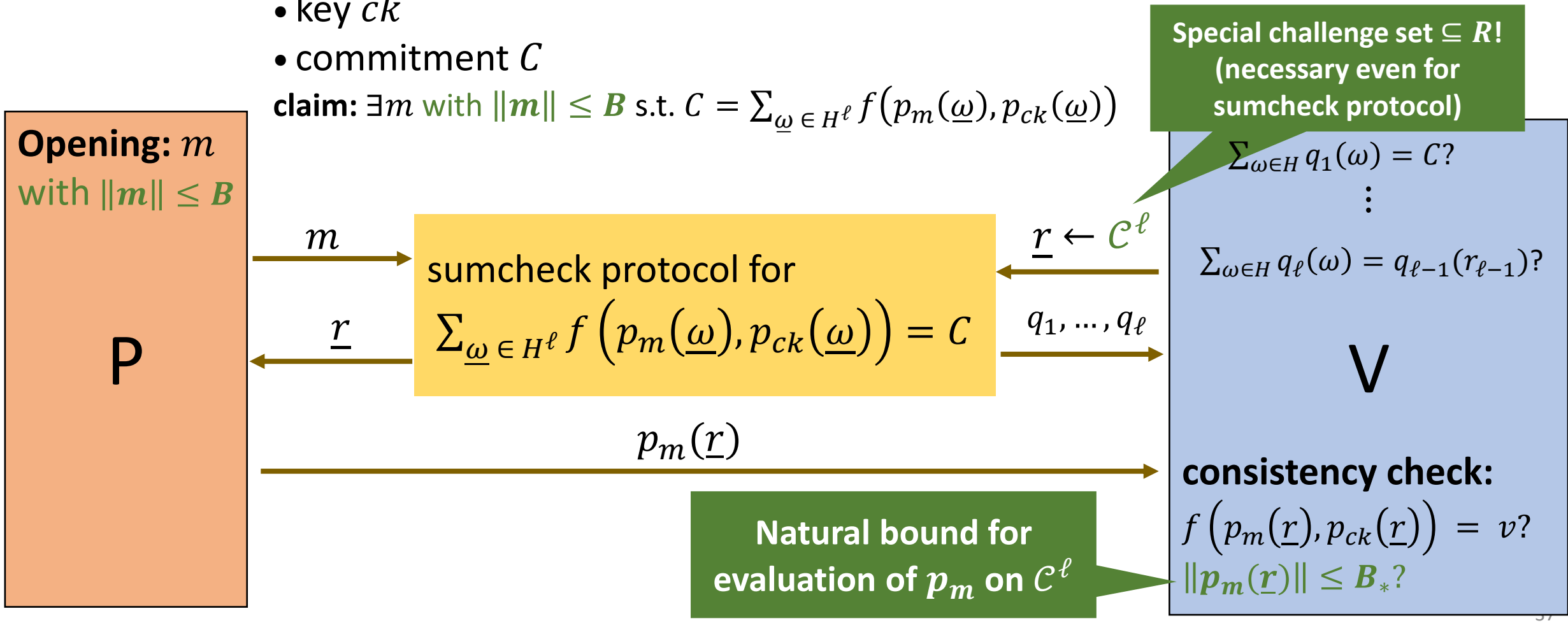
Norm checks: only "short" elements are valid messages e.g., for ring-SIS

From groups to rings: sumcheck arguments

common input:

- key ck
- commitment C

claim: $\exists m$ with $\|m\| \leq B$ s.t. $C = \sum_{\underline{\omega} \in H^\ell} f\left(p_m(\underline{\omega}), p_{ck}(\underline{\omega})\right)$



From groups to rings: soundness

Challenges:

1. Linear algebra different over rings and modules
2. Norm considerations arise

Lemma: If commitment scheme is invertible, there exists an extractor that, given a suitable *tree of accepting transcripts* for key ck and commitment C, finds a **relaxed** opening m.

Arithmetic over rings might cause slackness factors and increase in norm.

e.g., for Pedersen, the extracted relaxed opening $\underline{a}$ for C and $\underline{G}$:

$$\xi^{\ell} \cdot C = \langle \underline{a}, \underline{G} \rangle \text{ with } \|\underline{a}\| \leq N^{\ell} \cdot B_*$$

Tighter analysis in [LA21], [ACK21]

Parameters for lattices:

Ring	$\mathcal{C}$	ξ	N
$\frac{\mathbb{Z}_q[X]}{< X^d + 1 >}$	$\{X^i : 0 \leq i \leq 2d - 1\}$	8	$O(d^7)$

From groups to rings:
R1CS over rings

A remark about our R1CS result:

Without slackness!

Lemma (soundness): There exists an extractor that finds an **R1CS witness**.

e.g., for Pedersen, the extracted relaxed opening $\underline{a}$ for C and $\underline{G}$:

$$\xi^{\ell} \cdot C = \langle \underline{a}, \underline{G} \rangle \text{ with } \|\underline{a}\| \leq N^{\ell} \cdot B$$

$$C = \langle \underline{a}/\xi^{\ell}, \underline{G} \rangle \text{ with } \|\underline{a}/\xi^{\ell}\| \leq B'$$

Issues:
1. ξ might not be invertible
2. $\|\underline{a}/\xi^{\ell}\|$ might not be small

Ideal I such that $\xi \pmod I$ is invertible, $\|x \pmod I\|$ small for all x

$$C = \langle \underline{a}/\xi^{\ell} \pmod I, \underline{G} \rangle \text{ with } \|\underline{a}/\xi^{\ell} \pmod I\| \leq B'$$

Instantiations of bilinear modules

Assumption	Messages	Keys	Commitments	Ideal
BRA	small M_L	M_R	M_T	I
DLOG	$\mathbb{F}_p$	$\mathbb{G}$	$\mathbb{G}$	$\{0\}$
DPAIR[AFGHO10]	$\mathbb{G}_1$	$\mathbb{G}_2$	$\mathbb{G}_T$	$\{0\}$
UO [BFS20]	small $\mathbb{Z}$	$\mathbb{G}$	$\mathbb{G}$	$n\mathbb{Z}$ for suitable small n
RSIS [Ajtai94]	small R_q	R_q^d	R_q^d	$n\mathbb{Z}$ for suitable small n

Conclusion

Summary of results

Theorem 1:

The sumcheck protocol applied to a sumcheck-friendly commitment scheme is a succinct argument of knowledge of commitment openings.

Theorem 2: Let (M_L, M_R, M_T) be a secure bilinear module with M_L a ring and $I \subseteq M_L$ an ideal. There is a ZK succinct argument of knowledge for R1CS with

R1CS Ring	Prover and verifier time	Proof size
M_L/I	$O(n)$ ops M_L, M_R, M_T	$O(\log n)$ elems

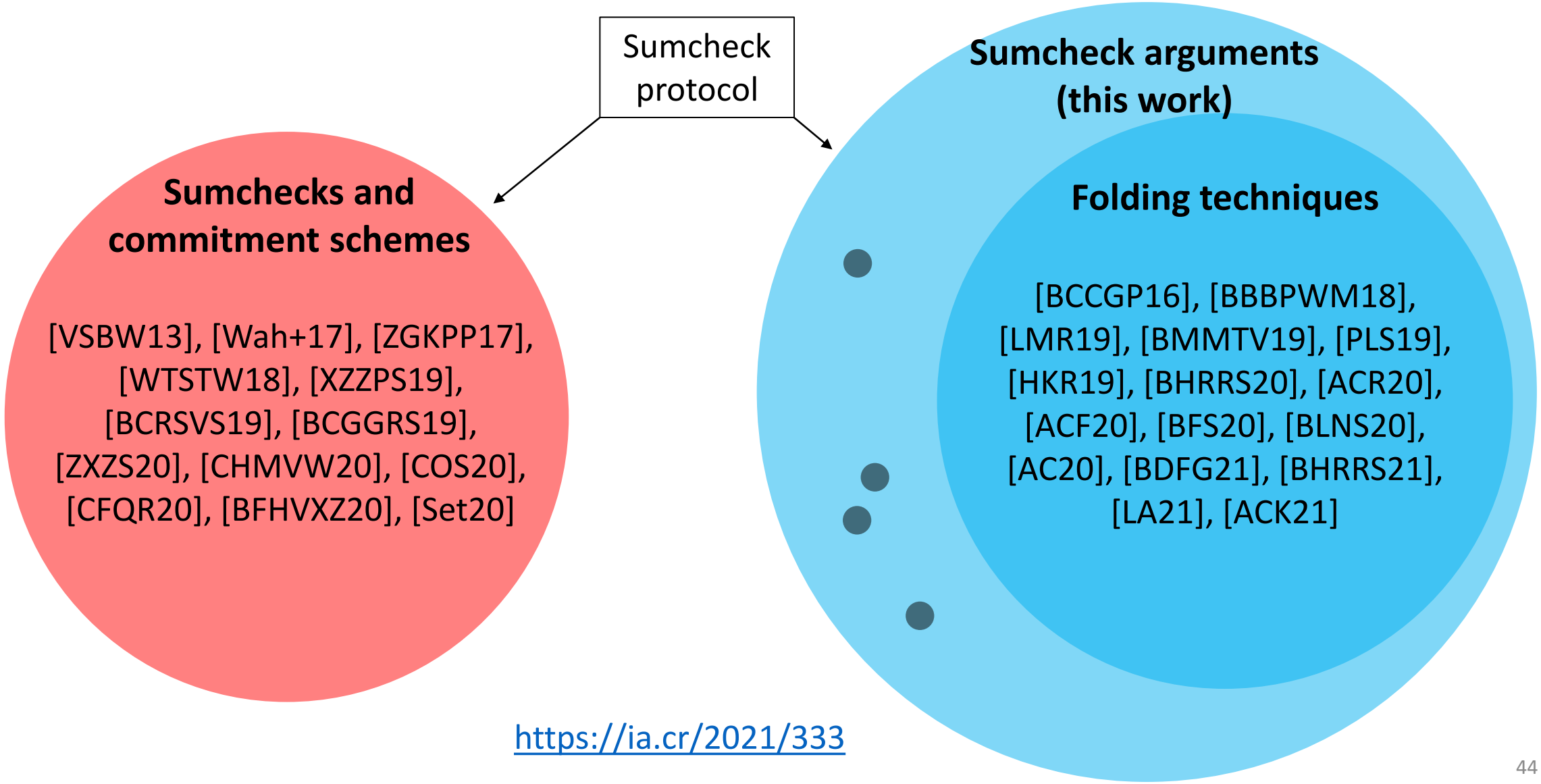
Corollary: Let $p \ll q$ primes, $R_p := \mathbb{Z}_p[X]/\langle X^d + 1\rangle$ and similarly for R_q. Then assuming SIS is hard, there is a ZK succinct argument of knowledge for R1CS with

R1CS Ring	Prover and verifier time	Proof size
R_p	$O(n)$ ops R_p, R_q	$O(\log n)$ elems R_q

Takeaways

- Many commitment schemes are sumcheck friendly
- We can recast many different cryptographic settings as bilinear modules
- In the paper: instantiations and polynomial commitment schemes

Thanks!



https://ia.cr/2021/333