On Succinct Arguments and Witness Encryption from Groups

Ohad Barta, Yuval Ishai, Rafail Ostrovsky, and David J. Wu

December 2020

Argument Systems

$x \in \{0,1\}^*$

NP language $\mathcal{L} \subseteq \{0,1\}^*$

Accept if $x \in \mathcal{L}$

Prover

Verifier

Completeness: $\forall x \in \mathcal{L} : \Pr[\langle P, V \rangle(x) = \text{accept}] = 1$

"Honest prover convinces honest verifier of true statements"

Soundness: $\forall x \notin \mathcal{L},\ \forall \text{ efficient } P^* : \Pr[\langle P^*, V \rangle(x) = \text{accept}] \leq \varepsilon$

"Efficient prover cannot convince honest verifier of false statement"

How Short Can a Proof Be?

This talk: laconic arguments for NP

NP language $\mathcal{L} \subseteq \{0,1\}^*$

$x \in \{0,1\}^*$

Prover

Accept if $x \in \mathcal{L}$

Verifier

Succinctness: $|\pi| = \mathrm{poly}(\lambda, \log|C|)$

"Proof size is much shorter than circuit size of classic NP verifier"

How Short Can a Proof Be?

This talk: laconic arguments for NP

$x \in \{0,1\}^*$

NP language $\mathcal{L} \subseteq \{0,1\}^*$

Accept if $x \in \mathcal{L}$

π

Sometimes, also require that verification complexity is sublinear/polylogarithmic

Prover

Verifier

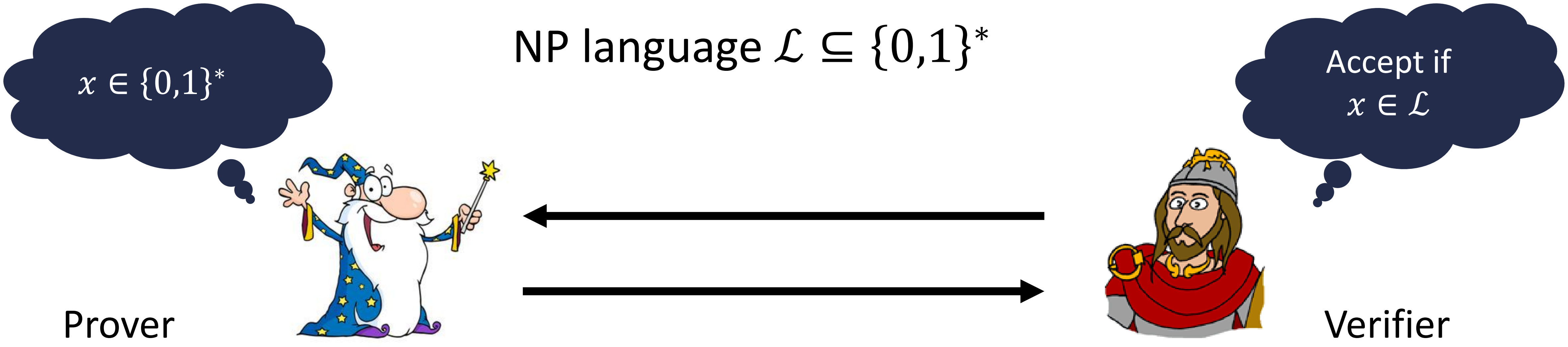
Succinctness: $|\pi| = \text{poly}(\lambda, \log|C|)$

“Proof size is much shorter than circuit size of classic NP verifier”

How Short Can a Proof Be?

This talk: laconic arguments for NP

NP language $\mathcal{L} \subseteq \{0,1\}^*$



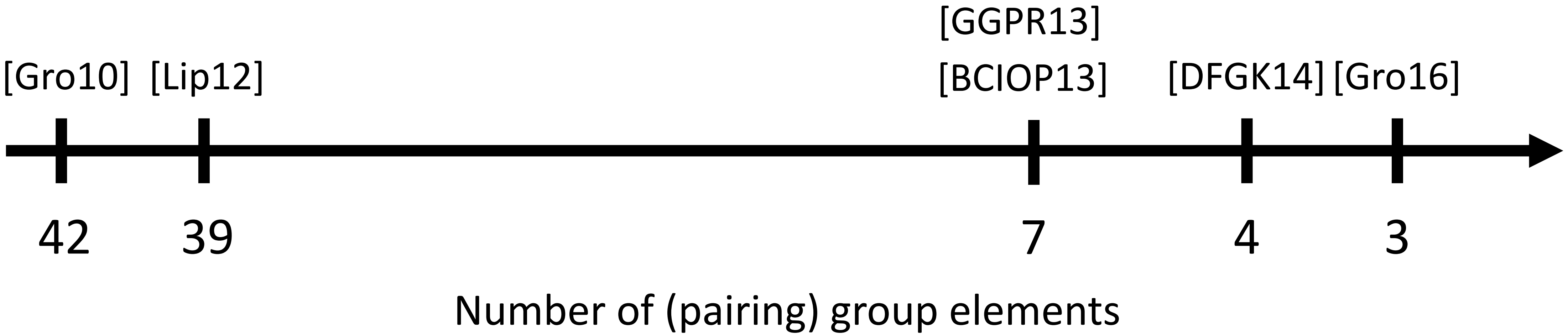
Focus of this talk: 2-message arguments

Special case: If verifier's message is statement-independent ⇒
succinct non-interactive argument (SNARG) in the CRS model

How Short Can a Proof Be?

Using indistinguishability obfuscation: 128-bit proofs (at 128-bit security level) [SW14]

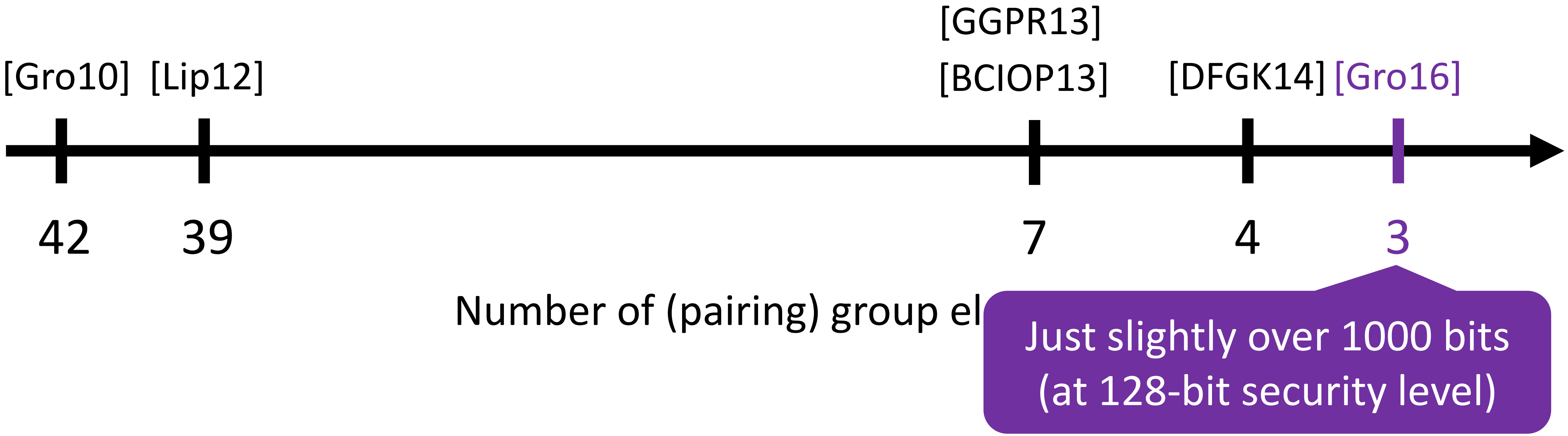
Many practical ("implementable") SNARGs are based on groups



How Short Can a Proof Be?

Using indistinguishability obfuscation: 128-bit proofs (at 128-bit security level) [SW14]

Many practical ("implementable") SNARGs are based on groups



How Short Can a Proof Be?

Using indistinguishability obfuscation: 128-bit proofs (at 128-bit security level) [SW14]

Many pr sed on groups

Using PCPs, can obtain a (designated-verifier) SNARG where proofs are 2 group elements (with inverse polynomial soundness)

Number of (pairing) group el

Just slightly over 1000 bits (at 128-bit security level)

Concretely-efficient arguments where proofs consist of 2 group elements?

Arguments where proof consists of 1 group element?

Summary of Results

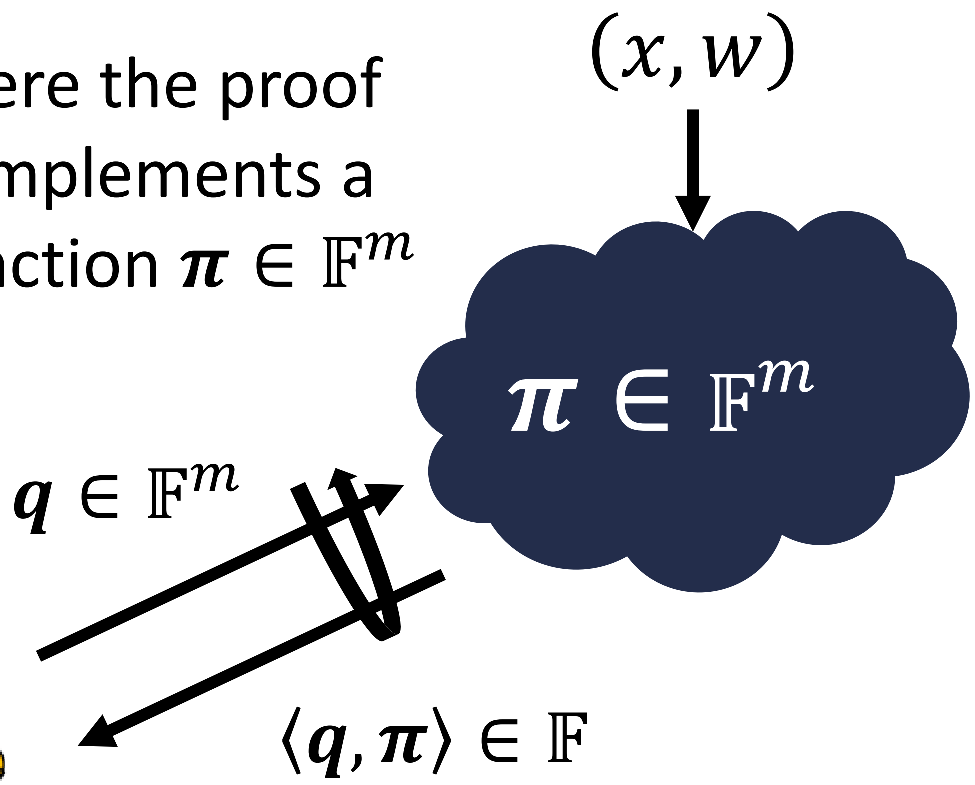
Construction	Group Type	Proof Size	Information-Theoretic Building Block	Soundness Error	Completeness Error	Argument Type
[Gro16]	bilinear	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$	linear PCP	$\mathrm{negl}(\lambda)$	0	SNARG
[BCIOP13]	linear	$8\lvert\mathbb{G}\rvert$	linear PCP	$1/\mathrm{poly}(\lambda)$	0	dvSNARG
[BCIOP13]	linear	$2\lvert\mathbb{G}\rvert$	PCP	$1/\mathrm{poly}(\lambda)$	0	dvSNARG
This work	linear	$2\lvert\mathbb{G}\rvert$	linear PCP	$1/\mathrm{poly}(\lambda)$	$\mathrm{negl}(\lambda)$	dvSNARG
This work	linear	$2\lvert\mathbb{G}\rvert$	PCP	$\mathrm{negl}(\lambda)$	$o(1)$	laconic argument
This work	linear	$\lvert\mathbb{G}\rvert$	PCP	$\mathrm{negl}(\lambda)$	$o(1)$	laconic argument

- Relies on a new hypothesis on the hardness of approximation of the minimal distance of linear codes
- Under the same hypothesis, implies a witness encryption scheme for NP in the generic group model

Main Ingredient: Linear PCPs (LPCPs)

[IKO07]

PCP where the proof oracle implements a linear function $\boldsymbol{\pi} \in \mathbb{F}^m$



Verifier

Instantiations (for circuit satisfiability):

- Walsh-Hadamard encoding [ALMSS92, IKO07]
  3 queries, $m = O(|C|^2)$
- Quadratic span programs [GGPR13]
  3 queries, $m = O(|C|)$
- Square span programs [DFGK14]
  2 queries, $m = O(|C|)$
- Traditional PCPs [BCIOP13]
  1 query, $m = \mathrm{poly}(|C|)$

Queries in these constructions are <u>statement-independent</u>

From Linear PCPs to Succinct Arguments

[BCIOP13]

Verifier encrypts its queries using a <u>linear-only</u> encryption scheme

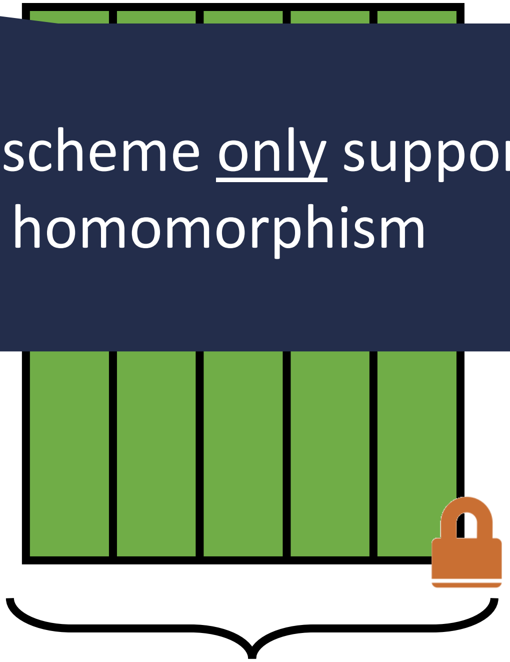
$$\boldsymbol{Q} = \underbrace{\begin{bmatrix} q_1 & q_2 & q_3 & \cdots & q_k \end{bmatrix}}_{\text{Part of CRS}}$$

From Linear PCPs to Succinct Arguments

[BCIOP13]

Verifier encrypts its queries using a linear-only encryption scheme

Encryption scheme only supports linear homomorphism



Part of CRS

From Linear PCPs to Succinct Arguments

[BCIOP13]

Verifier encrypts its queries using a <u>linear-only</u> encryption scheme

$$\boldsymbol{Q} = \underbrace{\begin{bmatrix} q_1 & q_2 & q_3 & \cdots & q_k \end{bmatrix}}_{\text{Part of CRS}}$$

Prover constructs linear PCP π from (x, w)

$$(x, w) \longrightarrow \boldsymbol{\pi} \in \mathbb{F}^m$$

Prover homomorphically computes responses to linear PCP queries

$\langle \pi, q_1 \rangle$	$\langle \pi, q_2 \rangle$	$\cdots$	$\langle \pi, q_k \rangle$

Prover's message

From Linear PCPs to Succinct Arguments

[BCIOP13]

Statement-independent LPCP ⇒ designated-verifier SNARG

Statement-dependent LPCP ⇒ 2-message laconic argument

(Also possible to instantiate compiler with a linear-only encoding scheme to obtain publicly-verifiable SNARGs)

Prover constructs linear PCP π from (x, w)

$$(x, w) \downarrow \boldsymbol{\pi} \in \mathbb{F}^m$$

Verifier decrypts ciphertexts and checks linear PCP responses

Prover homomorphically computes responses to linear PCP queries

$\langle \boldsymbol{\pi}, \boldsymbol{q}_1 \rangle$	$\langle \boldsymbol{\pi}, \boldsymbol{q}_2 \rangle$	$\cdots$	$\langle \boldsymbol{\pi}, \boldsymbol{q}_k \rangle$

Prover's message

Succinct Arguments based on ElGamal

Assumption: ElGamal encryption (with message in exponent) is linear-only
(holds unconditionally if we model $\mathbb{G}$ as a generic group)

sk: $x \leftarrow \mathbb{Z}_p$

pk: $h = g^x \in \mathbb{G}$

$\text{Encrypt}(\text{pk}, m): r \leftarrow \mathbb{Z}_p, \text{ct} = (g^r, h^r g^m)$

$|\text{ct}| = 2|\mathbb{G}|$

Decryption recovers message in the exponent, so need to solve discrete log to recover message

Assuming LPCP responses are "small"

k-query LPCP

[BCIOP13] compiler

Designated-verifier argument with proofs of size $2(k+1)|\mathbb{G}|$

$\mathbb{G}$: group with prime order p and generator g

Succinct Arguments based on ElGamal

Assumption: ElGamal encryption (with message in exponent) is linear-only (holds unconditionally if we model $\mathbb{G}$ as a generic group)

$\text{sk}: x \leftarrow \mathbb{Z}_p$

$\text{pk}: h = g^x \in \mathbb{G}$

$\text{Encrypt}(\text{pk}, m): r \leftarrow \mathbb{Z}_p, \text{ct} = (g^r, h^r g^m)$

$|\text{ct}| = 2|\mathbb{G}|$

Decryption recovers message in the exponent, so need to solve discrete log to recover message

Assuming LPCP responses are "small"

k-query LPCP → [BCIOP13] compiler → Designated-verifier argument with proofs of size $2(k+1)|\mathbb{G}|$

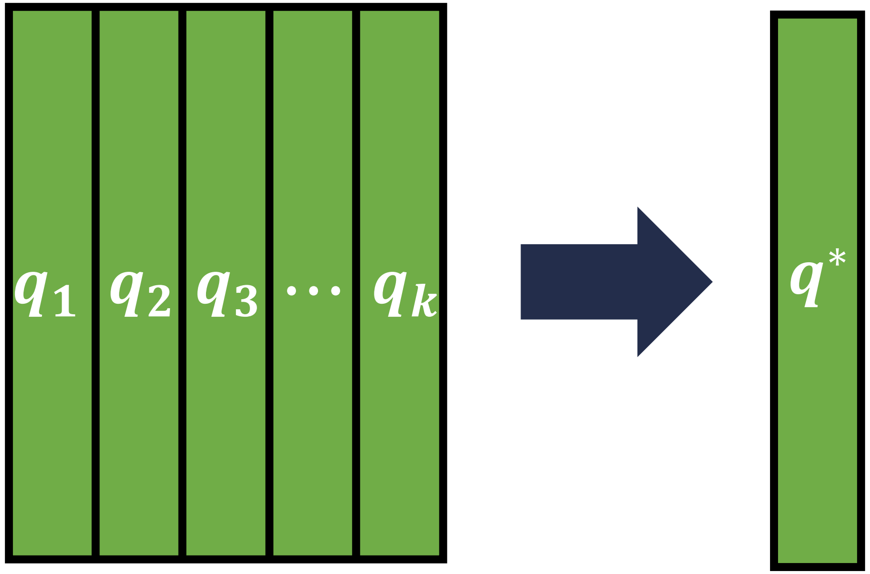
"Extra" query needed for consistency check (unnecessary when $k = 1$)

Observation: to obtain a SNARG with proof size $2|\mathbb{G}|$, sufficient to construct a <u>1-query linear PCP</u>

Query Packing for Linear PCPs

[BCIOP13]: k-query PCP ⇒ 1-query linear PCP

This work: k-query (bounded) linear PCP ⇒ 1-query linear PCP



$\boldsymbol{Q} \in \mathbb{Z}^{m \times k}$

$$\boldsymbol{q}^* = \sum_{i \in [k]} B^{i-1} \boldsymbol{q}_i$$

Suppose $\|\boldsymbol{Q}^T \boldsymbol{\pi}\|_\infty < B$ bounded LPCP

$$\langle \boldsymbol{q}^*, \boldsymbol{\pi} \rangle = \sum_{i \in [k]} B^{i-1} \langle \boldsymbol{q}_i, \boldsymbol{\pi} \rangle$$

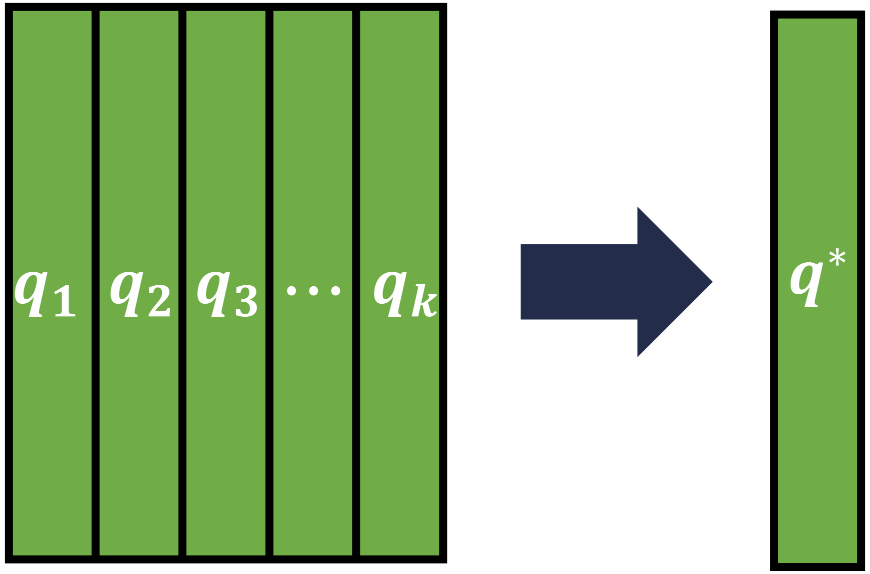
Can view value as an integer in base B with k digits (corresponding to LPCP responses)

Starting point: View linear PCP queries + proof over the integers

Query Packing for Linear PCPs

[BCIOP13]: k-query PCP $\Rightarrow$ 1-query linear PCP

This work: k-query (bounded) linear PCP $\Rightarrow$ 1-query linear PCP



$\boldsymbol{Q} \in \mathbb{Z}^{m \times k}$

$$\boldsymbol{q}^* = \sum_{i \in [k]} B^{i-1} \boldsymbol{q}_i$$

Suppose $\|\boldsymbol{Q}^T \boldsymbol{\pi}\|_\infty < B$ bounded LPCP

$$\langle \boldsymbol{q}^*, \boldsymbol{\pi} \rangle = \sum_{i \in [k]} B^{i-1} \langle \boldsymbol{q}_i, \boldsymbol{\pi} \rangle$$

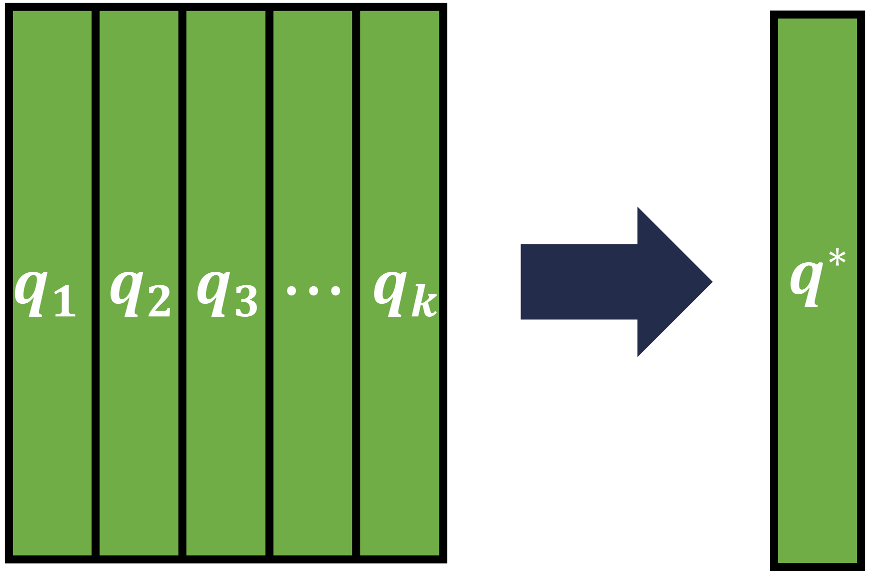
Problem: malicious prover can choose $\boldsymbol{\pi} \in \mathbb{Z}^m$ such that responses are *not* bounded

Then, packed responses cannot be explained by a single linear function

Query Packing for Linear PCPs

[BCIOP13]: k-query PCP $\Rightarrow$ 1-query linear PCP

This work: k-query (bounded) linear PCP $\Rightarrow$ 1-query linear PCP



$\boldsymbol{Q} \in \mathbb{Z}^{m \times k}$

$\boldsymbol{q}^* = \sum_{i \in [k]} r_i \boldsymbol{q}_i$

Suppose $\|\boldsymbol{Q}^T \boldsymbol{\pi}\|_\infty < B$ <u>bounded</u> LPCP

$$\langle \boldsymbol{q}^*, \boldsymbol{\pi} \rangle = \sum_{i \in [k]} r_i \langle \boldsymbol{q}_i, \boldsymbol{\pi} \rangle$$

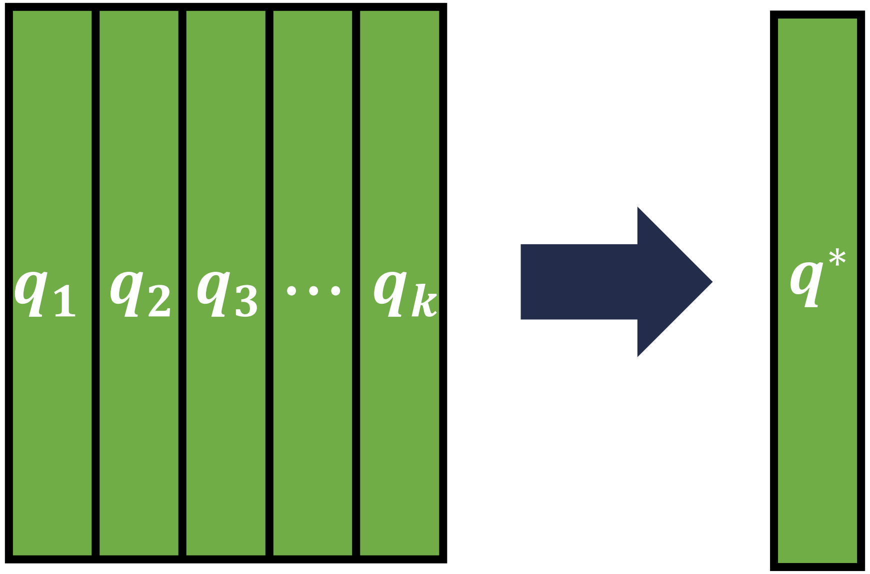
Solution: take a <u>random</u> linear combination of query vectors, where scalars r_i chosen from sufficiently-large interval

k-query B-bounded LPCP $\Rightarrow$
1-query $B^{O(k)}$-bounded LPCP

Query Packing for Linear PCPs

[BCIOP13]: k-query PCP $\Rightarrow$ 1-query linear PCP

This work: k-query (bounded) linear PCP $\Rightarrow$ 1-query linear PCP



$\boldsymbol{Q} \in \mathbb{Z}^{m \times k}$

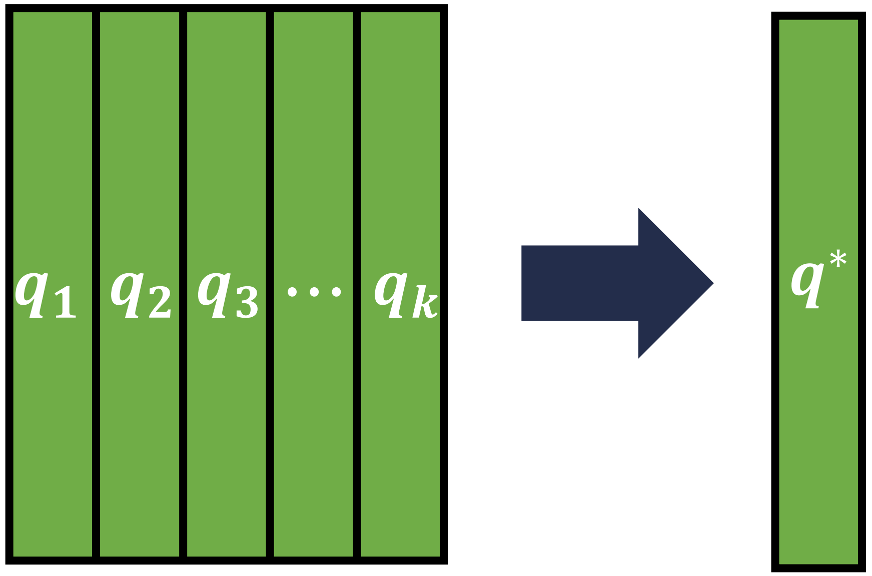
$$\boldsymbol{q}^* = \sum_{i \in [k]} r_i \boldsymbol{q}_i$$

Embed B-bounded integer linear PCPs over a finite field $\mathbb{F}_p$ where $p > B$

Compile linear PCP over $\mathbb{F}_p$ to succinct argument using [BCIOP13]

For packed linear PCP, meaningful if final bound satisfies $B^{O(k)} < p$

Hadamard LPCP Instantiation



$\boldsymbol{Q} \in \mathbb{Z}^{m \times k}$

$$\boldsymbol{q}^* = \sum_{i \in [k]} r_i \boldsymbol{q}_i$$

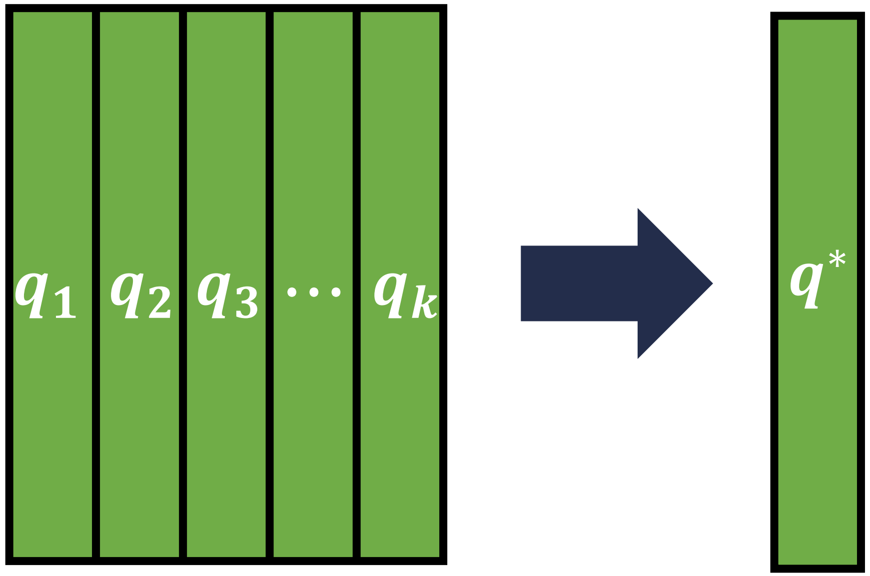
k-query (bounded) LPCP ⇒ 1-query LPCP

Hadamard instantiation [ALMSS92, IKO07]:

- 2-query B-bounded linear PCP

Previously described as a 3-query construction, but 2 of the queries can be combined

Hadamard LPCP Instantiation



$$\boldsymbol{Q} \in \mathbb{Z}^{m \times k} \qquad \boldsymbol{q}^* = \sum_{i \in [k]} r_i \boldsymbol{q}_i$$

k-query (bounded) LPCP $\Rightarrow$ 1-query LPCP

Hadamard instantiation [ALMSS92, IKO07]:

- 2-query B-bounded linear PCP
- Query dimension: $m = O(|C|^2)$
- For soundness error ε, $B = O(|C|^2/\varepsilon^2)$

Problematic: bound for packed LPCP is $B' = O(|C|^4/\varepsilon^4)$

Verification time requires computing a discrete log of this magnitude – requires time $O(|C|^2/\varepsilon^2)$

Hadamard LPCP Instantiation

Optimizing proof verification:

- Linear PCP verification corresponds to a quadratic test:

$$\underbrace{a_1^2 - a_2}_{\text{LPCP responses}} = \underbrace{t}_{\text{Target value (depends only on statement)}}$$

Hadamard instantiation [ALMSS92, IKO07]:

- 2-query B-bounded linear PCP
- Query dimension: $m = O(|C|^2)$
- For soundness error ε, $B = O(|C|^2/\varepsilon^2)$

Problematic: bound for packed LPCP is $B' = O(|C|^4/\varepsilon^4)$

Verification time requires computing a discrete log of this magnitude – requires time $O(|C|^2/\varepsilon^2)$

Hadamard LPCP Instantiation

Optimizing proof verification:

- Linear PCP verification corresponds to a quadratic test:
$$a_1^2 - a_2 = t$$
- **Packed representation:** verifier computes $g^a = g^{a_1 + r \cdot a_2}$ (verifier knows r)
- **Observation:** With overwhelming probability, $|a_1| \in O\left(\sqrt{|C|}/\varepsilon\right)$

Strict bound (with probability 1):
$|a_1| \in O(|C|/\varepsilon)$

Hadamard instantiation [ALMSS92, IKO07]:

- 2-query B-bounded linear PCP
- Query dimension: $m = O(|C|^2)$
- For soundness error ε, $B = O(|C|^2/\varepsilon^2)$

Problematic: bound for packed LPCP is $B' = O(|C|^4/\varepsilon^4)$

Verification time requires computing a discrete log of this magnitude – requires time $O(|C|^2/\varepsilon^2)$

Hadamard LPCP Instantiation

Optimizing proof verification:

- Linear PCP verification corresponds to a quadratic test:
$$a_1^2 - a_2 = t$$
- **Packed representation:** verifier computes $g^a = g^{a_1 + r \cdot a_2}$ (verifier knows r)
- **Observation:** With overwhelming probability, $|a_1| \in O\left(\sqrt{|C|}/\varepsilon\right)$

Strict bound (with probability 1):
$|a_1| \in O(|C|/\varepsilon)$

If g^a encodes a valid LPCP response, then there exists a_1 such that
$$g^a = g^{a_1 + r \cdot a_2} = g^{a_1 + r a_1^2} g^{-rt}$$
Equivalently:
$$g^a g^{-rt} = g^{a_1 + r a_1^2}$$

Statement independent

Implication: verifier can precompute accepting values of $g^{a_1 + r a_1^2}$

Verification consists of ElGamal decryption (to obtain g^a), multiplication by g^{-rt} and a table lookup (for $g^{a_1 + r a_1^2}$)

Designated-Verifier SNARGs based on ElGamal

q^*

1-query linear PCP

Encrypt
with ElGamal

q^*

Assuming ElGamal is linear-only (or modeling $\mathbb{G}$ as a generic group)

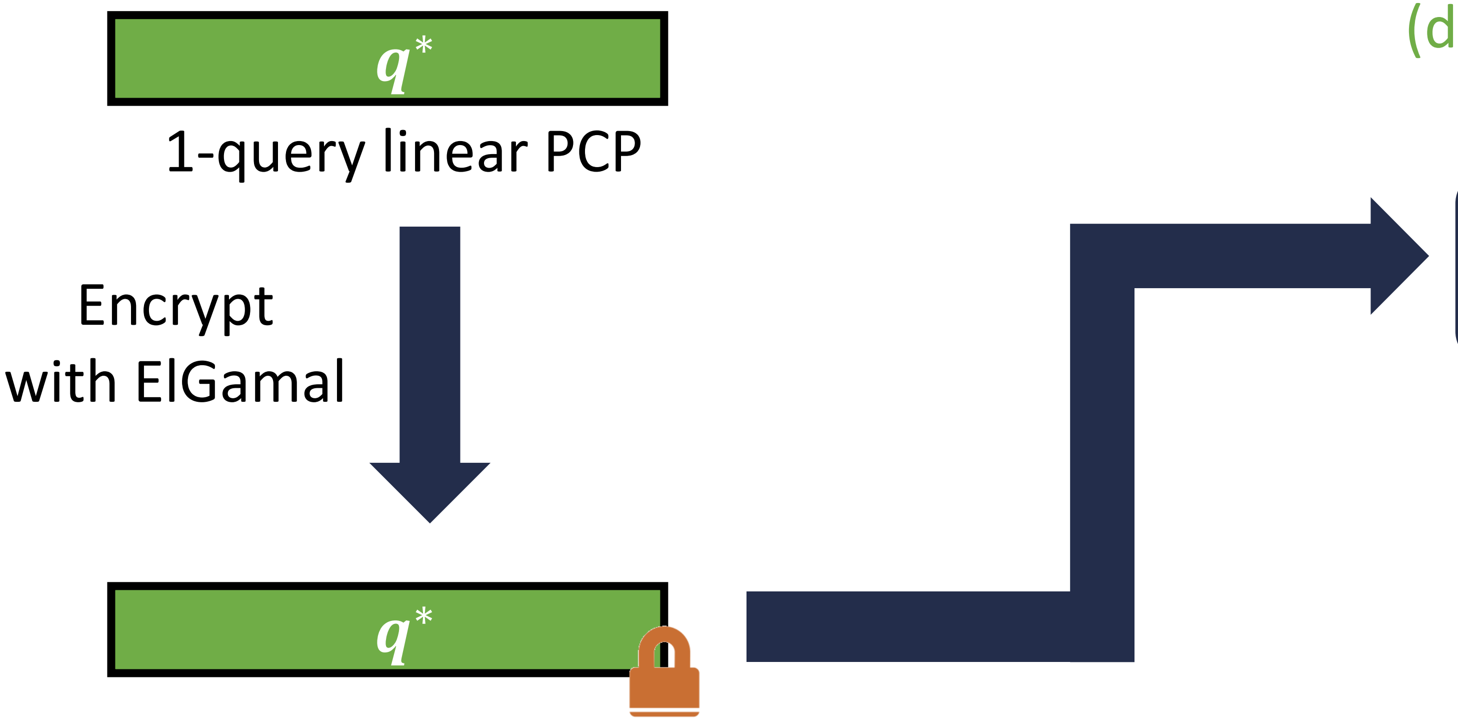
Designated-verifier SNARG for NP

To verify NP relation of size $|C|$:

- **Proof size:** $2|\mathbb{G}|$
- **CRS size + prover cost:** $O(|C|^2)$
- **Soundness error:** $\varepsilon = 1/\text{poly}(\lambda)$
- **Verifier cost:** $\tilde{O}\left(\sqrt{|C|}/\varepsilon\right)$

With a precomputed table of size $\tilde{O}\left(\sqrt{|C|}/\varepsilon\right)$, verification requires just 4 group operations and table lookup

Designated-Verifier SNARGs based on ElGamal



Shortest SNARG with good concrete efficiency
(does not need to use classical PCPs)

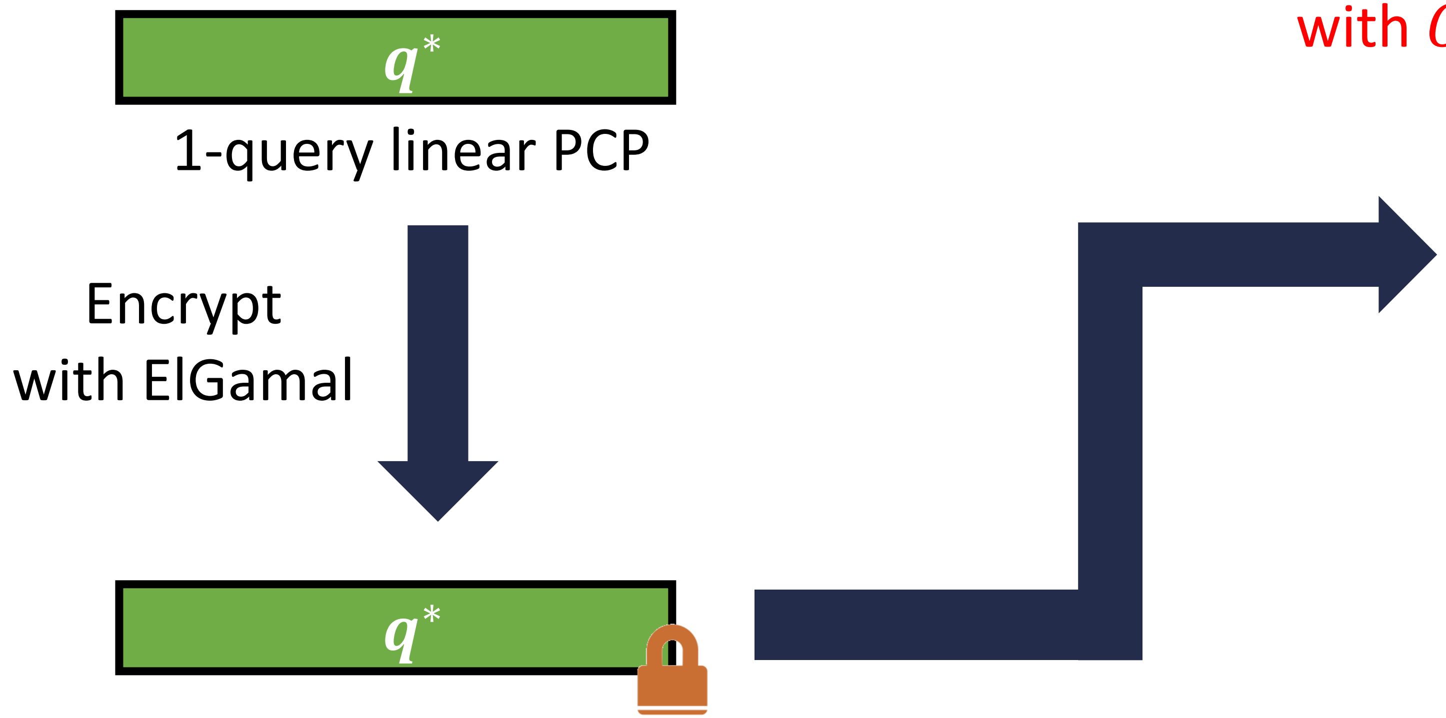
Designated-verifier SNARG for NP

To verify NP relation of size $|C|$:

- **Proof size:** $2|\mathbb{G}|$
- **CRS size + prover cost:** $O(|C|^2)$
- **Soundness error:** $\varepsilon = 1/\text{poly}(\lambda)$
- **Verifier cost:** $\tilde{O}\left(\sqrt{|C|}/\varepsilon\right)$

Designated-Verifier SNARGs based on ElGamal

Open question: Same level of succinctness but with $O(|C|)$ size CRS (and $O(|C|)$ prover cost)

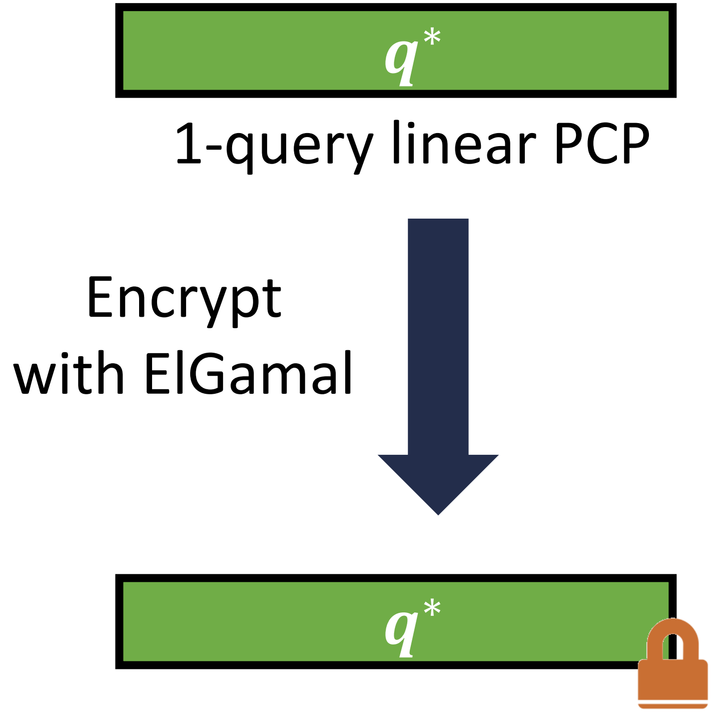


Designated-verifier
SNARG for NP

To verify NP relation of size $|C|$:

- **Proof size:** $2|\mathbb{G}|$
- **CRS size + prover cost:** $O(|C|^2)$
- **Soundness error:** $\varepsilon = 1/\text{poly}(\lambda)$
- **Verifier cost:** $\tilde{O}\left(\sqrt{|C|}/\varepsilon\right)$

Designated-Verifier SNARGs based on ElGamal



Designated-verifier SNARG for NP

To verify NP relation of size $|C|$:

- **Proof size:** $2|\mathbb{G}|$
- **CRS size + prover cost:** $O(|C|^2)$
- **Soundness error:** $\varepsilon = 1/\mathrm{poly}(\lambda)$
- **Verifier cost:** $\tilde{O}\left(\sqrt{|C|}/\varepsilon\right)$

Can we get <u>negligible</u> soundness without compromising correctness?

Achieving Negligible Soundness Error

q^*

1-query linear PCP

q^*

Encrypt query vector with ElGamal

Prover computes:

$\langle q^*, \pi \rangle$

$$\left(g^r, h^r g^{\langle q^*, \pi \rangle}\right)$$

Approach: If verification relation is linear, then possible to evaluate it in the exponent

Can we construct a 1-query linear PCP with a linear decision procedure?

Problem: linear PCP response computed in the exponent

"Decryption" yields $g^{\langle q^*, \pi \rangle}$

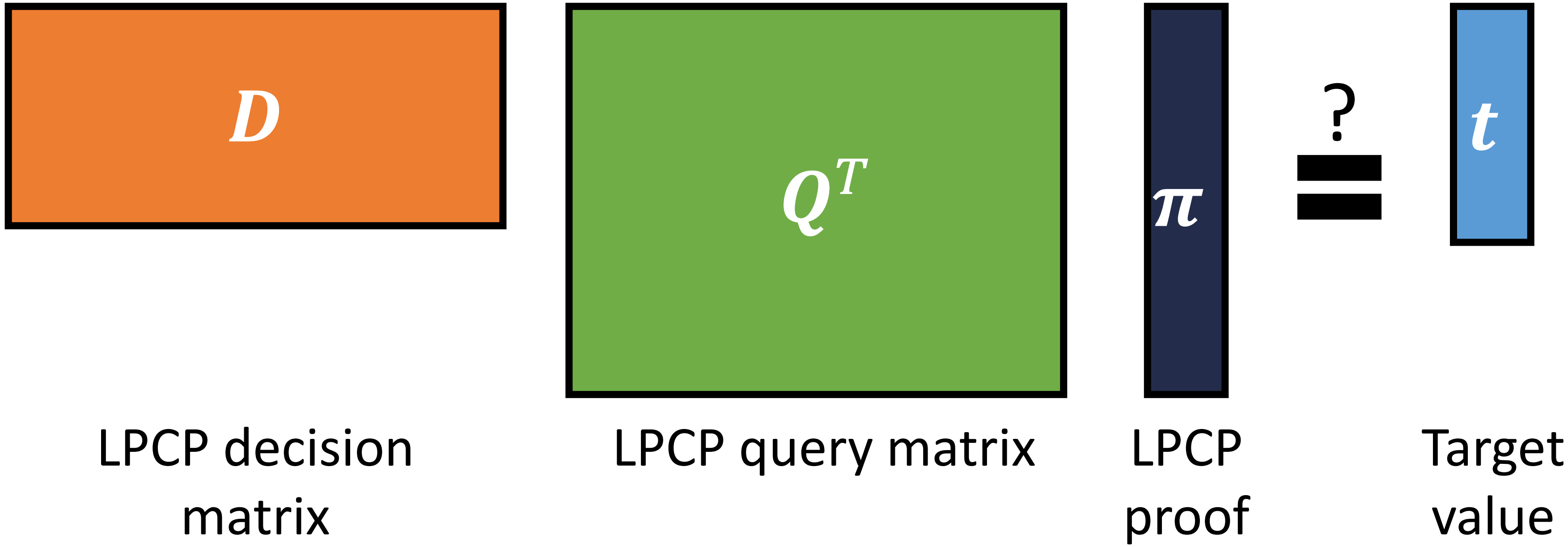
Achieving Negligible Soundness Error

Can we construct a 1-query linear PCP with a <u>linear</u> decision procedure?

[Gro16]: linear PCP with linear decision procedure is <u>impossible</u> (for hard languages)

but only if… *the underlying linear PCP has negligible completeness error*

Main intuition: if decision procedure is linear:



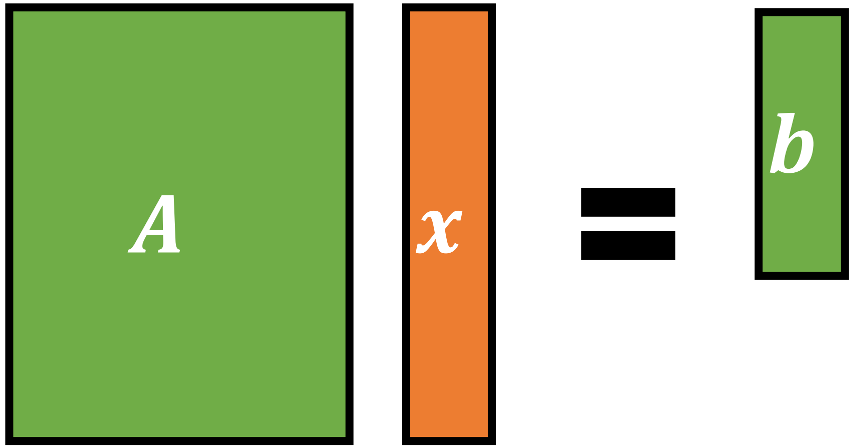
- **True statement:** satisfying π exists for all valid Q
- **False statement:** by union bound, no satisfying π for sufficiently many $Q_1, \dots, Q_\ell$

Linear PCPs from Hardness of Approximation

Can we construct a 1-query linear PCP with a linear decision procedure?

Implication of [Gro16]: LPCP with linear decision procedure must rely on imperfect completeness

This work: leverage hardness of approximation results to design new LPCPs

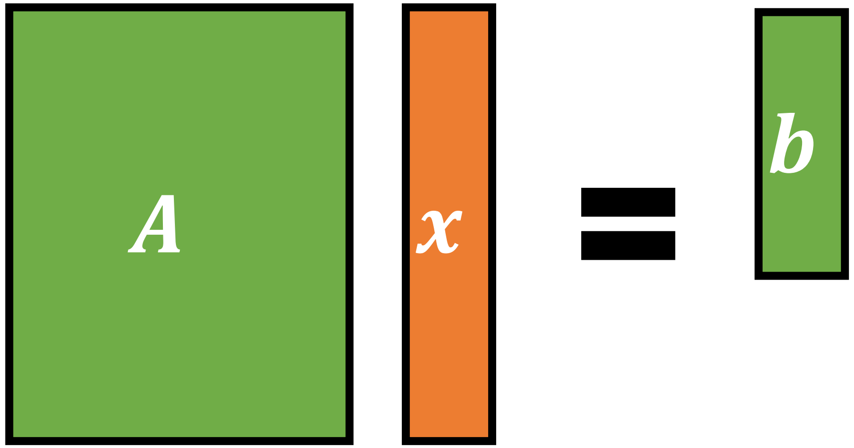


Given $\boldsymbol{A} \in \mathbb{F}^{m\times n}$ *and vector* $\boldsymbol{b} \in \mathbb{F}^{m}$*, find a sparse solution* $\boldsymbol{x} \in \mathbb{F}^{n}$ *where* $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$

Low Hamming weight
(number of nonzero entries)

Minimal weight solution problem (MWSP)

Linear PCP for GapMWSP



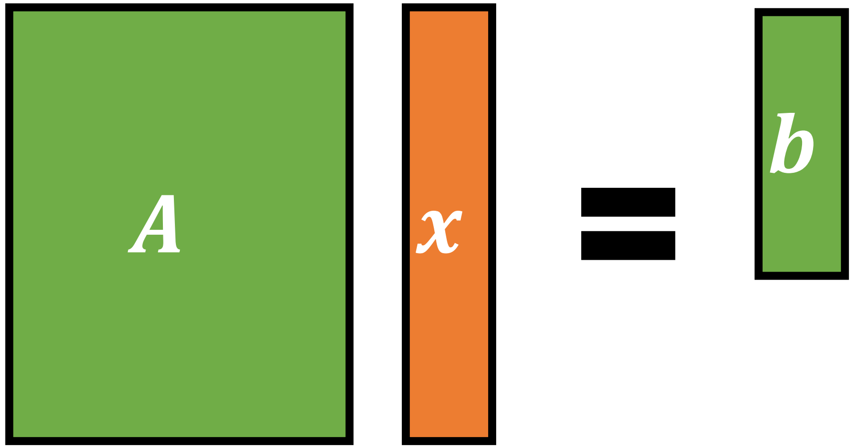
Given $\boldsymbol{A} \in \mathbb{F}^{m \times n}$ *and vector* $\boldsymbol{b} \in \mathbb{F}^{m}$*, find a sparse solution* $\boldsymbol{x} \in \mathbb{F}^{n}$ *where* $\boldsymbol{Ax} = \boldsymbol{b}$

$\mathbf{GapMWSP}_{\boldsymbol{\beta}}$**:**

- **YES instance** $(\boldsymbol{A}, \boldsymbol{b}, d)$: there exists $\boldsymbol{x}$ with weight $\leq d$ such that $\boldsymbol{Ax} = \boldsymbol{b}$
- **NO instance** $(\boldsymbol{A}, \boldsymbol{b}, d)$: all $\boldsymbol{x}$ where $\boldsymbol{Ax} = \boldsymbol{b}$ have weight $\geq \beta d$

Adaptation of [HKLT19]: $\mathrm{GapMWSP}_{\beta}$ is NP-hard for $\beta = \log^{c} n$ and field $\mathbb{F}$ where $\log|\mathbb{F}| = \mathrm{poly}(n)$

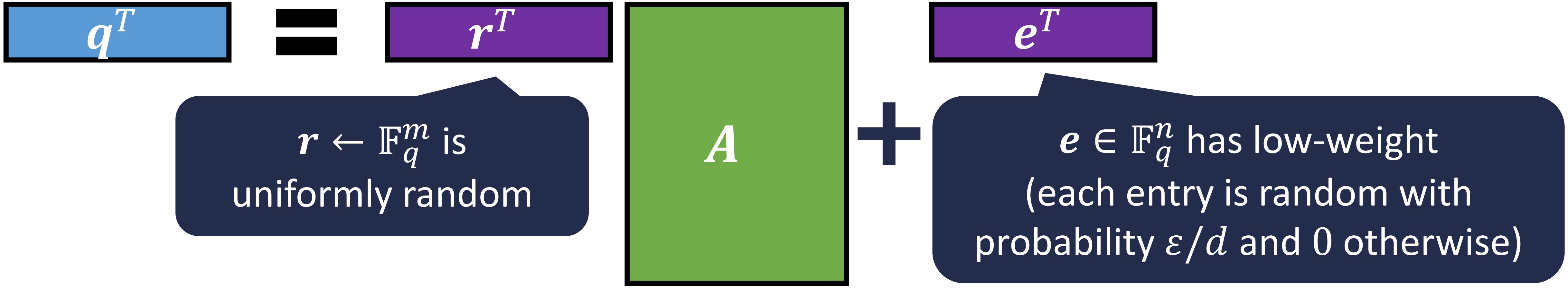
Linear PCP for GapMWSP



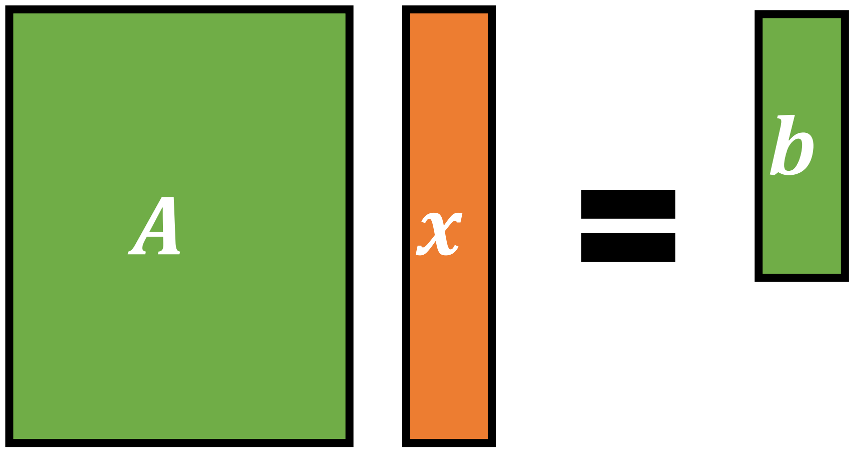
GapMWSP$_\beta$:

- **YES instance:** there exists x with weight $\leq d$ such that $Ax = b$
- **NO instance:** all x where $Ax = b$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of A



Linear PCP for GapMWSP



GapMWSP$_\beta$:

- **YES instance:** there exists $\boldsymbol{x}$ with weight $\leq d$ such that $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$
- **NO instance:** all $\boldsymbol{x}$ where $\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$)

Verification: accept if response a satisfies $a = \boldsymbol{r}^T\boldsymbol{b}$

YES instance:

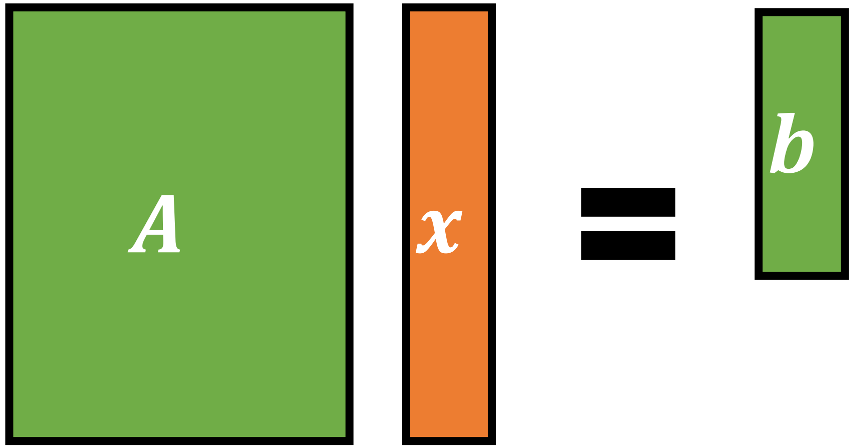
$$\boldsymbol{q}^T\boldsymbol{x} = \boldsymbol{r}^T\boldsymbol{A}\boldsymbol{x} + \boldsymbol{e}^T\boldsymbol{x} = \boldsymbol{r}^T\boldsymbol{b}$$

Suppose density of $\boldsymbol{e}$ is ε/d:

$$\Pr[\boldsymbol{e}^T\boldsymbol{x} = 0] \geq (1 - \varepsilon/d)^d \geq 1 - \varepsilon$$

completeness error ε

Linear PCP for GapMWSP



GapMWSP$_\beta$:

- **YES instance:** there exists x with weight $\leq d$ such that $Ax = b$
- **NO instance:** all x where $Ax = b$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of A

$$q^T = r^T A + e^T$$

Proof: low-weight solution x ($Ax = b$)

Verification: accept if response a satisfies $a = r^T b$

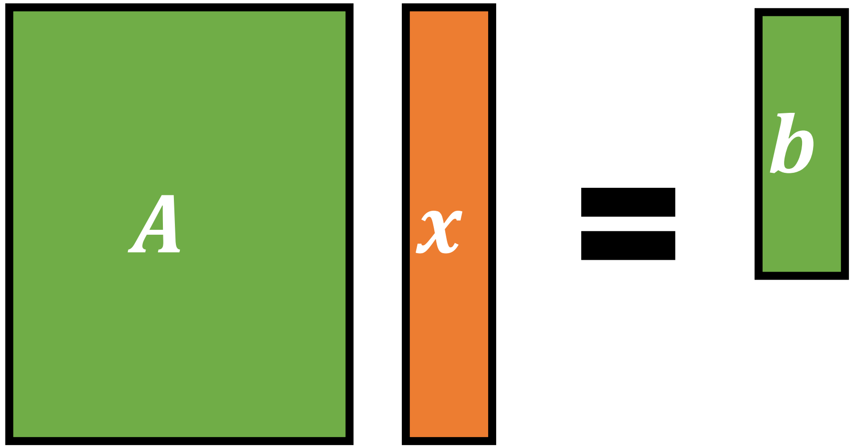
NO instance:

$$q^T x = r^T A x + e^T x = r^T b$$

Case 1: $Ax \neq b$

$r^T A x$ is uniform, so verifier accepts with probability at most $1/\mathbb{F}$

Linear PCP for GapMWSP



GapMWSP$_\beta$:

- **YES instance:** there exists $\boldsymbol{x}$ with weight $\leq d$ such that $\boldsymbol{Ax} = \boldsymbol{b}$
- **NO instance:** all $\boldsymbol{x}$ where $\boldsymbol{Ax} = \boldsymbol{b}$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T \boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{Ax} = \boldsymbol{b}$)

Verification: accept if response a satisfies $a = \boldsymbol{r}^T \boldsymbol{b}$

NO instance:

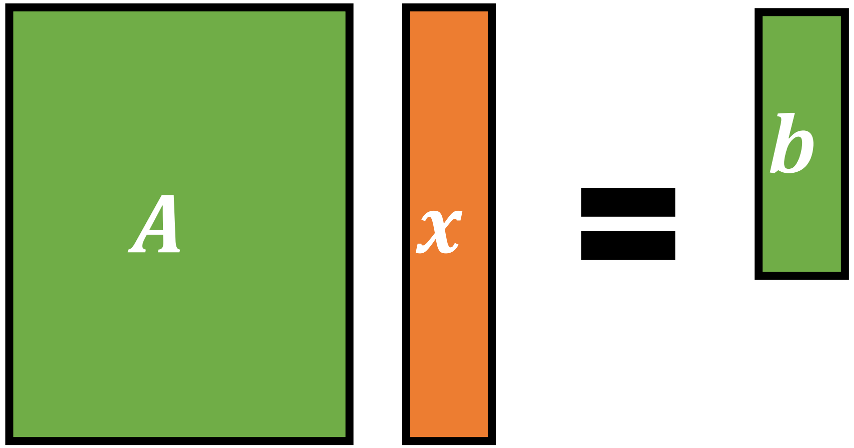
$$\boldsymbol{q}^T \boldsymbol{x} = \boldsymbol{r}^T \boldsymbol{Ax} + \boldsymbol{e}^T \boldsymbol{x} = \boldsymbol{r}^T \boldsymbol{b}$$

Case 2: $\boldsymbol{Ax} = \boldsymbol{b}$, weight$(\boldsymbol{x}) \geq \beta d$

$$\boldsymbol{e}^T \boldsymbol{x} = 0 \text{ with probability } \left(1 - \frac{\varepsilon}{d}\right)^{\beta d} \leq e^{-\beta\varepsilon}$$

negligible when $\varepsilon\beta = \omega(\log n)$

Linear PCP for GapMWSP



GapMWSP$_\beta$:

- **YES instance:** there exists x with weight $\leq d$ such that $Ax = b$
- **NO instance:** all x where $Ax = b$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{Ax} = \boldsymbol{b}$)

Verification: accept if response a satisfies $a = \boldsymbol{r}^T\boldsymbol{b}$

1-query linear PCP for NP with

- $o(1)$ completeness error
- negligible soundness error
- linear decision procedure

ElGamal is linear-only $\Rightarrow$ laconic argument for NP with negligible soundness where $|\pi| = 2|\mathbb{G}|$

Witness Encryption

[GGSW13]

Encrypt a message m *to a statement* x *(for NP language* $\mathcal{L}$*)*

Decrypt ciphertext ct *with any valid witness* w

Security: if $x \notin \mathcal{L}$, then ct provides semantic security

A “hub” for many cryptographic notions: PKE, IBE, ABE, etc. (“lightweight obfuscation”)

Existing constructions rely on indistinguishability obfuscation [GGHRSW13], multilinear maps [GGSW13, CVW18], or new algebraic structures [BIJMSZ20]

From Soundness to Confidentiality

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$)

Verification: accept if response a satisfies $a = \boldsymbol{r}^T\boldsymbol{b}$

Linear PCP is "predictable"

Verifier accepts only one response (that is known to verifier a priori)

[FNV17]: predictable arguments for $\mathcal{L} \Rightarrow$ witness encryption for $\mathcal{L}$

Idea: for $x \notin \mathcal{L}$, accepting response must be unpredictable (soundness) $\Rightarrow$ encrypt a message using a hard-core bit derived from the response

Predictable Argument from Hardness of Approximation

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ $(\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b})$

Verification: accept if response a satisfies $a = \boldsymbol{r}^T\boldsymbol{b}$

Linear PCP is "predictable"

Verifier accepts only one response (that is known to verifier a priori)

$$\text{Predictable linear PCP} \overset{?}{\Rightarrow} \text{Predictable argument}$$

Current compiler (encrypting with ElGamal) does <u>not</u> yield a predictable argument:

Proof is an <u>encryption</u> of the predicted linear PCP response

Predictable Argument from Hardness of Approximation

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T \boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{A}\boldsymbol{x} = \boldsymbol{b}$)

Verification: accept if response a satisfies
$a = \boldsymbol{r}^T \boldsymbol{b}$

Linear PCP is "predictable"

Verifier accepts only one response (that is known to verifier a priori)

Approach: instead of encrypting $\boldsymbol{q}^T$, directly encode it in the exponent

$$g^{\boldsymbol{q}^T} \quad \longleftarrow$$

$$g^{\boldsymbol{q}^T \boldsymbol{x}} = g^{\boldsymbol{r}^T \boldsymbol{b} + \boldsymbol{e}^T \boldsymbol{x}} \quad \longrightarrow$$

Accepting response: $g^{\boldsymbol{r}^T \boldsymbol{b}}$

Predictable Argument from Hardness of Approximation

Query: noisy linear combination of rows of $\boldsymbol{A}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T \boldsymbol{A} + \boldsymbol{e}^T$$

Proof: low-weight solution $\boldsymbol{x}$ ($\boldsymbol{Ax} = \boldsymbol{b}$)

Verification: accept if response a satisfies $a = \boldsymbol{r}^T \boldsymbol{b}$

Linear PCP is "predictable"

Verifier accepts only one response (that is known to verifier a priori)

Approach: instead of encrypting $\boldsymbol{q}^T$, directly

Problem: Does not hide $\boldsymbol{q}^T$ (and in particular, $\boldsymbol{e}^T$)

If there is low-weight $\boldsymbol{x}$ such that $\boldsymbol{Ax} = 0$, then adversary learns $g^{\boldsymbol{e}^T \boldsymbol{x}}$

$g^{\boldsymbol{q}^T}$

$g^{\boldsymbol{q}^T \boldsymbol{x}} = g^{\boldsymbol{r}^T \boldsymbol{b} +}$

Predictable Argument from Hardness of Approximation

Need to "rule out" low-weight solutions to homogeneous system

Minimum distance problem (MDP):

Given a matrix $\boldsymbol{G} \in \mathbb{F}^{m \times n}$, find the minimal distance (under Hamming metric) of the code generated by $\boldsymbol{G}$

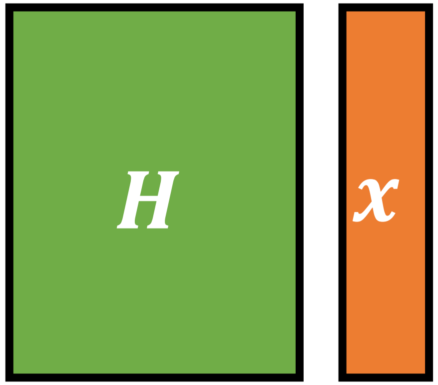
$\mathbf{GapMDP}_{\boldsymbol{\beta}}$:

- **YES instance $(\boldsymbol{G}, d)$:** minimal distance of code generated by $\boldsymbol{G}$ is $\leq d$
- **NO instance $(\boldsymbol{G}, d)$:** minimal distance of code generated by $\boldsymbol{G}$ is $\geq \beta d$

In terms of parity-check matrix $\boldsymbol{H}$ for $\boldsymbol{G}$:

minimal distance of $\boldsymbol{G}$ is $d \Leftrightarrow \exists \boldsymbol{x}: \boldsymbol{H}\boldsymbol{x} = \boldsymbol{0}$ where $\boldsymbol{x}$ has weight d

Predictable Argument from Hardness of Approximation



GapMDP$_\beta$:

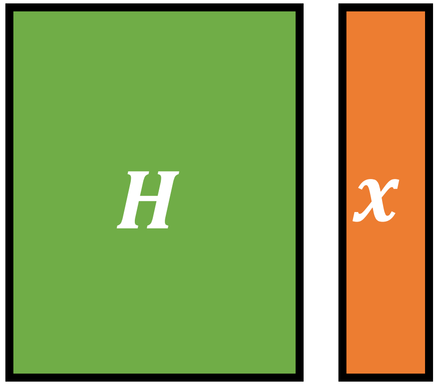
- **YES instance** (H, d): there exists $x \neq 0$ with weight $\leq d$ such that $Hx = 0$
- **NO instance** (H, d): all x where $Hx = 0$ have weight $\geq \beta \cdot d$

Hardness of GapMDP$_\beta$:

- NP-hard when $\beta = O(1)$ and $|\mathbb{F}| = \text{poly}(n)$ [DMS99]
- SAT reduces to GapMDP in <u>quasi-polynomial</u> time when $\beta = \omega(\log n)$ and $|\mathbb{F}| = \text{poly}(n)$ [CW09, AK14]

Hypothesis: SAT reduces to GapMDP_β in <u>polynomial</u> time when $\beta = \omega(\log n)$ and $|\mathbb{F}| = n^{\omega(1)}$

Predictable Argument from Hardness of Approximation



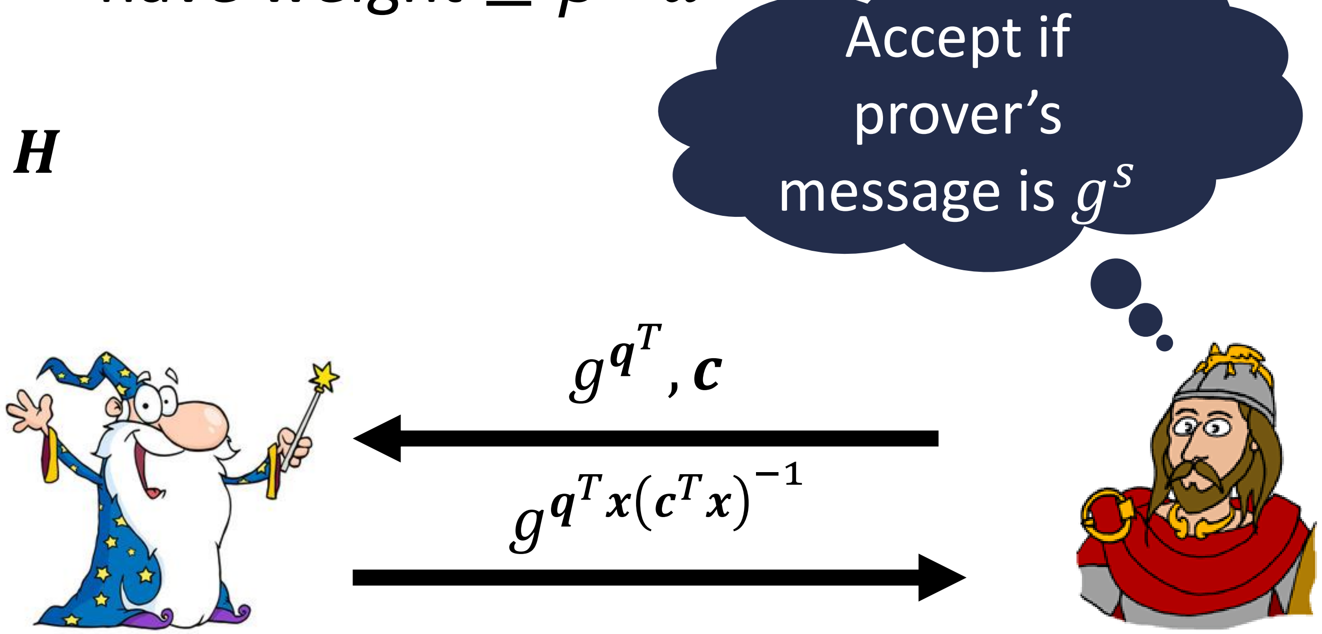
GapMDP$_\beta$:

- **YES instance** $(\boldsymbol{H}, d)$: there exists $\boldsymbol{x} \neq 0$ with weight $\leq d$ such that $\boldsymbol{Hx} = 0$
- **NO instance** $(\boldsymbol{H}, d)$: all $\boldsymbol{x}$ where $\boldsymbol{Hx} = 0$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{H}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{H} + \boldsymbol{e}^T + s\boldsymbol{c}^T$$

$\boldsymbol{r}$: uniformly random
$\boldsymbol{e}$: low-weight vector (with density ε/d)
$s, \boldsymbol{c}$: uniformly random



Predictable Argument from Hardness of Approximation

Completeness: $\boldsymbol{Hx} = 0$

$$\boldsymbol{q}^T\boldsymbol{x} = \boldsymbol{r}^T\boldsymbol{H}\boldsymbol{x} + \boldsymbol{e}^T\boldsymbol{x} + s\boldsymbol{c}^T\boldsymbol{x} = s\boldsymbol{c}^T\boldsymbol{x}$$

$\boldsymbol{e}^T\boldsymbol{x} = 0$ with probability at least $(1 - \varepsilon/d)^d \geq 1 - \varepsilon$

$\mathbf{GapMDP}_{\boldsymbol{\beta}}$:

- **YES instance** $(\boldsymbol{H}, d)$: there exists $\boldsymbol{x} \neq 0$ with weight $\leq d$ such that $\boldsymbol{Hx} = 0$
- **NO instance** $(\boldsymbol{H}, d)$: all $\boldsymbol{x}$ where $\boldsymbol{Hx} = 0$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{H}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T\boldsymbol{H} + \boldsymbol{e}^T + s\boldsymbol{c}^T$$

$\boldsymbol{r}$: uniformly random
$\boldsymbol{e}$: low-weight vector (with density ε/d)
$s, \boldsymbol{c}$: uniformly random

$\longleftarrow g^{\boldsymbol{q}^T}, \boldsymbol{c}$

$\longrightarrow g^{\boldsymbol{q}^T\boldsymbol{x}(\boldsymbol{c}^T\boldsymbol{x})^{-1}}$

Accept if prover's message is g^s

Predictable Argument from Hardness of Approximation

Soundness: if $\mathbb{G}$ is modeled as a generic group, then prover's message is always $g^{\alpha \boldsymbol{q}^T \boldsymbol{z}}$ for some $\alpha \in \mathbb{F}, \boldsymbol{z} \in \mathbb{F}^n$

Case 1: $\boldsymbol{H}\boldsymbol{z} \neq 0$: $\boldsymbol{r}^T \boldsymbol{H}\boldsymbol{z}$ is random (over choice of $\boldsymbol{r}$)
Case 2: $\boldsymbol{H}\boldsymbol{z} = 0$: $\boldsymbol{e}^T \boldsymbol{z}$ is random (over choice of $\boldsymbol{e}$)

$\text{GapMDP}_{\boldsymbol{\beta}}$:

- **YES instance** $(\boldsymbol{H}, d)$: there exists $\boldsymbol{x} \neq 0$ with weight $\leq d$ such that $\boldsymbol{H}\boldsymbol{x} = 0$
- **NO instance** $(\boldsymbol{H}, d)$: all $\boldsymbol{x}$ where $\boldsymbol{H}\boldsymbol{x} = 0$ have weight $\geq \beta \cdot d$

Query: noisy linear combination of rows of $\boldsymbol{H}$

$$\boldsymbol{q}^T = \boldsymbol{r}^T \boldsymbol{H} + \boldsymbol{e}^T + s\boldsymbol{c}^T$$

$\boldsymbol{r}$: uniformly random
$\boldsymbol{e}$: low-weight vector (with density ε / d)
$s, \boldsymbol{c}$: uniformly random

Accept if prover's message is g^s

$\xleftarrow{\quad g^{\boldsymbol{q}^T}, \boldsymbol{c} \quad}$

$\xrightarrow{\quad g^{\boldsymbol{q}^T \boldsymbol{x} (\boldsymbol{c}^T \boldsymbol{x})^{-1}} \quad}$

Witness Encryption from Hardness of Approximation

$$\xleftarrow{\;g^{\boldsymbol{q}^T}, \boldsymbol{c}\;}$$

$$\xrightarrow{\;g^{\boldsymbol{q}^T\boldsymbol{x}(\boldsymbol{c}^T\boldsymbol{x})^{-1}}\;}$$

Implies a predictable laconic argument for GapMDP_β in the generic group model

Hypothesis: SAT reduces to GapMDP in <u>polynomial</u> time when $\beta = \omega(\log n)$ and $|\mathbb{F}| = n^{\omega(1)}$

Corollary: Under this hypothesis, there exists:

- a predictable laconic argument for NP in the generic group model with proof size $|\mathbb{G}|$
- a witness encryption scheme for NP in the generic group model

Witness Encryption from Hardness of Approximation

Hypothesis: SAT reduces to GapMDP_β in <u>polynomial</u> time when $\beta = \omega(\log n)$ and $|\mathbb{F}| = n^{\omega(1)}$

Corollary: Under this hypothesis, there exists:

- a predictable laconic argument for NP in the generic group model with proof size $|\mathbb{G}|$
- a witness encryption scheme for NP in the generic group model

Implications:

- Our hypothesis may be proven in the future (no known barriers to doing so) ⇒ there exists an <u>unconditional</u> construction of witness encryption in the generic group model
- Ruling out witness encryption in the generic group model ⇒ falsify this hypothesis
  - Impossibility results known in the generic group model known for IBE [PRV12] and indistinguishability obfuscation [MMNPs16]

Witness Encryption from Hardness of Approximation

Hypothesis: SAT reduces to GapMDP_β in polynomial time when $\beta = \omega(\log n)$ and $|\mathbb{F}| = n^{\omega(1)}$

Corollary: Under this hypothesis, there exists:

- a predictable laconic argument for NP in the generic group model with proof size $|\mathbb{G}|$
- a witness encryption scheme for NP in the ge

> **More generally:** any argument where the proof consists of a single group element and the verification procedure is a *generic* algorithm ⇒ predictable argument

Implications:

- Our hypothesis may be proven in the future (
  exists an unconditional construction of witnes
- Ruling out witness encryption in the generic group model ⇒ falsify this hypothesis
  - Impossibility results known in the generic group model known for IBE [PRV12] and indistinguishability obfuscation [MMNPs16]

Summary of Results

Construction	Group Type	Proof Size	Information-Theoretic Building Block	Soundness Error	Completeness Error	Argument Type
[Gro16]	bilinear	$2\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert$	linear PCP	$\mathrm{negl}(\lambda)$	0	SNARG
[BCIOP13]	linear	$8\lvert\mathbb{G}\rvert$	linear PCP	$1/\mathrm{poly}(\lambda)$	0	dvSNARG
[BCIOP13]	linear	$2\lvert\mathbb{G}\rvert$	PCP	$1/\mathrm{poly}(\lambda)$	0	dvSNARG
This work	linear	$2\lvert\mathbb{G}\rvert$	linear PCP	$1/\mathrm{poly}(\lambda)$	$\mathrm{negl}(\lambda)$	dvSNARG
This work	linear	$2\lvert\mathbb{G}\rvert$	PCP	$\mathrm{negl}(\lambda)$	$o(1)$	laconic argument
This work	linear	$\lvert\mathbb{G}\rvert$	PCP	$\mathrm{negl}(\lambda)$	$o(1)$	laconic argument

- Relies on a new hypothesis on the hardness of approximation of the minimal distance of linear codes
- Under the same hypothesis, implies a <u>witness encryption</u> scheme for NP in the generic group model

Open Problems

Unconditional construction of witness encryption in the generic group model

- Show NP-hardness of GapMDP for our parameter regime
- Compile predictable linear PCP into predictable argument
- (VBB) obfuscate linear PCP verification (affine tester)

Concretely-efficient 2-element SNARGs with sub-quadratic prover overhead

2-element laconic arguments with perfect completeness

Thank you!

`https://eprint.iacr.org/2020/1319`