Quantum Rewinding for Many-Round Protocols

Nick Spooner, University of Warwick

TCC 2022, Chicago

Joint work with Russell Lai and Giulio Malavolta

"Lattice bulletproofs" [BLNS20, AL21, ACK21]

$A \leftarrow^{\$} \mathcal{R}^{h\times N}$ "wide" matrix

A

Succinct PoK of SIS preimage: short x such that $y = Ax$

x

$P(A, x, y)$ $\qquad$ $V(A, y)$

$\alpha \leftarrow^{\$} \mathcal{C} \subseteq \mathcal{R}$ $\longleftarrow$

$A' := A_L + \alpha A_R \in \mathcal{R}^{h\times N/2}$

$x' = \alpha x_L + x_R \in \mathcal{R}^{N/2}$ $\qquad$ $x', A_L x_R, A_R x_L$ $\longrightarrow$

$$A'x' = \alpha y + A_L x_R + \alpha^2 A_R x_L = y'$$

Recurse $t = \log N$ times; total communication $O(\log N)$

Our main result

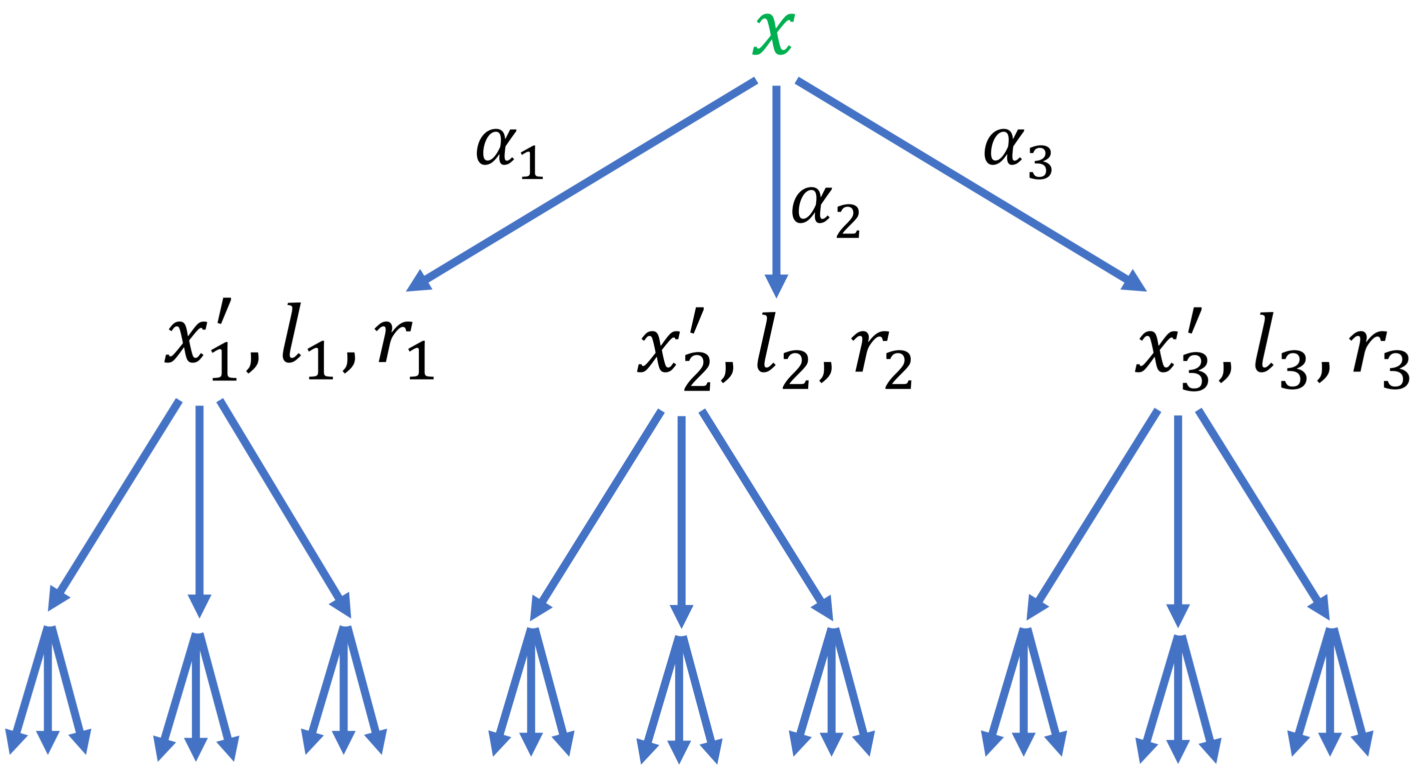
Theorem. Lattice bulletproofs is a **post-quantum** PoK of a SIS preimage, assuming quantum hardness of RLWE

(Prior reductions only for **classical** adversaries)

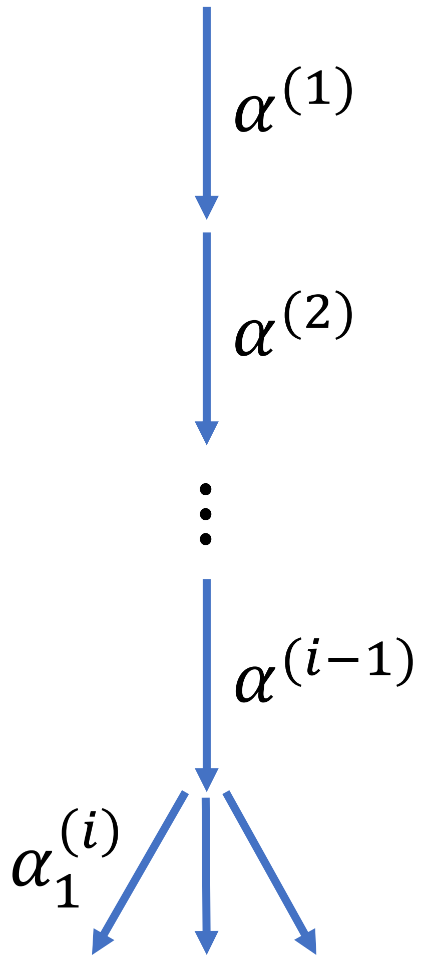
1. New soundness notions for multi-round protocols:
   recursive special soundness and *last-round collapsing*
2. We give a novel *quantum rewinding* algorithm for any protocol satisfying both properties
3. We show that lattice bulletproofs satisfies both properties, assuming QRLWE

Classical PoK: tree special soundness

$A \in \mathcal{R}^{h \times N}, y \in \mathcal{R}^h$



Classical recursive tree extraction algorithm



$T_i^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$:

Run $(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$

*Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, run $x_i^{(1)} \leftarrow T_{i+1}^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(i)}\right)$

If T_{i+1} outputs “fail”, output “fail”

Else repeat * until 2 more successes

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

$T_{t+1}^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(t)}\right)$:

Run $(x', l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \ldots, \alpha^{(t)}\right)$

If accepting transcript, return (x', l, r), else “fail”

Analysis

$T_i^{\tilde{P}}(\alpha^{(1)}, \dots, \alpha^{(i-1)})$:

Run $(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$

*Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, run $x_i^{(1)} \leftarrow T_{i+1}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i)}\right)$

If T_{i+1} outputs "fail", output "fail"

Else repeat * until 2 more successes

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

$$\mu \coloneqq \Pr[\tilde{P}\ wins]$$

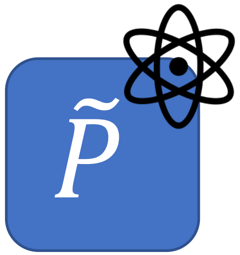
$$\mu(\alpha^{(1)}, \dots, \alpha^{(i-1)}) \coloneqq \Pr_{\alpha^{(i)}, \dots, \alpha^{(t)}}[\tilde{P}\left(\alpha^{(1)}, \dots, \alpha^{(t)}\right) \text{ wins}]$$

$$\Pr\left[T_i^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right) \rightarrow \text{fail}\right] = \mu\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$$

$$\mathbb{E}[\mathrm{Time}(T_i)] \approx \mathbb{E}[\mathrm{Time}(T_{i+1})] \cdot \left(1 + \mu \cdot \frac{2}{\mu}\right) = 3 \cdot \mathbb{E}[\mathrm{Time}(T_{i+1})]$$

$$\mathbb{E}[Time(T_1)] = \mathrm{poly}(\lambda) \cdot 3^{\log N} = \mathrm{poly}(\lambda, N)$$

Why does this fail in the quantum setting?



$T_i^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$:

Run $(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$

*Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, run $x_i^{(1)} \leftarrow T_{i+1}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i)}\right)$

If T_{i+1} outputs “fail”, output “fail”

Else repeat * until 2 more successes

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

By now we have **powerful** techniques for quantum rewinding [CMSZ21, LMS22, CCLY2?]… *why are they not already enough*?

$T_i^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$:

$(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$

$(x_i^{(1)}, x_i^{(2)}, x_i^{(3)}) \leftarrow \mathrm{QRewind}(T_{i+1}^{\tilde{P}})$

If QRewind outputs “fail”, output “fail”

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

Problem: Known QRewinds need T_{i+1} to be **projective**

Usually this is achieved by running T_{i+1} **coherently**

This won’t work here: T_{i+1} is only **expected polytime…**

Fixed polytime extraction, **classically**; first attempt

$T_{i,\varepsilon}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$:

$(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$

Repeat at most $^1/_\varepsilon$ times:

Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, run $x_i \leftarrow T_{i+1,\varepsilon}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i)}\right)$

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

Markov: $T_{i,\varepsilon}$ succeeds w.p. $\mu - N\varepsilon$ so need $\varepsilon \ll \mu$

But running time is $(^1/_\varepsilon)^{\log n} > (^1/_\mu)^{\log n}$ ☹

Fixed polytime extraction, classically

$T_{i,\gamma}^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$:

$(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \ldots, \alpha^{(i-1)}\right)$

Repeat at most ${}^{100\lambda t}/_{\gamma}$ times:

Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, estimate $\gamma' = \mu(\alpha^{(1)}, \ldots, \alpha^{(i)})$

If $\gamma' \geq \gamma(1 - \frac{1}{10t})$, compute $x_i \leftarrow T_{i+1,\gamma'}^{\tilde{P}}\left(\alpha^{(1)}, \ldots, \alpha^{(i)}\right)$

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

Succeeds w.p. $1 - 2^{-\lambda}$

$T_{1,\mu}^{\tilde{P}}$ succeeds w.p. $\Omega(\mu)$

Running time $O\left(3^{\log N} \cdot \frac{\mathrm{poly}(\lambda)}{\mu}\right) = \mathrm{poly}(\lambda, N)$

Quantum extractor via [CMSZ21] measure-and-repair

$T_{i,\gamma}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$:

$(l, r) \leftarrow \tilde{P}\left(\alpha^{(1)}, \dots, \alpha^{(i-1)}\right)$

Repeat at most $^{100\lambda t}/_{\gamma}$ times:

Choose $\alpha^{(i)} \leftarrow \mathcal{C}$, **measure** if $\mu(\alpha^{(1)}, \dots, \alpha^{(\boldsymbol{i})}) \geq \gamma(1 - \frac{1}{10t})$

If yes, measure $x_i \leftarrow T_{i+1,\gamma'}^{\tilde{P}}\left(\alpha^{(1)}, \dots, \alpha^{(i)}\right)$ *projectively* **(*)**

Repair $\mu(\alpha^{(1)}, \dots, \alpha^{(\boldsymbol{i-1})})$ to $\approx \gamma$

Return $x_{i-1} = K(l, r, x_i^{(1)}, x_i^{(2)}, x_i^{(3)})$

Proof idea: (*) is **comp. indistinguishable** from measuring if $\mu\left(\alpha^{(1)}, \dots, \alpha^{(i)}\right) \geq \gamma'$ (requires *last-round collapsing* to undetectably measure x_i)

Thanks!

ePrint 2022/889