Tighter Security Notions for a Modular Approach to Private Circuits

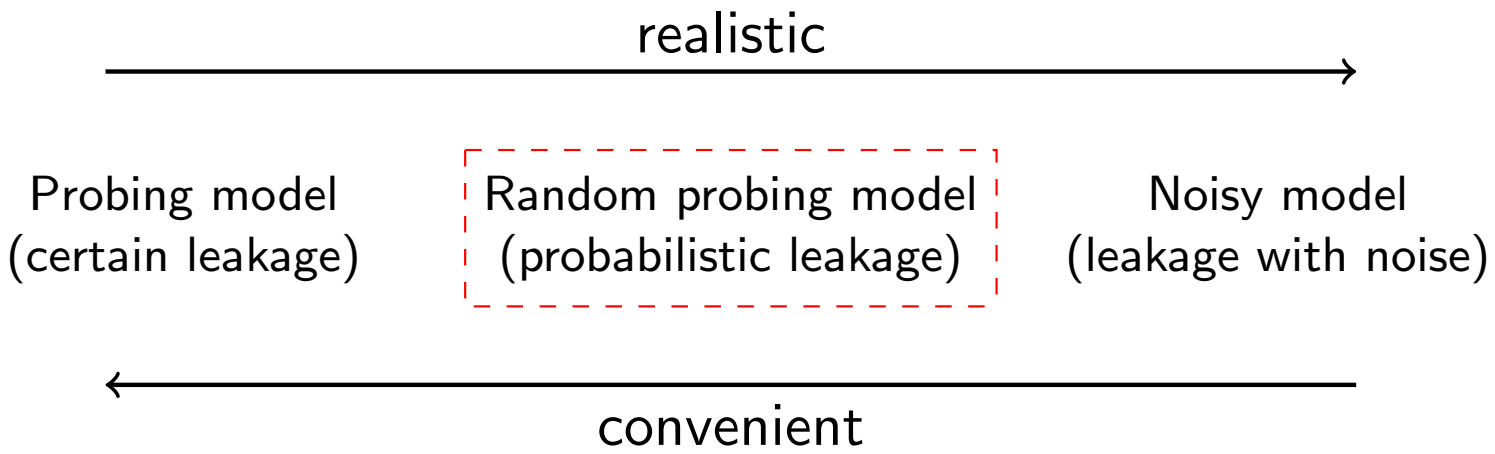
Bohan Wang[1,2], Juelin Zhang[1,2], Yu Yu[3,4] and Weijia Wang[1,2]

[1]Shandong University, [2]Quan Cheng Laboratory, [3]Shanghai Jiao Tong University and [4]Shanghai Qi Zhi Institute

April 30, 2025

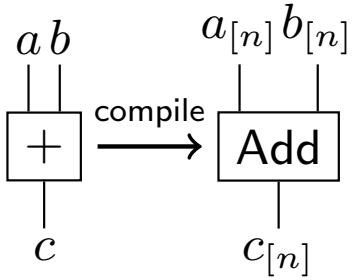
Side-channel Leakage

- Physical leakage $\rightarrow$ Information of wires
- Different models to formally describe leakage.



Masking

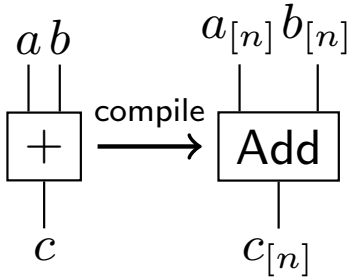
- Split each secret a into $a_{[n]} \stackrel{\text{def}}{=} (a_1, a_2, \ldots, a_n)$.
- Linear masking: $a = \sum_{i \in [1,n]} a_i, b = \sum_{i \in [1,n]} b_i, c = \sum_{i \in [1,n]} c_i$



Add is called an n-share gadget.

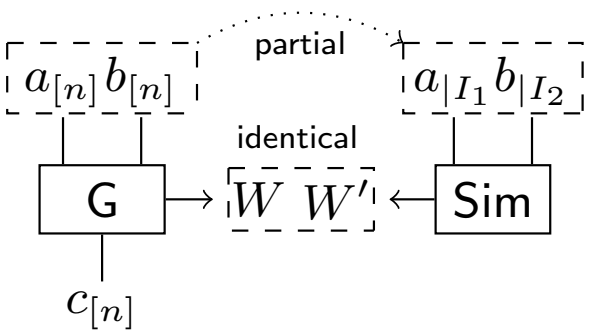
Masking

- Split each secret a into $a_{[n]} \stackrel{\text{def}}{=} (a_1, a_2, \ldots, a_n)$.
- Linear masking: $a = \sum_{i \in [1,n]} a_i, b = \sum_{i \in [1,n]} b_i, c = \sum_{i \in [1,n]} c_i$



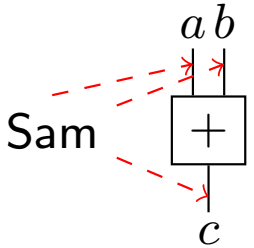
Add is called an n-share gadget.

- Simulation: $I_1, I_2 \subseteq [1, n]$



Random Probing Security (RPS)

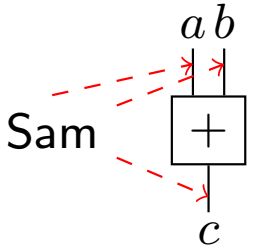
- Each wire is **independently** sampled by the adversary with probability p.
- Sampler $\mathsf{Sam}(C)$



$$\Longrightarrow \quad \mathsf{Sam}(a, b, a+b) = W \rightarrow \begin{cases} \Pr(a \in W) = p \\ \Pr(b \in W) = p \\ \Pr(a+b \in W) = p \end{cases}$$

Random Probing Security (RPS)

- Each wire is **independently** sampled by the adversary with probability p.
- Sampler $\mathsf{Sam}(C)$



$$\Longrightarrow \quad \mathsf{Sam}(a, b, a+b) = W \rightarrow \begin{cases} \Pr(a \in W) = p \\ \Pr(b \in W) = p \\ \Pr(a+b \in W) = p \end{cases}$$

- (p, ϵ)-RPS: For any wire set $W \in \mathbf{W}$ sampled from circuit C, where the sum of leakage probabilities of sets in $\mathbf{W}$ is $1 - \epsilon$, there exists a simulator Sim such that

$$\mathsf{Sim}(a^1_{|I_1}, \ldots, a^\ell_{|I_\ell}) = W$$

where $I_i \subsetneq [1, n]$ for $i \in [1, \ell]$ and $(a^i_{[n]})_{i \in [1,\ell]}$ are input sharings of C.

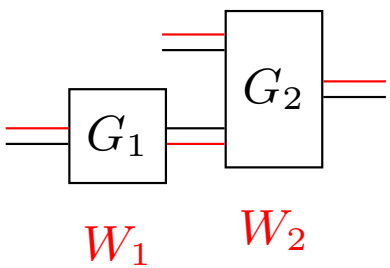
Prior Works

Foundational works

- Failure probability (Belaïd et al., Crypto 2020)
  - ϵ is a polynomial of p;
  - If there are s wires in circuit C and the simulation of wire set W fails (i.e. some $I_i = [1, n]$),

$$f(p) = f(p) + p^{|W|} \cdot (1-p)^{s-|W|} \quad .$$

- (t, f)-Random Probing Composability (RPC) (Belaïd et al., Crypto 2020)
  - Assume constant number (e.g. t) of leaking shares from each output sharing;
  - Require a simulation experiment similar to RPS, but $|I_i| \leqslant t$.

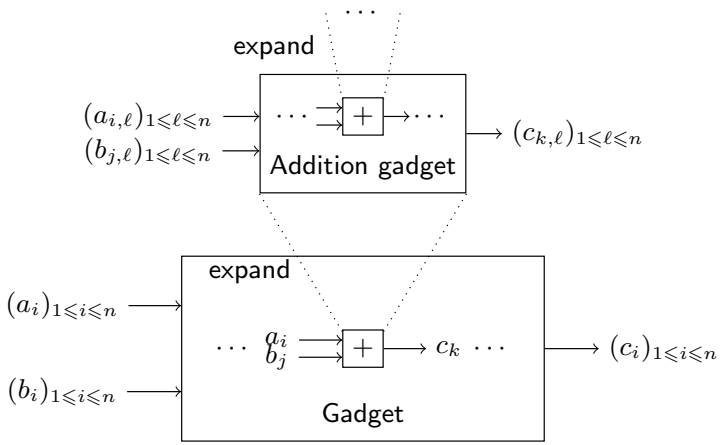


Prior Works

Expansion methods

- The modular approach (Ananth et al., Crypto 2018)
  - Each round of compilation replaces p with ϵ;
  - Arbitrary failure probability is achievable if $\epsilon < p$.

- Random Probing Expandability (RPE) (Belaïd et al., Crypto 2020)
  - Composability;
  - Failed simulation for each input sharing happens **independently**.

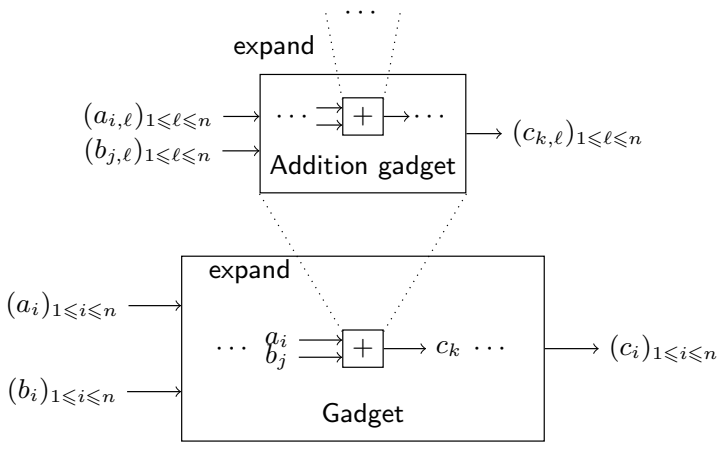


Prior Works

Expansion methods

- The modular approach (Ananth et al., Crypto 2018)
  - Each round of compilation replaces p with ϵ;
  - Arbitrary failure probability is achievable if $\epsilon < p$.

- Random Probing Expandability (RPE) (Belaïd et al., Crypto 2020)
  - Composability;
  - Failed simulation for each input sharing happens **independently**.



- Amplification order (Belaïd et al., Crypto 2020)
  - If the failure probability of gadget G is $f(p) = \sum_{i\in[d,s]} c_i p^i$, d is called the amplification order of G;
  - For a target failure probability $2^{-\kappa}$, a larger d refers to less expansion, leading to lower complexity for the expanded circuit.

Our Contributions

Motivations

- Some wires are inherently correlated to other wire(s).

$$\Pr(c = 0, b = i) \neq \Pr(c = 0) \cdot \Pr(b = i)$$

where $i \in \{0, 1\}$.

a	b	$c = a \cdot b$	Pr
0	0	0	$\frac{3}{4}$
0	1		
1	0		
1	1	1	$\frac{1}{4}$

Our Contributions

Motivations

- Some wires are inherently correlated to other wire(s).

$$\Pr(c = 0, b = i) \neq \Pr(c = 0) \cdot \Pr(b = i)$$

where $i \in \{0, 1\}$.

a	b	$c = a \cdot b$	Pr
0	0	0	$\frac{3}{4}$
0	1		
1	0		
1	1	1	$\frac{1}{4}$

- The independence assumption of RPE is sometimes inefficient.
  - If the initial failure probabilities are respectively

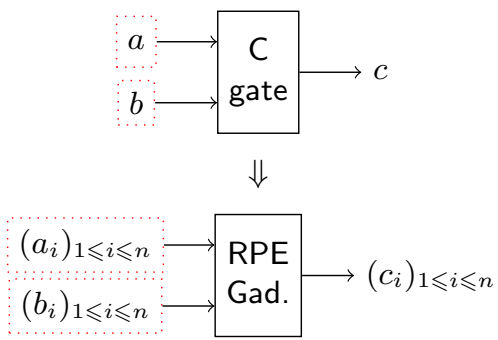
$$\begin{cases} f_a(p) = f_b(p) = \mathcal{O}(p^2) \\ f_{ab}(p) = \mathcal{O}(p^3) \end{cases},$$

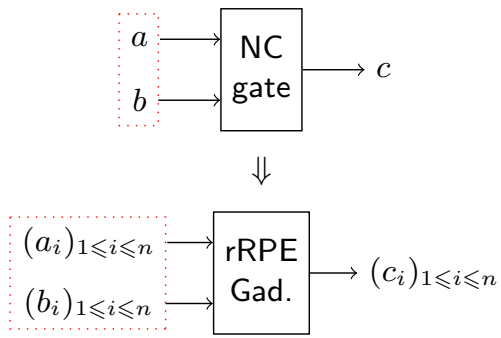
the RPE failure probability for single sharing is $\sqrt{f_{ab}} \approx \mathcal{O}(p^{1.5})$.

Our Contributions

Tighter classifications

- For a gate $\odot$ with uniform input(s),
  - if its output(s) is independent with its input(s), $\odot$ is a Complementary gate (C gate);
  - Otherwise, $\odot$ is Non-Complementary (NC).
- related RPE (rRPE)
  - Similar to RPE;
  - The requirement of independent failure is removed.
- Tighter compilation

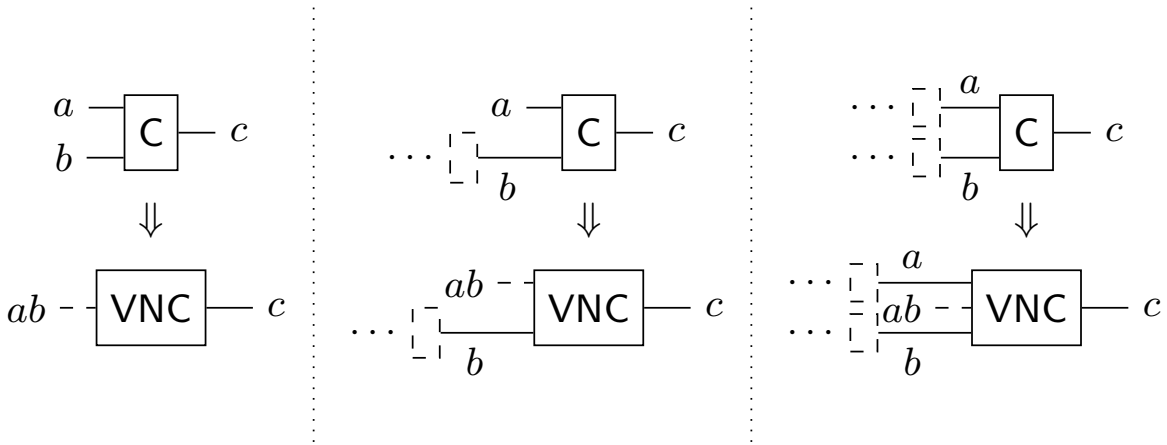




Our Contributions

Wider application for rRPE

- Virtual NC (VNC) gates
  - a gate transformation allowing the rRPE expansion of C gates
  - add a virtual wire for sampler, equivalent to all input wires
  - don't change the functionality of the initial C gate

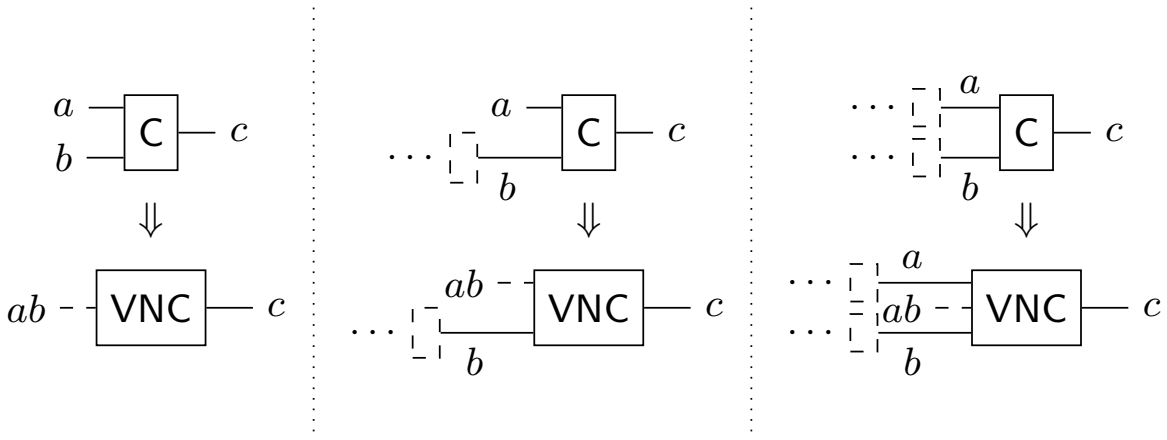


- VNC gates can be expanded by rRPE gadgets directly.

Our Contributions

Wider application for rRPE

- Virtual NC (VNC) gates
  - a gate transformation allowing the rRPE expansion of C gates
  - add a virtual wire for sampler, equivalent to all input wires
  - don't change the functionality of the initial C gate

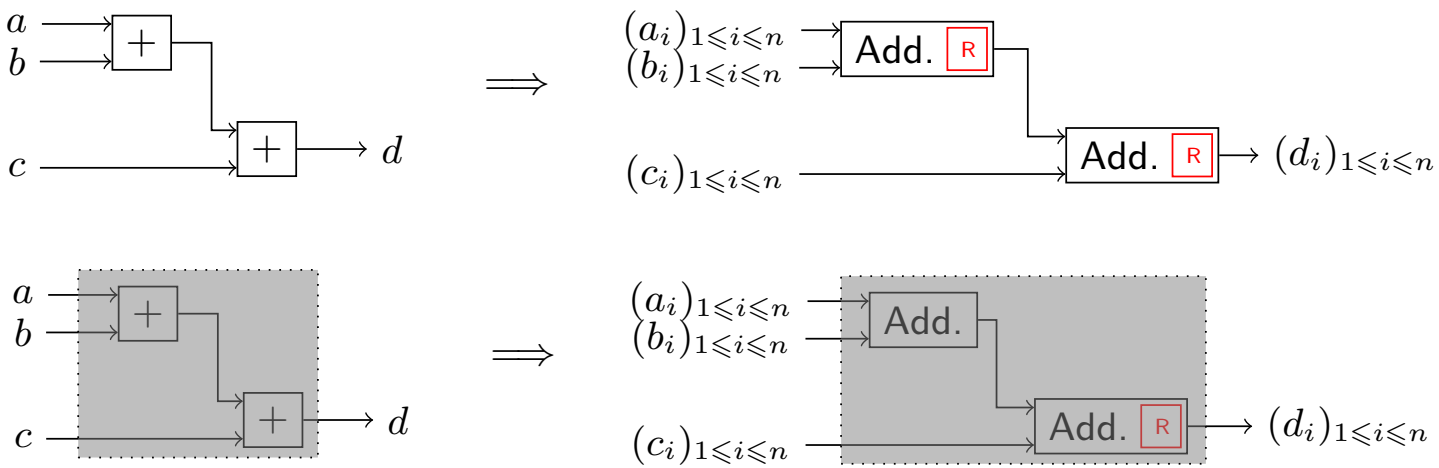


- VNC gates can be expanded by rRPE gadgets directly. $(+ \to \widetilde{+})$

Our Contributions

Further improved expansion method: motivation

- "Composability" demands additional cost for some cases rarely happened;
- It's exponentially harmful to expansion methods;
- Expansion for multiple gates can reduce such redundancy.



Our Contributions

Further improved expansion method: gates

- Half-Complementary gates with dependent sets $A_{[q]}$ ($A_{[q]}$-HC gates)
  - It's composed of C and VNC gates;
  - HC gate is not transformation but a composition of multiple gates;
  - If $|A_i| = 2$, $\beta_{|A_i}$ are the inputs of a VNC gate.

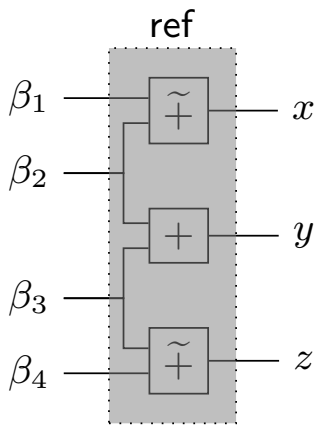
Our Contributions

Further improved expansion method: gates

- Half-Complementary gates with dependent sets $A_{[q]}$ ($A_{[q]}$-HC gates)
  - It's composed of C and VNC gates;
  - HC gate is not transformation but a composition of multiple gates;
  - If $|A_i| = 2$, $\beta_{|A_i}$ are the inputs of a VNC gate.

$$\mathsf{ref}(\beta_{[4]}) = \begin{cases} \beta_1 \widetilde{+} \beta_2 & \to x \\ \beta_2 + \beta_3 & \to y \\ \beta_3 \widetilde{+} \beta_4 & \to z \end{cases} .$$

ref is a $(\{1,2\},\{3,4\})$-HC gate.



Our Contributions

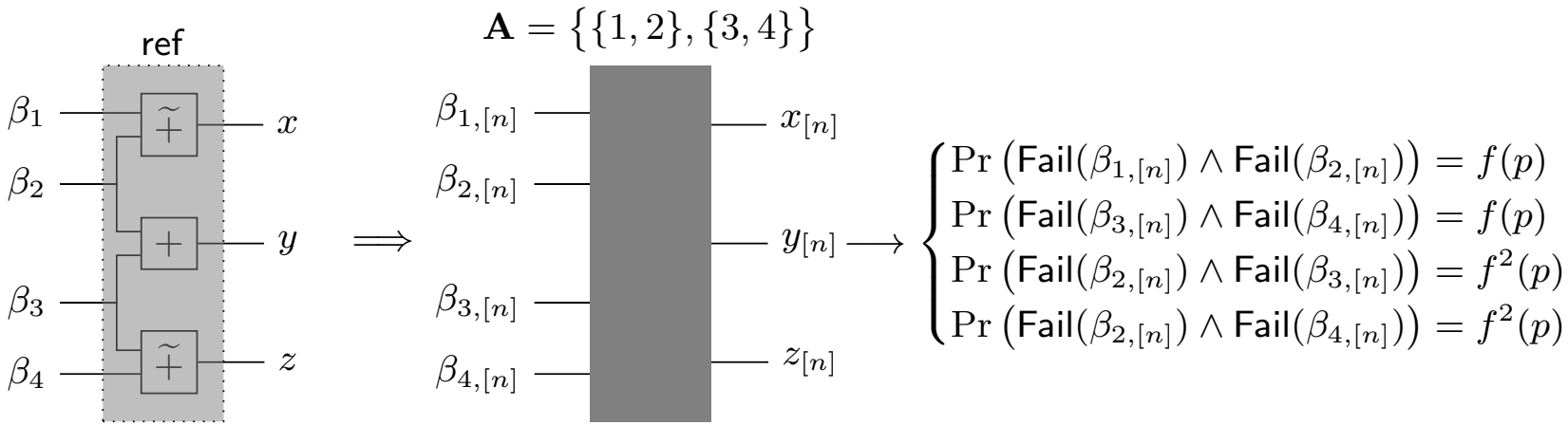
Further improved expansion method: gadgets

- $(t, f, \mathbf{A})$-Multiple inputs RPE (MiRPE)
  - A mixture of RPE and rRPE for gadgets with multiple input sharings.
  - Input sharings with correlated failures correspond to inputs of a VNC gate.
- $(\mathbf{A})$-HC gates could be expanded by $(t, f, \mathbf{A})$-MiRPE.

Our Contributions

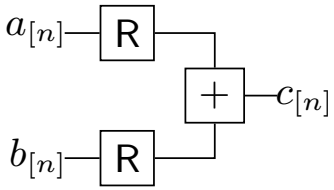
Further improved expansion method: gadgets

- $(t, f, \mathbf{A})$-Multiple inputs RPE (MiRPE)
  - A mixture of RPE and rRPE for gadgets with multiple input sharings.
  - Input sharings with correlated failures correspond to inputs of a VNC gate.
- $(\mathbf{A})$-HC gates could be expanded by $(t, f, \mathbf{A})$-MiRPE.

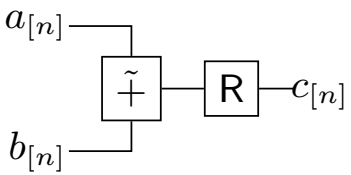


Our Contributions

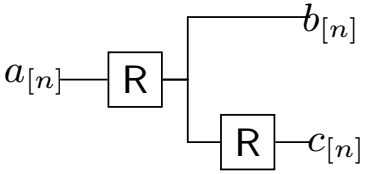
Further improved expansion method: example



RPE Addition

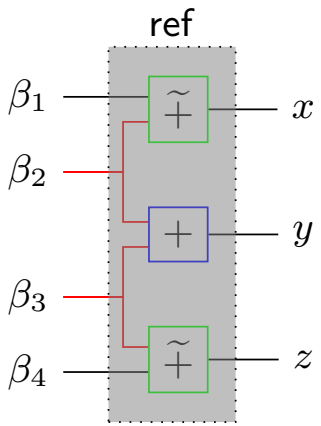


rRPE Addition



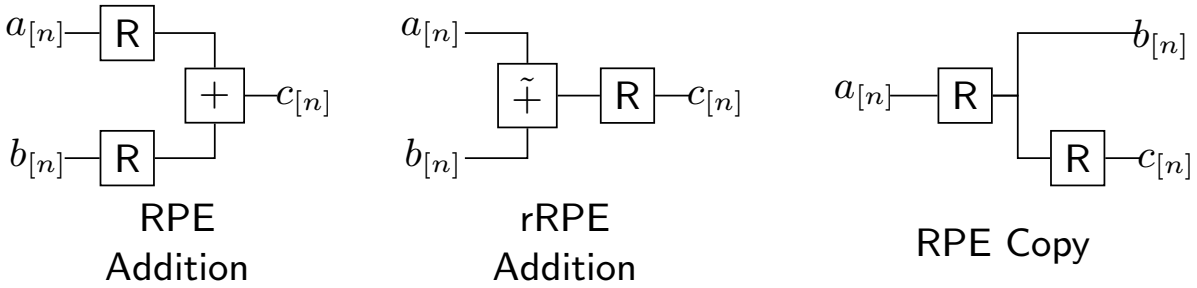
RPE Copy

- A detailed example for the improved expansion
  - R: $\mathcal{O}(n \log n)$ refreshing (Battistello et al., CHES 2016)
  - A trivial expansion of ref needs 2×2+2×1+1×2=8 R.

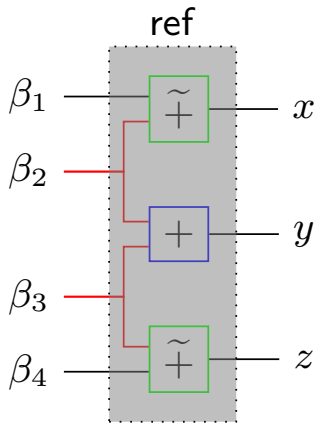


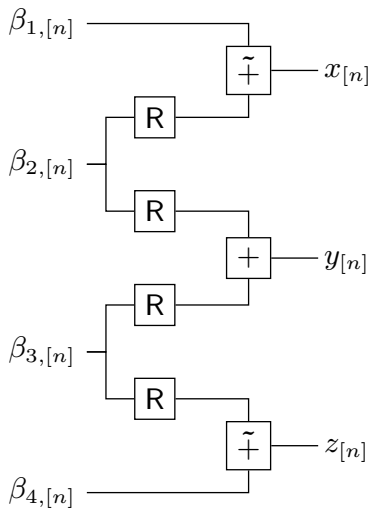
Our Contributions

Further improved expansion method: example



- A detailed example for the improved expansion
  - R: $\mathcal{O}(n \log n)$ refreshing (Battistello et al., CHES 2016)
  - A trivial expansion of ref needs 2×2+2×1+1×2=8 R.
  - The same security is achieved by an MiRPE gadget with 4 R.





Our Contributions

Results

- n-share ISW multiplication algorithm is $(\lfloor \frac{n}{2} \rfloor, f)$-rRPE with amplification order $d = \lfloor \frac{n}{2} \rfloor + 1$ for $n \geqslant 3$.
  - The amplification order is the same as the work proposed at AC21;
  - Multiplication complexity is reduced from $\mathcal{O}(n^2 \log n)$ to $\mathcal{O}(n^2)$.
- Improved circuit compiler with security level $2^{-\kappa}$

	Leakage probability	Complexity	
3-share	$2^{-7.5}$	$\mathcal{O}(s \cdot \kappa^{3.9})$	EC21
	$2^{-6.9}$	$\mathcal{O}(s \cdot \kappa^{3.2})$	Our works
5-share	$[2^{-9.7}, 2^{-7.6}]$	$\mathcal{O}(s \cdot \kappa^{3.2})$	EC21
	$\geqslant 2^{-9.4}$	$\mathcal{O}(s \cdot \kappa^{2.8})$	Our works

Our Contributions

Results

- n-share ISW multiplication algorithm is $(\lfloor \frac{n}{2} \rfloor, f)$-rRPE with amplification order $d = \lfloor \frac{n}{2} \rfloor + 1$ for $n \geqslant 3$.
  - The amplification order is the same as the work proposed at AC21;
  - Multiplication complexity is reduced from $\mathcal{O}(n^2 \log n)$ to $\mathcal{O}(n^2)$.
- Improved circuit compiler with security level $2^{-\kappa}$

	Leakage probability	Complexity	
3-share	$2^{-7.5}$	$\mathcal{O}(s \cdot \kappa^{3.9})$	EC21
	$2^{-6.9}$	$\mathcal{O}(s \cdot \kappa^{3.2})$	Our works
5-share	$[2^{-9.7}, 2^{-7.6}]$	$\mathcal{O}(s \cdot \kappa^{3.2})$	EC21
	$\geqslant 2^{-9.4}$	$\mathcal{O}(s \cdot \kappa^{2.8})$	Our works

Thank you!