PCG Part 4: Pseudorandom Correlation Functions from Paillier

Peter Scholl

26 January 2022, Bar-Ilan University Winter School

Based on joint work with:

Claudio Orlandi and Sophia Yakoubov

AARHUS UNIVERSITY

This week's talks

VOLE 1: introduction, basic protocols & applications

VOLE 2: application to efficient zero knowledge

PCG 1-2

PCG 3: PCGs from LPN: the gory details

PCG 4: PCFs from number-theoretic assumptions

Outline

- PCFs: recap
- A blueprint for PCFs from oblivious ciphertext sampling and share decryption
- Share conversion
  - DDH
  - Paillier & QR
- Public-key PCFs for VOLE and OT
- Non-interactive setup for PCFs

Secure Computation with Preprocessing

[Beaver ’91]

Preprocessing

Correlated randomness

x

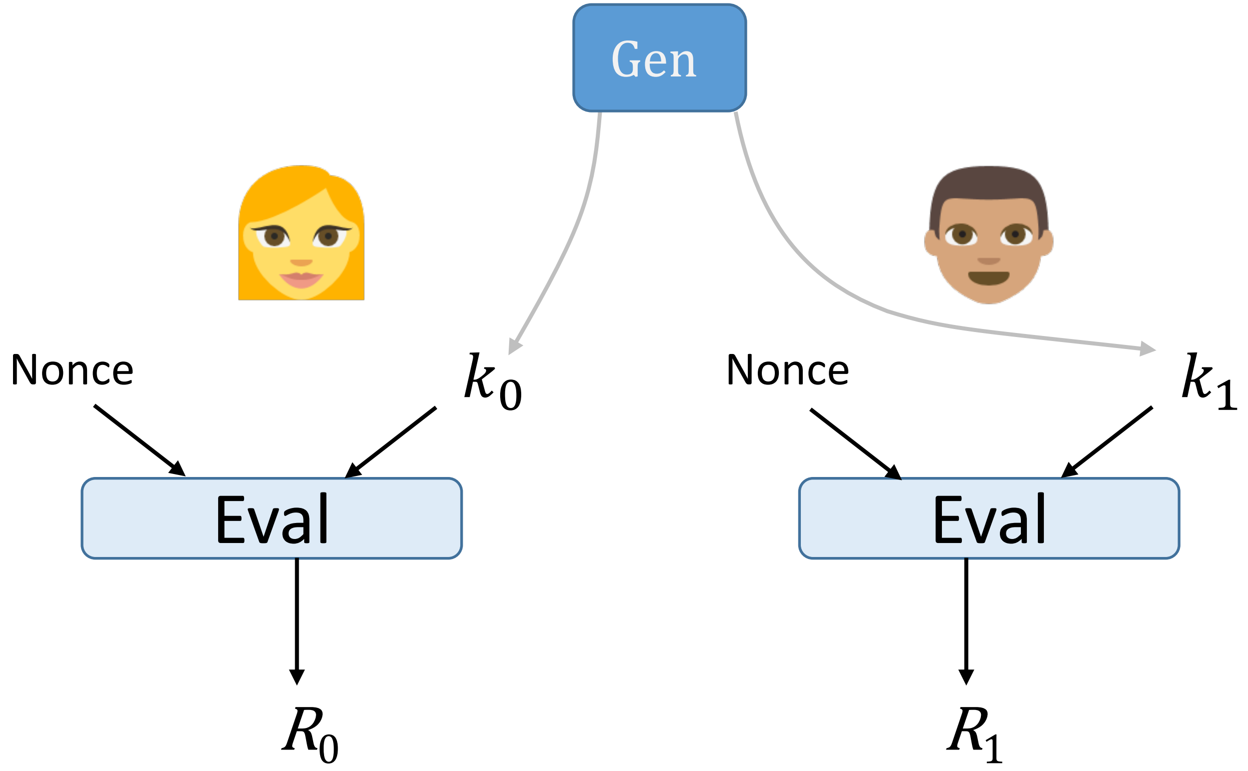
y

Online phase

$f(x, y)$

Pseudorandom Correlation Function

[BCGIKS20]

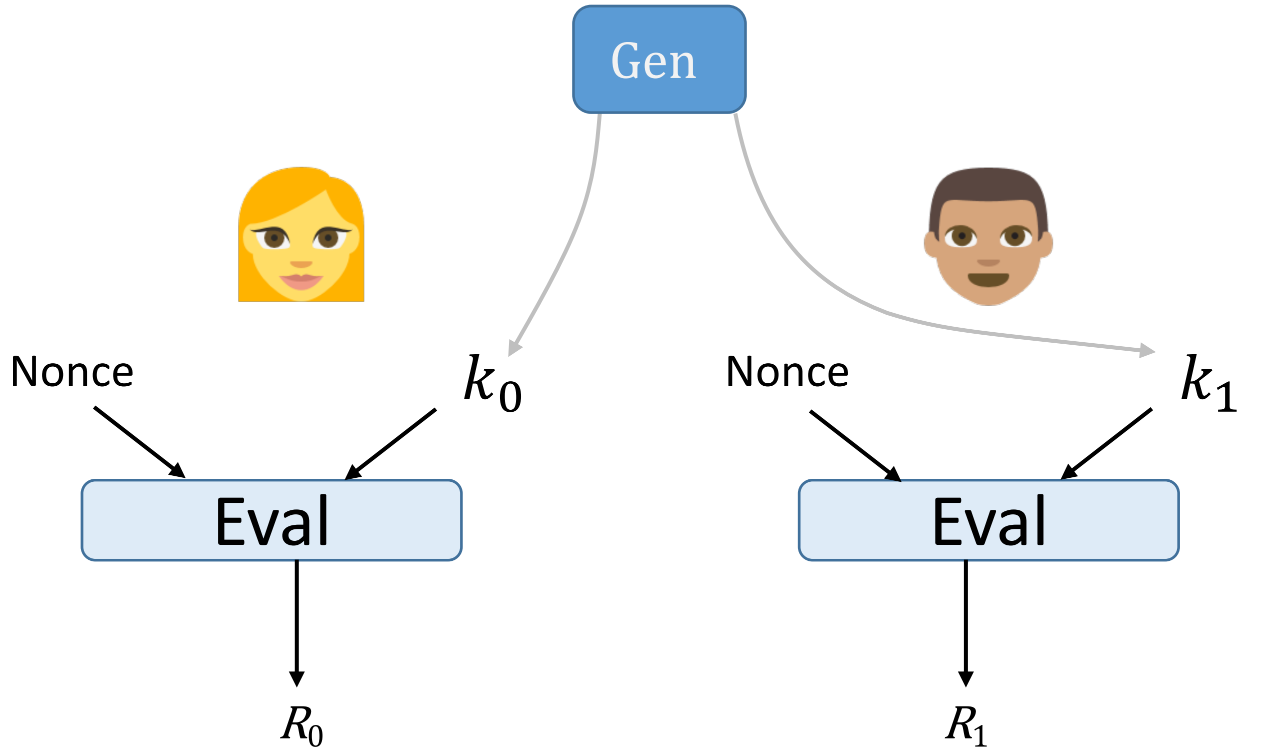


Correctness: $(R_0, R_1) \cong$ fresh sample of correlation

Security: against insiders

Pseudorandom Correlation Function

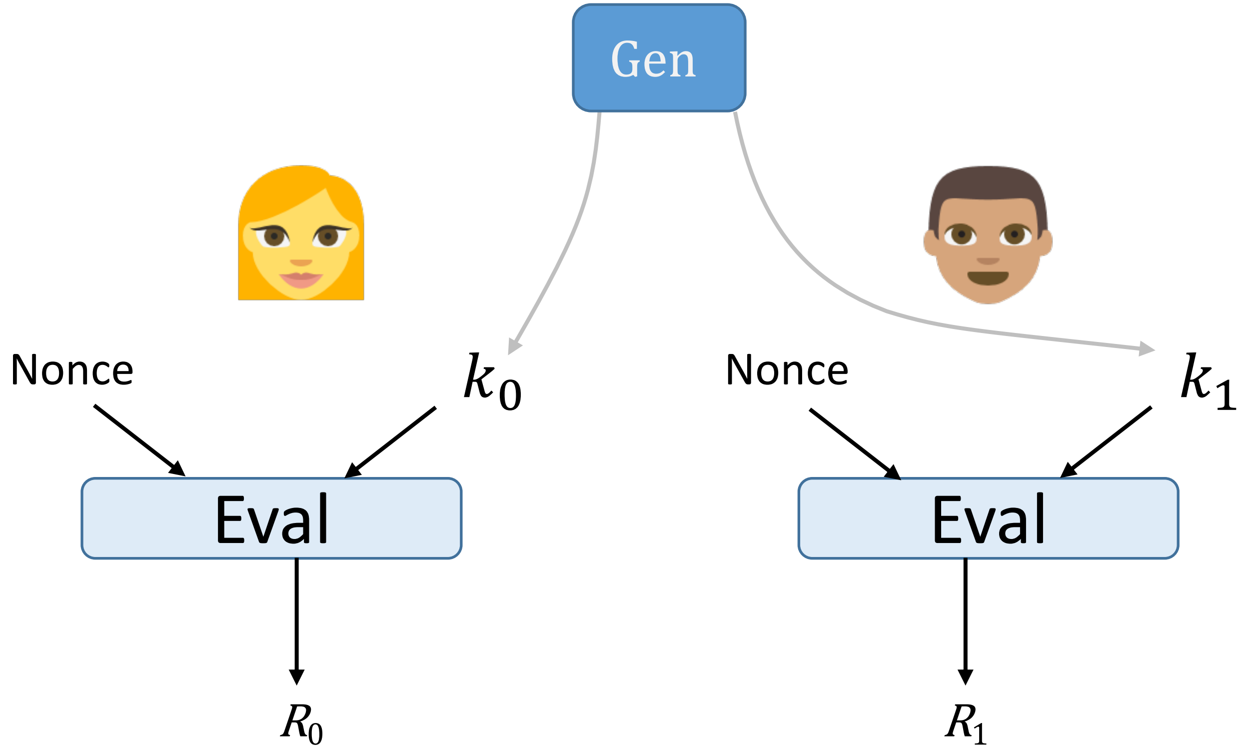
[BCGIKS20]



Assumption	Correlations	Setup?

Pseudorandom Correlation Function

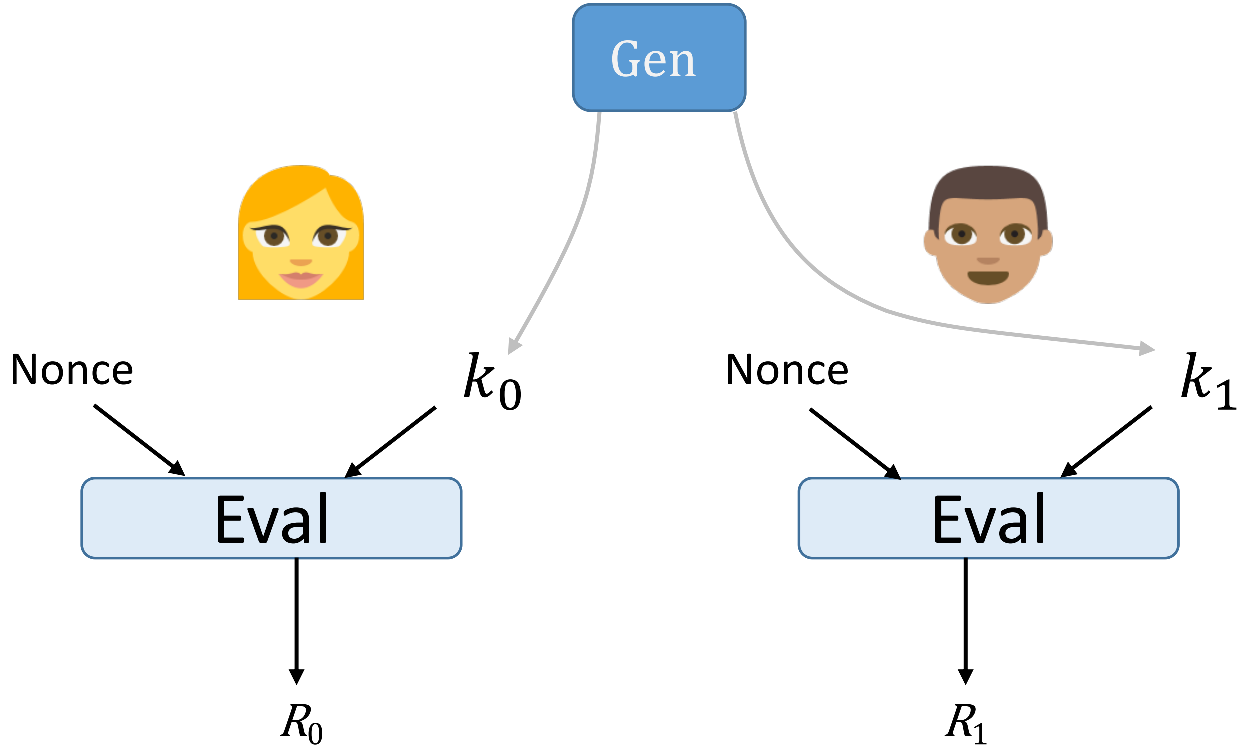
[BCGIKS20]



Assumption	Correlations	Setup?
LWE (via multi-key FHE)	additively shared	CRS + public keys

Pseudorandom Correlation Function

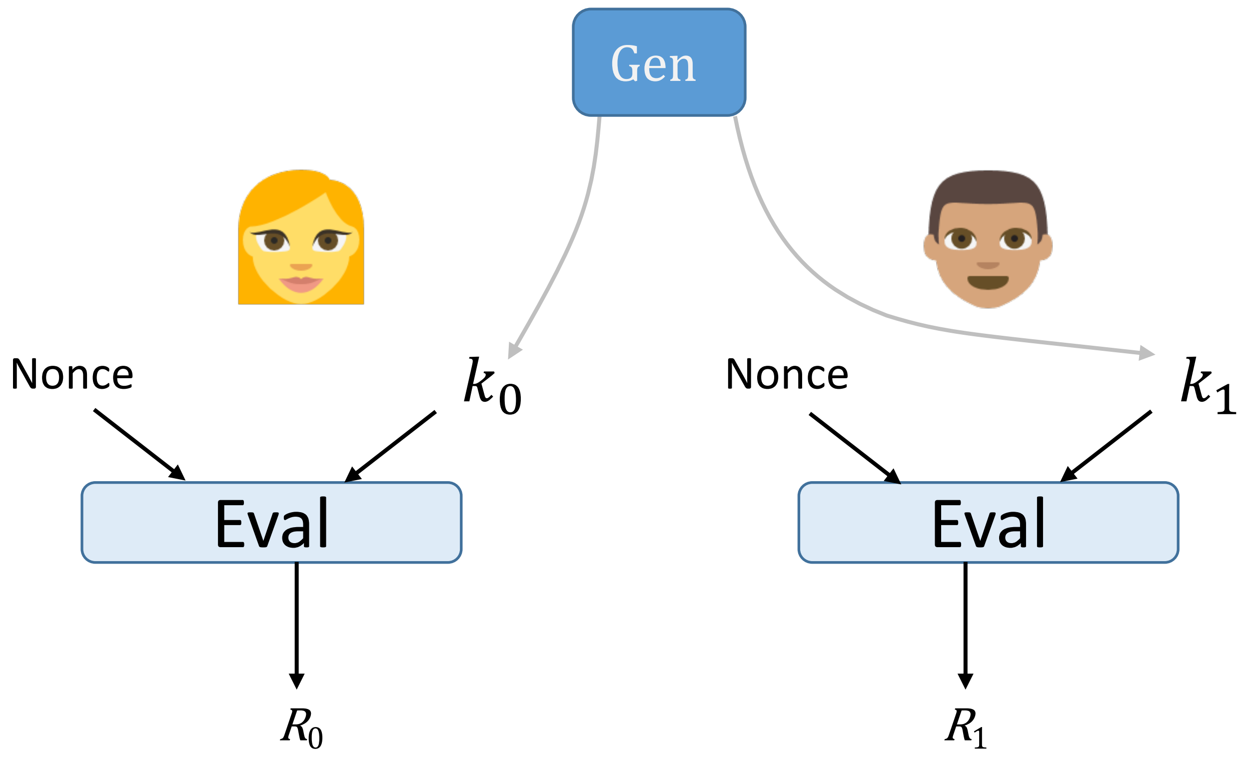
[BCGIKS20]



Assumption	Correlations	Setup?
LWE (via multi-key FHE)	additively shared	CRS + public keys
Variable-density LPN [BCGIKS 20]	OT, VOLE, constant deg.	trusted Gen

Pseudorandom Correlation Function

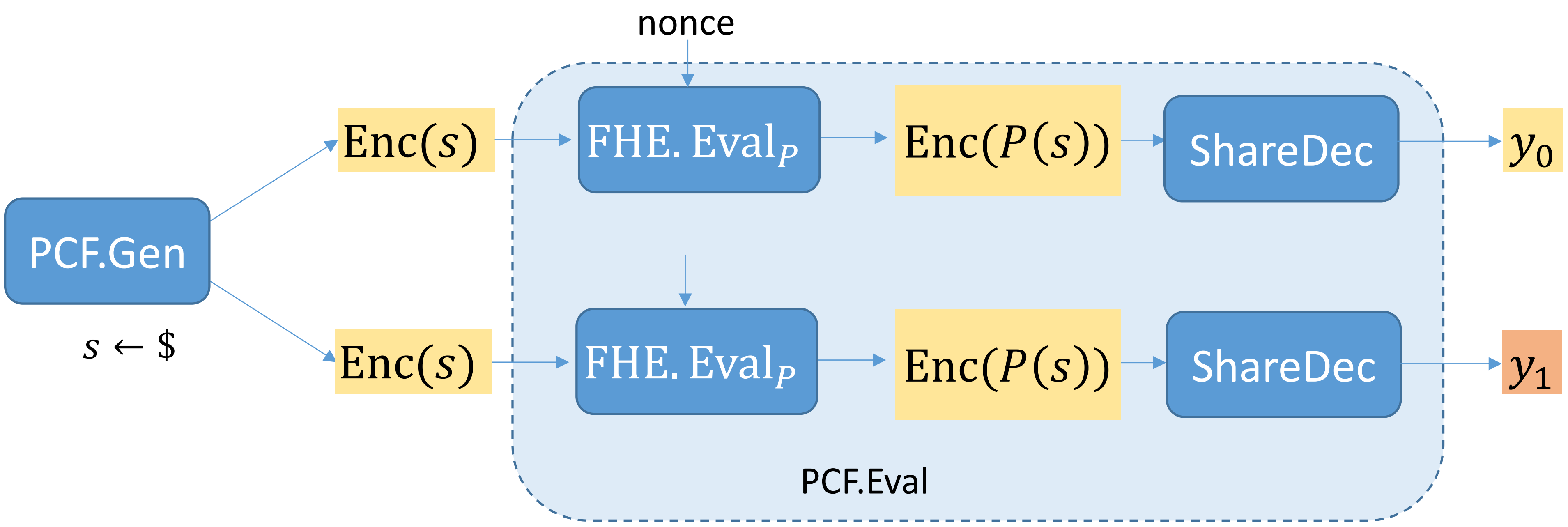
[BCGIK**S**20]



Assumption	Correlations	Setup?
LWE (via multi-key FHE)	additively shared	CRS + public keys
Variable-density LPN [BCGIK**S** 20]	OT, VOLE, constant deg.	trusted Gen
Quadratic residuosity [O**S**Y 21]	OT	CRS + public keys
DCR (Paillier) [O**S**Y 21]	VOLE	CRS + public keys

Warm-up: PCFs from FHE with share decryption

[DHRW 16]



- For e.g. Beaver triples:
  - $P(s) \rightarrow (a, b, ab)$ using $\mathrm{PRF}(s, nonce)$

Expensive in FHE!

- ShareDec correctness:

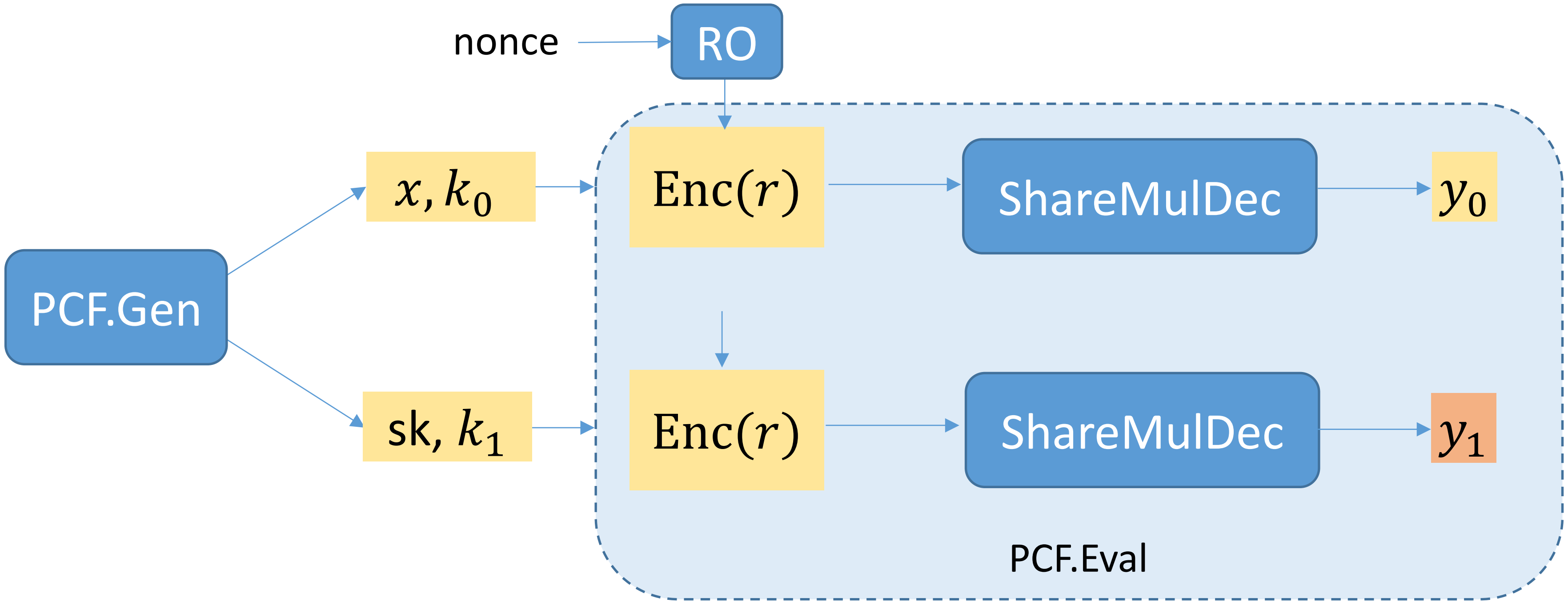
$$y_0 + y_1 = (a, b, c)$$

Can we optimize FHE-based PCF?

Instead of generating $Enc(a), Enc(b)$ inside FHE, can we sample them directly?

- Seems hard with LWE
  - Inefficient candidates used in iO schemes [WW 21, DQVWW 21]
- What about other schemes?
  - Paillier and Goldwasser-Micali have dense ciphertext space
  - Problem: only additive homomorphism

Blueprint for efficient PCF: oblivious sampling + share decryption



$y_0 + y_1 = rx$ → PCF for VOLE

Paillier encryption 101

- Paillier group: $Z_{N^2}^*, N = pq$

- $g := 1 + N$ is special:
  - Generates easy DLog subgroup with order N:

$$(1+N)^x = 1 + Nx \quad \bmod N^2 \quad \longrightarrow \quad DLog_{1+N}(y) = \frac{y-1}{N}$$

- Isomorphism

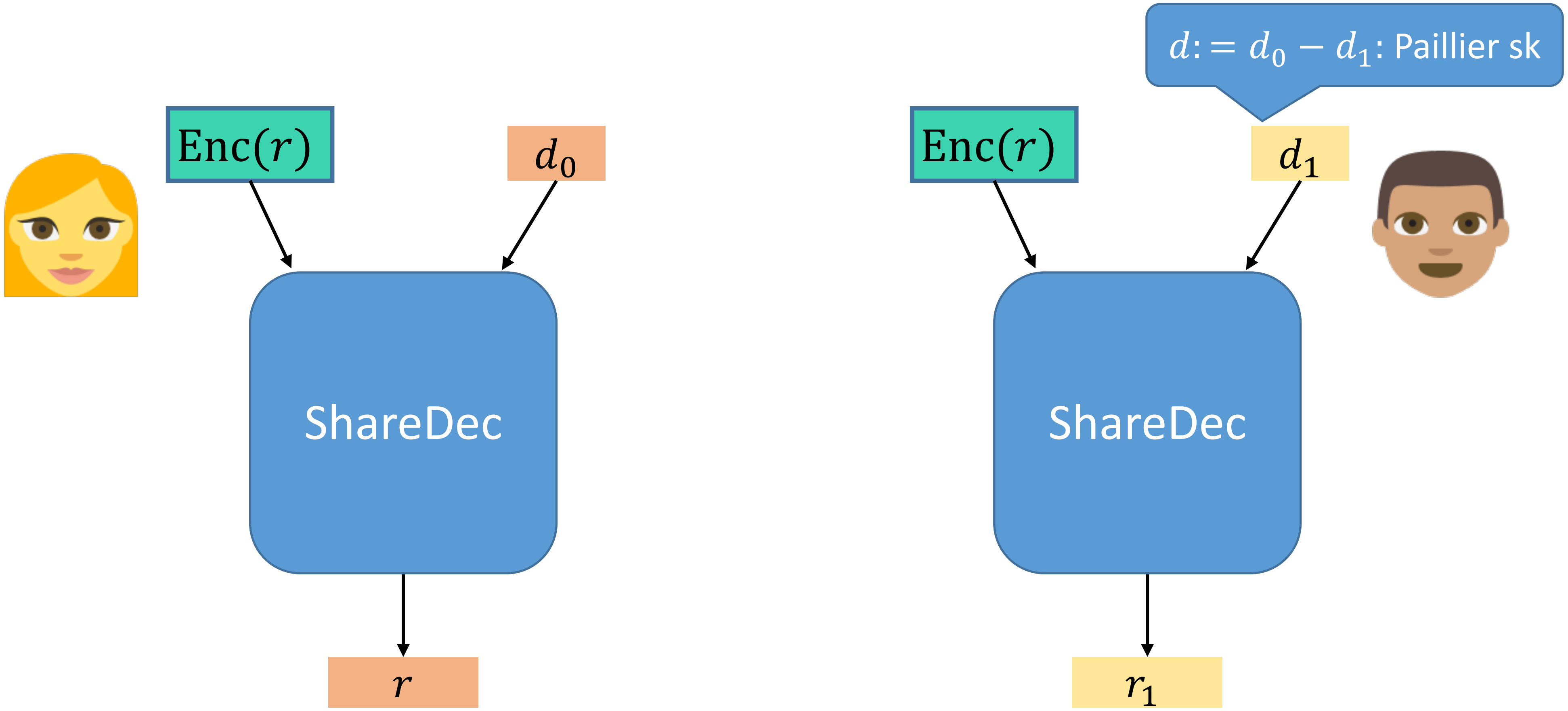
$$\mathbb{Z}_{N^2}^* \cong \mathbb{Z}_N \times \mathbb{Z}_N^*$$
$$\text{Enc}(x;r) = g^x r^N$$

Implies oblivious sampling!

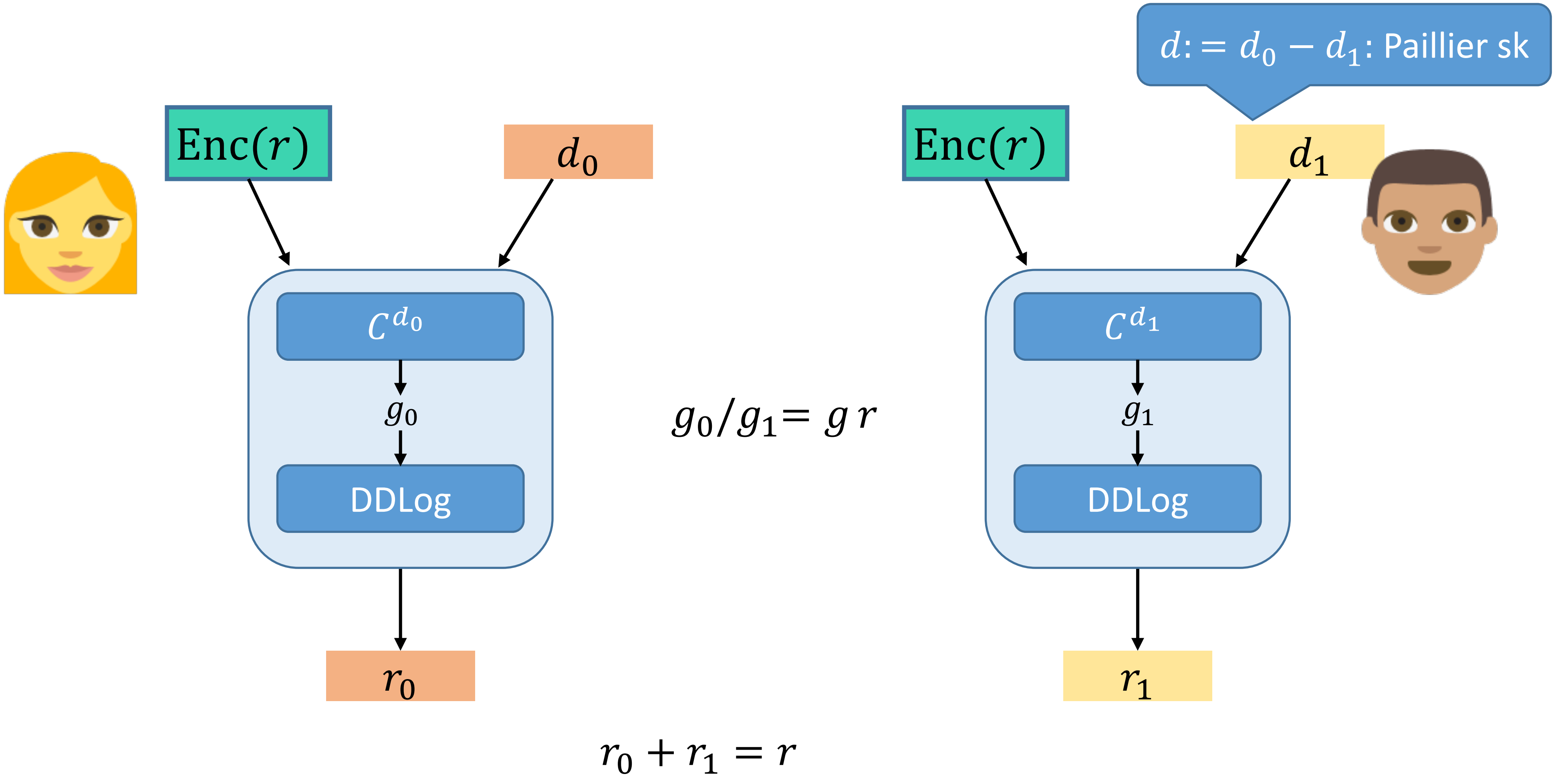
- Secret key: $d \in \mathbb{Z}$ such that

$$\text{Enc}(x)^d = g^x$$

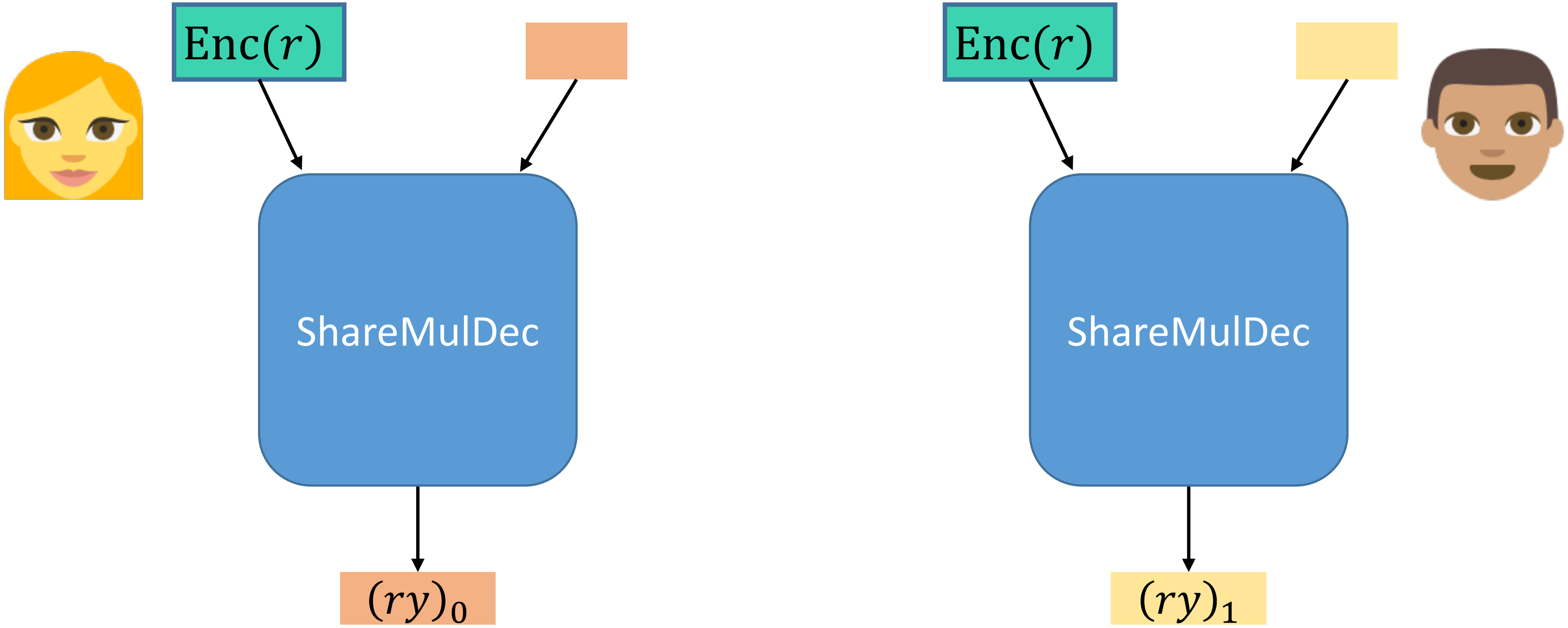
Paillier: local decryption to shares



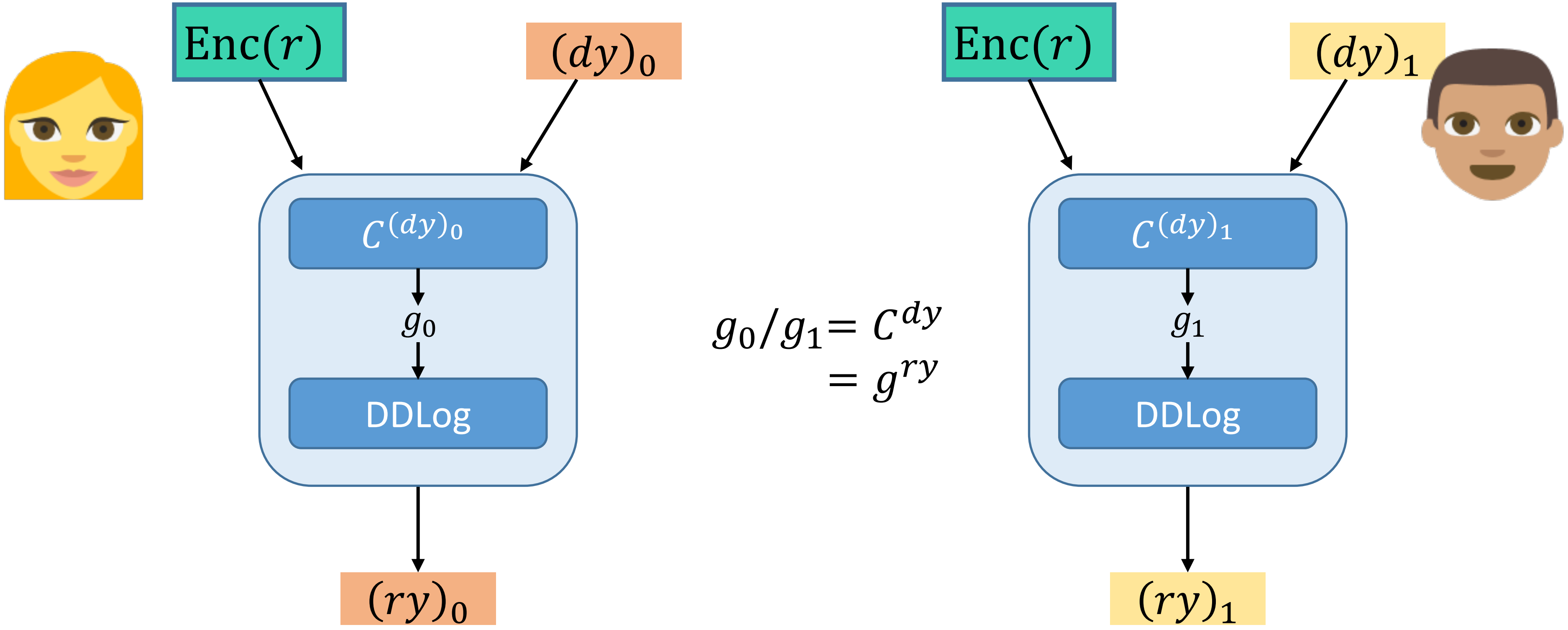
Paillier: local decryption to shares



Paillier: decryption to shares + multiplication



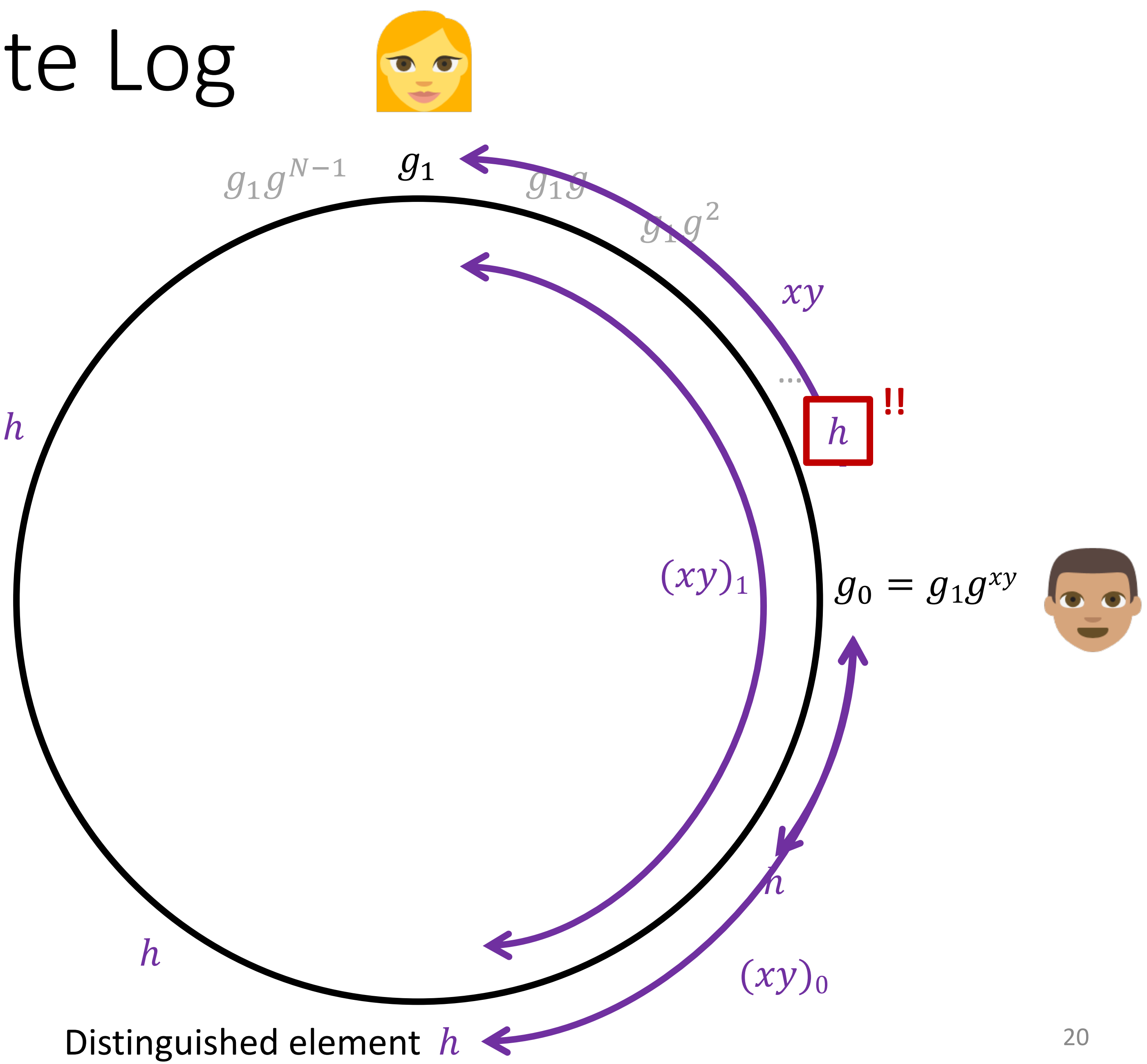
Paillier: decryption to shares + multiplication



$$(ry)_0 + (ry)_1 = ry$$

Distributed Discrete Log (DDH) [Boyle Gilboa Ishai 16]

- $g_0/g_1 = g^{xy}$
- $(xy)_1 - (xy)_0 = xy$
- Problem: what if $(xy)_0$, $(xy)_1$ are large?
  - Have many h's
  - Poly-size message space
- Problem: error if parties hit different h
  - Gives 1/poly error!



DDLog for DDH: state of the art

- Various optimizations for reducing error etc.

[BGI 16, BGI 17, BCGIO 17, DKK 18]

  - Still computationally heavy
  - $1/poly$ correctness error
  - Limited to small message spaces

- Variant in Paillier groups: same limitations [FGJS 17]

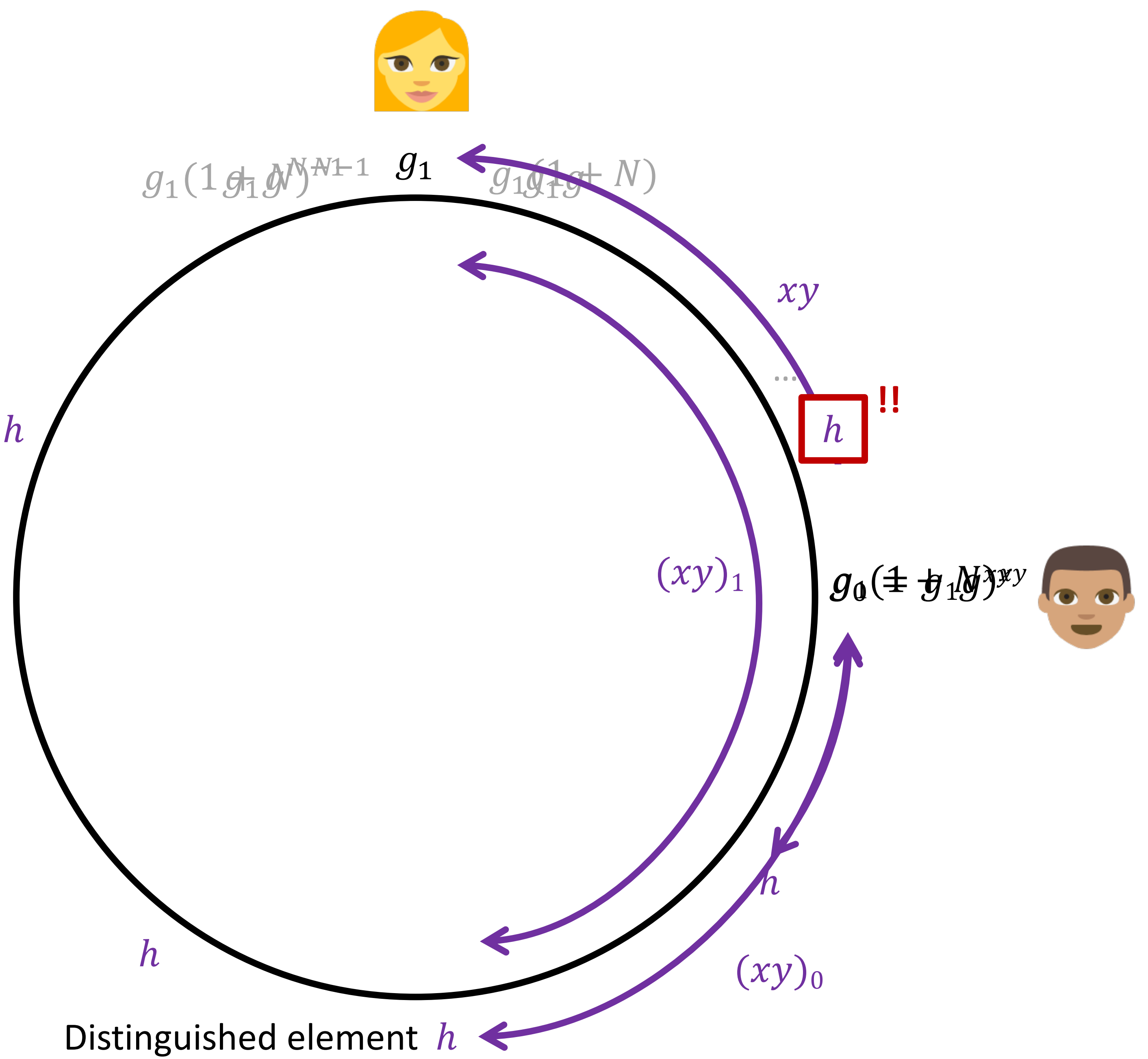
Q: Can we do better?

- Cannot do better without solving variant of discrete log [DKK 18]

DDLog for Paillier

- $g_0/g_1 = (1+N)^{xy} \mod N^2$
- Use just one h:
  - $h/g_i = (1+N)^{(xy)_i} \quad \rightarrow \quad (xy)_i$
  - Use $h := g_1 \bmod N = g_0 \bmod N$ (in Z_{N^2})
- h is in the same coset!

- Large message space, negl error!



DDLog for Paillier: formally

- **Private Inputs:** $g_0 \in Z_{N^2}^*$ $g_1 = g_0(1+N)^z$
  - $Z_N \times Z_N^* \cong Z_{N^2}^*$
- **Goal:** common output $h \in Z_{N^2}^*$, in the same coset

Claim: If $h = g_0 \bmod N = g_1 \bmod N$, then lies in the coset $\{g_0(1+N)^i\}_i$.

Proof:

PCF for VOLE: under the lens of a weak PRF

- For random ciphertext $C \in \mathbb{Z}_{N^2}$ and Paillier decryption key d:

$$F(d, C) = (C^d - 1)/N$$

is a weak PRF

- Additive shares of $d \cdot y \quad \Rightarrow \quad$ FSS keys for the class $\{y \cdot F(d,\cdot)\}_{y,d}$

PCF for OT from Goldwasser-Micali

- Goal: instead of VOLE, produce correlated OTs

$$y_{0,i} = r_i \Delta + y_{1,i} \;\; \in \mathbb{F}_2^\lambda$$

with $r_i \in \{0,1\}$, $\Delta \in \{0,1\}^\lambda$

  - Then hash to get random OT

- Goldwasser-Micali:
  - Encrypts $b \in \{0,1\}$
  - Secret sk $d \in \mathbb{Z}$ where

$$C^d = (-1)^b \mod N$$

PCF for OT from Goldwasser-Micali

- DDLog for Goldwasser-Micali: on input $Y \in \mathbb{Z}_N$
  - If $Y < N/2$ output 1, otherwise output 0

$$Y_0/Y_1 = (-1)^b \qquad \Rightarrow \qquad \mathrm{DDLog}(Y_0) \oplus \mathrm{DDLog}(Y_1) = b$$

- PCF
  - For each bit Δ_j of Δ, give out shares of $d \cdot \Delta_j$
  - Oblivious ciphertext $\Rightarrow$ $\mathrm{Enc}(r_i)$
  - Share dec + DDLog $\Rightarrow$ one bit of $y_{0,i} = r_i\Delta \oplus y_{1,i}$
  - Cost: $\sim \lambda$ exponentiations

Summary: PCFs from number-theoretic assumptions

Assumption	Correlation	Setup	Cost per Eval
Paillier (DCR)	VOLE in $\mathbb{Z}_N$	$y_0 - y_1 = d \cdot x$	1 exp in $\mathbb{Z}_N$
Quadratic Residuosity	Δ-OT	$y_{0,i} - y_{1,i} = d \cdot \Delta_i$	128 exp in $\mathbb{Z}_{N^2}$

Summary: PCFs from number-theoretic assumptions

Assumption	Correlation	Setup	Cost per Eval	Key size
Paillier (DCR)	VOLE in $\mathbb{Z}_N$	$y_0 - y_1 = d \cdot x$	1 exp in $\mathbb{Z}_{N^2}$	$\sim$1kB
Quadratic Residuosity	Δ-OT	$y_{0,i} - y_{1,i} = d \cdot \Delta_i$	128 exp in $\mathbb{Z}_N$	$\sim$50kB

What about OLE instead of VOLE?

- Bootstrap setup for many x_i?
- Challenge: setup shares are over $\mathbb{Z}$

(PCG only) **LPN + DCR**	**OLE in $\mathbb{Z}_N$**	**PCG for VOLE in $\mathbb{Z}$**	$\sim$1 **exp in** $\mathbb{Z}_{N^2}$	$O(\lambda \log m)$

Comparison with PCFs from VDLPN

- VDLPN [BCGIKS 20]: cons
  - More costly setup: non-constant round, many DPFs
  - Key size $120\text{kB} - 2\text{MB}$
  - New assumption

- VDLPN: pro
  - **Much** faster computation
  - $\sim 20\ 000$ Eval/s on one core
  - vs.
    - VOLE from Paillier: 100 eval/s
    - OT from QR: 1-2 eval/s

Bonus: HSS for Branching Programs from Paillier

[OSY 21]

- HSS for ”restricted multiplication” circuits ≈ log-depth circuits
  - Each multiplication must involve an input wire
  - Encrypt inputs, secret share intermediate values
  - Multiply using ShareDec

- Bottom line:
  - Negligible correctness error
  - Exponential plaintext space

  Not possible with previous DDH/Paillier constructions
  - vs RLWE: smaller ciphertexts, slower computation

What about PCF setup?

- Recall PCF keys:

VOLE: shares of $d \cdot x$

OT: shares of $d \cdot \Delta_i$

Both are just OLE!

- Can we make this non-interactive?

  i.e. one parallel message from Alice/Bob

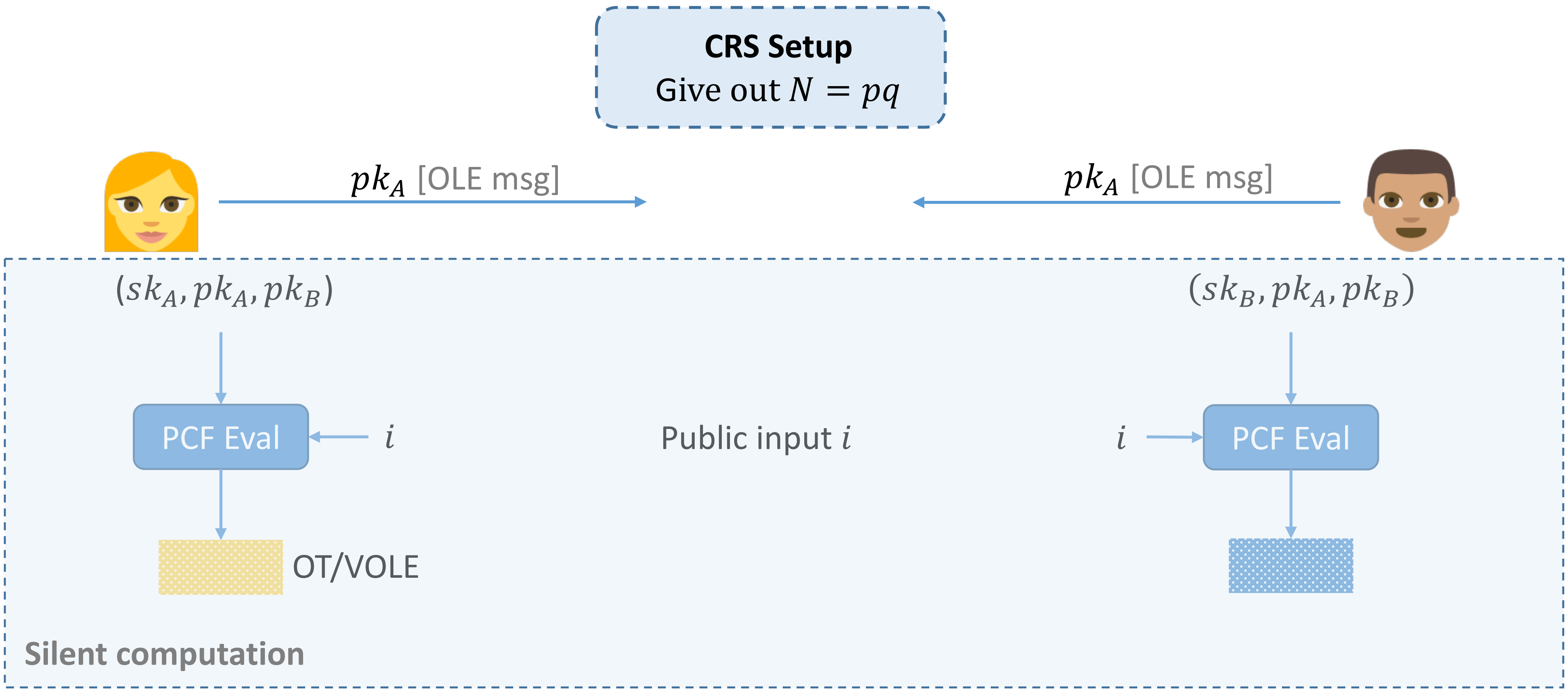
  - Yes! (Assuming a CRS…)
  - Gives public-key setup

Non-interactive (but not silent!) OLE from Paillier

Goal:

Output: shares of xy

Public-Key Silent OT/VOLE: Protocol Flow



Conclusion

- Blueprint for pseudorandom correlation functions:

  $\boxed{\text{Oblivious ciphertext sampling + distributed decryption}}$

  - Easily done with Paillier (VOLE) and Goldwasser-Micali (OT)

- PCFs from Paillier or QR
  - Produce arbitrary quantity of OT or VOLE
  - Small, one-time setup
  - Expensive computation

- (Non-silent) OLE from Paillier
  - One-round protocol
  - Gives public-key PCF (with CRS)

Open problems

- Other PKE schemes with oblivious ciphertext sampling?
  - Obtain PCF from other assumptions
  - HE or functional encryption?
    - Different properties maybe useful for more correlations

- Improve OT efficiency
  - $O(\lambda)$ exponentiations

- Remove CRS $N = pq$ from public-key PCFs

- Public-key setup for LPN-based PCG/PCF
  - Currently: two-round setup

- Beyond two parties?

Thank you!

The Rise of Paillier: Homomorphic Secret Sharing and Public-Key Silent OT
Orlandi, S, Yakoubov (2021)
https://ia.cr/2021/262