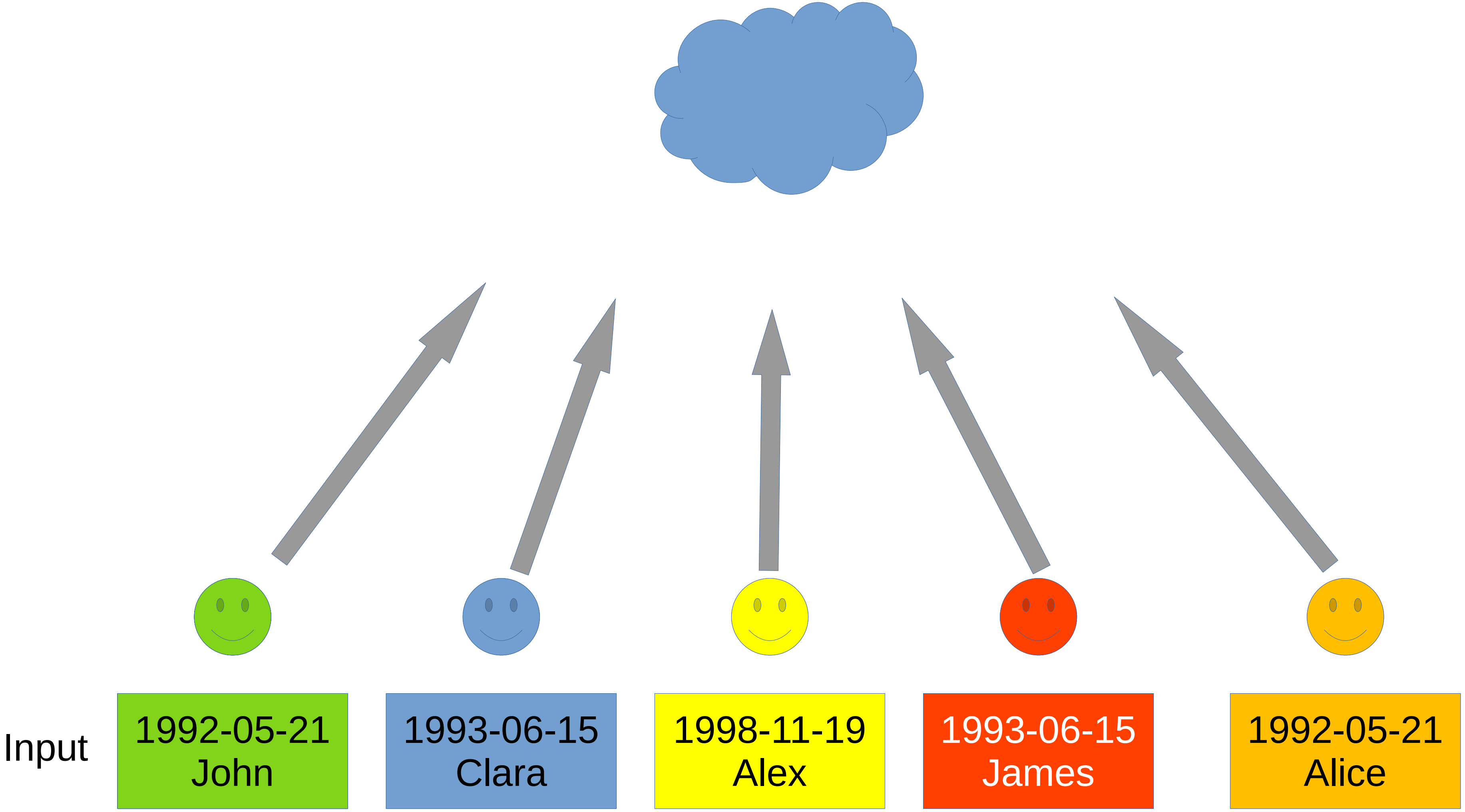
Private birth date match

- Find people with the same birth date as you



Input

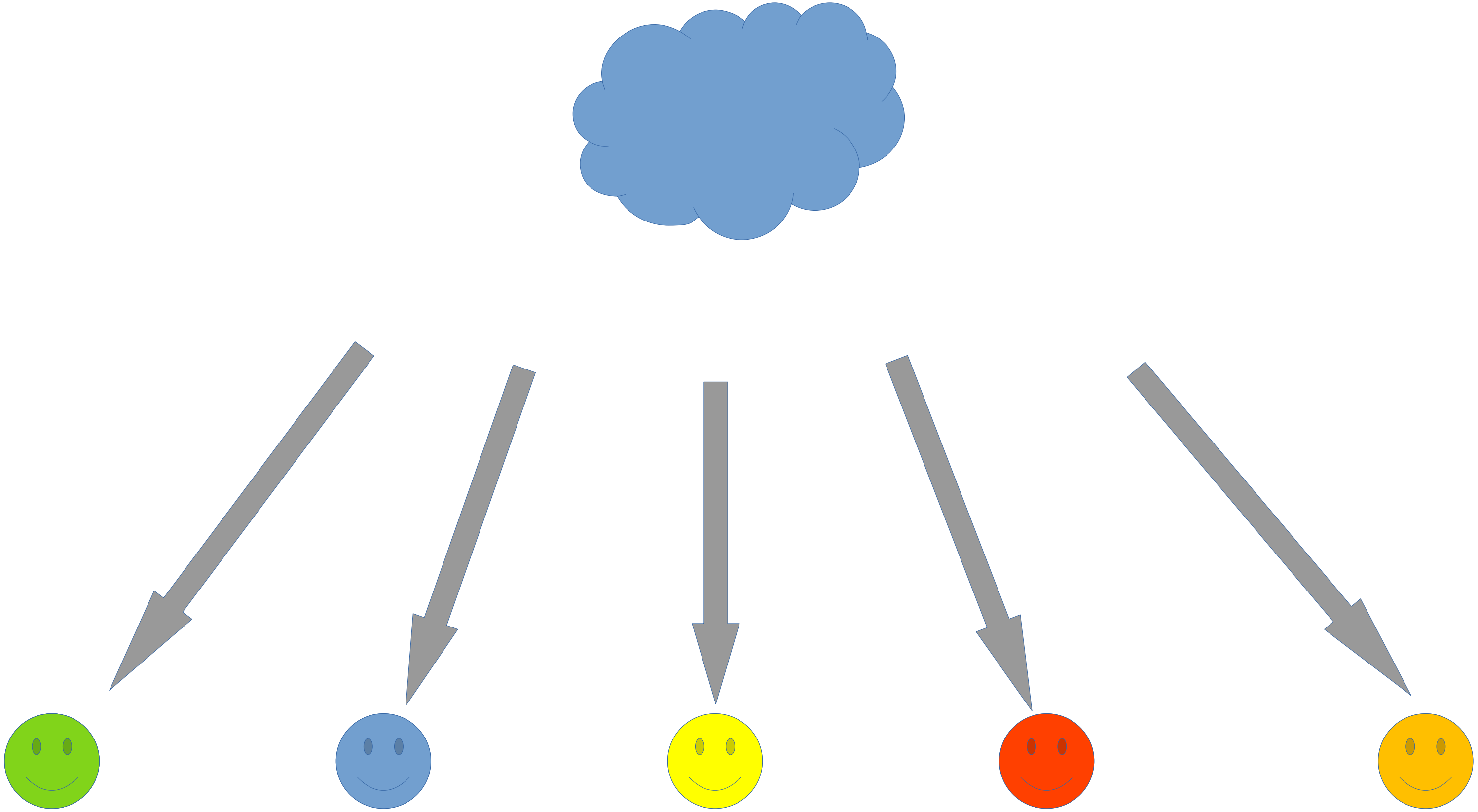
1992-05-21
John

1993-06-15
Clara

1998-11-19
Alex

1993-06-15
James

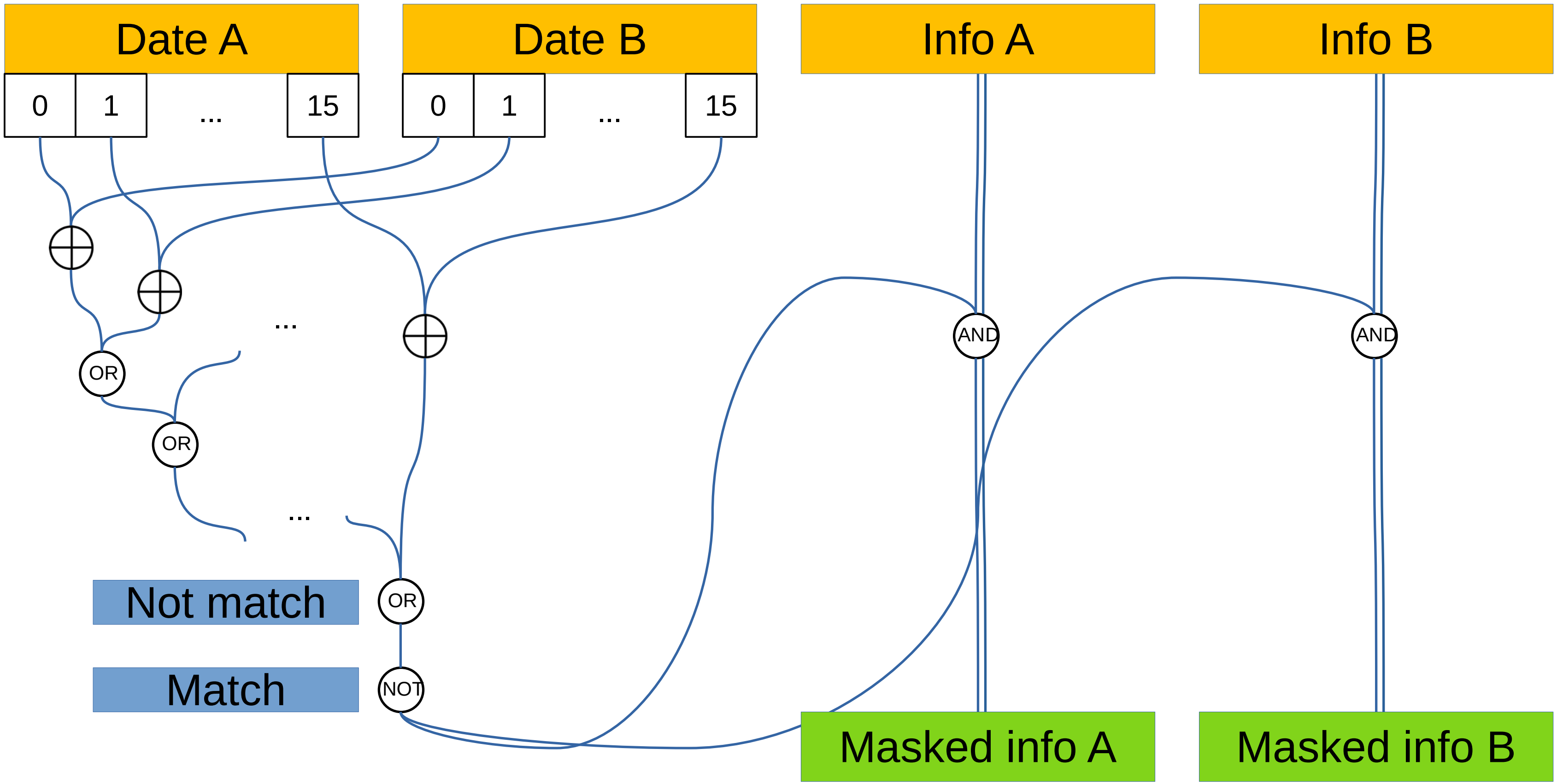
1992-05-21
Alice



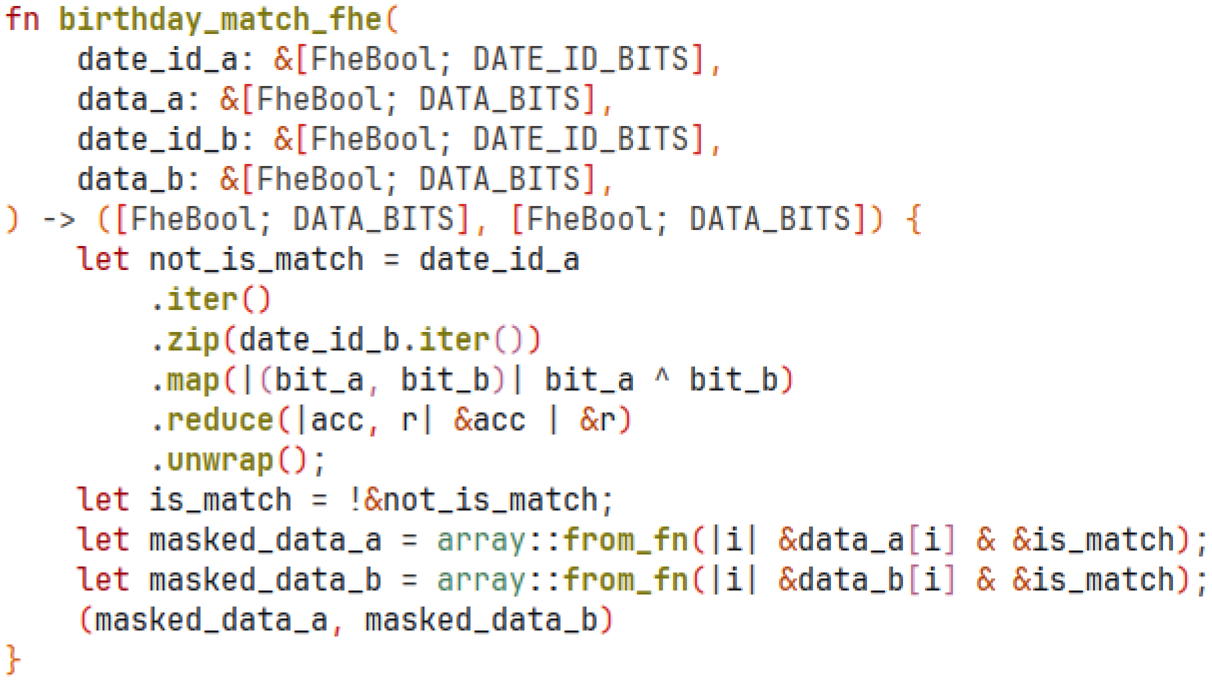
Input	1992-05-21 John	1993-06-15 Clara	1998-11-19 Alex	1993-06-15 James	1992-05-21 Alice
Output	Alice	James	:(	Clara	John

NxN 2-party FHE

	John	Clara	Alex	James	Alice
John		X	X	X	X
Clara			X	X	X
Alex				X	X
James					X
Alice					

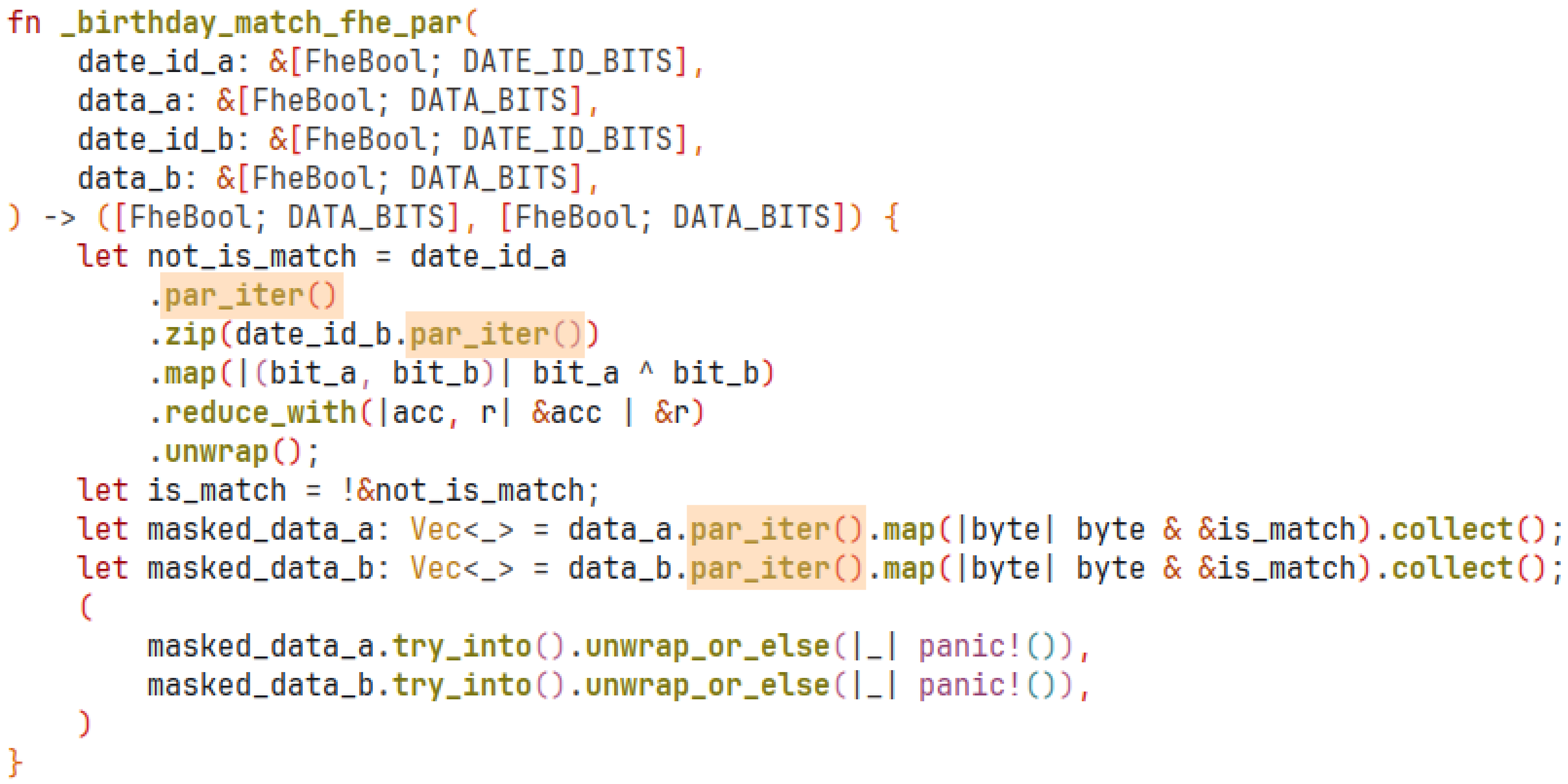

Date A
Date B
Info A
Info B
0
1
...
15
0
1
...
15
...
OR
OR
...
OR
NOT
AND
AND
Not match
Match
Masked info A
Masked info B

Circuit code



```rust
fn birthday_match_fhe(
    date_id_a: &[FheBool; DATE_ID_BITS],
    data_a: &[FheBool; DATA_BITS],
    date_id_b: &[FheBool; DATE_ID_BITS],
    data_b: &[FheBool; DATA_BITS],
) -> ([FheBool; DATA_BITS], [FheBool; DATA_BITS]) {
    let not_is_match = date_id_a
        .iter()
        .zip(date_id_b.iter())
        .map(|(bit_a, bit_b)| bit_a ^ bit_b)
        .reduce(|acc, r| &acc | &r)
        .unwrap();
    let is_match = !&not_is_match;
    let masked_data_a = array::from_fn(|i| &data_a[i] & &is_match);
    let masked_data_b = array::from_fn(|i| &data_b[i] & &is_match);
    (masked_data_a, masked_data_b)
}
```

Parallel Circuit code (with rayon's ParallelIterator)



```
fn _birthday_match_fhe_par(
    date_id_a: &[FheBool; DATE_ID_BITS],
    data_a: &[FheBool; DATA_BITS],
    date_id_b: &[FheBool; DATE_ID_BITS],
    data_b: &[FheBool; DATA_BITS],
) -> ([FheBool; DATA_BITS], [FheBool; DATA_BITS]) {
    let not_is_match = date_id_a
        .par_iter()
        .zip(date_id_b.par_iter())
        .map(|(bit_a, bit_b)| bit_a ^ bit_b)
        .reduce_with(|acc, r| &acc | &r)
        .unwrap();
    let is_match = !&not_is_match;
    let masked_data_a: Vec<_> = data_a.par_iter().map(|byte| byte & &is_match).collect();
    let masked_data_b: Vec<_> = data_b.par_iter().map(|byte| byte & &is_match).collect();
    (
        masked_data_a.try_into().unwrap_or_else(|_| panic!()),
        masked_data_b.try_into().unwrap_or_else(|_| panic!()),
    )
}
```

Benchmarks

- On my laptop:

```
Clients server key share gen time: 1.858942684s
Server key gen time: 40.147093803s
Server cyphertext extract time: 340.136156ms
Birthday match FHE evaluation time:
   (serial)   19.285879095s
   (parallel) 6.844518074s
Clients decryption share gen time: 19.461518ms
Client decrypt time: 9.832µs
```