Two-round Post-quantum Private Equality Test and OT from RLWE-encryption

Shengzhe Meng, Chengrui Dang,

Bei Liang, Jintai Ding

Tsinghua University

Beijing Institute of Mathematical Sciences and Application

ICICS 2024

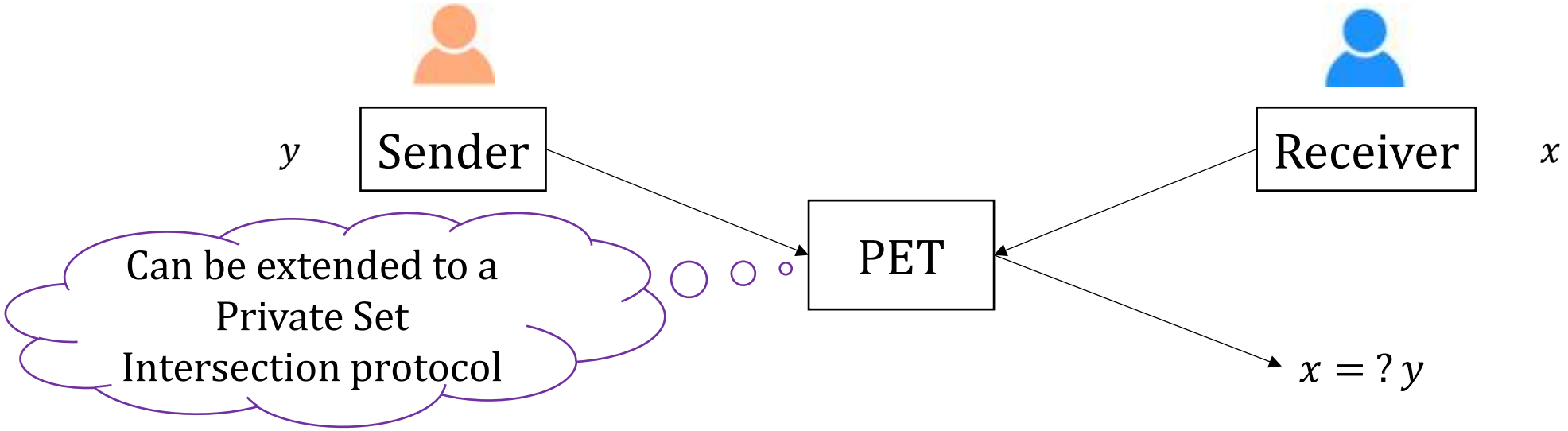
Overview

1. Preliminary
   - Private Equality Test(PET) functionality and related work
   - Oblivious transfer(OT) functionality and related work
   - RLWE problem and RLWE-PKE scheme

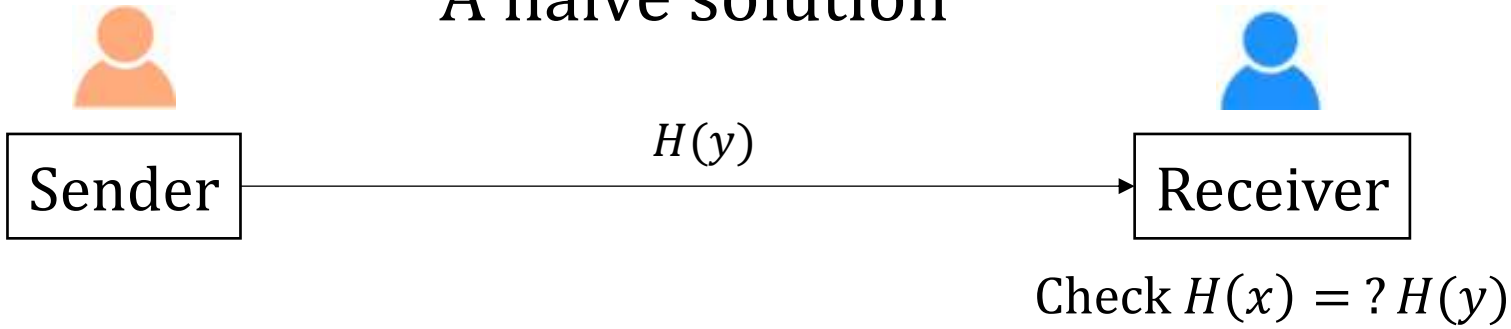
2. Protocols
   - PET protocol and two OT protocols

3. Efficiency

Private Equality Test Functionality



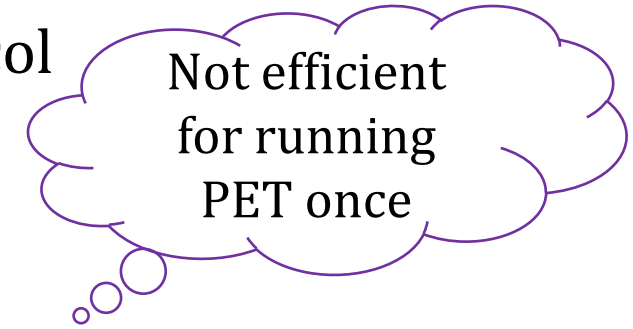
A naive solution



Not secure if the input domain is not large enough or does not have high entropy

Private Equality Test Related work

- PET from Oblivious Polynomial Evaluation [NP99]
  - 2 times oblivious polynomial evaluations pre one PET protocol



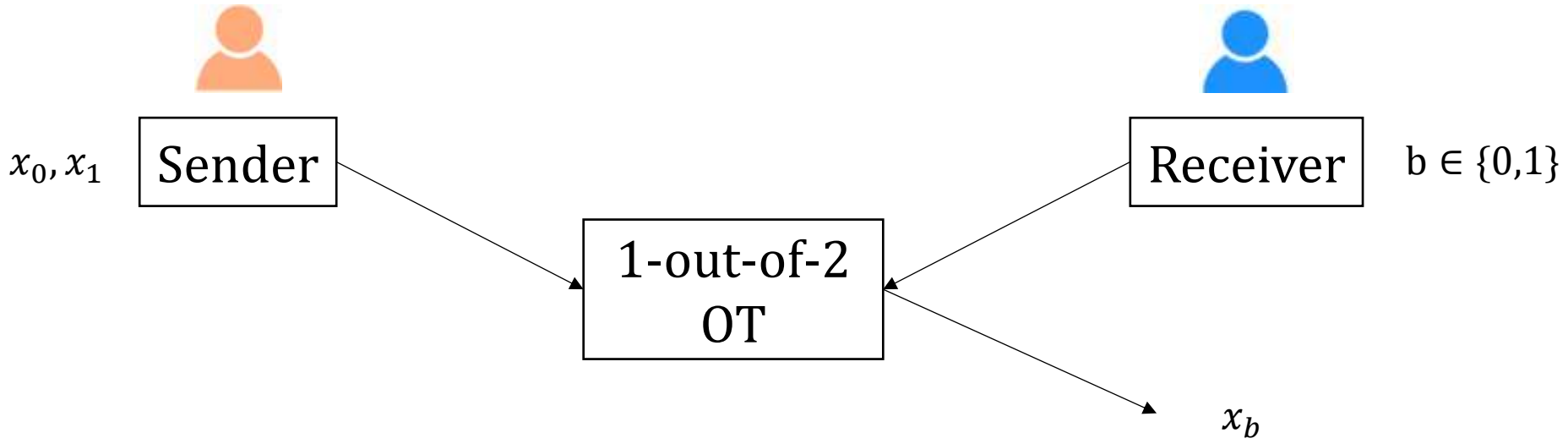
- PET from Oblivious Transfer/ Circuit [Lip03,Kar15]

  n oblivious transfers/gates to compare two n-bits secret messages.

- PET from Homomorphic Encryption [SK16,SK18]

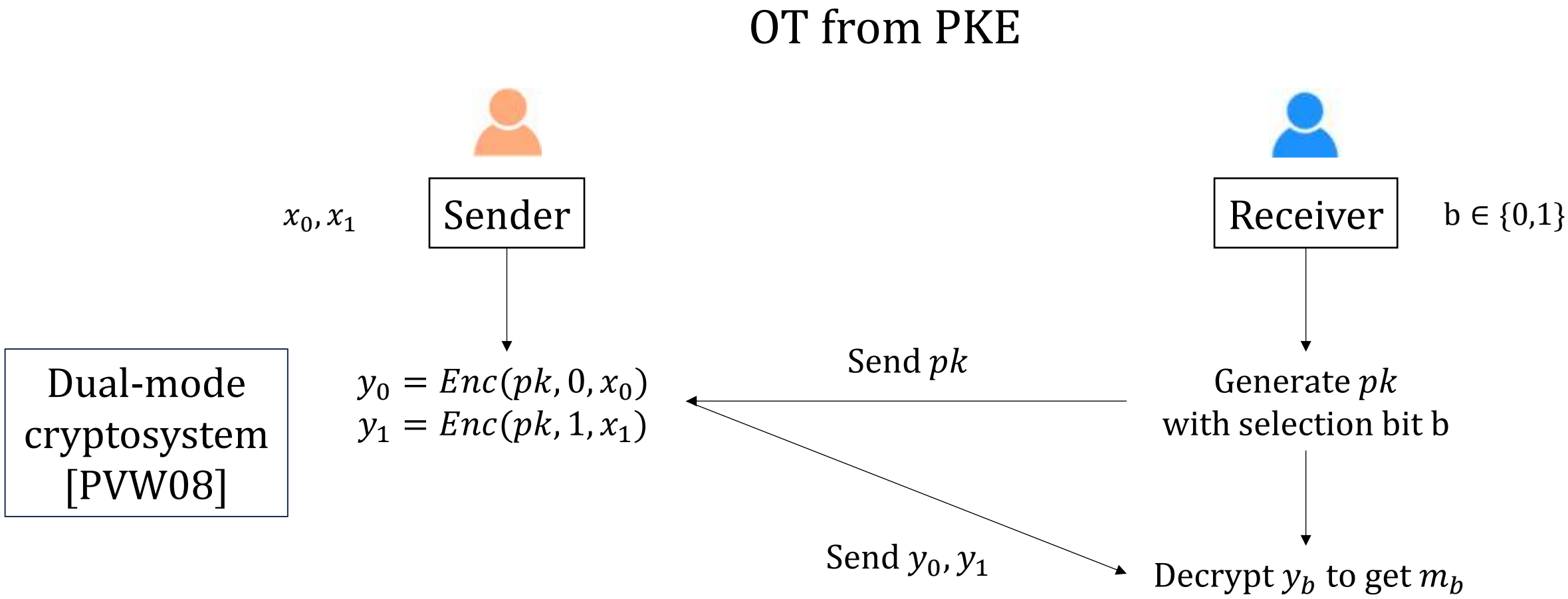
Is it possible to construct a PET protocol without homomorphic operation and achieve post-quantum secure?

Oblivious Transfer Functionality

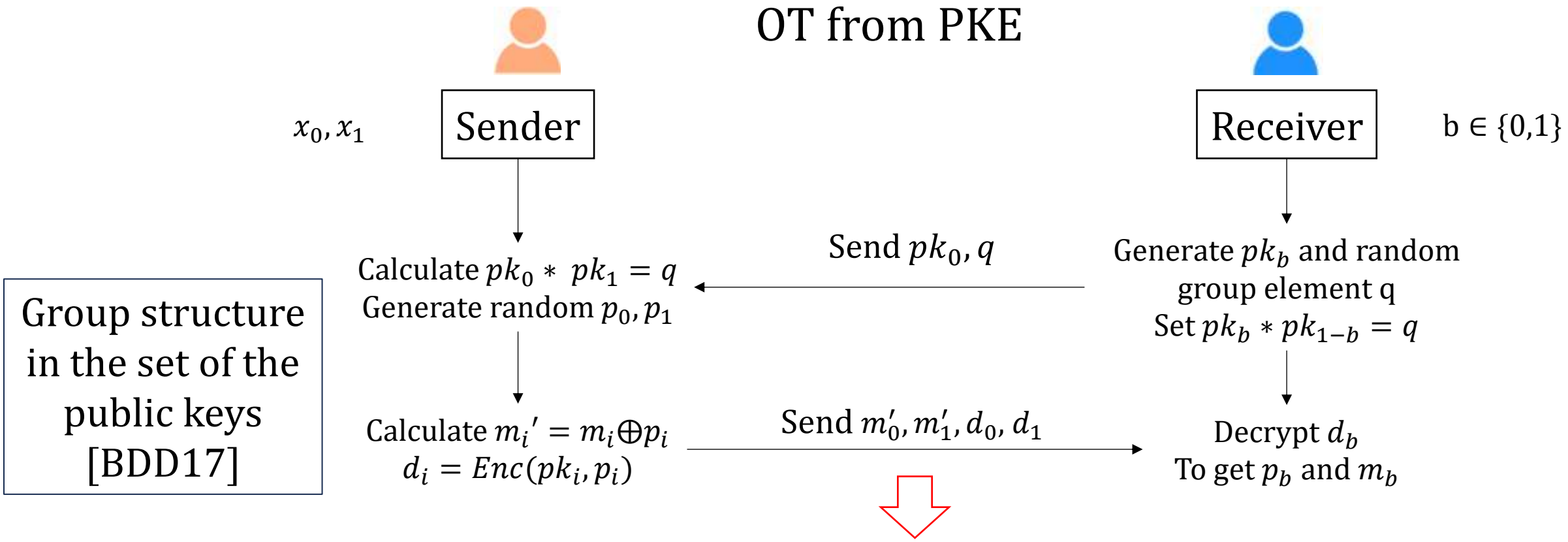


- Receiver learns x_b without learning any information about x_{1-b}
- Sender learns nothing about b

Oblivious Transfer Related work



Oblivious Transfer Related work



Group structure in the set of the public keys [BDD17]

RLWE-PKE is not suitable for those two frameworks

Is it possible to construct a OT protocol from RLWE-PKE?

Our Contribution

- PET protocol from RLWE-PKE scheme without homomorphic operation
  - Communication and computation cost less than a single round of RLWE encryption and decryption
- OT protocol from RLWE-PKE scheme
  - Based on the idea of our PET protocol
  - Communication and computation cost close to our PET protocol

RLWE problem

RLWE problem

- Given $R_q = Z_q[x]/\langle x^n + 1\rangle$, an Error distribution χ that satisfies $\Pr[\|p\|_\infty > \beta : p \xleftarrow{\$} \chi] \leq \text{negl(n)}$ for some $\beta \in N$, for $s \in R_q$, and choosing $a \xleftarrow{\$} R_q$, $e \xleftarrow{\$} \chi$, the RLWE distribution $A_{s,\chi} := (a, as + 2e \bmod q)$.
- The decision version of RLWE problem is to distinguish $A_{s,\chi}$ from uniformly chosen random values from $R_q \times R_q$.

Polynomial of degree less than n and coefficients ranging from $\{0, \dots, q-1\}$

HNF(Hermite Normal Form)-RLWE problem

- The decision version of HNF-RLWE problem is to distinguish $A_{s,\chi}$ from uniformly chosen random values from $R_q \times R_q$ where $s \xleftarrow{\$} \chi$.

RLWE-PKE scheme

- **Parameter**
  - $R_q = Z_q[x]/\langle x^n + 1\rangle$
  - Error distribution χ
  - $m \in \{0,1\}^n$
- **Private Key**
  - Sample $s, e \xleftarrow{\$} \chi$
- **Public Key**
  - Sample $a \xleftarrow{\$} R_q$
  - $b \leftarrow as + 2e$
- **Encryption**
  - Sample $s`, e`, e`` \xleftarrow{\$} \chi$
  - $c_1 \leftarrow bs` + m + 2e`$
  - $c_2 \leftarrow as` + 2\,e``$
- **Decryption**
  - $m = c_1 - c_2 s \; mod \; 2$

$c_1 = ass` + m + 2e` + 2es`$

PET Protocol Technique Overview

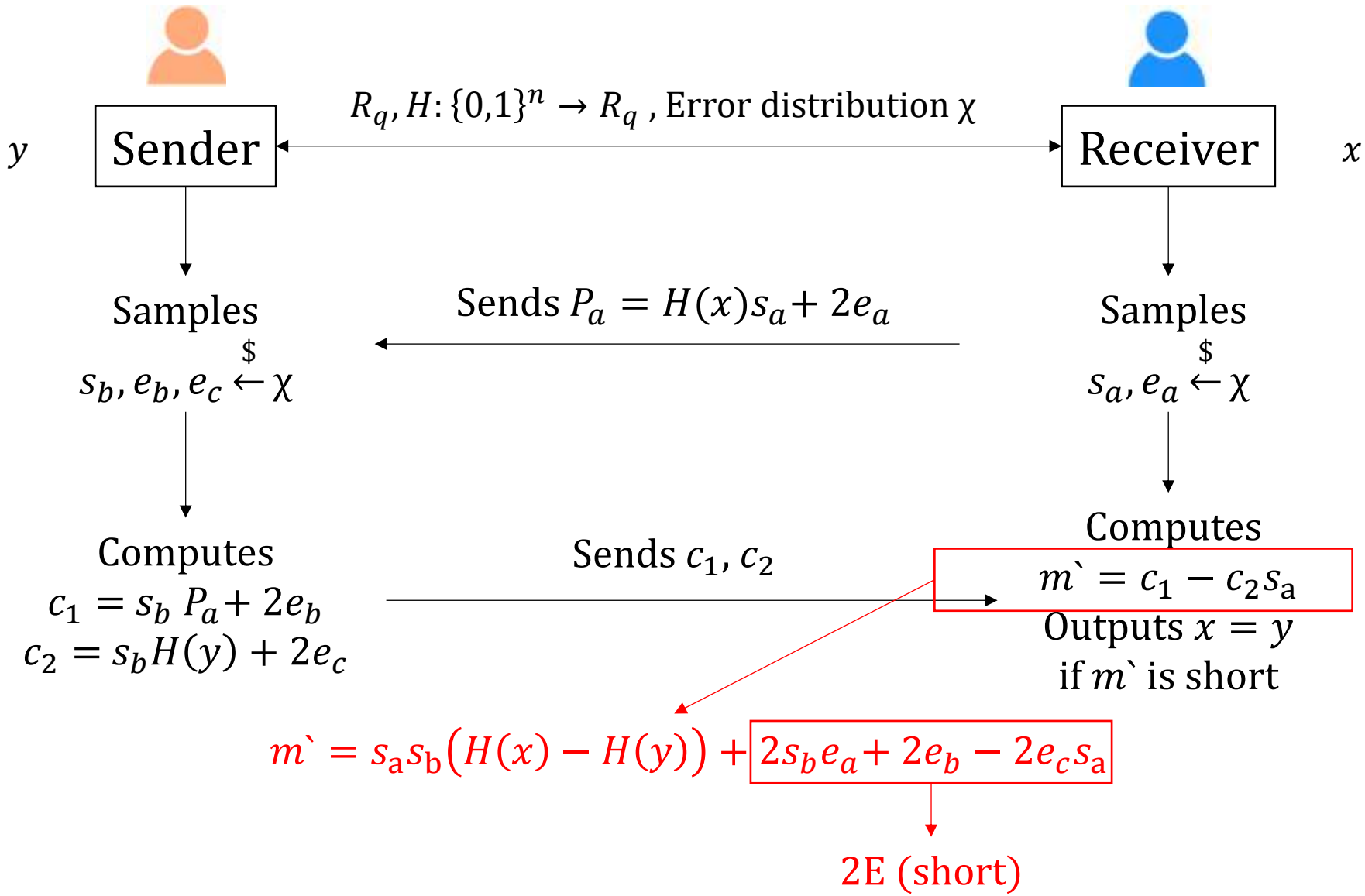
- **Parameter**
  - $R_q = Z_q[x]/\langle x^n + 1\rangle$
  - Error distribution χ
  - $m \in \{0,1\}^n$
- **Private Key**
  - Sample $s, e \xleftarrow{\$} \chi$
- **Public Key**
  - Sample $a \xleftarrow{\$} R_q$
  - $b \leftarrow as + 2e$

Only this part of the public key will be shared

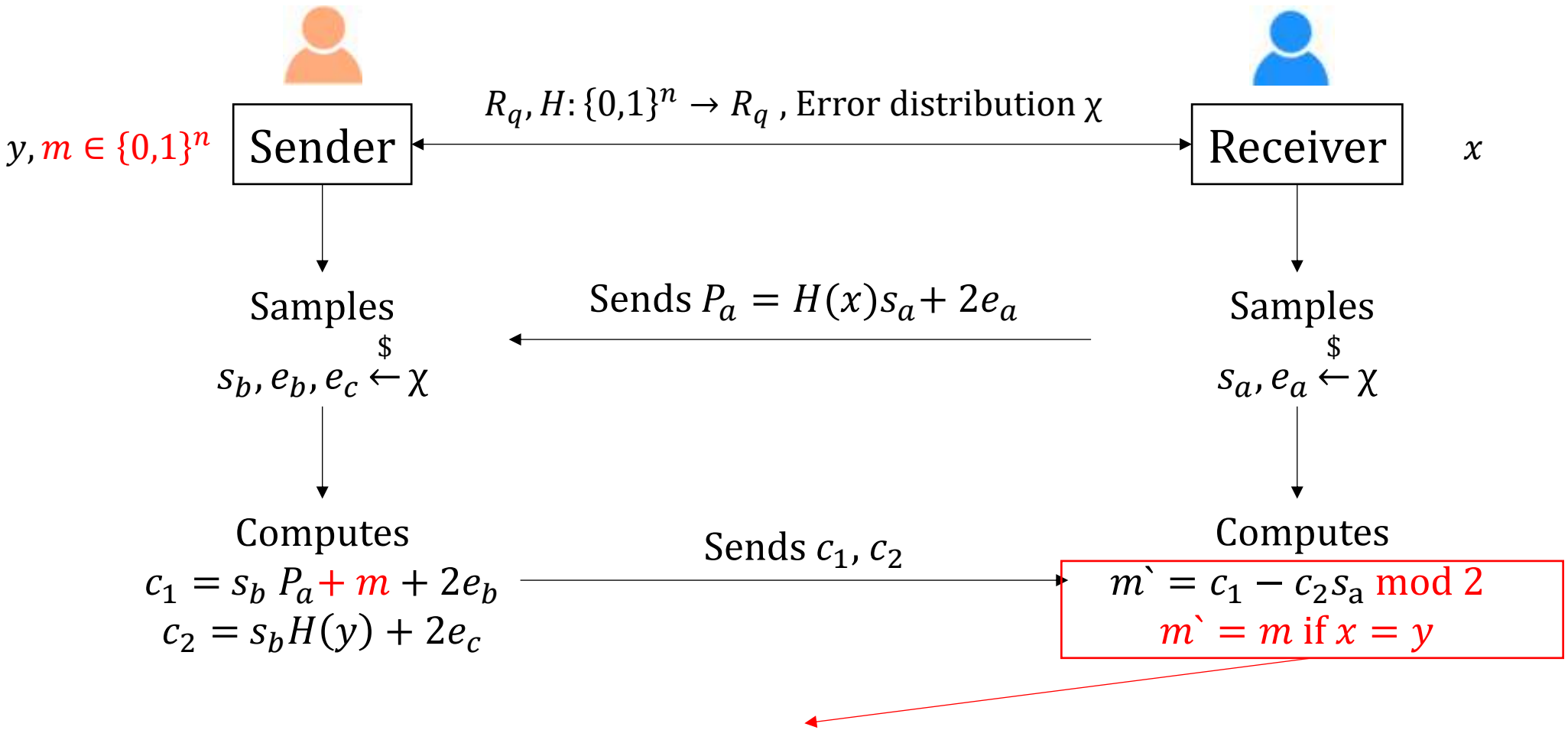
- **Encryption**
  - Sample $s`, e`, e`` \xleftarrow{\$} \chi$
  - $c_1 \leftarrow bs` + m + 2e`$
  - $c_2 \leftarrow as` + 2\,e``$
- **Decryption**
  - $m = c_1 - c_2 s \bmod 2$

c_1 and c_2 are the valid cipher-text only when the same public key a is used

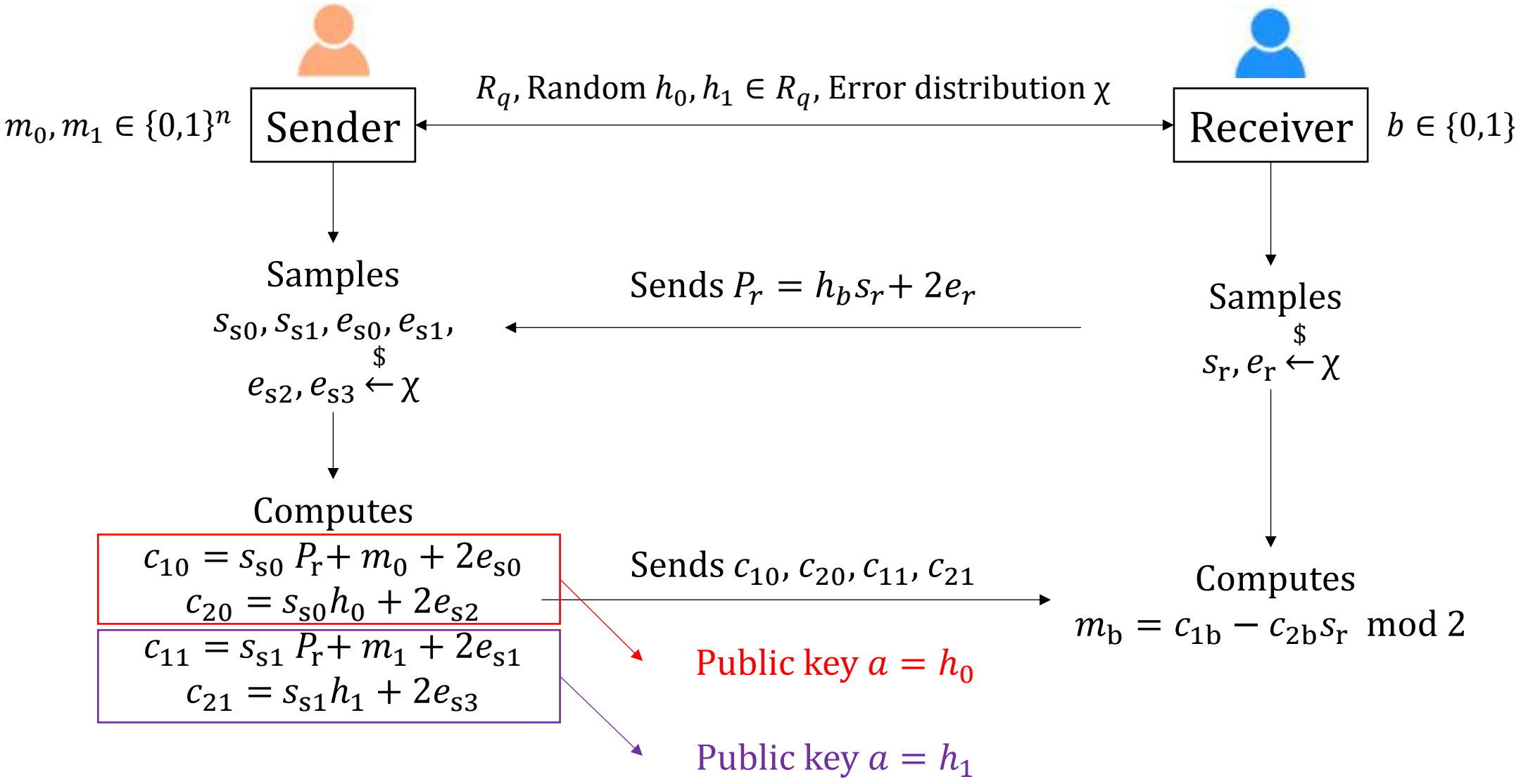
Our PET Protocol



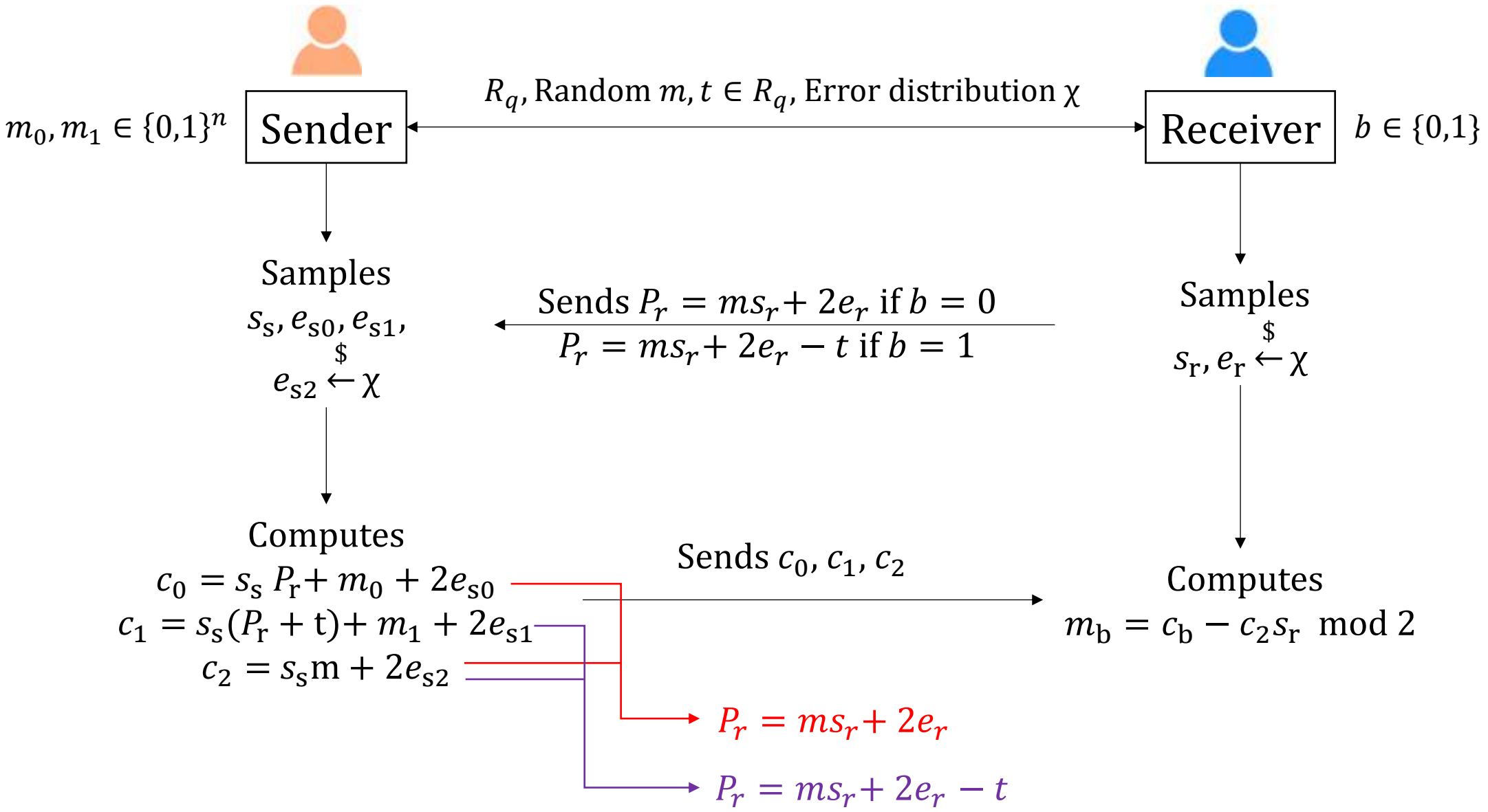
OT Protocol Technique Overview



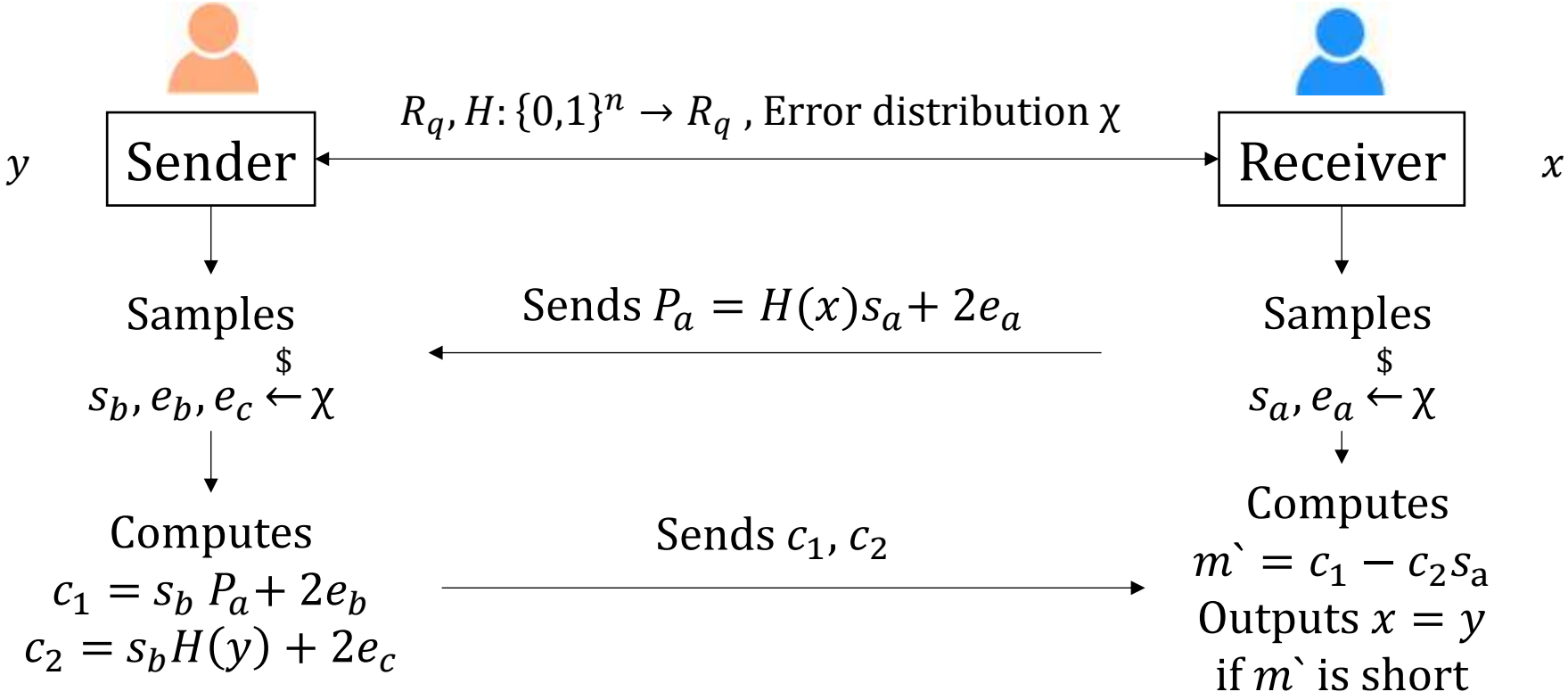
Our 1-out-of-2 OT Protocol



Our Improved 1-out-of-2 OT Protocol



PET Protocol Efficiency



Communication cost: 3nlog q bits

Computation cost: 4 multiplications in R_q, 5 random samples

Communication and computation cost less than a single round of RLWE encryption and decryption

OT Protocol Efficiency

Scheme	Communication Cost	Computation Cost
PET protocol	3nlog q bits	4 multiplications in R_q, 5 random samples
1-out-of-2 OT protocol	5nlog q bits	6 multiplications in R_q, 8 random samples
Improved 1-out-of-2 OT protocol	4nlog q bits	5 multiplications in R_q, 6 random samples

References

[BDD17] Barreto PSLM, David B, Dowsley R, et al. A framework for efficient adaptively secure composable oblivious transfer in the ROM[J]. arXiv preprint arXiv:1710.08256, 2017.

[KAR15] Karimian Ardestani N. Efficient Non-Interactive Secure Two-Party Computation for Equality and Comparison[D]. University of Calgary, 2015.

[Lip03] Lipmaa H. Verifiable homomorphic oblivious transfer and private equality test[C]//Advances in Cryptology-ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, November 30–December 4, 2003. Proceedings 9. Springer Berlin Heidelberg, 2003: 416-433.

[NP99] Naor M, Pinkas B. Oblivious transfer and polynomial evaluation[C]//Proceedings of the thirty-first annual ACM symposium on Theory of computing. 1999: 245-254.

[PVW08] Peikert C, Vaikuntanathan V, Waters B. A framework for efficient and composable oblivious transfer[C]//Annual international cryptology conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008: 554-571.

[SK16] Saha T K, Koshiba T. Private equality test using ring-LWE somewhat homomorphic encryption[C]//2016 3rd Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE). IEEE, 2016: 1-9.

[SK18] Saha T K, Koshiba T. Outsourcing private equality tests to the cloud[J]. Journal of information security and applications, 2018, 43: 83-98.

Thanks!