Development and Implementation of Novel Pair Value Encryption System

Rushil Mallarapu*

June 6, 2021

Abstract

Multiparty cryptography (MPC) is a cryptographic paradigm that seeks to have multiple, mutually distrustful parties compute a joint function of their inputs. Homomorphic encryption (HE) is a related, but distinct paradigm that seeks to allow arbitrary computations to be lifted over encrypted data. In both cases, general versions of such protocols are highly complex, requiring multiple rounds of communication, introducing implementation weaknesses and overheads which limit their practical efficacy. This research merges the insights behind these paradigms to develop what we term Pair Value Encryption (PVE), a lightweight protocol for performing arbitrary Boolean comparisons over encrypted data originating from potentially distrustful parties. We propose an abstract definition for PVE systems, demonstrate a protocol implementing this specification, and prove this protocol is both correct and secure. Python implementation and an example use case in patient matching in healthcare systems demonstrate both the low overhead and real-world applicability of this paradigm.

Keywords — Multiparty Communication, Homomorphic Encryption, RSA

1 Introduction

2 Theory

Theory – Algorithm, Proof of Correctness, Proof of Reducability to Strong RSA

3 Implementation

Implementation – Python code, performance benchmarks, examples

4 Discussion

Discussion – Reflect on performance, ease of implementation, and

5 Conclusion

* *rushil.mallarapu@gmail.com*

Use Euler's theorem to compute:

1. $5^{60} \pmod{21}$
2. $2^{35} \pmod{35}$

5.1

First, we verify that 5 and 21 are coprime, which they are. Then, we compute $\phi(21)$ via the standard route of decomposing 21 as its prime factorization $21 = 3 \cdot 7$. Thus, $\phi(21) = \phi(3)\phi(7) = 2 \cdot 6 = 12$. Now, by Euler's theorem, it holds that $5^{12} \equiv 1 \pmod{21}$. Dividing 60 by 12 gives $60 = 5 \cdot 12 + 0$, by the division algorithm. Therefore, $5^{60} \equiv (5^{12})^5 \equiv 1^5 \equiv 1 \pmod{21}$. Thus, $5^{60} \equiv 1 \pmod{21}$.

5.2

As before, we verify that 2 and 35 are coprime, which they are. Next, we compute $\phi(35)$ by decomposing 35 as its prime factorization $35 = 5 \cdot 7$. Thus, $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$. Now, by Euler's theorem, it holds that $2^{24} \equiv 1 \pmod{35}$. Dividing 35 by 24 gives $35 = 1 \cdot 24 + 11$, by the division algorithm. Therefore, $2^{35} \equiv (2^{24})^1 \cdot 2^{11} \equiv 1^1 \cdot 2^{11} \equiv 2048 \pmod{35}$. From here, we can use the division algorithm to divide 2048 by 35, giving $2048 = 58 \cdot 35 + 18$. Thus, $2^{35} \equiv 18 \pmod{35}$.

6

Find the last two digits of 123^{403}.

6.1

We want to find the value of $123^{403} \pmod{100}$. First, we verify that 123 and 100 are coprime, as indeed they are. Now, we find $\phi(100) = \phi(2^2 \cdot 5^2) = \phi(2^2)\phi(5^2) = (4-2)(25-5) = 2 \cdot 20 = 40$ as per the usual method. Thus, by Euler's theorem, we have that $123^{40} \equiv 1 \pmod{100}$. Using the division algorithm, we have that $403 = 10 \cdot 40 + 3$. As such, $123^{403} \equiv (123^{40})^10 \cdot 123^3 \equiv 1^10 \cdot 123^3 \equiv 123^3 \equiv 1860867 \pmod{100}$. Finally, taking the last two digits of this, we have that $123^3 \equiv 67 \pmod{100}$. Thus, the final two digits of 123^{403} are 67.

7

Alice chooses primes $p = 17$ and $q = 23$, as well as public key 7. What is the RSA decryption exponent?

7.1

Here, we start by applying the RSA cryptosystem to generate the modulus $n = pq$, which here is $n = 17 \cdot 23 = 391$. We also compute $\phi(n) = (p-1)(q-1) = 16 \cdot 22 = 352$ Next, the public encryption key is $e = 7$, and it is trivial to verify that 7 and 352 are coprime. Now, we must find the decryption key d by solving $ed \equiv 1 \pmod{\phi(n)}$, or $7d \equiv 1 \pmod{352}$.

To solve this, we start by knowing that $\gcd(7, 352)$ is of course one, so there will be only one unique solution d. Now, we apply the extended Euclidean algorithm to (352, 7).

$$\begin{aligned} &\gcd(352, 7) && 352 = 50 \cdot 7 + 2 \\ =&\gcd(7, 2) && 7 = 3 \cdot 2 + 1 \\ =&\gcd(2, 1) && 2 = 2 \cdot 1 + 0 \\ =&1 \end{aligned}$$

	x	y
352	1	0
7	0	1
2	1	-50
1	-3	151

Therefore, the solution to this congruence is $d \equiv 151 \cdot 1 \equiv 151 \pmod{352}$, and it is easy to verify that $7 \cdot 151 \equiv 1057 \equiv 1 \pmod{352}$. Thus, the decryption exponent is $d = 151$.