

To securely compute the scalar product $\vec{A} \cdot \vec{B}$ without sharing their inputs to each other, Alice and Bob can use the following Fairplay protocol:

Initialization phase:

- Alice and Bob agree on a common cryptographic hash function H , which will be used to generate random values in the protocol.
- They also agree on a common Boolean circuit C that computes the scalar product of two Boolean vectors of length 10.

Input masking phase:

- Alice and Bob each generate a random Boolean vector \vec{R} with 10 entries.
- They use H to compute two shared secrets $s1$ and $s2$, and they XOR their respective input vector and random vector with the shared secret to obtain the masked inputs \vec{A}' and \vec{B}' , such that $\vec{A}' = \vec{A} \oplus \vec{R} \oplus s1$ and $\vec{B}' = \vec{B} \oplus \vec{R} \oplus s2$.

Circuit evaluation phase:

- Alice and Bob evaluate the circuit C on the masked inputs \vec{A}' and \vec{B}' , which yields a masked output $0'$.
- They use H to compute a new shared secret $s3$, and XOR the masked output with the shared secret to obtain the final output 0 , such that $0 = 0' \oplus s3$.

Output phase:

- Alice and Bob exchange their respective shared secrets $s1$, $s2$, and $s3$.
- They each compute the unmasked output as $0 = 0' \oplus s1 \oplus s2 \oplus s3$, which is the scalar product $\vec{A} \cdot \vec{B}$.

The protocol ensures that Alice and Bob do not learn each other's inputs, as the input masking ensures that the masked inputs reveal no information about the inputs themselves. Moreover, the use of shared secrets ensures that the final output is only revealed to Alice and Bob, and cannot be computed by any eavesdropper who does not have access to all three shared secrets.

To implement this protocol using Fairplay, Alice and Bob can write their respective input and output functions in a Fairplay-compatible language. The functions can then be compiled into circuits and evaluated using the Fairplay runtime system.

Example Results

For $\vec{A} \cdot \vec{B} = 0$ result

Alice's private vector, \vec{A}

[0, 1, 0, 0, 1, 0, 1, 1, 0, 1]

Bob's private vector, \vec{B}

[0, 1, 0, 0, 0, 0, 0, 0, 0, 1]

Output

The scalar product of $\vec{A} \cdot \vec{B}$ is 0

For $\vec{A} \cdot \vec{B} = 1$ result

Alice's private vector, \vec{A}

[1, 1, 0, 1, 0, 0, 1, 0, 1, 1]

Bob's private vector, \vec{B}

[0, 0, 0, 1, 0, 0, 0, 1, 1, 1]

Output

The scalar product of $\vec{A} \cdot \vec{B}$ is 1