Suppose there are $u$ users and each user $i$ possesses $x_i \in \{0,1\}^n$ and a function $F_i : \{0,1\}^{nu} \to \{0,1\}^m$. Then we wish to construct a protocol such that at its completion, each user $i$ knows $F_i(x_1, \ldots, x_u)$ but knows nothing more about $x_j$ for $j \neq i$.

Clearly this could be done with a trusted third party, but we want to do it without one.

Security models:

- *Honest-but-curious*: all $u$ parties follow the protocol honestly, and a protocol is $t$-private if any $t$ parties who collude at the end of the protocol learn anything beyond their own outputs from their transcripts.
  To prove a protocol is $t$-private, we build a simulator that, when given inputs and outputs of $t$ colluding parties, generates $t$ transcripts from the same distribution as the actual protocol. (For this implies anything the colluding users can learn from their transcripts can be learnt from their inputs and outputs alone.)
- *Malicious users*: the adversary controls a fixed set of $t$ users. The remaining $u - t$ users are honest. A protocol is $t$-secure if the adversary learns nothing about the $u - t$ user inputs beyond the outputs of the $t$ corrupt parties.
  Usually, the goal is to construct a $t$-secure, $t'$-private protocol for some $t' \geq t$.
- *Dynamic adversary*: in this case, at any time period, the adversary can corrupt any $t$ users.

## Example

Suppose we have three users, who's secrets are $x_1, x_2, x_3 \in \mathbb{F}_p$, and their functions are $F_1 = F_2 = F_3 = x_1 + x_2 + x_3$.

Trivially, any valid protocol is 2-private because if two parties collude, they can determine the third party's secret.

A 1-private protocol can be constructed by using secret sharing:

User 1: $r_1, s_1 \leftarrow \mathbb{F}_p, 1 \to 2 : r_1, 1 \to 3 : s_1$

User 2: $r_2, s_2 \leftarrow \mathbb{F}_p, 2 \to 1 : r_2, 2 \to 3 : s_2$

User 3: $r_3, s_3 \leftarrow \mathbb{F}_p, 3 \to 1 : r_3, 3 \to 2 : s_3$

(can be done in parallel)

User 1: publishes $y_1 = (x_1 - r_1 - s_1) + r_2 + r_3$

User 2: publishes $y_2 = (x_1 - r_2 - s_2) + r_1 + s_3$

User 3: publishes $y_3 = (x_1 - r_3 - s_3) + s_1 + s_2$

Then each user computes $y_1 + y_2 + y_3 = x_1 + x_2 + x_3$.

1-privacy proof: user 1's transcript is $[x_1, r_1, s_1, r_2, r_3, y_2, y_3, x_1 + x_2 + x3]$. Then we construct a simulator as follows: given $x_1, z = x_1 + x_2 + x_3$, we generate the transcript by picking $r_1, s_1, r_2, r_3, y_2 \leftarrow \mathbb{F}_p$, setting $y_1 = (x_1 - r_1 - s_2) + r_2 + r_3$, and outputing $[x_1, r_1, x_1, r_2, r_3, y_2, z - y_1 - y_2, z]$. From user 1's view, $y_2$ is random because user 1 never sees $s_3$. We can construct simulators for the other users in a similar fashion.

This protocol generalizes to $n$ parties and any linear combination, and becomes a $(n-2)$-private protocol. It is sometimes referred to as Benaloh's protocol.

## Modeling Cryptographic Protocols

Practically any cryptographic protocol can be described in terms of SFE. For example:

- **Identification:** $A$ has a secret key $x$, and a public key $f(x)$ for some one-way function $f$, and wishes to prove possession of $x$ to $B$.
  In SFE terms: $A$'s input is $x$, $F_A = 0$, $B$'s input is $f(x) = y$, $F_B(x, y) = (y = f(x))?1 : 0$.
  (The SFE model captures the fact that $B$ should not learn anything about $x$.)
- **Key exchange:** (secure against eavesdropping). Three parties, Alice, Bob, Eve. $x_A = r, x_B = 0, x_E = 0, F_A = 0, F_B = r, F_E = 0$, and Eve is passive, i.e. does not send any messages.
- **Voting:**$x_i \in \{0, 1\}$ for $i = 1, \ldots, u$, $F_i = \ldots = F_u = MAJORITY(x_1, \ldots, x_u)$.
- **Threshold signatures:** Let $PK, SK$ be a public/private key pair for some signature scheme. Take $SK = SK_1 \oplus \ldots \oplus SK_u$. $x_i = SK_i$ for $i = 1, \ldots, u$, $F_i = \ldots = F_u = Sign(SK_1 \oplus \ldots \oplus SK_u, M)$.
- **Private auctions:** (sealed bid, 2nd-price auction) $x_i$ = bid of user $i$. Let $S = 2ND - MAX(x_1, \ldots, x_u)$.

$$F_1 = \ldots = F_u = (x_i = MAX(x_1, \ldots, x_u))?S : 0.$$

## Results

1. [Yao’82,Yao’86,GMW’87,G’97] 2-party SFE (using complexity assumptions)
2. [BGW’87] $n$-party SFE for $n > 2$, $\lfloor n/2 \rfloor - 1$-private (information theoretic result)

[My Homepage] *Email: blynn pleasedontspamme at cs dot stanford dot edu*