Anonymous Interaction for Collective Outcome with Verifiability

Mirko Randic

(Important notes: Dedicated to Aaron Swartz, 2013 USPTO – Patent Pending Status)

A process where everyone can interact by broadcasting encrypted conditional commitment segments, and at the end, everyone must undisputedly agree on quantifiable collective outcome, and no-one should know which way anyone else intentions was.

PROCESS EXPANATION

To describe the process we are using the simplest possible application example of voting with two participants and with two valid choices for each participant, which generate quantifiable outcome by adding each type of choice into summary groups. Other more complex applications can have different rules and boundary limits, but basic steps, as described here, are the same.

The process consists of three main phases: Preparation, Interaction and Conclusion as shown in block diagram of the process.

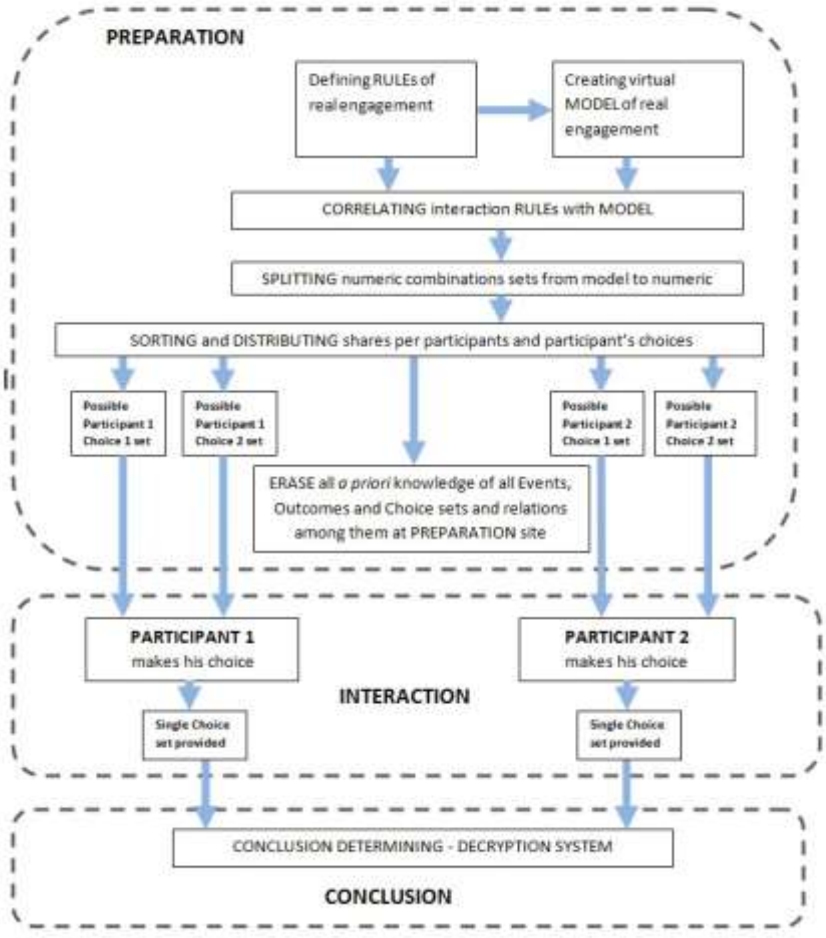
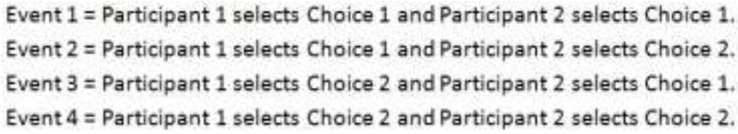

PREPARATION
Defining RULEs of real engagement
Creating virtual MODEL of real engagement
CORRELATING interaction RULEs with MODEL
SPLITTING numeric combinations sets from model to numeric
SORTING and DISTRIBUTING shares per participants and participant's choices
Possible Participant 1 Choice 1 set
Possible Participant 1 Choice 2 set
Possible Participant 2 Choice 1 set
Possible Participant 2 Choice 2 set
ERASE all *a priori* knowledge of all Events, Outcomes and Choice sets and relations among them at PREPARATION site
PARTICIPANT 1 makes his choice
PARTICIPANT 2 makes his choice
INTERACTION
Single Choice set provided
Single Choice set provided
CONCLUSION DETERMINING - DECRYPTION SYSTEM
CONCLUSION

Figure 1.

PREPARATION phase

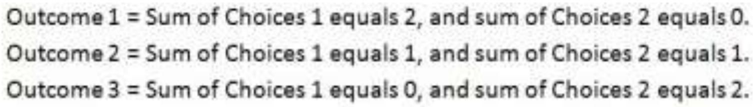
In preparation phase it is necessary to define real engagement rules for each possible real event of each possible interaction.

All possible REAL EVENTs; List 1



Event 1 = Participant 1 selects Choice 1 and Participant 2 selects Choice 1.
Event 2 = Participant 1 selects Choice 1 and Participant 2 selects Choice 2.
Event 3 = Participant 1 selects Choice 2 and Participant 2 selects Choice 1.
Event 4 = Participant 1 selects Choice 2 and Participant 2 selects Choice 2.

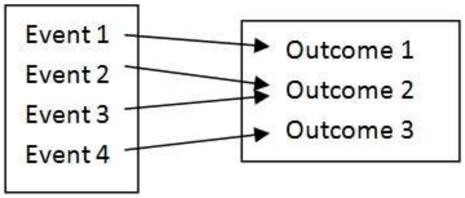
All possible REAL OUTCOMEs; List 2



Outcome 1 = Sum of Choices 1 equals 2, and sum of Choices 2 equals 0.
Outcome 2 = Sum of Choices 1 equals 1, and sum of Choices 2 equals 1.
Outcome 3 = Sum of Choices 1 equals 0, and sum of Choices 2 equals 2.

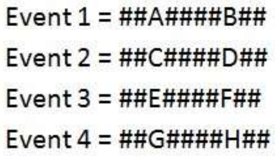
Relations among all possible REAL EVENTs and REAL OUTCOMEs;

Table 1.



Beside real environment there is abstract MODEL of such environment defined as:

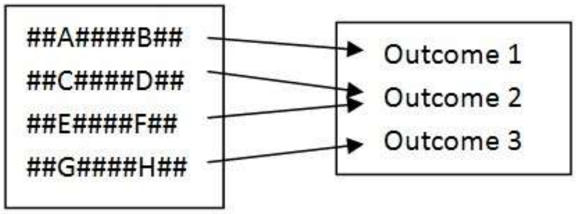
All modeled EVENTs; List 3.



Event 1 = ##A####B##
Event 2 = ##C####D##
Event 3 = ##E####F##
Event 4 = ##G####H##

and relations among modeled Events and Outcomes; should be compatible with table 1 and are shown in table 2.

Table 2.



Corresponding elements of both environments sets are all possible events, all possible outcomes and relation among them. In real environment we have simple human language logical description in plain text where each participant should understand the rules of the interaction for particular application. In modeled abstract environment instead of elements in natural language we have numerical combination of characters which have exactly the same relations among themselves as corresponding elements in real environment. The relations among real and virtual elements of two groups are homomorphic in nature because a transformation from one structure to another of the same type is made so that the structure is preserved.

Importantly, this means that for every kind of manipulation of original real data, there is a corresponding manipulation of the transformed modeled data. Surjective relations among elements from table 1 and table 2 are identical.

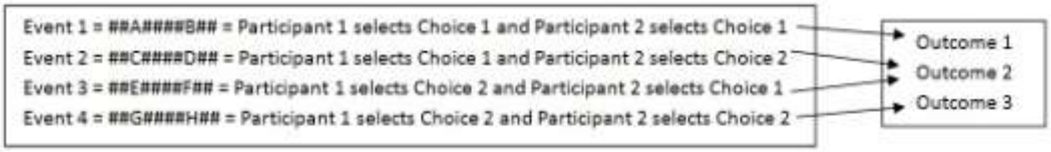

Event 1 = ##A####B## = Participant 1 selects Choice 1 and Participant 2 selects Choice 1
Event 2 = ##C####D## = Participant 1 selects Choice 1 and Participant 2 selects Choice 2
Event 3 = ##E####F## = Participant 1 selects Choice 2 and Participant 2 selects Choice 1
Event 4 = ##G####H## = Participant 1 selects Choice 2 and Participant 2 selects Choice 2
Outcome 1
Outcome 2
Outcome 3

Figure 2.

In process of creating cryptographic model of anonymous engagement, we use standard symmetrical encryption process with unique crypto key, which is associated with all modeled relations for particular application instance. Beside key there are Initiation Vectors (IV) to bring additional entropy for each encrypt transformation and provide surjective relations. IV mixes together with cipher and is not needed to decrypt back to plain source. The key and IV doesn't necessary need to be secret in simple applications, since data integrity and surjective properties of segments are objectives of this process. In case where single outcome models (Outcome2 in our example) need to correspond to multiple events (Event2 and Event3 in our example) we arbitrary use different numerical value for IV as seed in encryption process as shown on figure:

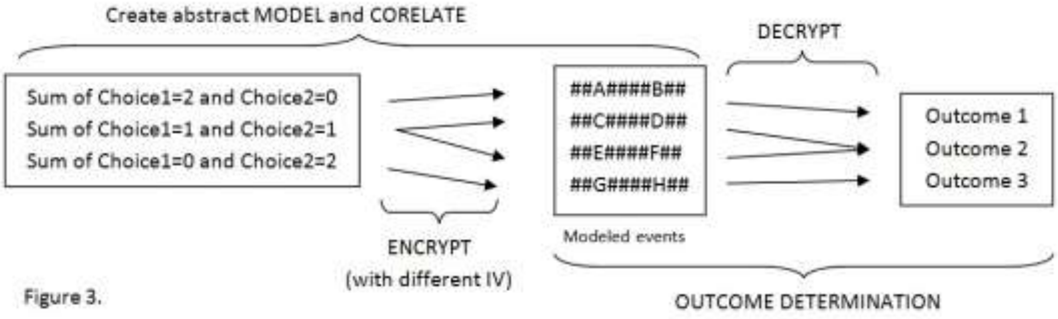


Figure 3.

However, different IV-s causes creation of different encryption results or ciphers or modeled events in our case, although for each of these ciphers by decryption we are starting the same source value or plaintext. On this way we can create table with the same surjective relations as defined for real relations among real events and real outcomes.

At this point we have all necessary components of *a priori* knowledge to calculate numerical values of abstract model for each event instance which would actually correlate in abstract environment on the same way as real world event instances are correlating in real environment. Now we can split events to multiple sub-segments which would correspond to different participants and different choices;

SPLITTING POINT SPLITTING POINT of real event descriptive sentence is to separate
. ↓ ↓ participants to their unique choice instances.

##A## ##B## = Participant 1 selects Choice 1 and Participant 2 selects Choice 1
##C## ##D## = Participant 1 selects Choice 1 and Participant 2 selects Choice 2
##E## ##F## = Participant 1 selects Choice 2 and Participant 2 selects Choice 1
##G## ##H## = Participant 1 selects Choice 2 and Participant 2 selects Choice 2

↓

SORTING into sub segments based on participants

↓

Sub-segment 1 = ##A## = Participant 1 selects Choice 1
Sub-segment 2 = ##C## = Participant 1 selects Choice 1
Sub-segment 3 = ##E## = Participant 1 selects Choice 2
Sub-segment 4 = ##G## = Participant 1 selects Choice 2

Sub-segment 5 = ##B## = Participant 2 selects Choice 1
Sub-segment 6 = ##F## = Participant 2 selects Choice 1
Sub-segment 7 = ##D## = Participant 2 selects Choice 2
Sub-segment 8 = ##H## = Participant 2 selects Choice 2

↓

RE-GROUPING - by combining sub-segments for each participant into
. sets with equal choice.

↓

Possible Participant 1 Choice 1 set = ##A## and ##C## (set of two sub segments)
Possible Participant 1 Choice 2 set = ##E## and ##G## (set of two sub segments)

Possible Participant 2 Choice 1 set = ##B## and ##F## (set of two sub segments)
Possible Participant 2 Choice 2 set = ##D## and ##H## (set of two sub segments)

At this point all groups are only possibilities and need to be distributed to participants on a way that each participant has knowledge only of his choice sets, and not of other participant choice sets.

All reminding knowledge on preparation place or computer should and can be erased and only if all participants conspire together against one in the process with their segmented knowledge they can reveal identity of single participant. The exceptions are knowledge from list 2 which would be needed for interpretation of decryption result in conclusion phase of process.

INTERACTION phase

The interaction phase is when each participant makes his decision by publishing his single choice related to common outcome. In our example of simple voting this would be for participant 1 selecting and publishing one group of two sub-segments and participant 2 publish his choice the same way.

CONCLUSION phase

After collection of all published choices in form of sets of sub segments at one place in conclusion phase the actual collective outcome can be determined by decrypting all possible combinations of published and collected sub segments. The only one combination will produce valid model outcome from list 2. All other combinations should produce integrity violation warning during decryption process and should be discarded.

The unique and quantifiable collective outcome in real environment as determined from list 2 and is based on model outcome calculated using single-way cryptographic process from figure 3. The actual event causing particular outcome cannot be identified.

The verification can be performed by each participant in privacy of his computational environment to determine that his choice is implemented correctly into outcome. This can be done on the way that he uses his other choice instead with other participants already published segments to determine new outcome in privacy of his own cryptographic resources. The new outcome should accurately reflect only change participant made by his new hypothetical choice. If there are only two participants together in application the logical abstraction can be made by participant to discover other participant's choice selection. To preserve anonymity of other participants there should be three or more participants in application or self verification should be prevented by hiding common password.

Other applications can have multiple round of interaction with even different participants, or outcome calculation can involve complex mathematical algorithms, or even fuzzy logic. The number of choices and meaning of choices for participants can wary, depending on its role in application. The choices don't need to have equal leverage toward common outcome. The mix of anonymous, secret and open interaction can coexist.