(FV_{GEN}^{2PC}) and/or a two-party computation fuzzy vault opener (FV_{OPEN}^{2PC}), as described herein.

[0168] Referring now to FIG. 5B, and with continued reference to FIG. 5A, FIG. 5B is an exemplary swimlane diagram for a non-limiting embodiment or aspect of a two-party computation fuzzy vault generator (FV_{GEN}^{2PC}) relating to implementation 500 of FIG. 5A.

[0169] In some non-limiting embodiments or aspects, FV_{GEN}^{2PC} may generate fuzzy vault helper data (HD) that may allow for efficient oblivious authentication, as further described below. In some non-limiting embodiments or aspects, FV_{GEN}^{2PC} may be executed when the user first registers (e.g., using user device 506) with authentication system 502. In some non-limiting embodiments or aspects, user device 506a may be a trusted enrollment device (e.g., a device under the control of the organization deploying authentication system 502 and/or the like). Upon enrollment (e.g., upon execution of FV_{GEN}^{2PC} and/or the like), authentication system 502 may store (e.g., persistently store) the HD in association with an identifier of the user (e.g., a username, user identifier (U_{ID}) and/or the like).

[0170] As shown in FIG. 5B, FV_{GEN}^{2PC} may include user device 506a receiving inputs. For example, the inputs may include a user identifier (U_{ID}), first biometric input data (e.g., biometric template (BT)) associated with a first biometric input, first secret key data associated with a first secret key (K), any combination thereof, and/or the like. Additionally or alternatively, the inputs may include at least one parameter, such as a polynomial degree (d), a distance function (dist), a distance threshold (w), a number (m) of biometric data points (e.g., bt_1, …, bt_m), a number (n) of random data points (e.g., c_1, …, c_n), any combination thereof, and/or the like. In some non-limiting embodiments or aspects, authentication system 502 may not need any inputs (but, as further describe below, authentication system 502 may receive certain information from user device 506).

[0171] As shown in FIG. 5B, at line 1, FV_{GEN}^{2PC} may include extracting a plurality of first biometric data points from the first biometric input. For example, user device 506a may extract biometric data points from the biometric template (e.g., Ext(BT) = { bt_1, …, bt_m }). Additionally or alternatively, the extracted biometric data points may be stored in a first list (L_m).

may be selected from the set $\mathbb{Z}_p$ (e.g., $e \in \mathbb{Z}_p$), which may be finite. In some non-limiting embodiments or aspects, each respective data point in the set of encodings may be stored (e.g., by user device 506) as a tuple with the respective set of neighboring data points and/or the respective polynomial encoding. For example, a tuple (e, p_e) may be generated (e.g., by user device 506) for each e. Additionally or alternatively, each respective tuple may be associated with the respective set of neighboring data points (e.g., $[s_e, (e, p_e)]$). In some non-limiting embodiments or aspects, if the respective e is a biometric data point (e.g., $e \in L_m$), the respective p_e (e.g., in the tuple with the respective e) may include the polynomial encoding of the respective biometric data point (e.g., $p_e = P_k(e)$). Additionally or alternatively, if the respective e is a random data point (e.g., $e \in L_n$), the respective p_e (e.g., in the tuple with the respective e) may include the random encoding of the respective random data point (e.g., $p_e = \$\mathbb{Z}_p$). In some non-limiting embodiments or aspects, each biometric data point (e.g., $e \in L_m$) may be associated with a Shamir secret share of the key (K), and/or the shares of K and the random tuples may be indistinguishable given randomness of K. In some non-limiting embodiments or aspects, each of the elements $[s_e, (e, p_e)]$ for neighbor set (s_e) and tuple (e, p_e) may be added to the set (S).

[0179] As shown in FIG. 5B, at line 8, FV_{GEN}^{2PC} may include permuting (e.g., randomly shuffling and/or the like) the set of encodings. For example, the set (S) may be shuffled (e.g., by user device 506) using the random permutation (e.g., Π(S)). In some non-limiting embodiments or aspects, the shuffled set may be stored as a dataset (D).

[0180] As shown in FIG. 5B, at line 9, FV_{GEN}^{2PC} may include communicating the set (S) (and/or the dataset (D) based on shuffling the set (S)), e.g., from user device 506a to authentication system 502. For example, user device 506a may communicate the dataset (D) to authentication system 502. Additionally or alternatively, user device 506a may communicate other information in addition to the dataset (D), such as the user identifier (U_{ID}) and/or key data associated with the key (K). In some non-limiting embodiments or aspects, the key data may include K. Additionally or alternatively, the key data may include at least one hash based on the key (e.g., a first hash ($H_1(K)$), a second hash ($H_2(K)$), and/or the like). In some non-limiting embodiments or aspects, the hash(es) based on the key (K) may enable challenge-response based authentication, as described herein.

a two party computation PSI-Cardinality (2PC-PCI-CA) protocol to determine the set intersection cardinality between each second biometric data point (bt'_i) and a respective neighbor set s_j (if any). For example, based on the inputs of the second biometric data points (bt'_i) and the neighbor sets (s_j), the result of the 2PC-PCI-CA may include a binary value 1 if dist(bt'_i, e) < w (where e is the (first) biometric data point used to generate the respective neighbor set) and a binary value of 0 otherwise. As such, user device 506a may receive a plurality of encodings (a set of encodings (B_{ij})), e.g., based on the respective second biometric data points and/or the shuffled dataset.

[0191] As shown in FIG. 5C, at lines 5 and 6, FV_{OPEN}^{2PC} may include learning an intersection set (X) based on the set of encodings (B_{ij}). For example, each intersection data point (X_j) of the intersection set (X) may include the sum of the respective subset (e.g., B_{1j} + … + B_{mj}) of the set of encodings (B_{ij}), for all values of j from 1 to m+n. In some non-limiting embodiments or aspects, the intersection set (X) may be associated with positions in the HD that contain points that are close enough (e.g., within the threshold distance w) to each $bt'_i \in Lm$.

[0192] As shown in FIG. 5C, at line 7, FV_{OPEN}^{2PC} may include authentication system 502 communicating (e.g., to user device 506a) a tuple set (Y) (e.g., a set of all tuples (e, p_e)), which may be in the same order as the neighbor sets (s_j) from the shuffled dataset ($D_{\$}$). Additionally or alternatively, user device 506a may initialize and empty candidate set (C). In some non-limiting embodiments or aspects, authentication system 502 may also communicate a first hash of the secret key ($H_1(K)$) (e.g., to user device 506a).

[0193] As shown in FIG. 5C, at line 8, FV_{OPEN}^{2PC} may include populating the candidate set (C) based on the intersection set (X) and the tuple set (Y). For example, user device 506a may determine which tuples in the tuple set (Y) are most likely shares of the secret key (K) based on the intersection set (X). For example, for all values of j from 1 to m+n, if X_j is 1, the respective tuple (Yj) from the tuple set (Y) may be added to the candidate set (C). As such, the tuples added to the candidate set (C) may be considered likely to be shares of the secret key (K).

[0194] As shown in FIG. 5C, at line 8, FV_{OPEN}^{2PC} may include generating a reconstructed secret key based on polynomial encodings. For example, user device 506a may interpolate up to $\binom{m}{d}$ candidate polynomial encodings $P_{K'}(.)$ based on the