Figure 4

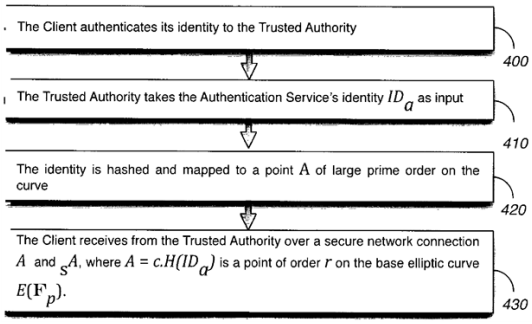


Figure 1

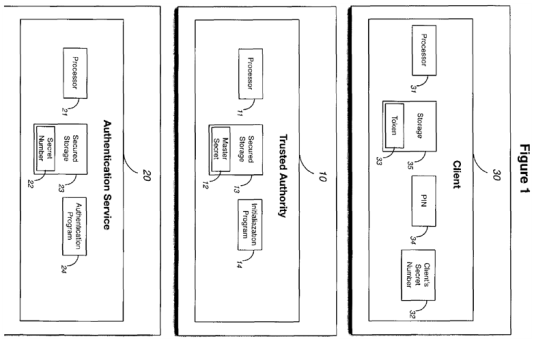


Figure 5

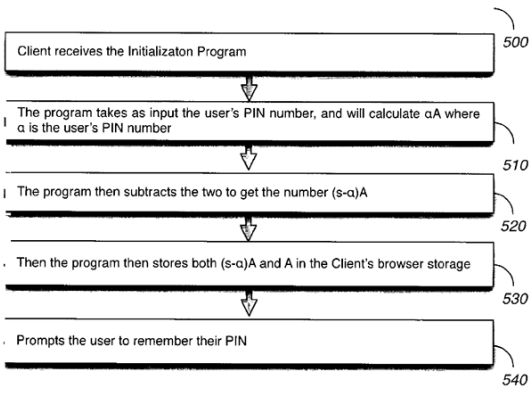


Figure 2

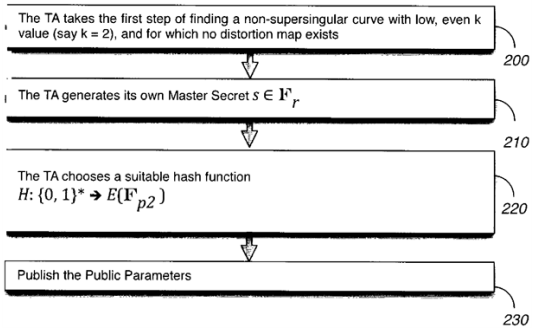


Figure 6

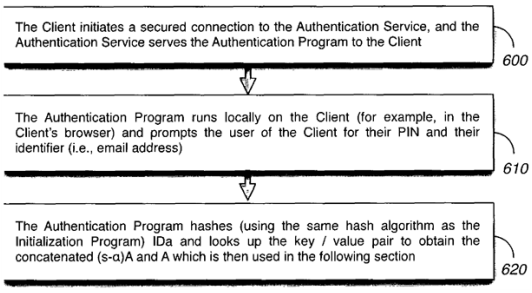
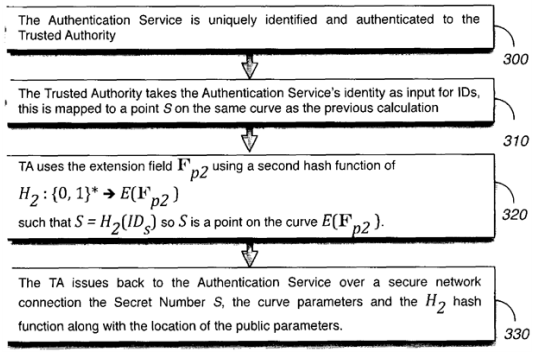


Figure 3



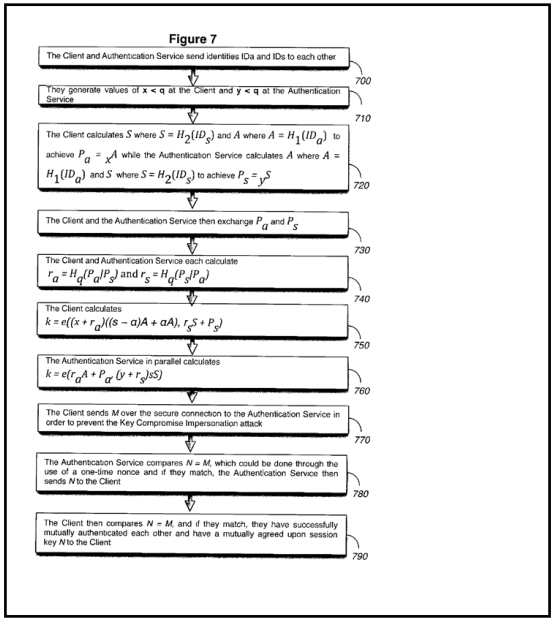


Figure 7
The Client and Authentication Service send identities IDa and IDs to each other
700
They generate values of x < q at the Client and y < q at the Authentication Service
710
The Client calculates S where $S = H_2(ID_S)$ and A where $A = H_1(ID_a)$ to achieve $P_a = xA$ while the Authentication Service calculates A where $A = H_1(ID_a)$ and S where $S = H_2(ID_S)$ to achieve $P_s = yS$
720
The Client and the Authentication Service then exchange P_a and P_s
730
The Client and Authentication Service each calculate $r_a = H_q(P_a|P_s)$ and $r_s = H_q(P_s|P_a)$
740
The Client calculates $k = e((x + r_a)/((s - a)A + aA), r_sS + P_s)$
750
The Authentication Service in parallel calculates $k = e(r_aA + P_a, (y + r_s)sS)$
760
The Client sends M over the secure connection to the Authentication Service in order to prevent the Key Compromise Impersonation attack
770
The Authentication Service compares N = M, which could be done through the use of a one-time nonce and if they match, the Authentication Service then sends N to the Client
780
The Client then compares N = M, and if they match, they have successfully mutually authenticated each other and have a mutually agreed upon session key N to the Client
790