

List of Figures

4.1	Entity registration phase of the proposed protocol.	38
4.2	Key agreement phase of the proposed protocol.	40
5.1	Proposed ID-AKGA protocol for imbalanced mobile networks.	58
7.1	Proposed pairing-free ID-PBS scheme.	113
7.2	Overview of the proposed online e-cash system.	124
7.3	Proposed withdrawal phase.	126
7.4	Proposed payment-deposit phase.	128
8.1	Stolen-verifier attack in Lin and Hwang's scheme.	137
8.2	Insider attack in Lin and Hwang's scheme.	138
8.3	Impersonation attack in Lin and Hwang's scheme.	140
8.4	Many logged-in users' attack in Lin and Hwang's scheme.	142
8.5	KSSTIA attack in Lin and Hwang's scheme.	143
8.6	The proposed ECC-based remote login scheme	147