

**Protocols with Trusted Third Party**

*Sometimes overlap!!*

Index	Protocol Title	File name	Assumptions	Properties	Deliverables	
O n l i n e	1	<b>Rabin's Beacon</b>		Needs Synchronization	no TTP, Parametrized time-out, On-Line TTP	Probabilistic fairness <sup>1</sup>
	2	<b>Zhang &amp; Shi</b>		PKI is used, stored DB at TTP	On-Line TTP, TTP publishes session keys, Stateful TTP	Confidentiality
	3	<b>Zhou &amp; Gollmann</b>		resilient <sup>1</sup> channel	Confidentiality is not ensured	strong fairness, timeliness
O f f l i n e	4	<b>A Fair non-Repudiation Protocol</b>		resilient channel (X-TTP), but non-reliable channel (A-B)	Ability to recover from error, no Timeliness	
	5	<b>A Fair non-Repudiation and Timeliness Protocol</b>		X-TTP channel is resilient, A-B channel is unreliable	Fairness, timeliness, 3 sub protocols (Main, recover, and abort), Time out is dynamic	timeliness is enforced. Confidentiality is not specified explicitly.
	6	<b>Optimal Efficiency of Optimistic CSP</b>		No obvious assumptions were encountered !!	Off-line TTP, round and message-optimal schemes, support async. networks through a <i>wakeup</i> signal. Stateful TTP <i>only in case of</i> time-optimal scheme	Non-repudiation, fairness, Correct execution, unforgeability of contracts, Valid contracts can be verified, No surprises with invalid contracts, timeliness, i.e. termination is guaranteed in both sync. and async. networks.
	7	<b>Optimistic Fair Contract Signing</b>		No obvious assumptions were encountered !!	Optimistic TTP, fairness, 3 sub-protocols (Exchange, Abort, and Resolve)	two types of contracts can result from this protocol: Notarized or Standard.

T T P	8	<b>Inductive Methods and CSPs</b>	TTP behaves well, and has no interest in the contract or any party. Each party has both private and public keys. A-B channel is rw accessible to intruder, while X-TTP channel is read-only accessible to intruder. TTP keeps a DB to store all protocol instances	Optimistic TTP, parties are modeled in terms of dishonesty (weakly and strongly), 3 sub protocols like 7, Use of "Partial Signatures", Abuse-freeness, fairness
	9	<b>An Abuse-Free and Fair CSP based on RSA Signatures</b>	timeliness is based on a predetermined time.	fair, optimistic and stateless TTP, abuse-free, provably secure (RSA), no advantage for any dishonest party whatsoever.

**Note 1:** On Line TTP Protocols are not applicable for dynamic VO, as our case, because, availability and efficiency of TTP is crucial

**Note 2:** Non-repudiation protocols needs good management of evidences, a secure digital signature scheme.

**Note 3:** Network nature and operation is vital, for instance, resilient vs. operational, Synchronous vs. Asynchronous. Thats why a clear definition of the network where the protocol is to be executed is important.

<sup>1</sup> resilient channel: Guaranteed delivery only