学术论文

匿名口令认证与客户端匿名认证的TLS模式

张振峰、杨糠、胡学先、王宇辰
zfzhang@tca.iscas.ac.cn

Practical Anonymous Password Authentication and TLS with Anonymous Client Authentication，ACM CCS 2016：1179-1191

- 随着互联网应用的快速发展，隐私保护备受关注。2016年信息泄漏事件频发，泄露数据近14亿条，隐私保护面临严重挑战。
- 匿名认证作为重要的隐私保护技术得到广泛研究, 在可信计算等领域得到应用；由于口令是最广泛应用的认证方式，匿名口令认证被寄予厚望，ISO/IEC在2010年开始研制相应国际标准。

✓ 我们建立了基于代数MAC的匿名口令认证构造理论，突破已有理论对同态加密的依赖；提出基于q-SDH的实例化方法，实现匿名认证的理论最优性能, 大幅提升ISO/IEC同类机制的性能。

✓ 提出客户端匿名认证的TLS模式， 突破当前模式中客户端“匿名无认证、认证非匿名”限制，研制了高效实用的密码套件。

✓ 实现了匿名认证TLS系统，完全兼容TLS标准，实现FIDO联盟倡导“消除口令文件”，提供用户可控的（不）可链接性。

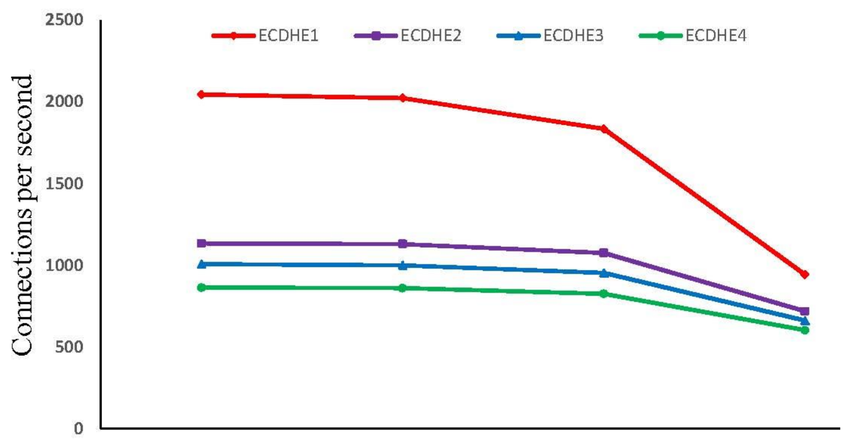

Table 2: Performance of HTTPS using Apache with OpenSSL

Ciphersuite	Connections / second				Connection time (ms)	Handshake (bytes)	Client Auth.
	10 B payload	1 KB payload	10 KB payload	100 KB payload			
ECDHE1	2043.678 (1.06)	2022.282 (1.61)	1833.658 (1.80)	943.266 (1.09)	1.54 (0.05)	2200	None
ECDHE2	1133.08 (1.50)	1129.442 (1.69)	1075.69 (0.48)	718.736 (0.21)	2.39 (0.05)	3806	plain sigs
ECDHE3	1007.308 (2.25)	999.994 (1.74)	953.698 (1.28)	661.652 (1.02)	2.80 (0.01)	4078	anon. sigs
ECDHE4	863.712 (1.49)	860.364 (1.32)	826.032 (0.92)	602.928 (0.24)	3.40 (0.02)	4179	anon. sigs w/revoc.

Legend: mean, (std. dev.) in columns 2-6; **Client Auth.** represents the type of signatures used to provide client authentication.