MPCAuth: Multi-factor Authentication for Distributed-trust Systems

Sijun Tan, Weikeng Chen, Ryan Deng, and Raluca Ada Popa
2023 IEEE Symposium on Security and Privacy

目录

CATALOGUE

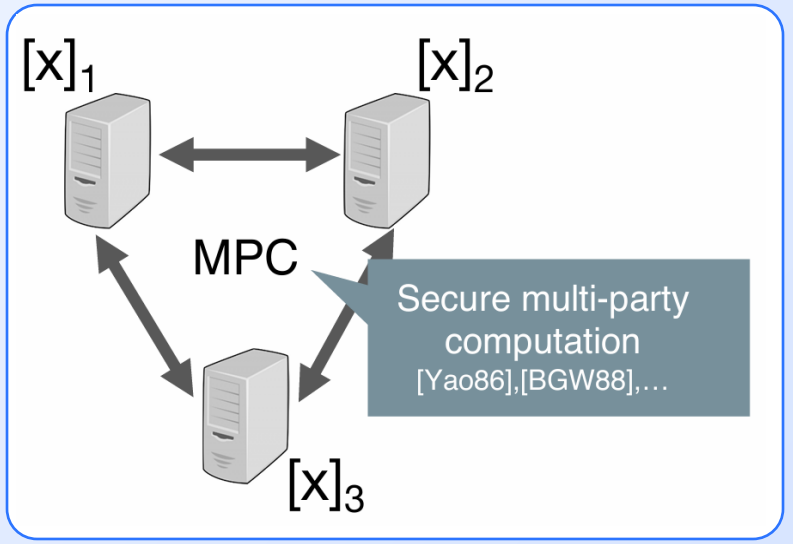
Part 01

研究背景与挑战

分布式信任系统的发展

分布式信任系统的应用场景

分布式信任系统在数字货币托管（如Curv、Fireblocks）、协作机器学习（如Meta、Ant Group）等领域广泛应用。这些系统通过将秘密分散存储在多个服务器上，避免了单点攻击风险，提升了系统的安全性。



[Yao86] Andrew Chi-Chih Yao. How to generate and exchange secrets. In FOCS ’ 86.
[BGW88] M. Ben-Or, S. Goldwasser, and A. Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended ab stract). In 20th STOC, pages 1–10, 1988.

分布式信任系统的认证挑战

易用性

可以让客户端向其他服务器信任的一个主服务器进行身份验证，但这种方法会破坏分布式信任；客户端可以独立地向N个服务器进行身份验证，但若含有M个身份认证因素，用户则需要进行N*M次认证。

隐私性

在集中式信任系统中，一个服务器了解客户的配置文件信息，而在分布式信任设置中，还有N-1台服务器也在学习这些私有信息。本质上，这是客户端身份数据的N倍攻击面

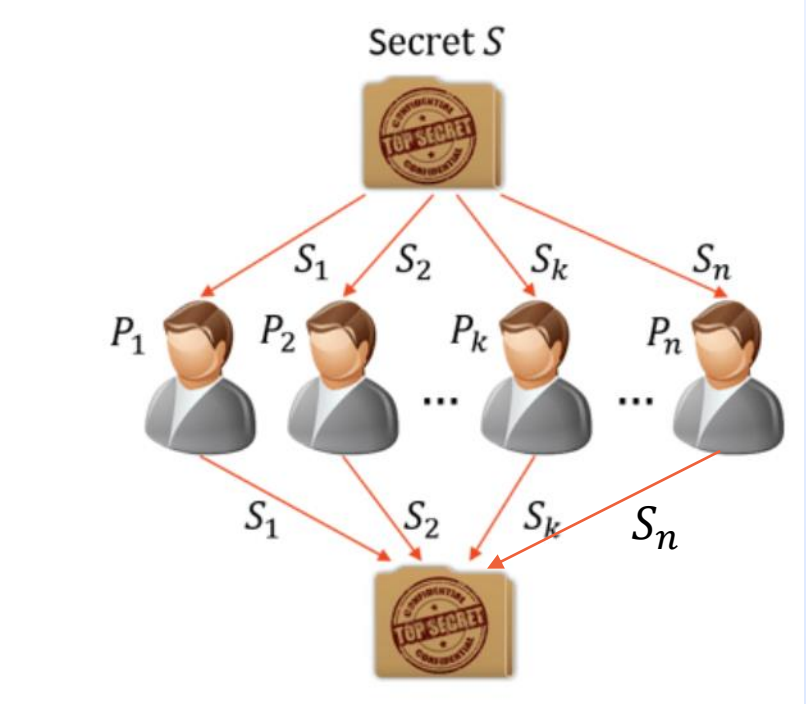
传统的认证方式无法满足分布式信任系统的需求，需要一种新的认证机制来解决这些问题。

Part 02

MPCAuth系统设计

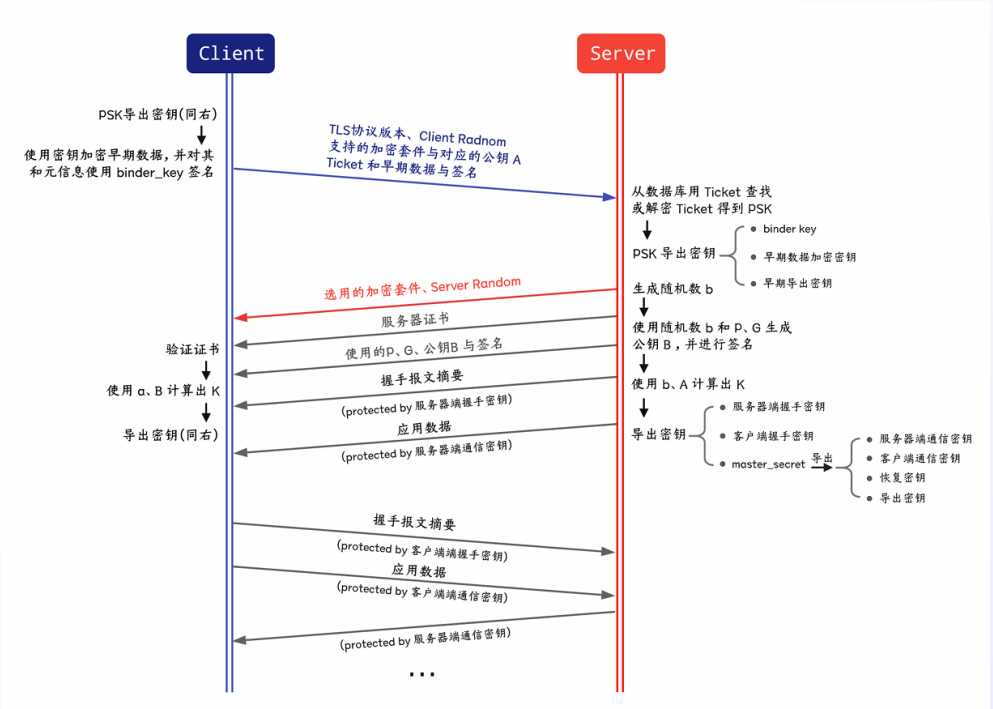
相关知识

秘密共享：将秘密以适当的方式拆分，拆分后的每一个份额由不同的参与者管理，单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息。

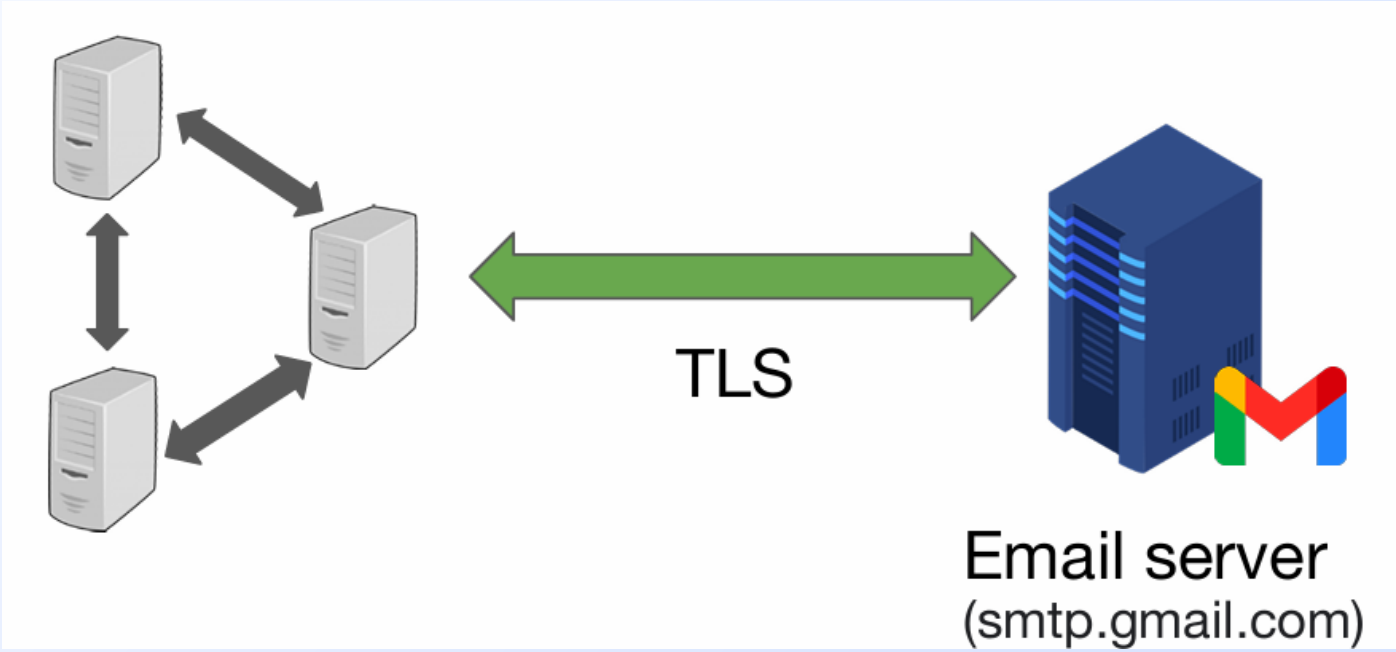


相关知识

传输层安全性协议（TLS）用于在两个通信应用程序之间提供保密性、数据完整性以及真实性。



TLS



TLS in SMPC

MPCAuth核心理念

01

单次认证实现多服务器认证

MPCAuth允许用户只需进行一次认证操作，即可完成对多个服务器的认证。该系统利用安全多方计算（SMPC）技术，将多个服务器视为一个逻辑服务器，联合生成认证挑战并验证用户响应，从而实现了单次认证的多服务器认证功能。

02

隐私保护与认证安全

MPCAuth还能够隐藏用户的认证信息，除非所有服务器都被攻破，否则用户的隐私信息不会泄露。系统支持多种常见的认证因素，包括邮箱验证码、短信验证码、U2F、安全问题/密码和生物识别等，并为每种认证因素设计了安全、高效的协议，确保在分布式信任环境下的认证安全。

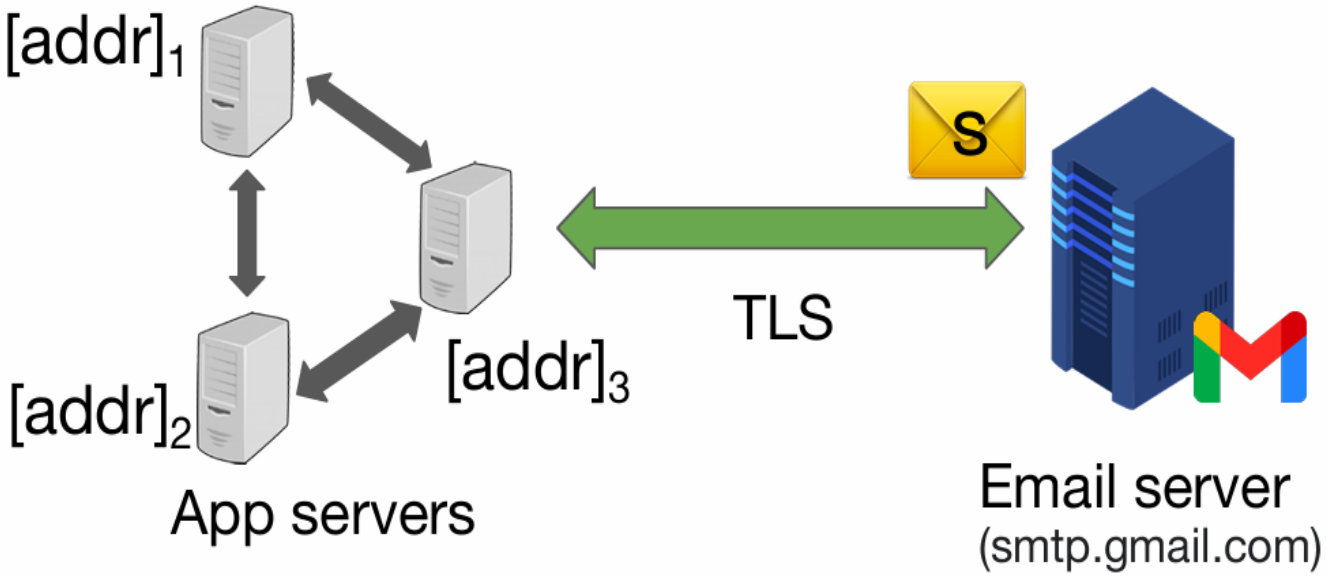
Part 03

MPCAuth认证协议

电子邮件认证

注册流程

用户基于邮件地址生成多个秘密共享份额并分别发送个N个服务器。N个服务器联合运行认证协议



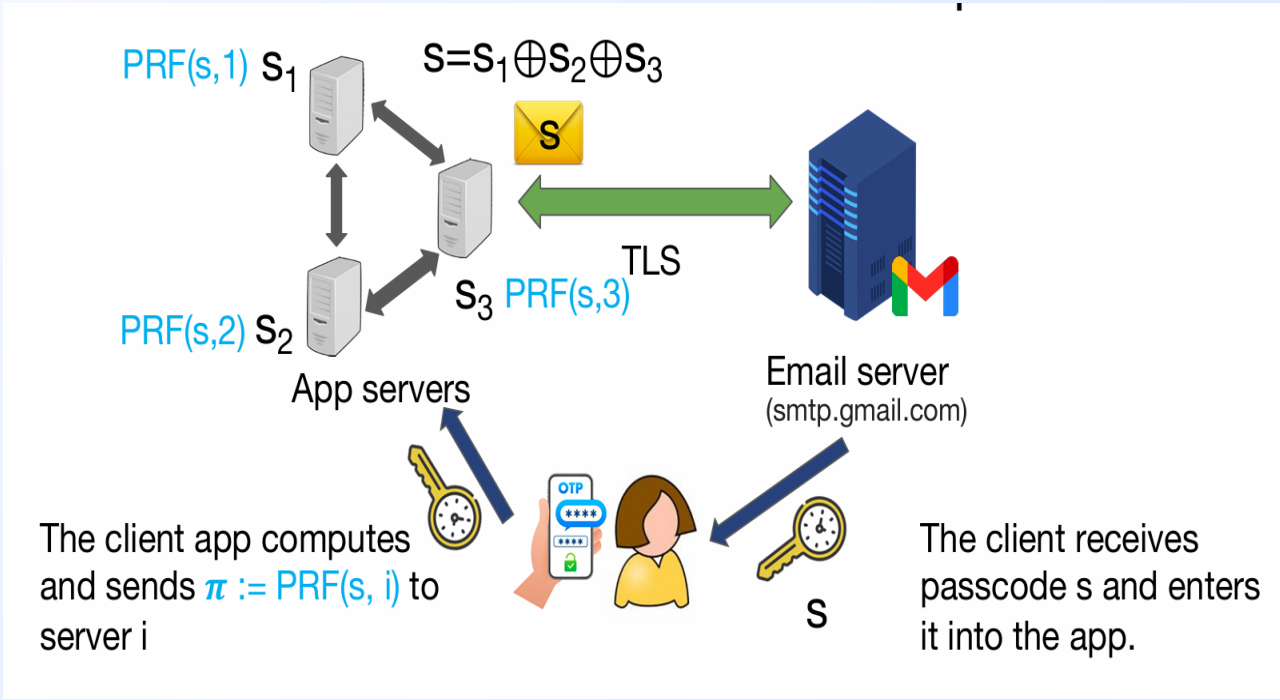
邮件认证

电子邮件认证

认证流程

N个服务器联合生成一次性验证码，通过TLS加密通道发送至客户端电子邮件地址。

客户端收到邮件后，输入验证码，客户端应用计算响应并发送至服务器，服务器验证响应。



邮件认证协议

电子邮件认证

安全性与隐私性

电子邮件作为秘密共享存储在服务器上，并且在身份验证期间，该地址在TLS的数据交换阶段在SMPC内加密和传输。没有服务器看到明文的电子邮件地址，仅在所有服务器都被攻破时才可能泄露电子邮件地址。

性能与优化

MPCAuth的电子邮件认证协议在N=5时，仅需1.81秒完成TLS握手和邮件发送，满足实际应用需求。

短信认证

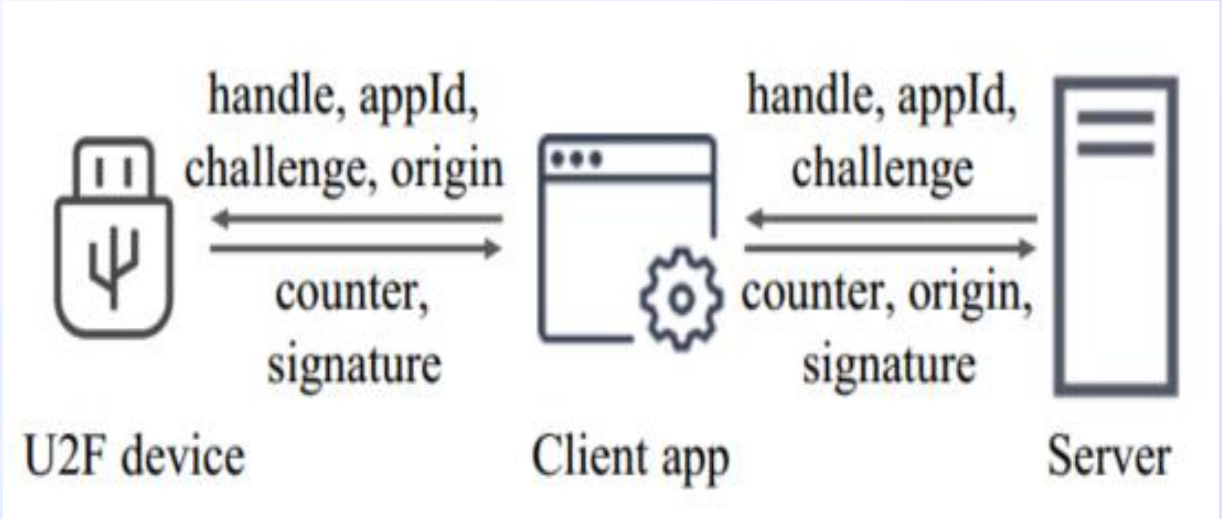
短信认证协议

短信认证协议与邮箱认证类似，通过联合生成短信验证码并发送给用户，用户输入验证码后完成认证。同样，用户的手机号码以秘密共享的形式存储，并在认证过程中通过TLS加密，防止隐私泄露。

U2F认证

U2F认证协议

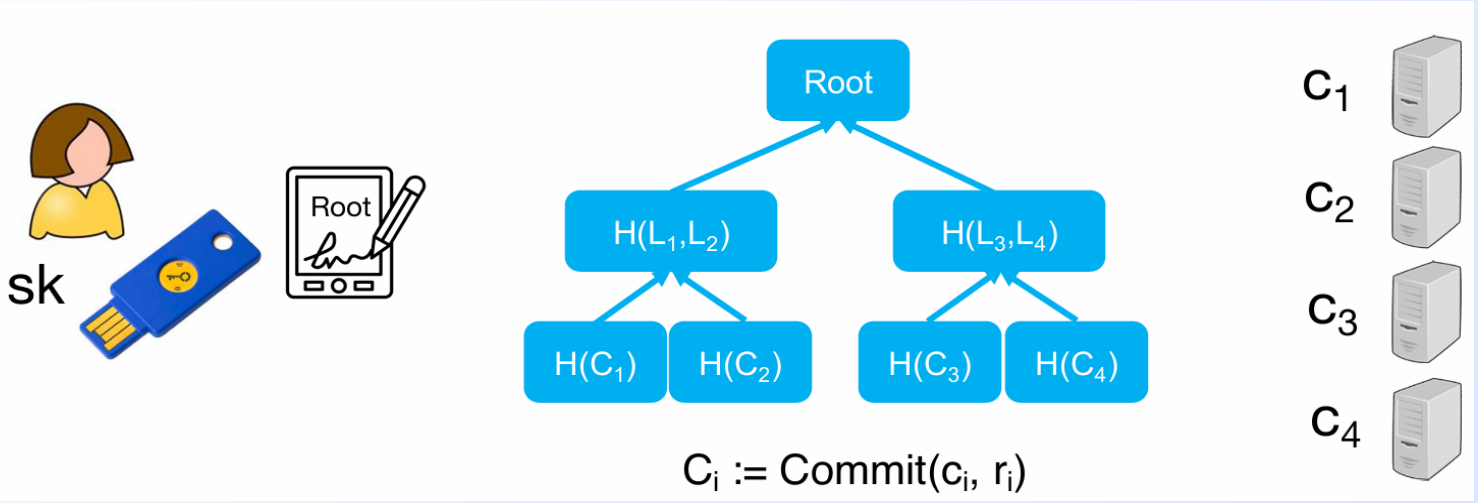
U2F设备生成特定于应用的密钥对，并将密钥句柄和公钥发送到服务器。在认证阶段，服务器生成随机质询，并将其与密钥句柄和应用标识符（appId）一起发送到U2F设备。然后，在用户确认时，U2F设备在请求上生成签名。 签名还包括一个单调计数器来发现克隆攻击。服务器接收签名并使用注册阶段存储的公钥对其进行验证。

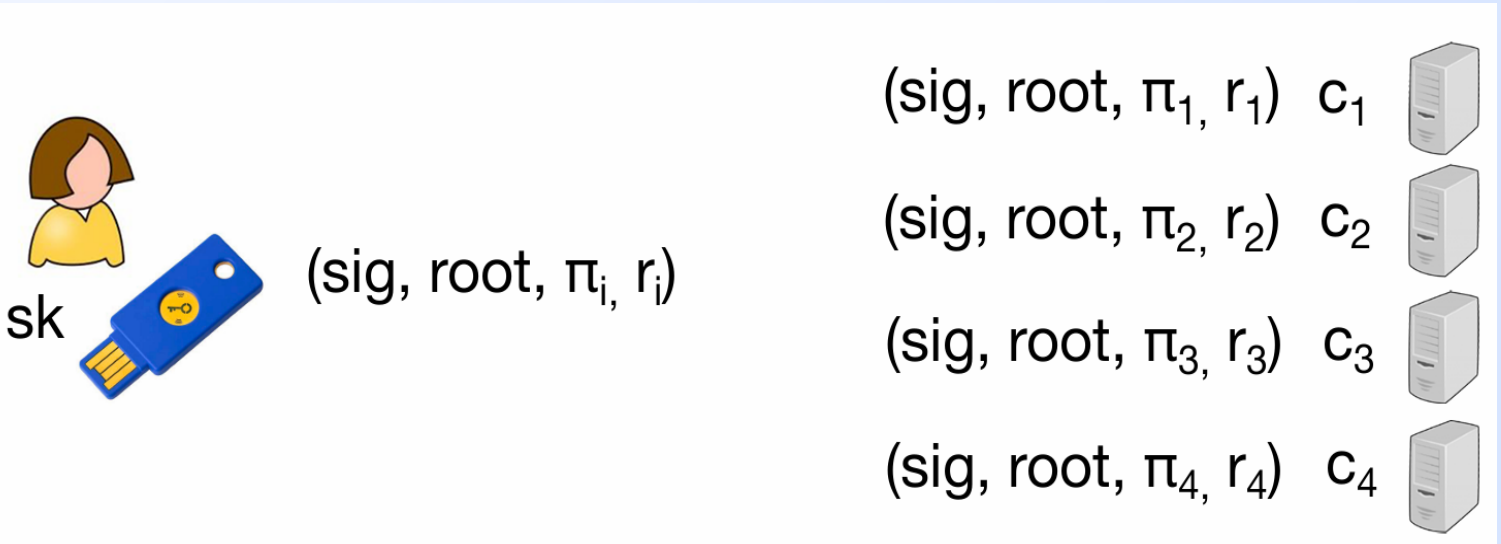


U2F认证

U2F认证协议

MPCAuth的U2F认证协议通过联合生成挑战并发送给用户的U2F设备，用户操作U2F设备生成签名后，系统验证签名的正确性，完成认证。该协议利用Merkle树和承诺方案，确保了认证的安全性和唯一性。

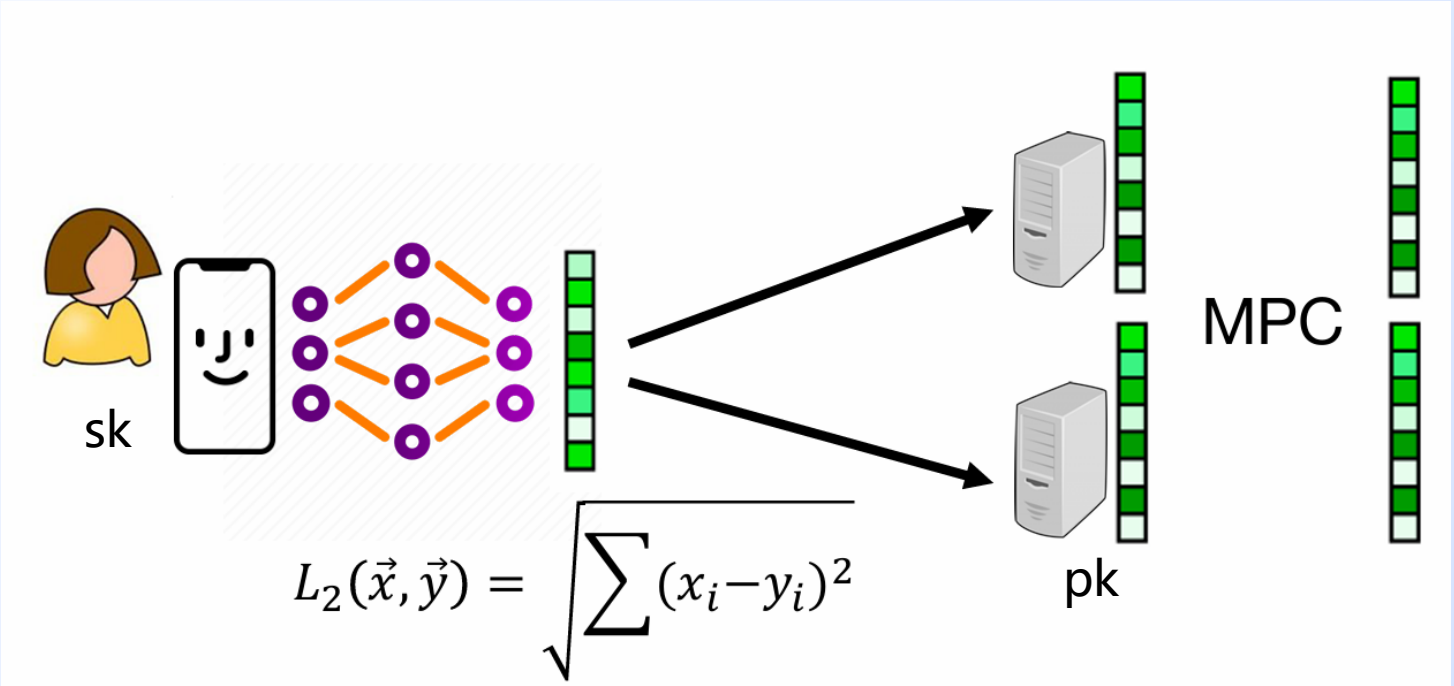




生物特征认证

生物特征认证协议

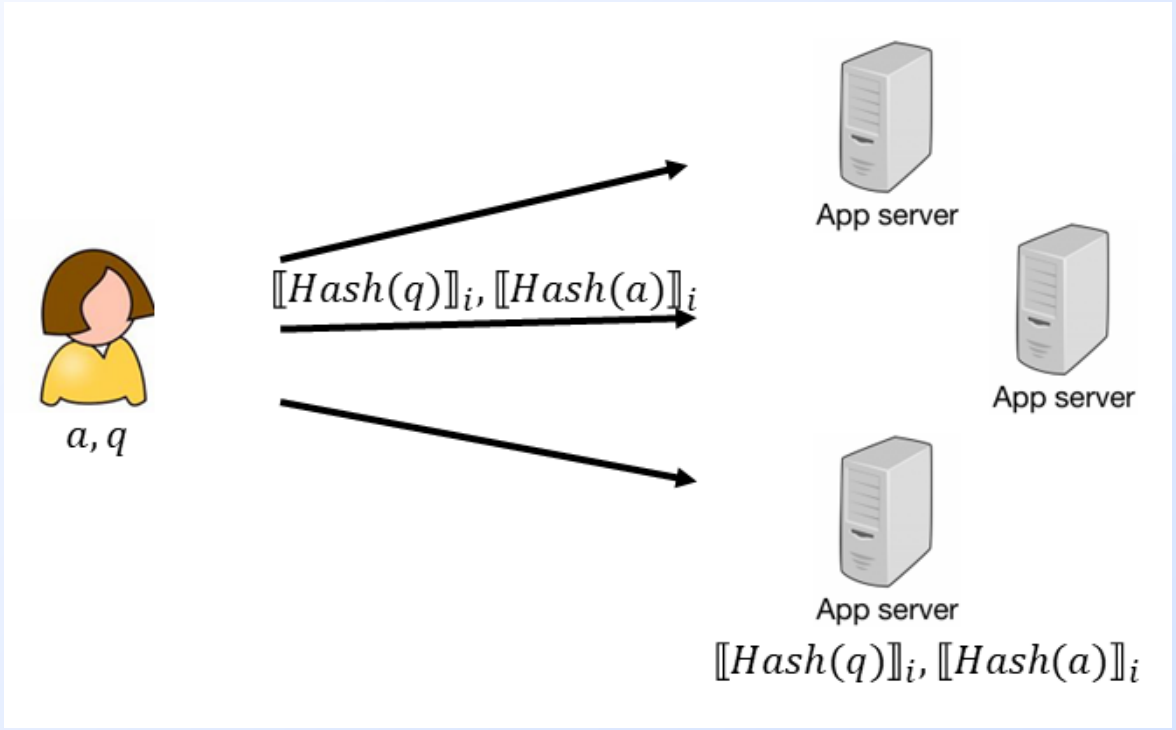
生物识别认证协议通过提取用户的生物特征（如面部识别、指纹等）生成特征向量，并在认证时与注册时的特征向量进行比较，计算其欧几里得距离，若距离小于阈值则认证成功。



安全问题认证

安全问题认证

用户将散列后的安全问题以及答案的秘密共享发送给N个服务器。认证过程中，用户再次向服务器发送安全问题和答案的哈希值秘密共享，N个服务器在SMPC内比较两次的哈希值是否相同，完成认证。



Part 04

系统实现与性能评估

TLS-in-SMPC性能评估

通过MP-SPDZ、emp-toolkit、wolfSSL实现TLS-in-SMPC协议

Component	Offline Phase Latency (s)				Online Phase Latency (s)			
	$N=2$	$N=3$	$N=4$	$N=5$	$N=2$	$N=3$	$N=4$	$N=5$
TLS connection establishment	7.43	8.16	11.11	14.83	0.67	0.92	1.08	1.38
◇ Key share generation	0.30	0.30	0.30	0.30	—	—	—	—
◇ Key exchange result computation	0.02	0.06	0.09	0.15	0.25	0.35	0.37	0.47
◇ Key derivation	6.55	7.05	9.73	13.1	0.37	0.51	0.64	0.83
◇ GCM power series ($L=5$)	0.49	0.65	0.87	1.15	0.03	0.04	0.05	0.06
◇ AES key schedule	0.07	0.10	0.12	0.13	0.02	0.02	0.02	0.02
Sending an email of 34 bytes in TLS	2.52	2.90	3.37	3.69	0.38	0.39	0.41	0.43
Sending a SMTP heartbeat in TLS	0.43	0.49	0.57	0.63	0.06	0.07	0.07	0.07

发送带有密码的电子邮件的TLS-in-SMPC延迟如上表所示，大部分计算都在离线阶段，而在线阶段的延迟很小

	Offline Phase Latency (s)	Online Phase Latency (s)
Email	10.96 (2.90)	1.29 (0.39)
SMS	12.26 (4.10)	1.48 (0.56)
U2F	—	0.03
Security Questions	0.03	0.04
Biometrics	8.89	0.38

MPCAuth 的latency

Part 05

结论与展望

MPCAuth的贡献与意义

01

02

解决分布式信任系统认证难题

MPCAuth解决了分布式信任系统中的认证难题，为分布式信任系统的广泛应用提供了有力支持。它不仅实现了单次认证的多服务器认证功能，还通过隐私保护机制隐藏了用户的认证信息，提高了系统的安全性。同时，系统支持多种常见的认证因素，具有良好的通用性和灵活性。

推动分布式信任系统发展

MPCAuth的出现为分布式信任系统的发展提供了新的思路和方法，推动了相关技术的创新和应用。它在数字货币托管、协作机器学习等领域的应用，展示了分布式信任系统的巨大潜力和价值。

未来研究方向

提高系统性能与可扩展性

未来的研究可以探索更高效的SMPC协议和优化技术，以进一步降低系统的计算和通信开销，提高系统的响应速度和处理能力。同时，还可以研究如何更好地支持大规模分布式信任系统的认证需求，提高系统的可扩展性。

加强隐私保护与安全机制

在隐私保护和安全机制方面，MPCAuth虽然已经采取了一系列措施，但仍有一些问题需要进一步解决。例如，如何处理拒绝服务攻击，构建一个客户端应用程序，自动为客户端执行身份验证但不影响客户端的隐私

论文分享

请大家批评指正