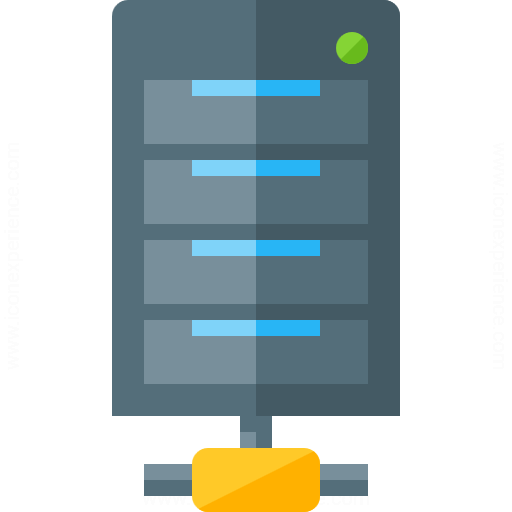
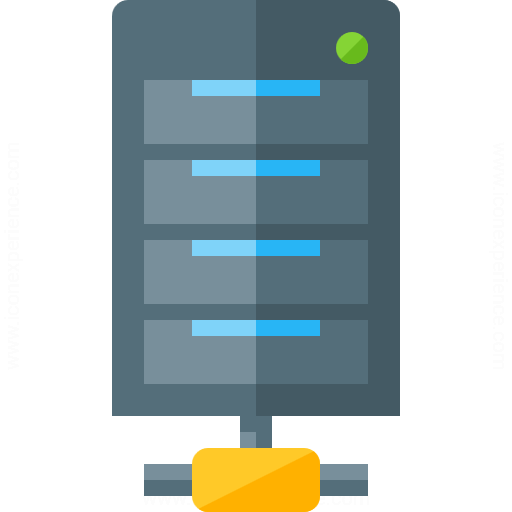
https://www.iconexperience.com/_img/g_collection_png/standard/256x256/key.pnghttps://www.iconexperience.com/_img/g_collection_png/standard/256x256/key2.png2BPR

Blind Password Registration for Two-Server Password

Authenticated Key Exchange and Secret Sharing Protocols

*Nach dem gleichnamigen Paper von Franziskus Kiefer und Mark Manulis*

1. **Hintergrund**

**2PAKE** = Two-Server Password Authenticated Key Exchange

**2PASS** = Two-Server Password Authenticated Secret Sharing

Auf mehreren Servern (meist 2) wird jeweils ein Passwortteil (Share genannt) gespeichert. Beim Userlogin arbeiten die Server ähnlich wie bei Diffie-Hellman zusammen, um den User anzumelden.

**+**

Man kann beiden Servern zu 100% vertrauen

**+**

Sicher gegen Brutforce

**+**

Sicher gegen Man-in-the-Middle

1. **Motivation**

Die Kontrolle der Passwortrichtlinie ist bisher unmöglich

Kein Server darf genügend Informationen erlangen, um das Passwort zu rekonstruieren

**+**

Wir erhalten als Ergebnis ein festdefiniertes Protokoll, an das man sich halten kann

1. **Begriffe**

|  |  |  |
| --- | --- | --- |
| **COMMITMENTS** | **ZERO KNOWLEDGE PROOF** | **PASSWÖRTER** |
| Binding = Man legt sich auf eine Wahl bindend fest (Münzwurf 🡪 Kopf / Zahl) | Ziel: Ich beweise einem Verifizierer V mit einer hohen Wahrscheinlichkeit, dass ich | Passwortrichtline f = (ulld,8)  Passwort Sharing π = s1 + s2  Passwort Wörterbuch |
| Hiding = Meine Wahl bleibt solange geheim, bis ich erlaube sie aufzudecken | als Beweiser P ein Geheimnis Kenne, ohne diese Geheimnis konkret zu enthüllen | enthält alle gültigen Pwds.  Passwortumwandlung String wird in Integer umgewandelt |

1. **Protokoll**
2. **Sicherhheitsanalyse**
3. **Fazit**