Prinzipiell:

* ~~Gliederung durchnummerieren und "Gliedern" (1-3 sind Grundlagen, 4-6 der Hauptteil) und Bezug auf den Folien zu Kapitel~~
* Protokolle stehen im Vordergrund und beschreiben zeitlichen Ablauf. Dieser zeitliche Ablauf sollte klar herausgearbeitet werden durch nummern und durch die graphische Veranschaulichung
* Erklärung, dass der Hauptteil, die Leistung der Autoren war/ist
* Quellen: Bitte nur bei der Abgabe mit anhängen / nicht im Vortrag, danke.
* Inhalte möglichst einfach und verständlich rüber zu bringen (Beispiel: "der das Verfahren beobachtet gewinnt keine Informationen" heißt anschaulich: Jemand, der die chiffrierte Kommunikation mitlesen kann, hat mathematisch dadurch keinen Vorteil bei der Berechnung des "Geheimnisses"

Hintergrund:

* 2PAKE und 2PASS bei noch mehr ausarbeiten bei verfügbarer Zeit

Motivation:

* Einhaltung der Serverrichtlinien als Problem hervorheben, da kein Server das Passwort kennt
* Vorteil der Sicherheit von 2 PAKE und 2PASS und 2BPRauch bei korrumpiertem Server hervorheben
* Die beiden Autoren haben als Eigenleistung / Forschungsergebnis das Protokoll 2BPR geliefert

Begriffe:

* Bei Commitments und ZeroKnowledge vorher erklären was man damit erreichen will
* Bei Trapdoor Commitment auch die Trapdoor erklären, also die Information, die die Trapdoor auslöst

Protokoll:

* "Offline Wörterbuch Attacken sind dadurch zwecklos solange ein Server ehrlich bleibt" besser erklären: wiederspricht dies nicht dem Ziel, dass selbst ein durch Angreifer korrumpierter Server den zweiten nicht gefährdet? (ggf. erläutern/seien Sie auf diese Rückfrage gefasst)
* Wer startet mit wem die Kommunikation
* Es sind drei Parteien vorhanden
* Schaubild planen
* Was wird hin und her gesendet und über welchen Kanal?
* Wie stellen die Server während der Share Verifikation sicher, dass der Client auch korrekt verifiziert oder muss man das nicht in Frage stellen 🡺 Commitments

Fazit:

* was man lösen wollte und wodurch man dies wie gut geschafft hat
* Eigene Stellungnahme, für wie relevant halten Sie das "Problem" und für wie gut (Sicherheit) und praktikabel halten Sie das Ergebnis