Research Methodology: Assignment 1

Karan Goel - 7836685

1. Brain Computer Interfaces (BCIs)

   (a) The main research question addressed by the authors is: "What are people's expectations and awareness regarding neuroprivacy as consumer grade neurotechnology becomes more popular?".

   (b) The contribution indicated by the authors is the first user study (n = 287) to understand people's expectations of neuroprivacy and awareness of neurotechnology implications.

   (c) The main results suggest that while there is interest in neurotechnology among users, privacy concerns are critical for its acceptability. The study underscores the significance of consent and the necessity for transparent practices regarding the sharing of neurodata.

   (d) The authors most probably used a quantitative research methodology, specifically a survey or questionnaire-based approach. This methodology allows them to gather data from a relatively large sample size (n = 287) and analyze the responses statistically to draw conclusions about users' attitudes towards neuroprivacy and neurotechnology.

   (e) The design of the research likely involved the following components:

   - Data Collection: Participants (n = 287) might have been recruited from diverse backgrounds to ensure a representative sample. The survey or questionnaire could include questions about participants' familiarity with neurotechnology, their concerns about privacy, their willingness to engage with neurotechnology in various domains, and their expectations regarding privacy of neurodata.
   - Statistical Analysis and Hypotheses: The authors likely hypothesized that individuals would show varying degrees of interest in neurotechnology based on demographic factors and familiarity with the technology. They may have used regression analysis to examine these relationships and conducted inferential statistics to compare attitudes across dif-

ferent groups. These analyses would provide insights into the factors influencing neuroprivacy concerns.

- Justification: Based on the analysis, the authors would draw conclusions regarding users' neuroprivacy expectations and awareness of neurotechnology implications like the significance of consent and the necessity for transparent practices in data sharing.
- Internal and External Validity:
  - Internal validity refers to the extent to which the study accurately measures what it intends to measure. In this case, internal validity would depend on factors such as the clarity and relevance of survey questions, the representation and background of the sample, and the soundness of the statistical analysis.
  - External validity refers to the generalization of findings beyond the studied sample. To enhance it, the authors could have reviewed related literature and trends on people's views on privacy. Additionally, conducting tests on diverse samples would reflect the broader population's attitudes.

2. ECDSA

   (a) The main research question addressed by the authors appears to be: "How can efficient threshold signature protocols be constructed for ECDSA scheme in scenarios where only two parties are involved?"

   (b) The contribution indicated by the authors is the development of a protocol for secure distributed ECDSA signing between two parties (with no honest majority) that is significantly faster than previous approaches. This protocol achieves substantial performance improvements while maintaining security guarantees.

   (c) The main results highlight the significant speedup achieved by the proposed protocol compared to previous methods. Specifically, the protocol achieves a single signing operation for curve P-256 in approximately 37 milliseconds between two standard machine types in Azure, utilizing only a single core. Additionally, the security of the protocol is proven under standard assumptions using a game-based definition and also demonstrated under a plausible yet non-standard assumption regarding Paillier.

   (d) The authors likely used a combination of scientific and experimental research methodologies. Scientific and Experimental methods would have been employed to design and analyze the new protocol, ensuring its security properties and efficiency. Quantitative

methods might also have been used to evaluate the protocol's performance on real-world computing platforms.

(e) The design of the research likely involved the following components:

- Data Collection: The data collection process would involve gathering information on existing approaches to distributed ECDSA signing protocols, identifying their limitations and areas for improvement.
- Hypotheses: The authors likely hypothesized that it is possible to design a more efficient threshold signature protocol for ECDSA in scenarios involving only two parties, without compromising security.
- Statistical Analysis: Statistical data analysis may have been used to compare the performance of the proposed protocol with existing approaches, measuring factors such as computational overhead, communication overhead, and overall signing latency.
- Justification: The conclusion drawn in the abstract is supported by empirical evidence demonstrating the significant speedup achieved by the proposed protocol compared to previous methods. Additionally, the security guarantees provided by the protocol are justified through theoretical analysis and cryptographic proofs.
- Internal and External Validity:
  - In this case internal validity would have been ensured through rigorous theoretical analysis and experimental evaluation, confirming that the proposed protocol achieves the stated performance improvements without sacrificing security.
  - External validity would have been enhanced by providing detailed descriptions of the protocol, experimental setup and the theory allowing other researchers to replicate the results and validate the findings in different environments.