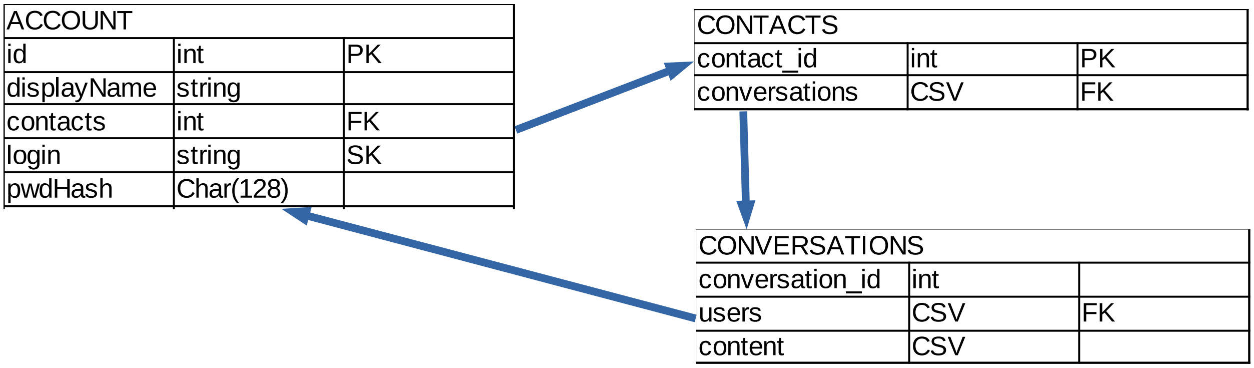
YOLOcrypto

This simple messaging app will be based on traditional client/server design. Prototype should be working on any common device, such as Android phone or desktop web browser. The repository is hosted on Github. It should be maintained open-source and under sufficiently liberated license, such as CC BY 4.0.

Server

SQL **Database** will be run in the back-end, keeping track of account info and corresponding messaging content. In the database design we make a huge use of CSV files, however, in some RDBMS feature called Foreign Key Arrays is supported, which might be better than CSV. Here is the database diagram:



ACCOUNT		
id	int	PK
displayName	string	
contacts	int	FK
login	string	SK
pwdHash	Char(128)	

CONTACTS		
contact_id	int	PK
conversations	CSV	FK

CONVERSATIONS		
conversation_id	int	
users	CSV	FK
content	CSV	

The separation of Contacts from Account might be a scalability issue in the future, yet it might also provide us with some functionality. The database is further described in server/database/dbStructure.md

Client

Users will be able to sign in with their email, which might be changed in the future or might even be only a burner email. The client will store some recent messaging content, as well as whole contacts table. Requests will be made by HTTP requests and will listen to notification messages, created by the server. The API is sketched in client/api.hpp header file.

Protocol

This is not yet fully resolved and in open for further discussion. While being innovative and interesting, using post-quantum crypto (PQ) would require to use new and obscure crypto library, such as LIBOQS, which lacks documentation and is not yet sufficiency reviewed. However, implementing this library might be of greater public utility than making thousandth implementation of commonly used libraries.

Other option is to use mbed, which is well documented, easy to use and properly established, but potentially boring, or to implement the famous Signal protocol using libsignal libraries, which offers quite a few cutting-edge cryptographic features. We want to discuss this in the seminar.