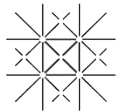


Universität
Basel

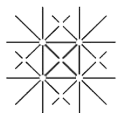
Monad Chain Chat

By Matthias Müller,
Betreuer: Christian Tschudin



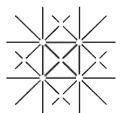
Inhaltsverzeichnis

- Idee & Konzept
- Elliptic Curve Cryptography
- Vom Chatlog zum Chat
- Probleme
- Demo & Fragen



Idee und Konzept

- Secure Scuttlebut: <https://scuttlebutt.nz/> oder <https://github.com/ssbc>
- Nicht online sondern anhand von Files “offline” bzw manuell übertragen
- Append Only Log
- Asymetrische Verschlüsselung -> ECC
- Abgeändertes Blockchain Konzept



Universität
Basel

Elliptic Curve Cryptography

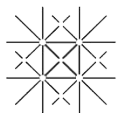
How it looks like:

Key:

```
PublicKey {public_curve = CurveFP (CurvePrime
  115792089237316195423570985008687907853269984665640564039457584007908834671663
  (CurveCommon {ecc_a = 0, ecc_b = 7, ecc_g = Point
    55066263022277343669578718895168534326250603453777594175500187360389116729240
    32670510020758816978083085130507043184471273380659243275938904335757337482424, ecc_n
    = 115792089237316195423570985008687907852837564279074904382605163141518161494337,
    ecc_h = 1})), public_q = Point
  75290335661880385322955696361059093774326996105887261955773094070789469598964
  35110338472591976258570797103594278113001174108035258980133808808597760348798}
```

Signature:

```
Signature {sign_r = 50852147293250169998661227733559703604901362459252362661916245754076566494260, sign_s =
  94909283324097635876178479383614827273991505566651051890998107085184272382821};Max;1663600632044792000;Hallo Max, wie geht
  es?
```



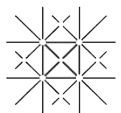
Universität
Basel

Vom Eventlog zum Chat

Wie komme ich von dem:


```
chatevent.txt Öffnen mit CodeRunner
```

```
New Chat EventPublicKey {public_curve = CurveFP (CurvePrime
115792089237316195423570985008687907853269984665640564039457584007908834671663 (CurveCommon {ecc_a = 0, ecc_b = 7,
ecc_g = Point 55066263022277343669578718895168534326250603453777594175500187360389116729240
32670510020758816978083085130507043184471273380659243275938904335757337482424, ecc_n =
115792089237316195423570985008687907852837564279074904382605163141518161494337, ecc_h = 1})), public_q = Point
75290335661880385322955696361059093774326996105887261955773094070789469598964
35110338472591976258570797103594278113001174108035258980133808808597760348798}
Signature {sign_r = 50852147293250169998661227733559703604901362459252362661916245754076566494260, sign_s =
94909283324097635876178479383614827273991505566651051890998107085184272382821};Max;1663600632044792000;Hallo Max, wie
geht es?
Signature {sign_r = 5073082720806148493495925842279573583167124471195076778605772206855762074983, sign_s =
115768323849134354364244057936158721930876930684531158057439444177551046361514};Max;1663672587402132000;Hallo Max lange
nichts mehr gehört
Signature {sign_r = 19593689136744161534980211718635794193361402546839302132844615718001325034221, sign_s =
96583762257287647690995372325584013459424650753308274642901442603479269511305};Max;1663672610226109000;dies ist ein
wiett... weiterer test
Signature {sign_r = 82622244279259617250816326791277446842111017410728445478399103200569977964623, sign_s =
95354478739665341409559050697904861532181562129731401582269553658055725615259};Fritz;1663672628057557000;dies ist ein
andere r Test
Signature {sign_r = 89368269026670378003573004880364724119060177871511426483234052296186719875131, sign_s =
50818072049115323965751182313677265287187823978868565441378351671443685830958};Matthias;1663744288791512000;Hallo
Matthias, mir gehts gut
```



Vom Eventlog zum Chat

zu dem:

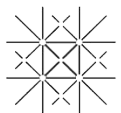
Max.txt			Öffnen mit CodeRunner	
"1663600632044792000"	to: "Max"	msg: "Hallo Max, wie geht es?"		
"1663672587402132000"	to: "Max"	msg: "Hallo Max lange nichts mehr geh\195\182rt"		
"1663672610226109000"	to: "Max"	msg: "dies ist ein wiet\DEL\DELt\DEL... weiterer test"		
"1663744288791512000"	to: "Matthias"	msg: "Hallo Matthias, mir gehts gut"		

EventBlock: [Signatur, Empfänger, Zeit, Nachricht]

Chat format: [Zeit, Empfänger, Nachricht]

Vorteile:

- übersichtlicher
- Daten von zwei Eventlogs vereint zu einem Chat
- Chronologisch geordnet

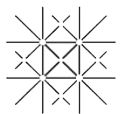


Vom Eventlog zum Chat

Was Passiert, wenn das Programm abstürzt, während dem Transfer von Eventlog zu Chat?

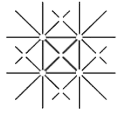
Kontrollmechanismen:

- zuerst werden beide Eventlogs ausgelesen (von mir und von Max)
- dann werden diese überprüft ob die Signaturen stimmen
- beim Kopieren wird ein Headerfile (z.B. "Chats/Max-header.txt") generiert
- dann wird das File mit einem Befehl (atomische Instruktion) zu "Chats/Max.txt" kopiert
- dann werden "Chats/Max-header.txt" und "Chats/Max.txt" miteinander abgeglichen
- zum schluss wenn alles gut ist, wird "Chats/Max-header.txt" gelöscht



Probleme

- Zeit schlecht eingeteilt
- Libraries die man nicht direkt importieren kann
- Monaden und Typstrukturen die nicht stimmen



Universität
Basel

Demo & Fragen