(Here?)

converts an integer to an ID

There is a first expression that

Since now less in TA

Community of less (bank)
of

The (doc+ts) is signed by a set

10 words

got signature on this doc from

2 fraud 102 IPs of now

Alex张某 Kiss Chen (10-31-2019)
Check sign

Get loss info

Find peak draw from paper

Acce pressure < 5 cc3 T5, loss info

Verif
4. Not too many people due

3. Cinema Access on weekends and bank holidays

2. Tea available to staff

1. Large community of users.
Secure multiparty computations
- Mental Poker
- Computing avg salary
- Dining Cryptographers

\[ \text{sub } R \quad \text{Alice } \text{sub } R+S_a \quad +S_b \quad \rightarrow \quad \rightarrow \rightarrow \]
Dining Cryptographers

Who paid?

Each person announces 2φ → 2p

If you paid, lie

Same or different?

Even # of diffs = someone else paid
Anonymous messaging (Onion Router)
(Mixmaster or Mixes)

Alice sends msg to Bob

\[ \rightarrow \quad 1. \text{Bob does not know} \]
\[ \quad \text{or} \]
\[ \quad 2. \text{No one other than Alice and Bob know.} \]
each part reverses "nothing goes"

and (n-1) pads

and

reverses (s)

all pads reverse to

and pad in

would also spread up

(s) have a spread (s)

Secret Solution
\[ p \cap R \cap R' \cap R'' \subseteq S \]

\[ \frac{r - r'}{r - r''} \]

Diagram: A square labeled with a down arrow labeled \( \Rightarrow \) and a right arrow labeled \( \rightarrow R \).
(r-1) \cdot (n-r) = (n \cdot r - r^2 - \frac{n(n-1)}{2})

Any k shares increase by checking n shares with the threshold
Suppose $k = 2$ and $n = (\text{donut case})$.
Compute \( y \) for \( x = 1 \), \( x = 2 \), \( x = 3 \):

\[
\begin{align*}
\text{when } & \begin{cases} 
(x = 3) \quad y = 3 \\
(x = 2) \quad y = 2 \\
(x = 1) \quad y = 1 
\end{cases} \\
\text{and eqn:} & \quad \sum_{i=1}^{L-1} a_{i-1} x_{i-1} + a_{1} x_{1} + a_{2} x_{2} + a_{3} 
\end{align*}
\]
$s = y^2$

$\therefore s = y^3$

Known

$A_1 r + A_2 r + A_3 r + s = y^1$

Unknown
\[ 9a_1 + 3a_2 + s = 0 \]

\[ n = 2 \]
\[ 4a_1 + 2a_2 + s = 36 \]
\[ n = 1 \]
\[ a_1 + a_2 + s = 18 \]

\[ n = 3 \]
\[ 2a_1 + 6 + a_0 = 36 \]
\[ n = 2 \]
\[ 5 + 3 + a_0 = 18 \]

\[ \int_0^{\infty} x^2 + 3x + 10 \, dx = 10 \]
et cetera

so far

very far

out there

Dreamers and believers

dare to sign for Alice (but it's a tough road to get here)

Stay strong
\( S_1 \times S_2 = \text{produce for } \text{dec}_1 \times \text{dec}_2 \)

\[ S_2 \text{ dec}_2 \leftrightarrow S_1 \text{ dec}_1 \text{ dec}_2 \]

If there exists dec_1 \text{ dec}_2 \leftrightarrow S_1

existence
1. Have a group key pool.
   Issue cert to members.
   Group members have private keys.

2. Make sure each member is identified.

3. Do not disclose...