Implementing Fiber-based Steganography for Pairings

Tolga Acar, Karen Easterbrook and Brian LaMacchia
Motivation

This is Mira Belenkiy

Mira’s new pairing:

\[ e(g^a, h^b) = e(g, h)^{ab} \]

For the past year, Mira’s been working on a new kind of pairing
Motivation

This is Mira Belenkiy

Mira’s new pairing:

\[ e(g^a, h^b) = e(g, h)^{ab} \]

For the past year, Mira’s been working on a new kind of pairing

No, not that kind of pairing...
Mira’s New Pairing

Nomi

Ellie
Problem Statement

• We want a protocol to send private information to the new pairing
  – Without Mommy Eve learning the message

• Encryption? Not an option in this model...
  – Yes, they’re Mira’s kids, but they still can’t do AES in their heads before they can walk
Problem Statement

• We want a protocol to send private information to the new pairing
  – Without Mommy Eve learning the message

• Encryption? Not an option in this model...
  – Yes, they’re Mira’s kids, but they still can’t do AES in their heads before they can walk

• Solution?
  – Steganography! Specifically, Fiber-based
  – Must be washable and drool-proof
Fiber-based Steganography

• Start with some fibers (cotton)
• Weave them together into dense sheets (cloth)
• Choose an alphabet to encode your message
  – Ours have 4 symbols: W, A, I, L
• Define width $d$, different lengths $l_W, l_A, l_I, l_L$
• Cut lots of strips of cloth, piled by length
We want randomized buckets
So, add appropriate randomization
Symbol encoding

• For each symbol, draw (w/o replacement) from the corresponding bucket
  – But if you get successive identical patterns, draw again
• Concatenate (e.g. sew) into a “stream”
  – One ginormous strip of cloth (~230 feet long)
• Segment the stream into 86in long “blocks” (strips)
• Tile the strips into a rectangle
  – This is the ciphertext
The Ciphertext
Decoding the Concealed Message
Decoding the Concealed Message
Decoding the Concealed Message
Decoding the Concealed Message
Decoding the Concealed Message

E L E C
Electronic cash is an important tool for preserving on-line privacy. It allows a user to make purchases without revealing his identity to the merchant and prevents banks from monitoring the transactions of all their users. In this thesis, we use secret sharing techniques to extend electronic cash.
Electronic cash is an important tool for preserving on-line privacy. It allows a user to make purchases without revealing his identity to the merchant and prevents banks from monitoring the transactions of all their users. In this thesis, we use secret sharing techniques to extend electronic cash.

We examine the problem of fair exchange that lets a user atomically exchange an electronic coin

Successful Message Transmission
Credits

Quilt Implementation: Karen Easterbrook
Consulting Cryptographer #1: Tolga Acar
Consulting Cryptographer #2: Brian LaMacchia
Entropy Injector #1: Skipper “Skip” Easterbrook
Entropy Injector #2: Fender “Fen” Easterbrook-Sutton