# Format-Preserving Encryption

Terence Spies

Voltage Security

# A Tiny Bit About My Perspective

- Voltage builds and sells key management and encryption systems to financial and health care enterprises.
  - Been doing this since 2003
  - Typical customer: large regulated enterprise
    - Motivations: PCI, HIPAA, risk reduction
- From this experience, I'll address:
  - How commercial customers look at encryption
  - A widely deployed solution that does primitive operations on ciphertext

# Why Don’t We Encrypt Data?

- Encryption is often a retrofit
  - Systems implemented without privacy
  - System requirements changing (PCI)
  - System assumptions changing (dial-up -> IP)
- Legacy lives longer than you think
  - Mainframe lives on
  - Payment edges expensive to upgrade (fuel, etc.)
- The Voodoo Factor
  - “I’d rather not encrypt than use a non FIPS solution”
  - Tokenization vs. Encryption

# Making Ciphertext Valuable

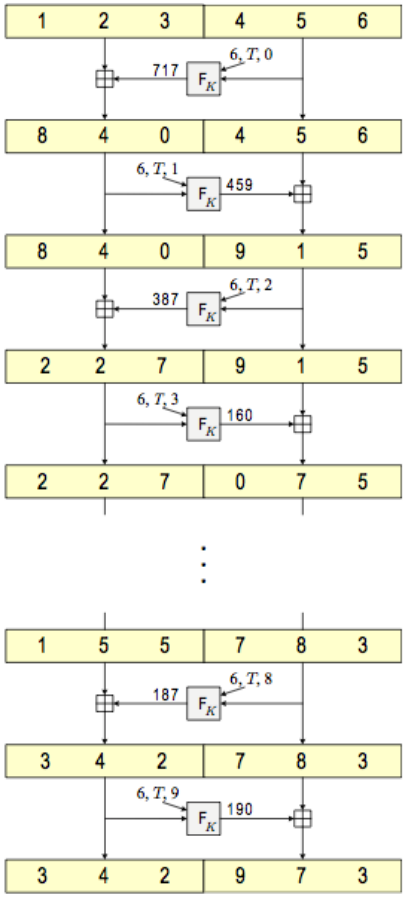
- Access control via crypto can be tricky
  - Key management overhead
  - Authenticating endpoints is hard
    - Semi-solved problem for humans
    - Authenticating a process, less so
- Partial solution
  - Give ciphertext some properties
  - Allow semi-trusted processes limited processing
    - Partial plaintext access
    - Searching
    - Sorting?

# Format Preserving Encryption

- The FPE setting:
  - Define a finite set of plaintexts
  - Encrypt onto that set
    - Encrypt a 16 digit CCN onto a random 16 digit value
    - Encrypt a 9 digit SSN onto a random 9 digit value
- The ideal FPE cipher functions a psuedorandom permuation over the set of plaintexts
  - In some situations, safe to use deterministically
- FPE ciphers are typically tweakable

# FFX FPE Framework

- FFX : Parameterized Finite Feistel framework
- Core idea
  - Express a string format as a length and radix
  - Build a Feistel network operating in that radix
  - Internal PRF based on AES



# FFX Security

- Security reductions
  - Given a random internal PRF, for some number of adaptive queries, FFX is IT indistinguishable from a PRP
  - Asymptotic results from Patarin at 6+ rounds, Rogaway shows unbalanced results
  - Bellare, Ristenpart, Rogaway, Stegers show results for message recovery, other models
- Best known attack
  - Essentially, enumeration of all possible internal PRFs (Patarin)

# Why do we care?

- Oblivious operations over ciphertexts
  - Deterministic encryption allows search
  - Tweaking allows selective revelation of plaintext
- Credit card example
  - Modern cards are 15-19 digits
  - First 6 digits identify issuing bank
  - Last 4 digits used for receipt printing
  - Typical format keeps first 6/last 4 clear, use to tweak encryption of inner digits

# Commercial adoption

- Products
  - Payment networks (all major POS vendors)
  - Data masking products
- Standards
  - X9.124 – FPE for Financial Industry
  - NIST – parallel FPE specification
  - VISA Guidance document

# Promising tools / Wishlist

- Order preserving encryption
- RASP (multi-dimensional query over data)
- Ideal Feistel security bounds