# Multivariate Cryptography

*ICERM Graduate Workshop on Linear Algebra over Finite Fields & Applications*

Ryann Cartor

Clemson University

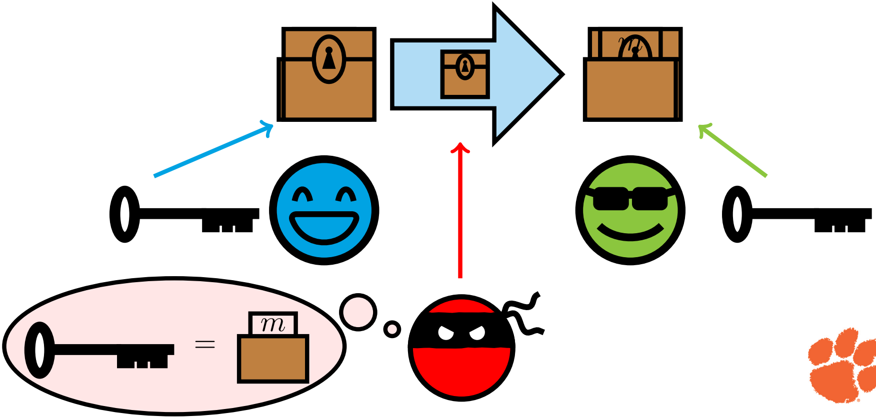
August 19, 2025

# What is Cryptography?

Goal: Secure communication over unsecure channels

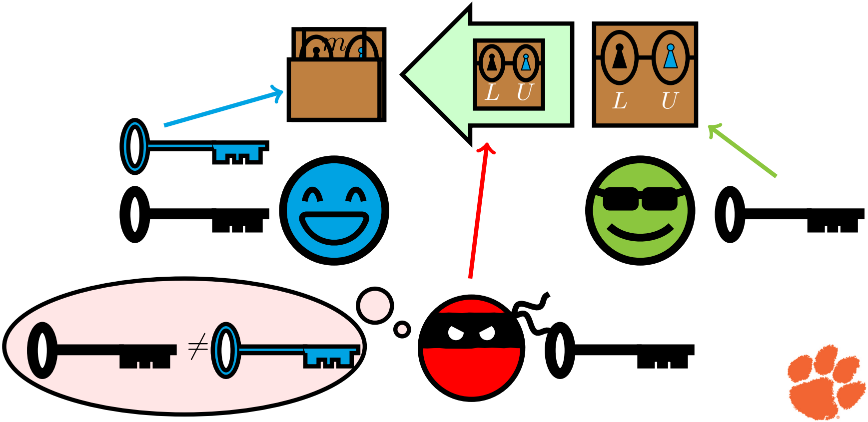
# Private Key Cryptography (aka Symmetric Cryptography)

- If you have enough information to encrypt, then you have enough information to decrypt.
- Alice and Bob need a shared secret



# Public Key Cryptography (aka Asymmetric Cryptography)

- Even if you have enough information to encrypt, you may not have enough information to decrypt.
- Alice and Bob do not need a shared secret

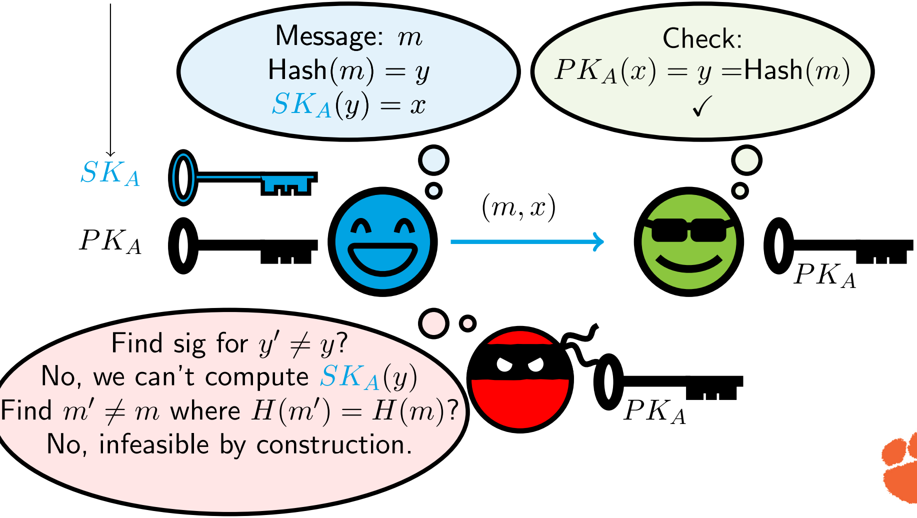


# Encryption Schemes vs. Signature Schemes

- Applications of public key cryptography
  - Encryption Schemes
    - Generating a shared secret
  - Signature Schemes
    - Authentication
    - Non-Repudiation

# Signature Schemes

$P(x) = P(S(y)) = y$

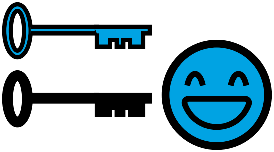


Now the question is... How do we choose $PK_A, SK_A$?

$$P(x) = P(S(y)) = y$$

$SK_A$

$PK_A$



We will use "hard problems" to generate PK and SK.

Difficult to *find* a solution to the problem, easy to *check* if something is or is not a solution.

# "Hard" Problem: Factoring into primes

What are the prime factors of...

$$15 = 3 \times 5$$
$$143 = 11 \times 13$$
$$12,709,189 = 3,559 \times 3,571$$

RSA: Rivest, Shamir, Adleman, 1977

# "Hard" Problem: Discrete Log

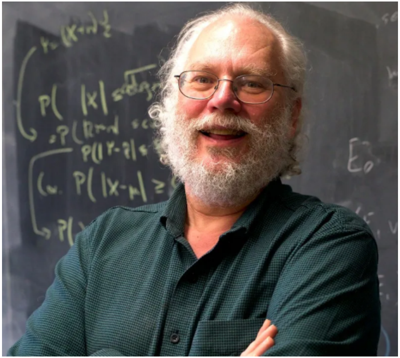
Find $x$ such that...

$$2^x \mod 59 = 8 \qquad x = 3$$
$$2^x \mod 59 = 5 \qquad x = 6$$
$$2^x \mod 59 = 44 \qquad x = 27$$

Diffie-Hellman Key Exchange, 1976

# Are we done?

"Give me a quantum computer and I can factor large primes and compute the discrete log in polynomial time!"
-Peter Shor, 1994



# Post-Quantum Cryptography

Cryptography that can be implemented on a classical computer but will (hopefully) be secure against attacks completed on either a classical or a quantum computer

*Focus on Public Key Cryptography*

Types of Post-Quantum Cryptography:

- **Multivariate**, Code-Based, Lattice-Based, Isogeny-Based, Hash-Based, MPCitH, ...

# Multivariate Cryptography

## Preliminaries

- Setting: finite field $\mathbb{F}_q$
- Multivariate equations: equations in many variables
  - Linear equations:
    - Example: 3 equations in 3 variables over $\mathbb{F}_5$

$$\begin{aligned} x_1 + 4x_2 + 2x_3 &= 2 \\ x_1 + 3x_2 &= 3 \\ x_1 + x_2 + 4x_3 &= 3 \end{aligned}$$

    - Ways to solve: Gaussian Elimination
  - Quadratic Equations:
    - Example: 3 equations in 3 variables over $\mathbb{F}_5$

$$\begin{aligned} x_1^2 + 4x_2x_1 + 2x_3x_2 &= 2 \\ x_1x_3 + 3x_2^2 + x_3 &= 3 \\ x_1x_2 + x_2 + 4x_3 &= 3 \end{aligned}$$

    - Ways to solve: Polynomial Solvers, Gröbner basis algorithms

# Multivariate Cryptography

## Hard Problem

**Problem (MQ: Multivariate Quadratic)**

Given a system of multivariate quadratic equations over a finite field, find a solution.

- General Public Key Structure:

$$P(x) = T(F(S(x)))$$

■ Linear, ■ Quadratic (Easy to invert),
■ Quadratic (hopefully, difficult to invert)

# The $C^*$ Cryptosystem

- Presented by Matsumoto and Imai at Eurocrypt '88
- Is an example of a **big field** scheme

# Big Field Schemes

- Let $\mathbb{F}_q$ denote the finite field with $q$ elements and consider the degree $n$ extension, $\mathbb{F}_{q^n}$.
- We choose an $\mathbb{F}_q$-vector space isomorphism $\phi : \mathbb{F}_q^n \to \mathbb{F}_{q^n}$ and a function $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$.

$$
\begin{tikzcd}
\mathbb{F}_{q^n} \arrow[r, dash, "f"] \arrow[d, dash, "\phi"'] & \mathbb{F}_{q^n} \arrow[d, dash, "\phi^{-1}"] \\
\mathbb{F}_q^n & \mathbb{F}_q^n
\end{tikzcd}
$$

# Big Field Schemes

## Example

- Let $q = 2, n = 3$. Then we can define:

$$\mathbb{F}_2 = \{0, 1\}$$

$$\mathbb{F}_{2^3} = \mathbb{F}_2[X]/\langle X^3 + X + 1\rangle = \{c_0 + c_1 X + c_2 X^2 \mid c_i \in \mathbb{F}_2\}$$

$$(c_0, c_1, c_2) \in \mathbb{F}_2^3 \xrightarrow{\phi} c_0 + c_1 X + c_2 X^2 \in \mathbb{F}_{2^3}$$

$$\begin{tikzcd} \mathbb{F}_{q^n} \arrow[r, dash, "f"] \arrow[d, dash, "\phi"'] & \mathbb{F}_{q^n} \arrow[d, dash, "\phi^{-1}"] \\ \mathbb{F}_q^n & \mathbb{F}_q^n \end{tikzcd}$$

# $C^*$ Encryption Scheme

- **Creating the secret key.** Choose:
  - $q, n, \phi$
  - $U, T \in \mathsf{GL}_n(\mathbb{F}_q)$
  - Exponent $\theta$ such that $\gcd(q^\theta + 1, q^n - 1) = 1$
- **Creating the public key.** Compute:

$$\color{violet}{P} = \color{magenta}{T} \circ \color{cyan}{\phi^{-1} \circ f \circ \phi} \circ \color{magenta}{U}.$$

■ Quadratic (hard to invert), ■ Linear, ■ Quadratic (we can invert)

$$\begin{tikzcd}
 & \mathbb{F}_{q^n} \arrow[r, "f = X^{q^\theta+1}"] & \mathbb{F}_{q^n} \arrow[d, "\phi^{-1}"] & \\
\mathbb{F}_q^n \arrow[r, "U"] & \mathbb{F}_q^n \arrow[u, "\phi"] & \mathbb{F}_q^n \arrow[r, "T"] & \mathbb{F}_q^n
\end{tikzcd}$$

# Notes About the $C^*$ Central Map

Q1: Why do we call $\phi \circ X^{q^\theta+1} \circ \phi^{-1}$ "$\mathbb{F}_q$-quadratic?"

- Fact: The Frobenius map $\varphi : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}, \varphi(\alpha) = \alpha^{q^i}$ is $\mathbb{F}_q$-linear. Meaning for $\alpha, \beta \in \mathbb{F}_q^n$, $\lambda \in \mathbb{F}_q$ :

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta) \text{ and } \varphi(\lambda\alpha) = \lambda\varphi(\alpha)$$

- Rewriting the central map:

$$X^{q^\theta+1} = \left(X^{q^\theta}\right)(X)$$

■ Quadratic, ■ Linear

# Notes About the $C^*$ Central Map

Q2: How do we compute $f^{-1}$?

- Fermat's Little Theorem for Finite Fields: Let $\mathbb{F}$ be a finite field with $m$ elements. Then for all $a \in \mathbb{F}^*$

$$a^m = a \text{ and } a^{m-1} = 1.$$

- Recall: We insisted $\gcd(q^\theta + 1, q^n - 1) = 1$ which means... there exists $\beta$ such that $(q^\theta + 1)(\beta) = 1 \mod q^n - 1$.
- Thus we compute:

$$\begin{aligned}\left(X^{q^\theta+1}\right)^\beta &= X^{(q^\theta+1)\beta}\\ &= X^{1+k(q^n-1)}\\ &= (X)\left(X^{k(q^n-1)}\right)\\ &= X\end{aligned}$$

# Cryptanalysis of $C^*$

$C^*$ was broken by Patarin in 1995 using linearization equations

1. Compute $v = u^{q^\theta + 1}$
   - Note, $u = \phi(x_1, \ldots, x_n)$ and $v = \phi(y_1, \ldots, y_n)$
2. Raise both sides to the $q^\theta - 1$ power
   - $v^{q^\theta - 1} = u^{q^{2\theta} - 1}$
3. Multiply both sides by $uv$
   - $uv^{q^\theta} = u^{q^{2\theta}} v$

This results in an equation that is $\mathbb{F}_q$-linear in both plain text and cipher text variables

# Oil and Vinegar + Variants

- 1997: Oil and Vinegar (OV), Patarin
- 1998: Unbalanced Oil and Vinegar (UOV), Kipnis and Shamir
- 2005: Rainbow, Ding and Schmidt

# Unbalanced Oil and Vinegar

$$\mathbf{x} \in \mathbb{F}_q^n \longrightarrow \mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_v \\ x_{v+1} \\ \vdots \\ x_n \end{pmatrix} \begin{array}{l} \leftarrow \text{vinegar variables} \\ \\ \\ \leftarrow \text{oil variables} \end{array}$$

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^{n-v}, \quad P = U \circ F \circ T, \quad F = (f^{(1)}, \ldots, f^{(n-v)})$$

$$f^{(k)}(\mathbf{x}) = \sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ijk} x_i x_j + \sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ijk} x_i x_j + \sum_{i=1}^{n} \gamma_{ik} x_i$$

---

Patarin, “The Oil and Vinegar Signature Scheme.” (1997)
Kipnis, Shamir, “Cryptanalysis of the Oil & Vinegar Signature Scheme.” (1998)

# Rainbow

$$P : \mathbb{F}_q^n \to \mathbb{F}_q^m, \quad P = U \circ F \circ T, \quad F = \left(F^{(1)}, F^{(2)}, \ldots, F^{(L)}\right)$$

$$f_\ell^{(k)}(\mathbf{x}) = \sum_{i=1}^{v_\ell} \sum_{j=1}^{v_\ell} \alpha_{ij\ell} x_i x_j + \sum_{i=1}^{v_\ell} \sum_{j=v_\ell+1}^{n} \beta_{ij\ell} x_i x_j$$

$$0 < v_1 < v_2 < \ldots < v_L < n, \quad O_L \subseteq \ldots \subseteq O_1 \subseteq \mathbb{F}_q^n$$

Ding, Schmidt, "Rainbow, a New Multivariable Polynomial Signature Scheme." Applied Cryptography and Network Security (2005)

# UOV: Signing and Verification

- Sign message $\mathbf{y}$, i.e. find a vector $\mathbf{x}$ such that $P(\mathbf{x}) = \mathbf{y}$
  1. Compute $\mathbf{w} = U^{-1}\mathbf{y}$
  2. Solve for $\mathbf{z}$ such that $F(\mathbf{z}) = \mathbf{w}$

$$f^{(k)} : \sum_{i=1}^{v}\sum_{j=i}^{v} \alpha_{ijk} r_i r_j + \sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ijk} r_i z_j + \sum_{i=1}^{v} \gamma_{ik} z_i + \delta - w_k = 0$$

  3. Compute $\mathbf{x} = T^{-1}\mathbf{z}$
- To verify a signature $\mathbf{x}$:
  1. Calculate

$$P(\mathbf{x}) = U \circ F \circ T\mathbf{x} = U \circ F\mathbf{z} = U \circ \mathbf{w} = \mathbf{y}$$

Thank you for your attention!
Questions?