Key Recovery Attack on The Cubic ABC Simple-Matrix Encryption Scheme

Dustin Moody, *Ray Perlner, Daniel Smith-Tone

Outline

- Multivariate Cryptography
- Cubic ABC
- Differential Structure (Band Spaces and Band Kernels)
- Finding the Structure
- Conclusion

Multivariate cryptography

- Public key is a system of m polynomial equations in n varibles over F_q

  E.g.

$$y_1 = 2x_1^3 + x_1^2x_2 + x_2^2 + 3x_1 + x_2 + 1$$
$$y_2 = 2x_1^2x_2 + 3x_1x_2^2 + x_1x_2 + 4x_1$$

- Plaintext is given by x_i and ciphertext is given by y_i.
- Solving multivariate systems of equations is NP hard in general for polynomials of degree 2 or higher.
  - Most schemes use degree 2 polynomials; we will be considering a degree 3 scheme.
- Private key is some special structure that allows the private-key holder to solve for x_i.
  - Most known schemes only produce secure signatures; we will be considering an encryption scheme.

Multivariate Cryptography 2
Butterfly Construction

- In most multivariate schemes (Cubic ABC included) the public key is constructed as:

$$f_{pub}(x) = \mathcal{T} \circ f \circ \mathcal{U}(x)$$

  - f is an easily invertible Quadratic/Cubic function
    - f is often defined by identifying $(F_q)^n$ with a larger algebraic structure (e.g. an extension field like F_{q^n}.)
    - The ABC scheme defines f using a *matrix algebra* over F_q.

  - $\mathcal{T}$ and $\mathcal{U}$ are affine maps
    - E.g.

$$u_1 = x_1 + 3x_2 + 4$$
$$u_2 = 3x_1 + 2x_2 + 1$$

    - Singular maps are sometimes used for signatures. Here we use invertible maps.

Cubic ABC (Ding, Petzoldt, Wang 2014)

- Cubic ABC is a multivariate encryption scheme
  - One of the few promising candidates
- Modifies the (quadratic) Simple Matrix Encryption Scheme (Tao, Dienne, Tang, Ding 2013)
  - Heuristic argument claiming to rule out structural attacks
- Parameters
  - q: size of the finite field for the variables
  - s: dimension of matrices used in the central map
    - The central map has s^2 input variables and $2s^2$ output variables.

Cubic ABC: The Core Map

- Central map is $s^2 \to 2s^2$ function where the equations are grouped as the elements of two matrices $f(\vec{x}) = \left(E_1(\vec{x}), E_2(\vec{x})\right)$

$$E_1 = AB;\ E_2 = AC$$

  - b_i,c_i are linear functions of $\vec{x}$.
  - p_i are quadratic functions of $\vec{x}$.

$$A = \begin{bmatrix} p_1 & p_2 & \cdots & p_s \\ p_{s+1} & p_{s+2} & \cdots & p_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ p_{s^2-s+1} & p_{s^2-s+2} & \cdots & p_{s^2} \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2} \end{bmatrix},$$

- Decryption proceeds by solving:

$(A(\vec{x}))^{-1}E_1 = B(\vec{x})$

$(A(\vec{x}))^{-1}E_2 = C(\vec{x})$

for $(A(\vec{x}))^{-1}$ and $\vec{x}$. (Linear)

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s^2-s+1} & c_{s^2-s+2} & \cdots & c_{s^2} \end{bmatrix}.$$

Cubic ABC: The Core Map

- Central map is $s^2 \rightarrow 2s^2$ function where the equations are grouped as the elements of two matrices $f(\vec{x}) = \left(E_1(\vec{x}), E_2(\vec{x})\right)$

$$E_1 = AB;\ E_2 = AC$$

  - b_i,c_i are linear functions of $\vec{x}$.
  - p_i are quadratic functions of $\vec{x}$.

$$A = \begin{bmatrix} p_1 & p_2 & \cdots & p_s \\ p_{s+1} & p_{s+2} & \cdots & p_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ p_{s^2-s+1} & p_{s^2-s+2} & \cdots & p_{s^2} \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2} \end{bmatrix},$$

- Decryption proceeds by solving:

$(A(\vec{x}))^{-1}E_1 = B(\vec{x})$

$(A(\vec{x}))^{-1}E_2 = C(\vec{x})$

for $(A(\vec{x}))^{-1}$ and $\vec{x}$. (Linear)

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s^2-s+1} & c_{s^2-s+2} & \cdots & c_{s^2} \end{bmatrix}.$$

Quadratic ABC: The Core Map

- Central map is $s^2 \to 2s^2$ function where the equations are grouped as the elements of two matrices $f(\vec{x}) = \left(E_1(\vec{x}), E_2(\vec{x})\right)$

$$E_1 = AB;\ E_2 = AC$$

  - b_i,c_i are linear functions of $\vec{x}$.
  - $p_i = x_i$.

$$A = \begin{bmatrix} p_1 & p_2 & \cdots & p_s \\ p_{s+1} & p_{s+2} & \cdots & p_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ p_{s^2-s+1} & p_{s^2-s+2} & \cdots & p_{s^2} \end{bmatrix}, B = \begin{bmatrix} b_1 & b_2 & \cdots & b_s \\ b_{s+1} & b_{s+2} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s^2-s+1} & b_{s^2-s+2} & \cdots & b_{s^2} \end{bmatrix},$$

- Decryption proceeds by solving:

$(A(\vec{x}))^{-1}E_1 = B(\vec{x})$

$(A(\vec{x}))^{-1}E_2 = C(\vec{x})$

for $(A(\vec{x}))^{-1}$ and $\vec{x}$. (Linear)

$$C = \begin{bmatrix} c_1 & c_2 & \cdots & c_s \\ c_{s+1} & c_{s+2} & \cdots & c_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ c_{s^2-s+1} & c_{s^2-s+2} & \cdots & c_{s^2} \end{bmatrix}.$$

Special structure of Quadratic ABC (Row Band Spaces)

$$AB = E_1$$

$$\begin{pmatrix} x_{(i-1)s+1} & x_{(i-1)s+2} & \cdots & x_{is} \end{pmatrix} \begin{pmatrix} b_j \\ b_{s+j} \\ \vdots \\ b_{s^2-s+j} \end{pmatrix} = \begin{pmatrix} E_{(i-1)s+j} \end{pmatrix}$$

- Note that all quadratic monomials in $(E_{(i-1)s+1}, \ldots, E_{is})$ contain one of the s variables $(x_{(i-1)s+1}, \ldots, x_{is})$
- We previously used this structure to cryptanalyze the quadratic ABC scheme. (Moody, Perlner, Smith-Tone 2014)

Special Structure of Cubic (and Quadratic) ABC (Column Band Spaces)

$$AB = E_1$$

$$\begin{pmatrix} p_{(i-1)s+1} & p_{(i-1)s+2} & \cdots & p_{is} \end{pmatrix} \begin{pmatrix} b_j \\ b_{s+j} \\ \vdots \\ b_{s^2-s+j} \end{pmatrix} = \begin{pmatrix} E_{(i-1)s+j} \end{pmatrix}$$

- Under a basis $(u'_1, \ldots u'_{s^2})$ where $(u'_1, \ldots u'_s) = (b_j(\vec{x}), b_{s+j}(\vec{x}) \ldots b_{s^2-s+j}(\vec{x}))$:
  - All cubic monomials in column j of E, i.e. $(E_j(\vec{x}), E_{s+j}(\vec{x}) \ldots E_{s^2-s+j}(\vec{x}))$ contain at least one factor of $(u'_1, \ldots u'_s)$
- We will call these s equations (and their linear combination) *band-space maps*
- We will also define the band kernel: The space of vectors $\vec{x}$, such that

$$(u'_1(\vec{x}), \ldots, u'_s(\vec{x})) = 0$$

How many band spaces are there:

- **Not only do the columns of $E_1 = AB$ and $E_2 = AC$ define band spaces, but fixed linear combinations of the columns $(\vec{\beta}, \vec{\gamma})$ do as well.**
  - *Band Space*:

$$\mathcal{B}_{\beta,\gamma} = Span(\mathcal{E}_{\beta,\gamma,1}, \ldots, \mathcal{E}_{\beta,\gamma,s})$$

$$\mathcal{E}_{\beta,\gamma,i} = \sum_{j=1}^{s} (\beta_j \mathcal{E}_{(i-1)s+j} + \gamma_j \mathcal{E}_{s^2+(i-1)s+j})$$

$$= \sum_{l=1}^{s} \left(p_{(i-1)s+l} \sum_{j=1}^{s} (\beta_j b_{(l-1)s+j} + \gamma_j c_{(l-1)s+j}) \right)$$

  - *Band Kernel*:

$(x \in \mathcal{BK}_{\beta,\gamma})$

$$u_i' = \sum_{j=1}^{s} (\beta_j b_{(i-1)s+j}(x) + \gamma_j c_{(i-1)s+j}(x)) = 0$$

A Formal Tool for Describing the Structure: The Discrete Differential

- Definition: $\boldsymbol{Df(\vec{x},\vec{a}) = f(\vec{x}+\vec{a}) - f(\vec{x}) - f(\vec{a}) + f(\vec{0})}$
- We will be considering the structure of cubic monomials, **so we will use $\boldsymbol{D^2 f(\vec{a},\vec{b},\vec{x})}$**
- Useful properties:
  - **Its entries are the coefficients of cubic monomials in $\boldsymbol{f}$**

$$f(\vec{x}) = \sum_{i\le j\le k} a_{ijk} x_i x_j x_k$$

$$\Rightarrow D^2 f(\vec{a},\vec{b},\vec{x}) = \sum_{i\le j\le k} (D^2 f)_{ijk} a_i b_j x_k\,;$$

$$(D^2 f)_{ijk} = \begin{cases} a_{ijk} & i \neq j \neq k \\ 2a_{ijk} & i = j \neq k \\ 6a_{ijk} & i = j = k \end{cases}$$

  - **$\boldsymbol{D^2 f}$ is a 3-tensor: i.e for linear maps/ changes of basis $\boldsymbol{U}$:**

$$f'(\vec{x}) = f(U\vec{x})$$

$$\Rightarrow D^2 f'(\vec{a},\vec{b},\vec{x}) = D^2 f(U\vec{a}, U\vec{b}, U\vec{x})$$

Or equivalently:

$$(D^2 f')_{ijk} = \sum_{l,m,n} (D^2 f)_{lmn} U_{li} U_{mj} U_{nk}$$

The (2nd) Differential Form of Band-Space Maps

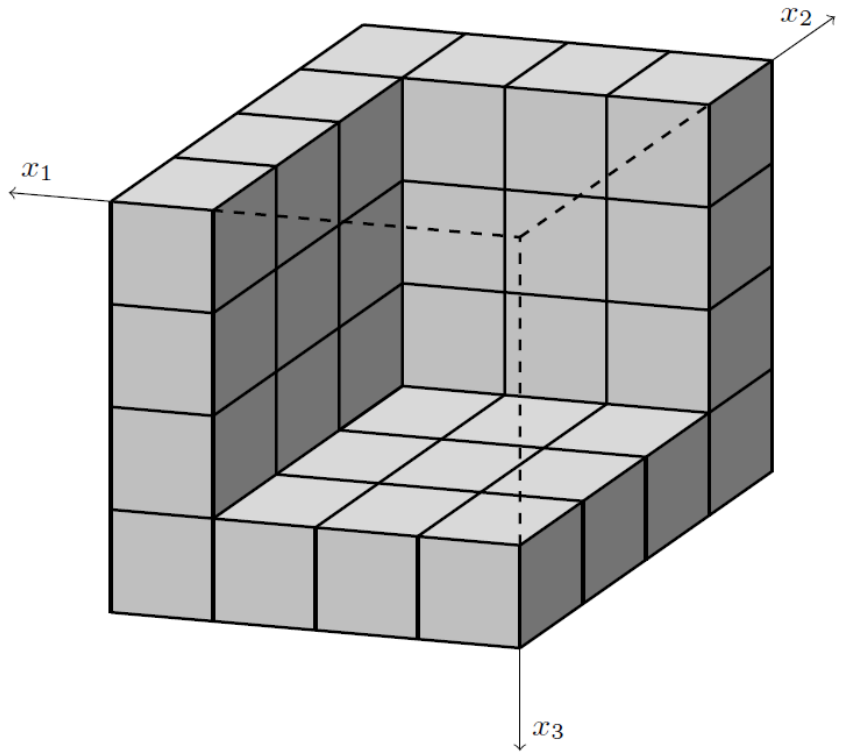


Fig. 1. 3-tensor structure of the second differential of a band space map. Solid regions correspond to nonzero coefficients. Transparent regions correspond to zero coefficients.

Some properties of band-space differentials.
(in the u'_i basis)

- For three vectors $x_1, x_2, x_3 \in \mathcal{BK}_{\beta,\gamma}$:
$$D^2\mathcal{E}_{\beta,\gamma}(x_1, x_2, x_3) = 0$$

- For two vectors $x_1, x_2 \in \mathcal{BK}_{\beta,\gamma}$:
$$D^2\mathcal{E}_{\beta,\gamma}(x_1, x_2) = (y(u'_1), \dots, y(u'_s), 0, \dots, 0)$$
  - Note that $D^2\mathcal{E}_{\beta,\gamma}$ maps x_1, x_2 to an s-dimensional subspace of linear forms

- For one vector $x_1 \in \mathcal{BK}_{\beta,\gamma}$:
$$D^2\mathcal{E}_{\beta,\gamma}(x_1) = \begin{pmatrix} S & - & R & - \\ | & & & \\ R^T & & 0 & \\ | & & & \end{pmatrix}$$
  - Note that the rank of the resulting 2-tensor (matrix) is at most $2s$.
- But the components of the public key aren't band-space maps, but linear combinations of them, under the private transformation $\mathcal{T}$, since $f_{pub}(x) = \mathcal{T} \circ f \circ \mathcal{U}(x)$

Our attack strategy (Modified MinRank)

- Select s^2-dimensional vectors, x_1, x_2, x_3, x_4.

- Solve

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_2) = 0$$

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_3, x_4) = 0$$

For t_i.

- Hope that $\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i \in \mathfrak{B}_{\beta,\gamma}$ and $x_1, x_2, x_3, x_4 \in \mathcal{BK}_{\beta,\gamma}$
    - If so, the 2-tensor $\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_k)$ will have rank at most $2s$.

Setting some vectors equal

- We can increase the probability that the vectors share a band kernel by setting some of them equal to one another (e.g. by solving:)

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i (x_1, x_1) = 0$$

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i (x_2, x_2) = 0$$

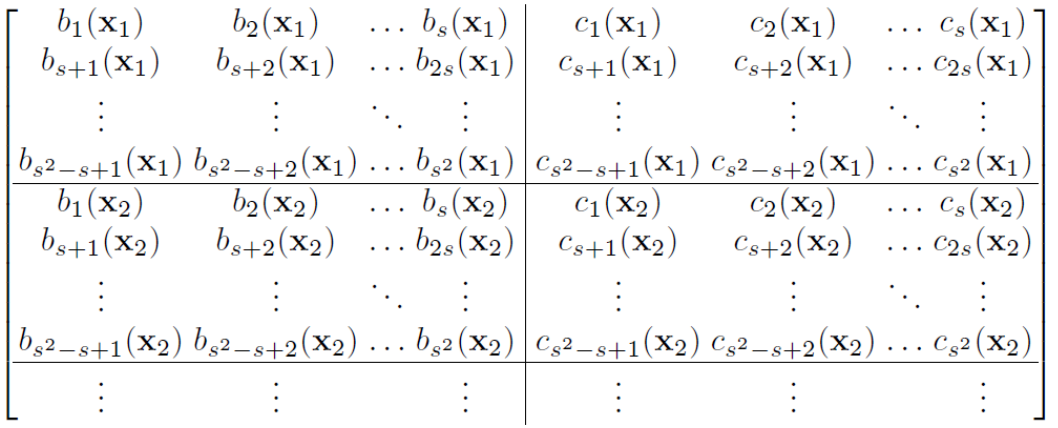
  - This works in odd characteristic, but in characteristic 2, $D^2\mathcal{E}_i(x_1, x_1) = 0$ by symmetry. So the best we can do there is:

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i (x_1, x_2) = 0$$

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i (x_1, x_3) = 0$$

How likely are random vectors to share a band kernel?

- $x_1, x_2, \ldots$ share a band kernel if there is a nontrivial linear relation on the columns of the matrix at right:



- If all four vectors are randomly chosen it's a random $4s \times 2s$
  - Probability is $\sim \frac{1}{q-1} q^{-2s}$
- If we set a pair of vectors equal (e.g. $x_4 = x_1$) it's a random $3s \times 2s$
  - Probability is $\sim \frac{1}{q-1} q^{-s}$
- If we set two pairs of vectors equal (e.g. $x_1 = x_2; x_3 = x_4$) it's a random $2s \times 2s$
  - Probability is $\sim \frac{1}{q-1}$

If the vectors share a band kernel, how likely are we to find a band-space map?

- We find a band space map if there exists nonzero $(\tau_1, \dots, \tau_s)$ such that:

$$\sum_{i=1}^{s} \tau_i D^2 \mathcal{E}_{\beta,\gamma,i}\,(x_1, x_2) = 0$$

$$\sum_{i=1}^{s} \tau_i D^2 \mathcal{E}_{\beta,\gamma,i}\,(x_3, x_4) = 0$$

- Recall that $\sum_{i=1}^{s} \tau_i D^2 \mathcal{E}_{\beta,\gamma,i}$ maps band kernel vectors to an s-dimensional space of linear forms.
- Thus we have $2s$ (random) linear constrains on s variables
  - The probability that there is a nontrivial solution is $\sim \frac{1}{q-1} q^{-s}$

How big a space of solutions do we have to search through

- Even if a low rank solution exists to

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_2) = 0$$

$$\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_3, x_4) = 0,$$

it isn't necessarily the only one.

- Generically we'd expect a 0 dimensional solution space ($2s^2$ equations in $2s^2$ variables.) However, low characteristic imposes some linear dependencies:
  - Characteristic 2
    - $\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_2)(x_1) = \sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_2)(x_2) = \sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_3, x_4)(x_3) = \sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_3, x_4)(x_4) = 0$
    - And if x_4=x_1: $\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_2)(x_3) + \sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_3)(x_2) = 0$
    - So we expect a 5 dimensional solution space which requires $q^4 + q^3 + q^2 + q + 1$ rank computations to search.
  - Characteristic 3 ($x_1 = x_2; x_3 = x_4$)
    - $\sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_1, x_1)(x_1) = \sum_{i=1}^{2s^2} t_i D^2 \mathcal{E}_i\,(x_2, x_2)(x_2) = 0$
    - So we expect a 2 dimensional solution space which requires $q + 1$ rank computations to search.

Putting it all together

- Finding a band-space map costs approximately
  - $q^{2s+6}s^{2\omega}$ for characteristic 2.
  - $q^{s+3}s^{2\omega}$ for characteristic 3.
  - $q^{s+2}s^{2\omega}$ for higher characteristic.

  ($\omega \approx 2.373$ is the linear algebra constant.)

- Once a band space map is found, a full key recovery is possible at minimal additional cost.

How bad is the attack

- Finding a band-space map costs approximately
  - $q^{2s+6}s^{2\omega}$ for characteristic 2.
  - $q^{s+3}s^{2\omega}$ for characteristic 3.
  - $q^{s+2}s^{2\omega}$ for higher characteristic.

    ($\omega \approx 2.373$ is the linear algebra constant.)
  - Once a band space map is found, a full key recovery is possible at minimal additional cost.
- We previously did a similar analysis of quadratic ABC:
  - $q^{s+4}s^{2\omega}$ for characteristic 2.
  - $q^{s+2}s^{2\omega}$ for higher characteristic.
- Cubic ABC does not eliminate structural attacks (which was the original goal)
- The proposed parameters are still ok (since they used characteristic 2)
- However, our attack breaks odd characteristic versions of cubic ABC that previously published analysis says should be secure.

Thank You!

Key Recovery: Overall Strategy

- Find an equivalent private key. i.e. $\mathcal{T}'$, A', B', C' such that
$$\mathcal{T}' \circ \big(A'(x)B'(x), A'(x)C'(x)\big) = \mathcal{E}_{pub}(x)$$
  - Note that $\mathcal{U}'$ is unnecessary, since $p\big(\mathcal{U}'(x)\big)$ is still a random quadratic polynomial in x and $b\big(\mathcal{U}'(x)\big)$ and $c\big(\mathcal{U}'(x)\big)$ are still random linear polynomials.
- Multistep process starting with a single band space map and two band kernel vectors:
  1. Solve for the whole band kernel.
  2. Solve for the whole band space.
  3. Solve for a column of B': $(v_1, \dots, v_s)^T$.
  4. Solve for A' (mod $v_1, \dots, v_s$).
  5. Solve for B' and C' (mod $v_1, \dots, v_s$) and $\mathcal{T}'$.
  6. Select another column of B' (mod $v_1, \dots, v_s$) and solve for the corresponding band space.
  7. Solve for the band kernel corresponding to the band space in step 6.
  8. Solve for the rest of A'.
  9. Solve for the rest of B' and C'

Key Recovery Step 1: Solving for the whole band kernel.

- Once we've found a band-space map $\mathcal{E}_{\beta,\gamma}$ and at least two vectors from the band kernel, we can find the whole band kernel by taking the *span of the union of the kernels* of $D^2\mathcal{E}_{\beta,\gamma}(x_1)$ and $D^2\mathcal{E}_{\beta,\gamma}(x_2)$
  - This works because, in a basis including generators of the band kernel

$$D^2\mathcal{E}_{\beta,\gamma}(x_k) = \begin{pmatrix} S_k & - & R_k & - \\ | & & & \\ R_k{}^T & & 0 & \\ | & & & \end{pmatrix}$$

  - With high probability each kernel contains $s^2 - 2s$ basis vectors of the (s^2-s)-dimensional band kernel, and the union contains a full basis.

Key Recovery Step 2: Solving for the whole band space

- The band space maps $\mathcal{E}_{\beta,\gamma}$ are simply the maps in the span of the public equations $\mathcal{E}_i$ such that

$$D^2\mathcal{E}_{\beta,\gamma}(x_1, x_2, x_3) = 0$$

$\forall x_1, x_2, x_3 \in \mathcal{BK}_{\beta,\gamma}$

- Call a basis of this space $(\mathcal{E}_{\beta,\gamma,1}, \ldots, \mathcal{E}_{\beta,\gamma,s})$

Key Recovery Step 3:
Solving for the space of linear forms in $B\beta + C\gamma$
(This can be our first column of B')

- These are simply the space of linear forms v such that

$$v(x) = 0$$

$\forall x \in \mathcal{BK}_{\beta,\gamma}$

- Call a basis of this space $(v_1, \ldots, v_s)$

Key Recovery Step 4: Solving for A' (mod $v_1, \ldots, v_s$)

- $A(B\beta + C\gamma)$ and $B\beta + C\gamma$ are related to $(\mathcal{E}_{\beta,\gamma,1}, \ldots, \mathcal{E}_{\beta,\gamma,s})^T$ and $(v_1, \ldots, v_s)^T$ by simple row operations:
  - $A(B\beta + C\gamma) = \Omega_1 \begin{pmatrix} \mathcal{E}_{\beta,\gamma,1} \\ \vdots \\ \mathcal{E}_{\beta,\gamma,s} \end{pmatrix}$
  - $B\beta + C\gamma = \Omega_2 \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix}$
- Therefore $A' = {\Omega_1}^{-1} A \Omega_2$ is a solution of

$$A' \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} = \begin{pmatrix} \mathcal{E}_{\beta,\gamma,1} \\ \vdots \\ \mathcal{E}_{\beta,\gamma,s} \end{pmatrix}$$

- However, the solution is only unique over polynomials modulo $v_1, \ldots, v_s$
  - This is because we can get cancellations like $p_1 v_1 + p_2 v_2 = (p_1 + u v_2) v_1 + (p_2 - u v_1) v_2$

Key Recovery Step 5: Solving for B' and C' (mod $v_1, \ldots, v_s$) and $\mathcal{T}'^{-1}$

- We can solve linear equations for B', C', and $\mathcal{T}'^{-1}$ (mod $v_1, \ldots, v_s$)

$$(A'B', A'C') = \mathcal{T}'^{-1} \circ \mathcal{E}_{pub} \text{ (mod } v_1, \ldots, v_s)$$

- The solution (mod $v_1, \ldots, v_s$) is (with high probability) unique up to column operations on (B', C')
  - i.e. any solution will generate a valid private key.
- Note that the coefficients of $\mathcal{T}'^{-1}$ are scalars, not polynomials, so (mod $v_1, \ldots, v_s$) does not affect $\mathcal{T}'^{-1}$
  - We now have our $\mathcal{T}'$.

Key Recovery Step 6:
Solving for another Band Space

(corresponding to another column of B' (mod $v_1, \ldots, v_s$))

- Select a column $(v_{s+1}, \ldots, v_{2s})^T$ of B' (mod $v_1, \ldots, v_s$)

- We can find the band space maps corresponding to this column of B' by taking the corresponding column $(F_{s+1}, \ldots, F_{2s})^T$ of $\mathcal{T}'^{-1} \circ \mathcal{E}_{pub}$
  - Note these band space maps are completely known (no mod $v_1, \ldots, v_s$)!

Key Recovery Step 7: Solving for the Band Kernel

(For the Band Space we found in Step 6)

- We can solve for the intersection of our two band kernels as follows:
  - The intersection is the set of vectors x such that:

$$\big(v_{s+1}(x), \dots, v_{2s}(x)\big)\big(\mathrm{mod}\ v_1(x), \dots, v_s(x)\big) = 0$$
$$(v_1(x), \dots, v_s(x)) = 0$$

- Now we have (more than 1) equations in the second band space, and (more than 2) elements of the band kernel, so we can do what we did the last time:
  - Take the span of the union of the kernels of $D^2 F_{s+1} x_1$ and $D^2 F_{s+1} x_2$ for x_1 and x_2 in the band kernel of $(F_{s+1}, \dots, F_{2s})$.

Key Recovery Step 8: Solving for the Rest of A'

- With high probability $(v_{s+1}, \dots, v_{2s})^T$ is fixed by
  - $(v_{s+1}, \dots, v_{2s})^T$ (mod $v_1, \dots, v_s$)
  - The condition that $\big(v_{s+1}(x), \dots, v_{2s}(x)\big) = 0$ for any x in the band kernel of $(F_{s+1}, \dots, F_{2s})$

- $A' \begin{pmatrix} v_1 \\ \vdots \\ v_s \end{pmatrix} = \begin{pmatrix} F_1 \\ \vdots \\ F_s \end{pmatrix}$ fixes A' (mod $v_1, \dots, v_s$)

- $A' \begin{pmatrix} v_{s+1} \\ \vdots \\ v_{2s} \end{pmatrix} = \begin{pmatrix} F_{s+1} \\ \vdots \\ F_{2s} \end{pmatrix}$ fixes A' (mod $v_{s+1}, \dots, v_{2s}$)

- Together the two equations fix A' entirely. (assuming $v_1, \dots, v_{2s}$ are linearly independent – high probability and easy to check.)

Key Recovery Step 9: Solving for the rest of B' and C'

- Same equation as before without the (mod $v_1, \ldots, v_s$)

$$(A'B', A'C') = \mathcal{T}'^{-1} \circ \mathcal{E}_{pub}$$