Black-Box Secret Sharing from Primitive Sets in Algebraic Number Fields

Ronald Cramer[1,2] Serge Fehr[1] Martijn Stam[3]

[1] CWI (Amsterdam)

[2] Mathematical Institute, Leiden University

[3] Department of Computer Science, University of Bristol

17 August 2005

Outline

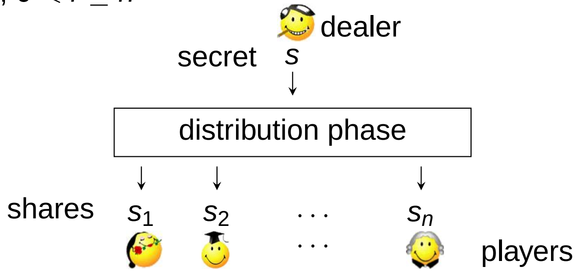
Threshold Secret Sharing

Dealing

n the number of participants;

s the secret;

s_i A share, $0 < i \leq n$



Threshold Secret Sharing

Requirements

n the number of participants;
t the threshold;
s the secret;
s_i A share, $0 < i \leq n$

Completeness: Any qualified subset A (of at least $t+1$ participants) can recover the secret;

Privacy: No non-qualified subset (of at most t participants) obtains any Shannon information about the secret.

Share Expansion: The average length of a share:

$$\frac{\sum_{i=1}^{n}(\text{length of } s_i)}{n \times \text{length of } s}$$

Shamir Secret Sharing

Based on polynomial evaluation.

Setting: $s \in \mathbb{F}$, where $\mathbb{F}$ any finite field.

Dealing: Pick $(g_0, \ldots, g_{t-1}) \in \mathbb{F}^t$ at random. Let $g_t = s$.

$$g(x) := g_0 + g_1 x + \cdots + g_t x^t$$

Participant i gets share $s_i = g(\alpha_i)$, where $\alpha_i \in \mathbb{F}$.

Reconstruction: Lagrange Interpolation,

$$s = g_t = \sum_{i \in A} \left(\prod_{j \in A, j \neq i} \frac{1}{\alpha_i - \alpha_j} \right) s_i$$

Defining Black Box Secret Sharing Schemes

A linear threshold secret sharing scheme for $s \in G$ where G can be an arbitrary finite abelian group (additive).

- Shares are computed as $\mathbb{Z}$-linear comb.'s (independent of G) of $s \in G$ and random group elements. Expansion factor equals the average number of group elements per share.
- Reconstruction works by $\mathbb{Z}$-linear comb.'s (independent of G) of the shares, and
- Correctness and Privacy must hold regardless of group G.

Defining Black Box Secret Sharing Schemes

A linear threshold secret sharing scheme for $s \in G$ where G can be an arbitrary finite abelian group (additive).

- Shares are computed as $\mathbb{Z}$-linear comb.'s (independent of G) of $s \in G$ and random group elements. Expansion factor equals the average number of group elements per share.
- Reconstruction works by $\mathbb{Z}$-linear comb.'s (independent of G) of the shares, and
- Correctness and Privacy must hold regardless of group G.

Defining Black Box Secret Sharing Schemes

A linear threshold secret sharing scheme for $s \in G$ where G can be an arbitrary finite abelian group (additive).

- Shares are computed as $\mathbb{Z}$-linear comb.'s (independent of G) of $s \in G$ and random group elements. Expansion factor equals the average number of group elements per share.
- Reconstruction works by $\mathbb{Z}$-linear comb.'s (independent of G) of the shares, and
- Correctness and Privacy must hold regardless of group G.

Defining Black Box Secret Sharing Schemes

A linear threshold secret sharing scheme for $s \in G$ where G can be an arbitrary finite abelian group (additive).

- Shares are computed as $\mathbb{Z}$-linear comb.'s (independent of G) of $s \in G$ and random group elements. Expansion factor equals the average number of group elements per share.
- Reconstruction works by $\mathbb{Z}$-linear comb.'s (independent of G) of the shares, and
- Correctness and Privacy must hold regardless of group G.

Defining Black Box Secret Sharing Schemes

A linear threshold secret sharing scheme for $s \in G$ where G can be an arbitrary finite abelian group (additive).

- Shares are computed as $\mathbb{Z}$-linear comb.'s (independent of G) of $s \in G$ and random group elements. Expansion factor equals the average number of group elements per share.
- Reconstruction works by $\mathbb{Z}$-linear comb.'s (independent of G) of the shares, and
- Correctness and Privacy must hold regardless of group G.

Goal: Minimizing the expansion factor, and keeping the computational cost low.

Using an Extension Ring

Special Case: Let $f \in \mathbb{Z}[X]$ be irreducible, monic, of degree m, define $R = \mathbb{Z}[X]/(f)$, i.e., univariate polynomials over the integers reduced modulo f.

Extending the Ring of Integers: R is a ring extension of $\mathbb{Z}$

Number Field: R is an order in the number field $\mathbb{Q}[X]/(f)$.
This allows the use of number theoretic means to analyse R.
In particular, R is a free $\mathbb{Z}$-module.

Tensor Product: The tensor product $R \otimes_{\mathbb{Z}} G$ is isomorphic to G^m.

Module Operation: $R \otimes_{\mathbb{Z}} G$ or G^m is an R-module.
In particular, for $g \in G^m$ and $r \in R$ the product $rg \in G^m$ is properly defined.

Shamir Secret Sharing over a Ring

Dealing

Setting: f monic irred. of degree m, $R = \mathbb{Z}[X]/(f)$ and $s \in G$. Define $S = (s, 0, \ldots, 0) \in G^m$.

Weak BBSSS: A BBSSS with weak reconstructability in that $\Delta \cdot S \in G^m$, not s, can be reconstructed for some $\Delta \in R$.

Adapting Shamir: Use coefficients in G^m, evaluation points in R. Pick $(g_0, \ldots, g_{t-1}) \in (G^m)^t$ at random, let $g_t = S$.

$$g(x) := g_0 + g_1 x + \cdots + g_t x^t$$

Participant i gets share $s_i = g(\alpha_i) \in G^m$, where $\alpha_i \in R$.

Privacy: Automatic for the people.

Expansion Factor: If this is all, the expansion factor would be m.

Shamir Secret Sharing over a Ring

Reconstruction

Recall Lagrange Interpolation,

$$s = \sum_{i \in A} \left(\prod_{j \in A, j \neq i} \frac{1}{\alpha_i - \alpha_j} \right) s_i$$

Problem: Possibly $(\alpha_i - \alpha_j)^{-1}$ not in R.

Solution: Multiply both sides with

$$\Delta = \prod_{0 < i < j \leq n} (\alpha_i - \alpha_j)$$

Shamir Secret Sharing over a Ring

Reconstruction

Recall Lagrange Interpolation,

$$S = \sum_{i \in A} \left(\prod_{j \in A, j \neq i} \frac{1}{\alpha_i - \alpha_j} \right) s_i$$

Problem: Possibly $(\alpha_i - \alpha_j)^{-1}$ not in R.

Solution: Multiply both sides with

$$\Delta = \prod_{0 < i < j \leq n} (\alpha_i - \alpha_j)$$

Shamir Secret Sharing over a Ring

Reconstruction

Recall Lagrange Interpolation,

$$\Delta \cdot S = \sum_{i \in A} \left(\prod_{j \in A, j \neq i} \Delta \frac{1}{\alpha_i - \alpha_j} \right) s_i$$

Problem: Possibly $(\alpha_i - \alpha_j)^{-1}$ not in R.

Solution: Multiply both sides with

$$\Delta = \prod_{0 < i < j \leq n} (\alpha_i - \alpha_j)$$

Previous Art

Finding R and Δ that allow extraction of s from $\Delta \cdot S$.

Desmedt and Frankel: Sufficient condition: Δ invertible in the ring R. Expansion factor $\approx n$.

Cramer and Fehr: Idea: Perform two sharings and reconstruct $\Delta_\alpha \cdot S$ and $\Delta_\beta \cdot S$ with coprime Δ_α and Δ_β.
Provided scheme with expansion factor $\lfloor \log_2 n \rfloor + 2$.

Also proved lower bound of $\lfloor \log_2 n \rfloor - 1$.

The New Scheme in Theory

The Underlying Idea

Primitive Element: Let R be an integral extension. Then $r \in R$ is called primitive if its only rational integer divisors are 1 and -1, i.e., $r \not\equiv 0 \bmod p$ for all primes $p \in \mathbb{Z}$. Such

Primitive Set: Let R be as above. Then $\alpha_1, \ldots, \alpha_n \in R$ is a primitive set if its Vandermonde determinant Δ is primitive.

$$\Delta = \prod_{0<i<j\leq n} (\alpha_i - \alpha_j)$$

The New Scheme in Theory

The Underlying Idea

Primitive Element: Let R be an integral extension. Then $r \in R$ is called primitive if its only rational integer divisors are 1 and -1, i.e., $r \not\equiv 0 \bmod p$ for all primes $p \in \mathbb{Z}$. Such

Primitive Set: Let R be as above. Then $\alpha_1, \ldots, \alpha_n \in R$ is a primitive set if its Vandermonde determinant Δ is primitive.

Observation: Let $\Delta \in R = \mathbb{Z}[X]/(f)$, then $\Delta \cdot S = \Delta(s, 0, \ldots, 0) = (\delta_0 s, \ldots, \delta_{m-1} s) \in G^m$. If Δ is primitive, then the δ_i's are coprime.
$\Rightarrow$ s can be reconstructed from $\Delta \cdot S$ (alone).

Goal: Find R that allows $\alpha_1, \ldots, \alpha_n \in R$ such that Δ is primitive, where m, the degree of R is as small as possible.

The New Scheme in Theory

The Underlying Idea

Primitive Element: Let R be an integral extension. Then $r \in R$ is called primitive if its only rational integer divisors are 1 and -1, i.e., $r \not\equiv 0 \bmod p$ for all primes $p \in \mathbb{Z}$. Such

Primitive Set: Let R be as above. Then $\alpha_1, \ldots, \alpha_n \in R$ is a primitive set if its Vandermonde determinant Δ is primitive.

Observation: Let $\Delta \in R = \mathbb{Z}[X]/(f)$, then $\Delta \cdot S = \Delta(s, 0, \ldots, 0) = (\delta_0 s, \ldots, \delta_{m-1} s) \in G^m$. If Δ is primitive, then the δ_i's are coprime.
$\Rightarrow$ s can be reconstructed from $\Delta \cdot S$ (alone).

Goal: Find R that allows $\alpha_1, \ldots, \alpha_n \in R$ such that Δ is primitive, where m, the degree of R is as small as possible.

The New Scheme in Theory

(Partial) Solution

Let f be monic irreducible and $R = \mathbb{Z}[X]/(f)$.
For all primes $p \in \mathbb{Z}$ we can factor f modulo p

$$f_p(x) \equiv f \bmod p \equiv \prod_i f_{p,i}^{e_{p,i}}$$

where the $f_{p,i}$ are irreducible modulo p of degree $d_{p,i}$.
Let $d_p = \max_i d_{p,i}$.

Theorem: There exists a primitive set in R of cardinality

$$\min_{p \text{ prime},} p^{d_p} .$$

Corollary: For any $t, n \in \mathbb{Z}$ there exists a BBSSS with expansion factor $\lceil \log_2 n \rceil$.

The New Scheme in Theory

(Partial) Solution

Let f be monic irreducible and $R = \mathbb{Z}[X]/(f)$.
For all primes $p \in \mathbb{Z}$ we can factor f modulo p

$$f_p(x) \equiv f \bmod p \equiv \prod_i f_{p,i}^{e_{p,i}}$$

where the $f_{p,i}$ are irreducible modulo p of degree $d_{p,i}$.
Let $d_p = \max_i d_{p,i}$.

Theorem: There exists a primitive set in R of cardinality

$$\min_{p \text{ prime},} p^{d_p} .$$

Corollary: For any $t, n \in \mathbb{Z}$ there exists a BBSSS with expansion factor $\lceil \log_2 n \rceil$.

Proof (Simplified Sketch)

Easier case

Let $p \in \mathbb{Z}$ be a prime, write

$$R/pR \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}} \cdots f_{p,\ell_p}^{\epsilon_{p,\ell_p}}) \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}^{\epsilon_{p,\ell_p}})$$

giving the canonical projection

$$R/pR \to \mathbb{F}_p[X]/(f_{p,1}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}) \simeq \mathbb{F}_{p^{d_{p,1}}} \times \cdots \times \mathbb{F}_{p^{d_{p,\ell_p}}}$$

If $n \leq p^{d_p}$ pick n distinct elements from $\mathbb{F}_{p^{d_p}}$ and lift to R giving $\alpha_1, \ldots, \alpha_n \in R$ such that $\Delta \not\equiv 0 \bmod pR$.

For a finite set of primes p combine solutions with CRT to one that holds modulo these primes simultaneously.

Problem: We need a solution modulo all primes.

Proof (Simplified Sketch)

Easier case

Let $p \in \mathbb{Z}$ be a prime, write

$$R/pR \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}} \cdots f_{p,\ell_p}^{\epsilon_{p,\ell_p}}) \simeq \mathbb{F}_p[X]/(f_{p,1}^{\epsilon_{p,1}}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}^{\epsilon_{p,\ell_p}})$$

giving the canonical projection

$$R/pR \to \mathbb{F}_p[X]/(f_{p,1}) \times \cdots \times \mathbb{F}_p[X]/(f_{p,\ell_p}) \simeq \mathbb{F}_{p^{d_{p,1}}} \times \cdots \times \mathbb{F}_{p^{d_{p,\ell_p}}}$$

If $n \leq p^{d_p}$ pick n distinct elements from $\mathbb{F}_{p^{d_p}}$ and lift to R giving $\alpha_1, \ldots, \alpha_n \in R$ such that $\Delta \not\equiv 0 \bmod pR$.
For a finite set of primes p combine solutions with CRT to one that holds modulo these primes simultaneously.
Problem: We need a solution modulo all primes.

The Proof (Simplified Sketch)

Induction: Use finite induction on the interpolation points. Suppose that $\alpha_1, \ldots, \alpha_{i-1}$ are already succesfully chosen, construct α_i such that

$$\Delta_i \qquad = \Delta_{i-1} \prod_{j<i} (\alpha_j - \alpha_i)$$

$$\not\equiv 0 \mod p \text{ for all } p.$$

Fix one coordinate: Set one coordinate of α_i such that the induction hypothesis holds for almost all primes.

CRT: Use Chinese Remainder Theorem to fix α_i for the finite number of remaining primes.

The Proof (Simplified Sketch)

Induction: Use finite induction on the interpolation points. Suppose that $\alpha_1, \dots, \alpha_{i-1}$ are already succesfully chosen, construct α_i such that

$$\Delta_i(x) = \Delta_{i-1} \prod_{j<i} (\alpha_j - x)$$

$\not\equiv 0 \mod p$ for all p.

Fix one coordinate: Set one coordinate of α_i such that the induction hypothesis holds for almost all primes.

CRT: Use Chinese Remainder Theorem to fix α_i for the finite number of remaining primes.

The Proof (Simplified Sketch)

Induction: Use finite induction on the interpolation points. Suppose that $\alpha_1, \ldots, \alpha_{i-1}$ are already succesfully chosen, construct α_i such that

$$\Delta_i(x) = \Delta_{i-1} \prod_{j<i} (\alpha_j - x)$$

$\not\equiv 0 \mod p$ for all p.

Fix one coordinate: Set one coordinate of α_i such that the induction hypothesis holds for almost all primes.

CRT: Use Chinese Remainder Theorem to fix α_i for the finite number of remaining primes.

The Proof (Simplified Sketch)

Induction: Use finite induction on the interpolation points. Suppose that $\alpha_1, \ldots, \alpha_{i-1}$ are already succesfully chosen, construct α_i such that

$$\Delta_i(x) = \Delta_{i-1} \prod_{j<i} (\alpha_j - x)$$

$\not\equiv 0 \mod p$ for all p.

Fix one coordinate: Set one coordinate of α_i such that the induction hypothesis holds for almost all primes.

CRT: Use Chinese Remainder Theorem to fix α_i for the finite number of remaining primes.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The Proof (Simplified Sketch)

Rewrite α_i: Write down α_i in basis of R, so

$$\alpha_i = a_0 + a_1 X + \cdots + a_{m-1} X^{m-1}$$

Consider the coefficients a_j as unknowns A_j.

Rewrite Δ_i: Write down Δ_i in basis of R in unknowns A_i.

$$\Delta_i = \Delta_{i-1}(G_0(A_0, A_1, \ldots, A_{m-1}) + \cdots + G_{m-1}(A_0, \ldots, A_{m-1}) X^{m-1})$$

Use Algebra: $\Delta_i \equiv 0 \bmod p$ iff $G_j(A_0, \ldots, A_{m-1}) \equiv 0 \bmod p$ for all j. Then also all linear combinations of the polynomials G_j.

Find Univariate Polynomial: Construct a univariate polynomial $P(A_0) \in \mathbb{Z}[A_0]$ that is a linear comb. of the G_j.

Pick a non-root: Then instantiate with a_0 such that $P(a_0) \neq 0$ as integer. Then for all p not dividing $P(a_0)$ we have that $\Delta_i \not\equiv 0 \bmod p$.

The New Scheme in Practice

Relevant Complexities

Cramer & Fehr: α_i's may be chosen with coeffs in $\{0, 1\}$, but $f(X)$'s coeffs seem to be bound to bitlength n.

$\rightsquigarrow \tilde{O}(n^3)$

Cramer, Fehr & Stam: Evidence that α_i's may be chosen with coeffs in $\{0, 1\}$ and $f(X)$ with coeffs in $\{-1, 0, 1\}$ (Shown for n up to 4096, but no general proof).

$\rightsquigarrow \tilde{O}(n^2)$

The New Scheme in Practice

Relevant Complexities

Cramer & Fehr: α_i's may be chosen with coeffs in $\{0,1\}$, but $f(X)$'s coeffs seem to be bound to bitlength n.

$\rightsquigarrow \tilde{O}(n^3)$

Cramer, Fehr & Stam: Evidence that α_i's may be chosen with coeffs in $\{0,1\}$ and $f(X)$ with coeffs in $\{-1,0,1\}$ (Shown for n up to 4096, but no general proof).

$\rightsquigarrow \tilde{O}(n^2)$

The New Scheme in Practice

Relevant Complexities

Cramer & Fehr: α_i's may be chosen with coeffs in $\{0, 1\}$, but $f(X)$'s coeffs seem to be bound to bitlength n.

$\rightsquigarrow \tilde{O}(n^3)$

Cramer, Fehr & Stam: Evidence that α_i's may be chosen with coeffs in $\{0, 1\}$ and $f(X)$ with coeffs in $\{-1, 0, 1\}$ (Shown for n up to 4096, but no general proof).

$\rightsquigarrow \tilde{O}(n^2)$

Conclusion

- Constructing black box secret sharing schemes is intricately entwined with finding certain number fields (orders).
  - DF: Initially invertible Δ;
  - CF: Huge improvement using coprime Δ_α and Δ_β;
  - New: Further improvement using primitive Δ.
    Additive factor of at most 2 away from the best known lower bound.
- Proved existence of number fields with sufficiently large primitive sets. Efficiency is questionable.
- But experimental results indicate 'good' ones are around abundantly.
- Provided tight lower and upper bounds on the amount of random elements required.