Secret sharing protocols based on the Closest Vector Theorem and Nielsen transformation

Anja Moldenhauer and Gerhard Rosenberger

Anja Moldenhauer
anja.moldenhauer@uni-hamburg.de

University of Hamburg

Moscow 12 June 2014

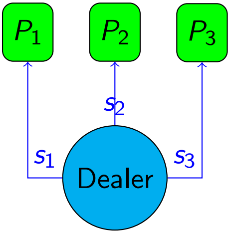
Topics

1. **Secret sharing using Clostest Vector Theorem**
    1. modification to a challenge and response system
2. Combinatorial (n,t) secret sharing
3. Secret sharing using Nielsen transformation
    1. with $SL(2, \mathbb{Q})$
    2. in general free group of rank m

(n,t) secret sharing protocol

n: Number of participants
t: Threshold

Example: (3,2) secret sharing



secret: S

An (n, t) **secret sharing protocol** (or (n, t) threshold scheme), with $n, t \in \mathbb{N}$ and $t \leq n$, is a method to distribute a secret among a group of n participants in such a way that it can be recovered only if at least t of them combine their shares.

First published
⇝ CFRZ Scheme

C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang.
A proposed alternative to the shamir secret sharing scheme.
Contemporary Mathematics, 582:47 – 50, 2012.

Theorem (Closest Vector Theorem)

Let W be a real inner product space and V a subspace of finite dimension t. Suppose that $w^* \in W$, with $w^* \notin V$, and $e_1, e_2, \ldots, e_t$ is an orthonormal basis of V. Then the unique vector $w \in V$ closest to w^* is given by

$$w = \langle w^*, e_1 \rangle e_1 + \langle w^*, e_2 \rangle e_2 + \ldots + \langle w^*, e_t \rangle e_t$$

where $\langle \cdot, \cdot \rangle$ is the inner product on W.

Idea behind the secret sharing scheme (CFRZ Scheme) I

First published

⇝ CFRZ Scheme

C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang.
A proposed alternative to the shamir secret sharing scheme.
Contemporary Mathematics, 582:47 – 50, 2012.

Theorem (Closest Vector Theorem)

Let W be a real inner product space and V a subspace of finite dimension t. Suppose that $w^* \in W$, with $w^* \notin V$, and $e_1, e_2, \ldots, e_t$ is an orthonormal basis of V. Then the unique vector $w \in V$ closest to w^* is given by

$$w = \langle w^*, e_1 \rangle e_1 + \langle w^*, e_2 \rangle e_2 + \ldots + \langle w^*, e_t \rangle e_t$$

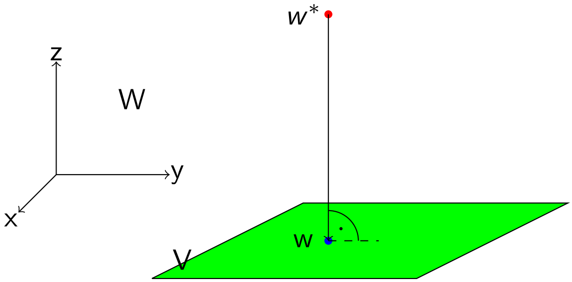
where $\langle \cdot, \cdot \rangle$ is the inner product on W.

Proof:

K. Atkinson.
An Introduction to Numerical Analysis.
Wiley, second edition, 1989.

$(5, 2)$ secret sharing

Real inner product space:
$W := \mathbb{R}^3$
Subspace V with $dim(V) = 2$
$\dim(W) > dim(V)$



Secret $w \in V$ is the closest vector to $w^* \in W \setminus V$.
Closest vector theorem:

$$\sum_{i=1}^{t} \langle w^*, e_i \rangle e_i = w$$

$t := dim(V)$ $\{e_1, e_2, \ldots, e_t\}$ orthonormal basis of V

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,
      $w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \in W \setminus V$,
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall$ $1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \quad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \left\{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\right\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \qquad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \left\{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\right\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{\left(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp\right)}_{:= v^\perp \in V^\perp} \qquad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall$ $1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \qquad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \qquad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W$, $dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \dots, v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \dots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \left\{b_1^\perp, b_2^\perp, \dots, b_{m-t}^\perp\right\}$ basis of $V^\perp$,
   $$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp} \qquad \in W \setminus V,$$
   $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant P_i $\forall\, 1 \leq i \leq n$,
   public w^*.

Number of participants : $n \in \mathbb{N}$
$V \subset W,\ dim(V) = t \in \mathbb{N}$

Dealer:

1. $m := dim(W),\ m \in \mathbb{N},\ m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.
4. Determine $M = \{v_1, v_2, \ldots, v_n\},\ v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.
5. Compute closest vector $w^* \in W \setminus V$ to $w \in V$:
   1. Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$ of V.
   2. $B^\perp = \left\{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\right\}$ basis of $V^\perp$,
      $$w^* = \underbrace{w}_{\in\ V} + \underbrace{\left(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp\right)}_{:=\ v^\perp\ \in\ V^\perp} \qquad \in W \setminus V,$$
      $\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$, with $1 \leq i \leq m - t$.
6. v_i distributed to participant $P_i\ \forall\ 1 \leq i \leq n$,
   public w^*.

t out of n participants:

1. Gram-Schmidt procedure: t vectors from $M \rightsquigarrow$ orthonormal basis $G = \{e_1, e_2, \ldots, e_t\}$ of V.
2. Reconstruct the secret w: public w^* and closest vector theorem:
   $w = \langle w^*, e_1\rangle e_1 + \langle w^*, e_2\rangle e_2 + \ldots + \langle w^*, e_t\rangle e_t$.

Complexity: $\mathcal{O}(t^2 m)$

$t = dim(V) \qquad V \subset W$

$m = dim(W)$

t out of n participants:

1. Gram-Schmidt procedure: t vectors from $M \rightsquigarrow$ orthonormal basis $G = \{e_1, e_2, \ldots, e_t\}$ of V.
2. Reconstruct the secret w: public w^* and closest vector theorem:
   $w = \langle w^*, e_1 \rangle e_1 + \langle w^*, e_2 \rangle e_2 + \ldots + \langle w^*, e_t \rangle e_t$.

Complexity: $\mathcal{O}(t^2 m)$

$t = dim(V) \qquad V \subset W$

$m = dim(W)$

t out of n participants:

1. Gram-Schmidt procedure: t vectors from $M \rightsquigarrow$ orthonormal basis $G = \{e_1, e_2, \ldots, e_t\}$ of V.
2. Reconstruct the secret w: public w^* and closest vector theorem:
   $w = \langle w^*, e_1\rangle e_1 + \langle w^*, e_2\rangle e_2 + \ldots + \langle w^*, e_t\rangle e_t$.

Complexity: $\mathcal{O}(t^2 m)$

$t = dim(V) \qquad V \subset W$

$m = dim(W)$

t out of n participants:

1. Gram-Schmidt procedure: t vectors from $M \rightsquigarrow$ orthonormal basis $G = \{e_1, e_2, \ldots, e_t\}$ of V.
2. Reconstruct the secret w: public w^* and closest vector theorem:
   $w = \langle w^*, e_1 \rangle e_1 + \langle w^*, e_2 \rangle e_2 + \ldots + \langle w^*, e_t \rangle e_t.$

Complexity: $\mathcal{O}(t^2 m)$

$t = dim(V) \qquad V \subset W$

$m = dim(W)$

Security

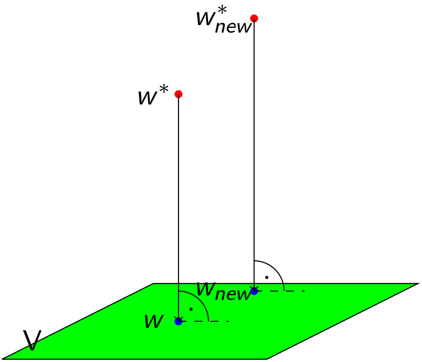
Less than t participants come together:

- Generate a subspace U with $dim(U) < t$.
- W: Infinitely many extensions with dimension t to a subspaces which contains the subspace U.
- The probability to determine V from U is negligible.
- Secret $w \in V$ cannot be reconstructed, because any point in W is a possible secret.

CFRZ (n,t) secret sharing

A valuable property: new secret property

It is easy to generate a new secret without changing the shares from the participants.



Topics

1. **Secret sharing using Clostest Vector Theorem**
    1. **modification to a challenge and response system**
2. Combinatorial (n,t) secret sharing
3. Secret sharing using Nielsen transformation
    1. with $SL(2, \mathbb{Q})$
    2. in general free group of rank m

modification to a challenge and response system I

Verifier **Prover**

$$\xrightarrow{\textit{Challenge}}$$

$$\xleftarrow{\textit{Response}}$$

- Private shared secret: (P, V),
  P standard password for prover,
  $V \subset W$ associated challenge space.
- Assumption: Challenge ("question") is difficult, i.e. infeasible to answer if V is unknown.
  Repeat a finite number of times,
  answers correct: prover (and the password) is verified.

modification to a challenge and response system I

Verifier **Prover**

$$\xrightarrow{\textit{Challenge}}$$

$$\xleftarrow{\textit{Response}}$$

- Private shared secret: (P, V),
  P standard password for prover,
  $V \subset W$ associated challenge space.
- Assumption: Challenge ("question") is difficult, i.e. infeasible to answer if V is unknown.
  Repeat a finite number of times,
  answers correct: prover (and the password) is verified.

modification to a challenge and response system I

$$
\begin{array}{ccc}
\textbf{Verifier} & & \textbf{Prover} \\
 & \xrightarrow{\textit{Challenge}} & \\
 & \xleftarrow{\textit{Response}} & \\
\end{array}
$$

- Private shared secret: (P, V),
  P standard password for prover,
  $V \subset W$ associated challenge space.
- Assumption: Challenge ("question") is difficult, i.e. infeasible to answer if V is unknown.
  Repeat a finite number of times,
  answers correct: prover (and the password) is verified.

Challenge:

`How long is the distance in the subspace` V `between the associated vectors` $v, w \in V$ `given the vectors` $v^*, w^* \in W \setminus V$`?`

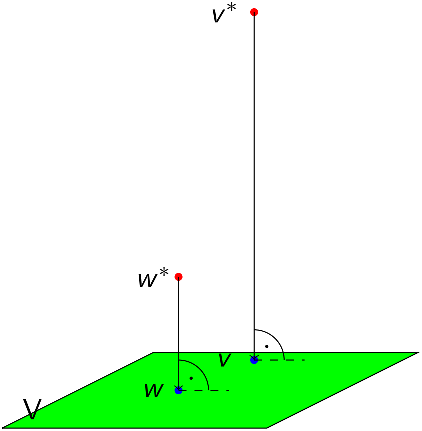
`Note:`

- $\|v^* - w^*\| \neq \|v - w\|$.

Two way authentication:

Prover: Distance in a special interval.

Verifier: Only if he knows V he can ask the right challenges.



Topics

1. Secret sharing using Clostest Vector Theorem
   1. modification to a challenge and response system
2. **Combinatorial (n,t) secret sharing**
3. Secret sharing using Nielsen transformation
   1. with $SL(2, \mathbb{Q})$
   2. in general free group of rank m

D. Panagopoulos:
A secret sharing scheme using groups.
arXiv:1009.0026v1, 2010.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}$$

$a_j \in \mathbb{N}$
$m := \binom{n}{t-1}$

Distribution of the shares (D. Panagopoulos):

1. (n,t) secret sharing scheme: $m = \binom{n}{t-1}$ number of elements we need to reconstruct the secret; $\{a_1, a_2, \ldots, a_m\}$, $a_j \in \mathbb{N}$.
2. $A_1, A_2, \ldots, A_m$ enumeration of the subsets of $\{1, 2, \ldots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \ldots, R_n$ of the set $\{a_1, a_2, \ldots, a_m\}$ with the property
$$a_j \in R_i \iff i \notin A_j$$
for $j = 1, 2, \ldots, m$ and $i = 1, 2, \ldots, n$.
3. The dealer distributes to each of the n participants one of the sets $R_1, R_2, \ldots, R_n$.

D. Panagopoulos:
A secret sharing scheme using groups.
arXiv:1009.0026v1, 2010.

Distribution of the shares (D. Panagopoulos):

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}$$

$a_j \in \mathbb{N}$
$m := \binom{n}{t-1}$

1. (n,t) secret sharing scheme: $m = \binom{n}{t-1}$ number of elements we need to reconstruct the secret; $\{a_1, a_2, \ldots, a_m\}$, $a_j \in \mathbb{N}$.
2. $A_1, A_2, \ldots, A_m$ enumeration of the subsets of $\{1, 2, \ldots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \ldots, R_n$ of the set $\{a_1, a_2, \ldots, a_m\}$ with the property

$$a_j \in R_i \quad \Longleftrightarrow \quad i \notin A_j$$

for $j = 1, 2, \ldots, m$ and $i = 1, 2, \ldots, n$.
3. The dealer distributes to each of the n participants one of the sets $R_1, R_2, \ldots, R_n$.

D. Panagopoulos:
A secret sharing scheme using groups.
arXiv:1009.0026v1, 2010.

Distribution of the shares (D. Panagopoulos):

1. (n, t) secret sharing scheme: $m = \binom{n}{t-1}$ number of elements we need to reconstruct the secret; $\{a_1, a_2, \ldots, a_m\}$, $a_j \in \mathbb{N}$.
2. $A_1, A_2, \ldots, A_m$ enumeration of the subsets of $\{1, 2, \ldots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \ldots, R_n$ of the set $\{a_1, a_2, \ldots, a_m\}$ with the property

$$a_j \in R_i \quad \Longleftrightarrow \quad i \notin A_j$$

for $j = 1, 2, \ldots, m$ and $i = 1, 2, \ldots, n$.
3. The dealer distributes to each of the n participants one of the sets $R_1, R_2, \ldots, R_n$.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}$$

$a_j \in \mathbb{N}$
$m := \binom{n}{t-1}$

D. Panagopoulos:
A secret sharing scheme using groups.
arXiv:1009.0026v1, 2010.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}$$

$a_j \in \mathbb{N}$
$m := \binom{n}{t-1}$

Distribution of the shares (D. Panagopoulos):

1. (n, t) secret sharing scheme: $m = \binom{n}{t-1}$ number of elements we need to reconstruct the secret; $\{a_1, a_2, \dots, a_m\}$, $a_j \in \mathbb{N}$.
2. $A_1, A_2, \dots, A_m$ enumeration of the subsets of $\{1, 2, \dots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \dots, R_n$ of the set $\{a_1, a_2, \dots, a_m\}$ with the property

$$a_j \in R_i \iff i \notin A_j$$

for $j = 1, 2, \dots, m$ and $i = 1, 2, \dots, n$.

3. The dealer distributes to each of the n participants one of the sets $R_1, R_2, \dots, R_n$.

D. Panagopoulos:
A secret sharing scheme using groups.
arXiv:1009.0026v1, 2010.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}$$

$a_j \in \mathbb{N}$
$m := \binom{n}{t-1}$

Distribution of the shares (D. Panagopoulos):

1. (n,t) secret sharing scheme: $m = \binom{n}{t-1}$ number of elements we need to reconstruct the secret; $\{a_1, a_2, \ldots, a_m\}$, $a_j \in \mathbb{N}$.
2. $A_1, A_2, \ldots, A_m$ enumeration of the subsets of $\{1, 2, \ldots, n\}$ with $t-1$ elements. Define n subsets $R_1, R_2, \ldots, R_n$ of the set $\{a_1, a_2, \ldots, a_m\}$ with the property

$$a_j \in R_i \quad \Longleftrightarrow \quad i \notin A_j$$

   for $j = 1, 2, \ldots, m$ and $i = 1, 2, \ldots, n$.
3. The dealer distributes to each of the n participants one of the sets $R_1, R_2, \ldots, R_n$.

Example (4,3) secret sharing

1. $m = \binom{n}{t-1} = \binom{4}{2} = 6 \rightsquigarrow \{a_1, a_2, \ldots, a_6\}$, $a_j \in \mathbb{N}$.
   $a_1 := 2, a_2 := 1, a_3 := 2, a_4 := 8, a_5 := 4, a_6 := 2.$
2. $m = 6$ subsets with size $t - 1 = 2$ of the set $\{1, 2, 3, 4\}$:

   $$A_1 = \{1,2\}, \quad A_2 = \{1,3\}, \quad A_3 = \{1,4\},$$
   $$A_4 = \{2,3\}, \quad A_5 = \{2,4\}, \quad A_6 = \{3,4\}.$$

   Get the sets R_1, R_2, R_3 and R_4:

   $$a_j \in R_i \iff i \notin A_j$$

   $$1 \notin A_4, A_5, A_6 \iff R_1 = \{a_4, a_5, a_6\} = \{a_4 = 8, a_5 = 4, a_6 = 2\},$$
   $$2 \notin A_2, A_3, A_6 \iff R_2 = \{a_2, a_3, a_6\} = \{a_2 = 1, a_3 = 2, a_6 = 2\},$$
   $$3 \notin A_1, A_3, A_5 \iff R_3 = \{a_1, a_3, a_5\} = \{a_1 = 2, a_3 = 2, a_5 = 4\},$$
   $$4 \notin A_1, A_2, A_4 \iff R_4 = \{a_1, a_2, a_4\} = \{a_1 = 2, a_2 = 1, a_4 = 8\}.$$
3. Each participant get one of the sets R_1, R_2, R_3, R_4.

Example (4,3) secret sharing

1. $m = \binom{n}{t-1} = \binom{4}{2} = 6 \rightsquigarrow \{a_1, a_2, \ldots, a_6\}$, $a_j \in \mathbb{N}$.
   $a_1 := 2, a_2 := 1, a_3 := 2, a_4 := 8, a_5 := 4, a_6 := 2.$
2. $m = 6$ subsets with size $t - 1 = 2$ of the set $\{1, 2, 3, 4\}$:

$$A_1 = \{1,2\}, \quad A_2 = \{1,3\}, \quad A_3 = \{1,4\},$$
$$A_4 = \{2,3\}, \quad A_5 = \{2,4\}, \quad A_6 = \{3,4\}.$$

Get the sets R_1, R_2, R_3 and R_4:

$$a_j \in R_i \iff i \notin A_j$$

$$1 \notin A_4, A_5, A_6 \iff R_1 = \{a_4, a_5, a_6\} = \{a_4 = 8, a_5 = 4, a_6 = 2\},$$
$$2 \notin A_2, A_3, A_6 \iff R_2 = \{a_2, a_3, a_6\} = \{a_2 = 1, a_3 = 2, a_6 = 2\},$$
$$3 \notin A_1, A_3, A_5 \iff R_3 = \{a_1, a_3, a_5\} = \{a_1 = 2, a_3 = 2, a_5 = 4\},$$
$$4 \notin A_1, A_2, A_4 \iff R_4 = \{a_1, a_2, a_4\} = \{a_1 = 2, a_2 = 1, a_4 = 8\}.$$

3. Each participant get one of the sets R_1, R_2, R_3, R_4.

Example (4,3) secret sharing

1. $m = \binom{n}{t-1} = \binom{4}{2} = 6 \rightsquigarrow \{a_1, a_2, \dots, a_6\},\ a_j \in \mathbb{N}$.
   $a_1 := 2, a_2 := 1, a_3 := 2, a_4 := 8, a_5 := 4, a_6 := 2.$
2. $m = 6$ subsets with size $t - 1 = 2$ of the set $\{1, 2, 3, 4\}$:

$$A_1 = \{1,2\}, \quad A_2 = \{1,3\}, \quad A_3 = \{1,4\},$$
$$A_4 = \{2,3\}, \quad A_5 = \{2,4\}, \quad A_6 = \{3,4\}.$$

   Get the sets R_1, R_2, R_3 and R_4:

$$a_j \in R_i \iff i \notin A_j$$

$$1 \notin A_4, A_5, A_6 \iff R_1 = \{a_4, a_5, a_6\} = \{a_4 = 8, a_5 = 4, a_6 = 2\},$$
$$2 \notin A_2, A_3, A_6 \iff R_2 = \{a_2, a_3, a_6\} = \{a_2 = 1, a_3 = 2, a_6 = 2\},$$
$$3 \notin A_1, A_3, A_5 \iff R_3 = \{a_1, a_3, a_5\} = \{a_1 = 2, a_3 = 2, a_5 = 4\},$$
$$4 \notin A_1, A_2, A_4 \iff R_4 = \{a_1, a_2, a_4\} = \{a_1 = 2, a_2 = 1, a_4 = 8\}.$$

3. Each participant get one of the sets R_1, R_2, R_3, R_4.

Security

- Each number a_j is exactly in $n-(t-1)$ sets from $R_1, \ldots, R_n$
  $\rightsquigarrow$ a_j is exactly in $t-1$ sets R_k not contained.
- t out of n: reconstruct the secret.
  Less then t: there exists j so that a_j is not contained in the union of the sets from the participants.
  Do not have all a_j: cannot reconstruct the secret

$$S := \sum_{j=1}^{m} \frac{1}{a_j} \in \mathbb{Q}.$$

Topics

1. Secret sharing using Clostest Vector Theorem
   1. modification to a challenge and response system
2. Combinatorial (n,t) secret sharing
3. **Secret sharing using Nielsen transformation**
   1. **with** $SL(2, \mathbb{Q})$
   2. in general free group of rank m

Secret sharing using Nielsen transformation I

F free group on $X := \{x_1, x_2, \ldots\}$: $F = \langle X | \;\; \rangle$
$U = \{u_1, u_2, \ldots\} \subset F$

Definition (elementary Nielsen transformation)

An *elementary Nielsen transformation* is one of the following transformations on the set $U \subset F$

(T1) replace some u_i by u_i^{-1};

(T2) replace some u_i by $u_i u_j$ where $j \neq i$;

(T3) delete some u_i where $u_i = 1$.

In all three cases the u_k for $i \neq k$ are not changed.

(Finite) product of elementary Nielsen transformations: **Nielsen transformation**.
Finite product of the transformation $(T1)$ and $(T2)$: **regular** Nielsen transformation otherwise **singular**.

Secret sharing using Nielsen transformation I

F free group on $X := \{x_1, x_2, \ldots\}$: $F = \langle X | \quad \rangle$
$U = \{u_1, u_2, \ldots\} \subset F$

Definition (elementary Nielsen transformation)

An *elementary Nielsen transformation* is one of the following transformations on the set $U \subset F$

(T1) replace some u_i by u_i^{-1};

(T2) replace some u_i by $u_i u_j$ where $j \neq i$;

(T3) delete some u_i where $u_i = 1$.

In all three cases the u_k for $i \neq k$ are not changed.

(Finite) product of elementary Nielsen transformations:
Nielsen transformation.
Finite product of the transformation $(T1)$ and $(T2)$:
regular Nielsen transformation otherwise **singular**.

Secret sharing using Nielsen transformation I

F free group on $X := \{x_1, x_2, \ldots\}$: $F = \langle X | \quad \rangle$
$U = \{u_1, u_2, \ldots\} \subset F$

Definition (elementary Nielsen transformation)

An *elementary Nielsen transformation* is one of the following transformations on the set $U \subset F$

(T1) replace some u_i by u_i^{-1};

(T2) replace some u_i by $u_i u_j$ where $j \neq i$;

(T3) delete some u_i where $u_i = 1$.

In all three cases the u_k for $i \neq k$ are not changed.

(Finite) product of elementary Nielsen transformations: **Nielsen transformation**.

Finite product of the transformation $(T1)$ and $(T2)$: **regular** Nielsen transformation otherwise **singular**.

Secret sharing using Nielsen transformation I

F free group on $X := \{x_1, x_2, \ldots\}$: $F = \langle X | \quad \rangle$
$U = \{u_1, u_2, \ldots\} \subset F$

Definition (elementary Nielsen transformation)

An *elementary Nielsen transformation* is one of the following transformations on the set $U \subset F$

(T1) replace some u_i by u_i^{-1};

(T2) replace some u_i by $u_i u_j$ where $j \neq i$;

(T3) delete some u_i where $u_i = 1$.

In all three cases the u_k for $i \neq k$ are not changed.

(Finite) product of elementary Nielsen transformations:
Nielsen transformation.
Finite product of the transformation $(T1)$ and $(T2)$:
regular Nielsen transformation otherwise **singular**.

Secret sharing using Nielsen transformation II

- Regular Nielsen transformation form a group.
- U is called **Nielsen-equivalent** (N-equivalent) to V, if there is a regular Nielsen transformation from U to V.
- Get V from U by Nielsen transformation, it is $\langle U \rangle = \langle V \rangle$.

Secret sharing using Nielsen transformation II

- Regular Nielsen transformation form a group.
- U is called **Nielsen-equivalent** (N-equivalent) to V, if there is a regular Nielsen transformation from U to V.
- Get V from U by Nielsen transformation, it is $\langle U \rangle = \langle V \rangle$.

Secret sharing using Nielsen transformation II

- Regular Nielsen transformation form a group.
- U is called **Nielsen-equivalent** (N-equivalent) to V, if there is a regular Nielsen transformation from U to V.
- Get V from U by Nielsen transformation, it is $\langle U \rangle = \langle V \rangle$.

Secret sharing using Nielsen transformation III

$$SL(2,\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Q} \text{ and } ad - bc = 1 \right\}$$

(n,t) secret sharing;
free group $F \subset SL(2,\mathbb{Q})$ with m generators;
$m := \binom{n}{t-1} \rightsquigarrow$ D. Panagopoulos method for share distribution.

1. Abstract presentation $F = \langle X \mid \ \rangle$, with $X := \{x_1, x_2, \ldots, x_m\}$.
2. Explicit presentation $F = \langle M \mid \ \rangle$, with $M := \{M_1, M_2, \ldots, M_m\}$ and $M_i \in SL(2,\mathbb{Q})$.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \qquad \text{with } tr(M_j) = a_j \in \mathbb{Q};$$

$tr(M_i) := a + d$ for $M_i := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Secret sharing using Nielsen transformation III

$$SL(2,\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a,b,c,d \in \mathbb{Q} \text{ and } ad - bc = 1 \right\}$$

(n,t) secret sharing;
free group $F \subset SL(2,\mathbb{Q})$ with m generators;
$m := \binom{n}{t-1} \rightsquigarrow$ D. Panagopoulos method for share distribution.

1. Abstract presentation $F = \langle X| \quad \rangle$, with $X := \{x_1, x_2, \ldots, x_m\}$.
2. Explicit presentation $F = \langle M| \quad \rangle$, with $M := \{M_1, M_2, \ldots, M_m\}$ and $M_i \in SL(2,\mathbb{Q})$.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \qquad \text{with } tr(M_j) = a_j \in \mathbb{Q};$$

$tr(M_i) := a + d$ for $M_i := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Secret sharing using Nielsen transformation III

$$SL(2,\mathbb{Q}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Q} \text{ and } ad - bc = 1 \right\}$$

(n,t) secret sharing;
free group $F \subset SL(2,\mathbb{Q})$ with m generators;
$m := \binom{n}{t-1} \rightsquigarrow$ D. Panagopoulos method for share distribution.

1. Abstract presentation $F = \langle X | \quad \rangle$, with $X := \{x_1, x_2, \ldots, x_m\}$.
2. Explicit presentation $F = \langle M | \quad \rangle$, with $M := \{M_1, M_2, \ldots, M_m\}$ and $M_i \in SL(2,\mathbb{Q})$.

Secret:

$$S := \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \qquad \text{with } tr(M_j) = a_j \in \mathbb{Q};$$

$tr(M_i) := a + d$ for $M_i := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Secret sharing using Nielsen transformation IV

Dealer:

- $X := \{x_1, x_2, \ldots, x_m\}$ abstract generating set.
- $M := \{M_1, M_2, \ldots, M_m\}$, $M_i \in SL(2, \mathbb{Q})$ explicit generating set.

Simultaneous regular Nielsen transformation (forward extension)

$X := \{x_1, x_2, \ldots, x_m\}$ $\xrightarrow{\text{regular Nielsen transformation}}$ $U := \{u_1, u_2, \ldots, u_m\}$

u_i words in elements from X

$|u_i| > |x_i|$

$| \bullet |$ free length of a word

$M := \{M_1, M_2, \ldots, M_m\}$ $\xrightarrow{\text{regular Nielsen transformation}}$ $N := \{N_1, N_2, \ldots, N_m\}$

N_i words in the elements from M, i.e. $N_i \in SL(2, \mathbb{Q})$

Secret sharing using Nielsen transformation IV

Dealer:

- $X := \{x_1, x_2, \ldots, x_m\}$ abstract generating set.
- $M := \{M_1, M_2, \ldots, M_m\}$, $M_i \in SL(2, \mathbb{Q})$ explicit generating set.

<u>Simultaneous regular Nielsen transformation (forward extension)</u>

$$X := \{x_1, x_2, \ldots, x_m\} \qquad\qquad M := \{M_1, M_2, \ldots, M_m\}$$

$$\Big\downarrow \text{regular Nielsen transformation} \qquad\qquad \Big\downarrow \text{regular Nielsen transformation}$$

$U := \{u_1, u_2, \ldots, u_m\}$
u_i words in elements from X
$|u_i| > |x_i|$
$|\bullet|$ free length of a word

$N := \{N_1, N_2, \ldots, N_m\}$
N_i words in the elements from M,
i.e. $N_i \in SL(2, \mathbb{Q})$

Do with both sets U and N D. Panagopoulos method to distribute shares (R_i, S_i) to the participant P_i.
$R_i \subset U$ and $S_i \subset N$;
t out of n **participants** get the sets U and N.

Simultaneous regular Nielsen transformation (backwards extension)

$$\begin{array}{ccc} U := \{u_1, u_2, \dots, u_m\} & \qquad & N := \{N_1, N_2, \dots, N_m\} \\ \Big\downarrow{\scriptstyle \text{regular Nielsen transformation}} & & \Big\downarrow{\scriptstyle \text{regular Nielsen transformation}} \\ X := \{x_1, x_2, \dots, x_m\} & & M := \{M_1, M_2, \dots, M_m\} \end{array}$$

Security

Remember D. Panagopoulos method: less then t participants cannot reconstruct the set U (Nielsen-equivalent to X) nor the set N (Nielsen-equivalent to M).

Need the complete set N and U to do the right Nielsen transformation to get the right set M.
Secret reconstruction only with the set M.

- Know only U or subsets of it (Nielsen-equivalent to X) cannot get M.
- Know only N or subsets of it (Nielsen-equivalent to M) cannot get M.

Secret sharing using Nielsen transformation VI

Security

Remember D. Panagopoulos method: less then t participants cannot reconstruct the set U (Nielsen-equivalent to X) nor the set N (Nielsen-equivalent to M).

Need the complete set N and U to do the right Nielsen transformation to get the right set M.
Secret reconstruction only with the set M.

- Know only U or subsets of it (Nielsen-equivalent to X) cannot get M.
- Know only N or subsets of it (Nielsen-equivalent to M) cannot get M.

Security

Remember D. Panagopoulos method: less then t participants cannot reconstruct the set U (Nielsen-equivalent to X) nor the set N (Nielsen-equivalent to M).

Need the complete set N and U to do the right Nielsen transformation to get the right set M.
Secret reconstruction only with the set M.

- Know only U or subsets of it (Nielsen-equivalent to X) cannot get M.
- Know only N or subsets of it (Nielsen-equivalent to M) cannot get M.

Secret sharing using Nielsen transformation VII

J. Lehner:
Discontinuous Groups and Automorphic Function.
American Mathematical Society, Mathematical Surveys Number VIII, 1964.

Example (In general)

Free group F with countable number of generators $x_1, x_2, \ldots$.
Corresponding to x_j define

$$M_j = \begin{pmatrix} -r_j & -1 + r_j^2 \\ 1 & -r_j \end{pmatrix}$$

with $r_j \in \mathbb{Q}$ and

$$\begin{aligned} r_{j+1} - r_j &\geq 3 \\ r_1 &\geq 2. \end{aligned}$$

Lehner: G* generated by $\{M_1, M_2, \ldots\}$ is isomorphic to F.

$(4,2)$ secret sharing example

$n = 4, t = 2,\ m := \binom{4}{1} = 4.$

- $X := \{x_1, x_2, x_3, x_4\}$ abstract generating set.
- $M := \{M_1, M_2, M_3, M_4\},\ M_i \in SL(2,\mathbb{Q})$ explicit generating set.

$$M_1 = \begin{pmatrix} -2 & -1+2^2 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix},$$

$$M_2 = \begin{pmatrix} -\frac{11}{2} & -1+\left(\frac{11}{2}\right)^2 \\ 1 & -\frac{11}{2} \end{pmatrix} = \begin{pmatrix} -\frac{11}{2} & \frac{117}{4} \\ 1 & -\frac{11}{2} \end{pmatrix},$$

$$M_3 = \begin{pmatrix} -10 & -1+10^2 \\ 1 & -10 \end{pmatrix} = \begin{pmatrix} -10 & 99 \\ 1 & -10 \end{pmatrix},$$

$$M_4 = \begin{pmatrix} -\frac{27}{2} & -1+\left(\frac{27}{2}\right)^2 \\ 1 & -\frac{27}{2} \end{pmatrix} = \begin{pmatrix} -\frac{27}{2} & \frac{725}{4} \\ 1 & -\frac{27}{2} \end{pmatrix}.$$

$(4,2)$ secret sharing example

$n=4, t=2,\ m:=\binom{4}{1}=4.$

- $X := \{x_1, x_2, x_3, x_4\}$ abstract generating set.
- $M := \{M_1, M_2, M_3, M_4\},\ M_i \in SL(2,\mathbb{Q})$ explicit generating set.

$$M_1 = \begin{pmatrix} -2 & -1+2^2 \\ 1 & -2 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix},$$
$$M_2 = \begin{pmatrix} -\frac{11}{2} & -1+\left(\frac{11}{2}\right)^2 \\ 1 & -\frac{11}{2} \end{pmatrix} = \begin{pmatrix} -\frac{11}{2} & \frac{117}{4} \\ 1 & -\frac{11}{2} \end{pmatrix},$$
$$M_3 = \begin{pmatrix} -10 & -1+10^2 \\ 1 & -10 \end{pmatrix} = \begin{pmatrix} -10 & 99 \\ 1 & -10 \end{pmatrix},$$
$$M_4 = \begin{pmatrix} -\frac{27}{2} & -1+\left(\frac{27}{2}\right)^2 \\ 1 & -\frac{27}{2} \end{pmatrix} = \begin{pmatrix} -\frac{27}{2} & \frac{725}{4} \\ 1 & -\frac{27}{2} \end{pmatrix}.$$

Secret sharing using Nielsen transformation IX

Dealer: Simultaneous regular Nielsen transformation **NT**

$$M_1 = \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix}, M_2 = \begin{pmatrix} -\frac{11}{2} & \frac{117}{4} \\ 1 & -\frac{11}{2} \end{pmatrix}, M_3 = \begin{pmatrix} -10 & 99 \\ 1 & -10 \end{pmatrix}, M_4 = \begin{pmatrix} -\frac{27}{2} & \frac{725}{4} \\ 1 & -\frac{27}{2} \end{pmatrix}.$$

NT	theoretical set	explicit set
	$X := \{x_1, x_2, x_3, x_4\}$	$M := \left\{M_1, M_2, M_3, M_4\right\}$
$(T2)_{12}$ $[(T2)_{34}]^2$	$\{x_1x_2, x_2, x_3x_4^2, x_4\}$	$\left\{\begin{pmatrix} 14 & -75 \\ -\frac{15}{2} & \frac{161}{4} \end{pmatrix}, \begin{pmatrix} -\frac{11}{2} & \frac{117}{4} \\ 1 & -\frac{11}{2} \end{pmatrix}, \begin{pmatrix} -6308 & 84924 \\ \frac{1267}{2} & -\frac{34115}{4} \end{pmatrix}, \begin{pmatrix} -\frac{27}{2} & \frac{725}{4} \\ 1 & -\frac{27}{2} \end{pmatrix}\right\}$

Secret sharing using Nielsen transformation X

NT	theoretical set	explicit set
$(T2)_{21}$ $(T1)_3$ $(T2)_{41}$	$\{x_1x_2, x_2x_1x_2,$ $(x_3x_4^2)^{-1}, x_4x_1x_2\}$	$\left\{\begin{pmatrix} 14 & -75 \\ -\frac{15}{2} & \frac{161}{4} \end{pmatrix}, \begin{pmatrix} -\frac{2371}{8} & \frac{25437}{16} \\ \frac{221}{4} & -\frac{2371}{8} \end{pmatrix}, \begin{pmatrix} -\frac{34115}{4} & -84924 \\ -\frac{1267}{2} & -6308 \end{pmatrix}, \begin{pmatrix} -\frac{12387}{8} & \frac{132925}{16} \\ \frac{461}{4} & -\frac{4947}{8} \end{pmatrix}\right\}$
$\vdots$	$\vdots$	$\vdots$
	$U := \{u_1, u_2, u_3, u_4\}$	$N := \{N_1, N_2, N_3, N_4\}$

Secret sharing using Nielsen transformation XI

$U := \{u_1, u_2, u_3, u_4\}$

$$u_1 := x_1x_2(x_4x_1x_2)^3(x_3x_4^2x_2^{-1}x_1^{-1}x_2^{-1})^4x_4x_1x_2,$$
$$u_2 := x_2x_1x_2x_4^{-2}x_3^{-1}((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2,$$
$$u_3 := ((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2,$$
$$u_4 := x_2^{-1}x_1^{-1}x_4^{-1}(x_2x_1x_2x_4^{-2}x_3^{-1})^4.$$

Secret sharing using Nielsen transformation XII

$$N := \{N_1, N_2, N_3, N_4\}$$

$$N_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \qquad N_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}$$

$$a_1 := \frac{66542596427956187828582196681199917757627687 3}{524288}$$

$$b_1 := -\frac{71406865988266064345528737870923869027489120 43}{1048576}$$

$$c_1 := -\frac{28532708651831142965000137233592385544633522 69}{4194304}$$

$$d_1 := \frac{30618452124714071336436267510627140548281900727}{8388608}$$

$$a_2 := -\frac{12002314405411966962824287810472414299348307892296643001383731643730423222506377956021 33}{562949953421312}$$

$$b_2 := \frac{32317202130608840477510994802545162192543628980433478881354803514076560407470703930775509}{1125899906842624}$$

$$c_2 := \frac{11187226832013179812847560952981376596114097200751794882248309367200402647134852065393 1}{281474976710656}$$

$$d_2 := -\frac{30122512925350353976147567673240417166963274180184868740775926809112030584430539243467 31}{562949953421312}$$

Secret sharing using Nielsen transformation XIII

$$N_3 = \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \qquad N_4 = \begin{pmatrix} a_4 & b_4 \\ c_4 & d_4 \end{pmatrix}$$

$$a_3 := -\frac{17274718784827820759613292350041627442169501421072947928184581776518095089429309}{35184372088832}$$

$$b_3 := \frac{465135772869752741329431664014905210283617966614809684008911971064867155893869629}{70368744177664}$$

$$c_3 := -\frac{1609794077912542401777325081836598849358539831783165811585876116215648997682179}{17592186044416}$$

$$d_3 := \frac{43345007343832398092074993797699781408476274086506590850498428957455449152060163}{35184372088832},$$

$$a_4 := -\frac{102303031641708426816114320037645}{32768}$$

$$b_4 := -\frac{254667523147409477390369802167441}{8192}$$

$$c_4 := -\frac{9533410063129335801682019025887}{16384}$$

$$d_4 := -\frac{23731945074987538082296716533451}{4096}$$

Secret sharing using Nielsen transformation XIV

D. Panagopoulos: Get the share (R_i, S_i) for the participant P_i with $R_i \subset U$ and $S_i \subset N$ as follow:

1. It is $m = \binom{n}{t-1} = \binom{4}{1} = 4$.
2. The dealer has the elements a_1, a_2, a_3, a_4.
   - The four subsets with size 1 of the set $\{1, 2, 3, 4\}$ are
     $$A_1 = \{1\}\,, \quad A_2 = \{2\}\,, \quad A_3 = \{3\}\,, \quad A_4 = \{4\}\,.$$
     Get the sets R_1, R_2, R_3 and R_4:
     $$a_j \in R_i \quad \Longleftrightarrow \quad i \notin A_j$$
     $$1 \notin A_2, A_3, A_4 \Longleftrightarrow R_1 = \{a_2, a_3, a_4\}\,,\ 2 \notin A_1, A_3, A_4 \Longleftrightarrow R_2 = \{a_1, a_3, a_4\}\,,$$
     $$3 \notin A_1, A_2, A_4 \Longleftrightarrow R_3 = \{a_1, a_2, a_4\}\,,\ 4 \notin A_1, A_2, A_3 \Longleftrightarrow R_4 = \{a_1, a_2, a_3\}\,.$$
   - In this example he gets the sets
     $$\begin{aligned} R_1 &= \{u_2, u_3, u_4\}\,, & S_1 &= \{N_2, N_3, N_4\}\,, \\ R_2 &= \{u_1, u_3, u_4\}\,, & S_2 &= \{N_1, N_3, N_4\}\,, \\ R_3 &= \{u_1, u_2, u_4\}\,, & S_3 &= \{N_1, N_2, N_4\}\,, \\ R_4 &= \{u_1, u_2, u_3\}\,, & S_4 &= \{N_1, N_2, N_3\}\,. \end{aligned}$$

Secret sharing using Nielsen transformation XV

t Participants : Simultaneous regular Nielsen transformation **NT**

$$u_1 := x_1x_2(x_4x_1x_2)^3(x_3x_4^2x_2^{-1}x_1^{-1}x_2^{-1})^4x_4x_1x_2,$$
$$u_2 := x_2x_1x_2x_4^{-2}x_3^{-1}((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2,$$
$$u_3 := ((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2,$$
$$u_4 := x_2^{-1}x_1^{-1}x_4^{-1}(x_2x_1x_2x_4^{-2}x_3^{-1})^4.$$

NT	theoretical set	explicit set
	$U := \{u_1, u_2, u_3, u_4\}$	$N := \{N_1, N_2, N_3, N_4\}$
$(T1)_3$	$\{x_1x_2(x_4x_1x_2)^3(x_3x_4^2x_2^{-1}x_1^{-1}x_2^{-1})^4x_4x_1x_2,$ $x_2x_1x_2x_4^{-2}x_3^{-1}((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2,$ $(((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2)^{-1},$ $x_2^{-1}x_1^{-1}x_4^{-1}(x_2x_1x_2x_4^{-2}x_3^{-1})^4\}$	$\{N_1, N_2, N_3^{-1}, N_4\}$

Secret sharing using Nielsen transformation XVI

t Participants : Simultaneous regular Nielsen transformation **NT**

NT	theoretical set	explicit set
$(T2)_{14}$ $(T2)_{23}$	$\{x_1x_2(x_4x_1x_2)^3,$ $x_2x_1x_2x_4^{-2}x_3^{-1},$ $(((x_2^{-1}x_1^{-1}x_4^{-1})^3x_2^{-1}x_1^{-1})^5x_4x_1x_2x_3x_4^2)^{-1},$ $x_2^{-1}x_1^{-1}x_4^{-1}(x_2x_1x_2x_4^{-2}x_3^{-1})^4\}$	$\{N_1N_4, N_2N_3^{-1}, N_3^{-1}, N_4\}$
$\vdots$	$\vdots$	$\vdots$
	$X = \{x_1, x_2, x_3, x_4\}$	$M = \{M_1, M_2, M_3, M_4\}$

$$M = \left\{ \begin{pmatrix} -2 & 3 \\ 1 & -2 \end{pmatrix}, \begin{pmatrix} -\frac{11}{2} & \frac{117}{4} \\ 1 & -\frac{11}{2} \end{pmatrix}, \begin{pmatrix} -10 & 99 \\ 1 & -10 \end{pmatrix}, \begin{pmatrix} -\frac{27}{2} & \frac{725}{4} \\ 1 & -\frac{27}{2} \end{pmatrix} \right\},$$

Secret:

$$\begin{aligned} S &:= \sum_{j=1}^{m} \frac{1}{|a_j|} \in \mathbb{Q}^+ \qquad \text{with } tr(M_j) = a_j \in \mathbb{Q} \\ &= \frac{1}{|-4|} + \frac{1}{|-11|} + \frac{1}{|-20|} + \frac{1}{|-27|} \\ &= \frac{1271}{2970} \end{aligned}$$

Topics

1. Secret sharing using Clostest Vector Theorem
   1. modification to a challenge and response system
2. Combinatorial (n,t) secret sharing
3. **Secret sharing using Nielsen transformation**
   1. with $SL(2, \mathbb{Q})$
   2. **in general free group of rank** m

In general: Free matrix group F of rank m

Simultaneous regular Nielsen transformation

abstract:

$$X := \{x_1, x_2, \dots, x_m\} \xrightarrow{\text{regular Nielsen transformation}} U := \{u_1, u_2, \dots, u_m\}$$

u_i words in elements from X

explicit with matrices:

$$M := \{M_1, M_2, \dots, M_m\} \xrightarrow{\text{regular Nielsen transformation}} N := \{N_1, N_2, \dots, N_m\}$$

N_i words in elements from M, i.e. $N_i \in SL(2, \mathbb{C})$

Shares for the participants:
(R_i, S_i) with $R_i \subset U$ and $S_i \subset N$.

Secret:

$$S := tr\left(\prod_{i=1}^{m} M_i\right) \text{ or } S := tr\left(\sum_{i=1}^{m} M_i\right) \text{ or}$$
$$S := tr\left(\prod_{i=1}^{m} M_i^2\right) \text{ or } S := tr\left(\sum_{i=1}^{m} M_i^2\right) \text{ or}$$
$$S := tr([M_1, M_2]) \cdot \ldots \cdot tr([M_{m-1}, M_m]) \text{ if } m \text{ is even or}$$
$$S := tr([M_1, M_2]) + \ldots + tr([M_{m-1}, M_m]) \text{ if } m \text{ is even.}$$

Shares for the participants:
(R_i, S_i) with $R_i \subset U$ and $S_i \subset N$.

Secret:

$$S := tr\left(\prod_{i=1}^{m} M_i\right) \text{ or } S := tr\left(\sum_{i=1}^{m} M_i\right) \text{ or}$$

$$S := tr\left(\prod_{i=1}^{m} M_i^2\right) \text{ or } S := tr\left(\sum_{i=1}^{m} M_i^2\right) \text{ or}$$

$$S := tr([M_1, M_2]) \cdot \ldots \cdot tr([M_{m-1}, M_m]) \text{ if } m \text{ is even or}$$

$$S := tr([M_1, M_2]) + \ldots + tr([M_{m-1}, M_m]) \text{ if } m \text{ is even.}$$

$PSL(2,\mathbb{K}) = SL(2,\mathbb{K})/\{\pm I\}$, $\mathbb{K}$ large finite field, I Identity Matrix

Remark

Elements in $PSL(2,\mathbb{K})$ are pairs of the Form $\{A, -A\}$.

(1) $(tr(A))^2 = tr(A^2) + 2$

(2) $tr([A,B]) := tr\left(ABA^{-1}B^{-1}\right)$

are unique.

Do secret sharing from above with free groups of rank m in $PSL(2,\mathbb{K})$ with $\mathbb{K}$ a large finite field.

Secret:

$$S := \prod_{j=1}^{m} tr(M_j^2) \;\text{ or }\; S := \sum_{j=1}^{m} tr(M_j^2) \;\text{ or}$$

$$S := tr([M_1, M_2]) \cdot \ldots \cdot tr([M_{m-1}, M_m]) \text{ if } m \text{ is even or}$$

$$S := tr([M_1, M_2]) + \ldots + tr([M_{m-1}, M_m]) \text{ if } m \text{ is even.}$$

$PSL(2,\mathbb{K}) = SL(2,\mathbb{K})/\{\pm I\}$, $\mathbb{K}$ large finite field, I Identity Matrix

Remark

Elements in $PSL(2,\mathbb{K})$ are pairs of the Form $\{A,-A\}$.

(1) $(tr(A))^2 = tr(A^2) + 2$

(2) $tr([A,B]) := tr\left(ABA^{-1}B^{-1}\right)$

are unique.

Do secret sharing from above with free groups of rank m in $PSL(2,\mathbb{K})$ with $\mathbb{K}$ a large finite field.

Secret:

$$S := \prod_{j=1}^{m} tr(M_j^2) \text{ or } S := \sum_{j=1}^{m} tr(M_j^2) \text{ or}$$

$$S := tr([M_1, M_2]) \cdot \ldots \cdot tr([M_{m-1}, M_m]) \text{ if } m \text{ is even or}$$

$$S := tr([M_1, M_2]) + \ldots + tr([M_{m-1}, M_m]) \text{ if } m \text{ is even.}$$

$PSL(2,\mathbb{K}) = SL(2,\mathbb{K})/\{\pm I\}$, $\mathbb{K}$ large finite field, I Identity Matrix

Remark

Elements in $PSL(2,\mathbb{K})$ are pairs of the Form $\{A, -A\}$.

(1) $(tr(A))^2 = tr(A^2) + 2$

(2) $tr([A,B]) := tr\left(ABA^{-1}B^{-1}\right)$

are unique.

Do secret sharing from above with free groups of rank m in $PSL(2,\mathbb{K})$ with $\mathbb{K}$ a large finite field.

Secret:

$$S := \prod_{j=1}^{m} tr(M_j^2) \quad \text{or} \quad S := \sum_{j=1}^{m} tr(M_j^2) \quad \text{or}$$

$$S := tr([M_1, M_2]) \cdot \ldots \cdot tr([M_{m-1}, M_m]) \text{ if } m \text{ is even} \quad \text{or}$$

$$S := tr([M_1, M_2]) + \ldots + tr([M_{m-1}, M_m]) \text{ if } m \text{ is even.}$$

Appendix

Thank you!

1. Secret sharing using Clostest Vector Theorem
2. Nielsen transformation

Appendix Nielsen transformation

1. Collaboration-Protocol
2. Special secret

Appendix

(n, t) Collaboration-Protocol

$m = \binom{n}{t-1}$, free group F of rank m

Team 1:
n participants P_i

Team 2:
n participants $\tilde{P}_i$

theoretical set
$X := \{x_1, x_2, \ldots, x_m\}$

$$\Big\downarrow \text{regular Nielsen transformation}$$

$U := \{u_1, u_2, \ldots, u_m\}$

explicit set
$M := \{M_1, M_2, \ldots, M_m\}$

$$\Big\downarrow \text{regular Nielsen transformation}$$

$N := \{N_1, N_2, \ldots, N_m\}$

D. Panagopoulos: share distribution

set $R_i \subset U$

P_i gets R_i, $1 \leq i \leq n$

set $S_i \subset N$

$\tilde{P}_i$ gets N_i, $1 \leq i \leq n$

t shares and t shares $\rightsquigarrow$ secret

- only red/green participants (dose not matter how many) cannot reconstruct the secret
- need collaboration of both teams $\rightsquigarrow$ t green and t red shares.

Appendix NIelsen transformation

If the Dealer needs a special secret $\tilde{S} \in \mathbb{Q}$ he can give every participant one more element $x \in \mathbb{Q}$ in every R_i. It is

$$x := \frac{\tilde{S}}{S}.$$

If the participants multiply the secret S with x they get the special secret $\tilde{S}$.

◂ Appendix Nielsen transformation

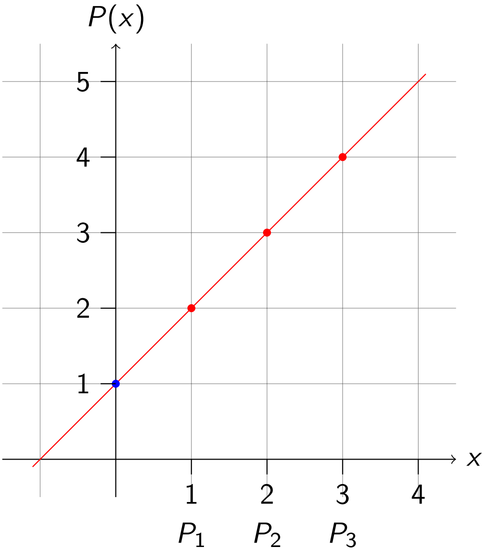
Appendix CFRZ

1. Shamir's (n,t) secret sharing $\leftrightarrow$ CFRZ (n,t) secret sharing
2. Modification to a private key cryptosystem
3. About the set M
4. Example for an $(5,2)$ CFRZ secret sharing

B. Fine, A. I. S. Moldenhauer, G. Rosenberger
A secret sharing scheme based on the Closest Vector Theorem and a modification to a private key cryptosystem.
Groups Complex. Cryptol. **5** (2013), 223-238.

Appendix

Example: Shamir's $(3, 2)$ secret sharing

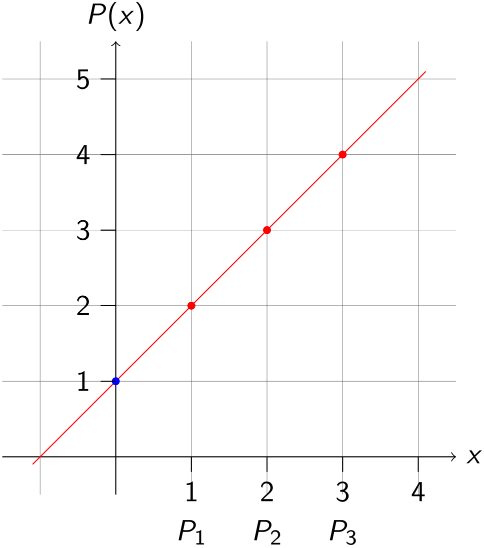


Theorem

Let F be any field and $x_0, x_1, \ldots, x_n$ be $n+1$ distinct elements of F and $y_0, y_1, \ldots, y_n$ any element of F. Then there exists a **unique** *polynomial of degree smaller or equal than n that interpolates the $n+1$ points $(x_i, y_i), i = 0, 1, \ldots, n$.*

K. Atkinson.
An Introduction to Numerical Analysis.
Wiley, second edition, 1989.

Example: Shamir's $(3, 2)$ secret sharing



Field: $F = \mathbb{R}$

Dealer: $P(x) = x + 1$

Shares: P_1: $\mathrm{P}(1) = 2$

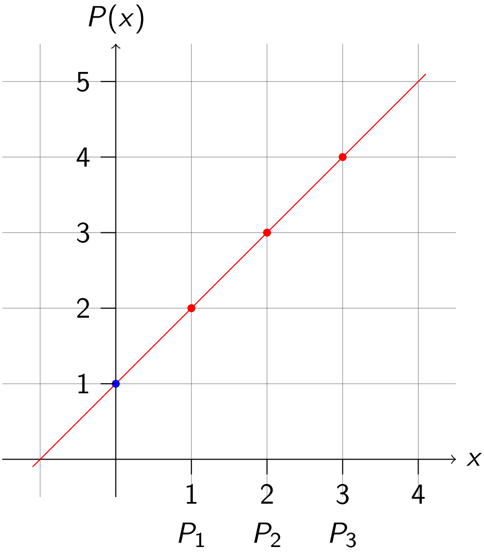
P_2: $\mathrm{P}(2) = 3$

P_3: $\mathrm{P}(3) = 4$

Secret: $\mathrm{P}(0) = 1$

Shamir's (n,t) secret sharing ↔ CFRZ (n,t) secret sharing

Example: Shamir's $(3, 2)$ secret sharing



t out of n participants:
Polynomial interpolation e. g.
Lagrange interpolation

$$S = P(0) = \sum_{i=0}^{t-1} y_i \prod_{j=0, j \neq i}^{t-1} \frac{x_j}{x_j - x_i}.$$

Shamir's (n,t) secret sharing $\leftrightarrow$ CFRZ (n,t) secret sharing

Shamir suggested using a finite field $\mathbb{Z}/_{p\mathbb{Z}}$, p a large prime.
He lists the following properties:

A. Shamir
How to share a secret.
Communications of the AMS, 22(11):612-613, 1979.

- Size of each share does not exceed the size of the secret.

CFRZ

Secret: Vector $w \in V \subset W$
Shares: Basis vector of $V \subset W$

$\rightsquigarrow$ CFRZ $\surd$

Shamir's (n,t) secret sharing $\leftrightarrow$ CFRZ (n,t) secret sharing

- Fixed number t: shares can be dynamically added or deleted without affecting the other shares.

CFRZ

Pay attention, that every possible combination of t shares form a basis for the subspace V.

$\rightsquigarrow$ CFRZ $\surd$

- Easy to change shares without changing the secret.

CFRZ

Need only another subspace $U \neq V$, with $w \in U$ and $dim(U) = t$.
Calculate new shares, with the desired property: every t of them form a basis for U.
Construct a new public vector w^* as above.

$\rightsquigarrow$ CFRZ $\surd$

- Asymmetric system is possible.

CFRZ

Generally: Every (n, t) secret sharing scheme can be converted into an asymmetric secret sharing protocol.
• (n, t) secret sharing scheme: Every share is equivalent.
• Asymmetric secret sharing protocol: Every participant gets a different number of shares.
• Depending: Importance of the participant.

Example (modify (8,4) secret sharing into an asymmetric)

$D_1 := (v_1, v_2)$,
$D_2 := (v_3, v_4)$,
$V_1 := (v_5)$, $V_2 := (v_6)$,
$V_3 := (v_7)$ and $V_4 := (v_8)$.

Reconstruct the secret if:
• two presidents (D_i) or
• four vice-presidents (V_i) or
• one president and two vice-presidents.

$\rightsquigarrow$ CFRZ $\surd$

Shamir's (n,t) secret sharing $\leftrightarrow$ CFRZ (n,t) secret sharing

Note: CFRZ scheme has all properties Shamir's has.

Running time for the participants:
Shamir: $\mathcal{O}(t^2)$
CFRZ: $\mathcal{O}(t^2 m)$ with $m := dim(W)$ and $m > t$

Probability to guess the right secret:
Shamir: $\frac{1}{p}$ with p a prime
CFRZ: negligible

Another valuable property: new secret property

It is easy to generate a new secret without changing the shares from the participants.

Another valuable property: new secret property

It is easy to generate a new secret without changing the shares from the participants.

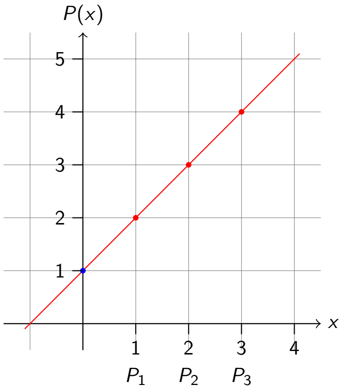
False for Shamir.

True for CFRZ.

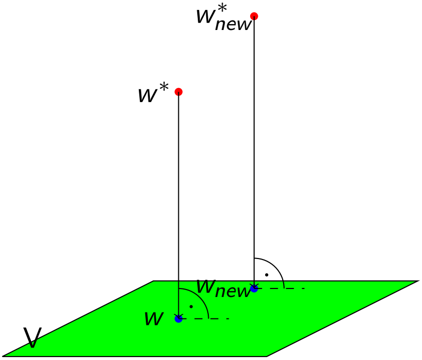
Appendix CRFZ

Another valuable property: new secret property

It is easy to generate a new secret without changing the shares from the participants.



False for Shamir.

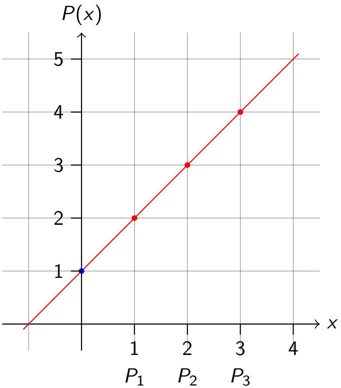


True for CFRZ.

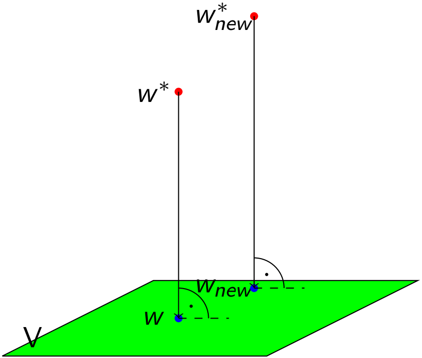
Appendix CRFZ

Another valuable property: new secret property

It is easy to generate a new secret without changing the shares from the participants.



False for Shamir.



True for CFRZ.

Appendix CRFZ

private key cryptosystem based on CFRZ Scheme

$dim(V) = t$
$dim(W) = m$

$\boxed{\texttt{Private key: } \text{Basis for subspace } V \subset W}$

Bob

Encryption: $\xrightarrow{m=(w^*,v)}$

- Need arbitrary basis of V $\{v_1, v_2, \dots, v_t\}$.
- Compute $B^{\perp}$ basis of $V^{\perp}$ $\{v_1^{\perp}, v_2^{\perp}, \dots, v_{m-t}^{\perp}\}$.
- Plain text: $p \in W$
  Compute $v := w - p$,
  with $w \in V$ random.
- $w^* = w + \sum_{i=1}^{m-t} \alpha_i v_i^{\perp}$
  at least one $\alpha_i \neq 0$.

Alice

Decryption:

- Need orthonormal basis of V $\{e_1, e_2, \dots, e_t\}$.
- Compute $w = \sum_{i=1}^{t} \langle w^*, e_i \rangle e_i$.
- Calculate $p = w - v$.

Why the form $m = (w^*, v)$

Plain text: $p \in W$.
We have two possibilities: $p \notin V$ or $p \in V$.

Observation:

1. $p \notin V$: need extra vector $w \in V$.
   Because: Clothes vector theorem works in the subspace V.
   Calculate: w^*.
   To receive the plain text, the vector w^* is send with the vector $v := w - p$.
   Alice gets: $m := (w^*, v)$.
2. $p \in V$: The encrypted message is $m := p^*$.

Act as in Step 1: no adversary can obtain additional information on m.
Hence in both cases fulfill the same steps: Message is a tuple $m := (w^*, v)$.

Appendix CFRZ

Why the form $m = (w^*, v)$

Plain text: $p \in W$.
We have two possibilities: $p \notin V$ or $p \in V$.

<u>Observation:</u>

1. $p \notin V$: need extra vector $w \in V$.
   Because: Clothes vector theorem works in the subspace V.
   Calculate: w^*.
   To receive the plain text, the vector w^* is send with the vector $v := w - p$.
   Alice gets: $m := (w^*, v)$.
2. $p \in V$: The encrypted message is $m := p^*$.

Act as in Step 1: no adversary can obtain additional information on m.
Hence in both cases fulfill the same steps: Message is a tuple $m := (w^*, v)$.

Appendix CFRZ

Why the form $m = (w^*, v)$

Plain text: $p \in W$.
We have two possibilities: $p \notin V$ or $p \in V$.

<u>Observation:</u>

1. $p \notin V$: need extra vector $w \in V$.
   Because: Clothes vector theorem works in the subspace V.
   Calculate: w^*.
   To receive the plain text, the vector w^* is send with the vector $v := w - p$.
   Alice gets: $m := (w^*, v)$.
2. $p \in V$: The encrypted message is $m := p^*$.

Act as in Step 1: no adversary can obtain additional information on m.
Hence in both cases fulfill the same steps: Message is a tuple $m := (w^*, v)$.

Appendix CFRZ

Why the form $m = (w^*, v)$

Plain text: $p \in W$.
We have two possibilities: $p \notin V$ or $p \in V$.

Observation:

1. $p \notin V$: need extra vector $w \in V$.
   Because: Clothes vector theorem works in the subspace V.
   Calculate: w^*.
   To receive the plain text, the vector w^* is send with the vector $v := w - p$.
   Alice gets: $m := (w^*, v)$.
2. $p \in V$: The encrypted message is $m := p^*$.

Act as in Step 1: no adversary can obtain additional information on m.
Hence in both cases fulfill the same steps: Message is a tuple $m := (w^*, v)$.

Appendix CFRZ

$m, n, t \in \mathbb{N},\ t \leq n,\ W = \mathbb{R}^m,\ V \subset W$ with $dim(V) = t \Rightarrow V \cong \mathbb{R}^t$

It gives a set M composed of n vectors $v_i \in \mathbb{R}^t$, s. t. each random subset of size t defines a basis for $\mathbb{R}^t$.

Notation:

$$[n] := \{1, 2, \dots, n\} \qquad \text{with } n \in \mathbb{N},$$
$$H_{k_1} := Span\{v_i \mid i \in [t] \setminus \{k_1\}\} \qquad \text{with } k_1 \in [t] \text{ and } v_i \in B.$$

Note: It gives infinity many different hyperplanes in the $\mathbb{R}^t$.

Existence of M:

$B := \{v_1, v_2, \dots, v_t\}$ basis for $\mathbb{R}^t$. New vector

$$v_{t+1} \notin \bigcup_{k_1 \in [t]} H_{k_1} \text{ (union over all possible hyperplanes)}$$

$$M_1 := B \cup \{v_{t+1}\}$$

Move on with this procedure:
Notation at step p:

$$H_{k_1,\dots,k_p} := Span\left\{v_i \mid i \in [t+p-1] \setminus \{k_1,\dots k_p\}\right\}$$

pairwise different $k_1,\dots,k_p \in [t+p-1]$ and $v_i \in M_{p-1}$with

$$M_{p-1} := M_{p-2} \cup \left\{v_{t+p-1}\right\} = B \cup \left\{v_{t+1},\dots,v_{t+p-1}\right\},$$

At the step p: pick v_{t+p} with the property

$$v_{t+p} \in \left(\mathbb{R}^t \setminus \bigcup_{k_1,\dots,k_p \in [t+p-1]} H_{k_1,\dots,k_p}\right) \neq \emptyset.$$

Because we take $\binom{t+p-1}{t-1}$ hyperplanes out of the $\mathbb{R}^t$.
We get the set $M_p := M_{p-1} \cup \left\{v_{t+p}\right\}$ with the desired property.
We perform this $(n-t)$ times to get the desired set

$$M := M_{n-t} = \left\{v_1, v_2, \dots, v_t, v_{t+1}, \dots, v_n\right\}.$$

Generate M:

Lemma (Exchange Lemma)

Be B a basis for the space V with dimension k and $w \in V$ arbitrary. If $w \neq 0$ then there exists a vector $b \in B$ so that

$$B' := (B \setminus \{b\}) \cup \{w\}$$

is also a basis for V.

Addition:

We can choose every vector b_j from the basis B for the vector b, which has a nonzero coefficient α_j in the linear combination

$$w = \sum_{i=1}^{k} \alpha_i b_i .$$

If every coefficients $\alpha_i \neq 0$: Every vector b_i can be replaced from the basis B (of $\mathbb{R}^t$) by the vector

$$w = \sum_{i=1}^{k} \alpha_i b_i.$$

Get $M := B \cup \{v_{t+1}, v_{t+2}, \dots, v_n\}$: Calculate the new vectors as

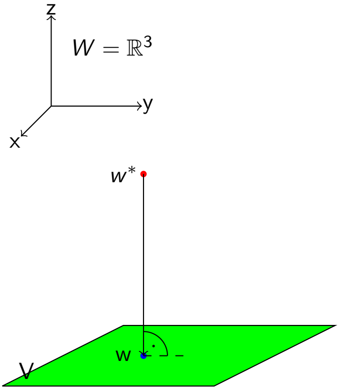
$$v_{j+1} = \sum_{i=1}^{t} p_{i_j} b_i \qquad \text{for } t \leq j \leq n-1.$$

p_{i_j}: pairwise distinct prime numbers ($\forall$ i and j).
Check that every t distinct vectors from M form a basis of $\mathbb{R}^t$:

- Write all $\binom{n}{t}$ combinations of the vectors in a matrix and proof the rank of the matrix.
- If the rank is at all times t: Get the desired property.
- If not, we have to test other coefficients.

◂ Appendix CRFZ

Secret: $w \in \mathbb{R}^3$
$dim(V) = t = 2$
$w \in V$



Example for an $(5, 2)$ CFRZ secret sharing II

Dealer:

1. $m := dim(W)$, $m \in \mathbb{N}$, $m > t$.
2. Secret: $w \in W$.
3. Choose $V \subset W$, s. t. dim(V)=t and $w \in V$.

Classic Worksheet Maple 13

<u>Step 1 and 2:</u>

```
> with(LinearAlgebra):
> m:= 3:    t:=2:    n:=5:
> w:=Transpose(<1,2,12>):
```

<u>Step 3:</u>

```
> B:=Matrix([[w],[RandomMatrix(t-1,m)]]);
```

$$B := \begin{bmatrix} 1 & 2 & 12 \\ 92 & -31 & 67 \end{bmatrix}$$

```
> Rank(B);
```

$$2$$

Example for an $(5, 2)$ CFRZ secret sharing III

Dealer:

4. Determine $M = \{v_1, v_2, \ldots v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.

Step 4:

```
> M:=Matrix(n,m):
> M[1]:=B[2]:
> M[2]:=31*B[1]+23*B[2]:
> M[3]:=7*B[1]+13*B[2]:
> M[4]:=5*B[1]-19*B[2]:
> M[5]:=17*B[1]-3*B[2]:
> M;
```

$$\begin{bmatrix} 92 & -31 & 67 \\ 2147 & -651 & 1913 \\ 1203 & -389 & 955 \\ -1743 & 599 & -1213 \\ -259 & 127 & 3 \end{bmatrix}$$

Example for an (5, 2) CFRZ secret sharing IV

Dealer:

4. Determine $M = \{v_1, v_2, \ldots v_n\}$, $v_i \in V$.
   Property: Any subset of M of size t defines a basis of V.

Step 4:

```
> for i from 1 to 4 do
>     for j from i+1 to 5 do
>         N:=Matrix([[M[i]],[M[j]]]):
>         R:=Rank(N):
>         print(R):
>     end:
> end:
```

2	2
2	2
2	2
2	2
2	2

Dealer:

5. Closest vector $w^* \in W \setminus V$ to $w \in V$:

a) Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$.

b) $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,

$$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp}$$

$\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$.

Step 5:

```
a):
> N:=Matrix([[M[1]],[M[2]]]);
```

$$N := \begin{bmatrix} 92 & -31 & 67 \\ 2147 & -651 & 1913 \end{bmatrix}$$

```
> kern:=NullSpace(N);
```

$$kern := \left\{ \begin{bmatrix} \frac{-506}{215} \\ \frac{-1037}{215} \\ 1 \end{bmatrix} \right\}$$

Dealer:

5. Closest vector $w^* \in W \setminus V$ to $w \in V$:

a) Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$.

b) $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,

$$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp}$$

$\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$.

Step 5:

```
b):
> r:=m-t:
> R:=RandomVector(r):
> while Equal(R,Vector(r)) do
>     R:=RandomVector(r):
> end:
> R;
```

[44]

Example for an $(5, 2)$ CFRZ secret sharing VII

Dealer:

5. Closest vector $w^* \in W \setminus V$ to $w \in V$:

a) Choose basis $\{b_1, b_2, \ldots, b_t\}$ of V, compute the orthogonal complement $V^\perp$.

b) $B^\perp = \{b_1^\perp, b_2^\perp, \ldots, b_{m-t}^\perp\}$ basis of $V^\perp$,

$$w^* = \underbrace{w}_{\in V} + \underbrace{(\alpha_1 b_1^\perp + \alpha_2 b_2^\perp + \ldots + \alpha_{m-t} b_{m-t}^\perp)}_{:= v^\perp \in V^\perp}$$

$\alpha_i \in \mathbb{R}$, at least one $\alpha_i \neq 0$.

Step 5:

```
b):
> vv:=Vector(m):
> for k from 1 to r do
>      vv:=vv+ kern[k]*R[k]:
> end:
> w*:=Transpose(w)+vv;
```

$$w^* := \begin{bmatrix} \frac{-22049}{215} \\ \frac{-45198}{215} \\ 56 \end{bmatrix}$$

Participants:

P_2 and P_5 reconstruct w:

1. Gram-Schmidt procedure: t vectors from $M \rightsquigarrow$ orthonormal basis $G = \{e_1, e_2, \dots, e_t\}$ of V.

```
> C:=Matrix([[M[2]],[M[5]]]);
```

$$C := \begin{bmatrix} 2147 & -651 & 1913 \\ -259 & 127 & 3 \end{bmatrix}$$

Step 1:

```
> L:=[seq(C[j],j=1..t)]:
> G:=GramSchmidt(L, normalized);
```

$$G := \left[\left[\frac{2147\sqrt{8692979}}{8692979}, -\frac{651\sqrt{8692979}}{8692979}, \frac{1913\sqrt{8692979}}{8692979}\right], \left[-\frac{921908\sqrt{1330634295530}}{1995951443295}, \frac{1429583\sqrt{1330634295530}}{3991902886590}, \frac{511169\sqrt{1330634295530}}{798380577318}\right]\right]$$

Example for an $(5, 2)$ CFRZ secret sharing IX

Participant:

2. Reconstruct the secret w: Public w^* and closest vector theorem:

$$w = \sum_{i=1}^{t} \langle w^*, e_i \rangle e_i$$

<u>Step 2:</u>

```
> v:=Transpose(Vector(m)):
> for k from 1 to t do
>   v := v + DotProduct(w*, G[k]) * G[k] :
> end:
> V:=Transpose(v);
```

$$V := \begin{bmatrix} 1 \\ 2 \\ 12 \end{bmatrix}$$

Appendix CRFZ