Secret Sharing

https://iuk.one/1033-1011

Clemens H. **Cap**
ORCID: 0000-0003-3958-6136

Department of Computer Science
University of **Rostock**
Rostock,Germany
clemens.cap@uni-rostock.de

Version 2

Overview

1. Basic Secret Sharing

We introduce into the topic and illustrate a first method for secret sharing.

Cryptographic Anecdote

Problem:

- Trent wants to give Alice and Bob access to the safe.
- Trent does not trust one of them completely.
- Trent wants to split the access key.
- Alice alone or Bob **alone** shall have **no** information at all.
- Alice and Bob **together** shall have the **complete** information.

Solution:

- Trent wants to share key $K \in \{0,1\}^n$.
- Trent generates random bit string $R \in \{0,1\}^n$.
- Trent gives $A = R \oplus K$ to Alice and $B = R$ to Bob ($\oplus$ calculated bitwise).
- Alice and Bob regenerate key K by forming $A \oplus B$.
- Alone, both only have random noise.

Splitting and Threshold Problem

Splitting Problem:

- There are n recipients of shares.
- Trent wants to split key K into n shares $A_1, \ldots, A_n$.
- Each collection of $n-1$ shares shall contain no information on the key K at all.
- All participants together shall be able reconstruct the key.

Threshold Problem

- **Question:** What, if one participant loses the key?
- (k, n)-threshold scheme splits a secret K into n parts.
- k or more parts allow a reconstruction of the secret K.
- Less than k parts do not allow reconstruction of the secret S.
- **Answer:** At most $n-k$ shares may be lost without problem.

Perfect Threshold Schemes

Perfect Threshold schemes

A (k, n) threshold scheme is called **perfect**, if less than k parts provide no information on the secret in the sense that even with knowledge of these parts the distribution of the secret is the equidistribution.

Thus: Perfect threshold schemes are secure in the **unconditionally secure model**.

The Perfect Secret Sharing Scheme by Shamir

Construction of Splitting for a (k, n) threshold scheme.

- Pick point $(0, S)$ with S being the secret to be shared.
- Generate a random polynomial P of degree $k-1$ through this point.
- Pick n pairwise different non-zero points $x_1, \ldots, x_n$.
- Generate $y_j = P(x_j)$.
- Distribute the pairs $(x_1, y_1), \ldots, (x_n, y_n)$ to the n parties.

Reconstruction:

- Gather k pairs (x_j, y_j).
- Construct the Lagrange interpolation polynomial of degree (at most) $k-1$ from these pairs.
- This polynomial must be the polynomial P.
- Evaluating the polynomial in $x = 0$ provides the secret $S = P(0)$.

Reference: Shamir: How to Share a Secret

Application

Problem: Random polynomials over $\mathbb{R}$ are problematic.

- There is no equidistribution on $\mathbb{R}$.
- Not every real number may be represented in a computer.

Solution: Use a finite field $GF(p^k)$.

Task: Exercise on Secret Sharing

Situation:

- Trent wants to share a secret among his friends Alice, Bob and Carol.
- He decides to use a $(2, 3)$ threshold scheme on $GF(4)$.
- The value of the secret is 2 in the binary decoding of $GF(4)$.

Tasks:

- Pick a suitable (random) polynomial of suitable degree.
- Calculate the shares for Alice, Bob and Carol.
- Determine the secret from the shares of Alice and Carol.
- Why would GF(256) be more secure?
- Would GF(4) work out if Trent had 4 friends?

2. Advanced Variants

2.1. Verifiable Secret Sharing

2.2. Proactive Secret Sharing

2.3. Weighted Schemes

We shall develop an understanding of some further problems and solution strategies in secret sharing.

Verifiable Secret Sharing: The Cheating Dealer

Problem: Dealer might be cheating

- Assumption thus far was: Dealer of the secret works as described.
- In a $(3, 7)$ threshold-scheme A, B and C meet and construct secret X.
- C, D and E meet and construct secret $Y \neq X$.
- Obviously: Someone is cheating.
- Is this C? Or B? Or has it been the dealer?
- Share holders want to check if dealer was cheating.

Solution:

- Verify: All k shares lead to the same secret
- But: Should not need to reconstruct the secret for this purpose
- There exists a zero knowledge proof of correctness.

Proactive Secret Sharing: Stolen Shares

Problem: Shares are stolen by attackers.

Example: Assume a threshold scheme of (3,9) is in use.

- Two shares get stolen.
- If another share gets stolen, the attacker can reconstruct the secret.

Solution: Update Protocol.

- All parties update their shares.
- All old shares are destoyed so that no further share can be compromised.
- The compromised shares are of no value any more
  as they communicate no information of the secret.

Update Protocol

Mechanism:

- Trustworthy party constructs a random polynomial Q with $Q(0) = 0$.
- Party j holding share (x_j, y_j) gets value $z_j = Q(x_j)$.
- Party j will now use $(x_j, y_j + z_j)$ as its share.
- This corresponds to a completely fresh polynomial $P + Q$ being used instead of P.
- Secret stays the same since $(P + Q)(0) = P(0) + Q(0) = P(0) + 0 = P(0)$.

Advanced Variants

Possible Scenarios:

- Assumption that some share holders are liars.
- Assumption that distributor of secret is a liar.
- Assumption that some shares get lost.
- Literature knows protocols which mix verifiable and proactive secret sharing.

Example

Question: Do more general access schemes make sense?

Example: Access to the safe for any 3 employees or supervisor plus 1 employee.

Idea: Allow more than one share per person.

Mechanism: Weighted Threshold Schemes

- Use a threshold scheme requiring 3 shares.
- Supervisor gets 2 shares, employees get 1 share.

Notion of General Access Schemes

Question: What is a good mathematical model of a "general access scheme"?

Idea:

- Let P be the set of persons considered.
- An access scheme $\mathcal{S}$ is a set of sets of persons who are allowed to access the safe.
- Formally: $\mathcal{S} \subseteq 2^P$

Example: $P = \{A, B, C, D\}$.

- Access scheme $\mathcal{S} = \{\{A, B\}, \{C, D\}\ \}$.
- Obviously also $\{A, B, C\}$ can access the safe.
- Every superset of a set in a scheme can access the safe.
- **True** scheme is:
  $\{\{A, B\}, \{C, D\}, \{A, B, C\}, \{A, B, D\}, \{A, C, D\}, \{B, C, D\}, \{A, B, C, D\}, \}$.

Thus: Definition needs some modification.

General Access Schemes (1)

General Access Schemes: First Variant of Definition

A **general access scheme** is a set $\mathcal{S}$ of sets which is closed by formation of supersets.

Semantics: A set Q of persons is permitted access, if and only if Q is an element of $\mathcal{S}$.

Note:

- Every set of sets can be turned into a general access scheme by adding all supersets of its member sets.
- Let us call this process the **saturation**.
- So why use a larger set to denote a general access scheme than required?
- We could use a smaller set with the understanding that we "mean" its saturated version.

General Access Schemes (2)

Elaboration:

- We may remove a set X from an access scheme $\mathcal{S}$ if it is the superset of another set Y in the access scheme.
- The resulting set $S \setminus \{X\}$ still **generates** the original access scheme $\mathcal{S}$.
- After some removals we get minimal sets: Further removals are no longer possible.
- Let us call such a set **removal-minimal**.
- **Question:** Is there a **unique** removal-minimal generating set for an access scheme?
- **Answer:** Yes. (Proof by induction on the number of persons).

General Access Schemes: Second Variant of Definition

A **general access scheme** is a removal-minimal set of sets, i.e. there is no element X in $\mathcal{S}$ such that a subset of X also is in $\mathcal{S}$.

Semantics: Set Q of persons allowed access if it contains an element of $\mathcal{S}$ as a subset.

Limitations on Weighted Threshold Schemes (1)

Question: Can every access scheme be realized as weighted threshold scheme?

Answer: No.

Counterexample: $S = \{\{A, B\}, \{C, D\}\}$

Assumption: There exists a threshold scheme with threshold k.

Let the participants have share weights a, b, c, d.

In the first set: From A and B one of the two has the larger-or-equal number of weights.

This shall be A.

Same thought for the second set.

Thus: Without loss of generality: $a \geq b$ and $c \geq d$.

$a + b \geq k$ since A and B together can access.

$c + d \geq k$ since C and D together can access.

$a + a \geq a + b \geq k$ so $2a \geq k$ and $a \geq k/2$.

Limitations on Weighted Threshold Schemes (2)

Similarly show $c \geq k/2$.

Thus $a + c \geq k/2 + k/2 \geq k$.

Thus A and C may access the safe.

This is in contradiction to the requirements of which we (incorrectly) assumed the threshold scheme is a solution.

Therefore (by indirect proof) the assumption must be wrong.

3. General Access Schemes

Question: Which general access schemes can be implemented by sharing schemes?

Answer: All.

Example

Question: Can we realize this access scheme by different means?

Answer: Yes – and even with a threshold scheme.

Idea: Reuse shares: One share is distributed to more than one person.

Assume a $(4, 4)$. Let the shares be e, f, g, h.

Allocation of shares:

- A gets e, g
- B gets f, h
- C gets e, f
- D gets g, h

Correctness of implementation:

- $\{A, B\}$ and $\{C, D\}$ can access.
- $\{A, C\}$, $\{A, D\}$, $\{B, C\}$ and $\{B, D\}$ cannot access.

Generic Example and Method (1)

Access scheme is $\mathcal{S} = \{\{A, B, D\},\ \{A, C, D\},\ \{B, C\}\}$.

Step 1: Construct Access Function

- Write conjunction as multiplication, disjunction as addition.
- Write down access function $f(A, B, C, D) = ABD + ACD + BC$.
- With appropriate settings of A, B, C, D:
  Function is true exactly on the permitted situations.

Step 2: Obtain Dual Access Function as Sum of Products

- Dualize: $f^*(A, B, C, D) = (A + B + D)(A + C + D)(B + C)$
- Resolve the multiplication using the **distributive** law.
- Simplify using **idempotence**: $AA = A$
- Simplify using **dominance**: $ABC + BC = BC$
- Get simplified **sum of product** form: $f^*(A, B, C, D) = AB + AC + BC + BD + CD$

Generic Example and Method (2)

Step 3: Obtain Dual Access Scheme

- Derive access scheme from dual access function
  $f^*(A, B, C, D) = AB + AC + BC + BD + CD$
- $S^* = \{\{A, B\},\ \{A, C\},\ \{B, C\},\ \{B, D\},\ \{C, D\}\}.$

Step 4: Take Set-Wise Complements

- Take the complement of the sets in the DA scheme.
- It is: $S^*_{\complement} = \{\{C, D\}, \{B, D\}, \{A, D\}, \{A, C\}, \{A, B\}\}$
- This is the complemental dual access scheme (CDA).

What have we done so far?

- Scheme was $\{\{A, B, D\},\ \{A, C, D\},\ \{B, C\}\}$
- Sets in scheme are **minimal allowed sets** of persons.
- Complemental dual scheme is $\{\{C, D\},\ \{B, D\},\ \{A, D\},\ \{A, C\},\ \{A, B\}\}$
- Sets in complemental dual scheme are **maximal not-allowed sets**.

Generic Example and Method (3)

Step 5: Construct Cumulation Matrix and Read-Off Share Distribution

- **Rows** are persons.
- **Columns** are sets of the complemental dual scheme (CDA).
- **Shares** use (5,5) threshold scheme for the 5 sets of CDA.
- **Scheme** was $\{\{C, D\}, \{B, D\}, \{A, D\}, \{A, C\}, \{A, B\}\}$

Mechanism: For every maximal not-allowed set, one share is constructed.

Cumulation

	S_1	S_2	S_3	S_4	S_5	5 Shares
	$\{C, D\}$	$\{B, D\}$	$\{A, D\}$	$\{A, C\}$	$\{A, B\}$	5 Sets in CDA
A	1	1	0	0	0	
B	1	0	1	1	0	
C	0	1	1	0	1	
D	0	0	0	1	1	

Allocation

Party	Shares
A	S_1, S_2
B	S_1, S_3, S_4
C	S_2, S_3, S_5
D	S_4, S_5

Generic Example and Method (4)

Check:

- $\{A, B, D\}$ is allowed access.
- $\{A, C, D\}$ is allowed access.
- $\{B, C\}$ is allowed access.

	Allocation
A	S_1, S_2
B	S_1, S_3, S_4
C	S_2, S_3, S_5
D	S_4, S_5

Check:

- $\{C, D\}$ not allowed since share S_1 is missing.
- $\{B, D\}$ not allowed since share S_2 is missing.
- $\{A, D\}$ not allowed since share S_3 is missing.
- $\{A, C\}$ not allowed since share S_4 is missing.
- $\{A, B\}$ not allowed since share S_5 is missing.

4. Computing with Shared Secrets

Privacy preserving computational schemes are one of the most important applications of secret sharing next to the secret sharing property as such.

Sum: Algorithmus

There are n parties.

Every party j has a private value k_j.

Let $x_1, x_2, \ldots, x_n$ be pairwise different values, x_j for party j.

Party j shares value k_j with the parties by

1. Generating a random polynomial P_j with $P_j(0) = k_j$
2. Sending $P_j(x_i)$ to party i.

Every party i receives n shares $P_1(x_i), \ldots, P_n(x_i)$.

Every party i forms $P_1(x_i) + \ldots + P_n(x_i) = (P_1 + \ldots + P_n)(x_i) = \sigma_i$

The pairs (x_i, σ_i) reconstruct to $(P_1 + \ldots + P_n)(0) = k_1 + \ldots + k_n$.

Sum: Result

Properties of the Algorithm:

- Every party learns the sum of the n values.
- No party learns more about the private values than can be derived from the sum and the own private value.

Product

Problem 1: Product of two polynomials has higher degree.

Problem 2: Product of two random polynomials is not equidistributed.

Solution:

- Both problems are solvable.
- Solution produces no additional principle insights,
- Paper describing the solution: Ben-Or Goldwasser, Widgerson: Completeness theorems for non-cryptographic fault-tolerant distributed computation.

Appendix

Contents of Appendix

Terms of Use (1)

Terms of Use (2)

Disclaimer: Die sich immer wieder ändernde Rechtslage für digitale Urheberrechte erzeugt ein nicht unerhebliches Risiko bei der Einbindung von Materialien, deren Status nicht oder nur mit unverhältnismäßig hohem Aufwand abzuklären ist. Ebenso kann den Rechteinhabern nicht auf sinnvolle oder einfache Weise ein Honorar zukommen, obwohl deren Leistungen genutzt werden.

Daher binde ich gelegentlich Inhalte nur als Link und nicht durch Framing ein. Lt EuGH Urteil 13.02.2014, C-466/12 (Pressemitteilung, Blog-Beitrag, Urteilstext). ist das unbedenklich, da die benutzten Links ohne Umgehung technischer Sperren auf im Internet frei verfügbare Inhalte verweisen.

Wenn Sie diese Rechtslage stört, dann setzen Sie sich für eine Modernisierung des völlig veralteten Vergütungs- und Anreizsystems für urheberrechtliche Leistungen ein. Bis dahin klicken Sie bitte auf die angegebenen Links und denken Sie darüber nach, warum wir keine für das digitale Zeitalter sinnvoll angepaßte Vergütungs- und Anreizsysteme digital erbrachter Leistungen haben.

Zu Risiken und Nebenwirkungen fragen Sie Ihren Rechtsanwalt oder Gesetzgeber.

Weitere Hinweise finden Sie im Netz hier und hier oder hier.

Citing This Document

If you use contents from this document or want to cite it,
please do so in the following manner:

Clemens H. Cap: Secret Sharing. Electronic document. https://iuk.one/1033-1011 27. 6. 2023.

Bibtex Information: https://iuk.one/1033-1011.bib

```
@misc{doc:1033-1011,
   author      = {Clemens H. Cap},
   title       = {Secret Sharing},
   year        = {2023},
   month       = {6},
   howpublished = {Electronic document},
   url         = {https://iuk.one/1033-1011}
}
```

Typographic Information:
Typeset on ?today?
This is pdfTeX, Version 3.14159265-2.6-1.40.21 (TeX Live 2020) kpathsea version 6.3.2
This is pgf in version 3.1.5b
This is preamble-slides.tex myFormat©C.H.Cap

List of Slides

Legend:
continuation slide
slide without title header
image slide