Challenging the Adversary Model in Secret Sharing Schemes

Keith Martin

Information Security Group, Royal Holloway, University of London

Brussels Contact Forum: Coding theory and cryptography II 2007

Geometrical aspects of secret sharing theory

Keith Martin
Information Security Group, Royal Holloway, University of London

Brussels Contact Forum: Coding theory and cryptography II 2007

A Bird's Eye View of Secret Sharing Research

Keith Martin
Information Security Group, Royal Holloway, University of London

Brussels Contact Forum: Coding theory and cryptography II 2007

Challenging the Adversary Model in Secret Sharing Schemes

Keith Martin

Information Security Group, Royal Holloway, University of London

Brussels Contact Forum: Coding theory and cryptography II 2007

The plan

1. **Traditional secret sharing**
2. **Secret sharing research: a bird's eye view**
3. **Changing the adversary model**

A few caveats before we start

- This is not a complete survey (how long have I got?)
- There are bits of mathematics here (but you might have to pay attention closely)
- I might mention the word code a few times (but it won't be more than that)
- All the schemes are of theoretical interest (but don't implement them at home before checking their applicability!)
- Just my perspective...

Traditional secret sharing schemes

Traditional secret sharing schemes

A **secret sharing scheme** is a method of distributing a **secret** amongst a set of **participants** by giving each participant a **share** in such a way that only certain specified subsets of participants (defined by the **access structure** Γ) can reconstruct the secret from a pooling of their shares.

Secret sharing schemes have been extensively studied by:

- **mathematicians** as objects of intrinsic interest in their own right
- **cryptographers** as important cryptographic primitives
- **security engineers** as techniques to employ in distributed security applications.

Two fundamental properties

Secret sharing schemes have two fundamental properties:

1. **Privacy**: Unauthorised subsets of participants should be prevented from learning the secret.
2. **Recoverability**: Authorised subsets of participants should be able to recover the secret by pooling their shares.

Imaginary friends

Most secret sharing schemes involve two "hidden" entities who are not always discussed at length:

- The **dealer** is the entity normally responsible for:
  - generating system parameters
  - generating the secret
  - creating initial shares
  - sending initial shares to participants
- The **combiner** is the entity responsible for:
  - pooling shares
  - reconstructing the secret

Basic concepts

- **Monotone access structures**: Γ has the property that if $A \in \Gamma$ then all supersets A' of A are also in Γ.
- **(k, n)-threshold schemes**: Where the access structure consists of all subsets of n participants of at least size k.
- **Information-theoretic security**: Security is independent of the computing power of any adversary.
- **Perfect**: Subsets of participants **not** in the access structure do not learn any information about the security via their shares.
- **Information rates**: Measures of efficiency of a secret sharing scheme based on the relationship between share size and secret size (in perfect schemes share must be at least size of secret).
- **Ideal**: perfect schemes with optimal information rate.

Traditionally...

Defined in an information-theoretic model.

The traditional model makes the following important assumptions about the potentially malicious behaviour of an **adversary**:

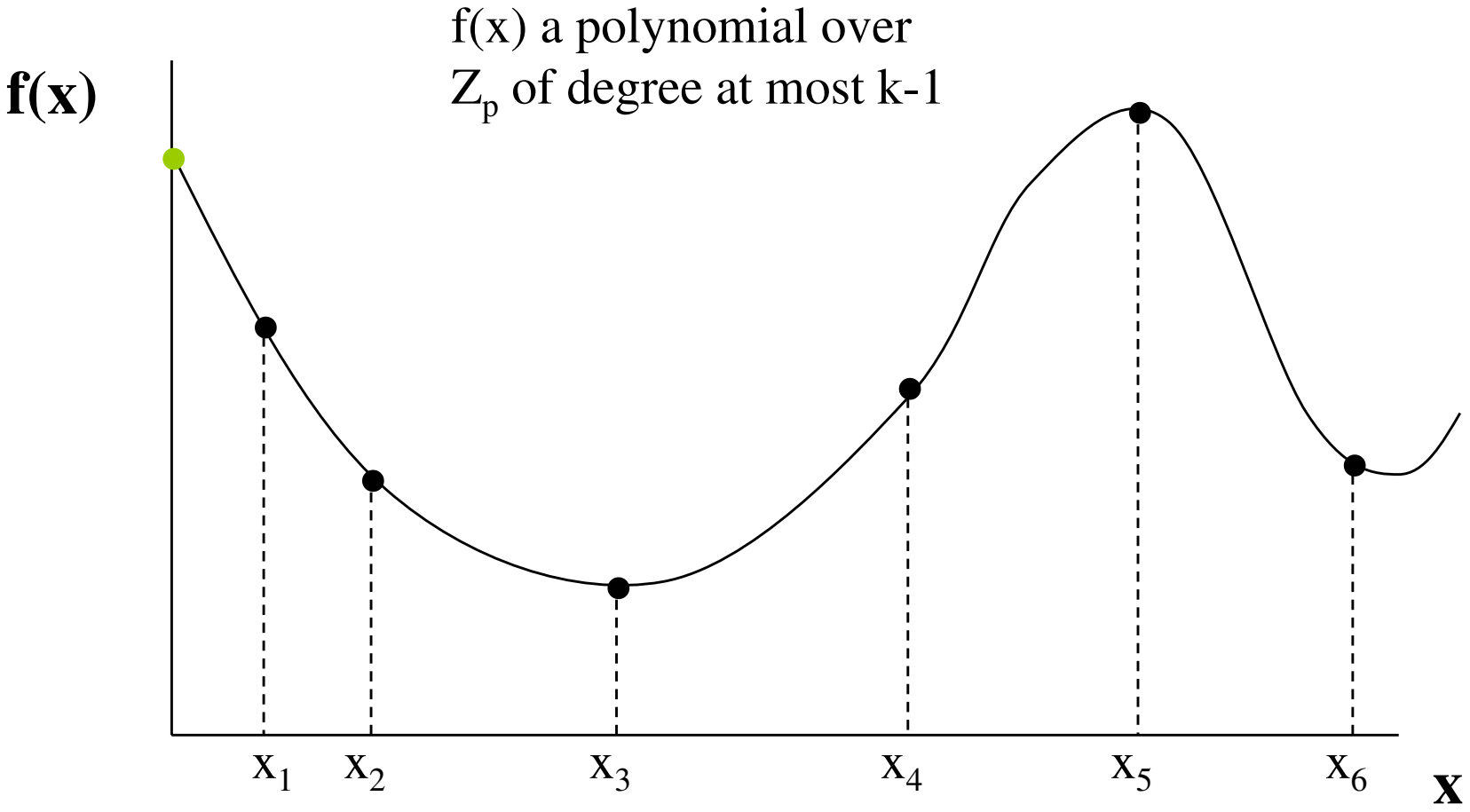
- **Trusted dealer**: An adversary cannot corrupt the dealer.
- **Passive**: An adversary can captures shares, but otherwise the scheme is followed correctly and shares are not corrupted.
- **Polarised participants**: Participants are either **honest** (follow the rules) or **malicious** (captured by an adversary who may not follow the rules).

Secret sharing models

There are numerous ways of modelling an information-theoretically secure secret sharing scheme:

- **Information theory**: By representing entities as probability distributions and making statements about conditional entropy.
- **Combinatorially**: By defining a matrix of possible distribution rules.
- **Algorithmically**: As two algorithms *Share* and *Reconstruct* and defining related properties.

Shamir's (k, n)-threshold scheme



Ideal threshold schemes

The following are combinatorially equivalent:

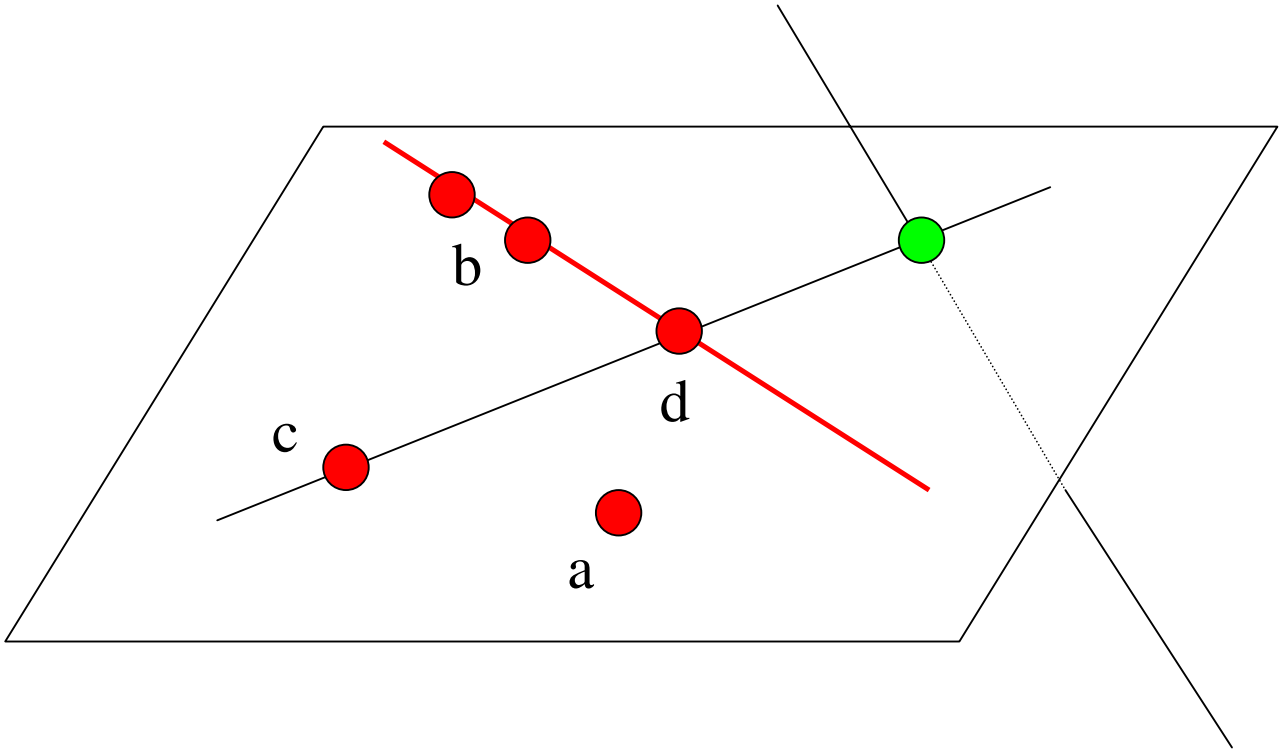
- An ideal (k, n)-threshold scheme on q secrets
- A transversal design $TD_1(k, n+1, q)$
- An orthogonal array $OA(q, n+1, k; 1)$
- A maximum distance separable code $MDS(k, 1, q, n+1)$
- A $(k, 1, q, n+1)$-affine structure
- An $(k-1)$-optimal cartesian authentication code $AC(n+1, q(n+1), q^k)$

Linear schemes

Linear secret sharing schemes are the most studied secret sharing schemes (with good reason). They can be defined in terms of:

- Vector spaces
- Projective geometry
- Error correcting codes
- Monotone span programmes

Geometric linear secret sharing scheme



$$\Gamma = ab + bc + cd$$

Secret sharing research: a bird's eye view

Secret sharing research: a bird's eye view

- The fundamental theoretical problem
- Changing the privacy model
- Changing the adversary model
- Extended capabilities
- Different networking models
- Secret sharing with a difference
- Applications

The fundamental theoretical problem

How efficient can we make a secret sharing scheme for a given Γ?

- Which access structures are ideal?
- If an access structure is not ideal, how close to ideal can it be?
- Can we determine efficient processes for building "good" secret sharing schemes for a given access structure?

Changing the privacy model

By demanding perfect privacy in an information-theoretic setting, the shares must be at least the size of the secret. If we don't want this then something has to give:

1. **Statistical privacy**: Slacken the **perfect** requirement in the information-theoretic model (this is sometimes called **non-perfect** secret sharing).
2. **Computational privacy**: Slacken the security model to one of **computational security**, dependent on the difficulty of hard problems.

Changing the adversary model

Coming soon...

Extended capabilities

- **Proactive secret sharing** (ability to refresh)
- **Dynamic secret sharing** (ability to change access structure)
- **Multiple secret sharing** (ability to share more than one secret)
- **Secret sharing with veto capability** (ability to block reconstruction)

Secret sharing under different network models

- **Asynchronous secret sharing** models secret sharing schemes in asynchronous networks, where delays in communications can be expected.
- **Dealer-free secret sharing** models secret sharing in environments where it is not possible to identify one entity to act in the role of the dealer.

Secret sharing with a difference

- **Chinese Remainder scheme** (schemes based on the Chinese Remainder Theorem)
- **Homomorphic secret sharing** (useful for many applications)
- **Multiplicative secret sharing** (required for multiparty computation)
- **Black box secret sharing** (schemes that are independent of the underlying group)
- **Anonymous secret sharing** (identities of participants not required for reconstruction)
- **Weighted secret sharing** (shares have different relative importance)
- **Visual secret sharing** (secret and shares are images)

(Just some) Applications

- Secure multiparty computation
- Threshold cryptography
- Key recovery mechanisms
- Master key establishment
- Distributed Certificate Authorities
- Distributed information storage
- Location privacy
- Key management in ad-hoc networks
- Information hiding
- Fair exchange
- Secure online auctions
- Electronic voting

Changing the adversary model

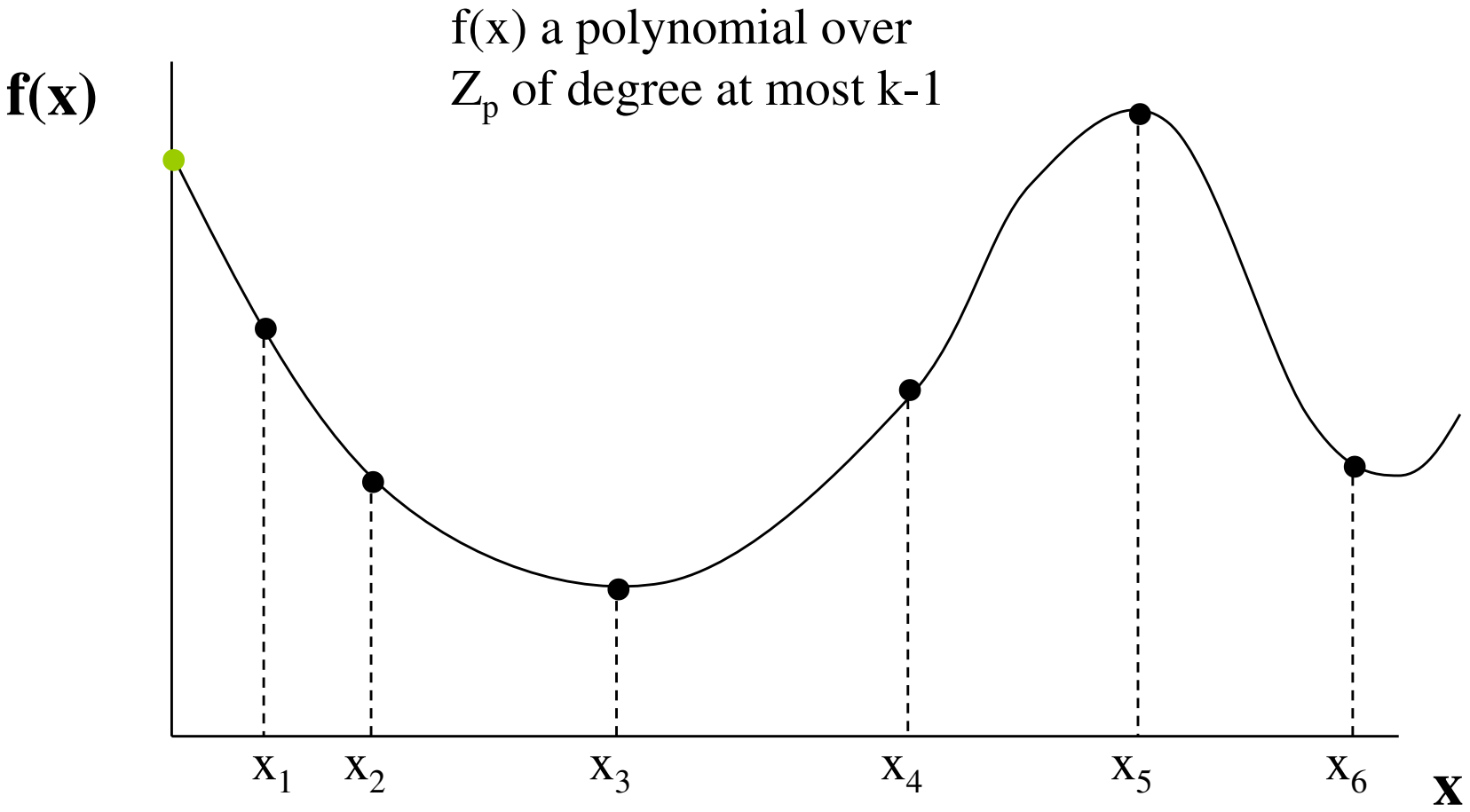
Changing the adversary model

Recall the traditional adversary assumptions:

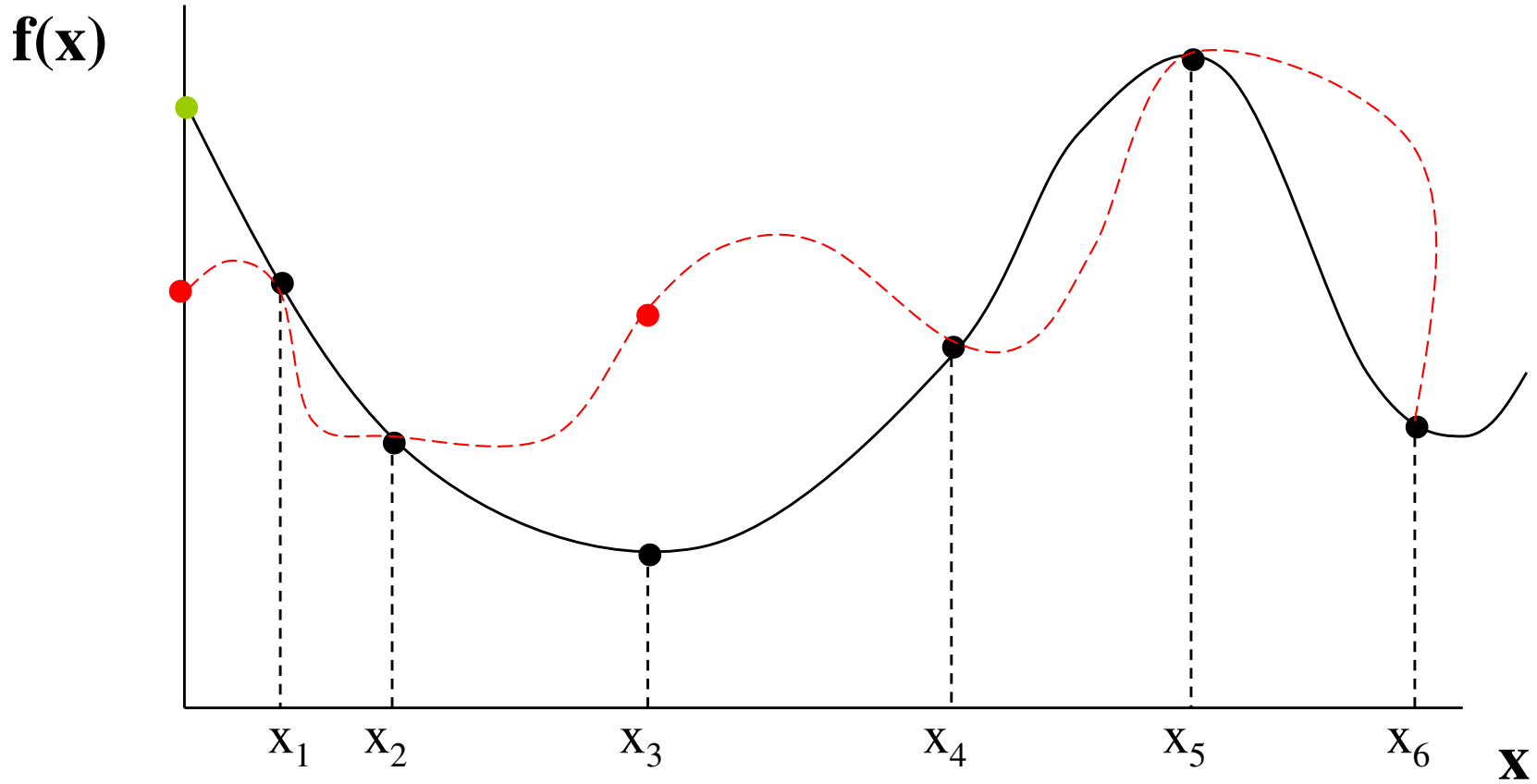
- **Trusted dealer**: An adversary cannot corrupt the dealer.
- **Passive**: An adversary can captures shares, but otherwise the scheme is followed correctly and shares are not corrupted.
- **Polarised participants**: Participants are either **honest** (follow the rules) or **malicious** (captured by an adversary who may not follow the rules).

For the time being we assume a trusted dealer!

Tompa and Woll's attack



Tompa and Woll's attack



Undesirable consequences

Tompa and Woll's attack has several undesirable consequences:

1. Prevents the honest participants from learning the correct secret
2. Fails to alert the other participants that they have not reconstructed the correct secret
3. Allows the adversary to learn the correct secret.

Countering the consequences

	Honest users learn secret?	Honest users alerted?	Adversary learns secret?
Robust schemes	Yes	Sometimes	Yes
Cheater identification	No	Yes	Yes
Cheater detection	No	Yes	Yes
Fairness schemes	Sometimes	Yes	Sometimes
Cheating immune	No	No	No

Issues arising from active adversaries

- **Who is the combiner?**
  - an *uncorrupted participant* or an *external party*?
- **Are shares revealed during reconstruction?**
  - *open* or *closed* reconstruction?
- **How versatile are adversaries?**
  - *static* or *dynamic*?
- **What are the goals of the adversary?**
  - *Corruption* or *disruption*?

Robust secret sharing schemes

Robust secret sharing schemes allow the secret to be reconstructed by an honest set of authorised participants in the presence of an active adversary who is able to corrupt shares.

- Assume a trusted dealer.
- Honest participants want to recover the secret even if an adversary corrupts shares.
- The main recoverability goal of the adversary is to prevent the correct secret from being reconstructed.

Bellare and Rogaway's framework

Bellare and Rogaway recently proposed a framework for robust secret sharing schemes:

Privacy	Recoverability	Adversary	Examples
PSS	PR	0	Perfect secret sharing
SSS	PR	0	Non-perfect secret sharing
CSS	PR	0	Computational secret sharing
PSS	PR	2	Linear perfect threshold schemes
PSS	SR	1	Tompa and Woll
CSS	CR	2	Krawczyk

Schemes with cheater detection (identification)

Allow honest participants to detect (identify) any corrupt shares that have been submitted by an adversary.

Secret sharing schemes with cheater detection (identification):

- Assume a trusted dealer.
- Honest participants are willing to sacrifice recovery of the secret if an adversary corrupts shares, so long as corrupt shares are detected (identified).
- The main recoverability goal of the adversary is to prevent the correct secret from being reconstructed while remaining undetected (unidentified).
- Potentially allow the adversary to obtain the correct secret while the honest participants do not.

Schemes with cheater detection (identification)

Normally proposed in information-theoretic model since computationally-secure environments can use digital signatures.

The capability cost is typically that such schemes either:

- **Have large shares**: Each participant is equipped with extra information that allows them to recognise malicious behaviour.
- **Require extra cooperation**: Need more than a minimum coalition of participants to co-operate in a recovery attempt.

Ideal (k, n)-threshold schemes

It has been widely noted for the linear case, but also holds for non-linear ideal (k, n)-threshold schemes that they:

- Can detect t cheating participants if $k + t$ participants (at most t of whom are cheating) collaborate.
- Can identify t cheating participants, but only if $k + 2t$ participants (at most t of whom are cheating) collaborate.
  In fact in this case they can also recover the correct secret.

Two flavours of schemes with cheater detection

- In **uninformed schemes** cheating participants do not know the secret when they try to cheat
  - otherwise referred to as *secure* or under the *OKS assumption*
  - $|\mathcal{S}_i| \geq \frac{|\mathcal{S}|-1}{\epsilon} + 1$
- In **informed schemes** cheating participants know the secret when they try to cheat
  - otherwise referred to as *robust* or under the *CDV assumption*
  - $|\mathcal{S}_i| \geq \frac{|\mathcal{S}|-1}{\epsilon^2} + 1$

Cheater detection schemes

	Flavour	Construction	Share size	Error
1	**Uninformed**	Ogata et al	$q^2 - q + 1$	$1/q$
2	**Uninformed**	Cabello et al	q^2	$1/q$
3	**Informed**	Cabello et al	q^3	$1/q$
4	**Informed**	Obana and Araki	p^{N+2}	$(N+1)/p$

1. Optimal scheme
2. Share of secret k plus share of k^2
3. Share of secret k plus share of r and kr
4. Share of secret k plus share of universal hash function key

Fairness schemes (Almost PSS-SR1 robust)

Give each participant:

- share of (k, n)-threshold scheme that can detect $r < k/2$ cheaters with secret k_1
- share of $(k - r, n)$-threshold scheme that can identify $r < k/2$ cheaters with secret k_2.
- secret $s = k_1 \oplus k_2$.

1. Use first shares to check for cheaters.
2. If cheaters noted then recovery aborted.
3. If no cheaters, use second shares to check for cheaters. Even if r cheaters identified, the $k - r$ honest participants still recover k_2.
4. Secret s is computed from k_1 and k_2.

Cheating immune schemes

- Assume a trusted dealer.
- Assume a third party (external) combiner.
- Honest participants are willing to sacrifice recovery of the secret if an adversary corrupts shares, so long as the adversary does not as a result have an advantage over the honest participants with respect to recovery of the genuine secret.
- The main recoverability goal of the adversary is to have more knowledge about the secret than a set of honest participants.
- If an adversary submits corrupted shares then nobody obtains the secret.

Rational schemes

- a trusted dealer,
- open reconstruction;
- **participants neither fully honest nor fully malicious**.

Rational participants:

1. want to recover the secret (this is their top priority)
2. will take the opportunity to cheat if it is in their interest.

In each of many rounds the dealer either:

- *with probability* β *generates shares of the real secret*
- *with probability* $1-\beta$ *generates shares of a random secret*

After each round, participants who wish to take part broadcast their shares.

Verifiable schemes

Verifiable secret sharing schemes (**VSS schemes**):

- **Do not assume a trusted dealer**.
- Honest participants want to recover secret even if adversary corrupts dealer and some shares.
- Main recoverability goal of adversary is to prevent correct secret from being reconstructed.

Have additional algorithm **Verify** which allows participants to check:

- **Consistency**: any authorised group of participants $A \in \Gamma$ that all *accept* their shares will be able to reconstruct the same secret value u.
- **Correctness**; if dealer was honest then u is the genuine secret.

Types of VSS scheme

A VSS scheme is

1. **interactive** if **Verify** involves participants exchanging messages between themselves
2. **non-interactive** if **Verify** only involves participants exchanging messages with the dealer
3. **publicly-verifiable** if honest participants are assured of the validity of their own share *and* the shares of other participants

Information-theoretically secure VSS schemes

- are necessarily interactive
- can only be established if access structure Γ has the property that **no three subsets not in Γ span the entire participant set**
- (k, n)-threshold VSS scheme can be constructed from symmetric bivariate polynomials over a finite field
- this construction generalises into a conversion from any linear secret sharing scheme for a qualified access structure...
- ... but given that the dealer may be corrupt, can you always place trust in the system parameters?
- are related to **error-set correcting codes**
- research interest in minimising number of rounds

Computationally secure VSS schemes

Two options for relaxing this security model:

1. relax security of underlying secret sharing scheme (Feldman)
2. relax security of verifiability of the shares (Pedersen)

Most computationally secure VSS schemes are non-interactive (although interactive schemes have been proposed).

Publicly-VSS schemes

- **non-interactive** by nature, but are often called:
  - **interactive** if algorithm **Publicly-Verify** requires interaction between participants and the dealer
  - **non-interactive** if this is not necessary
- work by publishing asymmetrically encrypted shares and allowing the consistency check to be performed on these encrypted shares
- typically rely on zero-knowledge proof techniques to prove correctness of shares

Concluding remarks

- There is a lot going on (steadily but surely)
- Applications for secret sharing schemes seem to be getting more important
- Despite an absence in this talk, there is a lot of mathematics behind secret sharing schemes
- Expect more formalisation of secret sharing adversary models in the near future

For more details...

- **Of the first talk** (see *Geometrical contributions to secret sharing theory*. Journal of Geometry, Vol. 79 1-2 (2004) 102–133 (with W.-A. Jackson and C.M. O'Keefe).
- **Of the second talk** (work in progress).
- **Of this talk** (see proceedings).