On Actively Secure Fine-Grained Access Structures from Isogeny Assumptions

Fabio Campos[1,2] Philipp Muth[3]

[1]RheinMain University of Applied Sciences, Wiesbaden, Germany

[2]Radboud University, Nijmegen, The Netherlands

[3]Technische Universität Darmstadt, Germany

September 13, 2022

Where are we? I

Hard Homogeneous Spaces (Couveignes [Cou06])

A hard homogeneous space $(\mathcal{E}, \mathcal{G})$ is

- a set $\mathcal{E}$,
- a group $(\mathcal{G}, \odot)$ and
- an action $* : \mathcal{G} \times \mathcal{E} \to \mathcal{E}$

Properties of $*$

- Compatibility: $\forall g, g' \in \mathcal{G}\ \forall E \in \mathcal{E} \colon g * (g' * E) = (g \odot g')\, E$
- Identity: $\forall E \in \mathcal{E} \colon i * E = E \Leftrightarrow i$ is the neutral element in $\mathcal{G}$
- Transitivity: $\forall E, E' \in \mathcal{E}\ \exists! g \in \mathcal{G} \colon g * E = E'$

Where are we? II

Notation

For arbitrary $E \in \mathcal{E}$, $g \in \mathcal{G}$ with prime order $p | \#\mathcal{G}$ and $s \in \mathbb{Z}_p$, we denote

$$[s]\, E := g^s * E.$$

Remark

For $s, s' \in \mathbb{Z}_p$ and $E \in \mathcal{E}$, we have

$$[s]\left(\left[s'\right] E\right) = \left[s + s'\right] E.$$

The Group Action Inverse Problem (GAIP)

Given two elements $E, E' \in \mathcal{E}$, find $g \in \mathcal{G}$ with

$$g * E = E'.$$

Secret Sharing Schemes

- Distribute a secret s among shareholders $P_1, \ldots, P_n$ via

$$\mathcal{S}.\mathsf{Share}(s)$$

- Reconstruct a shared secret via

$$\mathcal{S}.\mathsf{Rec}\left(\{s_i\}_{P_i \in S'}\right)$$

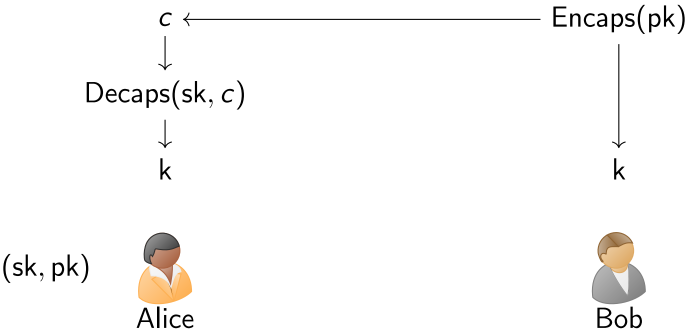
for an authorised set $S' \in \Gamma$.

Definition (Superauthorised Sets)

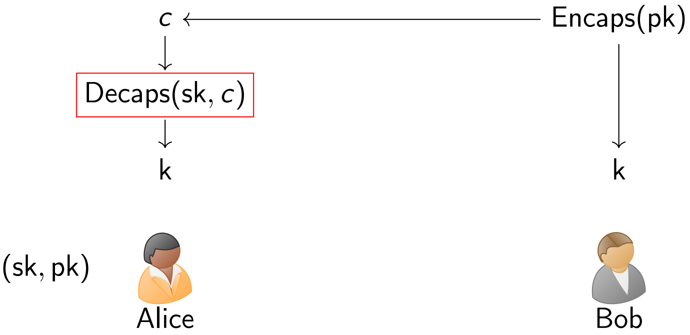
A *superauthorised set* of shareholders is a set S^*, so that

$$\forall P \in S^* \colon S^* \setminus \{P\} \in \Gamma.$$

Key Exchange Mechanisms



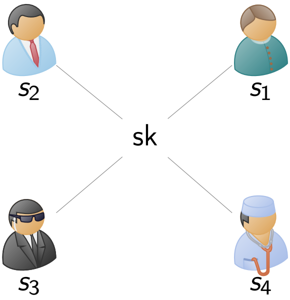
Key Exchange Mechanisms



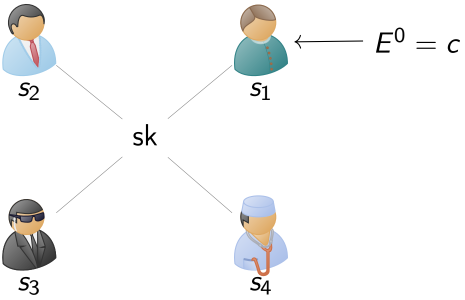
Key Exchange Mechanisms in a HHS

KeyGen()	Encaps(pk)	Decaps(sk, c)
$\mathsf{sk} \leftarrow_{\$} \mathbb{Z}_p$	$b \leftarrow_{\$} \mathcal{G}$	$\mathsf{k} \leftarrow [\mathsf{sk}]\, c$
$\mathsf{pk} \leftarrow [\mathsf{sk}]\, E_0$	$\mathsf{k} \leftarrow b * \mathsf{pk}$	return k
return (sk, pk)	$c \leftarrow b * E_0$	
	return (k, c)	

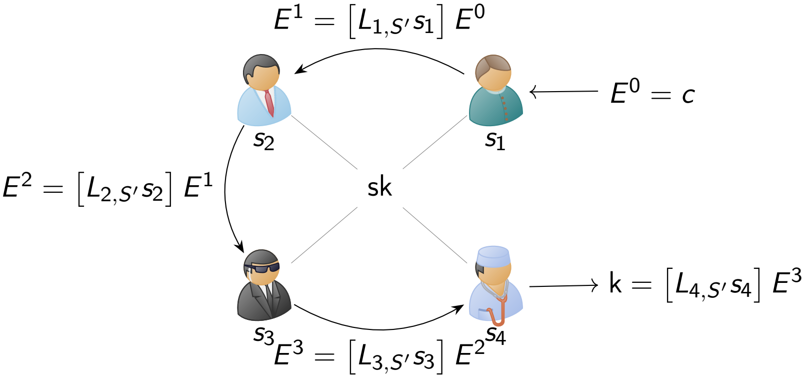
Decapsulation w/ Shared Secret [FM20]



Decapsulation w/ Shared Secret [FM20]



Decapsulation w/ Shared Secret [FM20]



Features of the Protocol

Threshold Group Action

$$E^{\# S'} = \left[L_{j,S'} s_j\right] \left(\left[\ldots\right] E^0\right) = \left[\sum_{P_i \in S'} L_{i,S'} s_i\right] E^0 = [s]\, c.$$

Advantages

- Simulatable
- Authorised set of shareholders suffices
- Turn order is variable

Features of the Protocol

Threshold Group Action

$$E^{\#S'} = \left[L_{j,S'} s_j\right] \left(\left[\ldots\right] E^0\right) = \left[\sum_{P_i \in S'} L_{i,S'} s_i\right] E^0 = [s]\, c.$$

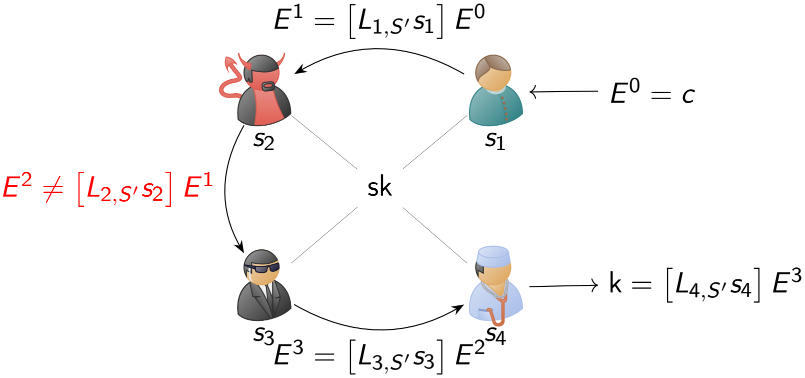
Advantages

- Simulatable
- Authorised set of shareholders suffices
- Turn order is variable

Problem

Passive security: misbehaving shareholders cannot be detected.

A Misbehaving Shareholder



Measures for Active Security

Definition (Zero-knowledge Proof of Knowledge in $(\mathcal{E}, \mathcal{G})$ [BDPV21])

A party proves knowledge of s with

$$[s]\, E_i = E_i'$$

for pairs $(E_i, E_i') \in \mathcal{E}^2$, $i = 1, \ldots, m$.

Definition (Piecewise Verifiable Proof [BKV19])

A party proves knowledge of a polynomial f for a statement

$$x = \left(\left(E_0, E_1\right), s_1, \ldots, s_n\right),$$

where $E_1 = [f(0)]\, E_0$ and $s_i = f(i) \in \mathbb{Z}_p$ for $i = 1, \ldots, n$.

What to do?

- Transfer PVP proof to threshold setting
- Integrate both to decapsulation protocol to achieve active security
- Prove, that resulting protocol is at least as secure as original decapsulation

Key Generation

KeyGen($\mathcal{S}$)

$\mathsf{sk} \leftarrow_\$ \mathbb{Z}_p$

$\mathsf{pk} \leftarrow [\mathsf{sk}]\, E_0$

$\{s_1, \ldots, s_n\} \leftarrow \mathcal{S}\,.\mathsf{Share}(s)$

for $i = 1, \ldots, n$

  $f_i \leftarrow_\$ \mathbb{Z}_p\,[X]_{\leq k-1} : f_i(0) = s_i$

endfor

publish pk

for $i = 1, \ldots, n$

  send $\left\{ s_i, f_i, \{f_j(i)\}_{j=1,\ldots,n} \right\}$ to P_i

endfor

Encapsulation

Encaps(pk)

$b \leftarrow_{\$} \mathcal{G}$

$\mathsf{k} \leftarrow b * \mathsf{pk}$

$c \leftarrow b * E_0$

return (k, c)

Shareholder P_i's Turn in the Decapsulation I

Let S^* be a superauthorised set of shareholders executing the decapsulation protocol.

1. Ascertain $E^{k-1} \in \mathcal{E}$, where E^{k-1} is previous shareholder's output or $E^0 = c$
2. Sample $R_k \leftarrow_{\$} \mathcal{E}$, compute $R'_k \leftarrow [L_{i,S^*} s_i]\, R_k$.
3. Compute and publish

$$\left(\pi^k, \left\{\pi_j^k\right\}_{P_j \in S^*}\right) \leftarrow \mathsf{PVP}.P\Big(i, f_i, S^*, \Big(\left(R_k, R'_k\right), \left(f_i(j)\right)_{P_j \in S^*}\Big)\Big),$$
$$E^k \leftarrow [L_{i,S^*} s_i]\, E^{k-1},$$
$$zk \leftarrow \mathsf{ZK}.P\Big(\left(R_k, R'_k\right), \left(E^{k-1}, E^k\right), L_{i,S^*} s_i\Big).$$

Shareholder P_i's Turn in the Decapsulation II

4. All other participants $P_j \in S^*$ verify

$$\text{PVP}.V\left(i, j, S^*, f_i(j), \left(\pi^k, \pi_j^k\right)\right),$$
$$\text{PVP}.V\left(i, 0, S^*, \left(R_k, R_k'\right), \left(\pi^k, \pi_0^k\right)\right),$$
$$\text{ZK}.V\left(\left(R_k, R_k'\right), \left(E^{k-1}, E^k\right), zk\right).$$

5. If irregularities occur and more than half the participants convict P_i, the protocol is started over without P_i.
6. Decapsulation terminates with the last shareholder's output $E^{\#S^*}$ as result.

Features of our Protocol

- IND-CPA, i.e., the encapsulated key cannot be distinguished from the ciphertext, assuming the hardness of the GAIP
- Simulatable (as was [FM20])
- Actively secure, i.e., a misbehaving shareholder can be detected, if the PVP and ZK proof are sound

Why actively secure signature schemes?

Correctness of a signature is easily verified with the public key and the signed message.
BUT: An incorrect signature does not identify the misbehaving shareholder.

Signature Scheme

- KeyGen: Keep KeyGen of the key exchange mechanism, i.e., the secret key is two-level shared among parties $P_1, \ldots, P_n$
- Sign: Apply Fiat-Shamir-transform [FS87] to the decapsulation protocol, resulting in a signing protocol with secret shared secret key
- Vf: Arises naturally from the Fiat-Shamir-transformation

Necessary Characteristics for Compatibility

- Independent reconstruction: a shareholder's input in reconstructing a secret is independent of other shares
- Self-contained reconstruction: the shares of a secret live in the same space as the secret to enable two-level sharing
- Compatibility with zero-knowledge proof and the piecewise verifiable proof in the HHS

Examples

- Shamir's polynomial secret sharing: compatible (our protocol was initially based on it)
- Tassa's hierarchical threshold secret sharing [Tas04]: compatible (extension of Shamir's approach)
- Damgard and Thorbek's linear integer secret sharing [DT06]: incompatible, since it is only computationally hiding
- Additive secret sharing: incompatible, because superauthorised sets of shareholders do not exist

Conclusion

- Transfer PVP to threshold setting
- Actively secure key exchange mechanism
- Transformed into signature scheme
- Define, which field of secret sharing schemes is compatible

Ward Beullens, Lucas Disson, Robi Pedersen, and Frederik Vercauteren, *CSI-RAShi: distributed key generation for CSIDH*, Post-Quantum Cryptography - 12th International Workshop, PQCrypto 2021, Daejeon, South Korea, July 20-22, 2021, Proceedings (Jung Hee Cheon and Jean-Pierre Tillich, eds.), Lecture Notes in Computer Science, vol. 12841, Springer, 2021, pp. 257–276.

Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren, *CSI-FiSh: efficient isogeny based signatures through class group computations*, Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I (Steven D. Galbraith and Shiho Moriai, eds.), Lecture Notes in Computer Science, vol. 11921, Springer, 2019, pp. 227–247.

Jean Marc Couveignes, *Hard homogeneous spaces*, IACR Cryptol. ePrint Arch. (2006), 291.

Ivan Damgård and Rune Thorbek, *Linear integer secret sharing and distributed exponentiation*, Public Key Cryptography - PKC 2006, 9th International Conference on Theory and Practice of Public-Key Cryptography, New York, NY, USA, April 24-26, 2006, Proceedings (Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, and Tal Malkin, eds.), Lecture Notes in Computer Science, vol. 3958, Springer, 2006, pp. 75–90.

Luca De Feo and Michael Meyer, *Threshold schemes from isogeny assumptions*, Public-Key Cryptography - PKC 2020 - 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4-7, 2020, Proceedings, Part II (Aggelos Kiayias, Markulf Kohlweiss, Petros Wallden, and Vassilis Zikas, eds.), Lecture Notes in Computer Science, vol. 12111, Springer, 2020, pp. 187–212.

Amos Fiat and Adi Shamir, *How to prove yourself: Practical solutions to identification and signature problems*, 1987, pp. 186–194.

Tamir Tassa, *Hierarchical threshold secret sharing*, Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings (Moni Naor, ed.), Lecture Notes in Computer Science, vol. 2951, Springer, 2004, pp. 473–490.