Malleable Commitments from Group Actions and Zero-Knowledge Proofs for Circuits based on Isogenies

Mingjie Chen, Yi-Fu Lai, **Abel Laval**, Laurane Marco, Christophe Petit

October 15, 2023

Overview

Asymmetric cryptography allows for a wide variety of schemes with interesting features :

- Threshold signatures
- Fully Homomorphic Encryption
- Zero-knowledge proofs
- Oblivious transfer
- Verifiable Delay Functions
- *etc...*

Asymmetric cryptography allows for a wide variety of schemes with interesting features :

- Threshold signatures
- Fully Homomorphic Encryption
- Zero-knowledge proofs
- Oblivious transfer
- Verifiable Delay Functions
- *etc...*

Problem : Shor's algorithm

Asymmetric cryptography allows for a wide variety of schemes with interesting features :

- Threshold signatures
- Fully Homomorphic Encryption
- Zero-knowledge proofs
- Oblivious transfer
- Verifiable Delay Functions
- *etc...*

- Lattices
- Codes
- Isogenies
- Multivariates polynomials
- Hash functions

Problem : Shor's algorithm

Overview

Asymmetric cryptography allows for a wide variety of schemes with interesting features :

- Threshold signatures
- Fully Homomorphic Encryption
- **Zero-knowledge proofs**
- Oblivious transfer
- Verifiable Delay Functions
- *etc...*

- Lattices
- Codes
- **Isogenies**
- Multivariates polynomials
- Hash functions

Problem : Shor's algorithm

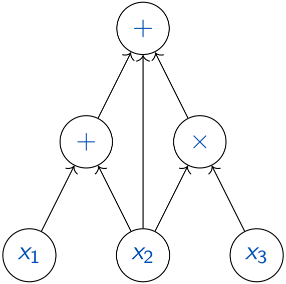
Proofs of knowledge, but... knowledge of what ?
of everything !

Proofs of knowledge, but... knowledge of what ?
of everything !

How ?

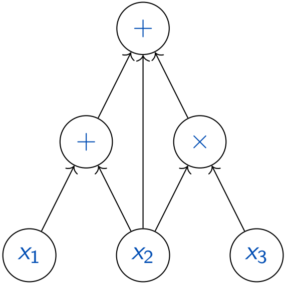
1. Construct a proof of knowledge for a NP-complete statement.
2. Reduce any other NP problem to this.

An arithmetic circuit encodes a polynomial.



$\simeq (x_1 + x_2) + x_2 + x_2 x_3$

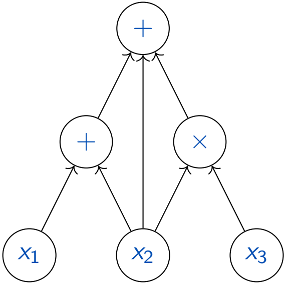
An arithmetic circuit encodes a polynomial.



$\simeq (x_1 + x_2) + x_2 + x_2 x_3$

- The SAT problem for arithmetic circuit :
  Given a polynomial f and an output value s, are there input values $x_1, \cdots, x_n$ such that $f(x_1, \cdots, x_n) = s$?

An arithmetic circuit encodes a polynomial.



$\simeq (x_1 + x_2) + x_2 + x_2 x_3$

- The SAT problem for arithmetic circuit :
  Given a polynomial f and an output value s, are there input values $x_1, \cdots, x_n$ such that $f(x_1, \cdots, x_n) = s$?

Theorem

The satisfiability problem for arithmetic circuits is NP-complete.

Commitment Schemes

Definition (Commitment Scheme)

A *commitment scheme* is a tuple $(\mathcal{M}, \mathcal{R}, \mathcal{C}, \text{Commit}, \text{Verify})$ where $\text{Commit} : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$ and $\text{Verify} : \mathcal{M} \times \mathcal{R} \times \mathcal{C} \to \{0, 1\}$ are PPTA algorithms

Commitment Schemes

Definition (Commitment Scheme)

A *commitment scheme* is a tuple $(\mathcal{M}, \mathcal{R}, \mathcal{C}, \mathsf{Commit}, \mathsf{Verify})$ where $\mathsf{Commit} : \mathcal{M} \times \mathcal{R} \to \mathcal{C}$ and $\mathsf{Verify} : \mathcal{M} \times \mathcal{R} \times \mathcal{C} \to \{0, 1\}$ are PPTA algorithms

Related security notions :

Hiding

An attacker cannot retrieve m or r from c.

Binding

It's hard to find $(m, r) \neq (m', r')$ that give the same commitment.

Homomorphism and malleability

- Efficient solutions use homomophic property :

$$\forall m, m', r, r', \;\; \mathsf{Commit}(m + m', r + r') = \mathsf{Commit}(m, r) \cdot \mathsf{Commit}(m', r')$$

Homomorphism and malleability

- Efficient solutions use homomophic property :

$$\forall m, m', r, r', \;\; \mathrm{Commit}(m + m', r + r') = \mathrm{Commit}(m, r) \cdot \mathrm{Commit}(m', r')$$

- Too restrictive for isogenies $\rightsquigarrow$ Relaxed notion : *malleability*.

Homomorphism and malleability

- Efficient solutions use homomophic property :

$$\forall m, m', r, r', \;\; \mathsf{Commit}(m + m', r + r') = \mathsf{Commit}(m, r) \cdot \mathsf{Commit}(m', r')$$

- Too restrictive for isogenies $\rightsquigarrow$ Relaxed notion : *malleability*.

Definition (Malleable commitment)

A commitment scheme is malleable if :
Given a single commitment, we can derive a related second one.

Homomorphism and malleability

- Efficient solutions use homomophic property :

$$\forall m, m', r, r', \quad \mathsf{Commit}(m + m', r + r') = \mathsf{Commit}(m, r) \cdot \mathsf{Commit}(m', r')$$

- Too restrictive for isogenies $\rightsquigarrow$ Relaxed notion : *malleability*.

Definition (Malleable commitment)

A commitment scheme is malleable if :
Given a single commitment, we can derive a related second one.

We assume no structure *a priori*.

Group Action Malleable Commitment

An *GAMC* is a commitment scheme exploiting additional structure for $\mathcal{M}$ and $\mathcal{R}$.

Group Action Malleable Commitment

An *GAMC* is a commitment scheme exploiting additional structure for $\mathcal{M}$ and $\mathcal{R}$.

Definition

A GAMC is a commitment scheme satisfying :

- $\mathcal{M}$ and $\mathcal{R}$ are groups. $\mathcal{C}$ is a set.
- We have a group action $\star : (\mathcal{M} \times \mathcal{R}) \times \mathcal{C} \to \mathcal{C}$
- $C_0 := \mathsf{Commit}(0_{\mathcal{M}}, 0_{\mathcal{R}})$
- $\mathsf{Commit}(m, r) := (m, r) \star C_0$.
- $(m', r') \star \mathsf{Commit}(m, r) = \mathsf{Commit}(m + m', r + r')$

Group Action Malleable Commitment

An *GAMC* is a commitment scheme exploiting additional structure for $\mathcal{M}$ and $\mathcal{R}$.

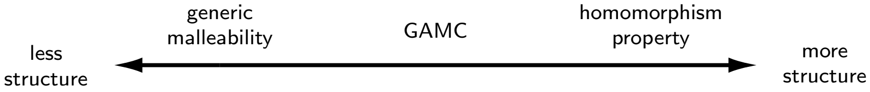
Definition

A GAMC is a commitment scheme satisfying :

- $\mathcal{M}$ and $\mathcal{R}$ are groups. $\mathcal{C}$ is a set.
- We have a group action $\star : (\mathcal{M} \times \mathcal{R}) \times \mathcal{C} \to \mathcal{C}$
- $C_0 := \mathsf{Commit}(0_{\mathcal{M}}, 0_{\mathcal{R}})$
- $\mathsf{Commit}(m, r) := (m, r) \star C_0$.
- $(m', r') \star \mathsf{Commit}(m, r) = \mathsf{Commit}(m + m', r + r')$

In our case :

- $\mathcal{M}$ and $\mathcal{R}$ are groups of isogenies (with composition).
- $\mathcal{C}$ is a set of elliptic curves (up to isomorphism).



How to use GAMC

Several GAMC ⇝ Proof systems for additions and multiplications ⇝ Proof system for arithmetic circuits

- CSIDH (for *Commutative Supersingular Isogeny Diffie-Hellman*) is a key agreement protocol.
- Analog of the Diffie-Hellman for isogenies.

- CSIDH (for *Commutative Supersingular Isogeny Diffie-Hellman*) is a key agreement protocol.
- Analog of the Diffie-Hellman for isogenies.

Diffie-Hellman	CSIDH
$\xrightarrow{g^a}$	$\xrightarrow{\mathfrak{a}\cdot E_0}$
$\xleftarrow{g^b}$	$\xleftarrow{\mathfrak{b}\cdot E_0}$
$g^{ab} = g^{ba}$	$\mathfrak{ab} \cdot E_0 = \mathfrak{ba} \cdot E_0$

- CSIDH (for *Commutative Supersingular Isogeny Diffie-Hellman*) is a key agreement protocol.
- Analog of the Diffie-Hellman for isogenies.

Diffie-Hellman	CSIDH
$\xrightarrow{g^a}$	$\xrightarrow{\mathfrak{a}\cdot E_0}$
$\xleftarrow{g^b}$	$\xleftarrow{\mathfrak{b}\cdot E_0}$
$g^{ab} = g^{ba}$	$\mathfrak{ab} \cdot E_0 = \mathfrak{ba} \cdot E_0$

- $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{C}\ell(\mathcal{O})$: the *ideal class group* (of $\mathbb{Z}[\pi]$).
- E_0 is a curve in SS_p : the set of supersingular curves "over $\mathbb{F}_p$".

An instance of an GAMC

In the CSIDH setting :

- $\mathcal{M} = \mathcal{R} := \mathcal{C}\ell(\mathcal{O})$ are groups (of ideals).
- $\mathcal{C} := \mathsf{SS}_p \times \mathsf{SS}_p$.
- $C_0 := (E_0, E_1)$

Malleability is given by

$$(\mathfrak{m}, \mathfrak{r}) \star (E, E') := (\mathfrak{r} \cdot E, \mathfrak{m}\mathfrak{r} \cdot E')$$

Conclusion

Contributions :

- New framework for generic NP statements ZK proofs.
- Proof-of-concept construction.

Performances :

- Strong security assumptions and no trusted setup.
- Proof system for an arithmetic circuit $= O(|\mathcal{M}|)$ malleability computations.
- Size of the proof $= O(\lambda|\mathcal{M}|)$ bits.

Future work :

- Cannot use higher security parameters than CSIDH-512.
- The size of the message space is limited.