Compressed Σ-Protocols for Bilinear Group Arithmetic Circuits

and Application to Logarithmic Transparent Threshold Signatures

Thomas Attema and Ronald Cramer and Matthieu Rambaud

Asiacrypt - December 10, 2021

Setting - Proving General Constraints in Zero-Knowledge

ZK for General Constraint-Satisfiability:

- *Prove knowledge of commitment opening x such that $f(x) = 0$; i.e., x is f-constrained.*
- *Zero-Knowledge (ZK): no info released except veracity of claim.*

Goal:

- Low communication *for general f: minimize number of bits transmitted.*

Computation Model:

- Oftentimes the constraints f is described by an arithmetic circuit C.
- Sometimes other computation models are more natural.

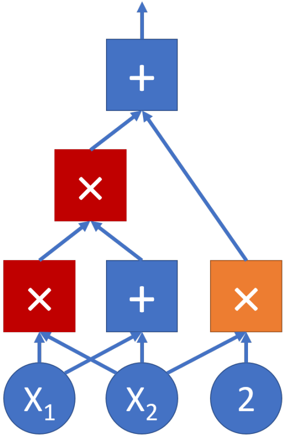
Computation Model: Arithmetic Circuits

Defined over: A finite field $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$.

Wire values: $\mathbb{Z}_q$-elements

Gates:

- Addition
- Multiplication



Computation Model: Bilinear Group (Arithmetic) Circuits

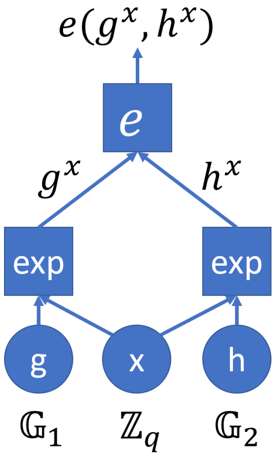
Defined over: A bilinear group $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H)$:

- Prime q
- Order q groups $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$
- Bilinear map (pairing) $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$
- Generators $G \in \mathbb{G}_1$, $H \in \mathbb{G}_2$ and $e(G, H) \in \mathbb{G}_T$

Wire values: $\mathbb{Z}_q$, $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_T$ elements

Gates:

- $\mathbb{Z}_q$-Addition, $\mathbb{G}_*$-Multiplication
- $\mathbb{Z}_q$-Multiplication
- Group exponentiation
- Pairings



Arithmetic Circuits vs. Bilinear Group Arithmetic Circuits (1/2)

$\Longrightarrow$ Arithmetic circuits are bilinear group arithmetic circuits.

$\Longleftarrow$ Bilinear group arithmetic circuits can be *expressed* as arithmetic circuits.

This requires:

1. Group elements to be represented as (vectors of) field elements.
2. Exponentiation and pairing gates to be expressed as arithmetic operations.

Arithmetic Circuits vs. Bilinear Group Arithmetic Circuits (2/2)

Reducing a Bilinear Circuit to an arithmetic circuit increases its size.

- Reductions are different for all bilinear groups.
- The blow-up is a constant factor $\implies$ asymptotic complexities of ZKPs are preserved.
- But the constant factor can be large, significantly influencing concrete efficiency.
  - E.g., a single group exponentiation in a highly optimized group of order $q \approx 2^{256}$ requires ≈ 800 $\mathbb{Z}_q$-multiplication gates [HBHW20].

This Work

A direct approach for communication-efficient ZKPs for Bilinear Group Arithmetic Circuits

Our approach: Avoids specialized reductions from *bilinear group arithmetic circuits* to arithmetic circuits.

- Conceptual Simplicity.
- Improved concrete efficiency.

An Application: Transparent and succinct threshold signature scheme.

Prior Work

Arithmetic Circuit ZKPs with logarithmic communication.

- **Bulletproofs [BCC$^+$16, BBB$^+$18]**
  - At its core: Recursive PoK for *quadratic* relations.
  - Presented as a replacement for Σ-Protocol Theory.
- **Compressed Σ-Protocols [AC20]**
  - Reconciliation of Bulletproofs and Σ-Protocols.

ZKPs for Bilinear Group Arithmetic Circuits.

- **Lai et al. [LMR19]**
  - Generalization of bulletproofs.
  - Direct approach; does not require reduction to arithmetic circuit.
  - Only applicable to a subclass circuits.

Our Approach:

Generalize Compressed Σ-Protocols to the Bilinear Circuit Model.

Compared to Lai et al. [LMR19]:

- Conceptual simplicity; our basic building block handles *linear* relations.
- Our approach works for *arbitrary* bilinear group arithmetic circuits.
- We improve the communication efficiency by roughly a factor 3.

Prior Work - Compressed Σ-Protocol Theory (CRYPTO 2020 [AC20])

High-Level Paradigm:

$\boxed{\textit{Solve linear instances first, and then linearize the non-linear instances.}}$

1. Natural Σ-protocol for *linear* constraints.
   - Σ-protocol theory is a well-established, widely-used basis for zero-knowledge proofs.
   - E.g., general-constraint ZK: $O(|C|) \cdot \kappa$ communication [CD97].
2. Adaptation of Bulletproof PoK [BCC+16, BBB+18].
   - Bulletproofs core: recursive PoK for *quadratic* relations $\implies$ logarithmic communication.
   - Repurposed as a *blackbox* compression for Σ-protocol 1.

$$[\mathbf{x}] \text{ s.t. } L(\mathbf{x}) = y$$

$$\begin{array}{ccc}
\mathcal{P} & & \mathcal{V} \\
 & \xrightarrow{[\mathbf{r}], L(\mathbf{r})} & \\
 & \xleftarrow{c} & \\
\mathbf{z} = \mathbf{r} + c\mathbf{x} & \xrightarrow{\mathbf{z}} & \text{Accept?}
\end{array}$$

Prior Work - Compressed Σ-Protocol Theory (CRYPTO 2020 [AC20])

3. Linearization strategy to handle non-linear constraints in a black-box manner.
   - Using arithmetic secret-sharing.

4. Instantiations.
   - *Logarithmic-communication*: DL, strong-RSA in class groups, (RSA + set-up)
   - *Constant-communication*: Knowledge of Exponent Assumption
   - *Polylogarithmic-communication*: Ring-SIS [ACK21]

5. Computation Model.
   - Constraints $f(x) = 0$ are expressed as an **arithmetic circuit**.

Generalized Compressed Σ-Protocol - Linear Constraints

Observation:
Compressed Σ-protocols for linear constraints can be viewed as proving knowledge of the preimage of a homomorphism

$$\Psi : \mathbb{G}^n \to \mathbb{H}$$

- $\mathbb{G}$ and $\mathbb{H}$ are order q groups.
- Communication: logarithmic number of $\mathbb{H}$-elements.

In [AC20], Ψ is of the form:

$$\Psi : \mathbb{Z}_q^n \times \mathbb{Z}_q \to \mathbb{G} \times \mathbb{Z}_q, \quad (\mathbf{x}, \gamma) \to (\textsc{Com}(\mathbf{x}, \gamma), L(\mathbf{x}))\,,$$

Crucial: $\textsc{Com}$ is a *homomorphic* and *compact* commitment scheme.

We need a homomorphic and compact commitment scheme for vectors in

$$\mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2} \times \mathbb{G}_T^{n_T}\,.$$

Commitment Scheme - Bilinear Group Vectors (1/3)

- Bilinear group: $(q, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e, G, H)$
- Pairing: $e\colon \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$

Pairing-based generalization of Pedersen Commitments [AFG$^+$10, LMR19]:

Setup:

- $g, h \leftarrow \mathbb{G}_T$
- $H \leftarrow \mathbb{G}_2$

Commit to an element $(x, y) \in \mathbb{Z}_q \times \mathbb{G}_1$:

$$\textsc{Com} : \mathbb{Z}_q \times \mathbb{G}_1 \times \mathbb{Z}_q \to \mathbb{G}_T,\ (x, y, \gamma) \mapsto h^\gamma \cdot g^x \cdot e(y, H)\,.$$

Commitment Scheme - Bilinear Group Vectors (2/3)

Commit to an element $(x, y) \in \mathbb{Z}_q \times \mathbb{G}_1$:

$$\textsc{Com} : \mathbb{Z}_q \times \mathbb{G}_1 \times \mathbb{Z}_q \to \mathbb{G}_T, \ (x, y, \gamma) \mapsto h^\gamma \cdot g^x \cdot e(y, H)\,.$$

Extensions:

1. Natural extension to vectors $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1}$.
   - Homomorphic.
   - Compact: Commitment is 1 $\mathbb{G}_T$-element, i.e., size independent of n_0 and n_1.
2. Extension to vectors $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2}$.
   - Binding: Some care is required.
   - Homomorphic.
   - Compact: Commitment is 2 $\mathbb{G}_T$-elements.

$\Longrightarrow$ Compressed Σ-Protocols for $(\mathbb{Z}_q, \mathbb{G}_1, \mathbb{G}_2)$-vectors.

Commitment Scheme - Bilinear Group Vectors (3/3)

The above approach does not enable commitments to $\mathbb{G}_T$-coefficients.

El-Gamal based commitment scheme for $\mathbb{G}_T$-vectors:

$$\textsc{Com}\colon \mathbb{G}_T^{n_T} \times \mathbb{Z}_q \to \mathbb{G}_T^{n_T+1}, \quad (\mathbf{x}, \gamma) \mapsto \begin{pmatrix} h^{\gamma} \\ \mathbf{x} * \mathbf{g}^{\gamma} \end{pmatrix}$$

$\Longrightarrow$ commitment scheme for vectors $\mathbf{x} \in \mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2} \times \mathbb{G}_T^{n_T}$

Commitment Size: $n_T + 3$ $\mathbb{G}_T$-elements.

- Independent of n_0, n_1 and n_2.
- Linear in n_T.

Compressed Σ-Protocol - Linear Bilinear Group Relations

$\Longrightarrow$ Compressed Σ-protocol for vectors $\mathbf{x} \in \mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2} \times \mathbb{G}_T^{n_T}$.

Communication costs:

- Logarithmic in n_0, n_1 and n_2.
- Linear in n_T.

Linearizing Non-Linear Gates (1/2)

Arithmetic Circuits

- Arithmetic secret sharing based technique to linearize non-linear multiplication gates [AC20]:

$$\mathbb{Z}_q \times \mathbb{Z}_q \to \mathbb{Z}_q, \quad (x, y) \mapsto x \cdot y$$

Bilinear Group Arithmetic Circuits

- Multiple types of non-linear gates:

$$\begin{aligned}
\mathbb{Z}_q \times \mathbb{Z}_q &\to \mathbb{Z}_q, & (x, y) &\mapsto x \cdot y \\
\mathbb{G}_1 \times \mathbb{Z}_q &\to \mathbb{G}_1, & (g, x) &\mapsto g^x \\
\mathbb{G}_2 \times \mathbb{Z}_q &\to \mathbb{G}_2, & (h, x) &\mapsto h^x \\
\mathbb{G}_T \times \mathbb{Z}_q &\to \mathbb{G}_T, & (k, x) &\mapsto k^x \\
\mathbb{G}_1 \times \mathbb{G}_2 &\to \mathbb{G}_T, & (x, y) &\mapsto e(g, h)
\end{aligned}$$

Linearizing Non-Linear Gates (2/2)

Observation

- All these non-linear gates are bilinear mappings
  $\Longrightarrow$ Linearization techniques of [AC20] have a generalization to these bilinear gates.

$\Longrightarrow$ Compressed Σ-protocol for vectors $\mathbf{x} \in \mathbb{Z}_q^{n_0} \times \mathbb{G}_1^{n_1} \times \mathbb{G}_2^{n_2} \times \mathbb{G}_T^{n_T}$ satisfying *arbitrary* constraints defined over a bilinear group arithmetic circuit.

Communication costs:

- Logarithmic in
  - n_0, n_1 and n_2
  - the number of non-linear gates with $\mathbb{Z}_q$, $\mathbb{G}_1$ or $\mathbb{G}_2$ outputs
- Linear in
  - n_T
  - the number of non-linear gates with $\mathbb{G}_T$ outputs

Application - Threshold Signatures (1/2)

Functionality: A valid signature can only be created by a subset of at least k-out-of-n players.

Trivial approach: Exhibit k individual signatures.

- Signature size *linear* in k.
- Reveals the identities of the k signers.

Standard approach [Sho00]: Secret share the private key of a standard signature scheme.

- Signature size *constant* in k and n.
- Trusted set-up required.
- Hides the identities of the k signers.

Application - Threshold Signatures (2/2)

Our approach: Zero-Knowledge Proof of Knowledge of k-out-of-n signatures.

Ingredients:

- BLS signature scheme [BLS01]: small bilinear group verification circuit.
- Proofs-of-partial knowledge: k-out-of-n threshold functionality [ACF21].
- Compressed Σ-Protocols for bilinear group arithmetic relations.

Properties:

- Signature size *logarithmic* in n.
- Transparent set-up.
- Hides the identities of the k signers.

Conclusion

$\boxed{\text{Compressed } \Sigma\text{-protocols for bilinear group arithmetic circuits.}}$

- Direct approach: no specialized reduction to arithmetic circuits.

Communication costs:

- Logarithmic in the "$\mathbb{Z}_q$, $\mathbb{G}_1$ and $\mathbb{G}_2$ parts".
- Linear in the "$\mathbb{G}_T$ part".
- Roughly factor 3 improvement over prior work.

Application:

- Transparent and logarithmic-size threshold signature scheme.

Thanks!

Bibliography I

Thomas Attema and Ronald Cramer.
Compressed sigma-protocol theory and practical application to plug & play secure algorithmics.
In *CRYPTO (3)*, volume 12172 of *Lecture Notes in Computer Science*, pages 513–543. Springer, 2020.

Thomas Attema, Ronald Cramer, and Serge Fehr.
Compressing proofs of k-out-of-n partial knowledge.
In *CRYPTO (4)*, volume 12828 of *Lecture Notes in Computer Science*, pages 65–91. Springer, 2021.

Thomas Attema, Ronald Cramer, and Lisa Kohl.
A compressed sigma-protocol theory for lattices.
In *CRYPTO (2)*, volume 12826 of *Lecture Notes in Computer Science*, pages 549–579. Springer, 2021.

Masayuki Abe, Georg Fuchsbauer, Jens Groth, Kristiyan Haralambiev, and Miyako Ohkubo.
Structure-preserving signatures and commitments to group elements.
In *CRYPTO*, volume 6223 of *Lecture Notes in Computer Science*, pages 209–236. Springer, 2010.

Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Gregory Maxwell.
Bulletproofs: Short proofs for confidential transactions and more.
In *IEEE Symposium on Security and Privacy*, pages 315–334. IEEE Computer Society, 2018.

Bibliography III

Jonathan Bootle, Andrea Cerulli, Pyrros Chaidos, Jens Groth, and Christophe Petit.
Efficient zero-knowledge arguments for arithmetic circuits in the discrete log setting.
In *EUROCRYPT (2)*, volume 9666 of *Lecture Notes in Computer Science*, pages 327–357. Springer, 2016.

Dan Boneh, Ben Lynn, and Hovav Shacham.
Short signatures from the weil pairing.
In *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 514–532. Springer, 2001.

Ronald Cramer and Ivan Damgård.
Linear zero-knowledge - A note on efficient zero-knowledge proofs and arguments.
In *STOC*, pages 436–445. ACM, 1997.

Daira Hopwood, Sean Bowe, Taylor Hornby, and Nathan Wilcox.
Zcash Protocol Specication - Version 2020.1.7, 2020.

Bibliography IV

Russell W. F. Lai, Giulio Malavolta, and Viktoria Ronge.
Succinct arguments for bilinear group arithmetic: Practical structure-preserving cryptography.
In *ACM Conference on Computer and Communications Security*, pages 2057–2074. ACM, 2019.

Victor Shoup.
Practical threshold signatures.
In *EUROCRYPT*, volume 1807 of *Lecture Notes in Computer Science*, pages 207–220. Springer, 2000.