# Strongly Multiplicative Ramp Schemes From High Degree Rational Points on Curves

**Hao Chen**
East China Normal University

**Ronald Cramer**
CWI & Leiden University

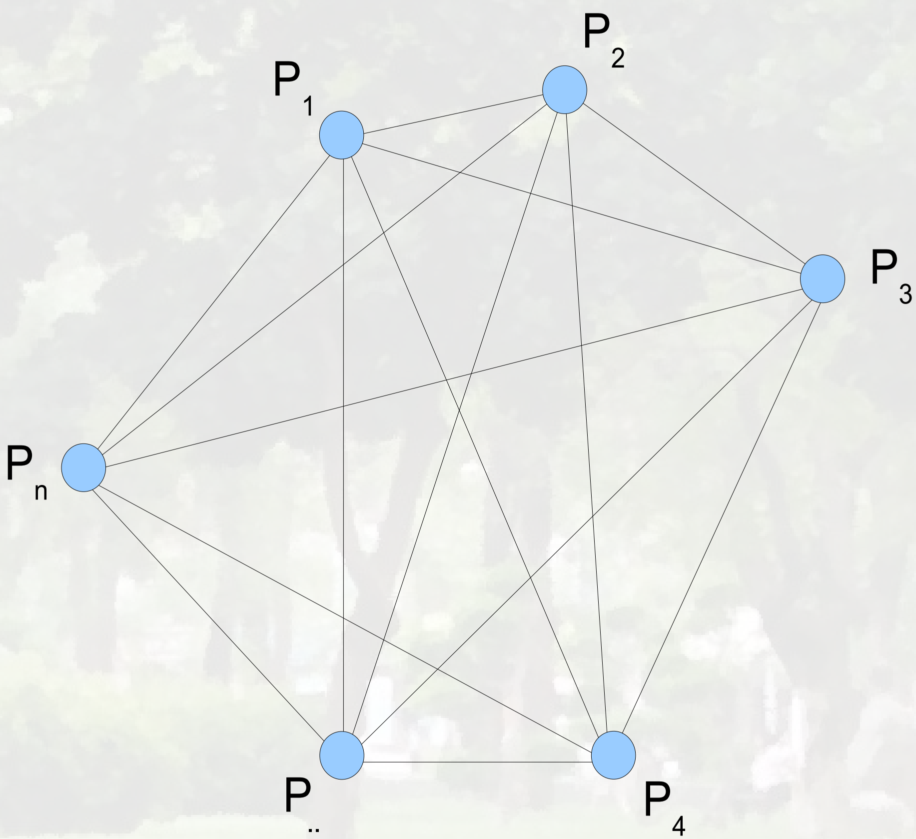
**Robbert de Haan**
CWI

**Ignacio Cascudo Pueyo**
Oviedo University

# Overview

- Multi-Party Computation
  - Model
  - Goal
- Applications
- Basic construction
- Recent improvements
- Our results

# Multi-Party Computation: Model




- *n* players
- Perfectly authenticated secure channels
- Authenticated broadcast
- Players computationally unbounded
- *t*-Adversary jointly controls up to *t* players
  - passively, or
  - actively.

# Multi-Party Computation: Goal

- Computing a function $F \in K[X_1,..,X_n]$ on the inputs of the $n$ players with
  - perfect privacy, and
  - perfect correctness (zero-error).

# Multi-Party Computation: Goal

- Computing a function $F \in K[X_1,..,X_n]$ on the inputs of the $n$ players with
  - perfect privacy, and
  - perfect correctness (zero-error).
- $t$-Adversary jointly controls up to $t$ players
  - passively (eavesdropping only), or
  - actively (deviates from the protocol).

# Multi-Party Computation: Goal

- Computing a function $F \in K[X_1,..,X_n]$ on the inputs of the $n$ players with
  - perfect privacy, and
  - perfect correctness (zero-error).
- $t$-Adversary jointly controls up to $t$ players
  - passively (eavesdropping only), or
  - actively (deviates from the protocol).
- Existence such protocols:
  - For a passive $t$-adversary if and only if $t<n/2$.
  - For an active $t$-adversary if and only if $t<n/3$.

# Recently Found Connections

- Zero-knowledge from zero-error MPC (IKOS07):
  - Idea:
    - Let the prover run an MPC protocol that verifies a witness.
    - Let the verifier randomly open some views to verify correctness.
  - Example result: Near constant-rate ZK when one can use bounded fan-in verification circuits.

# Recently Found Connections

- Zero-knowledge from zero-error MPC (IKOS07):
  - Idea:
    - Let the prover run an MPC protocol that verifies a witness.
    - Let the verifier randomly open some views to verify correctness.
- OT combiners from MPC (HIKN08):
  - Idea:
    - Two parties together emulate *n* pairs of players that each use one of the candidate combiners.
    - Faulty combiners correspond to corrupt players in the MPC.
  - Example result: Constant-rate OTs from a noisy channel.

# Recently Found Connections

- Zero-knowledge from zero-error MPC (IKOS07):
  - Idea:
    - Let the prover run an MPC protocol that verifies a witness.
    - Let the verifier randomly open some views to verify correctness.
- OT combiners from MPC (HIKN08):
  - Idea:
    - Two parties together emulate *n* pairs of players that each use one of the candidate combiners.
    - Faulty combiners correspond to corrupt players in the MPC.
- Communication cost of these protocols is proportional to communication cost of the underlying MPC protocol.
  - => We want low communication MPC!

# Basic Construction: Linear Secret Sharing

- Shamir secret sharing:
  - Secret $s \in K$ and $x_1, x_2, \ldots, x_n \in K$ non-zero, distinct.
  - Degree-$t$ polynomial $f \in K[X]$ with $f(0)=s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.

# Basic Construction: Linear Secret Sharing

- Shamir secret sharing:
  - Secret $s \in K$ and $x_1,x_2,\ldots,x_n \in K$ non-zero, distinct.
  - Degree-$t$ polynomial $f \in K[X]$ with $f(0)=s$.
  - Shares $f(x_1)$, $f(x_2)$, ..., $f(x_n)$.
- Linearity:
  - Shares for $s$ and $u \rightarrow$ shares for $s+u$.
  - Shares for $s$, constant $c \rightarrow$ shares for $cs$.

# Basic Construction: Linear Secret Sharing

- Shamir secret sharing:
  - Secret $s \in K$ and $x_1, x_2, \ldots, x_n \in K$ non-zero, distinct.
  - Degree-$t$ polynomial $f \in K[X]$ with $f(0)=s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.
- Linearity:
  - Shares for $s$ and $u \rightarrow$ shares for $s+u$.
  - Shares for $s$, constant $c \rightarrow$ shares for $cs$.
- Multiplication property for $t < n/2$:
  - $su = \sum \eta_i f(x_i) g(x_i)$ (where $g$ degree-$t$ with $g(0)=u$).

# Basic Construction: Linear Secret Sharing

- Shamir secret sharing:
  - Secret $s \in K$ and $x_1, x_2, \ldots, x_n \in K$ non-zero, distinct.
  - Degree-$t$ polynomial $f \in K[X]$ with $f(0)=s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.
- Linearity:
  - Shares for $s$ and $u$ $\rightarrow$ shares for $s+u$.
  - Shares for $s$, constant $c$ $\rightarrow$ shares for $cs$.
- Multiplication property for $t < n/2$:
  - $su = \sum \eta_i f(x_i)g(x_i)$ (where $g$ degree-$t$ with $g(0)=u$).
- Strong multiplication property for $t < n/3$.
  - Multiplication property on subsets with any $n$-$t$ players.

# Multi-Party Computation from LSSS

- Passive adversary protocol steps:
  - Every player secret shares his input using the selected secret sharing scheme.
  - Players locally perform addition and multiplication with a constant on the values.
  - Players interact to perform multiplications using the multiplication property.

# Multi-Party Computation from LSSS

- Passive adversary protocol steps:
  - Every player secret shares his input using the selected secret sharing scheme.
  - Players locally perform addition and multiplication with a constant on the values.
  - Players interact to perform multiplications using the multiplication property.
- Active adversary requires additional verification steps for secret sharing and multiplication
  - Can be bootstrapped from *strongly* multiplicative secret sharing schemes.

# Limitations Shamir-based MPC

- Size shares $\geq$ size secret.
  - Unavoidable for perfect secret sharing schemes.

# Limitations Shamir-based MPC

- Size shares ≥ size secret.
  - Unavoidable for perfect secret sharing schemes.
- $|K| = o(n)$.
  - Unavoidable for ideal threshold secret sharing schemes, due to correspondence with MDS codes.

# Limitations Shamir-based MPC

- Size shares ≥ size secret.
  - Unavoidable for perfect secret sharing schemes.
- $|K| = o(n)$.
  - Unavoidable for ideal threshold secret sharing schemes, due to correspondence with MDS codes.

- Note that the communication complexity of a multi-party computation protocol is proportional to the efficiency of the underlying secret sharing scheme.

# Limitations Shamir-based MPC

- Size shares ≥ size secret.
  - Unavoidable for perfect secret sharing schemes.
- $|K| = o(n)$.
  - Unavoidable for ideal threshold secret sharing schemes, due to correspondence with MDS codes.
- Note that the communication complexity of a multi-party computation protocol is proportional to the efficiency of the underlying secret sharing scheme.
- We consider several *ramp schemes* that get around one or both of these limitations.

# Recent Efficient Ramp Schemes

- Exploiting the structure of the function *F*:
  - Franklin and Yung 1991 (parallel multiplications)
  - CDH 2007 (extension field multiplication)

# Recent Efficient Ramp Schemes

- Exploiting the structure of the function *F*:
  - Franklin and Yung 1991 (parallel multiplications)
  - CDH 2007 (extension field multiplication)
- Enabling small fields:
  - Chen and Cramer 2006 (algebraic geometry codes)
  - CCGHV 2007 (arbitrary error correcting codes)

# Recent Efficient Ramp Schemes

- Exploiting the structure of the function *F*:
  - Franklin and Yung 1991 (parallel multiplications)
  - CDH 2007 (extension field multiplication)
- Enabling small fields:
  - Chen and Cramer 2006 (algebraic geometry codes)
  - CCGHV 2007 (arbitrary error correcting codes)

*generalizes*

# Recent Efficient Ramp Schemes

- Exploiting the structure of the function *F*:
  - Franklin and Yung 1991 (parallel multiplications)
  - CDH 2007 (extension field multiplication) ?
- Enabling small fields:
  - Chen and Cramer 2006 (algebraic geometry codes)
  - CCGHV 2007 (arbitrary error correcting codes)

generalizes

# Recent Efficient Ramp Schemes

- Exploiting the structure of the function *F*:
  - Franklin and Yung 1991 (parallel multiplications)
  - CDH 2007 (extension field multiplication) ?
- Enabling small fields:
  - Chen and Cramer 2006 (algebraic geometry codes)
  - CCGHV 2007 (arbitrary error correcting codes)

generalizes

- This work:
  - Replacement scheme CDH 2007, optimized parameters.
  - Generalization "CDH 2007" that enables to use small fields.
  - Low communication active adversary protocols for this general scheme and CC06.

# CDH 2007

- Perform multiplication in a finite field using communication and operations only involving elements in a subfield.

# CDH 2007

- Perform multiplication in a finite field using communication and operations only involving elements in a subfield.

- Let $L = K(\alpha)$ with $[L:K] = k$.
  - Secret $s_0 + s_1\alpha + \ldots + s_{k-1}\alpha^{k-1} \in L$.
  - Polynomial $f(X) = s_0 + s_1X + \ldots + s_{k-1}X^{k-1} + r(X)X^{2k-1} \in K[X]$, with $r(X) \in K[X]$ of degree at most $t$-$1$.
  - Shares $f(x_1),f(x_2),\ldots,f(x_k)$ with $x_1,x_2,\ldots,x_n \in K$ distinct, nonzero.

# CDH 2007

- Perform multiplication in a finite field using communication and operations only involving elements in a subfield.

- Let $L = K(\alpha)$ with $[L:K] = k$.
  - Secret $s_0 + s_1\alpha + \ldots + s_{k-1}\alpha^{k-1} \in L$.
  - Polynomial $f(X) = s_0 + s_1X + \ldots + s_{k-1}X^{k-1} + r(X)X^{2k-1} \in K[X]$, with $r(X) \in K[X]$ of degree at most $t$-$1$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_k)$ with $x_1, x_2, \ldots, x_n \in K$ distinct, nonzero.
- Parameters
  - $t$-privacy
  - $t+2k-1$ reconstruction

# CDH 2007

- Perform multiplication in a finite field using communication and operations only involving elements in a subfield.

- Let $L = K(\alpha)$ with $[L:K] = k$.
  - Secret $s_0 + s_1\alpha + \ldots + s_{k-1}\alpha^{k-1} \in L$.
  - Polynomial $f(X) = s_0 + s_1X + \ldots + s_{k-1}X^{k-1} + r(X)X^{2k-1} \in K[X]$, with $r(X) \in K[X]$ of degree at most $t$-$1$.
  - Shares $f(x_1),f(x_2),\ldots,f(x_k)$ with $x_1,x_2,\ldots,x_n \in K$ distinct, nonzero.
- Parameters
  - $t$-privacy
  - $t+2k-1$ reconstruction
- Multiplication property for $t+2k-2 < n/2$.

# New Basic Scheme (1)

- For $y \in L$, define $w(y) := [K(y) : K]$.
- Theorem:
  - Take $y_1, y_2, \ldots, y_l \in L$ such that no $y_i \neq y_j$ are Galois conjugate.
  - Then for any $b_1, b_2, \ldots, b_l$ with $b_i \in K(y_i)$, there is a unique polynomial $f(X) \in K[X]$ of degree at most $(\sum w(y_i))-1$ such that $f(y_i) = b_i$ for $i = 1, 2, \ldots, l$.

# New Basic Scheme (2)

- New scheme: Let $L = K(\alpha)$ with $[L : K] = k$.
  - Secret $s \in L$.
  - Select $e \in L$ such that $[K(e) : K] = k$.
  - Select random polynomial $f \in K[X]$ of degree at most $t+k-1$ such that $f(e) = s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.

# New Basic Scheme (2)

- New scheme: Let $L = K(\alpha)$ with $[L : K] = k$.
  - Secret $s \in L$.
  - Select $e \in L$ such that $[K(e) : K] = k$.
  - Select random polynomial $f \in K[X]$ of degree at most $t+k-1$ such that $f(e) = s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.
- Parameters
  - $t$-privacy
  - $(t+k)$-reconstruction

# New Basic Scheme (2)

- New scheme: Let $L = K(\alpha)$ with $[L : K] = k$.
  - Secret $s \in L$.
  - Select $e \in L$ such that $[K(e) : K] = k$.
  - Select random polynomial $f \in K[X]$ of degree at most $t+k-1$ such that $f(e) = s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.
- Parameters
  - $t$-privacy
  - $(t+k)$-reconstruction
- Multiplication property for $t+k-1 < n/2$.

# New Basic Scheme (2)

- New scheme: Let $L = K(\alpha)$ with $[L : K] = k$.
  - Secret $s \in L$.
  - Select $e \in L$ such that $[K(e) : K] = k$.
  - Select random polynomial $f \in K[X]$ of degree at most $t+k-1$ such that $f(e) = s$.
  - Shares $f(x_1), f(x_2), \ldots, f(x_n)$.
- Parameters
  - $t$-privacy
  - $(t+k)$-reconstruction
- Multiplication property for $t+k-1 < n/2$.
- This scheme extends to the algebraic curve setting.

# Sketch Shamir vs Algebraic Geometry SS

- Shamir SS
  - Points $x_i \in K$.
  - Polynomials $f \in K[X]$ of degree at most $t$.
  - Secret $s = f(x_0) \in K$.
  - Shares $f(x_i) \in K$.
- Algebraic geometry SS
  - Projective points $P_i$ on a suitable curve $C$.
  - $K$-rational functions $h=f/g \in L(D)$, where $L(D)$ is some $t$-dimensional Riemann Roch space.
  - Secret $s = h(P_0) \in K$.
  - Shares $h(P_i) \in K$.

# Sketch Shamir vs Algebraic Geometry SS

- Shamir SS
  - At most $|K|$ distinct evaluation points.
  - $t$-privacy.
  - $(t+1)$-reconstruction.
- Algebraic geometry SS
  - Can use all points on $C$, potentially many more than $|K|$.
  - $t$-privacy.
  - $(t+1+g)$-reconstruction.

# Sketch Shamir vs Algebraic Geometry SS

- Shamir SS
  - At most $|K|$ distinct evaluation points.
  - $t$-privacy.
  - $(t+1)$-reconstruction.
  - Achieves multiplication property for optimal $t < n/2$.
  - Achieves strong mult. property for optimal $t < n/3$.
- Algebraic geometry SS
  - Can use all points on $C$, potentially many more than $|K|$.
  - $t$-privacy.
  - $(t+1+g)$-reconstruction.
  - Achieves multiplication property for near-optimal $t < (1/2-\varepsilon)n$.
  - Achieves strong mult. Property for near-optimal $t < (1/3-\varepsilon)n$.

# New Algebraic Geometric Ramp Scheme

- Let
  - Let $C$ be a smooth, projective, irreducible curve over $F_q$.
  - $D = \{P_1, P_2, \ldots, P_n\}$ be a set of $F_q$-rational points on $C$.
  - $G$ be an $F_q$-rational divisor of degree $2g+t+k-1$ with $support(G) \cap D = \{\}$.
  - $Q$ be an $F_{q^k}$-rational point that is not $F_{q^t}$-rational for $t<k$.
- The secret is $s \in F_{q^k}$.

# New Algebraic Geometric Ramp Scheme

- Let
  - Let $C$ be a smooth, projective, irreducible curve over $F_q$.
  - $D = \{P_1,P_2,\dots,P_n\}$ be a set of $F_q$-rational points on $C$.
  - $G$ be an $F_q$-rational divisor of degree $2g+t+k-1$ with $support(G) \cap D = \{\}$.
  - $Q$ be an $F_{q^k}$-rational point that is not $F_{q^t}$-rational for $t<k$.
- The secret is $s \in F_{q^k}$.
- To secret share $s$:
  - Select random $F_q$-rational function $f \in L(G)$ such that $f(Q) = s$.
  - The shares are $f(P_1),f(P_2),\dots,f(P_n)$.

# New Algebraic Geometric Ramp Scheme

- To secret share $s$:
  - Select random $F_q$-rational function $f \in L(G)$ such that $f(Q) = s$.
  - The shares are $f(P_1), f(P_2), \ldots, f(P_n)$.
- Parameters:
  - $t$-privacy
  - $(2g+t+k)$-reconstruction

# New Algebraic Geometric Ramp Scheme

- To secret share *s*:
  - Select random $F_q$-rational function $f \in L(G)$ such that $f(Q) = \mathbf{s}$.
  - The shares are $f(P_1), f(P_2), \ldots, f(P_n)$.
- Parameters:
  - *t*-privacy
  - $(2g+t+k)$-reconstruction
- Multiplication property for $n \geq 4g+2t+2k-1$.
  - We specify how to determine the corresponding equation in the paper.

# Final remarks

- We additionally describe general low communication MPC protocols for the algebraic geometric schemes secure against an active adversary.
  - Somewhat technical due to the lack of the convenient polynomial structure introduced by Shamir-type schemes.
  - For the new scheme and $t,k = \Theta(n)$, we can perform multiplications in $F_{q^k}$ at a communication cost of $O(n^3)$ elements in $F_q$.
  - This matches CDH07. However, the size of the field $F_q$ can now be chosen independent of the number of players $n$.

# Strongly Multiplicative Ramp Schemes From High Degree Rational Points on Curves


**Hao Chen**
East China Normal University

**Ronald Cramer**
CWI & Leiden University

**Robbert de Haan**
CWI

**Ignacio Cascudo Pueyo**
Oviedo University