Amortized NISC over $\mathbb{Z}_{2^k}$ from RMFE

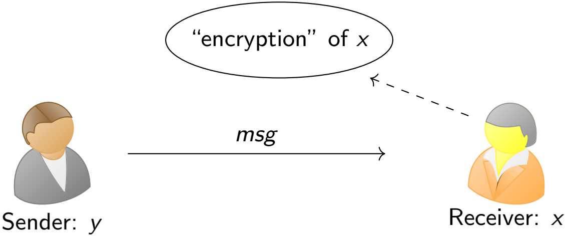
Fuchun Lin, Chaoping Xing, Yizhou Yao, Chen Yuan

Shanghai Jiao Tong University

Dec 8, 2023 - Asiacrypt 2023

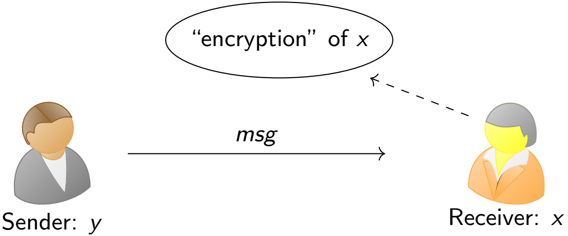
Reusable Non-Interactive Secure Computation

Reusable NISC: Two-round 2-PC for jointly computing a function $f(x, y)$, where it is safe to reuse the first message of Receiver.



Reusable Non-Interactive Secure Computation

Reusable NISC: Two-round 2-PC for jointly computing a function $f(x, y)$, where it is safe to reuse the first message of Receiver.



f is a function defined over the ring $\mathbb{Z}_{2^k}$ (i.e. $\mathbb{Z}/2^k\mathbb{Z}$).

- data types and computations of real-life computer programs are defined over $\mathbb{Z}_{2^{32}}$ or $\mathbb{Z}_{2^{64}}$.
- protocols based on $\mathbb{Z}_{2^k}$ arithmetic are easier and faster to implement.

Paradigms for Constructing Reusable NISC

Paradigms for Constructing Reusable NISC

1. Fully Homomorphic Encryption (FHE)
   - small communication complexity,
     large computation complexity due to bootstrapping.
   - existence of FHE over $\mathbb{Z}_{2^k}$?

Paradigms for Constructing Reusable NISC

1. Fully Homomorphic Encryption (FHE)
   - small communication complexity,
     large computation complexity due to bootstrapping.
   - existence of FHE over $\mathbb{Z}_{2^k}$?
2. Garble Circuit and Oblivious Transfer (OT)
   - trade-off of communication and computation,
     achieve reusability incurs additional overhead.
   - GC is a computational randomized encoding for Boolean circuits.

Paradigms for Constructing Reusable NISC

1. Fully Homomorphic Encryption (FHE)
   - small communication complexity, large computation complexity due to bootstrapping.
   - existence of FHE over $\mathbb{Z}_{2^k}$?
2. Garble Circuit and Oblivious Transfer (OT)
   - trade-off of communication and computation, achieve reusability incurs additional overhead.
   - GC is a computational randomized encoding for Boolean circuits.
3. Decomposable Affine Randomized Encoding (DARE) and Vector Oblivious Linear Function Evaluation (VOLE)
   - "free" reusability.
   - [IK02] there exists a perfect DARE for arithmetic $\mathbf{NC}^1$ circuits or arithmetic branching programs. ✓

[IK02] Yuval Ishai, Eyal Kushilevitz. Perfect Constant-Round Secure Computation via Perfect Randomizing Polynomials. In ICALP 2002.

Challenges for working over $\mathbb{Z}_{2^k}$

Goal: Construct statistical reusable NISC/VOLE for $\mathbf{NC}^1$ circuits over $\mathbb{Z}_{2^k}$.

Challenges for working over $\mathbb{Z}_{2^k}$

Goal: Construct statistical reusable NISC/VOLE for $\mathbf{NC}^1$ circuits over $\mathbb{Z}_{2^k}$.

Challenges:

The algebraic structure of $\mathbb{Z}_{2^k}$ is bad: half of $\mathbb{Z}_{2^k}$ are zero divisors.
This results in that, e.g.,

- polynomial interpolation. ✗
- random linear combination makes no sense (constant soundness).

$\Longrightarrow$ In most cases, naively instantiating protocols designed for a large field with $\mathbb{Z}_{2^k}$ leads to a constant soundness error.

Challenges for working over $\mathbb{Z}_{2^k}$

Goal: Construct statistical reusable NISC/VOLE for $\mathbf{NC}^1$ circuits over $\mathbb{Z}_{2^k}$.

Challenges:

The algebraic structure of $\mathbb{Z}_{2^k}$ is bad: half of $\mathbb{Z}_{2^k}$ are zero divisors.
This results in that, e.g.,

- polynomial interpolation. ✗
- random linear combination makes no sense (constant soundness).

$\Longrightarrow$ In most cases, naively instantiating protocols designed for a large field with $\mathbb{Z}_{2^k}$ leads to a constant soundness error.

Solutions:

There are two mainstream mechanisms in the context of MPC.

- the SPD$\mathbb{Z}_{2^k}$ idea: use a larger ring $\mathbb{Z}_{2^{k+s}}$. Does it work ?
- the Galois ring idea: use a large ring extension of $\mathbb{Z}_{2^k}$, that has a small fraction of zero divisors. ✓

Construction Overview

Roadmap:

1. Construct semi-honest NISC based on Galois ring arithmetic, which simulates the computation of arithmetic branching programs over $\mathbb{Z}_{2^k}$.
   - Apply the Reverse Multiplicative Friendly Embedding (RMFE) technique for amortization.
2. Lift semi-honest security to malicious security.
   - Design a new technique, Non-Malleable RMFE, to deal with the issue of introducing RMFE.
   - Adapt existing methods from Galois field to Galois ring.

Galois ring

Definition (Galois ring)

Let p be a prime, and $k, d \geq 1$ be integers. Let $f(X) \in \mathbb{Z}_{p^k}[X]$ be a monic polynomial of degree d such that $\overline{f(X)} := f(X) \mod p$ is irreducible over $\mathbb{F}_p$. A Galois ring over $\mathbb{Z}_{p^k}$ of degree d denoted by $\mathtt{GR}(p^k, d)$ is a ring extension $\mathbb{Z}_{p^k}[X]/(f(X))$ of $\mathbb{Z}_{p^k}$.

Galois ring

Definition (Galois ring)

Let p be a prime, and $k, d \geq 1$ be integers. Let $f(X) \in \mathbb{Z}_{p^k}[X]$ be a monic polynomial of degree d such that $\overline{f(X)} := f(X) \mod p$ is irreducible over $\mathbb{F}_p$. A Galois ring over $\mathbb{Z}_{p^k}$ of degree d denoted by $\mathtt{GR}(p^k, d)$ is a ring extension $\mathbb{Z}_{p^k}[X]/(f(X))$ of $\mathbb{Z}_{p^k}$.

- if $d = 1$, $\mathtt{GR}(p^k, d) = \mathbb{Z}_{p^k}$; if $k = 1$, $\mathtt{GR}(p^k, d) = \mathbb{F}_{p^d}$.
- $\mathtt{GR}(p^k, d)/(p) \cong \mathbb{F}_{p^d}$.
- "Schwatz-Zipple" Lemma for Galois ring:
  For any nonzero degree-r polynomial $f(x)$ over $\mathtt{GR}(p^k, d)$,

$$\Pr\left[f(\alpha) = 0 \,\middle|\, \alpha \xleftarrow{\$} \mathtt{GR}(p^k, d)\right] \leq rp^{-d}.$$

Reverse Multiplicative Friendly Embedding

Definition (Degree-D RMFE)

Let p be a prime, $k, r, m, d, D \geq 1$ be integers. A pair (ϕ, ψ) is called an $(m, d; D)$-RMFE over $\mathtt{GR}(p^k, r)$ if $\phi : \mathtt{GR}(p^k, r)^m \to \mathtt{GR}(p^k, rd)$ and $\psi : \mathtt{GR}(p^k, rd) \to \mathtt{GR}(p^k, r)^m$ are two $\mathtt{GR}(p^k, r)$-linear maps such that

$$\psi(\phi(\boldsymbol{x}_1) \cdot \phi(\boldsymbol{x}_2) \cdots \phi(\boldsymbol{x}_D)) = \boldsymbol{x}_1 * \boldsymbol{x}_2 * \cdots * \boldsymbol{x}_D \tag{1}$$

for all $\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_D \in \mathtt{GR}(p^k, r)^m$, where $*$ denotes the entry-wise multiplication operation.

Reverse Multiplicative Friendly Embedding

Definition (Degree-D RMFE)

Let p be a prime, $k, r, m, d, D \geq 1$ be integers. A pair (ϕ, ψ) is called an $(m, d; D)$-RMFE over $\mathtt{GR}(p^k, r)$ if $\phi : \mathtt{GR}(p^k, r)^m \to \mathtt{GR}(p^k, rd)$ and $\psi : \mathtt{GR}(p^k, rd) \to \mathtt{GR}(p^k, r)^m$ are two $\mathtt{GR}(p^k, r)$-linear maps such that

$$\psi(\phi(\mathbf{x}_1) \cdot \phi(\mathbf{x}_2) \cdots \phi(\mathbf{x}_D)) = \mathbf{x}_1 * \mathbf{x}_2 * \cdots * \mathbf{x}_D \tag{1}$$

for all $\mathbf{x}_1, \mathbf{x}_2, ..., \mathbf{x}_D \in \mathtt{GR}(p^k, r)^m$, where $*$ denotes the entry-wise multiplication operation.

Intuitions:

- ϕ is a linear map with limited multiplication capacity.
- RMFE relates arithmetic operations of $\mathtt{GR}(p^k, r)^m$ and $\mathtt{GR}(p^k, rd)$.
- Above ϕ, ψ can be naturally extended to establish a matrix multiplication relation for matrices over $\mathtt{GR}(p^k, r)$ and $\mathtt{GR}(p^k, rd)$.

Properties of Degree-D RMFE [EHLXY23]

1. There always exists an $(m, d; D)$-RMFE (ϕ, ψ) over Galois ring $\mathtt{GR}(p^k, r)$ with $\phi(\mathbf{1}) = 1$.
2. Let (ϕ, ψ) be an $(m, d; D)$-RMFE over Galois ring $\mathtt{GR}(p^k, r)$, with $\phi(\mathbf{1}) = 1$. We have

$$\mathtt{GR}(p^k, rd) = \mathrm{Ker}(\psi) \oplus \mathrm{Im}(\phi).$$

   Moreover, $\psi|_{\mathrm{Im}(\phi)}$ is a bijection.
3. There exists a family of $(m, d; D)$-RMFEs over $\mathbb{Z}_{2^k}$ for all $k \geq 1$ with

$$\lim_{m\to\infty} \frac{d}{m} = \frac{1+2D}{3}(D + \frac{D(3+1/(2^D-1))}{2^{D+1}-1}) = \mathcal{O}\left(D^2\right).$$

[EHLXY23] Daniel Escudero, Cheng Hong, Hongqing Liu, Chaoping Xing, Chen Yuan. Degree-D Reverse Multiplication-Friendly Embeddings: Constructions and Applications. In Asiacrypt 2023.

DARE of arithmetic branching programs

Example: $f(\boldsymbol{x}, \boldsymbol{y}) = \langle \boldsymbol{x}, \boldsymbol{y} \rangle = det \begin{pmatrix} y_1 & y_2 & 0 \\ -1 & 0 & x_1 \\ 0 & -1 & x_2 \end{pmatrix}$,

DARE of arithmetic branching programs

Example: $f(\boldsymbol{x},\boldsymbol{y}) = \langle \boldsymbol{x},\boldsymbol{y}\rangle = det \begin{pmatrix} y_1 & y_2 & 0 \\ -1 & 0 & x_1 \\ 0 & -1 & x_2 \end{pmatrix}$,

$$M := \underbrace{\begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 1 & a_3 \\ 0 & 0 & 1 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} y_1 & y_2 & 0 \\ -1 & 0 & x_1 \\ 0 & -1 & x_2 \end{pmatrix}}_{L(\boldsymbol{x},\boldsymbol{y})} \cdot \underbrace{\begin{pmatrix} 1 & 0 & b_1 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}}_{B}$$

$$= \begin{pmatrix} y_1 - a_1 & y_2 - a_2 & a_1 x_1 + a_2 x_2 + b_1 y_1 + b_2 y_2 - b_2 a_2 \\ -1 & -a_3 & x_1 + a_3 x_2 - b_1 - a_3 b_2 \\ 0 & -1 & x_2 - b_2 \end{pmatrix}$$

DARE of arithmetic branching programs

Example: $f(\boldsymbol{x},\boldsymbol{y}) = \langle \boldsymbol{x},\boldsymbol{y}\rangle = det\begin{pmatrix} y_1 & y_2 & 0 \\ -1 & 0 & x_1 \\ 0 & -1 & x_2 \end{pmatrix}$,

$$M := \underbrace{\begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 1 & a_3 \\ 0 & 0 & 1 \end{pmatrix}}_{A} \cdot \underbrace{\begin{pmatrix} y_1 & y_2 & 0 \\ -1 & 0 & x_1 \\ 0 & -1 & x_2 \end{pmatrix}}_{L(\boldsymbol{x},\boldsymbol{y})} \cdot \underbrace{\begin{pmatrix} 1 & 0 & b_1 \\ 0 & 1 & b_2 \\ 0 & 0 & 1 \end{pmatrix}}_{B}$$

$$= \begin{pmatrix} y_1 - a_1 & y_2 - a_2 & a_1x_1 + a_2x_2 + b_1y_1 + b_2y_2 - b_2a_2 \\ -1 & -a_3 & x_1 + a_3x_2 - b_1 - a_3b_2 \\ 0 & -1 & x_2 - b_2 \end{pmatrix}$$

$$= \begin{pmatrix} y_1 - a_1 & y_2 - a_2 & a_1x_1 + c_1 + a_2x_2 + b_1y_1 + b_2y_2 - b_2a_2 - c_1 \\ -1 & -a_3 & x_1 + c_2 + a_3x_2 - b_1 - a_3b_2 - c_2 \\ 0 & -1 & x_2 - b_2 \end{pmatrix}$$

- $det(M) = det(AL(\boldsymbol{x},\boldsymbol{y})B) = det(L(\boldsymbol{x},\boldsymbol{y})) = f(\boldsymbol{x},\boldsymbol{y})$.
- M decomposes into linear functions of x_1, x_2.

Combine DARE with RMFE

Goal: Jointly compute $f(\boldsymbol{x}_1, \boldsymbol{y}_1), ..., f(\boldsymbol{x}_m, \boldsymbol{y}_m)$, where f is an arithmetic branching program over $\mathbb{Z}_{2^k}$.
$\Longrightarrow$ m DAREs, $M_i := A_i L(\boldsymbol{x}_i, \boldsymbol{y}_i) B_i$, $i \in [m]$, where $L(\cdot, \cdot)$ is defined over $\mathbb{Z}_{2^k}$.

Combine DARE with RMFE

Goal: Jointly compute $f(\boldsymbol{x}_1, \boldsymbol{y}_1), \ldots, f(\boldsymbol{x}_m, \boldsymbol{y}_m)$, where f is an arithmetic branching program over $\mathbb{Z}_{2^k}$.

$\Longrightarrow$ m DAREs, $M_i := A_i L(\boldsymbol{x}_i, \boldsymbol{y}_i) B_i$, $i \in [m]$, where $L(\cdot, \cdot)$ is defined over $\mathbb{Z}_{2^k}$.

Let (ϕ, ψ) be an $(m, d; 3)$-RMFE over $\mathbb{Z}_{2^k}$.

i) Receiver computes $\boldsymbol{X} := \phi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$.

ii) Sender computes $A := \phi(A_1, \ldots, A_m)$, $B := \phi(B_1, \ldots, B_m)$, $\boldsymbol{Y} := \phi(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$.

Combine DARE with RMFE

Goal: Jointly compute $f(\mathbf{x}_1, \mathbf{y}_1), \ldots, f(\mathbf{x}_m, \mathbf{y}_m)$, where f is an arithmetic branching program over $\mathbb{Z}_{2^k}$.
$\Longrightarrow$ m DAREs, $M_i := A_i L(\mathbf{x}_i, \mathbf{y}_i) B_i$, $i \in [m]$, where $L(\cdot, \cdot)$ is defined over $\mathbb{Z}_{2^k}$.

Let (ϕ, ψ) be an $(m, d; 3)$-RMFE over $\mathbb{Z}_{2^k}$.

i) Receiver computes $\mathbf{X} := \phi(\mathbf{x_1}, \ldots, \mathbf{x}_m)$.

ii) Sender computes $A := \phi(A_1, \ldots, A_m)$, $B := \phi(B_1, \ldots, B_m)$, $\mathbf{Y} := \phi(\mathbf{y_1}, \ldots, \mathbf{y}_m)$.

- ϕ, ψ are $\mathbb{Z}_{2^k}$-linear,

$$\psi(L(\mathbf{X}, \mathbf{Y})) = (L(\mathbf{x}_1, \mathbf{y}_1), \ldots, L(\mathbf{x}_m, \mathbf{y}_m)).$$

Combine DARE with RMFE

Goal: Jointly compute $f(\boldsymbol{x}_1, \boldsymbol{y}_1), \ldots, f(\boldsymbol{x}_m, \boldsymbol{y}_m)$, where f is an arithmetic branching program over $\mathbb{Z}_{2^k}$.

$\Longrightarrow$ m DAREs, $M_i := A_i L(\boldsymbol{x}_i, \boldsymbol{y}_i) B_i$, $i \in [m]$, where $L(\cdot,\cdot)$ is defined over $\mathbb{Z}_{2^k}$.

Let (ϕ, ψ) be an $(m, d; 3)$-RMFE over $\mathbb{Z}_{2^k}$.

i) Receiver computes $\boldsymbol{X} := \phi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m)$.

ii) Sender computes $A := \phi(A_1, \ldots, A_m)$, $B := \phi(B_1, \ldots, B_m)$, $\boldsymbol{Y} := \phi(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$.

- ϕ, ψ are $\mathbb{Z}_{2^k}$-linear,

$$\psi(L(\boldsymbol{X}, \boldsymbol{Y})) = (L(\boldsymbol{x}_1, \boldsymbol{y}_1), \ldots, L(\boldsymbol{x}_m, \boldsymbol{y}_m)).$$

- Let $M := A \cdot L(\boldsymbol{X}, \boldsymbol{Y}) \cdot B$,

$$\begin{aligned}\psi(M) &= \psi(A \cdot L(\boldsymbol{X}, \boldsymbol{Y}) \cdot B) \\ &= \psi(\phi(A_1, \ldots, A_m) \cdot L(\phi(\boldsymbol{x}_1, \ldots, \boldsymbol{x}_m), \phi(\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)) \cdot \phi(B_1, \ldots, B_m)) \\ &= (\underbrace{A_1 \cdot L(\boldsymbol{x}_1, \boldsymbol{y}_1) \cdot B_1}_{M_1}, \ldots, \underbrace{A_m \cdot L(\boldsymbol{x}_m, \boldsymbol{y}_m) \cdot B_m}_{M_m}).\end{aligned}$$

Combine DARE with RMFE (continue)

$$\psi(M) = (\underbrace{A_1 \cdot L(x_1, y_1) \cdot B_1}_{M_1}, \ldots, \underbrace{A_m \cdot L(x_m, y_m) \cdot B_m}_{M_m})$$

iii) Receiver learns M by calling an ideal functionality of VOLE over $\mathtt{GR}(2^k, d)$.

iv) Receiver then computes $f(x_1, y_1), \ldots, f(x_m, y_m)$ from $\psi(M)$.

Combine DARE with RMFE (continue)

$$\psi(M) = (\underbrace{A_1 \cdot L(x_1, y_1) \cdot B_1}_{M_1}, \ldots, \underbrace{A_m \cdot L(x_m, y_m) \cdot B_m}_{M_m})$$

iii) Receiver learns M by calling an ideal functionality of VOLE over $\mathtt{GR}(2^k, d)$.

iv) Receiver then computes $f(x_1, y_1), \ldots, f(x_m, y_m)$ from $\psi(M)$.

- But M contains more information than $\psi(M)$.
  Essentially, the leakage is M's projection on $\mathrm{Ker}(\psi)$.
- Recall that $\mathtt{GR}(2^k, d) = \mathrm{Im}(\phi) \oplus \mathrm{Ker}(\psi)$, and $\psi|_{\mathrm{Im}(\phi)}$ is a bijection.

Combine DARE with RMFE (continue)

$$\psi(M) = (\underbrace{A_1 \cdot L(x_1, y_1) \cdot B_1}_{M_1}, \ldots, \underbrace{A_m \cdot L(x_m, y_m) \cdot B_m}_{M_m})$$

iii) Receiver learns M by calling an ideal functionality of VOLE over $\texttt{GR}(2^k, d)$.

iv) Receiver then computes $f(x_1, y_1), \ldots, f(x_m, y_m)$ from $\psi(M)$.

- But M contains more information than $\psi(M)$.
  Essentially, the leakage is M's projection on $\mathrm{Ker}(\psi)$.
- Recall that $\texttt{GR}(2^k, d) = \mathrm{Im}(\phi) \oplus \mathrm{Ker}(\psi)$, and $\psi|_{\mathrm{Im}(\phi)}$ is a bijection.

iii) Receiver learns $M' = M + C$ by calling an ideal functionality of VOLE over $\texttt{GR}(2^k, d)$, where C is a upper triangle matrix with each entry sampled uniformly at random from $\mathrm{Ker}(\psi)$. ✓

$$\psi(M + C) = \psi(M) + \psi(C) = \psi(M).$$

Achieve Malicious Security

Malicious Adversary has following two kinds of cheating behaviors.

1. Deviating from DARE
   - Only Sender computes DARE.
   - Adapt methods from [DIO21] (details omitted in this talk).
2. Deviating from RMFE
   - Both Sender and Receiver compute RMFE.
   - How to force both parties to follow RMFE in a statistical way, without increase of round complexity?

[DIO21] Samuel Dittmer, Yuval Ishai, Rafail Ostrovsky. Line-Point Zero Knowledge and Its Applications. In ITC 2021.

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.

Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\mathcal{F}_{\mathrm{VOLE}}$

Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.

Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$

$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$

$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

$\mathcal{F}_{\mathrm{VOLE}}$

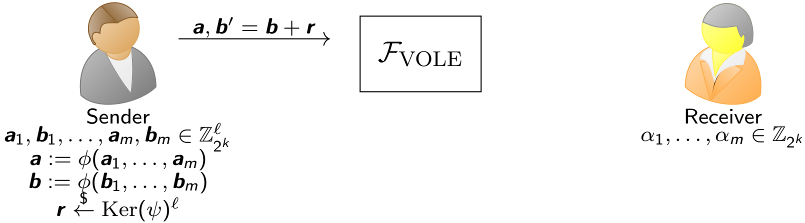
Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

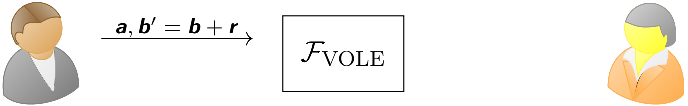
Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.



A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.



Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$

$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$

$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

Receiver

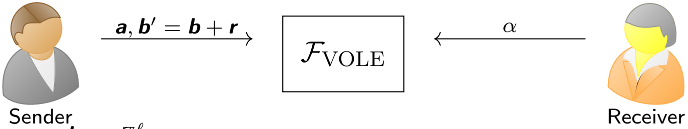
$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.



Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$

$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$

$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.

Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.

Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$

$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$

$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

Sender → $\mathcal{F}_{\mathrm{VOLE}}$: $\boldsymbol{a}, \boldsymbol{b}' = \boldsymbol{b} + \boldsymbol{r}$

$\mathcal{F}_{\mathrm{VOLE}}$

Receiver → $\mathcal{F}_{\mathrm{VOLE}}$: α

$\mathcal{F}_{\mathrm{VOLE}}$ → Receiver: $\boldsymbol{v} := \boldsymbol{a} \cdot \alpha + \boldsymbol{b}'$

Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$

$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) := \psi(\boldsymbol{v})$

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.
Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.

Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$

$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$

$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$

$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

Sender → $\mathcal{F}_{\mathrm{VOLE}}$: $\boldsymbol{a}, \boldsymbol{b}' = \boldsymbol{b} + \boldsymbol{r}$

$\mathcal{F}_{\mathrm{VOLE}}$

Receiver → $\mathcal{F}_{\mathrm{VOLE}}$: α

$\mathcal{F}_{\mathrm{VOLE}}$ → Receiver: $\boldsymbol{v} := \boldsymbol{a} \cdot \alpha + \boldsymbol{b}'$

Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$

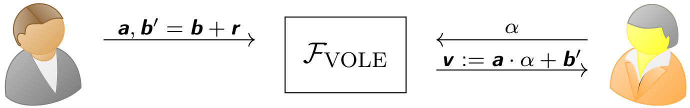
$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$

$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) := \psi(\boldsymbol{v})$

- **Correctness**: easy to verify that $\boldsymbol{v}_i = \boldsymbol{a}_i \cdot \alpha_i + \boldsymbol{b}_i$, for $i \in [m]$. ✓

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.
Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.



Sender

$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$
$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$
$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$
$\boldsymbol{r} \stackrel{\$}{\leftarrow} \mathrm{Ker}(\psi)^{\ell}$

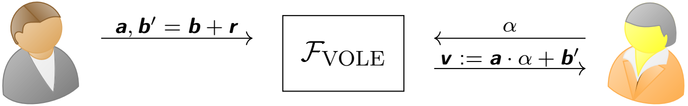
Receiver

$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$
$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$
$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) := \psi(\boldsymbol{v})$

- **Correctness**: easy to verify that $\boldsymbol{v}_i = \boldsymbol{a}_i \cdot \alpha_i + \boldsymbol{b}_i$, for $i \in [m]$. ✓
- **Security**: semi-honest ✓, malicious ✗.

A simple case for illustration

Goal: Construct VOLE over $\mathbb{Z}_{2^k}$ from VOLE over $\mathtt{GR}(2^k, d)$.
Let (ϕ, ψ) be an $(m, d; 2)$ RMFE over $\mathbb{Z}_{2^k}$.



Sender
$\boldsymbol{a}_1, \boldsymbol{b}_1, \ldots, \boldsymbol{a}_m, \boldsymbol{b}_m \in \mathbb{Z}_{2^k}^{\ell}$
$\boldsymbol{a} := \phi(\boldsymbol{a}_1, \ldots, \boldsymbol{a}_m)$
$\boldsymbol{b} := \phi(\boldsymbol{b}_1, \ldots, \boldsymbol{b}_m)$
$\boldsymbol{r} \xleftarrow{\$} \mathrm{Ker}(\psi)^{\ell}$

Receiver
$\alpha_1, \ldots, \alpha_m \in \mathbb{Z}_{2^k}$
$\alpha := \phi(\alpha_1, \ldots, \alpha_m)$
$(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m) := \psi(\boldsymbol{v})$

- **Correctness**: easy to verify that $\boldsymbol{v}_i = \boldsymbol{a}_i \cdot \alpha_i + \boldsymbol{b}_i$, for $i \in [m]$. ✓
- **Security**: semi-honest ✓, malicious ✗.

When Sender (Receiver) is corrupted, the simulator can extract $\boldsymbol{a}_i$ (α_i) for $i \in [m]$, if and only if $\boldsymbol{a} \in \mathrm{Im}(\phi)^{\ell}$ $(\alpha \in \mathrm{Im}(\phi))$.

Non-Malleable RMFE

Definition (Degree-D Non-Malleable RMFE)

Let $\mathtt{GR}(p^k, r)$ be a Galois ring and κ be the statistical security parameter. A pair of maps (ϕ, ψ) is called an $(m, d; D)$-NM-RMFE over $\mathtt{GR}(p^k, r)$, if it has the following properties:

1. $\phi : \mathtt{GR}(p^k, r)^m \times \{0, 1\}^{O(\kappa)} \to \mathtt{GR}(p^k, rd)$,
   $\psi : \mathtt{GR}(p^k, rd) \to \mathtt{GR}(p^k, r)^m \cup \{\perp\}$ are $\mathtt{GR}(p^k, r)$-linear maps, satisfying

   $$\psi(\phi(\boldsymbol{x}_1, r_1) \cdot \phi(\boldsymbol{x}_2, r_2) \cdots \phi(\boldsymbol{x}_D, r_D)) = \boldsymbol{x}_1 * \boldsymbol{x}_2 * \cdots * \boldsymbol{x}_D,$$

   for any $\boldsymbol{x}_1, ..., \boldsymbol{x}_D \in \mathtt{GR}(p^k, r)^m$ and $r_1, ..., r_D \stackrel{\$}{\leftarrow} \{0, 1\}^\kappa$.
2. if $Y \notin \mathrm{Im}(\phi)$, there exists a constant $\boldsymbol{y} \in \mathtt{GR}(p^k, r)^m$, such that for any $\boldsymbol{x}_1, ..., \boldsymbol{x}_{D-1} \in \mathtt{GR}(p^k, r)^m$, we have

   $$\psi(\phi(\boldsymbol{x}_1) \cdots \phi(\boldsymbol{x}_{D-1}) \cdot Y) = \boldsymbol{x}_1 * \cdots * \boldsymbol{x}_{D-1} * \boldsymbol{y} + \boldsymbol{\delta},$$

   where $\boldsymbol{\delta} \sim \mathcal{D}_{\boldsymbol{x}, Y} \stackrel{s}{\approx} \mathcal{D}_Y$ and $\mathcal{D}_Y$ is a PPT-sampleable distribution over $\mathtt{GR}(p^k, r)^m \cup \{\perp\}$ determined only by Y. We use the convention that for any $\boldsymbol{z} \in \mathtt{GR}(p^k, r)^m$, $\boldsymbol{z} + \perp = \perp$ to make ψ well-defined.

Construction of NM-RMFE: 1

High-level idea: "structured and randomized" RMFE for Non-Malleability.

In more detail, our construction consists of 2 layers of RMFEs:
a degree-D RMFE and a degree-D extended RMFE.

Definition (Degree-D extended RMFE)

Let $\mathbb{Z}_{p^k} = \mathbb{Z}/p^k\mathbb{Z}$ be a modulo ring, $d > n > m \geq 1$ and $D \geq 1$ be integers. A pair of maps (ϕ, ψ) is called an $(m, n, d; D)$-extended RMFE over $\mathbb{Z}_{p^k}$ if $\phi : \mathbb{Z}_{p^k}^m \times \mathtt{GR}(p^k, n) \to \mathtt{GR}(p^k, d)$ and $\psi : \mathtt{GR}(p^k, d) \to \mathbb{Z}_{p^k}^m \times \mathtt{GR}(p^k, n)$ are two $\mathbb{Z}_{p^k}$-linear maps satisfying

$$\psi(\phi(\mathbf{x}_1, y_1) \cdot \phi(\mathbf{x}_2, y_2) \cdots \phi(\mathbf{x}_D, y_D)) = (\mathbf{x}_1 * \mathbf{x}_2 * \cdots * \mathbf{x}_D, y_1 y_2 \cdots y_D),$$

for any $\mathbf{x}_i \in \mathbb{Z}_{p^k}^m$, $y_i \in \mathtt{GR}(p^k, n)$, $i \in [D]$.

Construction of NM-RMFE: 2

- Let (ϕ_1, ψ_1) be an $(m+\ell, n; D)$-RMFE over $\mathbb{Z}_{p^k}$.
- Let (ϕ_2, ψ_2) be an $(m+\ell, n, d; D)$-extended RMFE over $\mathbb{Z}_{p^k}$.

Construction of NM-RMFE: 2

- Let (ϕ_1, ψ_1) be an $(m+\ell, n; D)$-RMFE over $\mathbb{Z}_{p^k}$.
- Let (ϕ_2, ψ_2) be an $(m+\ell, n, d; D)$-extended RMFE over $\mathbb{Z}_{p^k}$.

We construct an $(m, d; D)$-NM-RMFE (ϕ, ψ) over $\mathbb{Z}_{p^k}$ as follows.

- $\phi : \mathbb{Z}_{p^k}^m \to \mathtt{GR}(p^k, d)$ is an $\mathbb{Z}_{p^k}$-linear map, such that
  $\phi : \boldsymbol{x} \mapsto \phi_2(\boldsymbol{x}\|\boldsymbol{r}, \phi_1(\boldsymbol{x}\|\boldsymbol{r}))$, where $\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_{p^k}^\ell$.

Construction of NM-RMFE: 2

- Let (ϕ_1, ψ_1) be an $(m+\ell, n; D)$-RMFE over $\mathbb{Z}_{p^k}$.
- Let (ϕ_2, ψ_2) be an $(m+\ell, n, d; D)$-extended RMFE over $\mathbb{Z}_{p^k}$.

We construct an $(m, d; D)$-NM-RMFE (ϕ, ψ) over $\mathbb{Z}_{p^k}$ as follows.

- $\phi : \mathbb{Z}_{p^k}^m \to \mathtt{GR}(p^k, d)$ is an $\mathbb{Z}_{p^k}$-linear map, such that $\phi : \boldsymbol{x} \mapsto \phi_2(\boldsymbol{x} \| \boldsymbol{r}, \phi_1(\boldsymbol{x} \| \boldsymbol{r}))$, where $\boldsymbol{r} \xleftarrow{\$} \mathbb{Z}_{p^k}^\ell$.
- For a $Y \in \mathtt{GR}(p^k, d)$, compute $(\boldsymbol{y} \| \boldsymbol{s}, e) := \psi_2(Y)$, where $\boldsymbol{y} \in \mathbb{Z}_{p^k}^m$, $\boldsymbol{s} \in \mathbb{Z}_{p^k}^\ell$ and $e \in \mathtt{GR}(p^k, n)$.

  Then $\psi : \mathtt{GR}(p^k, d) \to \mathbb{Z}_{p^k}^m$ is defined as follows:

$$\psi(Y) = \begin{cases} \boldsymbol{y}, & \text{if } \psi_1(e) = (\boldsymbol{y} \| \boldsymbol{s}), \\ \perp, & \text{otherwise}. \end{cases}$$

Summary

Semi-honest NISC over $\mathbb{Z}_{2^k}$

- A NISC/VOLE for branching programs over $\mathbb{Z}_{2^k}$ from combining DARE with RMFE.

Non-Malleable RMFE

- Put forward the notion of Non-Malleable RMFE.
- Show a Non-Malleable RMFE construction, which allows for constructing reusable NISC/VOLE over $\mathbb{Z}_{2^k}$.

Summary

Semi-honest NISC over $\mathbb{Z}_{2^k}$

- A NISC/VOLE for branching programs over $\mathbb{Z}_{2^k}$ from combining DARE with RMFE.

Non-Malleable RMFE

- Put forward the notion of Non-Malleable RMFE.
- Show a Non-Malleable RMFE construction, which allows for constructing reusable NISC/VOLE over $\mathbb{Z}_{2^k}$.

Open questions

- When $m \to \infty$, there exist $(m, d; 2)$-NM-RMFEs over $\mathbb{Z}_{2^k}$ with $\frac{d}{m} \to 29.13$; there exist $(m, d; 3)$-NM-RMFEs over $\mathbb{Z}_{2^k}$ with $\frac{d}{m} \to 80.15$.
  $\Longrightarrow$ Can we construct NM-RMFE with better asymptotic efficiency?
- Our NISC/VOLE is for branching programs over $\mathbb{Z}_{2^k}$.
  $\Longrightarrow$ Can we construct NISC for any circuit over $\mathbb{Z}_{2^k}$?

Full version on ePrint: https://eprint.iacr.org/2023/1363.