

What's New in the MiniMPC Submission

Team MPC MINlons

Hongrui Cui, Chun Guo, Xiaojie Guo, David Heath, Jonathan Katz,
Vladimir Kolesnikov, Alex Malozemoff, Samuel Ranellucci, Mike Rosulek,
Lawrence Roy, Xiao Wang, Chenkai Weng, Kang Yang, Yu Yu

Speaker: Xiaojie Guo @ Shanghai Qi Zhi Institute

NIST Workshop on Multi-Party Threshold Schemes 2026
Jan 28, 2026

Overview: New Gadgets in MiniMPC

- ▶ Simulatable multi-user Tweakable Circular Correlation Robustness with key Leakage (S-mTCCRL) secure hash function
 - Replacing (insecure) correlation robust hash function and (costly) random oracle
 - For authenticated shares \Rightarrow leaky authenticated AND (LaAND) triples

Overview: New Gadgets in MiniMPC

- ▶ **S**imulatable **m**ulti-user **T**weakable **C**ircular **C**orrelation **R**obustness with key **L**eakage (S-mTCCRL) secure hash function
 - Replacing (insecure) correlation robust hash function and (costly) random oracle
 - For authenticated shares \Rightarrow leaky authenticated AND (LaAND) triples
- ▶ **R**otation-based bucketing
 - Removing selective failure in LaAND triples
 - For LaAND triples \Rightarrow authenticated AND (aAND) triples

Overview: New Gadgets in MiniMPC

- ▶ Simulatable multi-user Tweakable Circular Correlation Robustness with key Leakage (S-mTCCRL) secure hash function
 - Replacing (insecure) correlation robust hash function and (costly) random oracle
 - For authenticated shares \Rightarrow leaky authenticated AND (LaAND) triples
- ▶ Rotation-based bucketing
 - Removing selective failure in LaAND triples
 - For LaAND triples \Rightarrow authenticated AND (aAND) triples
- ▶ Modified protocol for provable security
 - One-shot execution for malicious security in universal composability (UC) model
 - Zero sharing for global-key extraction
 - For LaAND triples

S-mTCCRL: A New Notion of Correlation Robustness

- ▶ Motivation: Insecure use of correlation robust hash function H
 - Protocols (e.g., LaAND) output global keys $\{\Delta_i\}_i$
 - Pseudorandomness of protocol messages $\Leftarrow \{\Delta_i\}_i$
 - The joint distribution is **trivially distinguishable**

$$\underbrace{(\Delta_i, H(x \oplus \Delta_i, \tau) \oplus b \cdot \Delta_i \oplus \text{"message"})}_{\text{Both included in the adversarial view, i.e., joint distribution}} \approx_c \$$$

Both included in the adversarial view, i.e., joint distribution

Even for the semi-honest security in the stand-alone model!

S-mTCCRL: A New Notion of Correlation Robustness

- ▶ Motivation: Insecure use of correlation robust hash function H
 - Protocols (e.g., LaAND) output global keys $\{\Delta_i\}_i$
 - Pseudorandomness of protocol messages $\Leftarrow \{\Delta_i\}_i$
 - The joint distribution is **trivially distinguishable**

$$\underbrace{(\Delta_i, H(x \oplus \Delta_i, \tau) \oplus b \cdot \Delta_i \oplus \text{"message"})}_{\text{Both included in the adversarial view, i.e., joint distribution}} \approx_c \$$$

Both included in the adversarial view, i.e., joint distribution

Even for the semi-honest security in the stand-alone model!

- ▶ Previous solution [NNOB12, HSS17]
 - A **programmable** random oracle H
 - Cons: (i) Slow instantiation from SHA256/SHA3, (ii) Non-modular proofs

S-mTCCRL: A New Notion of Correlation Robustness (cont.)

- Our solution: An S-mTCCRL secure hash H^{Prim} in an ideal model Prim

Real world	\approx_c	Ideal world (where a simulator \mathcal{S} has a global-key oracle for Δ)
An ideal primitive Prim , global keys $\Delta = (\Delta_1, \dots, \Delta_n)$	Initialization	A random function F , global keys $\Delta = (\Delta_1, \dots, \Delta_n)$
Distinguisher \mathcal{D} is given		Distinguisher \mathcal{D} is given
<ul style="list-style-type: none"> the oracle Prim the selective-failure oracle for Δ $\{H^{\text{Prim}}(x \oplus \Delta_i, \tau) \oplus b \cdot \Delta_i\}_{i,x,\tau,b}$ 	Phase 1	<ul style="list-style-type: none"> the simulated oracle $\mathcal{S}.\mathcal{O}$ the selective-failure oracle for Δ $\{F(i, x, \tau, b)\}_{i,x,\tau,b}$
\mathcal{D} is given Δ	Key revealing	\mathcal{D} is given Δ , \mathcal{S} is given the query-response pairs of F
\mathcal{D} is given the oracle Prim	Phase 2	\mathcal{D} is given the simulated oracle $\mathcal{S}.\mathcal{O}$

S-mTCCRL: A New Notion of Correlation Robustness (cont.)

- ▶ Pros of S-mTCCRL notion
 - All hash properties used in programming-based proofs
 - More modular proofs from its take-away bounds
 - Fast instantiation from AES-NI

$$H^{\text{Prim}}(x, i) = \widehat{\text{MMO}}^{\mathbf{E}}(x, i) = \mathbf{E}(+, i, \sigma(x)) \oplus \sigma(x),$$

Prim = \mathbf{E} is an ideal cipher model (ICM) and σ is a linear orthomorphism

S-mTCCRL: A New Notion of Correlation Robustness (cont.)

- ▶ Pros of S-mTCCRL notion
 - All hash properties used in programming-based proofs
 - More modular proofs from its take-away bounds
 - Fast instantiation from AES-NI

$$H^{\text{Prim}}(x, i) = \widehat{\text{MMO}}^{\mathbf{E}}(x, i) = \mathbf{E}(+, i, \sigma(x)) \oplus \sigma(x),$$

Prim = \mathbf{E} is an ideal cipher model (ICM) and σ is a linear orthomorphism

- ▶ More results are available at: <https://eprint.iacr.org/2025/1818>
 - LaAND protocol
 - Silent preprocessing of correlated oblivious transfer (COT)
 - ...

LaAND & Rotation-based Bucketing

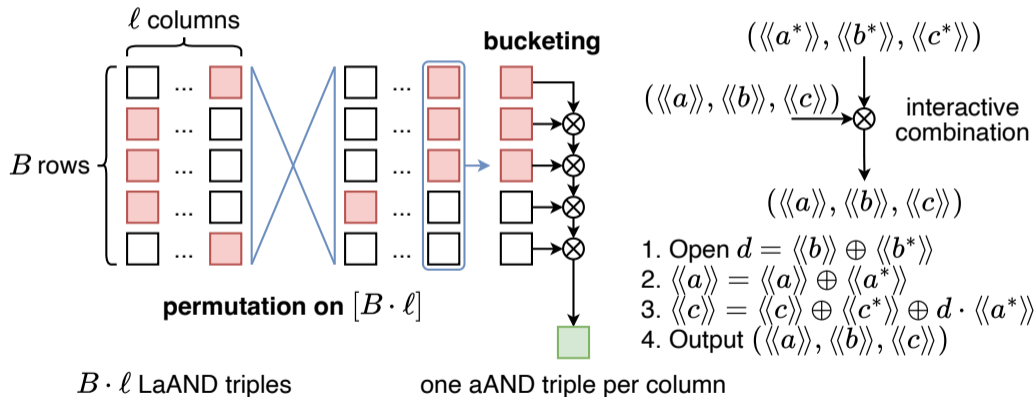
- ▶ An n -party LaAND triple $(\langle\langle a \rangle\rangle, \langle\langle b \rangle\rangle, \langle\langle c \rangle\rangle)$
 - $a, b \in \mathbb{F}_2, c = a \wedge b \in \mathbb{F}_2$
 - BDOZ-style authentication: Each party P_i has a global key $\Delta_i \in \mathbb{F}_{2^\lambda}$ and its share

$$\forall x \in \{a, b, c\} : \langle\langle x \rangle\rangle_i = \left(x^{(i)}, \left\{ M_j \left[x^{(i)} \right], K_i \left[x^{(j)} \right] \right\}_{j \neq i} \right)$$
$$\text{s.t. } \sum_{i \in [n]} x^{(i)} = x \text{ and } \forall j \neq i : M_j \left[x^{(i)} \right] = K_j \left[x^{(i)} \right] \oplus x^{(i)} \cdot \Delta_j$$

- **Leakage:** Selective failure against $\{a^{(i)}, \Delta_i\}_{i \in \mathcal{H}}$ for honest parties in $\mathcal{H} \subseteq [n]$
- ▶ An n -party aAND triple: Same as an LaAND triple but has no leakage

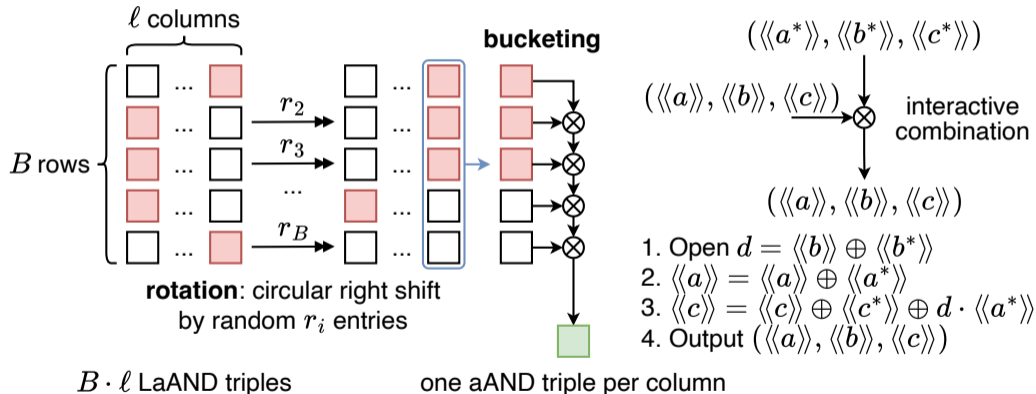
LaAND & Rotation-based Bucketing

- ▶ Previous LaAND \Rightarrow aAND: Permutation-based bucketing [NNOB12]



LaAND & Rotation-based Bucketing (cont.)

- Rotation-based bucketing: $B > 0$ LaAND triples \Rightarrow one aAND triple



LaAND & Rotation-based Bucketing (cont.)

▶ Intuition

- The adversary cannot have “too many” leaky triples without abort
- At least one non-leaky triple in a bucket \Rightarrow the combined triple is not leaky

▶ Why rotation-based bucketing?

- At least one non-leaky triple in every bucket, given “not many” leaky triples
- Much better efficiency than the permutation-based bucketing due to memory access patterns

Protocol Changes

- ▶ Change #1: One-shot LaAND generation for malicious security in the UC model
 - Soundness of check relies on the entropy of $\{\Delta_i\}_{i \in \mathcal{H}}$
 - $\{\Delta_i\}_{i \in \mathcal{H}}$ are revealed to the environment after the first generation
 - Not required in the stand-alone model

Protocol Changes (cont.)

- ▶ Change #2: Zero sharing for global-key extraction in LaAND
 - Protocol sim. guesses $\{\Delta_i\}_{i \in \mathcal{H}} \Rightarrow$ Transcripts to call S-mTCCRL sim. (key swit.)
 - Environment \mathcal{Z} makes $\{\Delta_i\}_{i \in \mathcal{H}}$ -related queries to Prim to distinguish two worlds
 - Given ICM-based hash $H^{\text{Prim}} = \widehat{\text{MMO}}^{\mathbf{E}}$, a real message for $i \in \mathcal{H}$

$$c_i = \mathbf{E}(+, \cdot, a_i) \oplus \mathbf{E}(+, \cdot, a_i \oplus \Delta_i) \oplus \sigma(\Delta_i) \oplus m_i$$

- Case 1: \mathcal{Z} queries $\mathbf{E}(+, \cdot, a_i)$ and $\mathbf{E}(+, \cdot, a_i \oplus \Delta_i)$, $\Delta_i = a_i \oplus (a_i \oplus \Delta_i)$
- Case 2: \mathcal{Z} queries $\mathbf{E}(+, \cdot, a_i)$ and $\mathbf{E}(-, c_i \oplus \mathbf{E}(+, \cdot, a_i) \oplus \sigma(\Delta_i) \oplus m_i)$, **infeasible**

Protocol Changes (cont.)

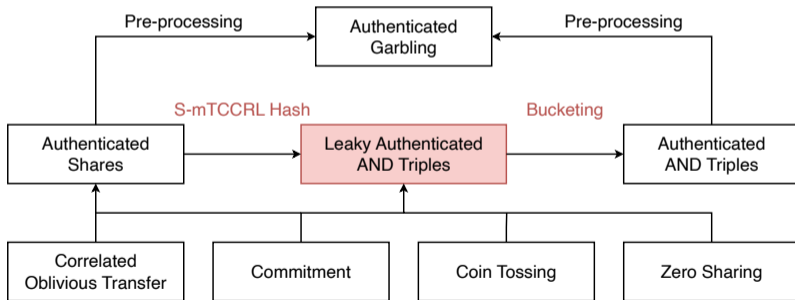
- ▶ Change #2: Zero sharing for global-key extraction in LaAND
 - Protocol sim. guesses $\{\Delta_i\}_{i \in \mathcal{H}} \Rightarrow$ Transcripts to call S-mTCCRL sim. (key swit.)
 - Environment \mathcal{Z} makes $\{\Delta_i\}_{i \in \mathcal{H}}$ -related queries to Prim to distinguish two worlds
 - Given ICM-based hash $H^{\text{Prim}} = \widehat{\text{MMO}}^{\mathbf{E}}$, a real message for $i \in \mathcal{H}$

$$c_i = \mathbf{E}(+, \cdot, a_i) \oplus \mathbf{E}(+, \cdot, a_i \oplus \Delta_i) \oplus \sigma(\Delta_i) \oplus m_i$$

- Case 1: \mathcal{Z} queries $\mathbf{E}(+, \cdot, a_i)$ and $\mathbf{E}(+, \cdot, a_i \oplus \Delta_i)$, $\Delta_i = a_i \oplus (a_i \oplus \Delta_i)$
- Case 2: \mathcal{Z} queries $\mathbf{E}(+, \cdot, a_i)$ and $\mathbf{E}(-, c_i \oplus \mathbf{E}(+, \cdot, a_i) \oplus \sigma(\Delta_i) \oplus m_i)$, **infeasible**
- ▶ **Observation:** Protocol correctness only needs the sum of all c_i 's, not each c_i
 - Replace c_i with $c'_i = c_i \oplus z_i$ s.t. zero sharing $\sum_i z_i = 0$ and $\sum_i c'_i = \sum_i c_i$
 - Uniform masks $\{z_i\}_{i \in \mathcal{H}}$ prevent the backward queries in Case 2

Summary

- ▶ S-mTCCRL hash function for modular proofs and fast implementation
- ▶ Rotation-based bucketing for transforming LaAND to aAND
- ▶ Modifications to LaAND protocol for provable UC security



Thanks!

Team MPC MINlons

Hongrui Cui, Chun Guo, **Xiaojie Guo**, David Heath, Jonathan Katz,
Vladimir Kolesnikov, Alex Malozemoff, Samuel Ranellucci, Mike Rosulek,
Lawrence Roy, Xiao Wang, Chenkai Weng, Kang Yang, Yu Yu