Linear Codes for Secure Computation

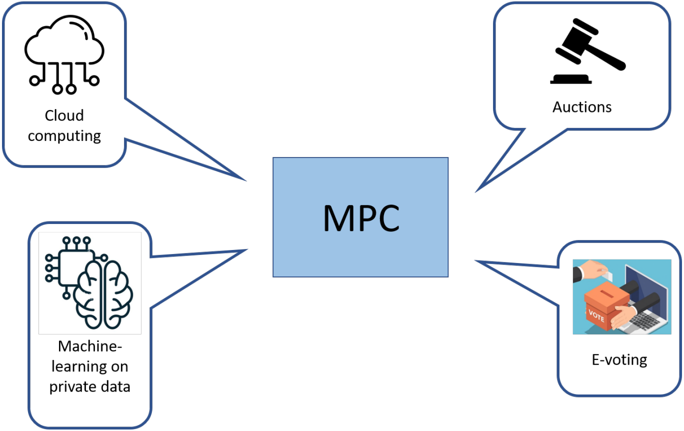
Clément Ducros
Geoffroy Couteau

IRIF

5 avril 2022

Secure Computation : what for ?

Classical cryptography goal : protecting communications. But data can be used in computations.



What is Secure Multiparty Computation (MPC)?

Goal : Consider n players, each ones owning a secret value x_i. Each player wants to compute the result of a function f_i on the entries $(x_j)_{1 \le j \le n}$

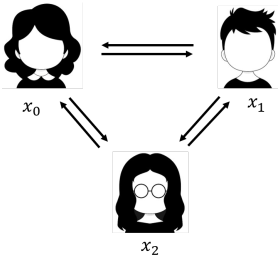
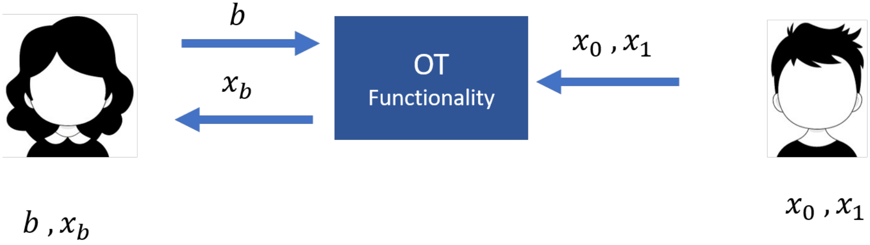


Figure: 3 players MPC

- *Correctness* $\rightarrow$ Each player should get the correct result.
- *Security* $\rightarrow$ Any group of players who ally themselves must not learn more than is already implied by their secret entries and their function.

Example 1 : Oblivious Transfer

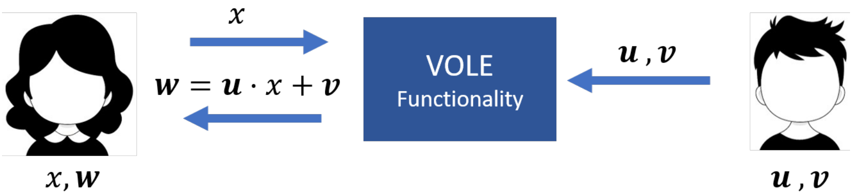


OT requires **public-key cryptography**
Useful correlation for efficiently computing Boolean circuit.

Example 2 : OLE and Vector OLE

OLE : Oblivious Linear Evaluation

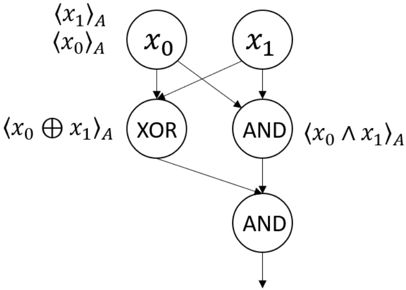
Useful correlation for efficiently computing arithmetic circuit.



How to achieve MPC? [GMW87]

Secret sharing of each inputs !

$$\langle x_0 \rangle_A \oplus \langle x_0 \rangle_B = x_0$$

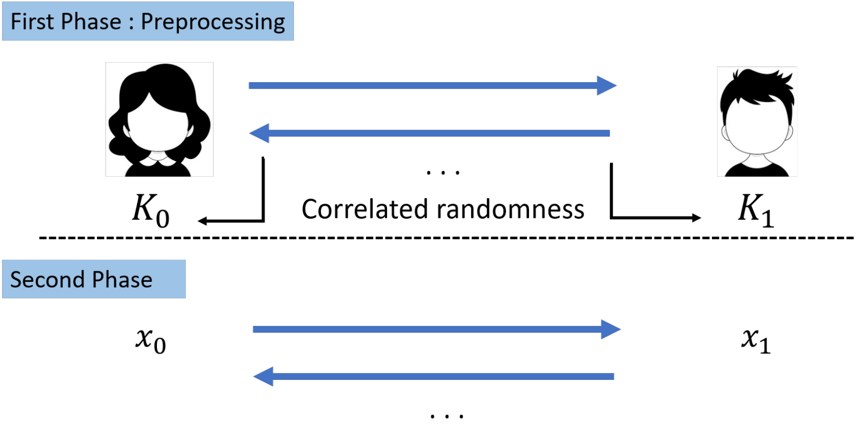


$\langle x_0 \oplus x_1 \rangle_A = \langle x_0 \rangle_A \oplus \langle x_1 \rangle_A$

$\langle x_0 \wedge x_1 \rangle_A =$? Requires 2 OT

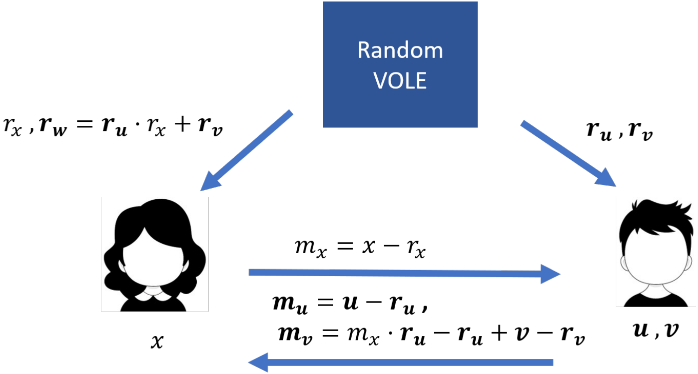
How to achieve MPC?

Research leads to split the protocol in two phases [Bea95, IKNP03]



The first phase is input-independent, and can be done ahead of time

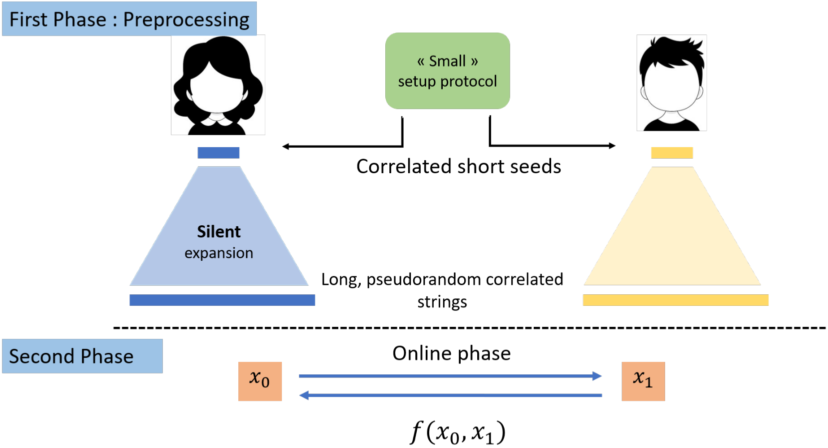
From random VOLE to Pseudorandom Vector OLE



$$\boldsymbol{w} = \boldsymbol{m_u} x + \boldsymbol{m_v} + \boldsymbol{r_w} = \boldsymbol{u} \cdot x + \boldsymbol{v}$$

Question: how to generate many random OTs ? (or others correlations).

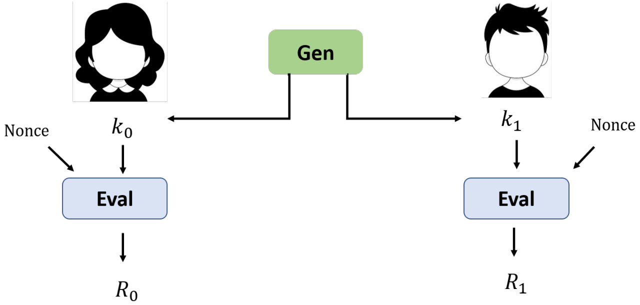
Correlated Randomness generation [BCGI18, BCG+19]



- Very fast online phase
- Few communication to compute
- Downside : we have to do again all the computation when it is done.

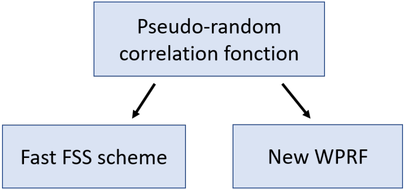
Pseudorandom Correlated Functions(PCF) [BCG+20]

PRF : functions that cannot be distinguished from truly random functions
Equivalent for correlation ?



Correctness : $(R_0, R_1) \approx$ fresh sample of correlation
Security : against insiders

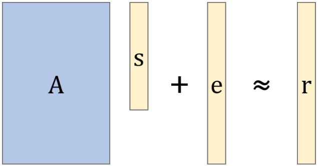
How to construct a PCF ?



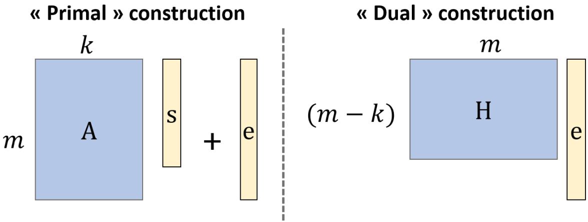
- A Weak Pseudo-Random Function = PRF but the adversary can't chose where to evaluate the functions.

The LPN assumption

Let $A \in \mathbb{F}_q^{m \times k}$, $s \in \mathbb{F}_q^k$, $e \in \mathbb{F}_q^m$, $r \overset{\$}{\in} \mathbb{F}_q^m$, with $\mathcal{HW}(e)$ small.

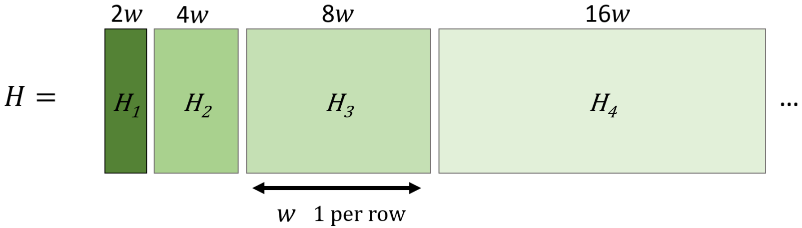


We mostly focus on the dual version of this assumption, which is equivalent

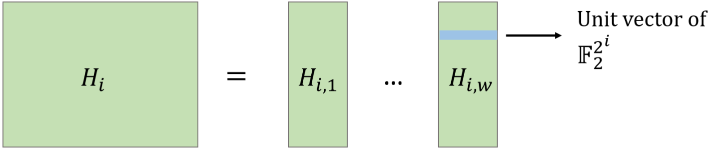


The LPN and the VDLPN assumption

The matrix H and the noise e have some structure !



Exponentially decreasing density. The noise have the shape of one line of H.



Linear attacks examples

Attacks	Types of attacks
Gaussian elimation	Linear
Stasistical decoding	Linear
Information set decoding	Linear
BKW	Linear
Algebraic	Non-linear
Statistical Query Algorithm	Non-linear

Linear attacks for our variants

Definition (Bias of a distribution)

Given a distribution $\mathcal{D}$ over $\mathbb{F}_2^n$, a vector $\mathbf{u} \in \mathbb{F}_2^n$:

$$\text{bias}_u(\mathcal{D}) = \left| \frac{1}{2} - \underset{\mathbf{v} \xleftarrow{\$} \mathcal{D}}{Pr} [\mathbf{u}^\top \cdot \mathbf{v} = 1] \right|$$

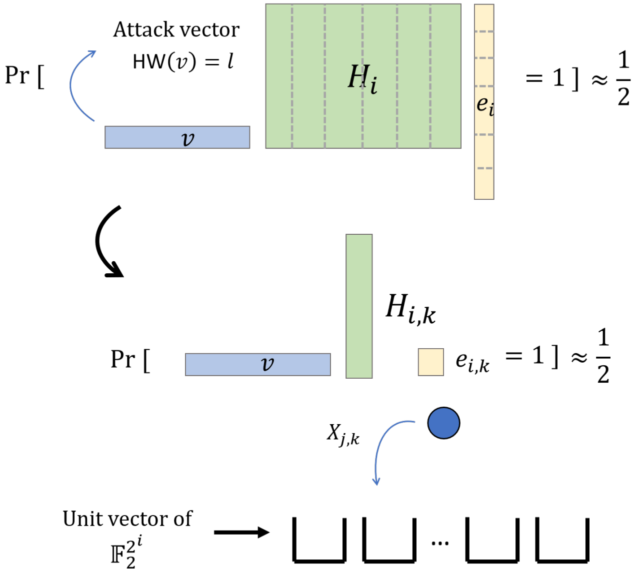
Definition (Resistance against linear attacks)

We obtain the resistance against linear attacks when

$$\underset{x^{(1)}, \cdots, x^{(N(\lambda))} \xleftarrow{\$} \mathbb{F}_2^{n(\lambda)}}{Pr} [\text{bias}(\mathcal{D}(x) > \epsilon(\lambda)] < \delta(\lambda)$$

where ϵ and δ are small depending on the security parameter λ.

Analysis of security



Analysis of security

We define $R_{i,l,k} = (\mathbf{v}^\top \cdot H_{i,k}) = \left(\bigoplus_{j=1}^{l} X_{j,k}\right)$ and $Z_{i,l,k}$ as $Z_{i,l,k} = |2^{i-1} - R_{l,k}|$.

Definition (δ-Bad Matrices)

Let $M \in \mathbb{F}_2^{N \times 2^i}$. We say that $M \in \mathrm{Bad}_{\delta,\mathbf{v}}$ with respect to a vector $\mathbf{v} \in \mathbb{F}_{2^N}$ if

$$(\mathbf{v}^\top \cdot M) = Z_{l,k} \in \left[(1/2 - \delta) \cdot 2^i, 2^{i-1}\right].$$

Given vector $\mathbf{v}$, we denote $B_{\delta,\mathbf{v}} = \#\mathrm{Bad}_{\delta,\mathbf{v}}$.

Lemma

For any $\mathbf{v} \in S_{i,N}$, there is a constant C such that

$$\Pr\left[B_{\delta,\mathbf{v}} > \alpha \cdot w\right] \leq 2^{-C \cdot 2^i \cdot w}$$

Analysis of security

We introduce a function Φ

$$\Phi\left(X_{1,1},\cdots,X_{l,w}\right)=2^{i-1}\cdot w-\sum_{k=1}^{w}Z_{l,k}.$$

$$\Pr\left[B_{\delta,\mathbf{v}}\geq\alpha\cdot w\right]\leq\Pr\left[\Phi(X_{1,1},\cdots,X_{l,w})<\gamma\cdot w\cdot 2^{i}\right],$$

Φ is 2-Lipschitz : we use the Bounded Difference Inequality.

Proposition (Bounded Difference Inequality)

Let $\Phi:[n]^m\to\mathbb{R}$ be a function satisfying the Lipschitz property with constant d, and let $(X_1,\cdots,X_m)$ e independant random variables over $[n]$)

$$\Pr[\Phi(X_1,\cdots,X_m)<\mathbb{E}[\Phi(X_1,\cdots,X_m)]-t]\leq\exp(-\frac{2t^2}{m\cdot d^2})$$

Analysis of security

Remains to find an upper bound of $\mathbb{E}[\Phi] \to$ find an upper bound of $\mathbb{E}[Z_{l,k}]$.
There was an error in the proof [BCG$^+$20]!
Correction

$$\mathbb{E}\left[Z_{l,k}\right] = \sum_{j=0}^{2^{i-1}-1} \Pr(R_{l,k} \geq j + 1 + 2^{i-1}) + \sum_{j=0}^{2^{i-1}-1} \Pr(R_{l,k} \leq 2^{i-1} - j - 1)$$

1. We bound the shares that we can with the Generalized Chernoff Inequality.
2. For that we had to prove that the distribution of the $R_{l,k}$ shows some kind of independence.
3. We bound the remaining shares with a trivial bound.

We have to remember the union bound !
This corrects the proof but is highly unpractical, with $w \approx 10^6$.

Analysis of security - Generalized Chernoff Inequality

Proposition

Let $n \in \mathbb{N}$ an integer, and let $(Y_1, \cdots, Y_n)$ be independent boolean random variables such that, for some $\eta \in [0,1]$ it holds that for every subset $S \in [n]$, $\Pr\left[\bigwedge_{q\in} Y_q\right] \leq \eta^{|S|}$. *Then for any $\kappa \in [\eta, 1]$,*

$$\Pr\left[\sum_{q=1}^{n} Y_q \geq \kappa n\right] \leq \exp\left(-n \cdot D_{KL}\left(\kappa || \eta\right)\right),$$

where $D_{KL}(\kappa||\eta)$ denotes the relative entropy function, defined as

$$D_{KL}\left(\kappa||\eta\right) = \kappa \cdot \ln \frac{\kappa}{\eta} + (1-\kappa) \ln\left(\frac{1-\kappa}{1-\eta}\right).$$

Analysis of security - New approach

A new proof :

- Simulation to prove that $\mathbb{E}[Z] < \beta^i$ with better β
- Erasing the corner cases.
- A new idea to bound the bias :

$$\Pr[\text{bias}_{\mathbf{v}}(\mathcal{O}^i_{\text{par}}) > B] = \Pr\left[\prod_{k=1}^{w} Z_{i,l,k} > 2^{(i-1)w} \times (2B)\right].$$

- The *sum* $\sum_k Z_{i,l,k}$ is minimized when all the terms in the product are equal.

$$\Pr[\text{bias}_{\mathbf{v}}(\mathcal{O}^i_{\text{par}}) > B] \leq \Pr\left[\sum_{k=1}^{w} Z_{i,l,k} > w \cdot 2^{(i-1)} \cdot c\right],$$

- With this sum we can apply again our results with the function Φ.

- We obtain with this new proof $w \approx 350$.

Estimation of the **concrete cost** of the PCFs.

- Seed size: 2.55MB
- PCF evaluation time: ≈ 500 PCF evaluations per second on a single 3GHz processor.

Another work of [BCG+20] also suggested an improved all prefix variant. No proof of the security for this variant yet, but very promising values.

- Seed size: 0.34MB.
- PCF evaluation time: around 3500 evaluations per second on a single 3GHz processor.

Conclusion and open questions

- Pseudo-random Function achieves very promising parameters.

Open Problems and ongoing works :

- All prefix Variant
- Variable density matrix shapes.
- Ring LPN and variants

Questions ?

References

Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl.
Efficient pseudorandom correlation generators: Silent OT extension and more.
In Alexandra Boldyreva and Daniele Micciancio, editors, *CRYPTO 2019, Part III*, volume 11694 of *LNCS*, pages 489–518. Springer, Heidelberg, August 2019.

Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, and Peter Scholl.
Correlated pseudorandom functions from variable-density LPN.
In *61st FOCS*, pages 1069–1080. IEEE Computer Society Press, November 2020.

Elette Boyle, Geoffroy Couteau, Niv Gilboa, and Yuval Ishai.
Compressing vector OLE.
In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 896–912. ACM Press, October 2018.

Donald Beaver.
Precomputing oblivious transfer.
In Don Coppersmith, editor, *CRYPTO'95*, volume 963 of *LNCS*, pages 97–109. Springer, Heidelberg, August 1995.

Oded Goldreich, Silvio Micali, and Avi Wigderson.
How to play any mental game or A completeness theorem for protocols with honest majority.
In Alfred Aho, editor, *19th ACM STOC*, pages 218–229. ACM Press, May 1987.

Yuval Ishai, Joe Kilian, Kobbi Nissim, and Erez Petrank.
Extending oblivious transfers efficiently.
In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 145–161. Springer, Heidelberg, August 2003.