When Bad News Become Good News
Towards Usable Instances of Learning with Physical Errors

Davide Bellizia\textsuperscript{1}  Clé\text{\'e}ment Hoffmann\textsuperscript{1}  Dina Kamel\textsuperscript{1}  Pierrick Méaux\textsuperscript{2}  François-Xavier Standaert\textsuperscript{1}

\textsuperscript{1} UCLouvain, ICTEAM, Crypto Group, Louvain-la-Neuve, Belgium
firstname.lastname@uclouvain.be

\textsuperscript{2} Luxembourg University, SnT, Luxembourg
pierrick.meaux@uni.lu

Monday 19\textsuperscript{th} September, 2022
Learning problems

Learning problems have proven to be interesting computationally hard problems.

- LPN
- LWE
- LWR
- MLWE

⇒

- One-way function
- Secret-key encryption scheme
- Post-quantum PKE
- Identity-based encryption
- Secure MPC
- Indistinguishability obfuscation

...
Learning problems - Presentation

\[ k \sim \mathbb{F}_2^n \]

\[ a \sim \mathbb{F}_2^n \rightarrow \langle a, k \rangle + e \]

LPN samples
Learning problems - Implementation

\[ a \leftarrow \mathbb{F}_2^n \quad \langle a, k \rangle + e \]

RNG$_1$ → LPN samples → RNG$_2$
Learning problems - Implementation

$ a \leftarrow \mathbb{F}_2^n \quad \langle a, k \rangle + e\]

side-channel weakness

LPN samples
Physical learning problems - Presentation

Side-channel weakness

\[ a \leftarrow \mathbb{F}_2^n \rightarrow \langle a, k \rangle + e \]

LPN samples
Physical learning problems - Presentation

\[ a \leftarrow \mathbb{F}_2^n \]

LPPN samples

e.g. clock or voltage manipulation

\[ \text{RNG}_1 \]

[Image of a diagram showing a process involving random number generation and mapping to a sample set.]
Physical learning problems - Data dependencies

**Output data dependencies:**

- Error probability depending on the correct output value
- Not negligible
- Reduction for LPPN

**Input data dependencies:**

- Computationally hard to exploit
- Can be made small by design

Error probability depending on the correct output value
Physical learning problems - Data dependencies

**OUTPUT DATA DEPENDENCIES:**

- Error probability depending on the correct output value
  - Not negligible
  - Reduction for LPPN

Error probability depending on the correct output value
Physical learning problems - Data dependencies

**Output data dependencies:**

- Error probability depending on the correct output value
  - Not negligible
  - Reduction for LPPN

**Input data dependencies:**

- Computationally hard to exploit
- Can be made small by design
Can this extend to LWE?

**Goal:**

- From $\mathbb{GF}_2$ to larger rings/fields
- Error distribution approximating a $\text{CBD}_2$ or $3$ (used in Kyber)
Inner product structure

\[ \langle a, k \rangle \]
Natural solution - Presentation

\[ \langle a, k \rangle \]
Inexact computation occurs at the final adder stage.
Natural solution - Results

LWPE\textsubscript{A}: Error distribution approximating $CBD_3$.
Bad news - Mathematical data dependencies (1/2)

**Toy Example:**
- $\langle a, k \rangle = 0$
- modulo 4
Toy example:

- $\langle a, k \rangle = 0$
- modulo 4

$\langle a, k \rangle = 00$
Bad news - Mathematical data dependencies

Regular LWE

\begin{align*}
\text{Value of last 2 LSBs of } & \langle a, k \rangle \\
\text{error} & \\
& 0 \quad 1 \quad 2 \quad 3
\end{align*}

LWPE\textsubscript{A}

\begin{align*}
\text{Value of last 2 LSBs of } & \langle a, k \rangle \\
\text{error} & \\
& 0 \quad 1 \quad 2 \quad 3
\end{align*}
Bad news - Mathematical data dependencies

Regular LWE

LWPE_A
Inexact computation occurs at the intermediate adder stage.
- Inexact computation occurs at the intermediate adder stage
- Inexact computation occurs on LSBs
Results

**LWPE**

*Learning With Physical Error*

Monday 19\textsuperscript{th} September, 2022
Good news - physical data dependencies

\[ a \times \langle a, k \rangle \]

Adding independent uniform diffuses mathematical data dependencies

Coupling could still cause output dependencies
Good news - physical data dependencies

- Adding independent uniform diffuses mathematical data dependencies

- Coupling could still cause output dependencies
FPGA prototype and data dependencies

LWPE FPGA prototype (dashed lines are only for configuration and testing).

Empirical verification that **data dependencies** cannot be observed
Conclusion - What did we gain?

Interesting potential against leakage
Conclusion - What did we gain?

Interesting potential against leakage

- **Linear** overhead in the shares number
Conclusion - What did we gain?

Interesting potential against leakage

- **Linear** overhead in the shares number
- Trivial composition (key-homomorphic)

\[ \langle a, k \rangle = \langle a, k_0 \rangle + \langle a, k_1 \rangle + \cdots + \langle a, k_{d-1} \rangle \]
Conclusion - What did we gain?

Interesting potential against leakage

- **Linear** overhead in the shares number
- Trivial composition (key-homomorphic)
- Inherently good against glitches

\[ \langle a, k \rangle = \langle a, k_0 \rangle + \langle a, k_1 \rangle + \cdots + \langle a, k_{d-1} \rangle \]
Conclusion - Next steps (1/2)

Find an application of this **design space** (e.g. CPE encryption, signature)
**Theoretical work:**

- Understanding the impact of physical data dependencies
- **Reduction** towards standard learning problems
Figure 6: LPPN processor calibration: error probability (top) and control signal (bottom).