Machine-Learning Side-Channel Attacks on the GALACTICS Constant-Time Implementation of BLISS

Soundes Marzougui[1] <soundes.marzougui@tu-berlin.de>, Nils Wisiol[1], Patrick Gersch[1]
Juliane Krämer[2], Jean-Pierre Seifert[1]
[1] Technical University of Berlin
[2]Technical University of Darmstadt

Motivation: Security of the GALACTICS Implementation

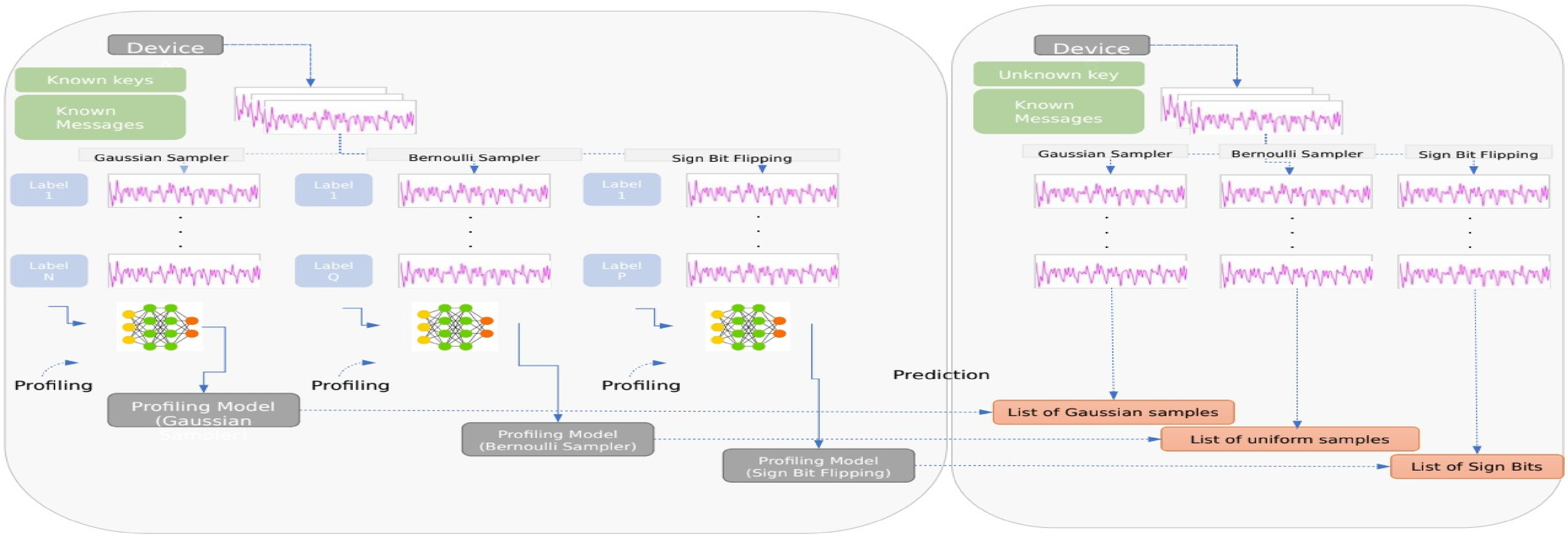
- GALACTICS [1] is a constant-time implementation of the BLISS lattice-based signature scheme
- A constant-time sign flip implementation that avoids the conditional branching on the sensitive information about the flipped sign.
- A constant-time implementation of the Cumulative Distribution Table-based Gaussian sampling routine
- A constant-time and efficient implementation of the Bernoulli sampling relying on polynomial approximation.
- The polynomial approximation employs integer polynomials and avoids floating point multiplication and division altogether, due to their non-constant time execution.
- It has been proven experimentally, using the dudect by Reparaz et al. [2], that the implementation is constant time.

Three Attacks on the GALACTICS Implementation

Attack	Leakage				Required Signatures
	CDT Samples x	Sign Bit a	Uniform sample	Sign Bit b	
Attack 1	•	•	•	•	320
Attack 2			•		2,000
Attack 3				•	250,000

Table 1: Comparison of required leaked information for different attacks on the GALACTICS Implementation

Machine-Learning Model for Profiled Attacks



Secret Key Retrieval

Key Idea: The first attack targets the entire signing process. The attacker is hence able to predict all leakages, with certain accuracy. By employing the predicted values, we demonstrate how to build a system of linear equations, such that its solution is the secret key. In the second attack, we assume that only information about Bernoulli rejection during the Gaussian sampling to obtain information on whether $yu = 0$ is available to the attacker[3]. The third attack consists of recovering the sign flip indicators b during the signing process. Then, the secret key recovery is carried out using a maximum likelihood estimation. [4].

$$z = (-1)^a(Kx + y_u) + (-1)^b < c.s >$$

Attack 1 | Attack 2 | Attack 3

(z,c) is the signature
s is the secret key
a, x, yu, and b are unknown to the public

Performance of our Profiling Models

Leakage	Labels Y	Accuracy on Device B		
		Trivial	Linear Regression	MLP
CDT Sample x	{0,1,2,…,4}	77%	82.03%	93.03%
Uniform Sample	{ = 0, 0}	99.6%	99.10%	*99.95%
Sign Bit a	{a= 0, a 0}	50.0%	99.80%	99.97%
Sign Bit b	{b= 0, b 0}	50.0%	99.67%	100%

- Optimized for a low false positive rate, at the expense of higher false negative rate, but exceeding linear regression in both false positive (reduction by 38%) and false negative rate (reduction by 28%)

Table 2: Overview on the GALACTICS power side-channel leakage studied in this work and the performance of our predicted models, trained on data from Device A

Future Work

- Masking the Bernoulli rejection and sign bit flipping is a possible way to avoid the three attacks we presented in this work.
- We propose partial masking techniques as a countermeasure to the first two attacks (similar to the method proposed by Barthe et al. in [1]).
- It consists in sampling each uniform samples in two halves and add them separately to the sample Gaussian samples. In this case, predicting *one of the two halves* would be useless, as would *the second half*.
- This results in an increasing number of needed signatures, scaling up exponentially with the number of shares.
- A similar approach can be taken to mask the sign flip as proposed in [1]. Here, n shares are generated uniformly at random to build a Boolean sharing of a value in {0,1}.

References

[1] *Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Mélissa Rossi, and Mehdi Tibouchi, GALACTICS: Gaussian Sampling for Lattice-Based Constant- Time Implementation of Cryptographic Signatures Revisited, In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 2147–2164. DOI:https://doi.org/10.1145/3319535.3363223*
[2] *Oscar Reparaz, Josep Balasch, and Ingrid Verbauwhede*, Dude, is my code constant time? In *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*, pages 1697–1702, 2017.
[3] *Groot Bruinderink, L., Hülsing, A. T., Lange, T., and Yarom, Y., Flush, Gauss, and reload : a cache attack on the BLISS lattice-based signature scheme*, (Cryptology ePrint Archive ; Vol. 2016/300). IACR. http://eprint.iacr.org/2016/300
[4] *Mehdi Tibouchi and Alexandre Wallet,* One Bit is All It Takes: A Devastating Timing Attack on BLISS's Non-Constant Time Sign Flips, Journal of Mathematical Cryptography, https://doi.org/10.1515/jmc-2020-0079