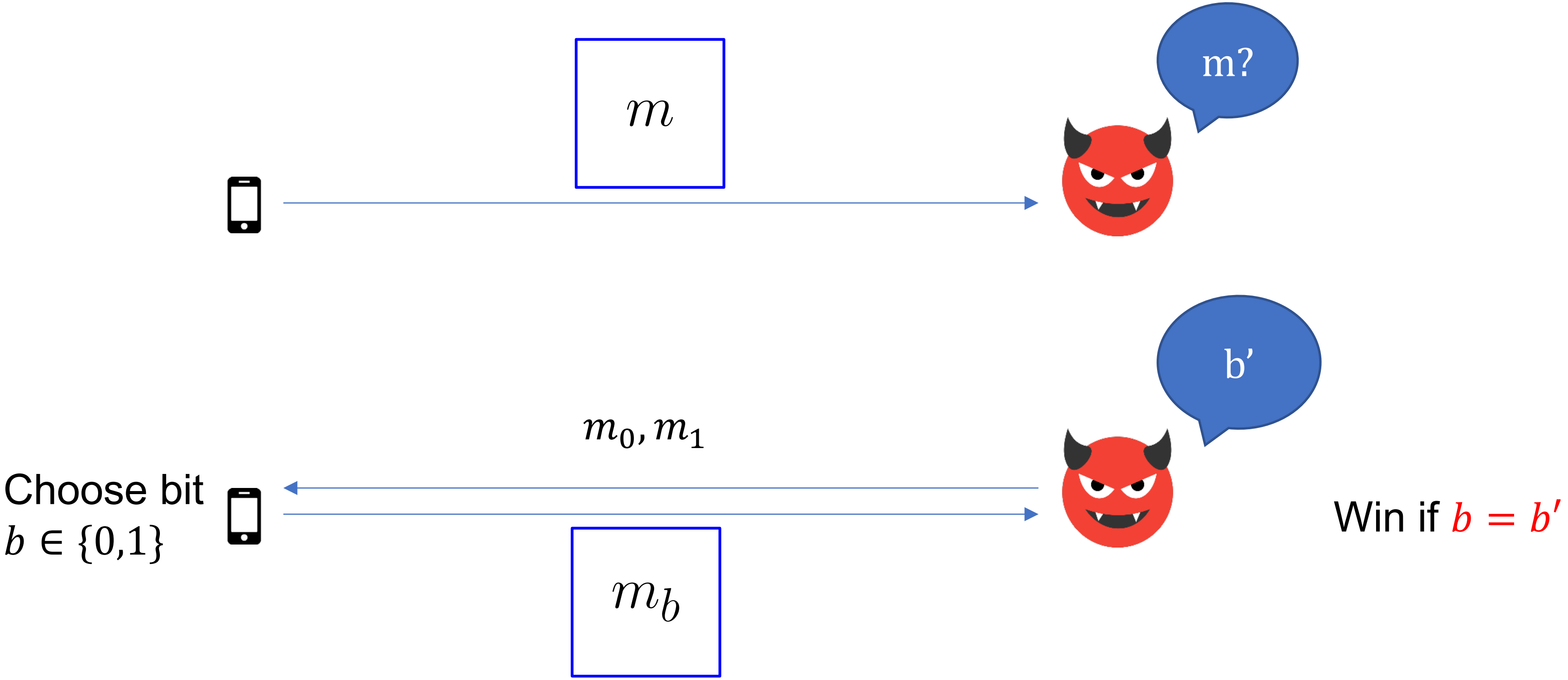
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

GG-GSW: CCA Leveled FHE from Gadget Trapdoors

Jérôme Nguyen

FHE.org Conference
08.03.26

Security Model: Chosen-Plaintext Attacks (CPA)



Stronger Security Models

CPA^D security	CCA1 security
• Decryption of legitimate ciphertexts • Queries may depend on challenge bit	• Decryption of any ciphertext • Queries cannot depend on challenge bit

The Cost of Stronger Security

Common techniques:

CPA^D security

- Noise flooding on decryption
- For "exact" FHE: perfect correctness

➢ Needs exponentially wide distribution
➢ Average-case and heuristic analysis is common

CCA1 security

- Use a proof of knowledge (NIZK/SNARK)

➢ Compatibility issues with FHE operations
➢ Often strong assumptions
➢ Can hurt compactness

Research Questions

Are there cheaper methods to obtain CPA^D & CCA1 security?

CPA^D security	CCA1 security
• Without exponential noise flooding • Security independent of correctness	• No proof of knowledge

GG-GSW: CCA1 secure leveled FHE

Introduce a new leveled FHE scheme:

- CCA1 secure, based on LWE in the standard model
- variant of (dual) GSW: same homomorphic operations
- preserves compactness, similar scaling to GSW

New method to obtain CPA^D security:

- security independent of correctness
- specialized for GSW over branching programs
- randomized homomorphic evaluation, “almost for free”

Gadget Matrix [MP11]

A gadget matrix G:

$$g = (1, 2, \ldots, 2^{k-1}) \in \mathbb{Z}^k$$

$$G = I_n \otimes g = \begin{pmatrix} \cdots g \cdots & & & \\ & \cdots g \cdots & & \\ & & \ddots & \\ & & & \cdots g \cdots \end{pmatrix} \in \mathbb{Z}^{n \times nk}$$

There exists a function G^{-1} such that for all matrices A

- $G^{-1}(A)$ has small coefficients
- $G \cdot G^{-1}(A) = A$

Gadget Trapdoors

Let A_1 be uniformly random, R short

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \end{pmatrix}$$

Given R, search-LWE is easy for A

$$C = AS + E$$
$$(S, E) \leftarrow \text{Invert}(R, A, C)$$

$\text{Invert}(R, A, C)$:

1. Compute $\hat{G}S + [R|I]E \leftarrow [R|I]C$
2. $\ldots$
3. Return (S,E)

GG-GSW: KeyGen and Encryption

$\mathrm{Gen}(1^\lambda)$:

1. Sample $A_1 \xleftarrow{\$} \mathbb{Z}^{m \times n}$ and short $R \in \mathbb{Z}^{nk \times m}$ and $x \in \mathbb{Z}^m$
2. Return

$$sk = (R, x), \quad pk = A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

$\mathrm{Enc}(pk, \mu)$:

1. Sample uniform S and short E
2. Return

$$C = AS + E + \mu G$$

$$g = (1, 2, \ldots, 2^{k-1}) \in \mathbb{Z}^k$$
$$G = I_{m+nk} \otimes g$$
$$\hat{G} = I_n \otimes g^\top$$

Use 2 gadget matrices

- G for multiplication
- $\hat{G}$ (smaller, transposed) as trapdoor for CCA1 security

GG-GSW: Decryption

Dec(sk, C):

1. Compute $\mu = \text{Round}((x, 0, 1)C)$
2. Compute $(S, E) \leftarrow \text{Invert}(R, A, C - \mu G)$
3. If E too big return $\perp$
4. Return μ

GG-GSW: Decryption

$\text{Dec}(sk, C)$:

1. Compute $\mu = \text{Round}((x, 0, 1)C)$
2. Compute $(S, E) \leftarrow \text{Invert}(R, A, C - \mu G)$
3. If E too big return $\perp$
4. Return μ

$$C = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix} S + E + \mu G$$

1. $(x, 0, 1)C = E' + \mu(x, 0, 1)G$
2. $C - \mu G = AS + E$
3. $(R, I, 0)(C - \mu G) = \hat{G}S + E''$

GG-GSW: Homomorphic operations

Unchanged from GSW!

$\mathrm{Add}(C_1, C_2)$:
  Return $C_1 + C_2$

$\mathrm{Mult}(C_1, C_2)$:
  Return $C_1 \cdot G^{-1}(C_2)$

Security Proof Sketch

Lemma:

$\text{Dec}(sk, C)$:

1. Compute $\mu = \text{Round}((x, 0, 1)C)$
2. Compute $(S, E) \leftarrow \text{Invert}(R, A, C - \mu G)$
3. If E too big return $\perp$
4. Return μ

$\text{stat-Dec}(C)$:

1. Solve search-LWE and recover (S, E, μ)
2. If E too big return $\perp$
3. Return μ

With overwhelming probability over the key generation randomness, for all ciphertexts, both procedures output the same value.

Security Proof Sketch

Game 0:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

$$C^* = AS + E + \mu_b G$$

Decryption:

$\mathrm{Dec}(sk, C)$

Lemma

Game 1:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

$$C^* = AS + E + \mu_b G$$

Decryption:

stat-Dec(C)

Security Proof Sketch

Game 1:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

$$C^* = AS + E + \mu_b G$$

Decryption:
stat-Dec(C)

LHL

Game 2:

$$A = \begin{pmatrix} A_1 \\ RA_1 \\ -xA_1 \end{pmatrix}$$

$$C^* = AS + E + \mu_b G$$

Decryption:
stat-Dec(C)

Security Proof Sketch

Game 2:

$$A = \begin{pmatrix} A_1 \\ RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
stat-Dec(C)

$$C^* = AS + E + \mu_b G$$

Stat.

Game 3:

$$A = \begin{pmatrix} A_1 \\ -RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
stat-Dec(C)

$$C^* = \begin{pmatrix} C_1 = A_1 S + E_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

Security Proof Sketch

Game 3:

$$A = \begin{pmatrix} A_1 \\ -RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
stat-Dec(C)

$$C^* = \begin{pmatrix} C_1 = A_1 S + E_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

LHL
+ Lemma

Game 4:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
Dec(sk, C)

$$C^* = \begin{pmatrix} C_1 = A_1 S + E_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

Security Proof Sketch

Game 4:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
$\mathrm{Dec}(sk, C)$

$$C^* = \begin{pmatrix} C_1 = A_1 S + E_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

LWE

Game 5:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
$\mathrm{Dec}(sk, C)$

$$C^* = \begin{pmatrix} C_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

Security Proof Sketch

Game 5:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
$\mathrm{Dec}(sk, C)$

$$C^* = \begin{pmatrix} C_1 \\ -RC_1 + E' \end{pmatrix} + \mu_b G$$

LHL
+ Lemma

Game 6:

$$A = \begin{pmatrix} A_1 \\ \hat{G} - RA_1 \\ -xA_1 \end{pmatrix}$$

Decryption:
stat-Dec(C)

$$C^* = \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} + \mu_b G$$

Conclusion

CCA1-secure leveled FHE scheme

- No proofs of knowledge required
- Complexity similar to GSW

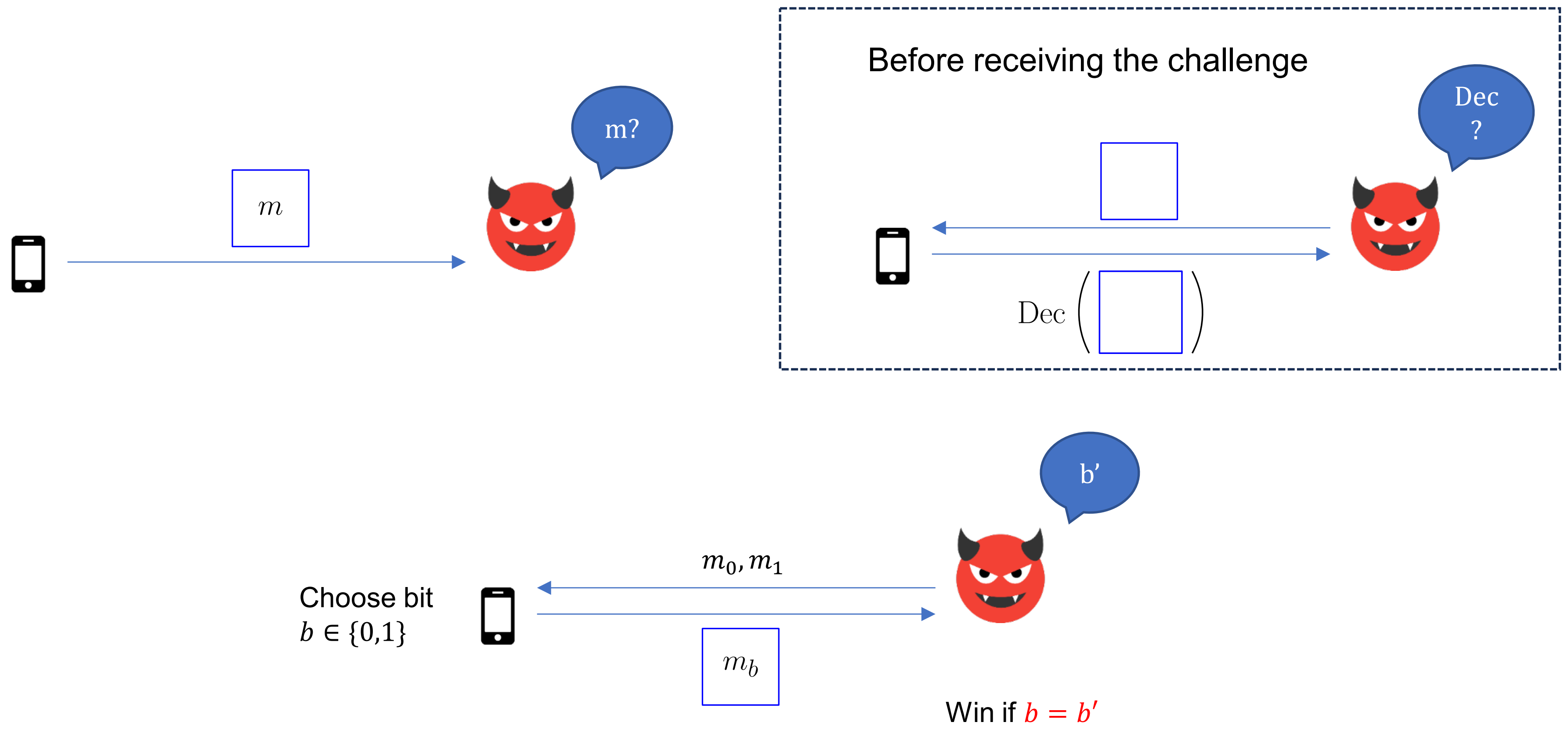
CPA^{D} security “almost for free”

- No need to rely on correctness
- Noise estimations can be average-case, heuristic, or even wrong ☺

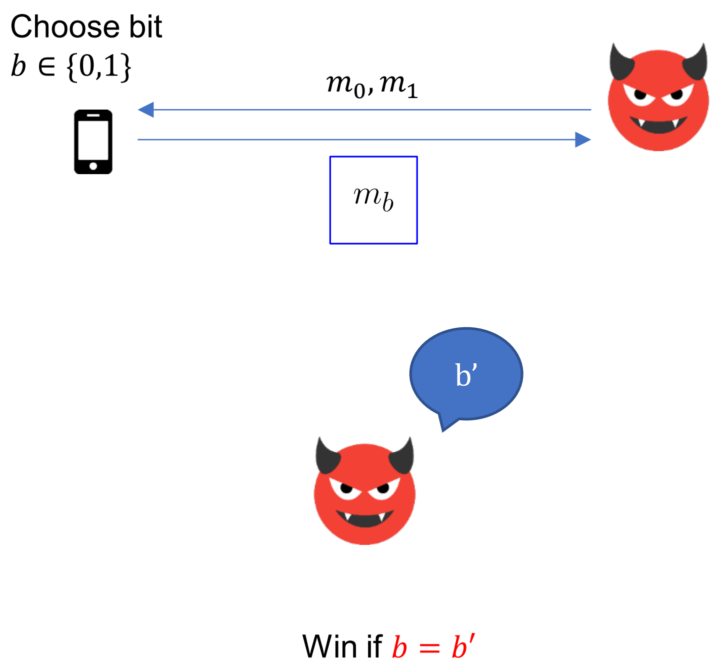
Thank You!

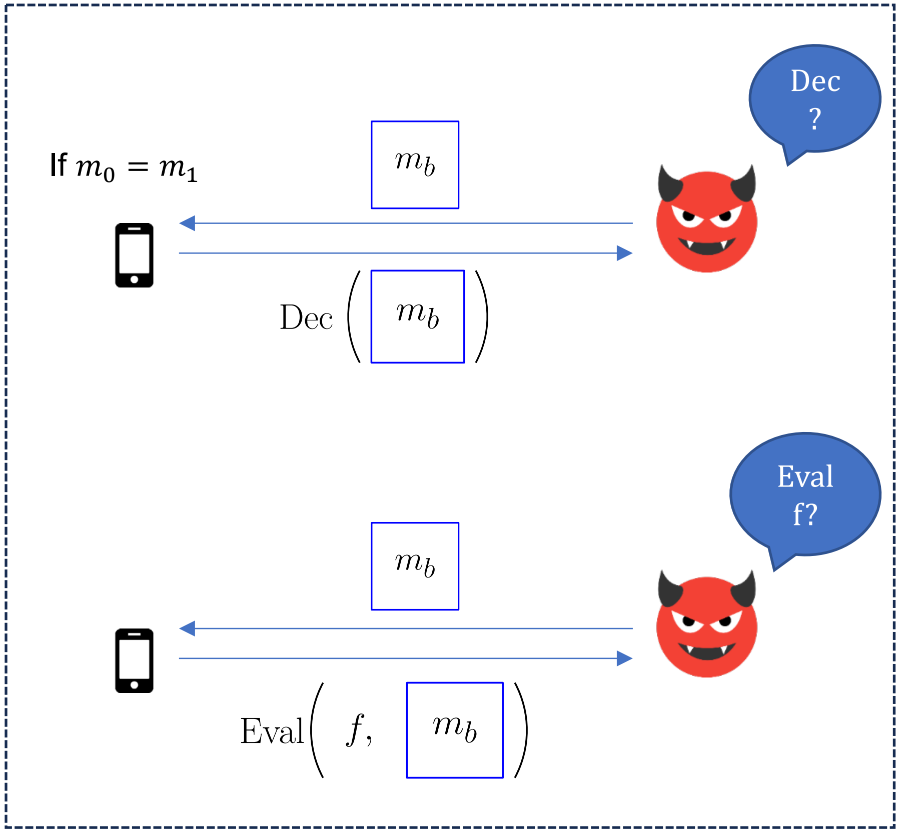
Paper available at:
eprint.iacr.org/2026/316

Security Model: CCA1



Security Model: CPA^{D}





Obtaining IND-CCA1 Security

Known methods for CCA1 Security		
Naor-Yung [NY90]	Cramer-Shoup [CS98]	Micciancio-Peikert [MP11]
Double encryption + NIZK	Hash proof system	Gadget trapdoor
Requires proof of HomEval	No lattice equivalent	Not homomorphic

CCA1 from gadget trapdoors [MP11]

- Based on LWE
- Uses a gadget trapdoor for CCA1 security

Gen(1^λ):

$A_1 \stackrel{\$}{\leftarrow} \mathbb{Z}^{n\times m}, R \leftarrow \mathbb{Z}^{m\times nk}$ short

$A_2 = -A_1 R$

$pk = [A_1 \| A_2], sk = R$

$Enc_{pk}(m)$:

$A_U = [A_1 | UG - A_1 R]$

$b = sA_U + e + (0, E(m))$

$c = (U, b)$

$Dec_{sk}(U, b)$:

$(s, e) \leftarrow \text{Invert}(R, (A_U, b))$

If $||e||$ small enough:

Return E(m)

The GSW FHE scheme [GSW13, AP14]

- Based on LWE
- Uses gadget matrices for homomorphic multiplication

$\text{Gen}(1^\lambda)$:

$sk = s \in \mathbb{Z}^n$

$$pk = A = \begin{pmatrix} A_1 \\ sA_1 + e \end{pmatrix}$$

$Enc_{pk}(\mu)$:

$C = AR + \mu G$

$Dec_{sk}(C)$:

Compute $(s, -1)C$

Recover μ from $\mu G + e'$

Return μ