# Exploiting Decryption Failures in Mersenne Number Cryptosystems

**Marcel Tiepelt**[1] and Jan-Pieter D'Anvers[2]

[1]Kastel, Karlsruhe Institute of Technology, marcel.tiepelt@kit.edu
[2]imec-COSIC, KU Leuven, janpieter.danvers@esat.kuleuven.be

APKC
Oct. 6, 2020, Taipei, Taiwan,

# Decryption Failures in Post-Quantum Cryptography

*What?*

- $m \neq decrypt(encrypt(m))$
- Artificial errors in post-quantum crypto

*Why?*

- Efficiency

# Decryption Failures in Post-Quantum Cryptography

*What?*

- $m \neq decrypt(encrypt(m))$
- Artificial errors in post-quantum crypto

*Why?*

- Efficiency
- Probabilities of failure:

Kyber: $2^{-160}$
Saber: $2^{-136}$

HQC: $2^{-138}$
LEDAcrypt: $2^{-64}$

Ramstake: $2^{-64}$

# Decryption Failures in Post-Quantum Cryptography

*What?*

- $m \neq decrypt(encrypt(m))$
- Artificial errors in post-quantum crypto

*Why?*

- Efficiency
- Probabilities of failure:

Kyber: $2^{-160}$
Saber: $2^{-136}$

HQC: $2^{-138}$
LEDAcrypt: $2^{-64}$

Ramstake: $2^{-64}$

*Disclaimer:*

- Ramstake

  (Secure?) Round 1 candidate for NIST post-quantum project

# Mersenne Number Cryptosystem

- Mersenne number $p = 2^n - 1$
- Secrets $a, b \in \mathbb{Z}_p$ with *low* Hamming weight
- Integer $G \in \mathbb{Z}_p$ with Hamming weight $\approx \frac{n}{2}$

# Mersenne Number Cryptosystem

- Mersenne number $p = 2^n - 1$
- Secrets $a, b \in \mathbb{Z}_p$ with *low* Hamming weight
- Integer $G \in \mathbb{Z}_p$ with Hamming weight $\approx \frac{n}{2}$

**Mersenne Low Hamming Combination Problem**

For random $n$-bit string $R$, distinguishing the tuples

$$(G, aG + b \mod p) \text{ or } (G, R)$$

is difficult.

# Mersenne Number Cryptosystem

| **Alice** | Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ | **Bob** |
| --- | --- | --- |
| $a, b \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$ | | $c, d \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$ |
| $P_A \equiv aG + b \mod p$ | | $P_B \equiv cG + d \mod p$ |

Secret

Public

# Mersenne Number Cryptosystem

| **Alice** | Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ | **Bob** |
|---|---|---|
| $a, b \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$ | | $c, d \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$ |
| $P_A \equiv aG + b \mod p$ | $\xrightarrow{P_A}$ | $P_B \equiv cG + d \mod p$ |

$$ctxt = m \oplus (cP_A \mod p)_{[0:|m|]}$$
$$= m \oplus (acG + bc \mod p)_{[0:|m|]}$$

Secret

Public

# Mersenne Number Cryptosystem

**Alice** — Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ — **Bob**

Secret

Public

$a, b \xleftarrow{\$} \mathrm{SMALL}_{\mathrm{HW}}(\mathbb{Z}_p)$ — $c, d \xleftarrow{\$} \mathrm{SMALL}_{\mathrm{HW}}(\mathbb{Z}_p)$

$P_A \equiv aG + b \mod p$ — $P_B \equiv cG + d \mod p$

$\xrightarrow{P_A}$

$$ctxt = m \oplus (cP_A \mod p)_{[0:|m|]}$$
$$= m \oplus (acG + bc \mod p)_{[0:|m|]}$$

$\xleftarrow{(ctxt, P_B)}$

$$m' = ctxt \oplus (aP_B \mod p)_{[0:|m|]}$$
$$= ctxt \oplus (acG + ad \mod p)_{[0:|m|]}$$

# Mersenne Number Cryptosystem

| Alice | Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ | Bob |
|---|---|---|
| $a, b \xleftarrow{\$} \text{SMALL}_{\text{HW}}(\mathbb{Z}_p)$ | | $c, d \xleftarrow{\$} \text{SMALL}_{\text{HW}}(\mathbb{Z}_p)$ |
| $P_A \equiv aG + b \mod p$ | $\xrightarrow{P_A}$ | $P_B \equiv cG + d \mod p$ |
| | | $ctxt = m \oplus (cP_A \mod p)_{[0:\lvert m \rvert]}$ <br> $= m \oplus (acG + bc \mod p)_{[0:\lvert m \rvert]}$ |
| $m' = ctxt \oplus (aP_B \mod p)_{[0:\lvert m \rvert]}$ <br> $= ctxt \oplus (acG + ad \mod p)_{[0:\lvert m \rvert]}$ | $\xleftarrow{(ctxt, P_B)}$ | |

Secret

Public

- $(acG + ad)_{[0:|m|]} \approx (acG + bc)_{[0:|m|]}$

# Mersenne Number Cryptosystem

**Alice** — Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ — **Bob**

| Secret |
| --- |
| Public |

Alice: $a, b \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$

Bob: $c, d \xleftarrow{\$} \mathsf{SMALL}_{\mathsf{HW}}(\mathbb{Z}_p)$

Alice: $P_A \equiv aG + b \mod p$

Bob: $P_B \equiv cG + d \mod p$

$\xrightarrow{P_A}$

Bob:

$$ctxt = m \oplus (cP_A \mod p)_{[0:|m|]}$$
$$= m \oplus (acG + bc \mod p)_{[0:|m|]}$$

$\xleftarrow{(ctxt, P_B)}$

Alice:

$$m' = ctxt \oplus (aP_B \mod p)_{[0:|m|]}$$
$$= ctxt \oplus (acG + ad \mod p)_{[0:|m|]}$$

- $(acG + ad)_{[0:|m|]} \approx (acG + bc)_{[0:|m|]}$
- $Pr[m \neq m']$ too high $\Longrightarrow$ introduce ECC

# Mersenne Number Cryptosystem

**Alice** — Fix Mersenne number $p$, $G \xleftarrow{\$} \mathbb{Z}_p$ — **Bob**

Secret

Public

Alice: $a, b \xleftarrow{\$} \mathrm{SMALL_{HW}}(\mathbb{Z}_p)$

Bob: $c, d \xleftarrow{\$} \mathrm{SMALL_{HW}}(\mathbb{Z}_p)$

Alice: $P_A \equiv aG + b \mod p$

Bob: $P_B \equiv cG + d \mod p$

Alice → Bob: $P_A$

Bob:

$$c_m = encode(m)$$
$$ctxt = c_m \oplus (cP_A \mod p)_{[0:|c_m|]}$$
$$= c_m \oplus (acG + bc \mod p)_{[0:|c_m|]}$$

Bob → Alice: $(ctxt, P_B)$

Alice:

$$c'_m = ctxt \oplus (aP_B \mod p)_{[0:|c_m|]}$$
$$= ctxt \oplus (acG + ad \mod p)_{[0:|c_m|]}$$
$$m' = decode(c'_m)$$

- $(acG + ad)_{[0:|c_m|]} \approx (acG + bc)_{[0:|c_m|]}$
- $Pr[m \neq m']$ too high $\implies$ introduce ECC
- $encode(\cdot)$, $decode(\cdot)$, correct up to $t$ errors

# Example Parameters

| Ramstake-756839 | |
|---|---|
| Mersenne exponent | $n = 756839$ |
| Hamming weight | 128 |
| #Corrected Errors | $t = 111$ |
| $Pr[m' \neq m]$ | $2^{-64}$ |
| quantum security | 128 |
| $\|pk\|$ | $93kB$ |
| $\|ctxt\|$ | $94kB$ |

- $p = 2^n - 1$
- $P_A = aG + b \mod p$

  $a, b \in \mathbb{Z}_p$ have *low* Hamming weight

# Example Parameters

| Ramstake-756839 | |
|---|---|
| Mersenne exponent | $n = 756839$ |
| Hamming weight | 128 |
| #Corrected Errors | $t = 111$ |
| $Pr[m' \neq m]$ | $2^{-64}$ |
| quantum security | 128 |
| $\|pk\|$ | $93kB$ |
| $\|ctxt\|$ | $94kB$ |

- $p = 2^n - 1$
- $P_A = aG + b \mod p$

  $a, b \in \mathbb{Z}_p$ have *low* Hamming weight

Our Attack: $\approx 2^{46}$ quantum steps + $2^{72}$ decryption queries

# Attacking Ramstake: Slice-and-Dice

Introduced by Beunardeau et al. [Beu+19]

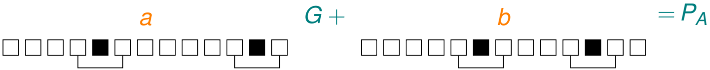
$a$ $G +$ $b$ $= P_A$

# Attacking Ramstake: Slice-and-Dice

Introduced by Beunardeau et al. [Beu+19]

- Guess approximate positions of 1's in the secrets $a, b$

  (128 of 756839 positions)

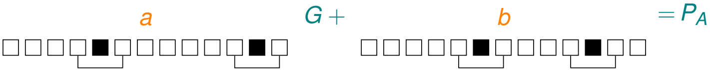


# Attacking Ramstake: Slice-and-Dice

Introduced by Beunardeau et al. [Beu+19]

- Guess approximate positions of 1's in the secrets $a, b$

  (128 of 756839 positions)
- Apply *some* lattice reduction technique

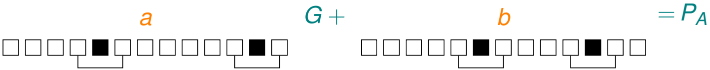


# Attacking Ramstake: Slice-and-Dice

Introduced by Beunardeau et al. [Beu+19]

- Guess approximate positions of 1's in the secrets $a, b$

  (128 of 756839 positions)
- Apply *some* lattice reduction technique



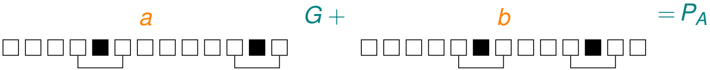

Guessing positions is **very** difficult

# Attacking Ramstake: Slice-and-Dice

Introduced by Beunardeau et al. [Beu+19]

- Guess approximate positions of 1's in the secrets $a, b$

  (128 of 756839 positions)
- Apply *some* lattice reduction technique




Guessing positions is **very** difficult

Decryption failures to make a good guess!

# Ramstake: Decryption Failures

**Alice**

$$c'_m = ctxt \oplus (aP_B \mod p)_{[0:|c_m|]}$$
$$= ctxt \oplus (acG + ad \mod p)_{[0:|c_m|]}$$
$$m' = decode(c'_m)$$

$\leftarrow (ctxt, P_B)$

**Bob**

$$c_m = encode(m)$$
$$ctxt = c_m \oplus (cP_A \mod p)_{[0:|c_m|]}$$
$$= c_m \oplus (acG + bc \mod p)_{[0:|c_m|]}$$

# Ramstake: Decryption Failures

**Alice**

$$c'_m = ctxt \oplus (aP_B \mod p)_{[0:|c_m|]}$$
$$= ctxt \oplus (acG + ad \mod p)_{[0:|c_m|]}$$
$$m' = decode(c'_m)$$

$\xleftarrow{(ctxt, P_B)}$

**Bob**

$$c_m = encode(m)$$
$$ctxt = c_m \oplus (cP_A \mod p)_{[0:|c_m|]}$$
$$= c_m \oplus (acG + bc \mod p)_{[0:|c_m|]}$$

## Decryption Failure

$$decode(c'_m) \text{ fails}$$
$$\Leftrightarrow \mathrm{HW}_{[0:|c_m|]}((acG + ad \mod p) \oplus (acG + bc \mod p)) > t$$
$$\approx \left(\mathrm{HW}_{[0:|c_m|]}(ad) + \mathrm{HW}_{[0:|c_m|]}(bc)\right) > t$$

# Ramstake Information Leak

- Consider only error *ad*
- Assume decryption returns *fail*

$\Rightarrow$ $\mathrm{HW}_{[0:|c_m|]}(ad)$ large

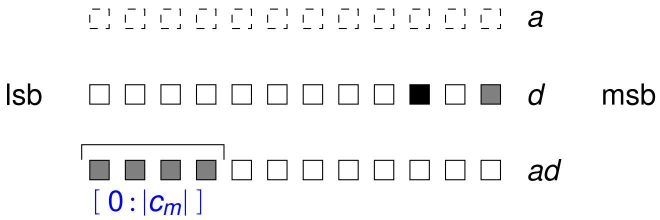
$\Rightarrow$ only possible for *some* values of $a$

# Ramstake Information Leak

- Consider only error *ad*
- Assume decryption returns *fail*

$\Rightarrow$ $\mathrm{HW}_{[0:|c_m|]}(ad)$ large

$\Rightarrow$ only possible for *some* values of *a*

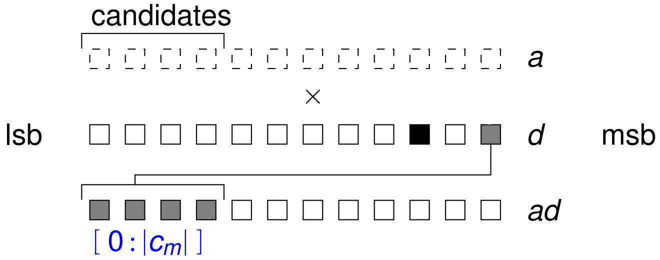


# Ramstake Information Leak

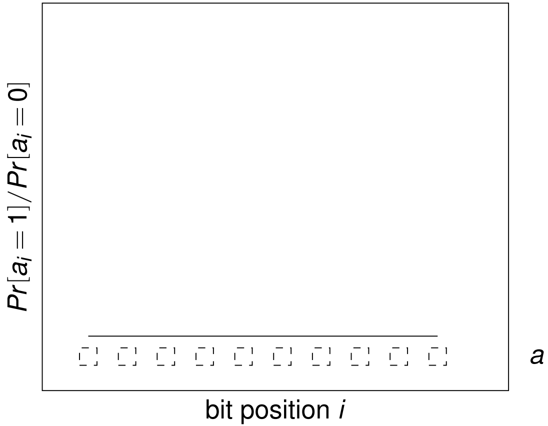
- Consider only error *ad*
- Assume decryption returns *fail*

$\Rightarrow$ $\mathrm{HW}_{[0:|c_m|]}(ad)$ large

$\Rightarrow$ only possible for *some* values of *a*



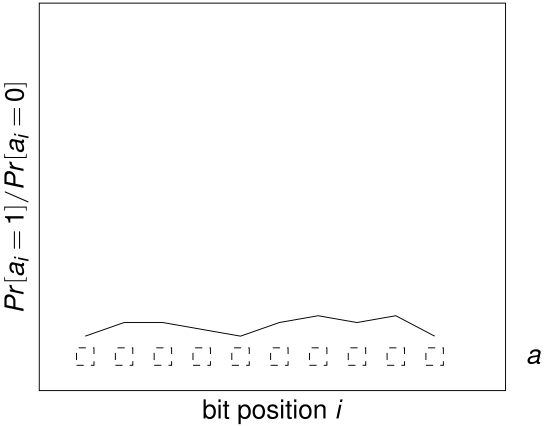
# Decryption Failure Attack




**Strategy**

- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

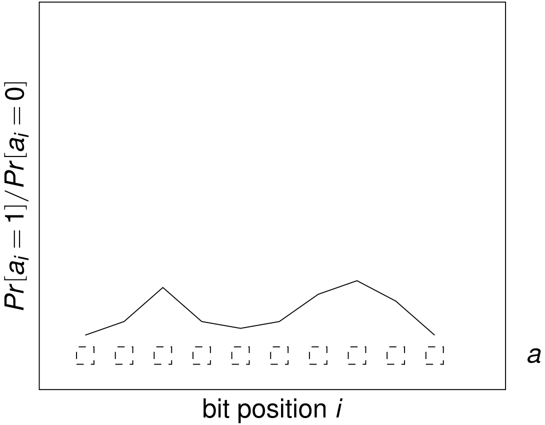
# Decryption Failure Attack




Strategy

- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

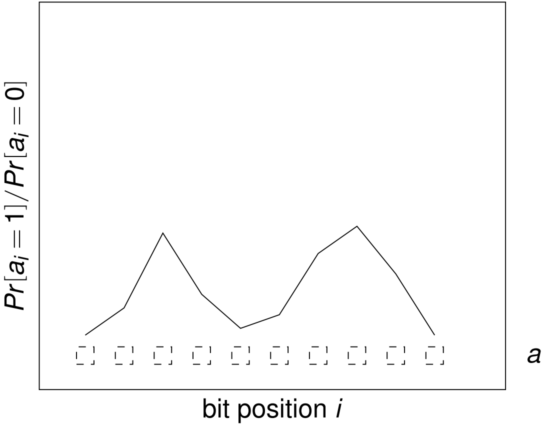
# Decryption Failure Attack




**Strategy**

- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

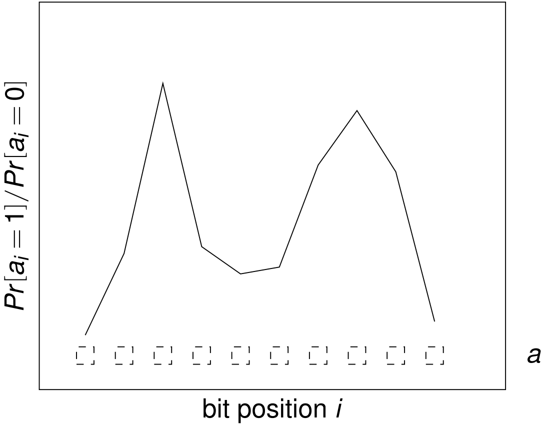
# Decryption Failure Attack




Strategy

- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

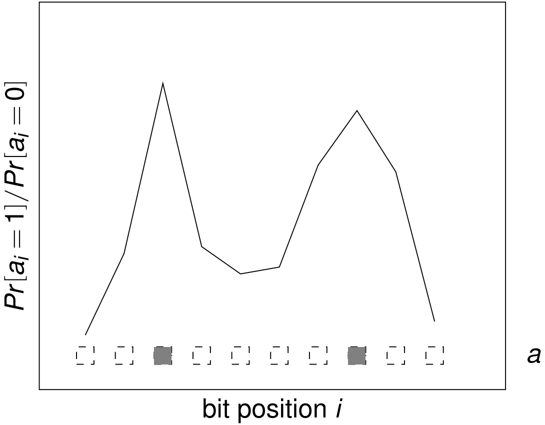
# Decryption Failure Attack




Strategy

- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

# Decryption Failure Attack

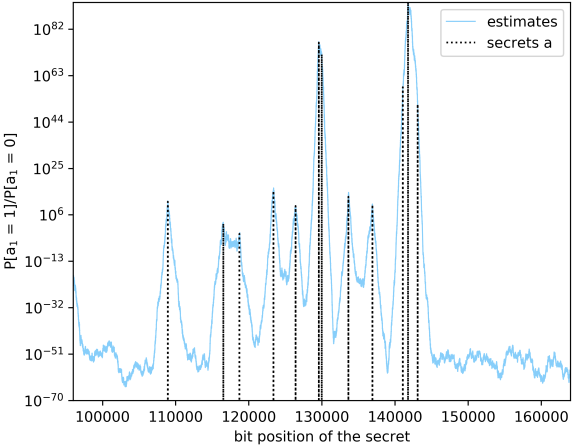



Strategy

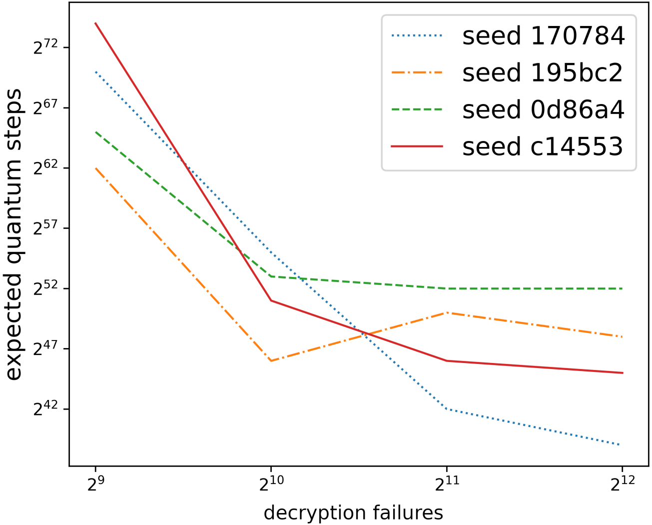
- Query decryption oracle with $(ctxt, P_B)$
- Estimate candidate bits of $a$
- Repeat *sufficiently often*.

# “Nothing-up-our-sleeves” Result

https://github.com/Fleeep/ramstake-failure-attack



# “Nothing-up-our-sleeves” Result

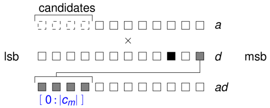



Ramstake-756839
(Security level: 128)

| #decryption failures | approx. # quantum steps |
|---|---|
| $2^9$ | $2^{68}$ |
| $2^{10}$ | $2^{52}$ |
| $2^{11}$ | $2^{48}$ |
| $2^{12}$ | $2^{46}$ |

# Conclusion

Mersenne number cryptosystems
leak information



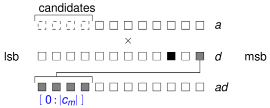
# Conclusion

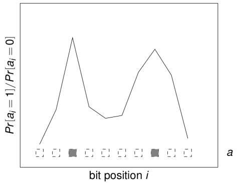
Mersenne number cryptosystems
leak information

↓

Information to estimate secrets.

*For Ramstake-756839:* $2^{12}$ *decryption failures*



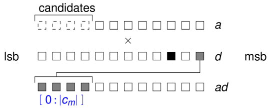
# Conclusion

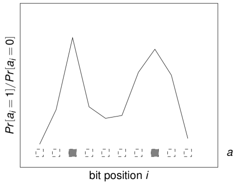
Mersenne number cryptosystems leak information

Information to estimate secrets.

*For Ramstake-756839:* $2^{12}$ *decryption failures*

Probability of failure should to be **very low.**



Thanks.

*Happy to answer any questions!*

**Exploiting Decryption Failures in Mersenne Number Cryptosystems**

**Marcel Tiepelt**[1] and Jan-Pieter D'Anvers[2]

[1]Kastel, KIT, marcel.tiepelt@kit.edu
[2]imec-COSIC, KU Leuven, janpieter.danvers@esat.kuleuven.be