# Cryptanalysis of Low-Data Instances of Full LowMCv2

Christian Rechberger[1] Hadi Soleimany [2] Tyge Tiessen[3]

[1]Graz University of Technology, Austria

[2]Shahid Beheshti University, Iran

[3]Technical University of Denmark, Denmark

FSE 2019, Paris, France

# Outline


Introduction
- LowMC Description
- Related Work

New Technique
- Overview of the Technique
- Proposed Framework

Key Recovery
- Simplified Representation of LowMC
- Impact on Applications of LowMC

Conclusion

Introduction
LowMC Description
Related Work

New Technique
Overview of the Technique
Proposed Framework

Key Recovery
Simplified Representation of LowMC
Impact on Applications of LowMC

Conclusion

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)
  - Fully homomorphic encryption (FHE)

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)
  - Fully homomorphic encryption (FHE)
  - Zero-knowledge proof systems like SNARKs or STARKs

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)
  - Fully homomorphic encryption (FHE)
  - Zero-knowledge proof systems like SNARKs or STARKs
  - Quantum-resilient public-key signature

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)
  - Fully homomorphic encryption (FHE)
  - Zero-knowledge proof systems like SNARKs or STARKs
  - Quantum-resilient public-key signature
- A main goal in the design of suitable ciphers/permutations/hash functions is to minimize the number of multiplications.

# New Designs for New Applications

- Some design choices that were sensible for classical applications are suboptimal for a range of new applications.
- Implementation properties are comlex, but linear operations come often almost for free whereas the bottleneck are nonlinear operations.
  - Multi-party computation (MPC)
  - Fully homomorphic encryption (FHE)
  - Zero-knowledge proof systems like SNARKs or STARKs
  - Quantum-resilient public-key signature
- A main goal in the design of suitable ciphers/permutations/hash functions is to minimize the number of multiplications.
- Examples of such designs include LowMC, Kreyvium, Flip, MiMC and Rasta.

# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].

# LowMC Description

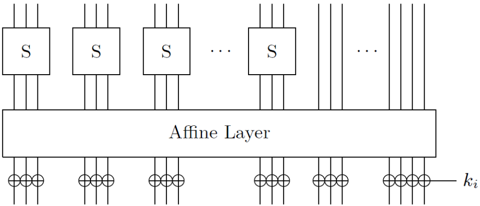
- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.

# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.
- Round function:

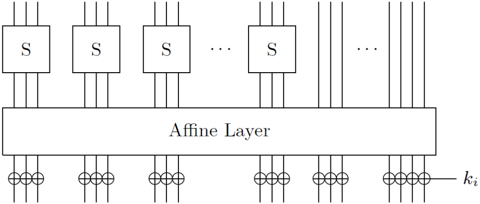
# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.
- Round function:
  - Using partial non-linear layers



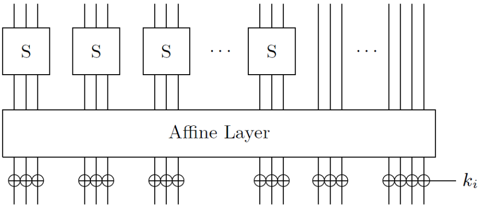
# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.
- Round function:
  - Using partial non-linear layers
  - Using $3 \times 3$ Sbox with algebraic degree 2.



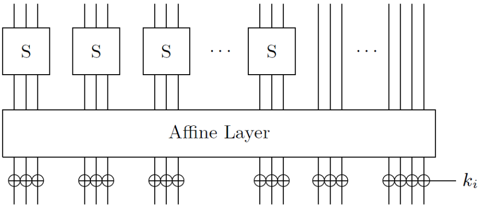
# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.
- Round function:
  - Using partial non-linear layers
  - Using $3 \times 3$ Sbox with algebraic degree 2.
  - Linear layers are binary invertible matrices that are chosen independently and uniformly at random.



# LowMC Description

- First design proposed at Eurocrypt 2015 [Albrecht et al. 15].
- Allows to create suitable instances for a wide range of applications, e.g. used for a signature scheme currently under consideration in round 2 of the NIST PQ process.
- Round function:
  - Using partial non-linear layers
  - Using $3 \times 3$ Sbox with algebraic degree 2.
  - Linear layers are binary invertible matrices that are chosen independently and uniformly at random.
  - Round key is generated by a randomly chosen multiplication of a full-rank $b \times k$ with the master key.



# LowMC Cryptanalysis and Impact

- 2012-2015: Authors provide analysis with a large variety of techniques. Given block size ($b$), allowable data complexity $D$, and number of Sboxes per round ($m$), a 'v0 round formular' ($r$) is provided to allows to create instances for any desired security level.

# LowMC Cryptanalysis and Impact

- 2012-2015: Authors provide analysis with a large variety of techniques. Given block size ($b$), allowable data complexity $D$, and number of Sboxes per round ($m$), a 'v0 round formular' ($r$) is provided to allows to create instances for any desired security level.
- Observations by Khovratovich, Leurent led to v1 (Eurocrypt 2015)

# LowMC Cryptanalysis and Impact

- 2012-2015: Authors provide analysis with a large variety of techniques. Given block size ($b$), allowable data complexity $D$, and number of Sboxes per round ($m$), a 'v0 round formular' ($r$) is provided to allows to create instances for any desired security level.
- Observations by Khovratovich, Leurent led to v1 (Eurocrypt 2015)
- Attacks by Dobraunig, Eichlseder and Mendel, and Dinur, Liu, Meier and Wang led to v2 (eprint 2016).

# LowMC Cryptanalysis and Impact

- 2012-2015: Authors provide analysis with a large variety of techniques. Given block size ($b$), allowable data complexity $D$, and number of Sboxes per round ($m$), a 'v0 round formular' ($r$) is provided to allows to create instances for any desired security level.
- Observations by Khovratovich, Leurent led to v1 (Eurocrypt 2015)
- Attacks by Dobraunig, Eichlseder and Mendel, and Dinur, Liu, Meier and Wang led to v2 (eprint 2016).
- Our new cryptanalysis led to v3 (github 2017).

# LowMC Cryptanalysis and Impact

- 2012-2015: Authors provide analysis with a large variety of techniques. Given block size ($b$), allowable data complexity $D$, and number of Sboxes per round ($m$), a 'v0 round formular' ($r$) is provided to allows to create instances for any desired security level.
- Observations by Khovratovich, Leurent led to v1 (Eurocrypt 2015)
- Attacks by Dobraunig, Eichlseder and Mendel, and Dinur, Liu, Meier and Wang led to v2 (eprint 2016).
- Our new cryptanalysis led to v3 (github 2017).

LowMCv3 is used in all applications we are aware of, e.g Picnic signature scheme (Zaverucha et al., CCS 2017), group signature schemes (Boneh et al., Derler et al.), or a protype Signal 'plugin' for private contact discovery.

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes, since it is a well-known cryptanalysis.

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes, since it is a well-known cryptanalysis.
- Truncated differential MITM cryptanalysis take advantage of positive properties in both methods. [Demirci et al. 09]

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes, since it is a well-known cryptanalysis.
- Truncated differential MITM cryptanalysis take advantage of positive properties in both methods. [Demirci et al. 09]
  - But it strongly depends on the properties of the linear layer.

# Overview of Previous Techniques

- Meet-in-the-middle cryptanalysis requires extremely limited data and it is almost independent of inner components.
  - But it is applicable to the ciphers with weak key schedule.
- Differential cryptanalysis is usually applicable on any round functions [Biham Shamir 90].
  - But there exists a lower bound for active S-boxes, since it is a well-known cryptanalysis.
- Truncated differential MITM cryptanalysis take advantage of positive properties in both methods. [Demirci et al. 09]
  - But it strongly depends on the properties of the linear layer.

## This Work

Exploit previous ideas to take advantage of the positive properties and overcome the limitations!

Introduction
LowMC Description
Related Work

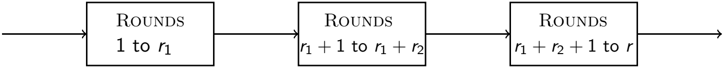
New Technique
Overview of the Technique
Proposed Framework

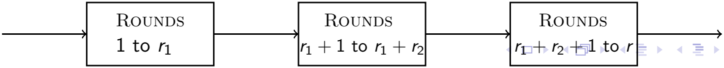
Key Recovery
Simplified Representation of LowMC
Impact on Applications of LowMC

Conclusion

# Overview of the Technique

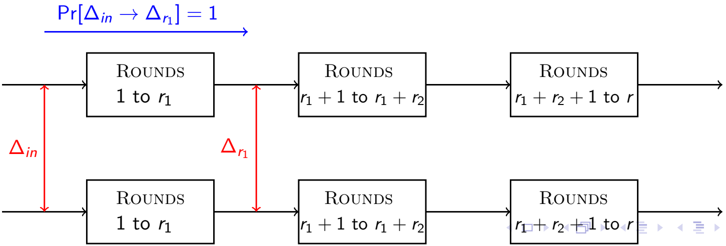
- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.



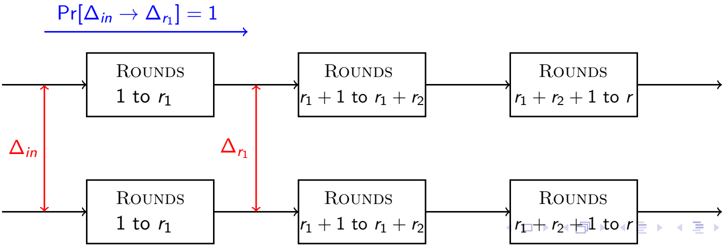
# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.



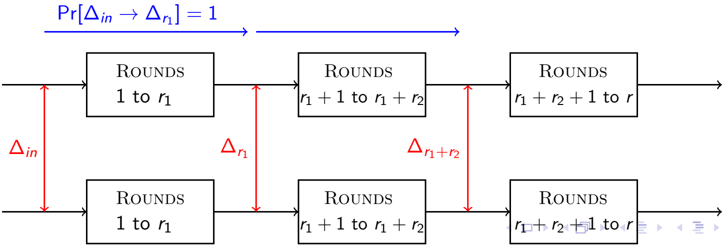
# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.
- Ask oracle to provide the corresponding ciphertexts of $P, P' = P \oplus \Delta_{in}$.



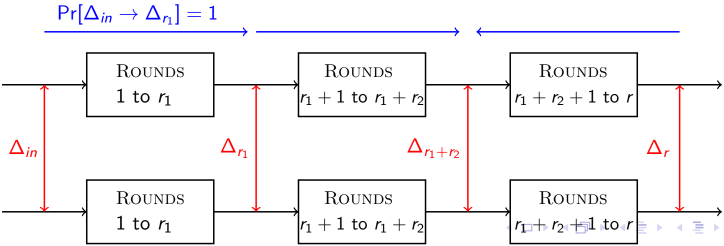
# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.
- Ask oracle to provide the corresponding ciphertexts of $P, P' = P \oplus \Delta_{in}$.
- Create a list of all reachable output differences after $r_2$ rounds.



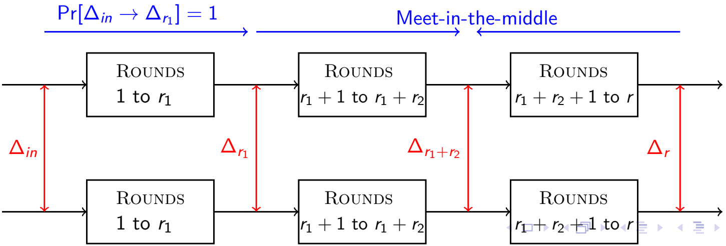
# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.
- Ask oracle to provide the corresponding ciphertexts of $P, P' = P \oplus \Delta_{in}$.
- Create a list of all reachable output differences after $r_2$ rounds.
- Create a list of all reachable differences over the last $r_3$ rounds.



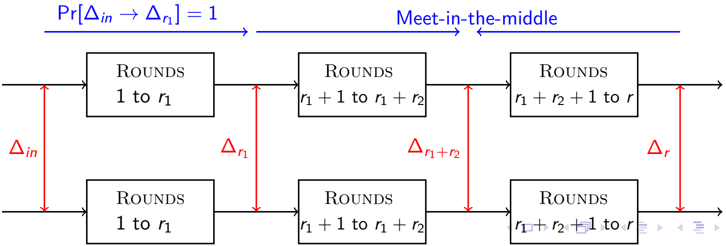
# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.
- Ask oracle to provide the corresponding ciphertexts of $P, P' = P \oplus \Delta_{in}$.
- Create a list of all reachable output differences after $r_2$ rounds.
- Create a list of all reachable differences over the last $r_3$ rounds.
- If these lists are significantly smaller than the set of all possible output differences, we can obtain the difference in the middle.



# Overview of the Technique

- Divide the cipher into three consecutive parts $r_1, r_2$ and $r_3$.
- Select an input difference $\Delta_{in}$ so that the output difference after $r_1$ rounds can be determined with a probability of one.
- Ask oracle to provide the corresponding ciphertexts of $P, P' = P \oplus \Delta_{in}$.
- Create a list of all reachable output differences after $r_2$ rounds.
- Create a list of all reachable differences over the last $r_3$ rounds.
- If these lists are significantly smaller than the set of all possible output differences, we can obtain the difference in the middle.
- Repeat the procedure to find all intermediate differences.



# First Part

- To have deterministic differential characteristic, all Sboxes should be passive.

# First Part

- To have deterministic differential characteristic, all Sboxes should be passive.

### Deterministic Differential Characteristic

On average for LowMC, there exist $2^{b-3.m.R}$ deterministic differential characteristics over $R$ rounds, i.e. $|\{\Delta_{in} \in \mathbb{F}_2^b | \Pr[\Delta_{in} \to \mathcal{L}_R \circ \cdots \circ \mathcal{L}_1(\Delta_{in})] = 1\}| = 2^{b-3.m.R}$.

# First Part

- To have deterministic differential characteristic, all Sboxes should be passive.

### Deterministic Differential Characteristic

On average for LowMC, there exist $2^{b-3.m.R}$ deterministic differential characteristics over $R$ rounds, i.e.
$|\{\Delta_{in} \in \mathbb{F}_2^b | \Pr[\Delta_{in} \to \mathcal{L}_R \circ \cdots \circ \mathcal{L}_1(\Delta_{in})] = 1\}| = 2^{b-3.m.R}$.

- We can cover $r_1 = \left\lceil \frac{b}{3 \cdot m} \right\rceil - 1$ rounds.

# Estimating the Number of Reachable Differences

## Possible of differences for one Sbox

For a bijective 3-bit Sbox each non-zero difference $\Delta_{in} \in \mathbb{F}_2^3$ can transfer to at most $2^2$ different differences.

# Estimating the Number of Reachable Differences

## Possible of differences for one Sbox

For a bijective 3-bit Sbox each non-zero difference $\Delta_{in} \in \mathbb{F}_2^3$ can transfer to at most $2^2$ different differences.

## Number of Differences

The number of possible differences in the output of the $R$-th round of LowMC is almost $2^{2.(m.R)}$, i.e.
$|\{\Delta' | Pr[\Delta \rightarrow \Delta'] > 0\}| = 2^{2.(m.R)}$.

# Estimating the Number of Reachable Differences

## Possible of differences for one Sbox

For a bijective 3-bit Sbox each non-zero difference $\Delta_{in} \in \mathbb{F}_2^3$ can transfer to at most $2^2$ different differences.

## Number of Differences

The number of possible differences in the output of the $R$-th round of LowMC is almost $2^{2.(m.R)}$, i.e.
$|\{\Delta' | Pr[\Delta \to \Delta'] > 0\}| = 2^{2.(m.R)}$.

## Time complexity

$$2^{2 \cdot m \cdot r_2} + 2^{2 \cdot m \cdot r_3} < 2^k$$

# Estimating the Number of Reachable Differences

## Possible of differences for one Sbox

For a bijective 3-bit Sbox each non-zero difference $\Delta_{in} \in \mathbb{F}_2^3$ can transfer to at most $2^2$ different differences.

## Number of Differences

The number of possible differences in the output of the $R$-th round of LowMC is almost $2^{2.(m.R)}$, i.e.
$|\{\Delta' | Pr[\Delta \to \Delta'] > 0\}| = 2^{2.(m.R)}$.

## Time complexity

$$2^{2 \cdot m \cdot r_2} + 2^{2 \cdot m \cdot r_3} < 2^k$$

## To Avoid Wrong Collision

$$2^{2 \cdot m \cdot (r_2 + r_3)} < 2^b \to r_2 + r_3 < \frac{b}{2 \cdot m}$$

# Estimating the Number of Reachable Differences

## Possible of differences for one Sbox

For a bijective 3-bit Sbox each non-zero difference $\Delta_{in} \in \mathbb{F}_2^3$ can transfer to at most $2^2$ different differences.

## Number of Differences

The number of possible differences in the output of the $R$-th round of LowMC is almost $2^{2.(m.R)}$, i.e.
$|\{\Delta' | Pr[\Delta \to \Delta'] > 0\}| = 2^{2.(m.R)}$.

## Time complexity

$$2^{2 \cdot m \cdot r_2} + 2^{2 \cdot m \cdot r_3} < 2^k$$

## To Avoid Wrong Collision

$$2^{2 \cdot m \cdot (r_2 + r_3)} < 2^b \to r_2 + r_3 < \frac{b}{2 \cdot m}$$

- How can we overcome this limitation?

# From Differential to Polytopic

### *d*-differences

A $d$-difference is the ordered tuple of the respective differences, i.e., $(x_1 \oplus x_0, \ldots, x_d \oplus x_0)$. [Tiessen 14]

# From Differential to Polytopic

### $d$-differences

A $d$-difference is the ordered tuple of the respective differences, i.e., $(x_1 \oplus x_0, \ldots, x_d \oplus x_0)$. [Tiessen 14]

### Possible of $d$ differences for one Sbox

The number of reachable $d$-differences over the 3-bit S-box for a non-zero input $d$-difference is *at most* $2^3$.

# From Differential to Polytopic

### $d$-differences

A $d$-difference is the ordered tuple of the respective differences, i.e., $(x_1 \oplus x_0, \ldots, x_d \oplus x_0)$. [Tiessen 14]

### Possible of $d$ differences for one Sbox

The number of reachable $d$-differences over the 3-bit S-box for a non-zero input $d$-difference is *at most* $2^3$.

### Estimating the Number of Reachable Differences

Simple upper bound on the number of reachable $d$-differences after $r$ rounds is $2^{3 \cdot m \cdot r}$.

# From Differential to Polytopic

### $d$-differences

A $d$-difference is the ordered tuple of the respective differences, i.e., $(x_1 \oplus x_0, \ldots, x_d \oplus x_0)$. [Tiessen 14]

### Possible of $d$ differences for one Sbox

The number of reachable $d$-differences over the 3-bit S-box for a non-zero input $d$-difference is *at most* $2^3$.

### Estimating the Number of Reachable Differences

Simple upper bound on the number of reachable $d$-differences after $r$ rounds is $2^{3 \cdot m \cdot r}$.

### Condition to Avoid Wrong Collision

$$2^{3 \cdot m \cdot (r_2 + r_3)} < 2^{b \cdot d} \quad \rightarrow \quad d > \frac{3 \cdot m \cdot (r_2 + r_3)}{b}$$

Introduction
LowMC Description
Related Work

New Technique
Overview of the Technique
Proposed Framework

Key Recovery
Simplified Representation of LowMC
Impact on Applications of LowMC

Conclusion

# Key Recovery

### Definition

An Sbox $S : \{0,1\}^n \to \{0,1\}^n$ is called to be differentially $\delta$-uniform if for any $(\alpha, \beta) \in (\mathbb{F}_2^n \times \mathbb{F}_2^n)$, we have:

$$|\{x \in \{0,1\}^n : \beta = S(x) \oplus S(x \oplus \alpha)| \leq \delta$$

# Key Recovery

## Definition

An Sbox $S : \{0,1\}^n \rightarrow \{0,1\}^n$ is called to be differentially $\delta$-uniform if for any $(\alpha, \beta) \in (\mathbb{F}_2^n \times \mathbb{F}_2^n)$, we have:

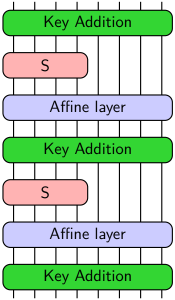
$$|\{x \in \{0,1\}^n : \beta = S(x) \oplus S(x \oplus \alpha)| \leq \delta$$

## Key candidates

We expect to have at most $2^{m.x}$ solutions for the quadratic $(X_r^I, X_r'^I, X_r^S, , X_r'^S)$, since each Sbox is differentially $2^x$-uniform. Each solution uniquely suggests a candidate for the round key $sk_r$ as follows:

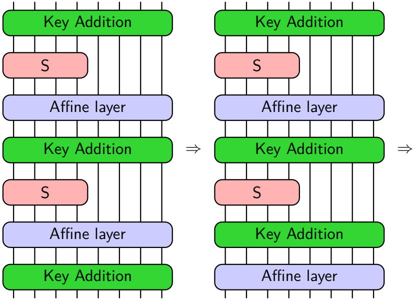
$$C \oplus sk_r = X_r^L = \mathcal{L}(X_r^S) \rightarrow sk_r = C \oplus \mathcal{L}(X_r^S)$$

# Equivalent representation with Equivalent Round Keys

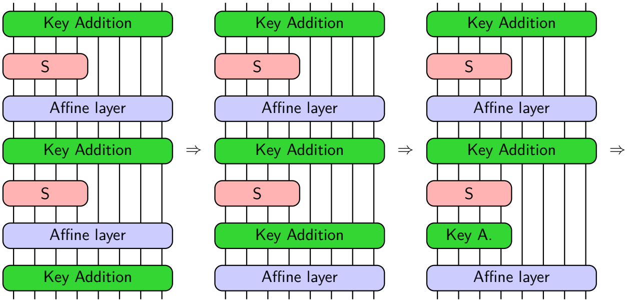



$\Rightarrow$

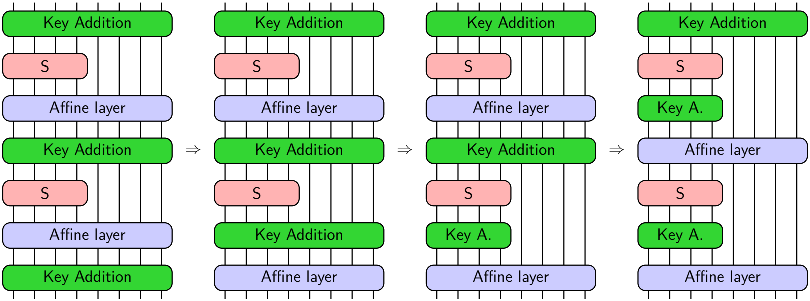
# Equivalent representation with Equivalent Round Keys



# Equivalent representation with Equivalent Round Keys



# Equivalent representation with Equivalent Round Keys



# Results

| Cipher Specification | | | | | Attack Details | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Block $n$ | S-boxes $m$ | Data $D$ | Key $k$ | Rounds $r$ | Dimension $d$ | $r_0$ $\lfloor\frac{n-\log_2 d}{3\cdot m}\rfloor$ | $r_1$ $\lfloor\frac{r-r_0}{2}\rfloor$ | $r_2$ $\lceil\frac{r-r_0}{2}\rceil$ | Time Complexity $2\cdot(\delta_d^{r_1}+\delta_d^{r_2})$ | Data $2(d+1)$ |
| 128 | 1 | 16 | 256 | 158 | 4 | 41 | 58 | 58 | $2^{164.9}$ | 10 |
| 128 | 5 | 16 | 256 | 37 | 4 | 8 | 14 | 15 | $2^{212.75}$ | 10 |
| 256 | 1 | 8 | 256 | 243 | 2 | 85 | 79 | 79 | $2^{223}$ | 6 |
| 256 | 5 | 8 | 256 | 53 | 2 | 17 | 18 | 18 | $2^{254.9}$ | 6 |
| 512 | 1 | 8 | 256 | 413 | 1 | 170 | 121 | 121 | $2^{226.6}$ | 4 |
| 1024 | 1 | 8 | 512 | 758 | 1 | 341 | 208 | 209 | $2^{389.9}$ | 4 |

- Several low-data instances of LowMCv2 can be broken significantly faster than exhaustive search.
- The type of instance that is vulnerable (few Sboxes per round) are used e.g. in post-quantum signature schemes.

Introduction
LowMC Description
Related Work

New Technique
Overview of the Technique
Proposed Framework

Key Recovery
Simplified Representation of LowMC
Impact on Applications of LowMC

Conclusion

# Conclusions

- New representation for the block ciphers with partial non-linear layer.

# Conclusions

- New representation for the block ciphers with partial non-linear layer.
- A new insight into the security evaluation of block ciphers with a partial non-linear layer by presenting a new cryptanalytic technique.

# Conclusions

- New representation for the block ciphers with partial non-linear layer.
- A new insight into the security evaluation of block ciphers with a partial non-linear layer by presenting a new cryptanalytic technique.
- Best results for some versions of LowMC. Led to a new round 'formula' v3.