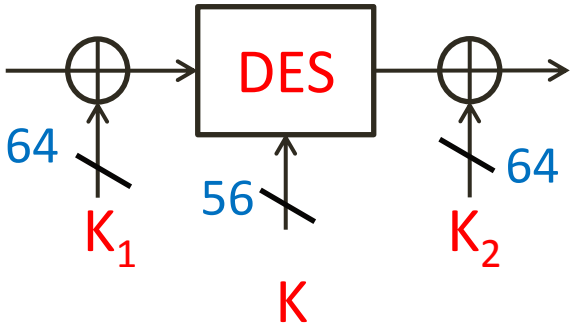
On the Security of the FX-Construction (feat. PRINCE and PRIDE)

Itai Dinur

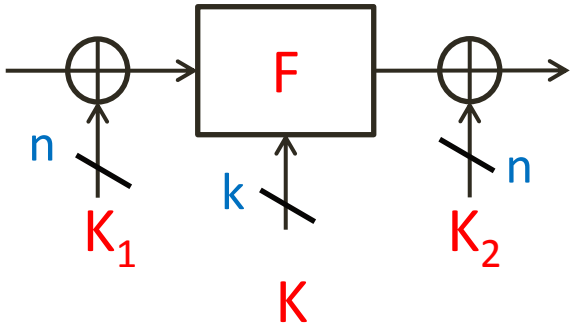
École normale supérieure, France

DESX



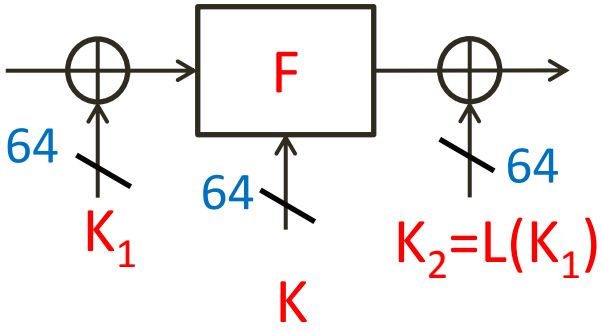
- **DESX** was proposed in 1984 by Ron Rivest
- A **simple** way to increase the security of **DES** by XORing 2 **masking keys**

FX-Construction[Kilian,Rogaway]



- Generalized to the **FX-construction** in 1996
- A generic and proven way to increase the security of a **core block cipher** F

Concrete FX-Constructions



- The FX-construction has been reused recently in 2 **new** designs: **PRINCE** (Asiacrypt'12)

  PRIDE (CRYPTO'14)
- Both ciphers use k=n=64
- Provide 128-d bits of security assuming that the adversary can get at most 2^d **data**

The PRINCE Challenge

- Focus on **practical analysis** of round-reduced variants of PRINCE
- “Practical”: $T=2^{64}$, $M=2^{45}$ B, $D=2^{30}$ KP

Our New Attacks

- We devise attacks which are not very far from practical according to "**The PRINCE Challenge**"
- "Practical": $T=2^{64}$, $M=2^{45}$, $D=2^{30}$ KP
- **Attack1**: $T=2^{64}$, $M=2^{51}$, $D=2^{32}$ ACP

Our New Attacks

- We devise attacks which are not very far from practical according to "**The PRINCE Challenge**"
- "Practical": $T=2^{64}$, $M=2^{45}$, $D=2^{30}$ KP
- **Attack1**: $T=2^{64}$, $M=2^{51}$, $D=2^{32}$ ACP
- The attacks are **generic**: can be applied to **any FX-construction** (including **PRIDE, DESX**) regardless of the number of rounds

Our New Attacks

- We devise attacks which are not very far from practical according to "**The PRINCE Challenge**"
- "Practical": $T=2^{64}$, $M=2^{45}$, $D=2^{30}$ KP
- **Attack1**: $T=2^{64}$, $M=2^{51}$, $D=2^{32}$ ACP
- The attacks are **generic**: can be applied to **any FX-construction** (including **PRIDE**) regardless of the number of rounds
- **Limitation**: Attack1 requires **preprocessing** of 2^{96}

Our New Attacks

- **Attack1**: $T=2^{64}$, $M=2^{51}$, $D=2^{32}$ ACP
- **Limitation**: requires **preprocessing** of 2^{96}

- **Attack2**: $T=2^{56}$, $M=2^{51}$, $D=2^{40}$ ACP
- **Preprocessing** is **reduced** to 2^{88}

Our New Attacks

- For success probability 1/256:

  Attack2: $T=2^{56}$, $M=2^{43}$, $D=2^{40}$ ACP
- Online attack can be implemented on **dedicated hardware** with **academic budget**!
- **Preprocessing** is **further reduced** to 2^{80}

Our New Attacks

- Do not “break” **PRINCE** or **PRIDE**
- Do not violate their **theoretical security claims**
- Show that the **security margin** of **PRINCE** or **PRIDE** against practical attacks is **smaller** than expected

Tweaking PRINCE and PRIDE

- **Lightly** tweak the key schedule of **PRINCE** and **PRIDE** so they resist our attacks
- The **FX security proof** is “lost”, but the **security margin** against practical attacks is **increased**

Conclusions

- **Lightly** tweak the key schedule of **PRINCE** and **PRIDE** so they resist our attacks
- The **FX security proof** is “lost”, but the **security margin** against practical attacks is **increased**

- The FX-construction is a simple way to increase the security of a **widely deployed cipher**
- Using the FX-construction for a **new cipher** seems **less reasonable**

Thank you for your attention!