Stream Ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression

Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, Renaud Sirdey

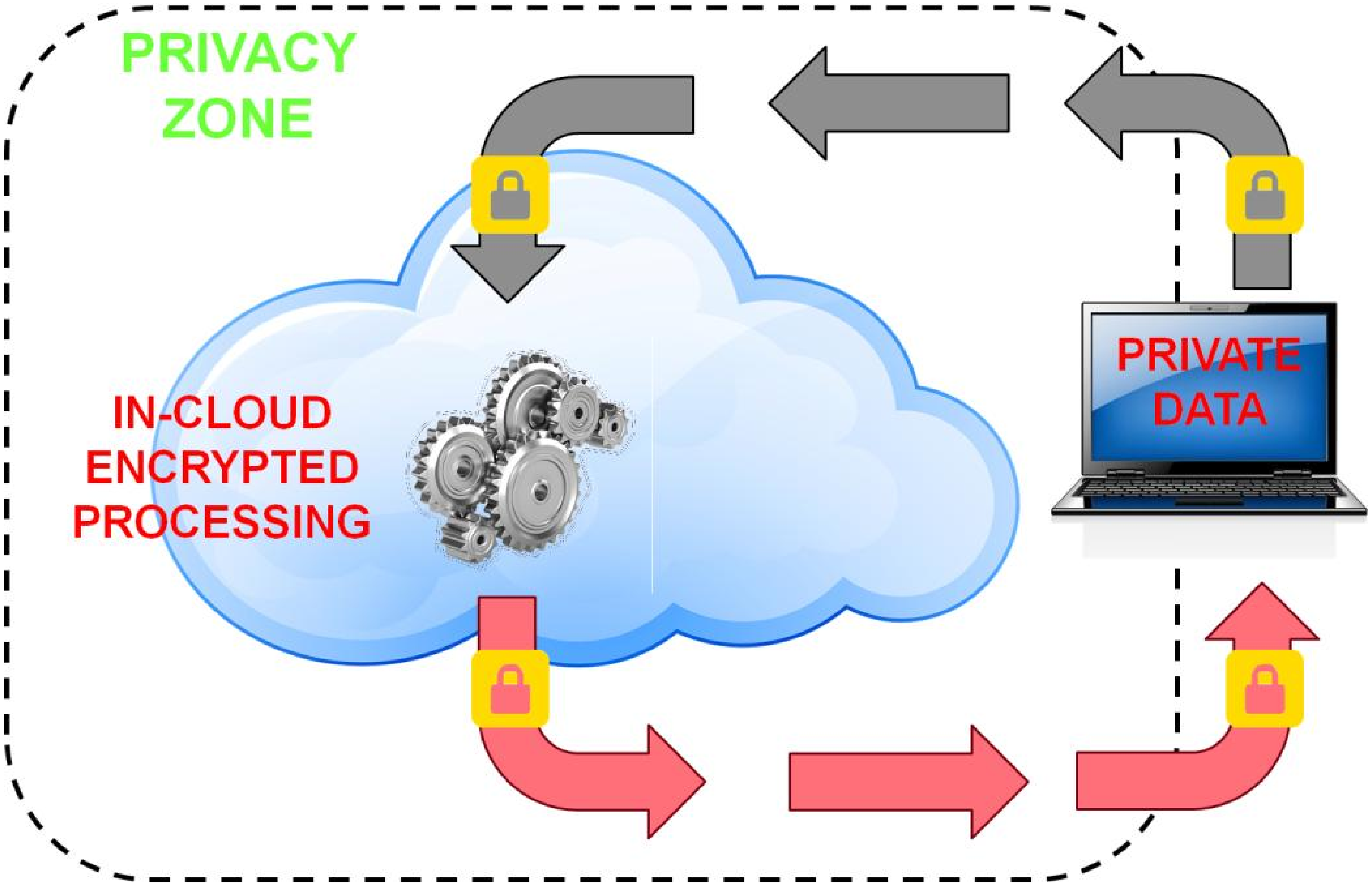
Stream ciphers: A Practical Solution for Efficient Homomorphic-Ciphertext Compression

Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, Renaud Sirdey

Inria Paris, CEA LIST, CNRS, Telecom Bretagne and UEB, CryptoExperts (France)

CryptoAction Symposium, Budapest, April 2016

Motivation

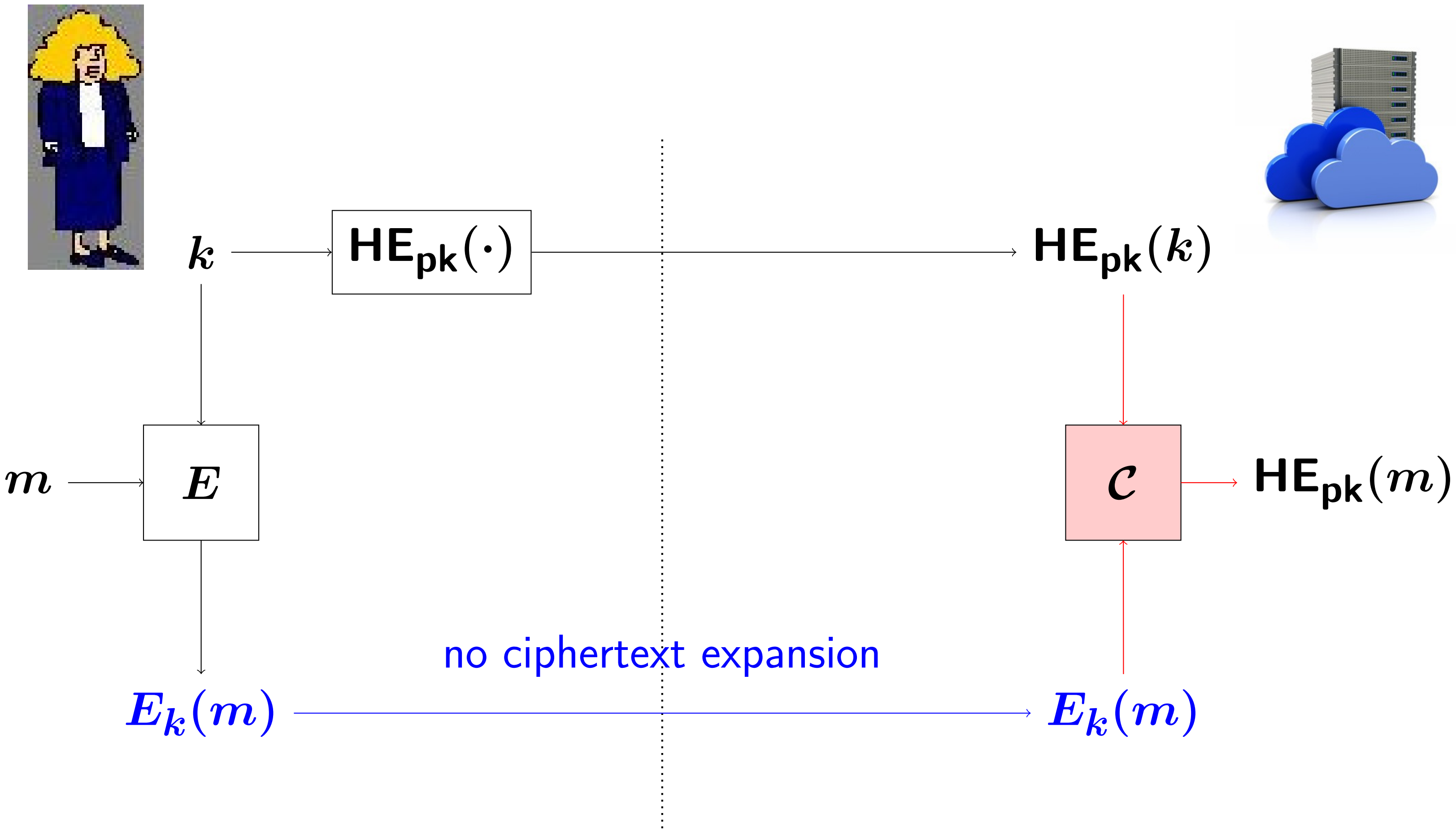


Homomorphic encryption

$$\mathsf{HE}_{\mathsf{pk}}(f(x)) = \mathsf{HE.Eval}_f(\mathsf{HE}_{\mathsf{pk}}(x))$$

Typical ciphertext expansion: 200 kBytes for encrypting a single bit

Optimizing communication using symmetric encryption [Naehrig et al. 11]



$$\mathcal{C} = \textbf{HE.Eval}_{E^{-1}}$$

Question: What kind of symmetric encryption is the most appropriate?

Prior HE-friendly ciphers

Aim:

Minimize the multiplicative depth of the decryption function.

Concrete proposals:

- Optimized implementations of AES [Gentry Halevi Smart 12][Cheon et al. 13] [Döroz Hu Sunar 14]
- Lightweight block ciphers: SIMON [Lepoint Naehrig 14], PRINCE [Doröz et al.14]
- Dedicated block cipher: Low-MC [Albrecht et al. 15]

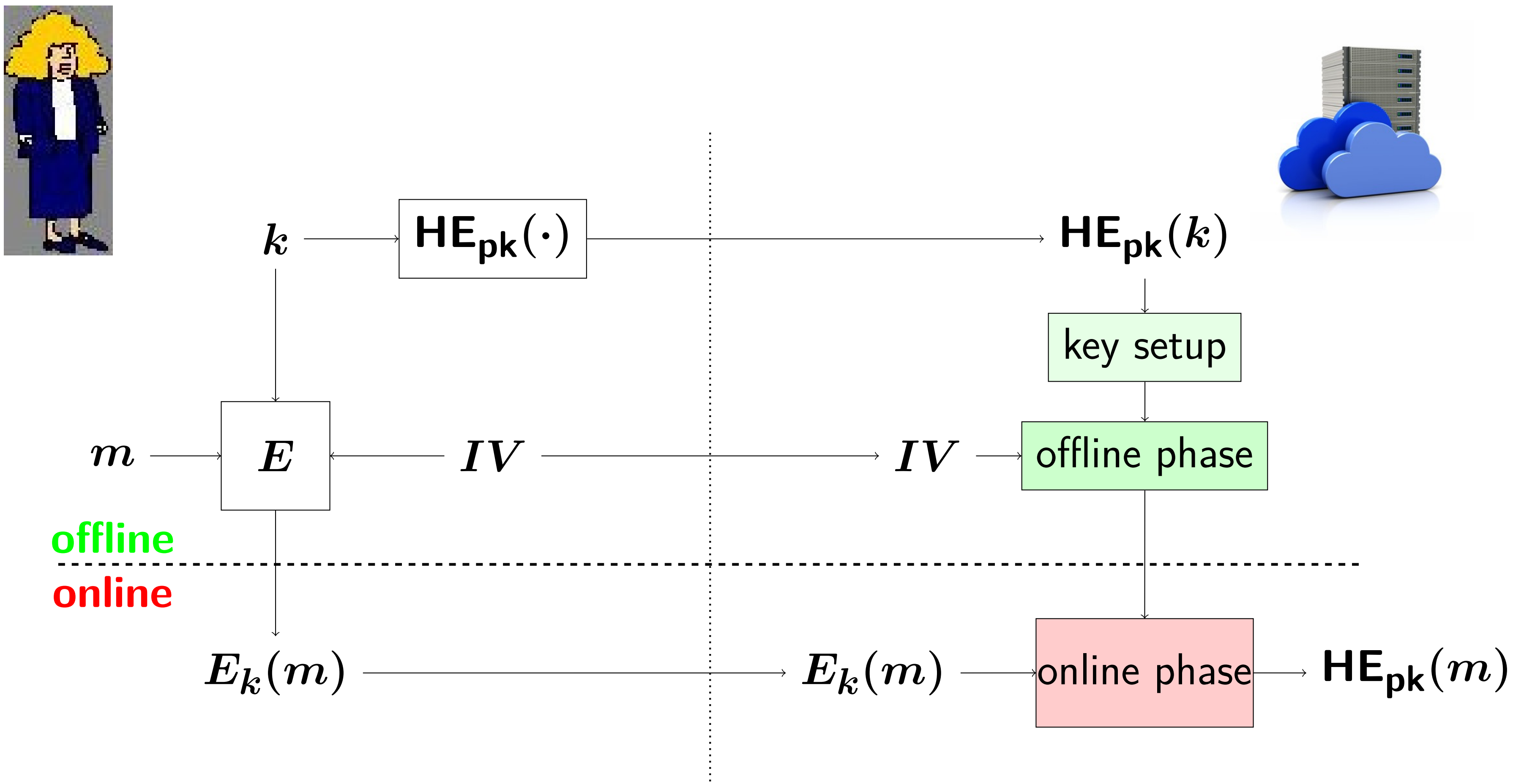
Outline

1. Revisiting the whole encryption scheme

2. Trivium and Kreyvium in the HE setting

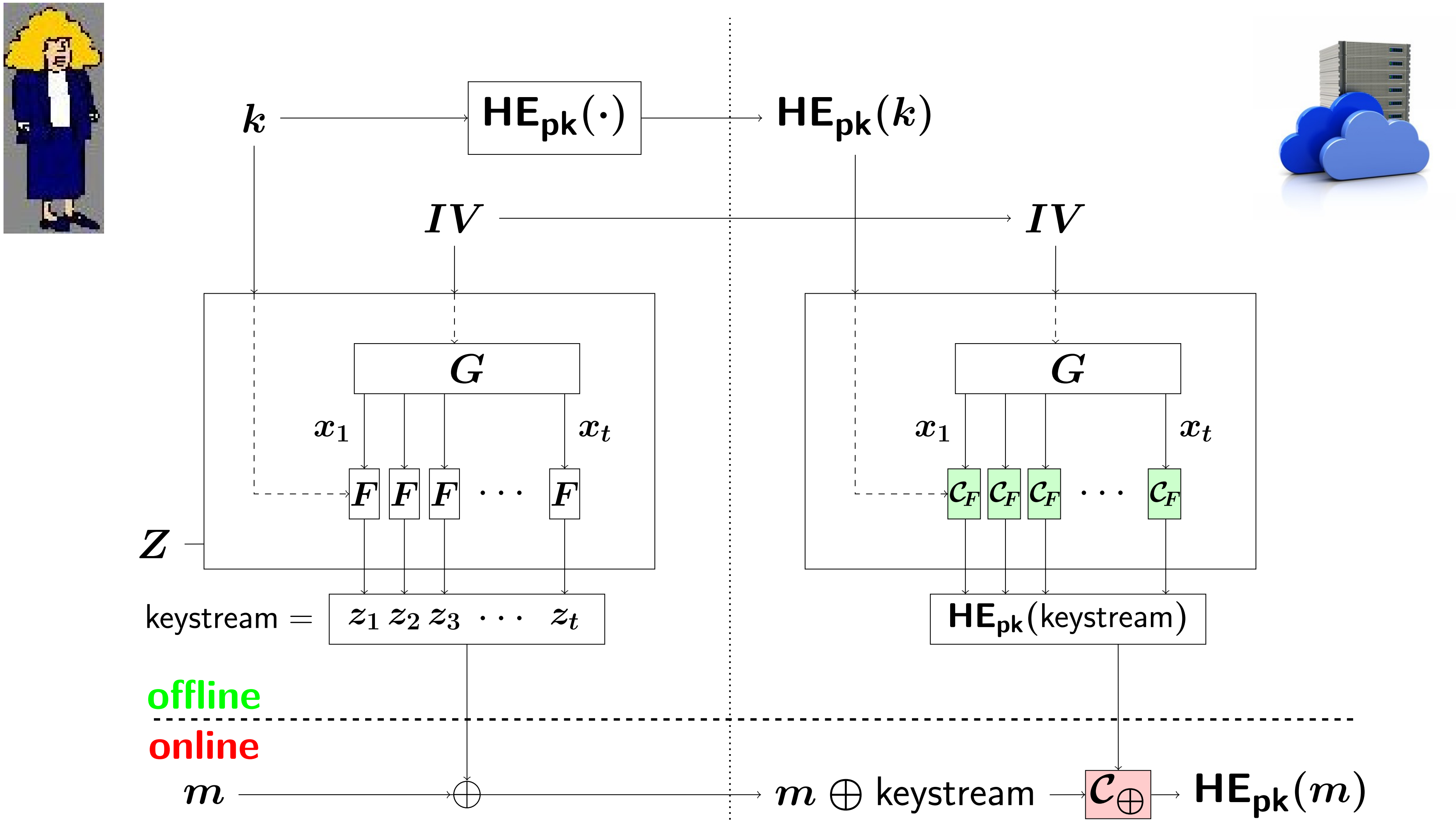
3. Experimental results

Ciphertext decompression with IV-based encryption



$\rightarrow$ Reduce the online phase to a minimum.

With an additive stream cipher



$\rightarrow$ Minimize the multiplicative depth of F.

Instantiation with a counter

Expansion function G:

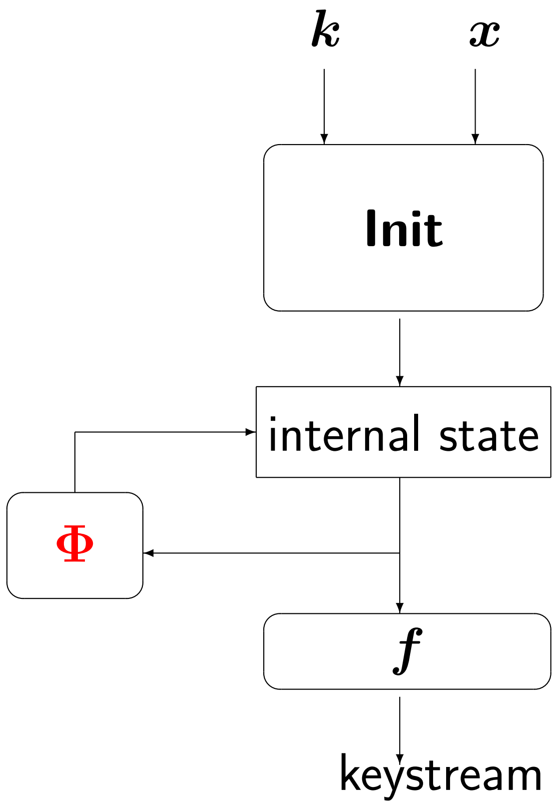
$$G(IV) = (IV,\ IV \boxplus 1,\ IV \boxplus 2, \ldots, IV \boxplus (t-1))$$

Why not use for F a block cipher?

security limited to $2^{n/2}$ where n is the block size.

$\rightarrow$ strong limitation for lightweight ciphers with $n = 64$ or 32.

Low-depth keystream geneartor



- We need a transition function Φ with a low multiplicative depth.
- No strong limitation of the size of the internal state.

Trivium and Kreyvium

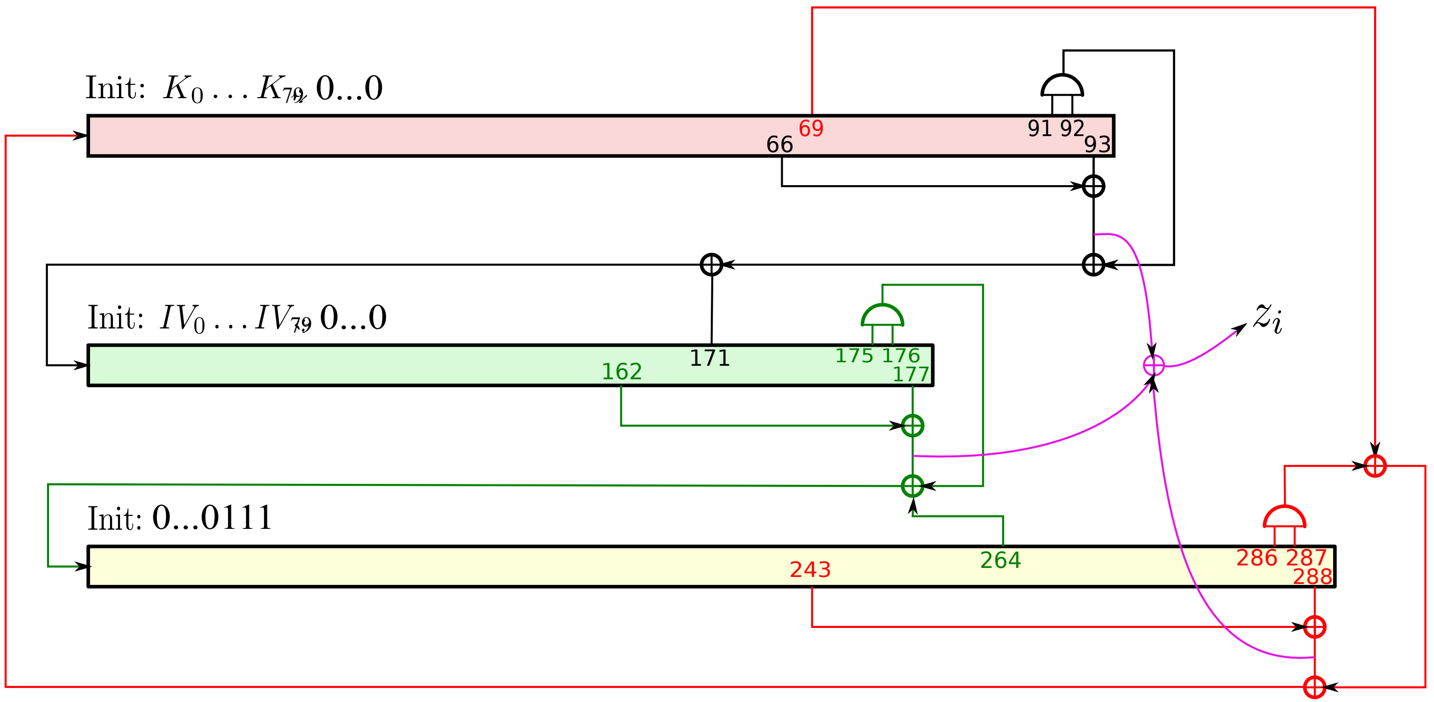
two low-depth stream ciphers

Trivium [De Cannière Preneel 08]

recommended by the eSTREAM project

- transition function with degree 2
- key size $= 80$ bits
- IV size $= 80$ bits
- initialization $= 1152$ blank rounds

Trivium [De Cannière Preneel 08]



93 bits: $(s_1, \ldots, s_{93})$

84 bits: $(s_{94}, \ldots, s_{177})$

111 bits: $(s_{178}, \ldots, s_{288})$

Multiplicative depth of Trivium

The keystream length which can be produced with a circuit of depth $\boldsymbol{d}$, $\boldsymbol{d} \geq \mathbf{4}$, is

$$\mathbf{282} \times \left\lfloor \frac{\boldsymbol{d}}{\mathbf{3}} \right\rfloor + \begin{cases} \mathbf{81} & \text{if } \boldsymbol{d} \equiv \mathbf{0} \bmod \mathbf{3} \\ \mathbf{160} & \text{if } \boldsymbol{d} \equiv \mathbf{1} \bmod \mathbf{3} \\ \mathbf{269} & \text{if } \boldsymbol{d} \equiv \mathbf{2} \bmod \mathbf{3} \end{cases}$$

- At depth $\mathbf{12}$, $\mathbf{57}$ bits
- At depth $\mathbf{13}$, $\mathbf{136}$ bits

Kreyvium, a 128-bit version of Trivium

key size $=$ IV size $=$ 128 bits

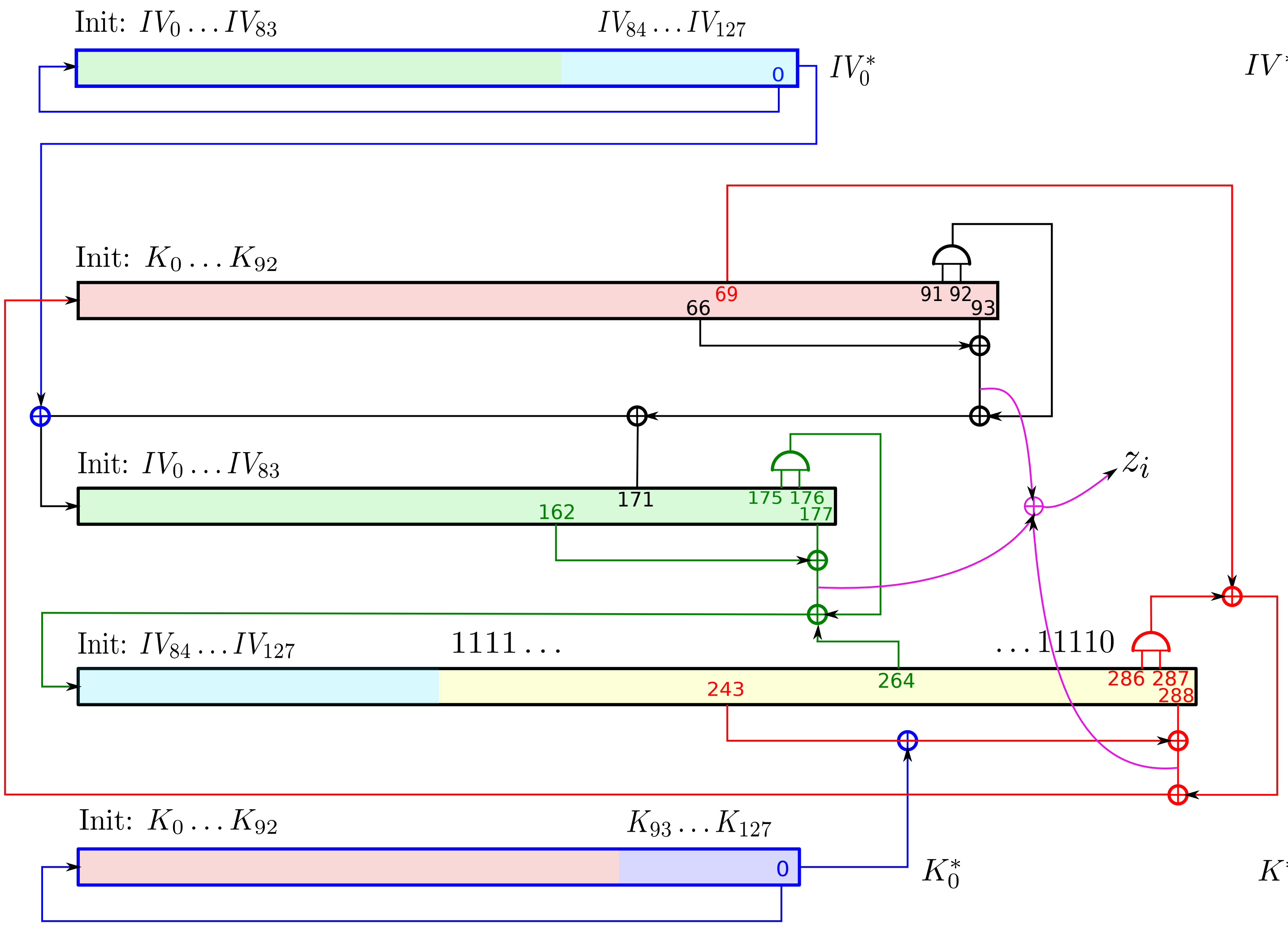
Increasing the size of the internal state.

- no cost if the additionnal part is updated linearly
- better resistance to TMDTO attacks and to algebraic attacks if the additionnal part contains some secret material

$\rightarrow$ the $\mathbf{128}$-bit key and the $\mathbf{128}$-bit IV are added to the internal state

Size of the internal state $=$ 544 bits (416 are unknown)

Kreyvium



IV^*: shift register of length 128

93 bits: $(s_1, \ldots, s_{93})$

84 bits: $(s_{94}, \ldots, s_{177})$

111 bits: $(s_{178}, \ldots, s_{288})$

K^*: shift register of length 128

Multiplicative depth of Kreyvium

The keystream length which can be produced with a circuit of depth d, $d \geq 4$, is

$$282 \times \left\lfloor \frac{d}{3} \right\rfloor + \begin{cases} 70 & \text{if } d \equiv 0 \bmod 3 \\ 149 & \text{if } d \equiv 1 \bmod 3 \\ 258 & \text{if } d \equiv 2 \bmod 3 \end{cases}$$

$\rightarrow$ 11 bits less than with Trivium

- At depth 12, 46 bits
- At depth 13, 125 bits

Some security arguments

Internal state collision:

the number of keystream bits generated from the same key/IV pair must be less than $\mathbf{2^{144}}$.

Algebraic attacks [Maximov Biryukov 07]:

every relation corresponding to a keystream bit introduces a new unknown in the system.

Cube testers [Dinur Shamir 09][Aumasson et al. 09][Fouque Vannet 13]:

two additional XORs per round $\rightarrow$ better mixing of the variables

Conditional differential cryptanalysis [Knellwolf et al. 11]

even in the weak-key setting, 64 bits can never be set to 0

Experimental results

Using HElib (on one core of a server with 4 x AMD Opteron 6172 processors)

	security level	N	used depth	#slots	latency (sec.)	throughput (bits/min)
Trivium-13	80	136	13	600	3650	1341
			20	720	11380	516
Kreyvium-13	128	125	13	682	3987	1272
			20	480	12451	287
LowMC-128	? ≤ 118	256	13	682	3369	3109
			20	480	9977	739

Using the Fan-Vercauteren scheme on a 48-core server

	security level	N	used depth	throughput (bits/min)		Speed gain
				1 core	48 cores	
Trivium-13	80	136	13	9.2	240	$\times$ 26.2
			20	3.4	106	$\times$ 31.0
Kreyvium-13	128	125	13	5.7	151	$\times$ 26.5
			20	2.2	77	$\times$ 34.0
LowMC-128	? ≤ 118	256	14	10.0	90	$\times$ 9.0
			21	4.6	47	$\times$ 10.2

Conclusions

- IV-based stream ciphers are the most appropriate ciphers.
- Good performances can be obtained with firmly-established symmetric ciphers.

Open question.

How many multiplicative levels are necessary to achieve a reasonable security level?
$\rightarrow$ (impractical) approach based on discrete-log achieving a multiplicative depth of $(\lceil \log \kappa \rceil + 1)$ for κ-bit security.