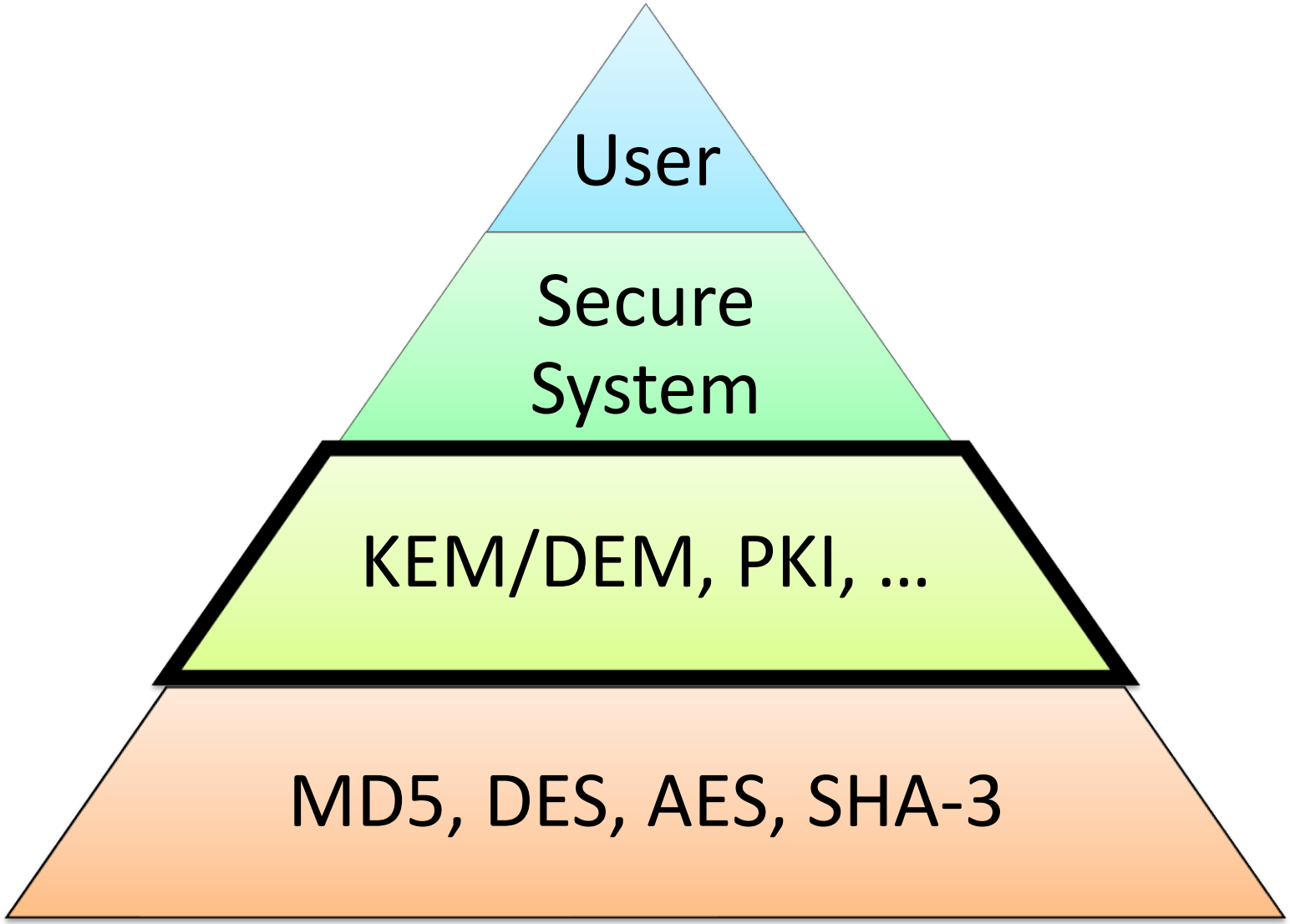
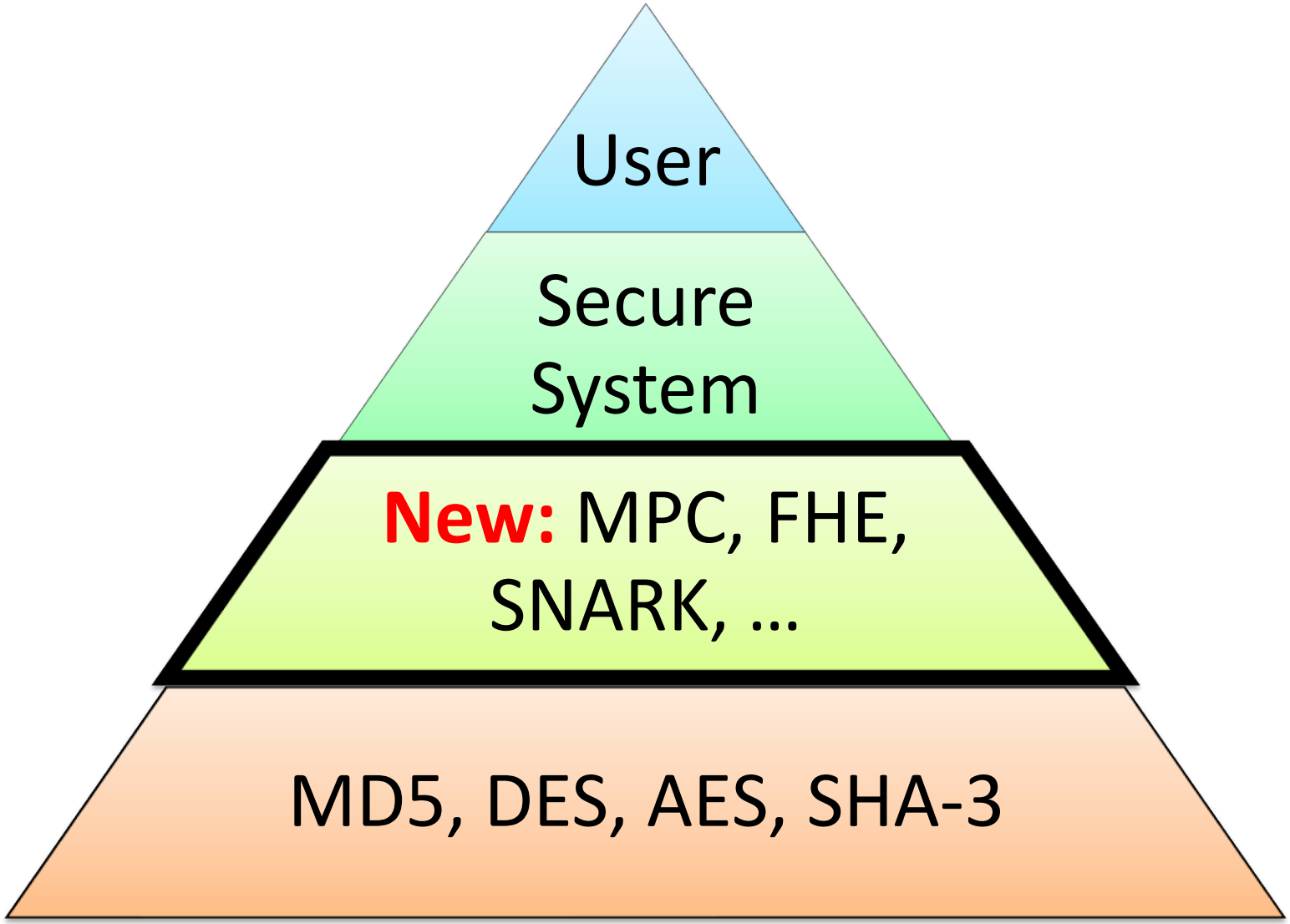
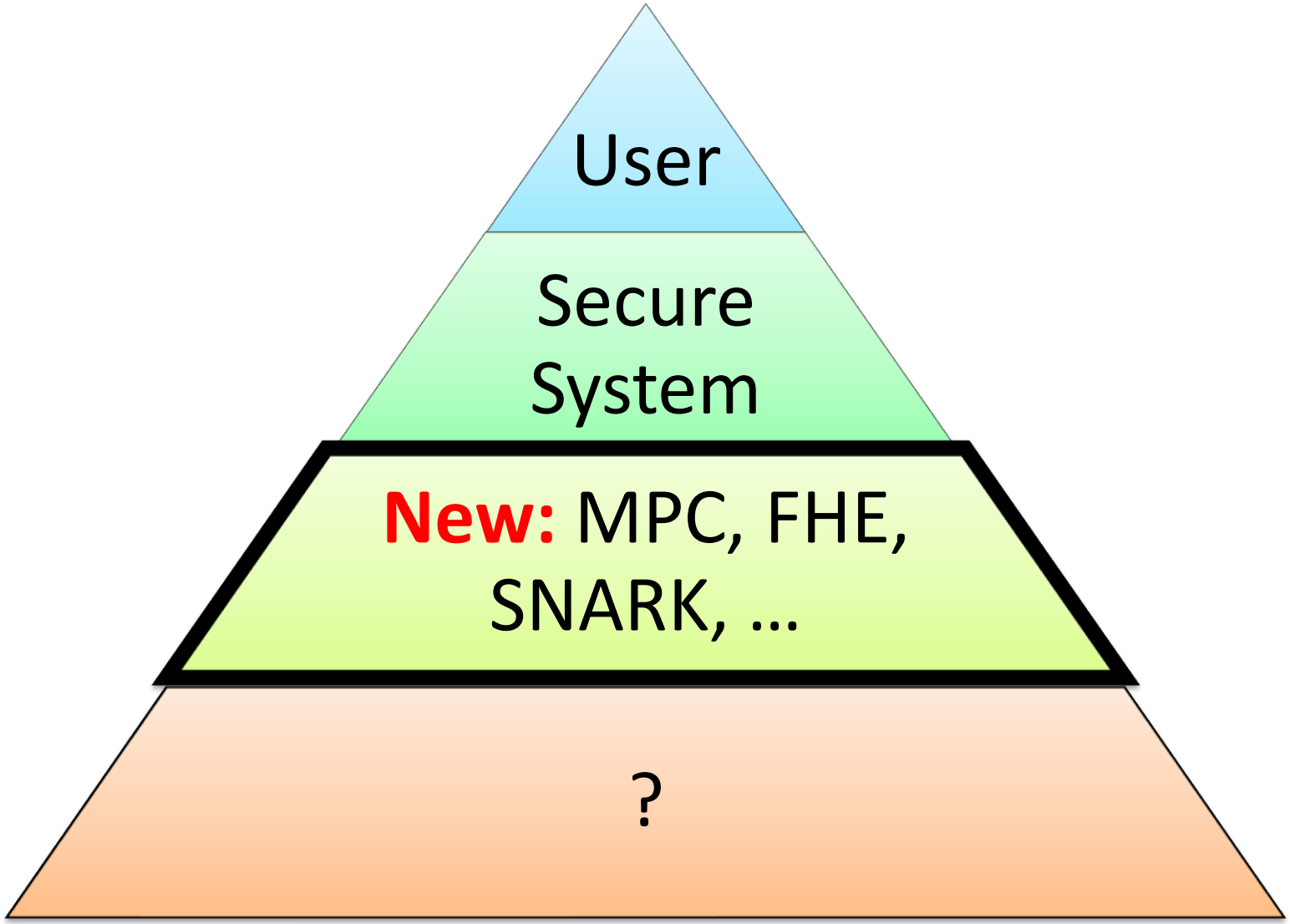
The FHEMPCZK-Cipher Zoo

Christian Rechberger


User
Secure System
KEM/DEM, PKI, …
MD5, DES, AES, SHA-3


User
Secure System
New: MPC, FHE, SNARK, …
MD5, DES, AES, SHA-3


User
Secure System
New: MPC, FHE, SNARK, …
?

The FHEMPCZK-Cipher Zoo

n: number of output bits

all parameters for 128-bit pre-quantum security level

	minMUL	MUL/bit	MULDepth	Who and Where?	Applications	Attacks?
LowMC	2268	8,86	12	Albrecht, Rechberger, Schneider, Tiessen, Zohner Eurocrypt 2016	FHE, MPC, ZK	yes
Kreyvium	1152+3*n	1152 down to 3	12+log(n)	Canteaut, Carpov, Fontaine, Lepoint, Naya-Plasencia, Paillier, Sirdey FSE 2016	FHE	

The FHEMPCZK-Cipher Zoo

n: number of output bits

all parameters for 128-bit pre-quantum security level

	minMUL	MUL/bit	MULDepth	Who and Where?	Applications	Attacks?
LowMC	2268	8,86	12	Albrecht, Rechberger, Schneider, Tiessen, Zohner Eurocrypt 2016	FHE, MPC, ZK	yes
Kreyvium	1152+3*n	1152 down to 3	12+log(n)	Canteaut, Carpov, Fontaine, Lepoint, Naya-Plasencia, Paillier, Sirdey FSE 2016	FHE	
FLIP	>500*n	>500?	4	Méaux, Journault, Standaert, Carlet Eurocrypt 2016	FHE	yes

The FHEMPCZK-Cipher Zoo

n: number of output bits

all parameters for 128-bit pre-quantum security level

	minMUL	MUL/bit	MULDepth	Who and Where?	Applications	Attacks?
LowMC	2268	8,86	12	Albrecht, Rechberger, Schneider, Tiessen, Zohner Eurocrypt 2016	FHE, MPC, ZK	yes
Kreyvium	1152+3*n	1152 down to 3	12+log(n)	Canteaut, Carpov, Fontaine, Lepoint, Naya-Plasencia, Paillier, Sirdey FSE 2016	FHE	
FLIP	>500*n	>500?	4	Méaux, Journault, Standaert, Carlet Eurocrypt 2016	FHE	yes
LowMC v2	**756**	5,91	252	Albrecht, Rechberger, Schneider, Tiessen, Zohner eprint soon	MPC, ZK	
LowMC v2	2646	13,5	**14**	Albrecht, Rechberger, Schneider, Tiessen, Zohner on eprint soon	FHE, MPC, ZK	
LowMC v2	2760	**2,7**	92	Albrecht, Rechberger, Schneider, Tiessen, Zohner on eprint soon	MPC, ZK	

The FHEMPCZK-Cipher Zoo

n: number of output bits

all parameters for 128-bit pre-quantum security level

	minMUL	MUL/bit	MULDepth	Who and Where?	Applications	Attacks?
LowMC	2268	8,86	12	Albrecht, Rechberger, Schneider, Tiessen, Zohner Eurocrypt 2016	FHE, MPC, ZK	yes
Kreyvium	1152+3*n	1152 down to 3	12+log(n)	Canteaut, Carpov, Fontaine, Lepoint, Naya-Plasencia, Paillier, Sirdey FSE 2016	FHE	
FLIP	>500*n	>500?	4	Méaux, Journault, Standaert, Carlet Eurocrypt 2016	FHE	yes
LowMC v2	**756**	5,91	252	Albrecht, Rechberger, Schneider, Tiessen, Zohner eprint soon	MPC, ZK	
LowMC v2	2646	13,5	**14**	Albrecht, Rechberger, Schneider, Tiessen, Zohner on eprint soon	FHE, MPC, ZK	
LowMC v2	2760	**2,7**	92	Albrecht, Rechberger, Schneider, Tiessen, Zohner on eprint soon	MPC, ZK	
MiMC GF(p), not GF(2)	87	0,68	87	Albrecht, Rechberger, Roy, Tiessen, on eprint soon	ZK, MPC	