Efficient Block-wise KDM Secure Public-Key Encryption

Tal Malkin

Isamu Teranishi

Moti Yung

KDM

- Also known as Circular Encryption
  - When the messages can depend on the secret key).
- Definition [D.E. Knuth]:
  - Circular: See under Circular

Key Dependent Message Security (KDM[Func])

Func : Set of fucntions $f : \{\text{SecretKeys}\}^n \rightarrow \{\text{Messages}\}$

For any function f of Func and any i,

$$\mathrm{Enc}_{pk_i}(f(sk_1, \cdots, sk_n)) \underset{\text{comp}}{\simeq} \mathrm{Enc}_{pk_i}(0).$$

Known schemes are inefficient (secure mult.party comp) or bitwise PKE.

And

- Used PK encryption are block wise M=string of bits (not bitwise: M is a bit) in implementations I have seen.
- So efficiency is an issue
- Also: extending the set of functions over keys is an issues

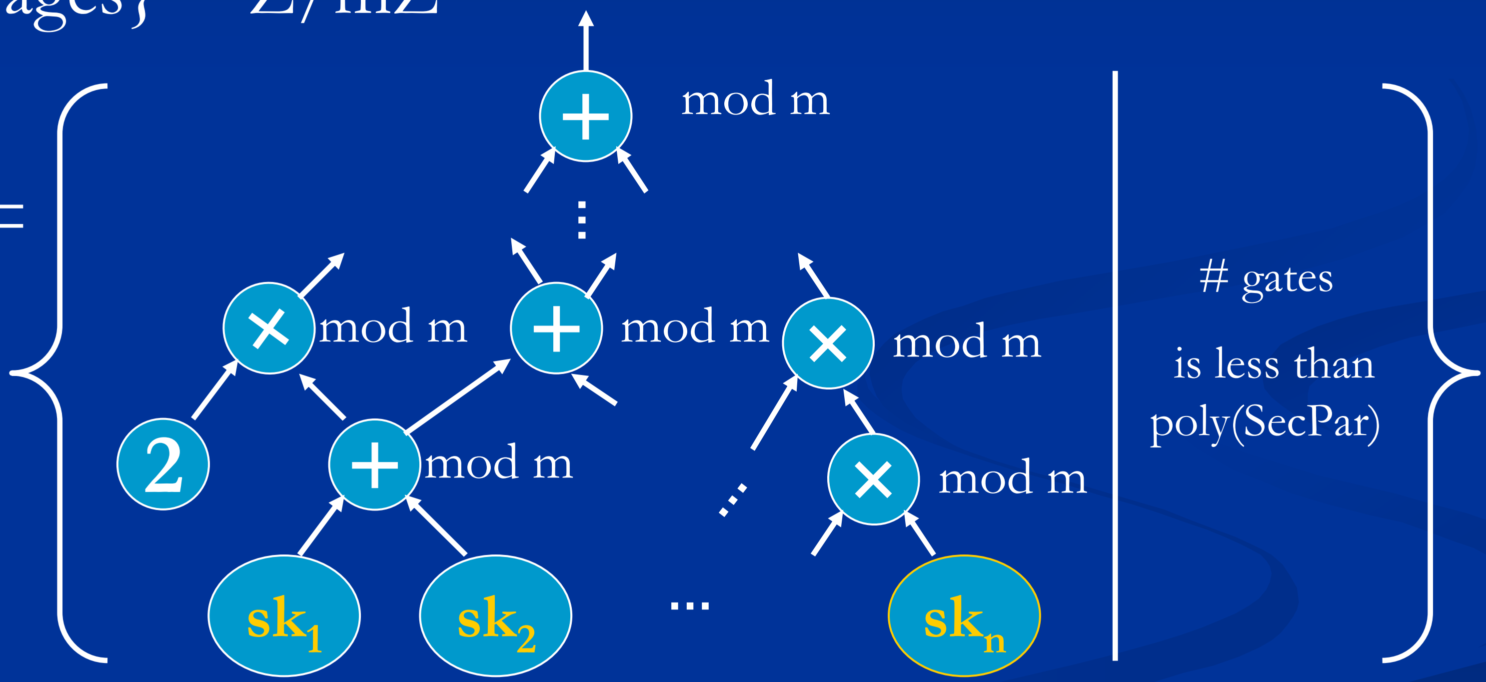
- These were mentioned as open problems in the first talk of the conference.

Proposed Scheme

We propose the first efficient and blockwise KDM secure PKE such that

{Messages} = Z/mZ

Func =



I.e. Set of polysize "modular arithmetic" circuits

with gates + mod m and × mod m .

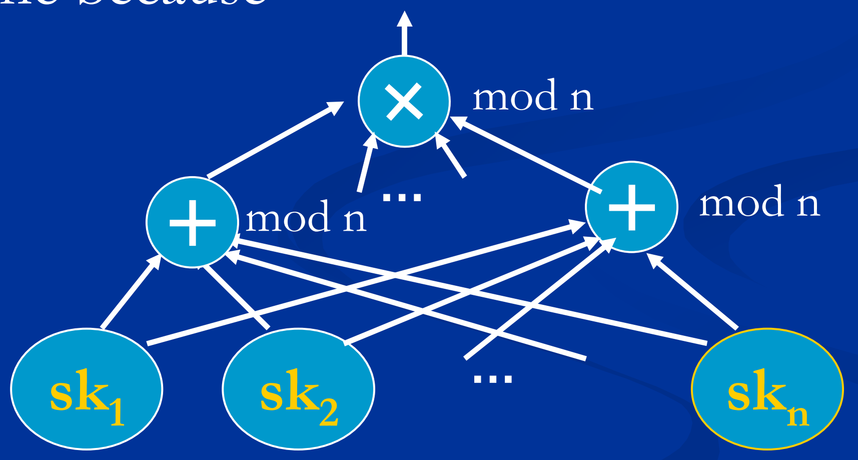
Example of a function.

$$f(sk_1,\dots,sk_n) = (sk_1+\dots+sk_n)^n \bmod n$$

$$= \sum_{\varepsilon_1+\dots+\varepsilon_n=n} sk_1^{\varepsilon_1}\dots\ sk_n^{\varepsilon_n} \bmod n.$$

is an element of our Func because

$f(sk_1,\dots,sk_n)=$



Our Func is the set of polynomials

which can have exponential number of terms.

Proposed Scheme

System param N : RSA modulus mutip of two strong primes.

$pk=(g,h)$, $sk= \log_g h$

$Enc_{pk}(M)$

$$= (g^{r_0}, h^{r_0} g^{r_1}, \ldots, h^{r_{d-1}} g^{r_d}, (1+N)^M h^{r_d}) \mod N^2$$

Our scheme is KDM secure for any f of Func with degree d at most under the DCR assumption.

Comparison

	Blockwise?	Func	Efficiency
[BHHO08] [ACPS09]	No	Linear	Ineffient
[BHHI 10]	No	Bounded Boolian Circuit	Ineffient
[BGK09] [BG10]	No	Polymomial of bits, deg =O(1)	Inefficient
Ours	Yes	Polysize Modular Arithmetic Circuit	Efficient.

Thank you.

Appendix

References

- [ACPS09] Applebaum, Cash, Peitkert, Sahai :
  Fast Cryptographic Primitives and Circular-Secure Encryption
  Based on Hard Learning Problems. Crypto 2009.
- [BG10] Brakerski, Goldwasser :
  Circular and Leakage Resilient Public-Key Encryption
  Under Subgroup Indistinguishability. Crypto 2010.
- [BGK09] Brakerski, Goldwasser, Kalai :
  Circular-Secure Encryption Beyond Affine Functions eprint.
- [BHHI10] Barak, Haitner, Hofheinz, Ishai :
  Bounded Key-Dependent Message Security. Eurocrypt 2010.
- [BHHO08] Boneh, Halevi, Hamburg, Ostrovsky :
  Circular-Secure Encryption from Decision Diffie-Hellman.
  Crypto 2008
- [CCS09] Camenisch, Chandran, Shoup :
  A Public Key Encryption Scheme Secure against Key Dependent
  Chosen Plaintext and Adaptive Chosen Ciphertext Attacks. Eurocrypt 2009

Idea Behind Proof (1)

Simulator sets

$$sk_1 = x + \alpha_1, \ldots, sk_n = x + \alpha_n$$

where x : unknown exponent.

α_i : random element selected by the simulator.

Because f of Func is a polynomial, f can be written as

$$f(sk_1, \ldots, sk_n) = a_0 + a_1 x + \ldots a_n x^n \bmod N.$$

Lemma : $a_0, \ldots, a_n$ can be computed in polytime if f is a polysize modular arithmetic circuit.

Idea Behind Proof (2)

T=1+N

lemma:

$(\quad g^r, T^{f(x)x+a}h^r) \bmod N^2$

Degree is reduced.

$\approx_{comp}$

$(T^{f(x)}g^r, T^{a} \quad h^r) \bmod N^2$

$(\ g^{r_1},\ h^{r_1} g^{r_2},\ \ldots\ ,\ h^{r_{d-1}} g^{r_d},\ T^{f(x)} h^{r_d}) \bmod N^2$

reduced. reduced. … reduced. reduced.

$\approx_{comp}$

$(T^{a_0} g^{r_0}, T^{a_1} h^{r_0} g^{r_1},\ \ldots\ , T^{a_{d-1}} h^{r_{d-1}} g^{r_d}, T^{a_d} h^{r_d}) \bmod N^2$