

On methods of shortening ElGamal-type signatures

Alexandra Babueva,
Engineer – analyst,
CryptoPro LLC

Liliya Akhmetzyanova, Evgeny Alekseev,
Stanislav Smyshlyayev



1 Motivation

2 Related works

3 ElGamal-type signatures

4 Three methods of shortening

5 Security model

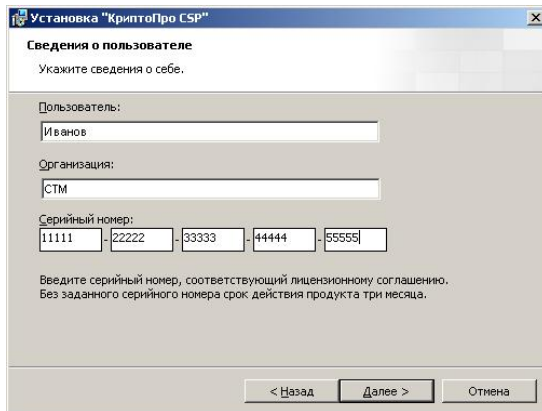
6 Security bounds

7 GOST-H_S scheme

kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּחְבֻּלָּה māt mǎ hoc криптография criptografia
 ծածկագիտություն kryptografia շրժճտգրագոօս криптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

Application

Product registration systems



Установка "КриптоПро CSP"

Сведения о пользователе

Укажите сведения о себе.

Пользователь:
Иванов

Организация:
СТМ

Серийный номер:
11111 - 22222 - 33333 - 44444 - 55555

Введите серийный номер, соответствующий лицензионному соглашению.
Без заданного серийного номера срок действия продукта три месяца.

< Назад Далее > Отмена

māt mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժճտգրագոօս криптография κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोग्राफी salauksen криптография การเข้ารหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密

kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מפתח mât mã hoc крпптография criptografia
 ծածկագիտություն kryptografia շրոճժշընդոօս kриптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מפתח
 mât mã hoc крпптография criptografia ծածկագիտություն kryptografia շրոճժշընդոօս kриптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोबाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密
 码 kriptografi cifrado מפתח מפתח mât mã hoc крпптография criptografia ծածկագիտություն kryptografia շրոճժշընդոօս kриптография

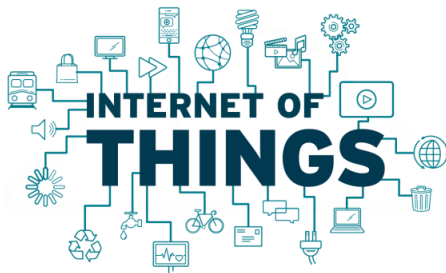
License code using GOST signature scheme with $q \sim 2^{256}$:

GHTYZ - TYRED - JHGYU - KJGYL - RESTG -
KJBIL - Q7SF9 - MNEWR - 298US - KAJB9 -
MNBUI - 98KBK - 3KJB4 - KJB9K - IEV8U -
WBER9 - W98WB - BVEWR - 9VG73 - BWE79 -
H8R

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado קריפטוגרפיה mât mã học крпптографія criptografia
 ծածկագիտություն kryptografia շրժձժեղճաջօօժ крпптография крпптоγράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen
 крпптаграфия การฉนวนรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado קריפטוגרפיה

Application

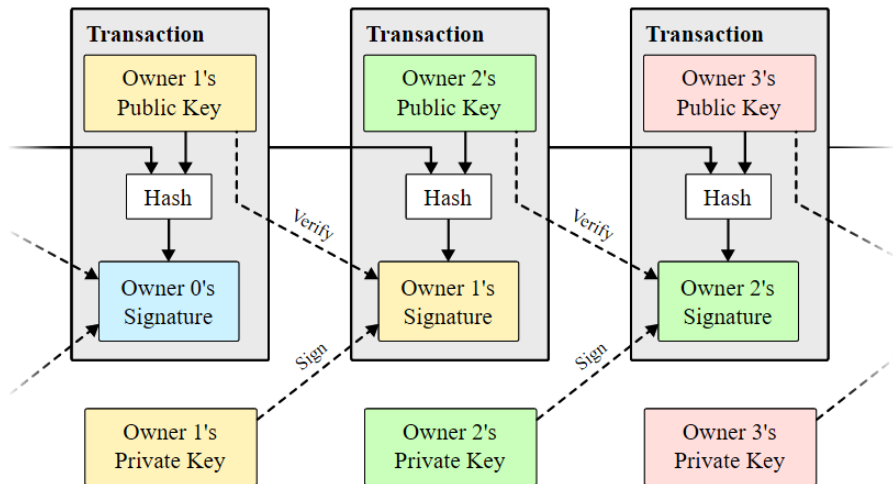
Low-bandwidth communication environments



крпптаграфия การฉนวนรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado קריפטוגרפיה
 mât mã học крпптографія criptografia ծածկագիտություն kryptografia շրժձժեղճաջօօժ крпптография крпптоγράφηση cryptography 暗号化
 kryptographie किप्टोबाफी salauksen крпптаграфия การฉนวนรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密碼

Application

Blockchain platforms



1 Motivation

2 Related works

3 ElGamal-type signatures

4 Three methods of shortening

5 Security model

6 Security bounds

7 GOST-H_s scheme

kriptografija 암호화 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado קריפטוגרפיה mật mã học криптография criptografia

BLS signature scheme

Boneh D., Lynn B., Shacham H. "Short Signatures from the Weil Pairing"

- based on Weil pairing;
- signature size: 160 bit;
- need "pairing-friendly" curves.

Multivariate signature schemes

Quartz, Gui, SFLASH, UOV, Rainbow

- based on Hidden Field Equations;
- signature size: from 110 bit;
- relatively large public key size.

Need new primitives!

BLS signature scheme

Boneh D., Lynn B., Shacham H. "Short Signatures from the Weil Pairing"

- based on Weil pairing;
- signature size: 160 bit;
- need "pairing-friendly" curves.

Multivariate signature schemes

Quartz, Gui, SFLASH, UOV, Rainbow

- based on Hidden Field Equations;
- signature size: from 110 bit;
- relatively large public key size.

Need new primitives!

Zheng Y. Digital signcryption or how to achieve $\text{cost}(\text{signature} \ \& \ \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$

Shortened schemes	Signature (r, s) on a message m	Recovery of $k = g^x \bmod p$	Length of signature
SDSS1	$r = \text{hash}(g^x \bmod p, m)$ $s = x/(r + x_a) \bmod q$	$k = (y_a \cdot g^r)^s \bmod p$	$ \text{hash}(\cdot) + q $
SDSS2	$r = \text{hash}(g^x \bmod p, m)$ $s = x/(1 + x_a \cdot r) \bmod q$	$k = (g \cdot y_a^r)^s \bmod p$	$ \text{hash}(\cdot) + q $

- Shnorr signature modification;
- no concrete bounds.

Zheng Y. Digital signcryption or how to achieve $\text{cost}(\text{signature} \& \text{encryption}) \ll \text{cost}(\text{signature}) + \text{cost}(\text{encryption})$

Shortened schemes	Signature (r, s) on a message m	Recovery of $k = g^x \bmod p$	Length of signature
SDSS1	$r = \text{hash}(g^x \bmod p, m)$ $s = x / (r + x_a) \bmod q$	$k = (y_a \cdot g^r)^s \bmod p$	$ \text{hash}(\cdot) + q $
SDSS2	$r = \text{hash}(g^x \bmod p, m)$ $s = x / (1 + x_a \cdot r) \bmod q$	$k = (g \cdot y_a^r)^s \bmod p$	$ \text{hash}(\cdot) + q $

- Shnorr signature modification;
- no concrete bounds.

To shorten ElGamal-type signature providing the sufficient security level

mật mã học криптография cryptografia δαδλσϗηυνηρυην kryptografia ვრბდტვგრდგოლ криптография κρυπτογράφηση cryptography 暗号化
kryptographie கிர்ப்தொகாபி salauksen крпптаграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密碼
kriptografi cifrado פצראשפיקר mât mã học криптография cryptografia δαδλσϗηυνηρυην kryptografia ვრბდტვგრდგოლ криптография
κρυπτογράφηση cryptography 暗号化 kryptographie கிர்ப்தொகாபி salauksen крпптаграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화
crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado פצראשפיקר mât mã học криптография cryptografia δαδλσϗηυνηρυην kryptografia
ვრბდტვग्रदगोल कुरिप्टोग्राफिया κρυπτογράφηση cryptography 暗号化 kryptographie கிர்ப்தொகாபி salauksen крпптаграфия การฉานรหึส kriptografija
رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado פצראשפיקר mât mã học криптография cryptografia
δαδλσϗηυνηρυην kryptografia ვრბდტवग्रदगोल कुरिप्टोग्राफिया κρυπτογράφηση cryptography 暗号化 kryptographie கிர்ப்தொகாபி salauksen
кρпптаграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado פצראשפיקר
mât mã học криптография cryptografia δαδλσϗηυνηρυην kryptografia ვრბდტவग्रदगोल कुरिप्टोग्राफिया κρυπτογράφηση cryptography 暗号化
kryptographie கிர்ப்தொகாபி salauksen крпптаграфия การฉานรหึส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密碼

1 Motivation

2 Related works

3 ElGamal-type signatures

3 ElGamal-type signatures

4 Three methods of shortening

Security model

Security bounds

ბეჭდურობის კრიპტოგრაფია

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה mât mã học крпптографія criptografia
 ծածկագիտություն kryptografia շրժժեղացրացոօս криптография крптоγράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה

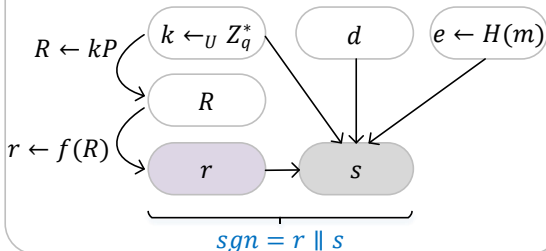
GenEG scheme

GenEG.KGen():

$$d \leftarrow_U Z_q^*$$

$$Q \leftarrow dP$$

GenEG.Sig(d, m):



ծածկագիտություն kryptografia շրժժեղացրացոօս криптография крптоγράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה
 mât mã học крпптографія criptografia ծածկագիտություն kryptografia շրժժեղացրացոօս криптография крптоγράφηση cryptography 暗号化
 kryptographie किप्टोगाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密

GOST signature scheme

δω
kpi
mā
mā
碼
kpi
crit
ჯრ
مسي
δω
kpi
mā
kry
碼
kpi
crit
ჯრ
مسي
δω
kpi
mā

KGen()	Sig(d, m)	Vf($Q, m, \bar{r} \parallel \bar{s}$)
1 : $d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$	1 : $e \leftarrow H(m) \bmod q$	1 : if ($r = 0 \vee s = 0$) :
2 : $Q \leftarrow dP$	2 : if $e = 0$: $e \leftarrow 1$	2 : return 0
3 : return (d, Q)	3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$	3 : $e \leftarrow H(m)$
	4 : if $k = 0$: return $\perp$	4 : if $e = 0$: $e \leftarrow 1$
	5 : $R \leftarrow kP$	5 : $R \leftarrow e^{-1}sP - e^{-1}rQ$
	6 : $r \leftarrow R.x \bmod q$	6 : if $R.x \bmod q \neq r$:
	7 : if $r = 0$: return $\perp$	7 : return 0
	8 : $s \leftarrow ke + dr$	8 : return 1
	9 : if $s = 0$: return $\perp$	
	10 : return $\bar{r} \parallel \bar{s}$	

GOST signature scheme

δw
kpi
mā
mā
碼
kpi
crit
ჯრ
معی
δw
kpi
mā
kry
碼
kpi
crit
ჯრ
معی
δw
kpi
mā

KGen()	Sig(d, m)	Vf($Q, m, \bar{r} \parallel \bar{s}$)
1 : $d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$	1 : $e \leftarrow H(m) \bmod q$	1 : if ($r = 0 \vee s = 0$) :
2 : $Q \leftarrow dP$	2 : if $e = 0$: $e \leftarrow 1$	2 : return 0
3 : return (d, Q)	3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$	3 : $e \leftarrow H(m)$
	4 : if $k = 0$: return $\perp$	4 : if $e = 0$: $e \leftarrow 1$
	5 : $R \leftarrow kP$	5 : $R \leftarrow e^{-1}sP - e^{-1}rQ$
	6 : $r \leftarrow R.x \bmod q$	6 : if $R.x \bmod q \neq r$:
	7 : if $r = 0$: return $\perp$	7 : return 0
	8 : $s \leftarrow ke + dr$	8 : return 1
	9 : if $s = 0$: return $\perp$	
	10 : return $\bar{r} \parallel \bar{s}$	

GOST signature scheme

δw

kpi

mā

kpi

mā

kpi

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

crit

KGen()

Sig(d, m)Vf($Q, m, \bar{r} \parallel \bar{s}$)1 : $d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$ 2 : $Q \leftarrow dP$ 3 : **return** (d, Q)1 : $e \leftarrow H(m) \bmod q$ 2 : **if** $e = 0$: $e \leftarrow 1$ 3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$ 4 : **if** $k = 0$: **return** $\perp$ 5 : $R \leftarrow kP$ 6 : $r \leftarrow R.x \bmod q$ 7 : **if** $r = 0$: **return** $\perp$ 8 : $s \leftarrow ke + dr$ 9 : **if** $s = 0$: **return** $\perp$ 10 : **return** $\bar{r} \parallel \bar{s}$ 1 : **if** ($r = 0 \vee s = 0$) :2 : **return** 03 : $e \leftarrow H(m)$ 4 : **if** $e = 0$: $e \leftarrow 1$ 5 : $R \leftarrow e^{-1}sP - e^{-1}rQ$ 6 : **if** $R.x \bmod q \neq r$:7 : **return** 08 : **return** 1

GOST signature scheme

δω
kpi
mā
mā
碼
kpi
crit
ჯრ
معی
δω
kpi
mā
kry
碼
kpi
crit
ჯრ
معی
δω
kpi
mā

KGen()	Sig(d, m)	Vf($Q, m, \bar{r} \parallel \bar{s}$)
1 : $d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$	1 : $e \leftarrow H(m) \bmod q$	1 : if ($r = 0 \vee s = 0$) :
2 : $Q \leftarrow dP$	2 : if $e = 0$: $e \leftarrow 1$	2 : return 0
3 : return (d, Q)	3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$	3 : $e \leftarrow H(m)$
	4 : if $k = 0$: return $\perp$	4 : if $e = 0$: $e \leftarrow 1$
	5 : $R \leftarrow kP$	5 : $R \leftarrow e^{-1}sP - e^{-1}rQ$
	6 : $r \leftarrow R.x \bmod q$	6 : if $R.x \bmod q \neq r$:
	7 : if $r = 0$: return $\perp$	7 : return 0
	8 : $s \leftarrow ke + dr$	8 : return 1
	9 : if $s = 0$: return $\perp$	
	10 : return $\bar{r} \parallel \bar{s}$	

GOST signature scheme

δw

kpi

mā

kpi

mā

mā

kpi

crit

צר

crit

δw

kpi

mā

kpi

mā

kpi

crit

צר

crit

δw

kpi

mā

kpi

mā

δw

kpi

mā

kpi

mā

kpi

mā

KGen()

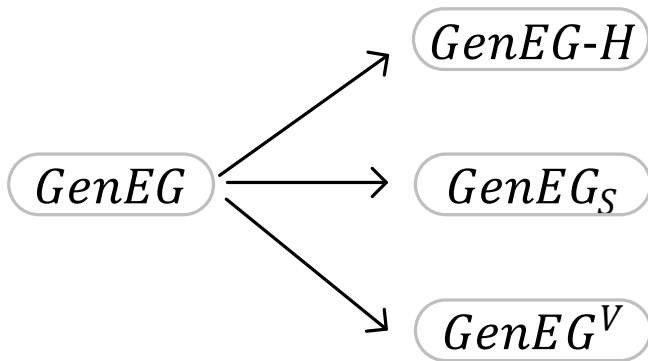
Sig(d, m)Vf($Q, m, \bar{r} \parallel \bar{s}$)1 : $d \xleftarrow{\mathcal{U}} \mathbb{Z}_q^*$ 2 : $Q \leftarrow dP$ 3 : **return** (d, Q)1 : $e \leftarrow H(m) \bmod q$ 2 : **if** $e = 0$: $e \leftarrow 1$ 3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$ 4 : **if** $k = 0$: **return** $\perp$ 5 : $R \leftarrow kP$ 6 : $r \leftarrow R.x \bmod q$ 7 : **if** $r = 0$: **return** $\perp$ 8 : $s \leftarrow ke + dr$ 9 : **if** $s = 0$: **return** $\perp$ 10 : **return** $\bar{r} \parallel \bar{s}$ 1 : **if** ($r = 0 \vee s = 0$) :2 : **return** 03 : $e \leftarrow H(m)$ 4 : **if** $e = 0$: $e \leftarrow 1$ 5 : $R \leftarrow e^{-1}sP - e^{-1}rQ$ 6 : **if** $R.x \bmod q \neq r$:7 : **return** 08 : **return** 1

2 Related works

4 Three methods of shortening

6 Security bounds

Three methods:

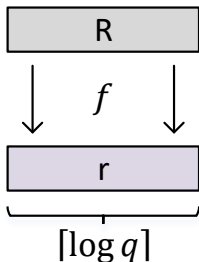


GenEG-H scheme

Idea:

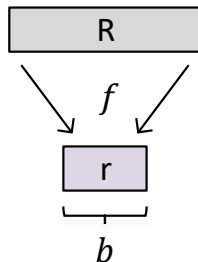
standard GenEG

$$f = R \cdot x \bmod q$$



GenEG-H

$$f = H(R \cdot x) \bmod 2^b$$



GenEG-H scheme

Parameter: b – size of truncated hash output, $b < \lceil \log_2 q \rceil$.

Hash function $H \rightarrow \begin{cases} H_1(x) & = H(0 \parallel x) \pmod{q} \text{ --- message hashing} \\ H_2(x) & = H(1 \parallel x) \pmod{2^b} \text{ --- } R.x \text{ hashing} \end{cases}$

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תעודת המידע мәт мә һөс криптография criptografia
 ծածկագրությունը kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

GenEG-H scheme

Parameter: b – size of truncated hash output, $b < \lceil \log_2 q \rceil$.

кри kriptografi cifrado תעודת המידע мәт мә һөс криптография criptografia ծածկագրությունը kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա

Hash function $H \rightarrow \begin{cases} H_1(x) = H(0 \parallel x) \bmod q & \text{— message hashing} \\ H_2(x) = H(1 \parallel x) \bmod 2^b & \text{— } R.x \text{ hashing} \end{cases}$

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

$$f(R) = \phi(H_2(R.x)),$$

ϕ maps argument to element in $\mathbb{Z}_q^*$: $\begin{cases} x \in \{0, 1\}^b \setminus \{0\} & \mapsto \text{int}(x) \\ 0 & \mapsto 2^b \end{cases}$

رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תעודת המידע мәт мә һөс криптография criptografia

ծածկագրությունը kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

кри kryptografia ճոճճոցճոցոօօ կռիթոգրաֆիա κρυπτογράφησης kryptographv 暗号化 kryptographie किप्टोग्राफी salauksen

GenEG-H scheme

Parameter: b – size of truncated hash output, $b < \lceil \log_2 q \rceil$.

Hash function $H \rightarrow \begin{cases} H_1(x) = H(0 \parallel x) \bmod q & \text{— message hashing} \\ H_2(x) = H(1 \parallel x) \bmod 2^b & \text{— } R.x \text{ hashing} \end{cases}$

$$f(R) = \phi(H_2(R.x)),$$

ϕ maps argument to element in $\mathbb{Z}_q^*$: $\begin{cases} x \in \{0, 1\}^b \setminus \{0\} & \mapsto \text{int}(x) \\ 0 & \mapsto 2^b \end{cases}$.

Signature size: $\lceil \log_2 q \rceil + b + 1$

GenEG-H scheme

Parameter: b – size of truncated hash output, $b < \lceil \log_2 q \rceil$.

Hash function $H \rightarrow \begin{cases} H_1(x) = H(0 \parallel x) \bmod q & \text{— message hashing} \\ H_2(x) = H(1 \parallel x) \bmod 2^b & \text{— } R.x \text{ hashing} \end{cases}$

$$f(R) = \phi(H_2(R.x)),$$

ϕ maps argument to element in $\mathbb{Z}_q^*$: $\begin{cases} x \in \{0, 1\}^b \setminus \{0\} & \mapsto \text{int}(x) \\ 0 & \mapsto 2^b \end{cases}$.

Signature size: $\lceil \log_2 q \rceil + b + 1$

GOST-H scheme

Sig(d, m)

```

1 :  $e \leftarrow H_1(m)$ 
2 : if  $e = 0$  :  $e \leftarrow 1$ 
3 :  $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$ 
4 : if  $k = 0$  : return  $\perp$ 
5 :  $R \leftarrow kP$ 
6 :  $r \leftarrow \phi(H_2(R.x))$ 
7 :  $s \leftarrow ke + dr$ 
8 : if  $s = 0$  : return  $\perp$ 
9 : return  $\bar{r} \parallel \bar{s}$ 

```

Vf($Q, m, \bar{r} \parallel \bar{s}$)

```

1 : if  $s = 0$  : return 0
2 :  $e \leftarrow H_1(m)$ 
3 : if  $e = 0$  :  $e \leftarrow 1$ 
4 :  $R \leftarrow e^{-1}sP - e^{-1}rQ$ 
5 : if  $\phi(H_2(R.x)) \neq r$  :
6 :   return 0
7 : return 1

```

 ϕ properties $\Rightarrow r \neq 0$

GOST-H scheme

$\text{Sig}(d, m)$	$\text{Vf}(Q, m, \bar{r} \parallel \bar{s})$
1 : $e \leftarrow H_1(m)$	1 : if $s = 0$: return 0
2 : if $e = 0$: $e \leftarrow 1$	2 : $e \leftarrow H_1(m)$
3 : $k \xleftarrow{\mathcal{U}} \mathbb{Z}_q$	3 : if $e = 0$: $e \leftarrow 1$
4 : if $k = 0$: return $\perp$	4 : $R \leftarrow e^{-1}sP - e^{-1}rQ$
5 : $R \leftarrow kP$	5 : if $\phi(H_2(R.x)) \neq r$:
6 : $r \leftarrow \phi(H_2(R.x))$	6 : return 0
7 : $s \leftarrow ke + dr$	7 : return 1
8 : if $s = 0$: return $\perp$	
9 : return $\bar{r} \parallel \bar{s}$	

ϕ properties $\Rightarrow r \neq 0$

GenEG_s scheme

Idea:

«Good» r : $r = r^* \parallel \underbrace{\text{const}}_l$

Sign

Generate $r \parallel s$ Until r is «good» $sgn = r^* \parallel s$

Verify

 $r = r^* \parallel \text{const}$ Verify ($r \parallel s$)

GenEG_s scheme

Parameters:

- l – number of fixed bits in r ;
- thr – number of attempts to generate valid signature.

Signature size is reduced by l bits.

Assumption: $lsb_l(f(R))$ distribution is close to uniform.

Probability to output failure indicator:

$$pr \approx (1 - 2^{-l})^{thr}.$$

Optimal: $thr = 2^l$. Thus $pr \leq e^{-1}$ for all l .

GenEG_s scheme

Parameters:

- l – number of fixed bits in r ;
- thr – number of attempts to generate valid signature.

Signature size is reduced by l bits.

Assumption: $\text{lsb}_l(f(R))$ distribution is close to uniform.

Probability to output failure indicator:

$$pr \approx (1 - 2^{-l})^{thr}.$$

Optimal: $thr = 2^l$. Thus $pr \leq e^{-1}$ for all l .

kriptogrāfija 암호화 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado מַאֵת מֵאָה קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia ვრცელდება კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen

GenEG_S scheme

Sig(d, m)

```

1 :  $cnt \leftarrow 0$ 
2 : if  $cnt > thr$  : return  $\perp$ 
3 :  $cnt \leftarrow cnt + 1$ 
4 :  $\bar{r} \parallel \bar{s} \leftarrow \text{GenEG.Sig}(d, m)$ 
5 : if  $\bar{r} \parallel \bar{s} = \perp$  : goto 2
6 : if  $\text{lsb}_l(\bar{r}) \neq \text{const}$  : goto 2
7 :  $\bar{r}^* = \text{msb}_{|\bar{r}|-l}(\bar{r})$ 
8 : return  $\bar{r}^* \parallel \bar{s}$ 
  
```

Vf($Q, m, \bar{r}^* \parallel \bar{s}$)

```

1 :  $\bar{r} \leftarrow \bar{r}^* \parallel \text{const}$ 
2 :  $res \leftarrow \text{GenEG.Vf}(Q, m, \bar{r} \parallel \bar{s})$ 
3 : return  $res$ 
  
```

криптография шифрование kryptografija رمز نویسی kriptografija 暗号化 crittografia dumlál cripteagrafalochta 密码 kriptografi cifrado מַאֵת מֵאָה קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia ვრცელდება კრიპტოგრაფია κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोग्राफी salauksen криптография การเข้ารหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafalochta 密码

kriptografija 암호화 criptografia dumlál criptografalocta 密码 kriptografi cifrado תריפוטוגרפיה mât mã học крпптографія criptografia
 ծածկագիտություն kryptografia շրժձժշջճաջոօօօ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen
 kriptografija 암호화 criptografia dumlál criptografalocta 密码 kriptografi cifrado תריפוטוגרפיה mât mã học крпптографія criptografia

GenEG^V scheme

Idea:

Sign

Generate

sgn

Cut

sgn'

t

Return sgn'

Verify



$sgn = sgn' \parallel i$

Verify sgn

2^t

кryptografija การฉนวนรหัส kriptografija رمز نویسی kriptografija 암호화 criptografia dumlál criptografalocta 密码 kriptografi cifrado תריפוטוגרפיה mât mã học крпптографія criptografia
 ծածկագիտություն kryptografia շրժձժշջճաջոօօօ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen кryptografija การฉนวนรหัส kriptografija رمز نویسی kriptografija 암호화 criptografia dumlál criptografalocta 密码

kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאת מאהוד קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримтаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאת מאהוד קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримтаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码

GenEG^V scheme

Parameter:

- t – number of truncated bits.

Signature size is reduced by t bits.

maet ma hoc кримтография crintografia ծածկագիտություն kryptografia շրժժեղանգոօս кримтография кρυπτογράφηση cryptography 暗号化
 kry It's possible to cut either r or s component. The method can be applied
 码 to any signature scheme (including GenEG_S scheme).
 cri

crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאת מאהוד קריפטוגרפיה criptografia ծածկագիտություն kryptografia
 շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen кримтаграфия การฉานรหัส kriptografija
 رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאת מאהוד קריפטוגרפיה criptografia
 ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримтаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码 kriptografi cifrado מאת מאהוד קריפטוגרפיה
 criptografia ծածկագիտություն kryptografia շրժժեղանգոօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримтаграфия การฉานรหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál criptagrafaiochta 密码

kriptografīju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפת מלל học криптография criptografia
 ծածկագիտություն kryptografia շրժժեղացում kriptografiya κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografīju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפת מלל học
 криптография criptografia ծածկագիտություն kryptografia շրժժեղացում kriptografiya κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोगाफी salauksen кримптография การเข้ารหัส kriptografija رمز نویسی kriptografīju 암호화 crittografia dumlál cripteagrafaiochta 密

GenEG^V scheme

Parameter:

- t – number of truncated bits.

Signature size is reduced by t bits.

It's possible to cut either r or s component. The method can be applied to any signature scheme (including GenEG_S scheme).

kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה mât mã học крпптографія criptografia
 ծածկագիտություն kryptografia շրժձժեղճաջօօժ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה

mâ GenEG^v scheme

Sig(d, m)

```

1 :  $\bar{r} \parallel \bar{s} \leftarrow \text{GenEG.Sig}(d, m)$ 
2 : if  $\bar{r} \parallel \bar{s} = \perp$  : return  $\perp$ 
3 :  $\bar{s}^* \leftarrow \text{msb}_{|\bar{s}| - t}(\bar{s})$ 
4 : return  $\bar{r} \parallel \bar{s}^*$ 

```

Vf($Q, m, \bar{r} \parallel \bar{s}^*$)

```

1 :  $i \leftarrow 0$ 
2 : if  $i \geq 2^t$  : return 0
3 :  $\bar{s} \leftarrow \bar{s}^* \parallel \text{str}_t(i)$ 
4 :  $i \leftarrow i + 1$ 
5 :  $res \leftarrow \text{GenEG.Vf}(Q, m, \bar{r} \parallel \bar{s})$ 
6 : if  $res = 0$  : goto 2
7 : return 1

```

ծածկագիտություն kryptografia շրժձժեղճաջօօժ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie किप्टोबाफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado קריפטוגרפיה
 mât mã học крпптографія criptografia ծածկագիտություն kryptografia շրժձժեղճաջօօժ крпптография κρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोबाफी salauksen крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptografija 암호화 crittografia dumlál cripteagrafaiochta 密码

5 Security model

(CryptoPro LLC)

CTCrypt 2020

30 / 46

Attack: chosen message attack

критографироу сурогатну нэгдл курогтарше тусгагчиг сагааксен крыптаграфя пидатиин криптогациа رمز نویسی криптогациа шифр

1 : $(pk, sk) \leftarrow \text{SS.KGen}()$ 1 : $sgn \leftarrow \text{SS.Sig}(sk, m)$

$$2: \quad \mathcal{L} \leftarrow \emptyset \qquad \qquad \qquad 2: \quad \mathcal{L} \leftarrow \mathcal{L} \cup \{(m, \text{sgn})\}$$

3 : $(m, sgn) \xleftarrow{\$} \mathcal{A}^{Sign}(pk)$ 3 : **return** sgn

```

4 :   if  $(m, sgn) \in \mathcal{L}$  : return 0

```

5 : $res \leftarrow \text{SS.Vf}(\text{pk}, m, \text{sgn})$ 6: **return** *res*

1: (pk, sk) ← SS.KGen() 1: *sign* ← SS.Sig(sk, *m*)

$$1: (\text{pk}, \text{sk}) \leftarrow \text{SS.KGen}()$$
$$2: \quad \mathcal{L} \leftarrow \emptyset \qquad \qquad \qquad 2: \quad \mathcal{L} \leftarrow \mathcal{L} \cup \{(m, \text{sgn})\}$$

```

3 :   (m sgn) ←  $\$$  4 Sign(pk)
3 :   return sgn

```

SUF-CMA model

Attack: chosen message attack

Threat: existential forgery (strong)

[illegible]

(C) 2020, Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has determined that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

(CryptoPro LLC) C1Crypt 2020 32 / 46

$$\mathbf{Exp}_{\text{SS}}^{\text{SUF-CMA}}(\mathcal{A})$$
$$1: (\text{pk}, \text{sk}) \leftarrow \text{SS.KGen}()$$
$$2: \quad \mathcal{L} \leftarrow \emptyset$$
$$3 : \quad (m, \text{sgn}) \xleftarrow{\$} \mathcal{A}^{\text{Sign}}(\text{pk})$$
4 : **if** $(m, \text{sgn}) \in \mathcal{L}$: **return** 05 : $res \leftarrow \text{SS.Vf}(pk, m, sgn)$

```

6 :   return res

```

Oracle $Sign(m)$
$$1: \text{sgn} \leftarrow \text{SS.Sig}(\text{sk}, m)$$
$$2: \quad \mathcal{L} \leftarrow \mathcal{L} \cup \{(m, \text{sgn})\}$$

```

3 :   return  $sgn$ 

```

kriptogrāfiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מלא học крпптография criptografia
 δαδλγαηηυνηυνη kryptografia ვრბტვგვრავოლ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מלא học крпптография criptografia
 δαδλγαηηυνηυνη kryptografia ვრბტვგვრავოლ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen

Assumptions

- Elliptic curve: ECDLP problem is hard.
- Family of hash functions H_1 :
 - signum-relative collision resistant;
 - signum-relative division resistant.

Signum-relative collision resistant:

$$\text{Adv}_{H_1}^{\text{SCR}}(\mathcal{A}) = \Pr \left[(m_1, m_2) \xleftarrow{\$} \mathcal{A} : H_1(m_1) = \pm H_1(m_2) \wedge m_1 \neq m_2 \right]$$

رمز نویسی kriptogrāfiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מלא học крпптография criptografia
 δαδλγαηηυνηυνη kryptografia ვრბტვგვრავოლ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מלא học крпптография criptografia
 δαδλγαηηυνηυνη kryptografia ვრბტვგვრავოლ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen
 крпптаграфия การฉานรหัส kriptografija رمز نویسی kriptogrāfiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado מפתח מלא học крпптография criptografia
 δαδλγαηηυνηυνη kryptografia ვრბტვგვრავოლ крпптография κρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen

Assumptions

- Elliptic curve: ECDLP problem is hard.
- Family of hash functions H_1 :
 - signum-relative collision resistant;
 - signum-relative division resistant.

Signum-relative collision resistant:

$$\text{Adv}_{H_1}^{\text{SCR}}(\mathcal{A}) = \Pr \left[(m_1, m_2) \xleftarrow{\$} \mathcal{A} : H_1(m_1) = \pm H_1(m_2) \wedge m_1 \neq m_2 \right]$$

Signum-relative division resistant:

$$\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{A}) =$$

$$\Pr[\beta_1, \beta_2 \stackrel{\mathcal{U}}{\leftarrow} \{0, 1\}^b; (m_1, \Gamma) \stackrel{\$}{\leftarrow} \mathcal{A}_1(\beta_1), m_2 \stackrel{\$}{\leftarrow} \mathcal{A}_2(\Gamma, \beta_2) : \frac{H_1(m_1)}{\phi(\beta_1)} = \pm \frac{H_1(m_2)}{\phi(\beta_2)}]$$

Signum-relative division resistant:

$$\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{A}) =$$

$$\Pr[\beta_1, \beta_2 \xleftarrow{\mathcal{U}} \{0, 1\}^b; (m_1, \Gamma) \xleftarrow{\$} \mathcal{A}_1(\beta_1), m_2 \xleftarrow{\$} \mathcal{A}_2(\Gamma, \beta_2) : \frac{H_1(m_1)}{\phi(\beta_1)} = \pm \frac{H_1(m_2)}{\phi(\beta_2)}]$$

$$\left. \begin{array}{l} \text{zero resistance} \\ \text{signum-relative preimage resistance} \end{array} \right\} \Rightarrow \text{SDR-property}$$

1 Motivation

2 Related works

3 ElGamal-type signatures

криптография การเข้ารหัส kriptografija رمز نویسی kriptografiju

6 Security bounds

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) (\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}))} + \\ + \frac{Q_o + 3}{2^b} + \text{Adv}_{H_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1};$$

H_2 is modelled as random oracle.

"... attacks and security emerge as opposite sides of the same coin, and complement each other." (Bellare)

Akhmetzyanova et al. "Practical significance of security bounds for..." (CTCrypt'18)

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) \left(\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}) \right) + \frac{Q_o + 3}{2^b} + \text{Adv}_{H_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}};$$

H_2 is modelled as random oracle.

"... attacks and security emerge as opposite sides of the same coin, and complement each other." (Bellare)

Akhmetzyanova et al. "Practical significance of security bounds for..." (CTCrypt'18)

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) (\text{Adv}_{\mathcal{H}_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}))} + \\ + \frac{Q_o + 3}{2^b} + \text{Adv}_{\mathcal{H}_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1};$$

H_2 is modelled as random oracle.

"... attacks and security emerge as opposite sides of the same coin, and complement each other." (Bellare)

Akhmetzyanova et al. "Practical significance of security bounds for..." (CTCrypt'18)

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) (\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathcal{G}}^{\text{ECDLP}}(\mathcal{D}))} + \\ + \frac{Q_o + 3}{2^b} + \text{Adv}_{H_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

b – size of truncated hash output;

Q_o – number of queries to H_2 ;

Q_s – number of signatures known to adversary $\mathcal{A}$.

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) (\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}))} + \\ + \frac{Q_o + 3}{2^b} + \text{Adv}_{H_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

Attack:

- 1 fix s ;
- 2 try r :

$$R \leftarrow e^{-1}sP - e^{-1}rQ \\ \phi(H_2(R.x)) = r ?$$

Q_o – number of queries to H_2 ; 2^b – number of possible variants for r .

Two messages with same hash value

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq$$

$$\sqrt{(Q_o + 2) (\text{Adv}_{\mathcal{H}_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathcal{G}}^{\text{ECDLP}}(\mathcal{D}))} + \\ + \frac{Q_o + 3}{2^b} + \text{Adv}_{\mathcal{H}_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

$$\frac{Q_s^2}{q}: \text{collision by } k \text{ value}$$

$$\frac{Q_o Q_s}{q}: \text{probability to find } k \text{ for given signatures}$$

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq \sqrt{(Q_o + 2) (\text{Adv}_{\mathcal{H}_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathcal{G}}^{\text{ECDLP}}(\mathcal{D}))} + \frac{Q_o + 3}{2^b} + \text{Adv}_{\mathcal{H}_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

$\frac{Q_s^2}{q}$: collision by k value

$\frac{Q_o Q_s}{q}$: probability to find k for given signatures

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq \sqrt{(Q_o + 2) (\text{Adv}_{\mathcal{H}_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}))} + \frac{Q_o + 3}{2^b} + \text{Adv}_{\mathcal{H}_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

$\frac{Q_s^2}{q}$: collision by k value

$\frac{Q_o Q_s}{q}$: probability to find k for given signatures

GOST-H security

$$\text{Adv}_{\text{GOST-H}}^{\text{SUF-CMA}}(\mathcal{A}) \leq \sqrt{(Q_o + 2) (\text{Adv}_{H_1}^{\text{SDR}}(\mathcal{M}) \cdot (Q_o + 2) + \text{Adv}_{\mathbb{G}}^{\text{ECDLP}}(\mathcal{D}))} + \frac{Q_o + 3}{2^b} + \text{Adv}_{H_1}^{\text{SCR}}(\mathcal{C}) + \frac{(2Q_o + Q_s + 1)Q_s}{q - 1}.$$

Reducing b up to $\frac{\lceil \log_2 q \rceil}{2}$ does not significantly change the final bound!

ճանկալիստություն kryptografia շրժձԵղճնցոօ կրիթոգրաֆիա κρυπτογράφηση cryptography 暗号化 kryptographie கிப்தொகரி salauksen
кryptography การเข้ารหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密碼 kriptografi cifrado תיפודת קריפטוגרפיה
mật mã học крпптография criptografia ճանկալիստություն kryptografia շրժձԵղճնցոօ կրիթոգրաֆիա κρυπτογράφηση cryptography 暗号化
kryptographie கிப்தொகரி salauksen кryptography การเข้ารหัส kriptografija رمز نویسی kriptogrāfija 암호화 crittografia dumlál cripteagrafaiochta 密

GenEG_S security

$$\text{Adv}_{\text{GenEG}_S}^{\text{SUF-CMA}}(\mathcal{A}) = \text{Adv}_{\text{GenEG}}^{\text{SUF-CMA}}(\mathcal{B});$$

$$Q'_S = Q_S \cdot \text{thr}.$$

Q_S – number of $\mathcal{A}$'s queries for signatures;

Q'_S – number of signatures known to $\mathcal{B}$;

thr – number of attempts to generate valid signature.

GenEG:

Collision by k : $\frac{Q_S^2}{q}$

GenEG_S:

Collision by k : $\frac{Q_S^2 \cdot \text{thr}^2}{q} = \frac{Q_S^2 \cdot 2^{2l}}{q}$

GenEG_S security

$$\text{Adv}_{\text{GenEG}_S}^{\text{SUF-CMA}}(\mathcal{A}) = \text{Adv}_{\text{GenEG}}^{\text{SUF-CMA}}(\mathcal{B});$$

$$Q'_S = Q_S \cdot thr.$$

Q_S – number of $\mathcal{A}$'s queries for signatures;

Q'_S – number of signatures known to $\mathcal{B}$;

thr – number of attempts to generate valid signature.

GenEG:

Collision by k : $\frac{Q_S^2}{q}$

GenEG_S:

Collision by k : $\frac{Q_S^2 \cdot thr^2}{q} = \frac{Q_S^2 \cdot 2^{2l}}{q}$

GenEG_S security

$$\text{Adv}_{\text{GenEG}_S}^{\text{SUF-CMA}}(\mathcal{A}) = \text{Adv}_{\text{GenEG}}^{\text{SUF-CMA}}(\mathcal{B});$$

$$Q'_S = Q_S \cdot thr.$$

Q_S – number of $\mathcal{A}$'s queries for signatures;

Q'_S – number of signatures known to $\mathcal{B}$;

thr – number of attempts to generate valid signature.

GenEG:

Collision by k : $\frac{Q_S^2}{q}$

GenEG_S:

Collision by k : $\frac{Q_S^2 \cdot thr^2}{q} = \frac{Q_S^2 \cdot 2^{2l}}{q}$

GenEG^V security

$$\text{Adv}_{\text{GenEG}^V}^{\text{SUF-CMA}}(\mathcal{A}) = \text{Adv}_{\text{GenEG}}^{\text{SUF-CMA}}(\mathcal{B});$$

$$T_{\mathcal{B}} = T_{\mathcal{A}} + c \cdot 2^t \cdot T_{\text{GenEG}}^V.$$

t – size of truncated part of the signature;

T_{GenEG}^V – computational resources needed to verify one signature by the GenEG.Vf procedure.

Attack for large t value:

- fix r ;
- try random s .

GenEG^V security

$$\text{Adv}_{\text{GenEG}^V}^{\text{SUF-CMA}}(\mathcal{A}) = \text{Adv}_{\text{GenEG}}^{\text{SUF-CMA}}(\mathcal{B});$$

$$T_{\mathcal{B}} = T_{\mathcal{A}} + c \cdot 2^t \cdot T_{\text{GenEG}}^V.$$

t – size of truncated part of the signature;

T_{GenEG}^V – computational resources needed to verify one signature by the GenEG.Vf procedure.

Attack for large t value:

- fix r ;
- try random s .

1 Motivation

ptographie किण्टोग्राफी salauksen kp

رمز نویی kriptogrāfiju 암호화 crittografia dulmál cripteagrafaio

4 Three methods of shortening

5 Security model

კოდებიდან კრიპტოგრაფია კρυπτογράφηση cryptography 暗号化 kryptographie क्रिप्टोग्राफी salauksen kryptografia การเข้ารหัส kriptografija

GOST- H_S^V scheme

We apply all three methods to GOST scheme with q , $2^{255} < q < 2^{256}$:

- $b = 100$;
- $l = 18, thr = 2^{18}$;
- $t = 18$.

Signature size: 320 bits

Security level: 2^{-35}

Signature generation time: ≈ 6 seconds;

Signature verification time: ≈ 3 seconds.

GOST- H_S^V scheme

We apply all three methods to GOST scheme with q , $2^{255} < q < 2^{256}$:

- $b = 100$;
- $l = 18, thr = 2^{18}$;
- $t = 18$.

Signature size: 320 bits

Security level: 2^{-35}

Signature generation time: ≈ 6 seconds;

Signature verification time: ≈ 3 seconds.

GOST- H_S^V scheme

We apply all three methods to GOST scheme with q , $2^{255} < q < 2^{256}$:

- $b = 100$;
- $l = 18, thr = 2^{18}$;
- $t = 18$.

Signature size: 320 bits

Security level: 2^{-35}

Signature generation time: ≈ 6 seconds;

Signature verification time: ≈ 3 seconds.

GOST- H_S^V scheme

We apply all three methods to GOST scheme with q , $2^{255} < q < 2^{256}$:

- $b = 100$;
- $l = 18, thr = 2^{18}$;
- $t = 18$.

Signature size: 320 bits

Security level: 2^{-35}

Signature generation time: ≈ 6 seconds;

Signature verification time: ≈ 3 seconds.

kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּיִפּוּט מַתְמָטִיקָה криптография criptografia
 ծածկագիտություն kryptografia շրժձժեղճոցօօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּיִפּוּט מַתְמָטִיקָה
 mat mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժձժեղճոցօօս криптография кρυπτογράφηση cryptography 暗号化

Thank you for your attention!

Questions?

Questions, comments:

- alekseev@cryptopro.ru
- babueva@cryptopro.ru
- lah@cryptopro.ru
- svs@cryptopro.ru

շրժձժեղճոցօօս կրիպտօգրաֆիա кримптография кρυπτογράφηση תַּיִפּוּט מַתְמָטִיקָה salauksen кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּיִפּוּט מַתְמָטִיקָה
 mat mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժձժեղճոցօօս криптография кρυπτογράφηση cryptography 暗号化 kryptographie किप्टोगाफी salauksen
 кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码 kriptografi cifrado תַּיִפּוּט מַתְמָטִיקָה
 mat mǎ hoc криптография criptografia ծածկագիտություն kryptografia շրժձժեղճոցօօս криптография кρυπτογράφηση cryptography 暗号化
 kryptographie किप्टोगाफी salauksen кримптография การเข้ารหัส kriptografija رمز نویسی kriptografiju 암호화 crittografia dumlál cripteagrafaiochta 密码