С. В. Запечников (к. т. н., доцент)
Московский инженерно-физический институт (государственный университет)

ОБЕСПЕЧЕНИЕ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ ПРИ КОМПРОМЕТАЦИИ ЧАСТИ КЛЮЧЕЙ

Изложены теоретические положения, задающие систему показателей и критериев обеспечения секретности ключей криптосистем. Приведены доказанные утверждения и теоремы о структуре ключевой системы, обеспечивающей выполнение требований секретности. Обсуждаются пути реализации условий секретности ключевого материала в криптографических конструкциях, приводится пример — одна из пороговых схем цифровой подписи на базе ГОСТ Р 34.10–2001.

Введение

Один из базовых принципов современной криптографии заключается в том, что стойкость систем криптографической защиты информации (СКЗИ) целиком основывается на предположении о безопасности используемых в них ключей. Криптоанализ требует от противника значительных вычислительных, временных и финансовых затрат. Похищение ключевого материала криптосистем или преднамеренное воздействие на него может быть значительно проще, а по эффективности сравнимо с криптоанализом. Так, раскрытие противником секретных ключей криптосистемы может повлечь за собой как несанкционированный доступ к информационным ресурсам, так и несанкционированное применение системных функций.

Обобщающий термин «*разрушение ключевого материала*» будем использовать для обозначения утраты одного или более свойств, которыми характеризуется безопасность ключевого материала: доступности, аутентичности и (или) секретности.

Исследование проблем криптографической стойкости СКЗИ в условиях частичного разрушения ключевых систем (КС) должно опираться на некоторую инструментально-методическую базу. С этой целью строится математическая модель КС СКЗИ, позволяющая описывать ее статическую структуру и динамику поведения. Основные элементы этой модели представлены автором в работе [1], более подробное изложение подхода к модельному представлению КС можно найти в статье [2], публикуемой в этом же номере журнала. Далее для элементов КС используются введенные там обозначения.

1. Показатели секретности ключевого материала

Для исследования проблем стойкости СКЗИ к разрушению части ключевого материала необходимо ввести меру безопасности ключевого материала и уметь получать количественные оценки безопасности. В связи с невозможностью достоверно распознавать причины, ведущие к утрате безопасности ключей, примем предположение о том, что она всегда происходит из-за деятельности противника. В статье [1] приведена общая характеристика системы количественных показателей безопасности КС. В настоящей работе более подробно рассматриваются показатели, характеризующие секретность ключевого материала.

Секретность компонента ОКС $Com_j \in Obj_i$ на непрерывном временном интервале λ определим как свойство компонента Com_j, заключающееся в том, что его значение в произвольный момент времени τ в границах временного интервала λ известно только владельцам ОКС $Own(Obj_i)$ и неизвестно никому более.

Нарушение секретности на одном временном интервале приводит к тому, что противнику становится известна часть секретного ключевого материала. Таким образом, количество ключевого материала, пригодного для восстановления секретности, с каждым временным интервалом может только сокращаться. Поэтому при анализе секретности необходим учет взаимосвязей между секретностью ключевого материала на разных временных интервалах.

Предположим, противник может нарушать секретность отдельных компонентов ОКС, т. е. ключи могут быть скомпрометированы, что не обнаруживается системными средствами СКЗИ, так как секретность не является объективно фиксируемой величиной. Поэтому особенность анализа показателей секретности состоит в том, что, хотя вероятность утраты секретности зависит от длины временных интервалов, на которых ключ принимает определенные значения, но независимо от времени наступления этого события утрата секретности происходит на всем рассматриваемом интервале. Противник самостоятельно выбирает стратегию компрометации экземпляров ОКС. Пусть Φ_1 — подмножество ОКС, заблокированных противником, Φ_2 — подмножество ОКС, аутентичность которых нарушена противником, X — подмножество открытых общедоступных компонентов ОКС. Обозначим $\Phi = \Phi_1 \cup \Phi_2$. Противник способен выполнять любые полиномиальные алгоритмы и имеет доступ к оракулам, реализующим применяемые в СКЗИ алгоритмы симметричного и открытого шифрования. Понятие оракула совпадает с общепринятым в учебной литературе по криптографии [3].

Вероятность успеха противника, т. е. вероятность того, что противнику в некоторый момент времени τ в течение временного интервала λ станет известно значение $Com_j \notin \Phi \setminus X$, обозначим $\gamma(Com_j, \lambda)$, считая, что она постоянна на данном временном интервале. Если эта вероятность зависит от времени, то в качестве $\gamma(Com_j, \lambda)$ примем ее максимальное значение на интервале λ. Формулы для оценки значений $\gamma(Com_j, \lambda)$ задаются следующими доказанными утверждениями (приводятся здесь без доказательства).

Если в КС имеется n экземпляров ОКС Obj_i, то для нарушения секретности достаточно, чтобы противник получил доступ хотя бы к одному экземпляру ОКС, т. е.

$$p_{ПДК}\left(Com_j\right) = p_{ПДК}\left(Com_j^{(n)}\right) = 1 - \prod_{(i)} \left(1 - p_{ПДК}^{(i)}\left(Com_j\right) \cdot p_{обх}^{(i)}\left(Com_j\right)\right) \qquad (1)$$

Где $\rho^{(i)}_{ПДК}$ — вероятность прямого доступа к i-му экземпляру ОКС, $\rho^{(i)}_{обх}$ — вероятность «обхода» противником механизма аутентификации.

Вероятность успеха противника при осуществлении одного из видов атак на КС определяется видом атаки. Вероятность случайного угадывания оценивается соотношением:

$$1/\left|E\left(Com_j\right)\right| \geq p_1\left(Com_j\right) \geq 1/\left|D\left(Com_j\right)\right| \geq 1/2^x, \qquad (2)$$

Где $D(Com_j) \subseteq \{0,1\}^x$ — множество допустимых значений Com_j, $E(Com_j)$ — множество значений, образующих составленный противником словарь.

Утверждение 1.

$$P\left(Com_0 \middle| Com_{j_1}, ..., Com_{j_q}\right) \leq 1 - \prod_{s=1}^{|\Omega[Com_0]|} \left(1 - p_s^{\Omega}\right),$$

где ρ_i^{Ω} — вероятность получения противником значений всех элементов i-го минимального множества вычислимости (ММВ).

Следствие. Вероятность утраты секретности компонента Com_0 снижается при замене его совокупностью компонентов $Com_{j_1}, ..., Com_{j_q}$ тогда и только тогда, когда

$$\prod_{s=1}^{|\omega_j|} \left(1 - \gamma\left(Com_{j_s}\right)\right) \geq 1 - \gamma\left(Com_0\right) \text{ для } \forall j, \text{ такого, что } \omega_j \in \Omega[Com_0].$$

Таким образом, вероятность восстановления компонента ОКС из функционально зависимых компонентов ОКС равна:

$$p_2\left(Com_j, \lambda_\tau\right) = 1 - \prod_{i=1}^{|\Omega[Com_j(\lambda_\tau)]|} \left(1 - \prod_{s=1}^{|\omega_i(Com_j(\lambda_\tau))|} \gamma\left(Com_s\left(\lambda_\tau\right)\right)\right) \qquad (3)$$

Утверждение 2.

$$P\left(Com_j(\lambda_\tau)\middle|Com_j(\lambda_{i_1}),...,Com_j(\lambda_{i_q})\right)\le 1-\prod_{s=1}^{|\Theta[Com_0]|}\left(1-p_s^{\Theta}\right),$$

где ρ_i^{Θ} — вероятность получения противником значений всех элементов i-й минимальной последовательности вычислимости (МПВ).

Следствие. Вероятность утраты секретности компонента $Com_j(\lambda_\tau)$ снижается при замене его совокупностью компонентов $Com_j(\lambda_{i_1}),...,Com_j(\lambda_{i_q})$ тогда и только тогда, когда

$$\prod_{s=1}^{|\theta_j|}\left(1-\gamma\left(Com_{j_s}\right)\right)\ge 1-\gamma\left(Com_0\right)$$ для $\forall j$, такого, что $\theta_j\in\Theta[Com_0]$.

Таким образом, вероятность восстановления компонента ОКС из последовательности изменяющихся во времени значений компонента ОКС равна:

$$p_3\left(Com_j,\lambda_\tau\right)=1-\prod_{i=1}^{|\Theta[Com_j(\lambda_\tau)]|}\left(1-\prod_{s=1}^{|\theta_i(Com_j(\lambda_\tau))|}\gamma\left(Com_j(\lambda_{i_s})\right)\right) \quad (4)$$

Утверждение 3.

$$\rho(Com_0\ (\lambda_\tau)|\ Com_{j1,i1}\ (\lambda_{i1}),\dots,\ Com_{jq,i1}(\lambda_{i1}),\dots,\ Com_{j1,i\rho}\ (\lambda_{i\rho}),\dots,\ Com_{jq,i\rho}\ (\lambda_{i\rho}))\le$$

$$\le 1-\prod_{r=1}^{|\Omega[Com_j(\lambda_\tau)]|}\left(1-p_{r,\tau}^{\Omega}\right)\cdot\prod_{s=1}^{|\Theta[Com_j(\lambda_\tau)]|}\left(1-p_{s,\tau}^{\Theta}\right),$$

где $\rho_{r,u}^{\Omega}$ — вероятность получения противником значений всех элементов r-го ММВ на временном интервале λ_u, $\rho_{s,v}^{\Theta}$ — вероятность получения противником значений всех элементов s-й МПВ на временном интервале λ_v.

Таким образом, вероятность восстановление компонента ОКС из последовательности изменяющихся во времени значений функционально зависимых компонентов ОКС равна:

$$p_4\left(Com_j,\lambda_\tau\right)=1-\prod_{r=1}^{|\Omega[Com_j(\lambda_\tau)]|}\left(1-\prod_{\omega\in\Omega[Com_j(\lambda_\tau)]}\prod_{\substack{u=1\\u\ne\tau}}^{|\theta(Com_\omega(\lambda_\tau))|}\gamma\left(Com_\omega,\lambda_u\right)\right)\times \quad (5)$$

$$\times\prod_{s=1}^{|\Theta[Com_j(\lambda_\tau)]|}\left(1-\prod_{\theta\in\Theta[Com_j(\lambda_\tau)]}\prod_{\substack{v=1\\v\ne j}}^{|\omega(Com_j(\lambda_\theta))|}\gamma\left(Com_v,\lambda_\theta\right)\right)$$

Лемма 1. Вероятность того, что компонент ОКС $Com_j\in Obj_i$ утратил секретность в произвольный момент времени τ в границах временного интервала λ, равна:

$$\gamma\left(Com_j,\lambda_\tau\right)=1-\left(1-p_{ПДК}\left(Com_j\right)\right)\cdot\prod_i\left(1-p_i\left(Com_j,\lambda_\tau\right)\cdot p_{НСП}\left(Com_j\right)\right), \quad (6)$$

где $\rho_{ПДК}$ определяется уравнением (1), ρ_i, $i=\overline{1,4}$ — уравнениями (2) — (5) соответственно.

Следствие. Вероятность того, что $Com_j\in Obj_i$ утратил секретность в фиксированный момент времени τ, приходящийся на некоторый временной интервал из непрерывной последовательности $\Lambda=<\lambda_1,\ \lambda_2,\dots,\ \lambda_m>$, равна:

$$\gamma\left(Com_j,\Lambda\right)=1-\prod_{s=1}^{m}\left(1-\gamma\left(Com_j,\lambda_s\right)\right) \quad (7)$$

2. Критерии секретности ключевого материала

Теорема 1. *(Критерий секретности ключевого материала на одном временном интервале.)* Пусть $Com_j \in Obj_i$ и пусть $\{\Psi_1, \Psi_2, \ldots, \Psi_\tau, \ldots, \Psi_m\}$ — множества компонентов ОКС, значения которых на временных интервалах, образующих непрерывную последовательность $\Lambda = <\lambda_1, \lambda_2, \ldots, \lambda_\tau, \ldots, \lambda_m>$, известны противнику. Если из множества известных противнику компонентов ОКС невозможно сформировать ни одного ММВ и ни одной МПВ, т. е.

$$\left(\nexists\omega\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_\tau\right)\vee\left(\nexists\theta\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_1\times\Psi_2\times\ldots\times\Psi_m\right)\vee$$

$$\vee\left(\nexists\omega\left(Com_r(\lambda_i)\right)\subseteq\Psi_i, i=i_1,i_2,\ldots,i_m:\left\{Com_r(\lambda_{i_1}),\ldots,Com_r(\lambda_{i_m})\right\}=\theta\left(Com_j(\lambda_\tau)\right), r\neq j\right)\vee$$

$$\vee\left(\nexists\theta\left(Com_s(\lambda_\tau)\right)\subseteq\Psi_{i_1}\times\ldots\times\Psi_{i_m}, s=s_1,,s_k:\left\{Com_{s_1}(\lambda_\tau),\ldots,Com_{s_k}(\lambda_\tau)\right\}=\omega\left(Com_j(\lambda_\tau)\right), s_1\neq\ldots\neq s_k\neq j\right),$$

то вероятность утраты секретности Com_j на произвольно выделенном из последовательности Λ интервале λ_τ не превосходит величины $P(Com_j(\lambda_\tau)|\{\Psi_1, \Psi_2, \ldots, \Psi_m\})\leq\gamma(Com_j,\lambda_\tau)$.

Если же хотя бы одно из этих условий не выполнено, то $P(Com_j(\lambda_\tau)|\{\Psi_1, \Psi_2, \ldots, \Psi_m\})=1$, и $Com_j(\lambda_\tau)\in\Psi_\tau$.

Теорема 2. *(Критерий секретности ключевого материала на непрерывной последовательности временных интервалов.)* Пусть $Com_j \in Obj_i$ и пусть $\{\Psi_1, \Psi_2, \ldots, \Psi_m\}$— множества компонентов ОКС, значения которых на временных интервалах, образующих непрерывную последовательность $\Lambda = <\lambda_1, \lambda_2, \ldots, \lambda_m>$, известны противнику. Если из множества известных противнику компонентов ОКС никаким способом невозможно сформировать ни одного ММВ и ни одной МПВ, т. е. для $\forall\lambda_\tau\in\Lambda$

$$\left(\nexists\omega\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_\tau\right)\vee\left(\nexists\theta\left(Com_j(\lambda_\tau)\right)\subseteq\Psi_1\times\Psi_2\times\ldots\times\Psi_m\right)\vee$$

$$\vee\left(\nexists\omega\left(Com_r(\lambda_i)\right)\subseteq\Psi_i, i=\overline{1,m}:\left\{Com_r(\lambda_1),\ldots,Com_r(\lambda_m)\right\}=\theta\left(Com_j(\lambda_\tau)\right), r\neq j\right)\vee$$

$$\vee\left(\nexists\theta\left(Com_s(\lambda_\tau)\right)\subseteq\Psi_1\times\ldots\times\Psi_m, s=s_1,,s_k:\left\{Com_{s_1}(\lambda_\tau),\ldots,Com_{s_k}(\lambda_\tau)\right\}=\omega\left(Com_j(\lambda_\tau)\right), s_1\neq\ldots\neq s_k\neq j\right),$$

то вероятность утраты секретности Com_j на непрерывной последовательности интервалов Λ для $\forall\lambda_\tau\in\Lambda$ не превосходит величины

$$P\left(Com_j(\lambda_\tau)\middle|\left\{\Psi_1,\Psi_2,\ldots,\Psi_m\right\}\right)\leq 1-\prod_{\lambda_i\in\Lambda}\left(1-\gamma\left(Com_j,\lambda_i\right)\right).$$

Секретность ОКС Obj_i на непрерывном временном интервале λ определим как свойство ОКС, заключающееся в том, что $\forall Com_j \in Obj_i$, для которого требуется обеспечение секретности, остается секретным в любой момент времени τ, приходящийся на временной интервал λ.

Обозначим $\gamma(Obj_i, \lambda)$ — вероятность того, что хотя бы один компонент Com_j, требующий обеспечения секретности, т. е. принадлежащий полям B,C ОКС, утратил секретность в некоторый момент времени τ в границах временного интервала λ. Если компрометация этих компонентов происходила независимо, то

$$\gamma\left(Obj_i,\lambda\right)=1-\prod_{Com_j\in Obj_i.B\cup C}\left(1-\gamma\left(Com_j,\lambda\right)\right) \tag{8}$$

Вероятность того, что хотя бы один компонент $Com_j \in B\cup C$ утратил секретность в фиксированный момент времени τ, приходящийся на некоторый временной интервал из непрерывной $\Lambda = <\lambda_1, \lambda_2, \ldots, \lambda_m>$, при независимых компрометациях равна:

$$\gamma\left(Obj_i,\Lambda\right)=1-\prod_{Com_j\in Obj_i.B\cup C}\left(1-\lambda\left(Com_j,\Lambda\right)\right). \tag{9}$$

Однако компрометации $Com_j \in B\cup C$ могут быть и зависимыми событиями — тогда эти формулы неприменимы, и расчет вероятностей утраты секретности нужно проводить исходя из конфигурации графа G_{Obj_i}.

Вследствие малости абсолютных величин γ для качественных механизмов обеспечения секретности экспериментальное определение γ затруднено, поэтому при расчетах следует пользоваться аналитическими выражениями.

3. Структура КС, обеспечивающая секретность ключевого материала

Требования секретности ключевого материала, выраженные через систему показателей, накладывают определенные ограничения на структуру КС.

Сформулируем сначала необходимые для дальнейшего анализа свойств КС утверждения, касающиеся отношений между компонентами ОКС внутри отдельных ОКС.

Утверждение 4. Пусть $Com_{i_1} \in Obj_i$, $Com_{i_2} \in Obj_i$. $Com_{i_1} \in \omega(Com_{i_2})$ тогда и только тогда, когда в орграфе G_{Obji} существует путь из вершины Com_{j1} в вершину Com_{i_2} длины ≥1.

Утверждение 5. Пусть $Com_{i_1} \in Obj_{i_1}$, $Com_{i_2} \in Obj_{i_2}$, $i_2 \neq i_1$. $Com_{i_1} \in \omega(Com_{i_2})$ тогда и только тогда, когда в орграфе G существует путь из вершины Obj_{i_1} в вершину Obj_{i_2} длины ≥1.

Утверждение 6. Если $Obj_{i_1} \succ Obj_{i_2}$, то для некоторого $Com_{i_2} \in Obj_{i_2}$, $Com_{i_1} \in Obj_{i_1}$, такой, что $Com_{i_1} \in \omega'(Com_{i_2})$, для которого $\{\omega'(Com_{i_2}) \setminus Com_{i_1}\} \cup \omega'(Com_{j1}) \in \Omega\lfloor(Com_{i_2})\rfloor$.

Утверждение 7. Если в орграфе существует путь, начинающийся из Com_{i_1}, принадлежащего полю D, E либо F, и заканчивающийся в Com_{i_2}, принадлежащем полю B либо C, то Com_{i_2} не может быть вычислен за полиномиальное время из открытых компонентов до тех пор, пока для $\forall\omega(Com_{i_2})$: $Com_{i_1} \in \omega(Com_{i_2})$ неизвестен хотя бы один элемент этого ММВ. Если в орграфе таких путей не существует, то Com_{i_2} не может быть вычислен за полиномиальное время из открытых компонентов Obj_i ни при каких условиях.

Используя утверждения 4–7, удается доказать следующие леммы и теорему, касающиеся отношений между ОКС, входящими в состав КС.

Лемма 2. Если $\exists Com_{i_1} \in Obj_{i_1}$, $\exists Com_{i_2} \in Obj_{i_2}$, такие, что для $\forall\omega(Com_{i_1})$, для которого $Com_{i_2} \in \omega(Com_{i_1})$, имеет место: $\omega(Com_{i_1}) \subseteq \omega(Com_{i2})$, то $\gamma(Obj_{i_2},\lambda) \geq \gamma(Obj_{i1},\lambda)$ при условии, что $\rho_{НСП}(Com_{i_1}) = \rho_{НСП}(Com_{i_2})$ и $\rho_{ПДК}(Com_{i_1}) = \rho_{ПДК}(Com_{i_2})$ для $\forall Com_{i_1} \in Obj_{i1}$, $\forall Com_{i_2} \in Obj_{i_2}$.

Отношения зависимости и зависимости во времени между ОКС [1, 2], обладают свойствами рефлексивности и транзитивности. Потребуем дополнительно, чтобы эти отношения обладали свойством антисимметричности, т. е. чтобы из и следовало, что $Obj_{i_1} = Obj_{i_2}$. Для этого достаточно, чтобы описывающий КС граф G не имел циклов. Тогда множество ОКС образует частично упорядоченное множество с отношением зависимости или зависимости во времени соответственно. Наибольшим элементом частично упорядоченного множества объектов ключевой системы KS называется элемент $Obj_R \in KS$, такой, что $Obj_R \succ Obj_i$ для $\forall Obj_i \in KS$. Далее будем рассматривать только такие КС, которые представляют собой частично упорядоченное множество ОКС с единственным наибольшим элементом. Вершину графа, соответствующую наибольшему элементу, обозначим Obj_R.

Уровнем вложенности ОКС Obj_i будем называть длину кратчайшего пути из Obj_R в Obj_i в орграфе G. Если Obj_i имеет уровень вложенности m, будем обозначать его $\underset{(m)}{Obj_i}$.

Лемма 3. Если ОКС ключевой системы (подсистемы) KS образуют частично упорядоченное множество с единственным наибольшим элементом и отношением зависимости, то

$$\gamma(KS,\lambda) = R + (1-R)\cdot\sum_{k=1}^{M}\left(\prod_{n=1}^{M-1}\Delta_n\cdot(1-\Delta_M)\right), \quad (10)$$

где

$$\Delta_k = \prod_{i_k}\left(1-\delta_k\left(\underset{(k)}{Obj_{k,i_k}},\lambda\right)\right),$$

$$\delta_k\left(\underset{(k)}{Obj_{k,i_k}},\lambda\right) = \gamma(Obj_{k,i_k},\lambda) - \sum_{l=1}^{k-1}\sum_{\underset{(l-1)}{Obj_{l-1,i_{l-1}}}\succ\underset{(l)}{Obj_{l,i_l}}}\gamma(Obj_{l-1,i_{l-1}},\lambda) - \gamma(Obj_R,\lambda),$$

$R=\gamma(Obj_R, \lambda)$, а $\gamma(Obj_i, \lambda)$ определяется уравнениями (8) и (6), в которых для $\forall Com_j \in Obj_i$ $p_{ПДК}(Com_j) = \max_{Com_j \in KS} p_{ПДК}(Com_j)$, $p_{НСП}(Com_j) = \max_{Com_j \in KS} p_{НСП}(Com_j)$.

Следствие 1. При прочих равных условиях вероятность компрометации ОКС не убывает с увеличением уровня вложенности ОКС.

Следствие 2. Отношения зависимости между ОКС показывают пути распространения компрометаций ключевого материала.

Теорема 3. Если ОКС ключевой системы KS образуют частично упорядоченное множество с единственным наибольшим элементом и отношением зависимости во времени, то

$$\gamma(KS, \Lambda) = 1 - \prod_{i=1}^{m}(1 - \gamma(KS, \lambda_i)) \cdot \prod_{Obj_i \in KS}\left(\prod_{\theta \in \Theta[Obj_i, Com_j]}\left(1 - \prod_{Com_j(\lambda_k) \in \theta(Com_j)} \gamma(Com_j, \lambda_k)\right)\right),$$

где $\gamma(KS, \lambda)$ определяется уравнением (10), $\gamma(Obj_i, \lambda)$ — уравнениями (9) и (7), в которых для $\forall Com_j \in Obj_i$ $p_{ПДК}(Com_j) = \max_{Com_j \in KS} p_{ПДК}(Com_j)$, $p_{НСП}(Com_j) = \max_{Com_j \in KS} p_{НСП}(Com_j)$, а $\gamma(Com_j, \lambda)$ — уравнением (6).

Следствие 1. Чем меньше для некоторого $Com_j \in Obj_i$ мощность подмножества ММВ или МПВ, ко всем элементам которых противник может получить несанкционированный доступ одновременно, тем ниже вероятность компрометации Com_j.

Следствие 2. Параметрическая зависимость между ОКС ключевой системы определяет абсолютные значения показателей секретности γ, а функциональная зависимость — относительные значения этих показателей.

4. Криптографические схемы, реализующие условия секретности ключевого материала

Условия теорем 1 — 3 могут быть выполнены на практике, если синтезирована соответствующая структура КС, а требуемые значения показателей секретности — при условии, если применены специальные схемы управления ключевым материалом (СУКМ).

Анализируя известные из литературы криптографические конструкции, можно выделить по меньшей мере восемь типовых СУКМ для построения криптосхем: 1) простое резервирование ключевого материала; 2) пороговая схема разделения секрета (СРС); 3) СРС с произвольной структурой доступа; 4) СРС, функционирующая в модели «активной безопасности»; 5) схема дистанционного управления ключами; 6) схема эволюции ключей, обеспечивающая совершенную опережающую безопасность (perfect forward security); 7) схема эволюции ключей с изоляцией ключа (key-insulated cryptosystem); 8) схема эволюции ключей с базой, устойчивая к вторжению (intrusion-resilient cryptosystem). Каждую из них можно описать формально в терминах модели [2].

В частности, для реализации протоколов, обеспечивающих стойкость криптосистем в условиях компрометации части КС, удобно выбирать СУКМ, реализующие пороговые СРС. Можно показать, что, используя всего три криптосхемы на основе этой СУКМ — пороговую схему электронной цифровой подписи (ЭЦП), пороговую схему открытого шифрования, пороговую схему вычисления псевдослучайных функций (ПСФ) — можно реализовать большинство наиболее востребованных функций СКЗИ, придав им свойство стойкости к компрометации части ключей. К таким функциям относятся, например, следующие: удостоверение открытых ключей в криптосистемах с инфраструктурой открытых ключей и сопутствующие с этим услуги — функции Удостоверяющего центра, генерация секретных ключей в идентификационных и бессертификатных криптосистемах — функции Центра генерации ключей, трансляция и распределение секретных ключей, нотариальное заверение сообщений, организация сетевой системы защищенного хранения данных и многое др. Таким образом, дальнейшая задача сводится к разработке перечисленных пороговых криптосхем.

Одна из возможных конструкций для пороговых схем вычисления ПСФ предложена автором ранее [4]. В связи с отсутствием российских стандартов на схемы открытого шифрования для реализации

пороговых схем открытого шифрования можно взять любую соответствующую схему, известную из зарубежной литературы: так, хорошим выбором представляются схемы [5—7]. Однако для пороговых схем ЭЦП необходимо обеспечить соответствие российским стандартам. Впервые пороговая схема ЭЦП для действовавшей в то время редакции стандарта на ЭЦП — ГОСТ Р 34.10—94 была предложена в работе [8]. С появлением новой редакции стандарта — ГОСТ Р 34.10—2001 [9] стала актуальной задача создания соответствующих ей пороговых схем ЭЦП. Ранее такие попытки предпринимались другими исследователями [10], однако предложенная в этой работе конструкция представляется не вполне корректной, и в ней отсутствуют доказательства стойкости схемы. В [11] описана пороговая схема ЭЦП на базе [9], основанная на аппарате парных отображений, но она предназначена для идентификационных криптосистем, и процедура проверки подписи в ней отличается от принятой в [9]. В связи с этим остается актуальной задача разработки пороговых схем ЭЦП для математического аппарата эллиптических кривых, полностью соответствующих процедуре проверки подписи [9], с сохранением ранее принятого подхода к доказательству стойкости [8].

С целью решения этой задачи автором разработаны три схемы (рис. 1), различающиеся предположениями о противнике, по отношению к которому достигается стойкость: противник может быть пассивным, активным статическим либо активным адаптивным.

Рис. 1. Структура пороговых схем ЭЦП на основе ГОСТ Р 34.10—2001

В качестве примера рассмотрим схему, стойкую к атакам пассивного противника.

Выработка долговременных параметров схемы ЭЦП выполняется либо доверенной третьей стороной, либо всеми участниками совместно. В соответствии с [9, §5.2] должны быть выбраны

следующие параметры схемы: модуль эллиптической кривой — простое число $p > 2^{256}$, эллиптическая кривая E над конечным полем Φ_p, задаваемая инвариантом $J(E)$ или коэффициентами $a,b \in \Phi_p$, порядок циклической подгруппы группы G_E точек эллиптической кривой — простое число q, точка $P \neq O$ эллиптической кривой с координатами (x_p, y_p), удовлетворяющая равенству $qP = O$. Все параметры должны удовлетворять условиям и ограничениям, оговоренным в [9].

Протокол генерации ключей ЭЦП и *протокол генерации ЭЦП* для пороговой схемы ЭЦП приведены в табл. 1.

Таблица 1. Протоколы пороговой схемы ЭЦП на основе ГОСТ Р 34.10–2001, стойкой к атакам пассивного противника.

№	Наименование шага протокола	Описание шага протокола	
Пороговый протокол генерации ключей ЭЦП «Thresh-Key-Gen-1»: (p,q,m,E,P,t) → ((d$_1$,...,d$_n$),Q)			
1	Генерация долей секретного ключа ЭЦП $d_1,\ldots, d_n$ и открытого ключа ЭЦП Q	Все узлы S_i, $i=\overline{1,n}$ выполняют *протокол совместного разделения случайного секрета на основе СРС Фельдмана.* Генерируются доли секрета $(d_1,...,d_n) \xleftarrow{(t,n)} d \bmod q$. В результате $\forall S_i$, $i=\overline{1,n}$ получает свою секретную долю d_i общего секрета d, проверочные данные $\{A_l\}$, $l=\overline{0,t}$ и вырабатывается общедоступная точка эллиптической кривой $Q = dP$. Число d принимается в качестве секретного, а набор (P,Q,q) – в качестве открытого ключа схемы ЭЦП соответственно. G – множество участников, корректно завершивших протокол.	
Пороговый протокол генерации ЭЦП «Thresh-Sig-1»: (p,q,m,E,t,(d$_1$,…,d$_n$),M) → (r,s)			
1	Генерация долей разового секретного ключа ЭЦП $k_1,\ldots,k_n$	Все узлы $S_i \in G$ выполняют *протокол совместного разделения случайного секрета на основе СРС Шамира*. Генерируются доли секрета $(k_1,...,k_n) \xleftarrow{(t,n)} k \bmod q$. В результате $\forall S_i, i=\overline{1,n}$ получает свою секретную долю k_i общего секрета k.	
2	Вычисление $r = x_C \bmod q$, где x_C – x-координата точки $C=kP$	2.1	Каждый $S_i \in G$ вычисляет $C_i=k_iP$ и рассылает всем остальным узлам сообщение: $S_i \to S_j$, $j=\overline{1,n}$, $j \neq i$: $[C_i]$ и принимает C_j от других узлов.
		2.2	Каждый $S_i \in G$ выполняет локально интерполяцию точки эллиптической кривой: $C=(x_C,y_C)=$Interpolate_ECPoint$(C_{i_1},...,C_{i_{t+1}})$.
		2.3	Каждый $S_i \in G$ вычисляет локально $r = x_C \bmod q$.
3	Генерация случайных полиномов с нулевым свободным членом	Все узлы $S_i \in G$ выполняют *протокол совместного «разделения нуля» на основе СРС Шамира*. Генерируются доли секрета $(c_1,...,c_n) \xleftarrow{(t,n)} 0 \bmod q$. В результате $\forall S_i$, $i=\overline{1,n}$ получает свою секретную долю c_i, такую, что общий «секрет» $c = 0$.	
4	Вычисление $e=h(M)$	Каждый $S_i \in G$ вычисляет локально *хэш-код сообщения* $e=h(M)$ по *алгоритму из стандарта ГОСТ Р 34.11–94*. Если $e \bmod q \equiv 0$, полагает $e=0^{255}1$.	
5	Вычисление $s = (rd + ke) \bmod q$	5.1	Каждый $S_i \in G$ вычисляет локально) $s_i = (rd_i+k_ie+c_i) \bmod q$, т. е. одну из долей разделенного секрета $(s_1,...,s_n) \xleftarrow{(t,n)} (rd+ke) \bmod q$.
		5.2	Каждый $S_i \in G$ уничтожает долю разового секретного ключа k_i.
		5.3	Каждый $S_i \in G$ рассылает s_i всем остальным узлам: $S_i \to S_j, j \neq i$: $[s_i]$ и принимает s_j от других узлов.
		5.4	Каждый $S_i \in G$ выполняет локально интерполяцию по Лагранжу: $s \bmod q =$ Interpolate$(s_{i_1},...,s_{i_{t+1}})$.
		5.5	Если $s = 0$, участники возвращаются к шагу (1).
6	Выдача результата	(r, s)– подпись под сообщением M.	

Определение 1 [3]. *(Стойкость схемы ЭЦП к атакам по выбранным сообщениям.)* Пусть $DS = (K,S,V)$ — некоторая схема ЭЦП, где K — вероятностный алгоритм генерации ключей, S — вероятностный алгоритм генерации подписи, V — детерминированный алгоритм проверки подписи. Пусть $b \in \{0,1\}$. Пусть A — алгоритм противника, который имеет доступ к оракулам, реализующим алгоритмы генерации и проверки подписи. Рассмотрим следующий эксперимент противника с криптографической схемой, описанный в виде алгоритма:

Experiment $Exp_{DS,A}^{ds-frg}$:

$(pk, sk) \xleftarrow{R} K$;

$(M^*, \sigma^*) \leftarrow A^{S_{sk}(\cdot)}(pk)$;

If ($V_{pk}(M^*, \sigma^*)=1$, и сообщение M^* не подавалось ранее на вход оракула $S_{sk}(.)$) then Return 1 else Return 0.

Преимущество противника над схемой DS определяется как величина

$Adv_{DS,A}^{ds-frg} = P\left[Exp_{DS,A}^{ds-frg} = 1\right]$,

где P — вероятность того, что эксперимент вернет ответ «1».

Функция небезопасности для схемы DS определяется следующим образом:

$InSec_{DS,A}^{ds-frg}(t,q,\mu) = \max_{A}\left\{Adv_{DS,A}^{ds-frg}\right\}$ для $\forall t,q,\mu$,

где максимум берется по всем алгоритмам, применяемым криптоаналитиком противника A, которые характеризуются временной сложностью t условных единиц и количеством запросов к оракулу $S_{sk}(.,.)$, не превышающим q, суммарная длина которых плюс длина сообщения M^* не превышает μ бит.

Схема ЭЦП считается стойкой, если значение функции небезопасности при заданных параметрах не превышает заранее установленной величины. В модели пассивного противника результат, полученный участниками протокола, никак не зависит от действий противника, поэтому для доказательства безопасности схемы ЭЦП в этом случае достаточно доказать ее стойкость к подделке — нет необходимости доказывать робастность.

Определение 2 [12]. (t,n)-пороговая схема ЭЦП TS называется *стойкой к подделке*, если никакой противник A, скомпрометировавший не более t участников схемы, не может сгенерировать подпись под любым ранее не подписанным сообщением M^*, имея ансамбли всех случайных величин $View_A$(Thresh-Key-Gen) и $View_A$(Thresh-Sig), полученные противником при наблюдении за протоколами, которые выполнялись при подписании сообщений $M_1,\ldots, M_q$, выбранных противником адаптивно.

Теорема 4. Если схема ЭЦП по ГОСТ Р 34.10–2001 является стойкой к подделке в смысле определения 1, то специфицированная в табл. 1 (t,n)-пороговая схема ЭЦП на основе ГОСТ Р 34.10–2001 является стойкой к подделке в смысле определения 2 при $t \le \lfloor (n-1)/2 \rfloor$ в условиях действия пассивного противника.

Идея доказательства теоремы основана на построении алгоритма, моделирующего действия противника в наихудшем для схемы ЭЦП случае, и доказательстве того факта, что из наблюдения реального протокола противник не сможет получить информации больше, чем моделируя этот протокол самостоятельно, «в лабораторных условиях».

Пороговые схемы ЭЦП на основе ГОСТ Р 34.10–2001, стойкие к атакам активного противника, строятся на тех же принципах, но более сложным образом. Доказательство их стойкости осуществляется тем же способом, но дополнительно доказывается их робастность.

Задача защиты криптосистемы от компрометации ключей усложняется, если она имеет большое число участников. Для этого случая разработан способ защищенной рассылки сообщений среди группы из n участников криптосистемы [13]. Одним из основных средств обеспечения безопасности предложенного протокола являются пороговые схемы ЭЦП.

5. Заключение

В работе обобщены некоторые результаты исследования, направленного на разработку теоретических основ и поиск путей реализации средств и систем криптографической защиты информации, сохраняющих стойкость при компрометации части ключей. Так, на основе разработанного автором подхода к модельному представлению ключевых систем предложена и обоснована система показателей секретности, доказаны критерии секретности единиц ключевого материала. Выяснены требования к структуре ключевых систем, обеспечивающие возможность оценки секретности ключевого материала по введенной системе показателей. Доказана теорема о показателях секретности ключевой системы. Поисковая часть исследования позволила выявить и формализовать типовые элементы конструкции ключевых систем, названные схемами управления ключевым материалом. На основе одного из типов таких схем — пороговых схем разделения секрета — разрабатывается система криптографических протоколов, позволяющая строить большой набор функциональных средств для решения наиболее востребованных криптографических задач. В качестве примера, подтверждающего возможность реализации средств криптографической защиты, стойких к частичной компрометации ключей, приводится пороговая схема цифровой подписи на основе ГОСТ Р 34.10–2001.

СПИСОК ЛИТЕРАТУРЫ:

1. *Запечников С. В.* Принципы обеспечения стойкости криптосистем к компрометации ключей // Безопасность информационных технологий. 2008. № 1. С. 80–87.
2. *Запечников С. В.* Модельное представление ключевых систем средств криптографической защиты информации // Безопасность информационных технологий. 2008. № 4. С. 84–9.
3. *Bellare M.* Introduction to modern cryptography. Lecture notes. University of California at San Diego, 2007. – http://www-cse.ucsd.edu/users/mihir/cse107/index.html
4. *Архангельская А. В., Запечников С. В.* Способ вычисления псевдослучайных функций с распределенным секретным ключом // Безопасность информационных технологий. 2006. № 3. С. 44–49.
5. *ElGamal T.* A public key cryptosystem and a signature scheme based on discrete logarithm // IEEE Transactions on Information Theory. 1985. № 31. P. 469–472.
6. *Canetti R., Goldwasser S.* An efficient threshold public key cryptosystem secure against adaptive chosen ciphertext attack // Advances in Cryptology. Proc. of Eurocrypt'99, LNCS Vol. 1592. Springer-Verlag, 1999. P. 90–106.
7. *Jarecki S., Lysyanskaya A.* Adaptively secure threshold cryptography: introducing concurrency, removing erasures (extended abstract) // Advances in Cryptology. Proc. of Eurocrypt'2000, LNCS Vol. 1807. Springer-Verlag, 2000. P. 221–242.
8. *Запечников С. В.* Пороговые схемы цифровой подписи на основе ГОСТ Р 34.10–94 // Безопасность информационных технологий. 2001. № 3. С. 45–51.
9. ГОСТ Р 34.10–2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи. М., 2001.
10. *Серов Р. Е.* Пороговая схема шифрования/подписи на основе ГОСТ Р 34.10–2001 // Безопасность информационных технологий. 2004. № 3. С. 87–90.
11. *Архангельская А. В., Запечников С. В.* Схемы цифровой подписи на основе алгоритмов ГОСТ Р 34.10–2001 с применением аппарата парных отображений // Известия ТРТУ. 2006. № 7 (62). С.194–201.
12. *Canetti R., Gennaro R., Jarecki S., Krawczyk H., Rabin T.* Adaptive security for threshold cryptosystems // Advances in Cryptology. Proc. of Crypto'99, LNCS. Springer-Verlag, 1999. Vol. 1666. P. 98–115.
13. *Запечников С. В.* Защищенная рассылка сообщений в распределенных системах обработки данных в условиях действия активного адаптивного противника // Безопасность информационных технологий. 2001. № 2. С. 67–76.